

LNCS 8491

Zhipeng Cai Chaokun Wang
Siyao Cheng Hongzhi Wang
Hong Gao (Eds.)

Wireless Algorithms, Systems, and Applications

9th International Conference, WASA 2014
Harbin, China, June 23–25, 2014
Proceedings



Springer

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Zhipeng Cai Chaokun Wang Siyao Cheng
Hongzhi Wang Hong Gao (Eds.)

Wireless Algorithms, Systems, and Applications

9th International Conference, WASA 2014
Harbin, China, June 23-25, 2014
Proceedings

Volume Editors

Zhipeng Cai
Georgia State University
Department of Computer Science
34 Peachtree Street, Atlanta, GA 30303, USA
E-mail: zcai@gsu.edu

Chaokun Wang
Tsinghua University
School of Software
East Main Building, 100084 Beijing, China
E-mail: chaokun@tsinghua.edu.cn

Siyao Cheng
Hongzhi Wang
Hong Gao
Harbin Institute of Technology
School of Computer Science and Technology
Zonghe Building, No. 92 West Dazhi Street, 150001 Harbin, China
E-mail: {csy,wangzh,honggao}@hit.edu.cn

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-319-07781-9

e-ISBN 978-3-319-07782-6

DOI 10.1007/978-3-319-07782-6

Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014939958

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 9th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2014) was held during June 23–25, 2014, in Harbin, Heilongjiang, China. The conference is motivated by the recent advances in cutting-edge electronic and computer technologies that have paved the way for the proliferation of ubiquitous infrastructure and infrastructureless wireless networks. WASA is designed to be a forum for theoreticians, system and application designers, protocol developers, and practitioners to discuss and express their views on the current trends, challenges, and state-of-the-art solutions related to various issues in wireless networks.

The technical program of the conference included 41 contributed papers together with 30 invited papers, selected by the Program Committee from 134 full submissions received in response to the call for papers. All the papers were peer reviewed by the Program Committee members or external reviewers. The papers cover various topics, including cognitive radio networks, wireless sensor networks, cyber-physical systems, distributed and localized algorithm design and analysis, information and coding theory for wireless networks, localization, mobile cloud computing, topology control and coverage, security and privacy, underwater and underground networks, vehicular networks, information processing and data management, programmable service interfaces, energy-efficient algorithms, system and protocol design, operating system and middle-ware support, and experimental test-beds, models and case studies.

We would like to thank the Program Committee members and external reviewers for volunteering their time to review and discuss the conference papers. We would like to extend special thanks to the steering and general chairs of the conference for their leadership, and to the finance, publication, publicity, and local organization chairs for their hard work in making WASA 2014 a successful event. Last but not least, we would like to thank all the authors for presenting their works at the conference.

April 2014

Zhipeng Cai
Chaokun Wang
Siyao Cheng
Hongzhi Wang
Hong Gao

Organization

Steering Committee

Xiuzhen Cheng	The George Washington University, USA (Chair)
Jiannong Cao	Hong Kong Polytechnic University, Hong Kong, China
Ness Shroff	The Ohio State University, USA
Wei Zhao	University of Macau, China
PengJun Wan	Illinois Institute of Technology, USA
Ty Znati	University of Pittsburgh, USA
Xinbing Wang	Shanghai Jiao Tong University, China
Yingshu Li	Georgia State University, USA

Honorary General Chair

Jianzhong Li	Harbin Institute of Technology, China
--------------	---------------------------------------

General Chairs

Hong Gao	Harbin Institute of Technology, China
My T. Thai	University of Florida, USA

Program Chairs

Zhipeng Cai	Georgia State University, USA
Chaokun Wang	Tsinghua University, China

Publication Chairs

Chunyu Ai	University of South Carolina Upstate, USA
Anu Bourgeois	Georgia State University, USA

Publicity Chairs

Longjiang Guo	Heilongjiang University, China
Selcuk Uluagac	Georgia Institute of Technology, USA

Finance Chair

Yan Zhang	Harbin Institute of Technology, China
-----------	---------------------------------------

VIII Organization

Local Organization Chair

Hongzhi Wang

Harbin Institute of Technology, China

Workshop Chairs

Jinbao Wang

Harbin Institute of Technology, China

Bo Yu

Chinese Academy of Sciences, China

Guilin Li

Xiamen University, China

Haiwei Pan

Harbin Engineering University, China

Program Committee

Habib M. Ammari

University of Michigan-Dearborn, USA

Zhipeng Cai

Georgia State University, USA

Ning Cao

Google Inc., USA

Mihaela Cardei

Florida Atlantic University, USA

Ionut Cardei

Florida Atlantic University, USA

Xiuzhen Cheng

The George Washington University, USA

Siyao Cheng

Harbin Institute of Technology, China

Song Ci

University of Nebraska-Lincoln, USA

Hongwei Du

Harbin Institute of Technology Shenzhen

Graduate School, China

Xiaofeng Gao

Shanghai Jiao Tong University, China

Mohammad Husain

University at Buffalo, USA

Hwangnam Kim

Korea University, Korea

Donghyun Kim

North Carolina Central University, USA

Ming Li

Utah State University, USA

Minming Li

City University of Hong Kong, China

Yingshu Li

Georgia State University, USA

Qun Li

College of William and Mary, USA

Pan Li

Mississippi State University, USA

Manki Min

South Dakota State University, USA

Thomas Nolte

Mälardalen University, Sweden

Zhou Su

Waseda University, USA

Zhi Sun

University at Buffalo, USA

Xiaohua Tian

Shanghai Jiao Tong University, China

Pengjun Wan

Illinois Institute of Technology, USA

Chaokun Wang

Tsinghua University, China

Yu Wang

University of North Carolina at Charlotte, USA

Qian Wang

Wuhan University, China

Xiaoming Wang

Shaanxi Normal University, USA

Jianping Wang

City University of Hong Kong, China

Xinbing Wang

Shanghai Jiao Tong University, China

Kui Wu

University of Victoria, USA

Xiaofu Wu	Nanjing University of Posts and Telecommunications, China
Jiang Xie	University of North Carolina at Charlotte, USA
Kai Xing	University of Science and Technology, China
Kuai Xu	Arizona State University, USA
Xiaohua Xu	Illinois Institute of Technology, USA
Dong Xuan	The Ohio State University, USA
Jianguo Yao	Shanghai Jiao Tong University, China
Chi Zhang	University of Science and Technology, China
Lichen Zhang	Shaanxi Normal University, China
Yanxiao Zhao	South Dakota School of Mines and Technology, USA
Liang Zhou	Nanjing University of Posts and Telecommunications, China
Haojin Zhu	Shanghai Jiao Tong University, China

Additional Reviewers

Bi, Ran	Sun, Jizhou
Ferreira, Joaquim	Sun, Xianwei
Huang, Jun	Wang, Boyang
Kim, Hyunbum	Willig, Andreas
Li, Jun	Wu, Yueshi
Li, Mohan	Zhang, Lichen
Liang, Wanchao	Zhang, Yuncong
Liu, Xueli	Zhao, Chang
Luo, Yu	Zhao, Sheng-Mei
Miao, Dongjing	Zhu, Haojin
Mihnea, Amalya	Zhu, Xudong
Pu, Lina	Zhuo, Shuguo
Sun, Guobao	

Table of Contents

Inter-service Time Guaranteed Scheduling in Wireless Networks..... <i>Xu Zheng, Jianzhong Li, and Hong Gao</i>	1
Wear-Leveling Optimization of Android YAFFS2 File System for NAND Based Embedded Devices	12
<i>Yuqiu Qian, Junjie Lu, and Kai Xing</i>	
Web Map Service Log Analysis	22
<i>Xiaofei Wang, Di Chen, Gan Lu, Yue Peng, and Chengchen Hu</i>	
NC-STP: A High Performance Network Coding Based Space Transport Protocol	34
<i>Hai Fu, Wanrong Yu, Chunqing Wu, Baokang Zhao, and Zhenqian Feng</i>	
Implementing the Matrix Inversion by Gauss-Jordan Method with CUDA	44
<i>Ning Tian, Longjiang Guo, Meirui Ren, and Chunyu Ai</i>	
Operator Scale Out Using Time Utility Function in Big Data Stream Processing	54
<i>Mahammad Humayoo, Yanlong Zhai, Yan He, Bingqing Xu, and Chen Wang</i>	
A New Channel Allocation Scheme for Vehicle Communication Networks	66
<i>Jing Xu, Wei Li, Zan Ma, and Shuo Zhang</i>	
Throughput Prediction-Based Rate Adaptation for Real-Time Video Streaming over UAVs Networks	78
<i>Tongqing Zhou, Haidong Zhang, Ming Xu, and Yingwen Chen</i>	
Table-Driven Bus-Based Routing Protocol for Urban Vehicular Ad Hoc Networks	90
<i>Tabouche Abdeldjalil, Fan Li, Ruiling Li, and Xin Li</i>	
Vehicular Ad Hoc Networks: Architectures, Research Issues, Challenges and Trends	102
<i>Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Yunchuan Sun, and Rongfang Bie</i>	

Empirical Study on Spatial and Temporal Features for Vehicular Wireless Communications	114
<i>Yingwen Chen, Ming Xu, Pei Li, and Bin Zhang</i>	
Schedule Algorithms for File Transmission in Vehicular Ad Hoc Networks	126
<i>Chao Wang, Maya Larson, Yingwen Chen, and Xiumei Fan</i>	
Joint Neighbor Discovery and Contention Relationship Inference in Wireless Networks	138
<i>Guanbo Zheng and Rong Zheng</i>	
An Improved Approximation Algorithm for the Shortest Link Scheduling Problem in Wireless Networks under SINR and Hypergraph Models	150
<i>Cui Wang, Jiguo Yu, Dongxiao Yu, and Baogui Huang</i>	
MIMO-Aware Spectrum Access and Scheduling in Multi-hop Multi-channel Wireless Networks	161
<i>Lin Luo, Dengyuan Wu, and Hang Liu</i>	
Minimized Gateway Placement in Hybrid Wireless Network	173
<i>Hao Wang and Hong Gao</i>	
Design and Analysis of a Downlink Multi-User MIMO MAC Protocol in WLANs	183
<i>Chao Guo, Changle Li, and Huiying Liu</i>	
RLNC in Practical Wireless Networks	194
<i>Kyu-Hwan Lee, Jae-Hyun Kim, and Sunghyun Cho</i>	
Accuracy Evaluation for Sensed Data	205
<i>Yan Zhang and Hongzhi Wang</i>	
Maximizing Probability of Data Packet Delivery within Deadline	215
<i>Ran Bi, Hong Gao, and Quan Chen</i>	
Model-Based Approximate Event Detection in Heterogeneous Wireless Sensor Networks	225
<i>Jing Gao and Jianzhong Li</i>	
Structural Health Monitoring Based on RealAdaBoost Algorithm in Wireless Sensor Networks	236
<i>Zhuorong Li, Junqi Guo, Wenshuang Liang, Xiaobo Xie, Guangzhi Zhang, and Shenling Wang</i>	
Probabilistic Threshold Based Monitoring Using Sensor Networks	246
<i>Ran Bi, Hong Gao, and Yingshu Li</i>	

Topology-Transparent STDMA Protocol with MIMO Link for Multicast and Unicast in Ad Hoc Networks.....	256
<i>Yueyang Song, Changle Li, Chao Guo, and Yu Zhang</i>	
Secure Device-to-Device Authentication in Mobile Multi-hop Networks	267
<i>Hyunsoo Kwon, Changhee Hahn, Daeyoung Kim, Kyungtae Kang, and Junbeom Hur</i>	
A New Representation of Photoplethysmography Signal.....	279
<i>Dazhou Li, Hai Zhao, Sinan Li, and Huanxia Zheng</i>	
Energy Efficient Social-Based Routing for Delay Tolerant Networks.....	290
<i>Chenfei Tian, Fan Li, Libo Jiang, Zeye Wang, and Yu Wang</i>	
Contract Theory for Incentive Mechanism Design in Cooperative Relaying Networks	302
<i>Yinshan Liu, Xiaofeng Zhong, Yang Yan, Jing Wang, and Walid Saad</i>	
Object-Oriented Big Data Security Analytics: A Case Study on Home Network Traffic	313
<i>Kuai Xu, Feng Wang, Richard Egli, Aaron Fives, Russell Howell, and Odayne McIntyre</i>	
SPS: A Novel Semantics-Aware Scheme for Location Privacy in People-Centric Sensing Network	324
<i>Ziling Wei, Baokang Zhao, and Jinshu Su</i>	
A Novel Resource-Efficient Privacy Amplification Scheme: Towards Ground-Satellite Quantum Key Distribution Post-processing	336
<i>Zhenning Zhang, Chunqing Wu, Baokang Zhao, and Bo Liu</i>	
Protecting Location Privacy Based on Historical Users over Road Networks	347
<i>Qilong Han, Hongbin Zhao, Zhiqiang Ma, Kejia Zhang, and Haiwei Pan</i>	
Towards More Secure Cardholder Verification in Payment Systems	356
<i>Abdulrahman Alhothaily, Arwa Alrawais, Xiuzhen Cheng, and Rongfang Bie</i>	
Fortifying Barrier-Coverage of Wireless Sensor Network with Mobile Sensor Nodes	368
<i>Biaoifei Xu, Donghyun Kim, Deying Li, Joonglyul Lee, Huaipan Jiang, and Alade O. Tokuta</i>	
2- <i>m</i> -Domatic Partition in Homogeneous Wireless Sensor Networks	378
<i>Lili Jia, Jiguo Yu, Dongxiao Yu, and Qingbo Zhang</i>	

Barrier Coverage Using Sensors with Offsets	389
<i>Haosheng Fan, Victor C.S. Lee, Minming Li, Xiao Zhang, and Yingchao Zhao</i>	
A Distance Ratio-Based Algorithm for Indoor Localization in Wireless Sensor Networks	401
<i>Xi-ruo Lu, Jian-xin Chen, Xuan-cheng Zhou, Yi Dong, and Liang Zhou</i>	
On Effectiveness of Clustering Principles in Maximizing Wireless Sensor Network Lifespan	412
<i>Xiaohui Kuang, Bowen Li, and Li Liu</i>	
Predictive Nearest Neighbor Queries over Uncertain Spatial-Temporal Data	424
<i>Jinghua Zhu, Xue Wang, and Yingshu Li</i>	
The Tempo-spatial Properties of Information Dissemination to Time-Varying Destination Areas in Mobile Opportunistic Networks	436
<i>Xia Wang, Shengling Wang, Wenshuang Liang, Jianhui Huang, Rongfang Bie, and Dechang Chen</i>	
Beamforming Design for Cognitive Bidirectional Relay Networks with Imperfect CSI	446
<i>Ruiqi Xue, Meng Zhang, Hui Yu, Hanwen Luo, and Huijiang Zhi</i>	
A Comparative Study on Full- and Half-Duplex Relaying Protocols with Practical Channel Estimates	458
<i>Youyun Xu and Xiaochen Xia</i>	
Identifying Missing and Spurious Interactions in Directed Networks	470
<i>Xue Zhang, Chengli Zhao, Xiaojie Wang, and Dongyun Yi</i>	
Online Auction Based Relay Selection for Cooperative Communications in CR Networks	482
<i>Tao Jing, Fan Zhang, Wei Cheng, Yan Huo, and Xiuzhen Cheng</i>	
Channel Selection for Rendezvous with High Link Stability in Cognitive Radio Network	494
<i>Zhenhua Han, Haisheng Tan, Yongcai Wang, and Jipeng Zhou</i>	
Game Theoretic Joint Beamforming and Power Allocation for Cognitive MIMO Systems with Imperfect Channel State Information	507
<i>Feng Zhao, Jiayi Zhang, and Rongfang Bie</i>	
Channel Allocation in Sociability-Assisted Cognitive Radio Networks Using Semi-definite Programming	519
<i>Zhen Li, Tao Jing, Yan Huo, Lili Pan, and Wei Zhou</i>	

Game-Theoretic Joint Power Allocation and Feedback Rate Control for Cognitive MIMO Systems with Limited Feedback	531
<i>Feng Zhao, Chen Wang, and Rongfang Bie</i>	
A Multi-model Based Range Query Processing Algorithm for the WSN	542
<i>Guilin Li, Xing Gao, Longjiang Guo, Juncong Lin, and Ying Gao</i>	
Secure Authentication Scheme Using Dual Channels in Rogue Access Point Environments	554
<i>Arwa Alrawais, Abdulrahman Alhothaily, and Xiuzhen Cheng</i>	
Approximate Self-Adaptive Data Collection in Wireless Sensor Networks	564
<i>Bin Wang, Xiaochun Yang, Wanyu Zang, and Meng Yu</i>	
R-Focus: A Rotating Platform for Human Detection and Verification Using Electronic and Visual Sensors	576
<i>Fan Yang, Yiran Xuan, Sihaoy Ding, Adam C. Champion, and Yuanfang Zheng</i>	
QS-PS: A New Approach for Emergency Packet Delivery in WBAN	589
<i>Ming Li, Jing Liu, Qiang Shen, and Bin Yuan</i>	
Resource Allocation for Uplink-Downlink Cellular Network with Small Cells and Relays Enhanced	601
<i>Yisha Lou, Meng Zhang, Hui Yu, Hanwen Luo, and Haiquan Wang</i>	
A Priority-Based Access Control Model for Device-to-Device Communications Underlaying Cellular Network Using Network Calculus	613
<i>Jun Huang, Zi Xiong, Jibi Li, Qianbin Chen, Qiang Duan, and Yanxiao Zhao</i>	
A Privacy Threat in 4th Generation Mobile Telephony and Its Countermeasure	624
<i>Changhee Hahn, Hyunsoo Kwon, Daeyoung Kim, Kyungtae Kang, and Junbeom Hur</i>	
Enabling Smartphone Based HD Video Chats by Cooperative Transmissions in CRNs	636
<i>Tao Jing, Xuewei Cui, Wei Cheng, Shixiang Zhu, and Yan Huo</i>	
A Transparent Correlation-Based Scheme for Energy Efficient Context Sensing and Fusion under Android Systems	648
<i>Nicholas Capurso, Liran Ma, Tianyi Song, and Xiuzhen Cheng</i>	
Exploiting and Defending Trust Models in Cooperative Spectrum Sensing	660
<i>David Jackson, Wanyu Zang, Qijun Gu, and Wei Cheng</i>	

Towards Reliable and Real-Time Routing with Active Slot Augmentation in Low-Duty-Cycle WSNs	672
<i>Quan Chen and Hong Gao</i>	
IDUC: An Improved Distributed Unequal Clustering Protocol for Wireless Sensor Networks	682
<i>Chuanqing Chen, Xin Gu, Jiguo Yu, and Dongxiao Yu</i>	
OFDP: A Distributed Algorithm for Finding Disjoint Paths with Minimum Total Energy Cost in Wireless Sensor Networks	694
<i>Kejia Zhang, Hong Gao, Guisheng Yin, and Qilong Han</i>	
Information Theory Based Opportunistic Sensing in Radar Sensor Networks	706
<i>Ishrat Maherin and Qilian Liang</i>	
Isolate Safe Area Detection for Rescue in Wireless Sensor Networks	718
<i>Chunyu Ai and Frank Haizhon Li</i>	
Multi-Hierarchies: Accurately Computing Realtime Statistical Measures on Data Streams	729
<i>Penghe Qi and Shengfei Shi</i>	
Iceberg Cube Query on Heterogeneous Information Networks	740
<i>Dan Yin and Hong Gao</i>	
An Energy Optimization Algorithm of Date Centers Base on Price Volatility	750
<i>Liang Hao, Gang Cui, Wende Ke, and Bindi You</i>	
Keyword Search on Graphs Based on Content and Structure	760
<i>Zhiqiang Zhang, Deping Xia, and Xiaoqin Xie</i>	
Max-Weight Algorithm for Mobile Data Offloading through Wi-Fi Networks	773
<i>Shirong Lin, Zhijun Li, and Shouxu Jiang</i>	
Capture Missing Values Based on Crowdsourcing	783
<i>Chen Ye and Hongzhi Wang</i>	
Sectional and Conditional Functional Dependencies	793
<i>Mingda Li, Hongzhi Wang, and Ye Li</i>	
Author Index	805

Inter-service Time Guaranteed Scheduling in Wireless Networks

Xu Zheng, Jianzhong Li, and Hong Gao

School of Computer Science and Technology,
Harbin Institute of Technology, Heilongjiang, China
`zhengxuhit@gmail.com, {lijzh,honggao}@hit.edu.cn`

Abstract. The regularity of inter-service time is essential for processing real-time traffic in wireless networks. Bounding the size of inter-service time for every single user is a precondition to support the normal operating of the network. Motivated by this, we design a framework for inter-service time guaranteed scheduling. We first define a new capacity region of networks with a strict inter-service time constraint. Then we propose a novel scheduling policy that is throughput-optimal and guarantees a bounded inter-service time for every user. Simulation results shows the policy performs well on inter-service time and throughput.

Keywords: Wireless Networks, Real-time Traffic, Inter-service Time, Scheduling Policy.

1 Introduction

As mobile devices and wireless communication technology keep improving in recent years, there have been more and more complicated wireless networks based applications like cyber physical systems, mobile social networks, etc. Real-time traffic occurs frequently in these applications. For example, in a cyber physical system, a packet must be delivered to the base or cluster head before its bringing ground truth[5][11] goes out of date. Real-time traffic often has some quality-of-service requirements besides the basic need of throughput and saving in the bandwidth[1]. These QoS requirements mainly include regularity of the inter-service times, packet delay constraints, packet delivery ratio and so on[4][3]. As we know, such requirements fail to be captured by those works that only focus on the optimality of throughput performance. Some efforts have been made to improve different aspects of QoS. For example, many scheduling policies [7] [8] are proposed to handle the transmitting of packets with deadlines. These policies differ in their definitions of delay constraints. And the performance of packet delivery ratio is considered in [9].

Inter-service time is the time between two consecutive services for a user, and regularizing the inter-service time means a user can get a second chance to transmit in less than a bounded period of time since its last transmission. The regularity of the inter-service time is a precondition to support real-time applications like multi-media streaming [12], and also an index to assess the

performance of real-time traffic. Only very few works study the regularity of the inter-service times [12][10]. Li. designs a new scheduling policy [12] that keeps the stability of the system under an arriving rate vector while ensuring the regularity of inter-service time. The policy is mainly designed to achieve a provable performance on the mean value of inter-service time. It may perform poorly on the throughput when bounding the inter-service time of single users. It is also non-trivial to determine parameters in the scheduling policy when the system hopes to regulate the inter-service time of every single user. Such a regulation is actually essential even when the mean value of inter-service time is bounded. A user may grow into impatience with large inter-service time, even though his real-time traffic is in fact supportable. In general, some problems remain open when the system has a strict constraint on the length of inter-service time of every user: The set of arriving rate vectors under which the system is stable and each user keeps a guarantee on the inter-service time. And if there is a scheduling policy that supports such set of arriving rate vectors while meets the requirement on service regularity.

In this work, we focus on designing a scheduling policy that keeps the wireless network stable while provides a guarantee on the regularity of inter-service time for each user. The contributions of this paper are: 1) We formulate the problem of service regularity guaranteed scheduling in wireless network. 2) We propose a novel max-weight type scheduling policy in which the inter-service time of any user is exactly below the required upper bound. 3) Simulation results indicate that our scheduling policy can meet the inter-service time constraint and performs well on the stability of networks.

The rest of the paper is organized as follow: In section 2, we bring a literature review on the development of scheduling policies in wireless network. In section 3, we introduce the network model used by our work. In section 4, the novel scheduling policy is proposed. In section 5, we prove some properties of the scheduling policy. In section 6, we show the simulation results of our scheduling policy. And section 7 concludes the paper.

2 Related Work

The design of scheduling policy is a fundamental task in the design of wireless networks. It is well-known that the Max Weight scheduling policy is throughput-optimal[14]. However, the problem of finding the disjoint set of links with max weight is NP-Hard. Hence, a max-weight scheduling policy incurs high overhead. There have been many efforts to design low complexity scheduling policies with throughput performance guarantees. Most of them focused on finding a *maximal weight independent set (MWIS)* of links. Sakai[13] and Wan[15] designed centralized policies that could find a MWIS with provable ratio bounds. Basagni[2],Hoepman[6], etc. separately proposed distributed scheduling policies for different network models. However, none of these works dealt with the QoS requirements of users.

Some scheduling policies were designed to meet the packet delay constraint for each[7] [8][9]. They all partitioned the time into frames, and packets would run

out of time before the end of their arriving frames. They mainly differed in the introducing of channel fading[7], nonidentical delays[8], etc. Kang[9] proposed a new policy that accommodated packet delivery ratio.

For all we know, very few works[12] [10] dealt with the performance of inter-service time. Li[12] used a new type of weight to capture the inter-service time performance. The weight was a combination of queue length and *time-since-last-service*. Then under the max weight scheduling policy, a user could get a second service with a growing probability as the *time-since-last-service* increased. And the inter-service time could be regulated. Li[10] extended his work to consider the inter-service time performance of rate vectors close to the edge of capacity region. Li's works failed in the situation when the inter-service time of each user is strictly bounded and one hopes to know the exactly set of arriving rate vectors that can meet the boundary.

3 Network Model

In our network, N users hope to transmit to a common destination via the same channel. Time is partitioned into slot, and in each slot only one user can communicate with the destination due to the destructive interference in wireless communication. In each slot, $A_i[t]$ packets arrive in user i . $A_i[t]$ is randomly and identically distributed over time with the expectation $E(A_i[t]) = \lambda_i$. These packets will join the delivering queue and be transmitted to the destination. We assume that the wireless channel is alway in good condition, and user i can send r_i packets in a slot. In our model, both λ_i s and r_i s are heterogeneous, which indicates the fact that the size of traffic and communication capability of different mobile device are often various.

We use boolean variable $S_i[t] \in \{0, 1\}$ to denote whether user i is scheduled in slot t . Only one user can be scheduled in each slot, thus we have

$$\sum_{i=1}^N S_i[t] = 1. \quad (1)$$

for arbitrary slot t .

$Q_i[t]$ is the size of packets waiting for transmission at user i at the beginning of slot t . $Q_i[t]$ is determined by three parts: $Q_i[t - 1]$, $A_i[t - 1]$ and $r_i S_i[t - 1]$, with the following equation:

$$Q_i[t] = \text{Max}\{Q_i[t - 1] + A_i[t - 1] - r_i S_i[t - 1], 0\} \quad (2)$$

$Q_i[t] = 0$ means that user i has delivered all its packets in slot $t - 1$.

Now we formalize the stability of networks by the following definitions.

Definition 1. *We say that the network is stable under an arriving rate vector if the underlying Markov chain $Q_i[t]$ is positive recurrent for each user, and*

$$\lim_{t \rightarrow \infty} \sum_{i=1}^N Q_i[t] \leq \infty$$

An arriving rate vector $\lambda = \{\lambda_i\}_{i=1,\dots,N}$ is *supported* by a network if the network is stable under λ by utilizing some scheduling policy. All supportable rate vectors compose the *capacity region* of the network, denoted by Λ .

Definition 2. A scheduling policy is throughput-optimal for a network if $\Lambda' = \Lambda$, where Λ' is the set of rate vectors supported by the network when using the scheduling policy.

Inter-service time is the number of slots between two consecutive transmission of a user. We use $T_i[m]$ to denote the number of time slots between the $m - 1$ th and m th transmissions of user i . Accordingly, $T_i = \lim_{m \rightarrow \infty} \frac{\sum_{j=1}^m T_i[j]}{m}$ is the long-term average inter-service time of user i .

In this paper, we focus on the network model with an extra constraint that $T_i \leq N + \epsilon, \forall i$, where ϵ is a non-negative real. Then the network is not only required to be stable, but also guarantees a bounded inter-service time for all users. ϵ is always non-negative since N is the lower bound for the constraint, and the proof is trivial. Then we can extend the definitions of stability, capacity region and throughput-optimal scheduling policies.

Definition 3. We say that the network is ϵ -stable under a rate vector λ if the network is stable and $T_i \leq N + \epsilon, \forall i$

The definitions of ϵ -supportable and ϵ -capacity region Λ_ϵ are similar.

Definition 4. A scheduling policy is ϵ -throughput-optimal for a network if $\Lambda'_\epsilon = \Lambda_\epsilon$, where Λ'_ϵ is the set of rate vectors ϵ -supported by the network when using the scheduling policy.

Our objective is to design a scheduling policy that is ϵ -throughput optimal for our network model.

4 Service-Guaranteed Maximum Weight Scheduling Policy

In this section, we propose our scheduling policy. The novel scheduling policy is a max weight type policy, while guaranteeing an upper bound on the average inter-service time of all users. We call this policy *Service-Guaranteed Maximum Weight* scheduling (SGMW for short).

SGMW partitions time into equal sized intervals. Each interval contains $N + \epsilon$ slots, where $N + \epsilon$ is the upper bound of the average inter-service time.

In each interval, the scheduling policy is composed of two components: *loose phase* and *tight phase*. The policy first starts in loose phase at the beginning of each interval. In loose phase, all users compete for the channel, and our policy is the same as maximum-weight scheduling. SGMW goes into tight phase when the number of time slots left in an interval is the same as the number of users that have not been scheduled in this interval. In tight phase, the policy repeatedly chooses the user whose weight is largest among the set of users never scheduled

in current interval. Obviously, the tight phase lasts until the end of the interval. An interval will terminate before $N + \epsilon$ slots if all the users have been scheduled at least once. Then the scheduling policy turns into the next interval.

The weight of user i at time slot t is calculated by the following equation:

$$w_i[t] = \frac{I_i[t]Q_i[t]}{r_i} \quad (3)$$

$Q_i[t]$ is the length of packets at user i at the beginning of slot t , r_i is transmission rate. $I_i[t] = -1$ when the policy is in tight phase and the user has been scheduled in current interval, and $I_i[t] = 1$ otherwise.

Our scheduling policy is a maximum-weight type policy and here is an instance about how it processes.

Example There are two users in the network, with $A_1[t] = \lambda_1$, $A_2[t] = \lambda_2$, $\frac{\lambda_1}{r_1} = \frac{1}{2}$, $\frac{\lambda_2}{r_2} = \frac{1}{8}$, $\epsilon = 1$, so the upper bound of average inter-service time is 3. In slot 1, the SGMW is in loose phase. $w_1[1] = \frac{1}{2}$, $w_2[1] = \frac{1}{8}$, then user 1 is scheduled. In slot 2, the SGMW is still in loose phase because there are 2 slots left and only user 2 has not been scheduled. $w_1[2] = \frac{1}{2}$, $w_2[2] = \frac{1}{4}$, user 1 is scheduled. In slot 3, the SGMW turns to the tight phase. $w_1[3] = -\frac{1}{2}$ since user 1 has been scheduled in current interval. $w_2[3] = \frac{3}{8}$, user 2 is scheduled. In slot 4, a new interval begins, and the process repeats. Figure 1. shows the evolution of the network during an interval.

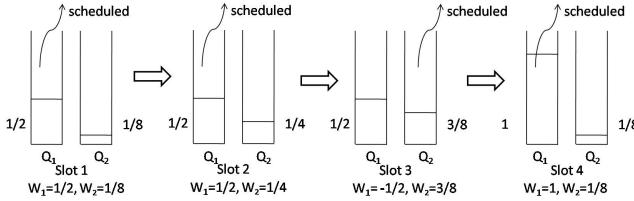


Fig. 1. An Instance of SGMW

The time complexity of the policy in each time slot is $O(N)$, the space complexity is $O(N)$.

5 Properties of SGMW

In subsection 5.1, we prove that SGMW is ϵ -throughput-optimal. We first put forward a necessary condition for a rate vector to be ϵ -supportable. Then we prove that SGMW can support all rate vectors following the necessary condition. SGMW can also bound the average inter-service time for each user, thus it is ϵ -throughput-optimal. In subsection 5.2, we derive the ratio between ϵ -capacity region and the original capacity region. The inter-service time guarantee of a given rate vector is discussed at the last of this section.

5.1 ϵ -throughput Optimal

We first give the necessary condition for a rate vector to be ϵ -supportable.

Lemma 1. *For any arriving rate vector $\lambda = \{\lambda_i\}_i$ that is ϵ -supportable by a network with some scheduling policies, $\sum_{i=1}^N \text{Max}\{\frac{\lambda_i * (N+\epsilon)}{r_i} - 1, 0\} \leq \epsilon$*

Proof. We prove the lemma by contradiction. Assume $\lambda' = \{\lambda'_i\}_i$ is an ϵ -supportable arriving rate vector, and $\sum_{i=1}^N \text{Max}\{\frac{\lambda'_i * (N+\epsilon)}{r_i} - 1, 0\} \geq \epsilon$.

The number of slots that user i is scheduled during a long period of T slots is no less than $\frac{T}{N+\epsilon}$. $Q'_i[T]$ denotes the number of packets that fail to be delivered by user i in these $\frac{T}{N+\epsilon}$ basic scheduling,

$$\sum_{i=1}^N E(Q'_i[T]) = \frac{T}{N+\epsilon} \sum_{i=1}^N \text{Max}\{\frac{\lambda'_i * (N+\epsilon)}{r_i} - 1, 0\}$$

There are in total $T - N * \frac{T}{N+\epsilon}$ extra slots except the basic scheduling for all users. The expectation of total queue length is estimated as follow:

$$\begin{aligned} E(\sum_{i=1}^N Q_i[T]) &= \sum_{i=1}^N E(Q_i[T]) = \sum_{i=1}^N E(Q'_i[T]) - (T - N * \frac{T}{N+\epsilon}) * 1 \\ &= \frac{T}{N+\epsilon} (\sum_{i=1}^N \text{Max}\{\frac{\lambda'_i * (N+\epsilon)}{r_i} - 1, 0\} - \epsilon) \end{aligned} \tag{4}$$

According to the constraint that $\sum_{i=1}^N \text{Max}\{\frac{\lambda'_i * (N+\epsilon)}{r_i} - 1, 0\} \geq \epsilon$,

$$E(\sum_{i=1}^N Q_i[T]) \rightarrow +\infty \text{ as } T \rightarrow +\infty$$

Then the network is instable under λ' , which contradicts with the assumption. So the condition $\sum_{i=1}^N \text{Max}\{\frac{\lambda_i * (N+\epsilon)}{r_i} - 1, 0\} \leq \epsilon$ holds for all ϵ -supportable rate vectors. \square

Lemma 2 proves that SGMW can support all the rate vectors following the condition in lemma 1.

Lemma 2. *For any arriving rate vector $\lambda = \{\lambda_i\}_i$ with the condition that $\sum_{i=1}^N \text{Max}\{\frac{\lambda_i * (N+\epsilon)}{r_i} - 1, 0\} \leq \epsilon$, the network is stable by utilizing the SGMW.*

Proof. Each interval can be partitioned into two parts: *Round Robin* stage and *Max Weight* stage. The round robin stage is composed of N slots, one for each user. The max weight stage includes ϵ slots, and the user with largest weight in each of these slots is scheduled. Slots of two stages may appear crosswise with each other. A slot belongs to the round robin stage if it is the only slot that the user transmits in current interval. And if a user transmits multi times, arbitrary one of them belongs to the round robin stage.

Then we are about to prove the system is stable in both of the two stages. For any user i ,

$$\frac{\lambda_i}{r_i} = \begin{cases} \frac{\lambda_i}{r_i} + 0 & \text{when } \frac{\lambda_i}{r_i} \leq \frac{1}{N+\epsilon} \\ \frac{1}{N+\epsilon} + (\frac{\lambda_i}{r_i} - \frac{1}{N+\epsilon}) & \text{when } \frac{\lambda_i}{r_i} > \frac{1}{N+\epsilon} \end{cases}.$$

The first part of the right side of the equation is supportable in the Round Robin stage since it is no larger than $\frac{1}{N+\epsilon}$.

The second part of the right side is supported by the Max Weight stage, which can be deduced as follow:

$$\sum_{i=1}^N \max\left\{\frac{\lambda_i}{r_i} - \frac{1}{N+\epsilon}, 0\right\} = \frac{1}{N+\epsilon} \sum_{i=1}^N \max\left\{\frac{\lambda_i * (N+\epsilon)}{r_i} - 1, 0\right\} \leq \frac{\epsilon}{N+\epsilon} \quad (5)$$

The network is stable in its Max Weight stage when $t * \sum_{i=1}^N \max\left\{\frac{\lambda_i}{r_i} - \frac{1}{N+\epsilon}, 0\right\} \leq \frac{t}{N+\epsilon} * \epsilon$, just as what is proved in (5).

Then the rate vector is supportable under our interval-based scheduling policy SGMW. \square

Lemma 3 is to prove SGMW can also keep a bound on the inter-service time for all users.

Lemma 3. *If an arriving rate vector $\lambda = \{\lambda_i\}_i$ is supported by SGMW, the average inter-service time T_i of any user i is no more than $N + \epsilon$.*

Proof Sketch: Time slots are partitioned into intervals in SGMW, and length of each interval is less than $N + \epsilon$. Each user can be scheduled at least once in each interval, thus the number of service for any user is no less than $\frac{t}{N+\epsilon}$, and average inter-service time T_i of any user i is no more than $t / \frac{t}{N+\epsilon} = N + \epsilon$. \square

SGMW is then ϵ -throughput optimal by combining lemma 2 and lemma 3.

5.2 Discussion

The constraint on inter-service time reduces the size of capacity region. This is due to the fact that some users with long queue and large arriving rate have to wait for other users to meet the constraint, and length of their queues could possibly trend to infinity. A smaller ϵ often leads to larger decrease in capacity region since the waiting appears more frequently. We formulate the decreasing in theorem 2. Lemma 4 estimates the size of vector space composed by all vectors $k = (k_1, k_2, \dots, k_N)$ that follow $k_i \geq 0, \forall i$ and $\sum_1^N k_i \leq \beta$. The result of lemma 4 is applied for the proof of theorem 2.

Lemma 4. *For any vector $k = (k_1, k_2, \dots, k_N)$, $\oint_0^\beta 1 d\sigma = \frac{\beta^n}{n!}$ if $k_i \geq 0, \forall i$ and $\sum_1^N k_i \leq \beta$. $\oint_0^\beta 1 d\sigma$ is a multiple integration on the N dimensions, also defined as the size of vector space composed of all vectors like k .*

Proof. We prove the lemma by induction.

Obviously, when $N = 1$, $\oint_0^\beta 1 d\sigma = \beta$, when $N = 2$, $\oint_0^\beta 1 d\sigma = \frac{\beta^2}{2}$.

Assume $\oint_0^\beta 1d\sigma = \frac{\beta^k}{k!}$ is true when $N = k$. When $N = k + 1$,

$$\oint_0^\beta 1d\sigma = \int_0^\beta \oint_\beta^0 1d\sigma' dx \quad (6)$$

where σ' is a k -dimensional space with $\sum_{i=1}^k r_i \leq \beta - r_{k+1}$, and

$$\begin{aligned} \int_0^\beta \oint_\beta^0 1d\sigma' dx &= \int_0^\beta \frac{(\beta - x)^n}{n!} dx = - \int_\beta^0 \frac{(\beta - x)^n}{n!} d(\beta - x) = - \int_\beta^0 \frac{(y)^n}{n!} d(y) \\ &= - \frac{1}{(n+1)!} (y)^{n+1}|_\beta^0 = \frac{\beta^{n+1}}{(n+1)!} \end{aligned}$$

Theorem 2 gives the ratio between ϵ -capacity region and the original one.

Theorem 1. *The size of ϵ -capacity region Λ_ϵ of a network is no more than $\frac{N!}{(N+\epsilon)^N} \sum_{i=0}^N \frac{C_N^i}{i!} \epsilon^i$ of its original capacity region Λ .*

Proof. Based on lemma 1, $\sum_{i=1}^N \text{Max}\left\{\frac{\lambda_i*(N+\epsilon)}{r_i} - 1, 0\right\} \leq \epsilon$ holds for any rate vector inside the ϵ -capacity region. We denote $\frac{\lambda_i}{r_i}$ as k_i , and rewrite the inequality as follow:

$$\sum_{i=1}^N \text{Max}\left\{k_i - \frac{1}{N+\epsilon}, 0\right\} \leq \frac{\epsilon}{N+\epsilon} \quad (7)$$

Assume there are t users with $k_i \geq \frac{1}{N+\epsilon}$, $i = 0, 1, \dots, N$, and we define σ_t as the size of vector space.

$$\sigma_t = C_N^t \oint_0^{\frac{\epsilon}{N+\epsilon}} 1d\sigma'_t * \left(\frac{1}{N+\epsilon}\right)^{N-t} \quad (8)$$

C_N^t is the combinatorial number of picking t out of N . The second part $\oint_0^{\frac{\epsilon}{N+\epsilon}} 1d\sigma'_t$ is the size of space composed by the vector $\{k_1 - \frac{1}{N+\epsilon}, k_2 - \frac{1}{N+\epsilon}, \dots, k_t - \frac{1}{N+\epsilon}\}$, where $\sum_{i=0}^t (k_i - \frac{1}{N+\epsilon}) \leq \frac{\epsilon}{N+\epsilon}$, and $k_i \geq \frac{1}{N+\epsilon}$ for $i = 1, \dots, t$. The third part $(\frac{1}{N+\epsilon})^{N-t}$ is the vector space of the users whose $k_i \leq \frac{1}{N+\epsilon}$. According to lemma 4, $\oint_0^{\frac{\epsilon}{N+\epsilon}} 1d\sigma'_t = \frac{\epsilon^t}{t!(N+\epsilon)^t}$. we add up all the σ_t from $t = 0$ to $t = N$,

$$\begin{aligned} \sigma &= \sum_{t=0}^N \sigma_t = \sum_{t=0}^N C_N^t \oint_0^{\frac{\epsilon}{N+\epsilon}} 1d\sigma'_t * \left(\frac{1}{N+\epsilon}\right)^{N-t} \\ &= \sum_{t=0}^N C_N^t \frac{\epsilon^t}{t!(N+\epsilon)^t} * \left(\frac{1}{N+\epsilon}\right)^{N-t} = \left(\frac{1}{N+\epsilon}\right)^N \sum_{t=0}^N \frac{C_N^t \epsilon^t}{t!} \end{aligned} \quad (9)$$

The size of original capacity region is $\Lambda = \frac{1}{N!}$, thus $\Lambda_\epsilon / \Lambda \leq \frac{N!}{(N+\epsilon)^N} \sum_{t=0}^N \frac{C_N^t \epsilon^t}{t!}$

SGMW can achieve the best performance when it is always in the loose phase. Such situations occur when the constraint $N + \epsilon$ is larger than the max inter-service time of users under the max-weight scheduling policy. Deriving the accurate max inter-service time of users under an arbitrary rate vector will be our future work.

6 Evaluation

In this section, we provide the simulation results of SGMW. Our results mainly include two parts. In section 6.1, we check the inter-service time performance of the policy. In section 6.2, we compare the SGMW with baseline max weight scheduling policy. We assume $r_i = 1$ for all user i in this section.

6.1 Inter-service Time Guarantee

To illustrate the inter-service time performance of SGMW, we assume four groups of flows, each with 4/8/16/32 flows. The arriving rate of user i is $\frac{1}{N+\epsilon} + \frac{\epsilon}{N+\epsilon} * 0.5^i$, where N is the number of flows, ϵ is the inter-service time constraint and i stands for the i th user. Such a rate vector is supported by the system since its summation is less than 1. Our result considers both the max and average inter-service time, as is shown in Fig. 2. The max inter-service time never violates the constraint while N and ϵ vary. We also find that the max inter-service time is equivalent to the constraint $N + \epsilon$ when $N = 64$, and this indicates the fact that some users with small rate can be scheduled only once in each interval. The average inter-service time increase with ϵ since the number of users only scheduled in the tight phase keeps increasing under our setting of arriving rates. In Fig. 3, we investigate the performance of SGMW when the variance of rate vector changes. The system is composed of 8 users, with $\epsilon = 8$. $\lambda_i = \frac{1}{N+\epsilon} + \frac{\epsilon}{N+\epsilon} * (1 - \delta)^{i-1} * \delta$ for each user i .

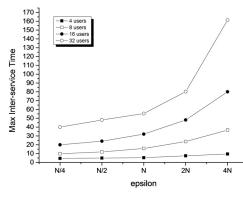
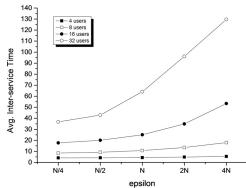


Fig. 2. Inter-Service Time Under Various Users

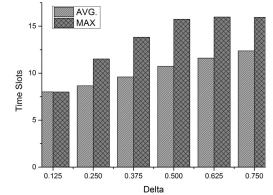


Fig. 3. Inter-Service Time Under Various Vectors

6.2 Throughput Performance

This subsection illustrates the throughput performance of SGMW. We compare it with the Max Weight scheduling policy. The total queue length and max queue length are two indicators that define the loads of a system and a single user. In Fig. 4, we check the performance under different number of users. We assume $\epsilon = 4N$, and $\lambda_i = \frac{1}{N+\epsilon} * 0.99^i + \frac{\epsilon}{N+\epsilon} * 0.5^i$, where N is the number of users. The total queue length of SGMW grows faster than Max Weight scheduling policy. This is due to the increasing number of users whose rate are less than $\frac{1}{N+\epsilon}$. To schedule such users will cause the waste of bandwidth and the occurrence of tight

phase. In Fig.5, we investigate the throughput performance of SGMW when the variance of arriving rate vector changes. The setting of the system is the same with that of simulation in Fig.3. The two policies are equal when δ is relatively small since the weight of any user can always grows to the maximum before the tight phase occurs. As δ keeps increasing, a growing number of users with small rate will only be scheduled in tight phase.

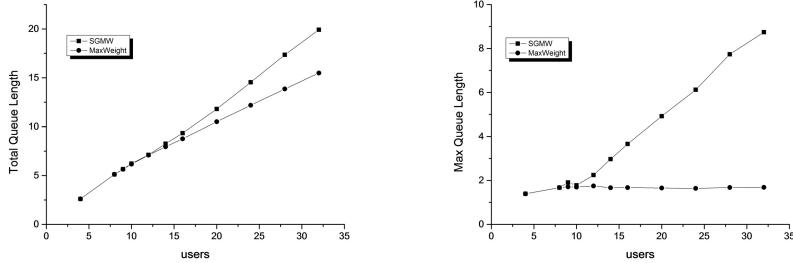


Fig. 4. Throughput Performance Under Various Users

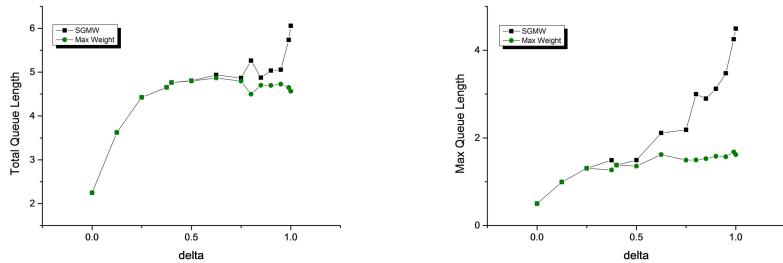


Fig. 5. Throughput Performance Under Various Arriving Vectors

7 Conclusion

This paper investigates the problem of inter-service time guaranteed scheduling policy designing in wireless networks. We formalize the definition of modified capacity region with inter-service time guarantee. The proposed scheduling policy is also proved to be throughput-optimal for the modified capacity region. Simulation results demonstrate that the scheduling policy has good performance on both the guarantee of inter-service time and the stability of networks.

Acknowledgements. This work was partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61190115,61033015, the National Science Foundation Distinguished Young Scholars of China under Grant No. 61300225.

References

1. Ai, C., Guo, L., Cai, Z., Li, Y.: Processing area queries in wireless sensor networks. In: 5th International Conference on Mobile Ad-hoc and Sensor Networks, MSN 2009, pp. 1–8. IEEE (2009)
2. Basagni, S.: Finding a maximal weighted independent set in wireless networks. *Telecommunication Systems* 18(1-3), 155–168 (2001)
3. Cai, Z., Chen, Z., Lin, G.: A 3.4713-approximation algorithm for capacitated multi-cast tree routing problem. *Theoretical Computer Science* 410(52), 5415–5424 (2009)
4. Cai, Z., Lin, G., Xue, G.: Improved approximation algorithms for the capacitated multicast routing problem. In: Wang, L. (ed.) COCOON 2005. LNCS, vol. 3595, pp. 136–145. Springer, Heidelberg (2005)
5. Cheng, S., Li, J., Cai, Z.: $\mathcal{O}(\varepsilon)$ -approximation to physical world by sensor networks. In: 2013 Proceedings IEEE INFOCOM, pp. 3084–3092. IEEE (2013)
6. Hoepman: Simple distributed weighted matchings. arXiv cs/0410047 (2004)
7. Hou, I.H., Kumar, P.: Scheduling heterogeneous real-time traffic over fading wireless channels. In: 2010 Proceedings IEEE INFOCOM, pp. 1–9. IEEE (2010)
8. Jaramillo, J.J., Srikant, R., Ying, L.: Scheduling for optimal rate allocation in ad hoc networks with heterogeneous delay constraints. *IEEE Journal on Selected Areas in Communications* 29(5), 979–987 (2011)
9. Kang, X., Wang, W., Jaramillo, J.J., Ying, L.: On the performance of largest-deficit-first for scheduling real-time traffic in wireless networks. In: 2013 Proceedings MobiHoc, pp. 99–108. ACM (2013)
10. Li, B., Li, R., Ery, A.: Heavy-traffic-optimal scheduling with regular service guarantees in wireless networks. In: 2013 Proceedings MobiHoc, pp. 79–88 (2013)
11. Li, J., Cheng, S., Gao, H., Cai, Z.: Approximate physical world reconstruction algorithms in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, <http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.2297121>
12. Li, R., Eryilmaz, A., Li, B.: Throughput-optimal wireless scheduling with regulated inter-service times. In: 2013 Proceedings IEEE INFOCOM, pp. 2616–2624 (2013)
13. Sakai, S., Togasaki, M., Yamazaki, K.: A note on greedy algorithms for the maximum weighted independent set problem. *Discrete Applied Mathematics* 126(2), 313–322 (2003)
14. Tassiulas, L., Ephremides, A.: Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. *IEEE Transactions on Automatic Control* 37(12), 1936–1948 (1992)
15. Wan, P.J., Frieder, O., Jia, X., Yao, F., Xu, X., Tang, S.: Wireless link scheduling under physical interference model. In: 2011 Proceedings IEEE INFOCOM, pp. 838–845. IEEE (2011)

Wear-Leveling Optimization of Android YAFFS2 File System for NAND Based Embedded Devices

Yuqiu Qian, Junjie Lu, and Kai Xing

University of Science and Technology of China

Abstract. The lifespan of flash memory has a close connection with its wear-leveling level. However, YAFFS2, a popular embedded file system does a poor work on it. This paper introduces a novel approach, easy to be achieved, to improve its wear-leveling level and retain its original format and strengthens. The new cold-data method is tested using real YAFFS2 file system for different parameters. Our results demonstrate that it is capable of improving the wear-leveling level as well as prolong devices lifespan significantly.

Keywords: Wear-leveling, YAFFS2, cold data.

1 Introduction

Flash Memory, consisting of NOR Flash Memory and NAND Flash Memory, is increasingly used nowadays. Compared with NOR Flash Memory, NAND Flash Memory attracts more and more people for its bigger storage and higher speed, which is better for big data storage. It is made up of several blocks, and each block consists of several pages. Each time, data is written by pages, but erased by blocks. Each block has a limited time of wearing(each time writing and erasing will wear the block, reading does less wear to the blocks, which can even be ignored), so once some blocks of the device exceed their limit, the entire device can not be used any more. As we can see, if all blocks are evenly wore, the entire lifespan of the device can be prolonged to some degree. As a result, the notion of wear-leveling is proposed to measure the deviation of all wearing times of blocks. The lower the wear-leveling is, the better the blocks are evenly used.

YAFFS2 is the next generation of YAFFS file system, which is designed specifically for NAND Flash Memory. It appears to have a lot of advantages, such as light weight, high speed, less memory usage and huge popularity among all the embedded operating systems. Taking these into consideration, Google chose it as the default file system for Android, a popular system for various embedded devices. However, as is observed in Fig.1 below given by TOSHIBA, it has an apparent weakness that it has a severe wear-levering level. YAFFS2 uses the same wear-leveling strategy as YAFFS that it allocates data among blocks in a circle sequence so that each block is treated equally. But blocks with cold data cannot be viewed equally actually in this strategy due to no allocation for a long time, which leads to low level of wear-leveling. From this point of view, we

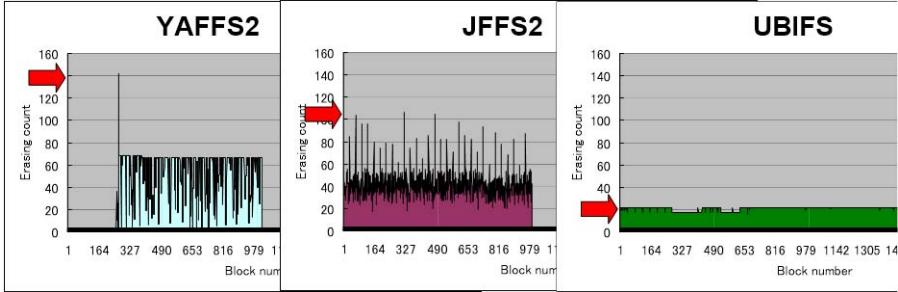


Fig. 1. Test Data on NAND File System given by TOSHIBA in 2009

develop our technique based on consideration of cold data, and have excellent experience results eventually.

There have already some work on the wear-leveling problems: Some work just rely on whether a block is hot or cold [1], [2]. A block is a hot block means that it has been wore at a high level among all the blocks, and on the other hand, a block is a cold block means that it has been wore for fewer times. Intuitively, if we reduce the amount of wear of a hot block as well as increasing the amount of wear of a cold block, we can to a certain extent reach a high level of wear-leveling. From this perspective, some algorithms are designed by exchanging data in hot blocks and those in cold blocks at some point to reach an average level of wear among all the blocks. However, just consider this situation: If a datum, which seldom changes, is just moved into a hot block. Intuitively, it is a good thing because it can help the hot block to avoid being wore more frequently. But in this algorithm, the cold data in this hot block will be exchanged immediately because this block is still a hot block, which is definitely unreasonable. One way to deal with this problem is to introduce the conception of cold data and hot data. Based on this conception, active wearing and passive wearing is then put forward by M-Systems Inc. [3], taking data into consideration instead of blocks like before. Active wearing is the active process of data writing, and passive wearing means the data exchange between cold data and hot data. The division of cold data and hot data is in accordance with the fact that some system data are quite different from user data in that former data can be viewed as cold data while the latter as hot data. So, blocks storing these cold data will be wore relatively less comparing other blocks with hot data. This thought truly inspires other researchers, but in their patent, we can hardly find any practical approaches. So, in 2007, Prof. L. P. Chang raised another algorithm [4] considering cold data and hot data. He uses two queues to identify them and achieves good results. However, as we all know, adding physical data structure is not practical because we have to change data format. Also, we cannot ensure the match of the file system with the drive existed.

As discussed above, these research on wear-leveling has inspires us how to deal with this practical problem. However, how to change the low wear-leveling level of YAFFS2 as well as keeping its own advantages, such as fast speed, using

existing data structure, and adding fewer extra wearing times, is still a problem to be solved. So, in this paper, we propose a new algorithm and have some tests on it.

2 Cold Data Approach to Deal with Wear-Leveling

2.1 Data and Blocks

With the help of temperature, we can describe different situations vividly. According to the modifying frequency, data can be divided into two types, cold data and hot data. Cold data are the data seldom modified or written in, and hot data are the opposite ones. According to the amount of wear times, blocks fall into two categories: cold blocks and hot blocks. A block is a hot block means that it has been wore at a high level among all the blocks, and on the other hand, a block is a cold block means that it has been wore for fewer times. As a result, when it comes to blocks and data, there are four different situations as is seen below in Table 1:

Table 1. Four Different Situations

	Cold data	Hot data
Cold blocks	Avoid	Recommend
Hot blocks	Recommend	Avoid

Whether cold data stored in a hot block to decrease its temperature or hot data stored in a cold block to increase its temperature are beneficial to achieve an average temperature among all the blocks, which is a representation of a high level of wear-leveling. On the other hand, a hot block storing hot data or a cold block storing cold data will make the hot block hotter or the cold block colder, which will eventually lead to the bigger gap among the temperature of all the blocks.

Instead of considering all situations listed above in Table 1, we introduce a technique only focusing on cold data, which is quite different from all research before. More importantly, we needn't add any extra data regions to YAFFS2 file system, which ensures it match its original drive.

In addition to the active wearing process, which means that each new data should be written in the next empty block in the circulation of all the blocks, we also have a passive wearing mechanism by removing cold data from cold blocks. If the probability of cold blocks containing cold data reduces, the probability of cold blocks containing hot data and the probability of hot blocks containing cold data will surely increase. At the same time, the probability of hot blocks containing hot data will definitely decrease. In the end, all goals listed in Table 1 seem to be approximately achieved.

2.2 Cold Data Approach

The temperature of data $DataTemperture_i$, standing for the length of data not modified in $block_i$, can be identified with the latest written time $DataBlock_i$ of $block_i$ stored in Seq_number region in the original YAFFS2 file system and Sum proposed by us to record the all writing times.

$$DataTemperture_i = Sum - DataBlock_i$$

It is an index to show whether data in $block_i$ is cold or hot by introducing *tolerance*. If $DataTemperture_i \leq tolerance$, we view it as a hot data. Only when $DataTemperture_i > tolerance$, we view it as a cold data, and we should exchange it to another block, which can also be simplified as an extra new writing process. So when each new data written in, we find the max $DataTemperture_i$ and rewrite its cold data. Due to the fixed Sum each time, it equals to finding the min $DataBlock_i$, which can be achieved by maintaining a min heap, whose cost is only $O(lgn)$.

The algorithm is operated periodically, and how often the algorithm is executed and how much the algorithm complexity is both are determined by *tolerance* as data will be exchanged often if *tolerance* is small. As a result, the wear-leveling level is high as well as the algorithm complexity is also high. On the other hand, the algorithm complexity will be much less if *tolerance* is large. Though how to choose *tolerance* is important to our approach for the balance between wear-leveling level and algorithm complexity, the overall complexity is decreased by focusing on cold data instead of hot data, because the number of cold data is much less compared to that of hot data.

Input: Sum,Block[1..n],tolerance,new data X

Output: Sum,Block[1..n]

- 1 $Sum = Sum + 1;$
- 2 Store X in the next empty $block_i$;
- 3 $Block[i] = Sum;$
- 4 Find Min Block[j];
- 5 **if** $Sum - Block[j] \geq tolerance$ **then**
- 6 Write Data(data in $block_j$);
- 7 **end**

Algorithm 1. Write Data(X)

In this simplified process, we set tolerance as below:

$$tolerance = (n - m) * a + m - 1 \quad a, t \in \mathbb{N}$$

where m stands for the number of blocks storing cold data, n is the number of blocks, which is t times of m. Also, we assume that cold data with fixed number are all written before hot data, and they both never transfer. As is seen in Fig. 2, n blocks are evenly wore after a circle, which is a strong support for our

algorithm's positive effects. Of course, this approach will definitely add extra wear to blocks, but in the simplified process in Fig. 2, it only brings n times extra wear comparing with

$$(t-1)an + n = \frac{nm + na(n-m)}{m}$$

times of writing, which is only

$$\frac{m}{an + (a-1)m}$$

of all times of writing and can be ignored. Also, it proved to be tolerated in our experimental research.

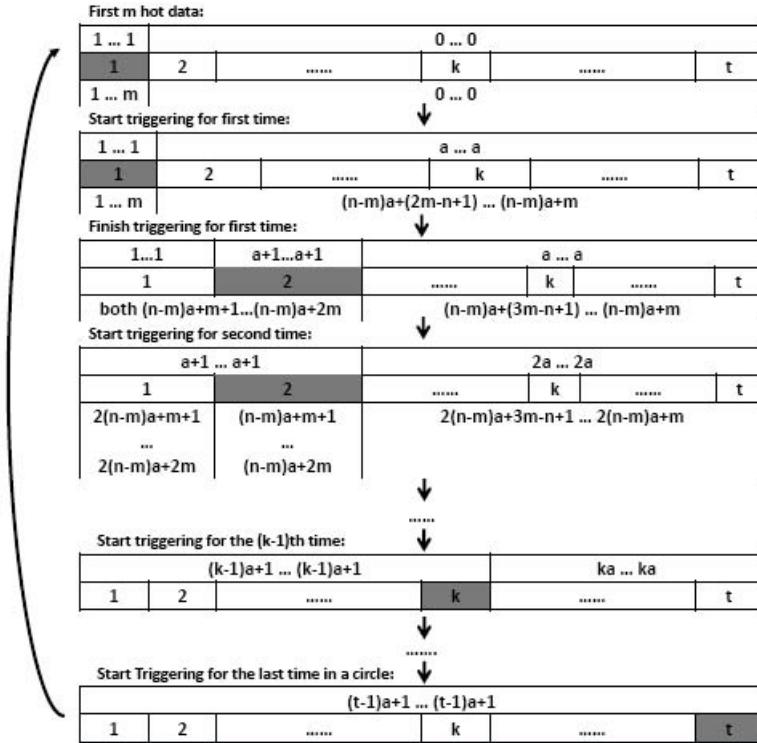


Fig. 2. A simplified process of our technique

3 Theory Results and Discussion

$n_i, i \in \{1, 2, \dots, n\}$, denotes $block_i$'s total times of wear. If we define A to be the point that one block has reached its limit B , then

$$A = \sum_{i=1}^n n_i \quad \exists j \in \{1, 2, \dots, n\}, s.t. n_j = B$$

All data come independently, and we use $\xi_{i,j}$ to describe the length of j th data in $block_i, i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, n_i\}$. $\xi_{i,j}$ is assumed to be governed by a $Exp(\lambda)$ -distribution in the original file system, because exponential distribution has an excellent feature that is called 'Memoryless Property', which matches the staying times of data well. Also, in our algorithm, we sum all probability that $\xi_{i,j} > T$ to $\xi_{i,j} = T$. So the distribution of $\xi_{i,j}$ looks (2), a changed $Exp(\lambda)$ -distribution.

$$f_1(\xi_{i,j}) = \begin{cases} \lambda e^{-\lambda \xi_{i,j}} & \text{if } \xi_{i,j} > 0 \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

$$f_2(\xi_{i,j}) = \begin{cases} \lambda e^{-\lambda \xi_{i,j}} & \text{if } 0 < \xi_{i,j} < T - \varepsilon \\ \frac{e^{-\lambda T}}{2\varepsilon} & \text{if } T - \varepsilon \leq \xi_{i,j} \leq T + \varepsilon \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

$P(n_i = k)$ is the probability that k data and only k data have been written into $block_i$ at point A . All these blocks are of the same place so that their probability distributions are the same:

$$P(n_i = k) = P(n_{i'} = k) \quad \forall i, i' \in \{1, 2, \dots, n\}, i \neq i'$$

Due to the big value of n , n_i of these n blocks can also be viewed as n random samples for this distribution. So the deviation and expectation of n_i can be estimated by this distribution $P(n_i = k)$ as below:

$$E(n_i) = \sum_k k * P(n_i = k), \quad D(n_i) = E(n_i - E(n_i))$$

Here comes the problem that how to get this distribution $P(n_i = k)$. If k data and only k data have been written into $block_i$ at point A , staying time of $k - 1$ data in $block_i$ can not reach this point as well as the point that k th data leave $block_i$ will surpass it. Then, this distribution $P(n_i = k)$ can be calculated as below:

$$\begin{aligned} P(n_i = k) &= P\left(\sum_{j=1}^{n_i-1} \xi_{i,j} < A, \sum_{j=1}^{n_i} \xi_{i,j} \geq A\right) \\ &= P\left(\sum_{j=1}^{k-1} \xi_{i,j} < A, \sum_{j=1}^k \xi_{i,j} \geq A\right) \\ &= P(\alpha < A, \alpha + \beta \geq A) \\ &= \int_{-\infty}^A \int_{A-\alpha}^{+\infty} f(\alpha) f(\beta) d\alpha d\beta \end{aligned} \quad (3)$$

where $\alpha = \sum_{j=1}^{k-1} \xi_{i,j}$, $\beta = \xi_{i,k}$, $A = (n-1)k + B$. Because $\xi_{i,j}, i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, n_i\}$ are independent from each other, both $f(\alpha)$ and $f(\beta)$ can be calculated directly by (1) and (2). Then we can get $P(n_i = k)$ by (3).

$$P_1(n_i = k) = \frac{e^{-\lambda A} (\lambda A)^{k-1}}{(k-1)!}$$

Formal $P_2(n_i = k)$ is too complicated to be listed. But as we can see, distribution of $\xi_{i,j} < T - \varepsilon$ is not changed in our algorithm. All we have done is to sum probabilities of $\xi_{i,j} \geq T + \varepsilon$ to that of $T - \varepsilon \leq \xi_{i,j} \leq T + \varepsilon$. Due to the opposite relationship between $\xi_{i,j}$ and k , that higher $\xi_{i,j}$ always comes with lower k , as well as the fact that all probabilities doomed to be summed to 1, it means that the probabilities of $k < \frac{A}{T}$ are all zeros and probabilities of $k \geq \frac{A}{T}$ are higher in our algorithm. So, our algorithm is supposed to have a higher $E(n_i)$ comparing the original one. This qualitative analysis also demonstrates that our algorithm can bring an improvement to devices' lifespan.

4 Experiment Results and Discussion

By simulating writing and deleting stochastic data on actual YAFFS2 file system with 512 blocks for over 300 thousand times, we get Table 2 below to evaluate our improvement on wear-leveling level of YAFFS2 file system. Due to large amount of stochastic data in our experiment, the test error can be eliminated to some extent. In our experiment, the proportion of hot data to cold data is almost 1/8, which is a statistic approximation.

Table 2. Experiment Results

tolerance chosen	origin	2n	3n	4n	5n	6n	7n	8n	9n	10n
Writing times	367290	316140	375892	378921	374654	365429	363630	370666	372610	373182
Writing times per block	717.4	617.5	734.2	740.1	731.7	713.7	710.2	724.0	727.8	728.9
Standard Derivation	0.343	0.171	0.159	0.172	0.161	0.178	0.179	0.183	0.172	0.183
extra writing	0	8903	9224	9048	9167	8547	8122	7677	7425	6645
extra writing percent(%)	0	2.82	2.45	2.39	2.45	2.34	2.23	2.07	1.99	1.78
total lifespan	218869	312556	324277	310024	338332	355119	281978	335933	336535	314507

Table 2 summarizes the experimental results we obtained choosing different tolerance values, as well as the performance of the original YAFFS2 file system. Standard Derivation of blocks' writing times is our index for the level of wear-leveling, which can be measured by

$$\text{Standard Derivation of writing times} = \frac{\text{Derivation of writing times}}{\text{Writing times per block}}$$

Our algorithm's side effect, measured as extra writing times and extra writing percent, are also listed in Table 2. Of course, whatever the standard derivation is, our ultimate target is to extend the lifespan of the devices, which is defined as the total writing times when some blocks reach 1000 times of wear.

Extracting test results when choosing $\text{tolerance} = 1024$, we can get Table 3 and Fig.3, from which the difference between original YAFFS2 file system and our improved YAFFS2 file system can be seen directly. The experiment

Table 3. Experiment Results when tolerance=1024

	Original YAFFS2	Improved YAFFS2
Writing times	367290	316140
Writing times per block	717.4	617.5
Derivation of writing times	245.8	105.3
Standard Derivation of writing times	0.343	0.171
extra writing	0	8903
extra writing percent(%)	0	2.82
total lifespan	218869	312556

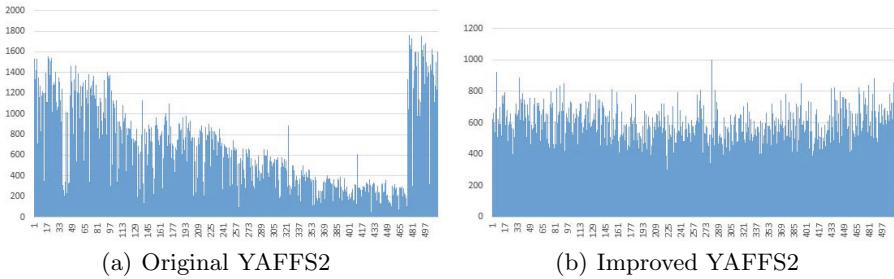


Fig. 3. Comparation of the results when choosing tolerance=1024. The X axis represents all 512 blocks and the Y axis represents the times of each block being worn. So, the shape of the picture gives insight of the wear-leveling level.

results proves that the Standard Deviation of writing times turns from 0.343 to 0.171 with our improvement, which is only 49.85 percent of before. Also, the lifespan has been prolonged from 218869 to 312556, which cannot be viewed as a significant improvement. Of course, our algorithm does bring extra writing for 8903 times, but it can be ignored because of only 2.82 percent of 316140 times of writing. An interesting question that arises naturally here is why the test result of original file looks like a 'V'? If it has no passive wear, shouldn't it look like a 'U'? To answer this question, we have to emphasize again that our algorithm is tested on the real YAFFS2 file system, which means the existence of GC-thread. It always makes some movement for these cold data, and leads to the final 'V' shape results. But we can still find our approach effective.

Another strengthness of our algorithm is that it only needs one parameter. Different tolerance can lead to different results. Actually, the original YAFFS2 file system is the particular case choosing $tolerance = \infty$. We test the performance of YAFFS2 file system with tolerance from $2 * n = 1024$ to $10 * n = 5120$. From Fig.4(a), the relationship between the the Standard Deviation of writing times and tolerance value are revealed clearly. Fig.4(b) reveals a comparison between original lifespan and improved lifespan of different tolerance. Around 3000 is revealed as being the best value for tolerance to achieve a peak. Respectively, it shows that both improved lifespan and Standard Deviation of all different

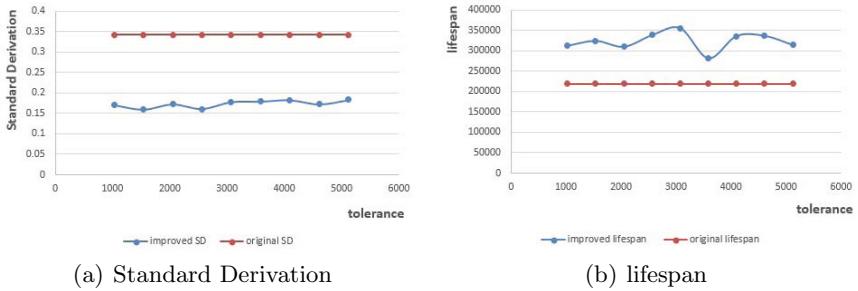


Fig. 4. Experiment on different tolerances. The algorithm has different performances when choosing different tolerances, but they all outperform the original ones: the standard derivation is shorter(*left*) and the lifespan is longer(*right*). The X axis represents the number of tolerance chosen and the Y axis represents the number of Standard Derivation of writing times and the length of lifespan.

tolerance are much better than the original ones, which is a strong demonstration for our approach.

Our study is of great significant: First of all, the entire lifespan will be increased. NAND Flash memory consists of many blocks and each block has a limited amount of wear times. Once some blocks overload wearing, it will break and cannot be written and erase any more. In this case, the entire NAND Flash memory will be affected. Even many blocks can still be used, the entire memory must be discarded. On the other hand, if we wear all blocks entirely, the entire lifespan will on some ways be prolonged. Also, it has practical meanings. YAFFS2 was the original file system for Android before 2012 and is still an important file system for embedded devices. So, reducing the wear-leveling level to almost 50 percent than before is of great significant. Last but not least, the entire process is easy to achieve. From our experiment, we find that it easy to improve original YAFFS2 file system with our technique only by exchanging file "yaffs.ko", even no need to be formatted, which is surely exciting for our research.

5 Conclusion

How to improve wear-leveling level without changing the original format of file systems, adding less extra wear, as well as maintaining its own advantages of Flash Memory file systems is with no doubts a problem needed to be solved. We put forward a new approach mainly focused on cold data and have excellent test results. Also, we find that we only have to replace the file "yaffs.ko" in YAFFS2 file system, which is definitely a good news for all people.

In this paper, we mainly propose a new idea focusing on cold data and compare it with the original YAFFS2. In future work, we are intended to compare the proposed scheme with other schemes addressing the wear-leveling problems and find out how our approach performs. Also, we are likely to test if this idea also

works well on other file systems which means that it can provide a totally new perspective for the improvement of wear-leveling level of file systems, not just YAFFS2.

References

1. Chang, L.P., Kuo, T.W.: Efficient Management for Large-Scale Flash-Memory Storage Systems with Resource Conservation. ACM Transactions on Storage (2005)
2. Kim, H.J., Lee, S.G.: An Effective Flash Memory Manager for Reliable Flash Memory Space Management. IEICE Transactions on Information and System (2002)
3. M-Systems, TruFFFS Wear-Leveling Mechanism
4. Chang, L.P.: On Efficient Wear Leveling for Large-Scale Flash-Memory Storage Systems. In: Proceeding of SAC 2007 Proceedings of the 2007 ACM Symposium on Applied Computing (2007)
5. C. Manning and Wookey, YAFFS Specification. Aleph One Limited (2001)
6. Chiang, M.L., Lee, P.C.H., Chang, R.C.: Using Data Clustering To Improve Cleaning Performance For Flash Memory. Software - Practice and Experience (1999)
7. Gleixner, T., Haverkamp, F., Bityutskiy, A.: UBI -Unsorted Block Images (2006), <http://www.linux-mtd.infradead.org/doc/ubi.html>
8. Wear Leveling in Single Level Cell NAND Flash Memories. STMicro electronics Application Note, AN1822 (2006)
9. Sandisk Flash Memory Cards Wear Leveling (2003),
<http://www.sandisk.com/Assets/File/OEM/WhitePapersAndBrochures/RS-MMC/WPaperWearLevelv1.0.pdf>

Web Map Service Log Analysis

Xiaofei Wang¹, Di Chen², Gan Lu¹, Yue Peng³, and Chengchen Hu²

¹ Baidu, Beijing, China

² Computer Science and Technology, Xi'an Jiaotong University, Xi'an

³ Beijing University of Posts and Telecommunication, Beijing

Abstract. With the rapid growth of location-based services (LBS), web map service (WMS) is becoming indispensable in our daily life. From a new perspective, this paper measures and analyzes the user behaviors and regional differences in WMS, based on a big log dataset from the PC clients of a large-scale WMS provider. We give analysis on users' searching times from both macro and micro perspective, and point out that WMS data has a feature of searching behavior prediction, which is absent in other location-based datasets. Then, we observe and verify that the searching frequencies of point of interests in a city conform to Zipf distribution, and explain the underlying physical meanings of the corresponding parameters. In addition, we present a simple and intuitive approach to quantitatively study the inter-city fluidity and intra-city mobility patterns, and give semantic analysis on query categories in each city. And our work can serve as a measurement basis for future work in the area of WMS data mining.

Keywords: Web Map Service, Point of Interest, searching behavior prediction, Zipf distribution, inter-city fluidity.

1 Introduction

In the age of Big Data, the volume, the updating velocity, and the variety of data are too big, too fast and too (semantically and syntactically) diverse because of the development of Internet. The Web map services (WMS) have become very popular, mainly driven by the availability of modern smart mobile devices. Prominent map service providers such as Google map, Baidu Map and Amap, are playing an important role in people's daily life. The users left huge volume of query logs when they enjoying the convenient services from the WMS.

Location-based Service (LBS) related mining researches have become more and more popular and attracted significant attention thanks to the LBS available with the modern mobile devices. [1] captured basic HTTP information of Web 2.0 based map application at Tsinghua campus network and analyzed the mash-up characteristics of the popular online maps. Zheng Yu (from MSRA) present their work towards understanding users from a geospatial view by studying GPS trajectory transportation mode categorization and co-located query pattern mining problems [2]. Zheng also

proposed a paper which mining similarity between users based on their geographic location histories [3]. They chose 65 volunteers respectively logged their life experiences with GPS traces over 6 months. All of them were suggested to switch on their devices as long as they traveled outdoors. However, people seldom open GPS devices all over the time.

In this paper, we analyzed the PC user search behavior by a beta version online map logs. We give analysis on users' searching times from both macro and micro perspective, and point out that WMS data has a feature of searching behavior prediction, which is absent in other location-based datasets. Then, we observe and verify that the searching frequencies of point of interests in a city conform to Zipf distribution, and explain the underlying physical meanings of the corresponding parameters. In addition, we present a simple and intuitive approach to quantitatively study the inter-city fluidity and intra-city mobility patterns.

Different with the previous data mining based on GPS data of users' behavior, our work present some new ideas for analyzing spatio-temporal data, which can be concluded as follows: First, our dataset is based on the log which exceeding 500 million WMS records. The dataset has the property of large-scale, unstructured, low value density, high authenticity, etc. The dataset also has the measurement statistics difficulties of discrete time, not-unified POI specifications, strong semantic, etc. Second, from a new analytical perspective, we seek the characteristics of WMS log data, urban search mode, inter-city mobility rule. Our subject of study is not confined to user behavior mining analysis. User searching behavior prospective characteristics and city searching behavior patterns provide a good measurement basis for further understanding of user behavior [4], recommendation based on geographical position [5], intelligent urban computing and planning [6], etc., which also have certain sociological significance.

The rest of the paper is organized as below. Section 2 provides an overview of our approach to collect data and process the logs with Hive platform. From Section 3 to Section 6, we discuss the analysis results from the data. Finally, we review related work in Section 7 and draw a conclusion in Section 8.

2 Data Collection and Pre-processing

The data used in this paper is collected a test version of one popular online map between Jan. 2013 and Mar. 2013. Overall, we collected more than 5 hundred million logs. There are 8,311,257 user search information. After filtering meaningless query, 3,199,752 logs can be used for analysis finally.

The data was generated by collecting user click and operation behavior via JavaScript code in the client. The custom generated data will be send to the corresponding server interface when the number of log is equal to the default value n ($n=10$ as default by considering of the performance).

2.1 Data Collection

We describe the data set used for analysis. Briefly speaking, as is shown in Fig. 1, we collect and process the logs with the following five steps:

1. Extract the search information by parsing JSON data.
2. Filter the invalid search information, such as blank query or meaningless query word.
3. Extract user cookie, IP address, search query, timetable and other useful information.
4. Geolocate where those IP addresses are geographically located.
5. Store the details persistently into database for analysis.

A unique user ID (uid) is generated with 24 random characters when a client cookie is not available. The following fields are used for analysis in our paper: Uid, IP, Geolocation, ISP, isEdu(in campus or not), Timestamp and Query word.

Niu0lyGkEhjYFvsVzA6MxbUpD7neLW, 114.247.50.2, Beijing, ChinaUnicom, 0, 2013-01-07 09:22:54, Sihui;

0WL7IQ4zFjuOBgHDZcSoksCTwEpRiIy, 60.10.8.6, Hebei Province Langfang City, ChinaUnicom ADSL, 0, 2013-01-16 14:08:46, Tianjin Wanda

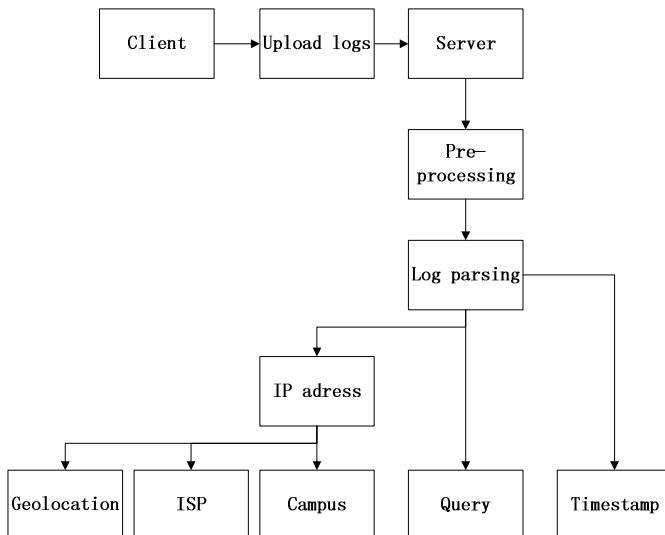


Fig. 1. Data acquisition and parsing process

2.2 Data Processing with Hive

There are many big data analytics platforms and database systems emerging in recent years, such as MongoDB database and Hive. Hive provides a mechanism to project structure onto this data and query the data using a SQL-like language called HiveQL[7]. There are many advantages of Hive and two interesting features for log

analysis are: 1) We can run our Hive queries in many ways. We can run them from a command line interface or from Hive Thrift Client which could be communicated with applications written in C++, Python or many other languages. 2) Hive has several interesting User Defined Function (UDF) packages and make it easy to control the map/reduce transform stages. The above three reasons ensure Hive can improve developer productivity when working with challenging data formats or complex analytical tasks.

We first create Hive table and insert the logs into it via script every day.

1. Create Hive table:

```
CREATE TABLE DATA (
    uid STRING, service STRING, platform STRING, query STRING,
    province STRING,
    ...
    IP STRING)
partitioned by (date STRING)
ROW FORMAT DELIMITED
FIELDS TERMINATED BY '$'
STORED AS TEXTFILE;
```

2. Query with HiveQL:

It takes very less time to change or modify HiveQL queries compared to Map/Reduce code. So we can update the HiveQL according to the result conveniently.

For instance, we can use the following HiveQL query to search the destinations and their corresponding frequency whose start province is Beijing.

```
hive -S -e "select count(destProvince) as sumDis, destProvince from DATA where
startProvince = 'Beijing' group by destProvince order by sumDis;" > result
```

3 Prediction of WMS Users' Behaviors

3.1 Macroscopic Analysis of Time Distribution

To discover and validate the differences between the WMS data and other spatio-temporal data, we analyze the users' behavior from January to March on a macroscopic view.

The cumulative frequency distribution (24 hours one day) of user's requests in Beijing from January to March in WMS data is shown in Fig.2. In the Fig., we can easily find that the peak of user's requests is happened in the morning among 10:00-12:00, 16:00-18:00 and 21:00- 23:00. Comparing with the other time, such as lunch time around 13:00 and dinner time around 19:00, the request number is reduced clearly. As compared to other spatio-temporal data, we collected a few GPS real-time logs and use this as a reference for real-time people traffic. As shown in Fig.3, this location is busy at 8:00-9:00, 12:00-14:00 and 18:00-19:00. Data analysis indicates that the user characteristic of WMS is different from that of GPS: the originations of search queries are usually dense in stable state, for example, office working hours at

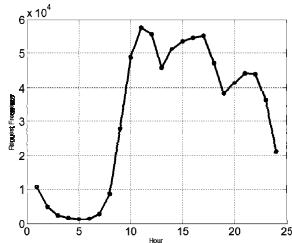


Fig. 2. Day distribution of WMS request# in Beijing

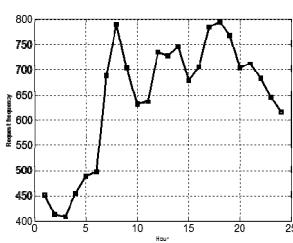


Fig. 3. Day distribution of GPS request# in Beijing

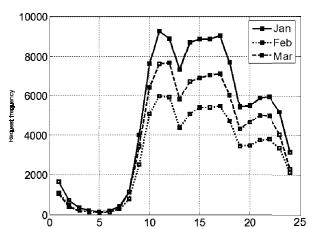


Fig. 4. Day distribution of WMS request# in Beijing from Jan. to Mar.

forenoon and afternoon or after super. Originations of search queries are relatively small when the state is unstable when traveling and having meals. By observing the statistics of Fig.4 from January to March, We can find that the fluctuation of query frequency distribution in one day is very small, but changes as the holiday changes. By analyzing the searching record of users, we can forecast users' future activities.

Though macroscopic analysis of time distribution above and comparing WMS data with GPS data, we contends that WMS data is kind of forward-looking. That is to say, users will do search before truly activity, which means a lot to the prediction of characteristics of the population flow and mass incidents.

3.2 Micro Analyzing of Users' Actions

Through macroscopic measure of time distribution, WMS log displays some characteristics, which can be demonstrated further by user self-action in finer granularity. In this section, we analyzing high-frequency users' search behavior, by regarding different users as research subjects. We selected 135,930 high-frequency users from 3,199,752 records of 2,447,336 users to do the analysis.

To verify the delay between the searching action and users' activity location, we selected 16,418 users which accord with two characteristics below.(1)IP, used by users, had changed;(2)the location of the searching POI keywords has changed. We divided these transregional users into two categories.

Category one: Inter-provincial offsite queries users, whose searching place and location are in different provinces.

For example:

Uid_A,113.9.226.158, Heilongjiang Province Harbin[,2013-03-02 14:51:21,Nanjing

Uid_A,113.9.10.43, Heilongjiang Province Harbin[,2013-03-04 21:58:17, Jiming Temple

Uid_A,222.49.253.204,Jiangsu Province Nanjing,Tietong,2013-03-17 23:35:51, Meiyuan new countryside

Uid_A,222.49.253.204,Jiangsu Province Nanjing,Tietong,2013-03-17 23:37:33, Airport

Category two: Same-provincial offsite queries users, whose searching place and location are in the same province but different cities. The sample logs are as follows.

Uid_B,123.5.162.115, Henan Province Luoyang, China Unicom, 2013-02-19 22:35:32, No. 9 road, Zhengzhou

Uid_B,123.5.162.100, Henan Province Luoyang, China Unicom, 2013-02-22 22:37:37, Zhang zhongjing pharmacy

Uid_B,123.52.5.25, Henan Province Zhengzhou, Chinanet, 2013-03-01 16:50:51, Huanghe Road, Zhengzhou

Uid_B,123.52.5.25, Henan Province Zhengzhou, Chinanet, 2013-03-04 16:06:24, Zhang zhongjing Ruhe Shop

The example data above demonstrated searching actions of users at PC port are prospective. Because nowadays IP Locator Database can only fix location on city level, we only selected and analyzed transregional users. Same-city searching actions are also before activity moving of users.

These searching actions can help us to predict user's next activity moving. If we analyze from the perspective of urban studies, these data can be used in the prediction of population flows and mass incidents in the city. If we excavate from the user's point, we can realize the intelligent match of similar friends, and intelligent selection of meeting place. In section 4, we made a quantitative measurement and analysis about flow characteristic between cities in intuitive way.

4 Zipf Distribution of Queried POIs in the City

An interesting phenomenon has been discovered from the statistics of high-frequency searched POIs in each city. After sorting the search frequency of POIs in ascending order, we find that the search frequency of the corresponding POI and its rank meet Zipf [8] distribution ranking.

For the sequence of the POI search keywords $POI_1, POI_2, \dots, POIn, \dots$, if it satisfies

$$freq(POI_1) < freq(POI_2) < \dots < freq(POI_n) < \dots$$

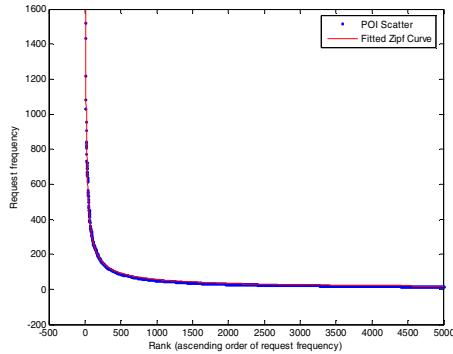
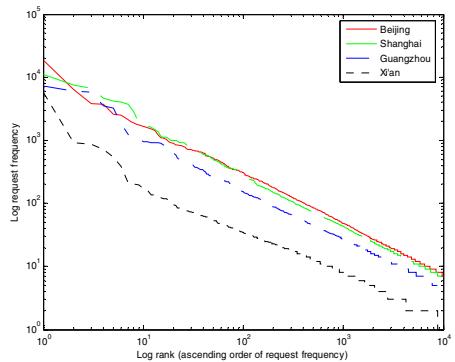
The search frequency of POI_r is the sorted r^{th} , then $freq(POI_r)$ and r meet

$$freq(POI_r) = \frac{\rho}{r^\alpha}$$

Zipf's principle reflects a power-law relationship between size and rank. The most repeated queried POI group represents the most attractive district, and Zipf's law also shows that only a few POIs are queried very frequently in each city.

Fig.5 shows scatter diagram of top 10000 queried POIs in Beijing and the fitting curve of the power function, the corresponding request frequency of top 500 queried POIs is higher, but accounts for only a small percentage of the total; after 500 ranking.

The request frequency of the rest POIs is distributed between 0-200. This can be explained by the physical meaning of the Zipf distribution, places with large crowd density and people's concern only preserve a minority proportion of all locations. Fig.6 is the Zipf fitting curves of Beijing, Shanghai, Guangzhou and Xi'an. And the

**Fig. 5.** Zipf curve of hot POIs in Beijing**Fig. 6.** Relationship between hot POIs' query frequency and their ranks in several cities

horizontal axis is the frequency of POI from the smallest to the largest place, vertical axis is the corresponding POI request frequency. As shown in the Fig.6, as α increases, the slope of the curve under log coordinates is greater, the request frequency of the POI keywords becomes more unbalanced. To sum up, α is inversely proportional to the average degree of the pedestrian mobility. That is, the greater α is, and the more unbalanced of the city's pedestrian mobility will be.

The above analysis shows that the distribution of POIs is not balanced enough, a handful of hot POIs fascinate most people flow. These hot POIs can be deeply analyzed so as to provide recommendation for urban planning, business locational choices and people's going out.

5 Analysis of Population Movements among Cities

People flow in each city is not fixed. People reach or leave the city in every random time period. Recent researches on population movements among cities usually are based on the survey data or predictions with few observations. In this section, we static and analysis the query records in January of several cities, provide reference predictions of population movements based on static works and the time delay analysis of trans-provincial user behaviors in Section 3.2 and describe the model for describing flows of cities as follows:

Definition 1. Out-degree of city

There are cities $c_1, c_2, \dots, c_i, \dots, c_n$, for a certain city c_i among them, population movements from c_i to other cities is:

$$OP_{ij} = \frac{o_{ij}}{t_i} \times \alpha$$

Among them
 OP_{ij} —— parameter to describe the scale of population inflows from city c_i to c_j

o_{ij} —— the number of requests that c_j is contained in search keywords in c_i

t_i —— amount of requests in c_i

α — coefficient of correction

Definition 2. In-degree of city

There are cities $c_1, c_2, \dots, c_i, \dots, c_n$, for a certain city c_i among them, population movements from other cities to c_i is:

$$IP_{ij} = \frac{i_{ij}}{t_j} \times \beta$$

Among them

IP_{ij} — parameter to describe the scale of population outflows from city c_i to c_j

i_{ij} — the number of requests that c_i is contained in search keywords in c_j

t_j — amount of requests in c_j

β — coefficient of correction

Definition 3. Mobility properties city

There are cities $c_1, c_2, \dots, c_i, \dots, c_n$, for a certain city c_i among them, the mobility properties of it is describe as below:

$$F_i = \frac{\sum_{j=1}^{j=n} OP_{ij}}{\sum_{j=1}^{j=n} IP_{ij}} \times \gamma$$

Among them

$j = 1, 2, \dots, i - 1, i + 1, \dots, n$

OP_{ij} — parameter to describe the scale of population inflows from city c_i to c_j

IP_{ij} — parameter to describe the scale of population outflows from city c_i to c_j

γ — coefficient of correction

According to the definition above, we static the population mobility of several cities and their movement flows. As shown in Table-2, each row records OP from the first city in the row to the other cities in the row, each column records IP from cities in the column to the first city in the column. In the last row, we calculate value of F for every city.

We can see from Table-1, for international large city such as Beijing and Shanghai, the population inflows from other city is large, and number of requests about other cities is relatively low, so their F value is less than 1. As for some smaller city such as Nanjing and Guangzhou, their F value is greater than 1. We also find that the population movements among cities are closely related to location and traffic conditions. Beijing-Xi'an high speed rail was put into service in January, among all of the Beijing-Xi'an population inflows (IP), the Beijing-Xi'an flow accounted for a large proportion of the total. Moreover, because the Nanjing-Shanghai high speed rail, the Nanjing-Shanghai IP value reaches up to 201.5.

These measurement and analysis work quantify the population movements between cities and describe people's mobility properties of each city. According to the prospects characteristics of PC log that have been revealed in Section2, these works can provide references for predicting the city traffic in order to provide deployment and planning.

Table 1. Population movement and mobility properties of cities

	Beijing	Shanghai	Guangzhou	Nanjing	Xi'an	$\sum OP$
Beijing	--	70.2	30.1	24.6	40.7	165.6
ShangHai	82.5	--	35.7	97.0	32.9	248.1
GuangZhou	84.0	44.1	--	14.5	24.9	167.5
Nanjing	68.8	201.5	27.0	--	29.4	326.7
Xi'an	128.4	71.7	37.8	12.2	--	250.1
$\sum IP$	363.7	387.5	130.6	148.3	127.9	--
F	0.45	0.64	1.28	2.20	1.96	--

6 Semantic Analysis of Population Movements among Cities

The analysis above aims to predict the inflows and outflows of a city, in this section, our goal is to gain insight into what attracts people in the city. Each city has its own characteristics, people shuttle in various cities holding different purposes. We can learn attractive functionality of the city according to distribution of the queried POIs from other cities. We have selected some representative cities to measure and analysis, and made some basic rules to complete semantic recognition. The results are shown in the following static graphs, they do give us important insights on the characteristics of different cities and regular patterns of users' query behavior.

From the static graphs, we can find out many interesting regular patterns.

1. *Transportation facility is necessary in different cities.* As we can see from the Fig.s above, POIs of transportation facility (such as airports, railway stations, bus stations etc.) are queried most frequently. The reason is obvious to explain, important transportation stations are necessary for users to enter another city no matter what destinations they want to go to.

2. *Proportions structure of POIs types is almost similar in one city.* As shown in Fig.7, the types of query POI distribution from Beijing to Shanghai and Hangzhou to Shanghai is very similar, we find that the sort order from the highest to the lowest according to queried frequency is the same. We can find this phenomenon from many other cities' data which is not shown here because of space constraints. This phenomenon indicates that each city has its own distinctive features and functionalities that attracts people.

3. *The adjacent regularity.* We can see from Fig.7 and Fig.8, The Hangzhou-Shanghai require amount is much higher than Hangzhou-Beijing require amount, and queries related to hospitals and universities occupy a very important proportion. However, there are few difference between Shanghai-Hangzhou require amount and

that of Beijing-Hangzhou, there are many queries are related to scenery spots. To sum up, when people need to go to a city for some affairs, they prefer go to cities that are relatively close to them, but do not consider this factor too much while going for a trip to the famous scenery spots.

The semantic study of population movements among cities according to WMS logs is a fertile field to explore, which have great commercial value as it enable to Fig. out the requirements of users and attractions of cities. There are huge logs are produced every day, which wait for measuring, mining and understanding, having many interesting but challenging research problems and unparalleled wealth of knowledge.

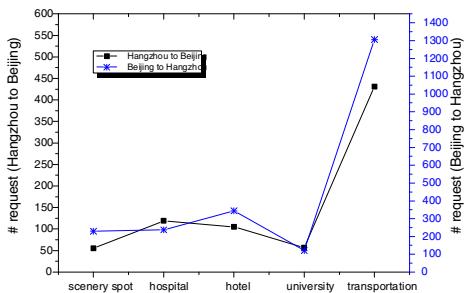


Fig. 7. Query categories of flows between Hangzhou and Shanghai

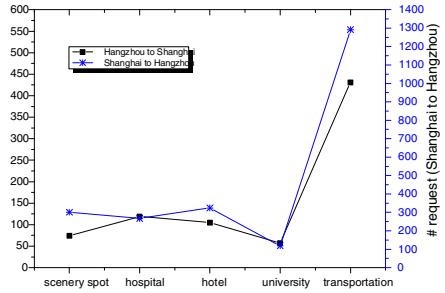


Fig. 8. Query categories of flows between Hangzhou and Beijing

7 Related Work

7.1 Urban Computing

With the rapid development of urbanization, the concept of urban computing came into being. Urban computing is a process of acquisition, integration, and analysis of big and heterogeneous data generated by a diversity of sources in urban spaces to tackle the major issues that cities face. Most of the related works are based on log records from handheld GPS devices of volunteers and GPS trajectory from taxicab. One of the most useful and prospective fields is quantitative urban planning, such as discovering regions of different functions in a city using human mobility and POIs [6], answering top-k similar region queries [9]; another popular field is recommender system based on GPS trajectory from taxicab, such as inferring taxi status using GPS trajectories [10], urban computing with taxicabs [11] etc.

7.2 Location-Based Social Networks

Nowadays, LBS services become an indispensable part of daily life and user behavior become more and more abundant, a new field of studying location-based social network (LBSN) emerges. A location-based social network (LBSN) bridge the gap

between users and their physical location, study the relationships between them, and complex networks they formed [12]. This field aims at understanding user behaviors, finding social relationships of users, and provide intelligent recommendation system for user based on data mining. One aspect of LBSN research focus on mining and understanding user behaviors, such as searching user's life on web maps according to history location records so as to remind user of daily routine [13], mining individual life pattern [14]. Another field of LBSN makes efforts on travel recommendations, discovering activities around [15] and so on.

Our work is very different from the above work. From the perspective of data objects, our work are based on large-scale WMS logs which possess many instinct properties including non-structured, low value intensity, prospects characteristics. From the perspective of research techniques, our difficulty focus on overcoming time discontinuity, non-structural data, non-uniformed specifications and so on. We combine the two methods including semantic logs analysis and spatio-temporal data computing together, so as to mining WMS log data, supplementary, we screening logs based on semantic analysis. Our work provide effective ideas for future studies on analyzing and mining of large-scale WMS logs.

8 Conclusion

Our research is based on the PC-end users' searching logs. First, by measuring the user behavior from both macro and micro perspective using cookie as users' identification, we show that the PC-end log information has prospective user behavior characteristics and could be used to predict group events and urban mobility. Second, we find out that the searching frequency of users' Point of Interest (POI) has Zipf distribution, which means most of people are interest in some minor POIs. We also explain the physical meaning of the parameters and present urban mobility distribution and the average degree of city functional modules. Finally, by combining the analysis result of trans-regional users' searching behavior and activity track delay, we analyze and predict several large cities' population mobility characteristics and the mutual population mobility relationship.

Acknowledgments. This paper is supported by the 863 plan (2013AA013501), the National Science and Technology Major Project under grant (no.2013ZX03002003-004), the NSFC (61272459, 61221063, 61170245), the Fundamental Research Funds for Central Universities.

References

1. Lin, S., Gao, Z., Xu, K.: Web 2.0 traffic measurement: analysis on online map applications. In: Proceedings of the 18th International Workshop on Network and Operating Systems Support for Digital Audio and Video, pp. 7–12. ACM (2009)
2. Xie, X., Zheng, Y., Trajectories, G.L.G.P.S.: Understanding User Behavior Geospatially. Contextual and Social Media Understanding and Usage

3. Li, Q., Zheng, Y., Xie, X., et al.: Mining user similarity based on location history. In: Proceedings of the 16th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, p. 34. ACM (2008)
4. Weber, I., Castillo, C.: The demographics of web search. In: Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 523–530. ACM (2010)
5. Bao, J., Zheng, Y., Mokbel, M.F.: Location-based and preference-aware recommendation using sparse geo-social networking data. In: Proceedings of the 20th International Conference on Advances in Geographic Information Systems, pp. 199–208. ACM (2012)
6. Yuan, J., Zheng, Y., Xie, X.: Discovering regions of different functions in a city using human mobility and POIs. In: Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 186–194. ACM (2012)
7. Hive, <http://hive.apache.org/>
8. Zipf, G.K.: The psycho-biology of language (1935)
9. Sheng, C., Zheng, Y., Hsu, W., Lee, M.L., Xie, X.: Answering top-k similar region queries. In: Kitagawa, H., Ishikawa, Y., Li, Q., Watanabe, C., et al. (eds.) DASFAA 2010, Part I. LNCS, vol. 5981, pp. 186–201. Springer, Heidelberg (2010)
10. Zhu, Y., Zheng, Y., Zhang, L., et al.: Inferring taxi status using gps trajectories. arXiv preprint arXiv:1205.4378 (2012)
11. Zheng, Y., Liu, Y., Yuan, J., et al.: Urban computing with taxicabs. In: Proceedings of the 13th International Conference on Ubiquitous Computing, pp. 89–98. ACM (2011)
12. Zheng, Y.: Tutorial on location-based social networks. In: WWW (2012)
13. Zheng, Y., Xie, X., Zhang, R., et al.: Searching your life on web maps. In: SIGIR Workshop on Mobile Information Retrieval (2008)
14. Ye, Y., Zheng, Y., Chen, Y., et al.: Mining individual life pattern based on location history. In: Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM 2009, pp. 1–10 IEEE (2009)
15. Zheng, Y., Xie, X.: Learning travel recommendations from user-generated gps traces. ACM Transactions on Intelligent Systems and Technology (TIST) 2(1), 2 (2011)

NC-STP: A High Performance Network Coding Based Space Transport Protocol*

Hai Fu, Wanrong Yu, Chunqing Wu, Baokang Zhao, and Zhenqian Feng

School of Computer, National University of Defense Technology, Changsha, China 410073
{harryford.hf, yu.wanrong}@gmail.com,
{wuchunqing, bkzhao, zhqfeng}@nudt.edu.cn

Abstract. Because of the long propagation delay and high PERs in space links, a proper transport protocol is required to transmit data reliably and effectively in space networks. To meet that demand, the Delay/Disruption Tolerant Network (DTN) is proposed, which calls for new designed principles in order to achieve efficient and reliable communication between DTN peers. In this paper, we propose a novel Network Coding based Space Transport Protocol (NC-STP) as a transport scheme for the space network. The NC-STP combines the advantages of auto retransmission and network coding, while at the same time keeps its controlling mechanism very simple. Known from other solutions, NC-STP retransmits the line combination of original packets instead of the original packets themselves and can transmit files in a continuous manner. We evaluate the performance of NC-STP both theoretically and experimentally. The results reveal that NC-STP can achieve better performance than DSTP.

Keywords: DTN, DSTP, Network Coding, Controlling Mechanism, Reliability.

1 Introduction

It is a great challenge to propose new transport protocols for transferring files efficiently over space links because the outer space links are characterized by high PERs and long propagation delays, and the classical transport protocol such as TCP[1] is no longer suitable in such environment. Thus, how to implement the InterPlaNetary (IPN) [2] Internet, has become a hot topic in the research of future network.

There are numerous researches focusing on deep space communication, such as Delay-/Disruption-Tolerant Networking (DTN)[3,4], the CFDP[5], LTP[6], DTTP[7], Saratoga[8], DSTP[9,10] and so on. Despite of so many works in this field, how to provide a considerable service in space communication remains a great challenge, due to the special characteristics of the deep space data link.

In this paper, we propose a novel transport protocol called Network Coding based Space Transport Protocol (NC-STP) by combining network coding technology[11]

* This work is supported by National Natural Science Foundation of China (NSFC), under agreement no 61103182 and 61379147.

with auto retransmission. In NC-STP, the sender side retransmits a coded packet every $1/x - 1$ original packets (x represents the PER), and the coded packet is a random linear combination of the previous $1/x - 1$ original packets, which is based on the technology of network coding. We evaluate the properties of NC-STP and make a comprehensive comparison between NC-STP and DS-TP. Through the simulation results, we conclude that NC-STP can transmit a file faster than DS-TP.

The rest of the paper is organized as follows: in Section 2, the related works on transport protocols over the space DTNs are discussed briefly. Section 3 proposes in detail the mechanisms and algorithms of the NC-STP. Section 4 includes the theoretical evaluation of NC-STP versus DS-TP. The extensive simulation results are provided in Section 5. Section 6 concludes the paper and provides some directions for future works.

2 Related Works

There are numerous transport layer protocols over outer space links, one of which is Saratoga [8]. It is a rate-based UDP/IP file transfer protocol, designed for dedicated point-to-point links between DTN Peers. Saratoga achieves efficient transmission by delivering data packets at the line rate. It also uses a negative acknowledgment strategy in order to deal with channel bandwidth asymmetries.

A similar protocol to Saratoga is the Licklider Transmission Protocol (LTP) [6], which is a point-to-point protocol applied as a DTN convergence layer. LTP can transfer unnamed blocks of data by dividing each block of data into two parts: the reliable “red” part and the unreliable “green part”.

Deep Space Transport Protocol (DS-TP) [9, 10] also can be adapted to serve as an efficient DTN convergence layer, by implementing a retransmission technique called Double Automatic Retransmission (DAR). DAR retransmits each packet at a certain time after the original transmission. Therefore, when packets are corrupted due to link error, they will eventually be replaced by the same packets that DAR retransmits.

Similarly to DS-TP, Network Coding based convergence layer Reliable TransPort mechanism (NC-RTP) [12] is proposed to provide effective communication service between DTN peers. It can reach a higher transmission rate by sending a redundant coded packet every M original packets (M represents $1/x - 1$). The coded packet is a random linear combination of previous M original packets. In case of a single packet lost, the receiver could decode and generate it using the $M - 1$ original packets and the corresponding coded packet.

3 Network Coding Based Space Transport Protocol

3.1 The Basic Idea

Network coding has great advantages in the communication networks, especially in the wireless networks. The central idea of network coding is to send the combination

of multiple original packets while not the single original packet. This makes data transmission over the lossy wireless networks robust and effective.

Applying network coding to the TCP protocol can enhance transmitting properties significantly [13]. To take advantages of network coding, the NC-STP automatically retransmits one coded packet every $\frac{1}{x} - 1$ original packets. Thus, the $\frac{1}{x} - 1$ original packets and the corresponding coded one make up a group. This coded packet is a random linear combination of the given original packets. More precisely, we use the simple linear computation to get the coded packet based on given original packets. For example, if the packets are as follows, 11010(packet 1), 10100(packet 2), 00111(packet 3), then the corresponding coded packet is 01001 (see Fig.1.).

$$\begin{array}{r}
 11010 \\
 + 10100 \\
 + 00111 \\
 \hline
 = 01001
 \end{array}$$

Fig. 1. Example computation of coded packet

In the ideal case, during the transmission, only one packet will be lost in a group on average. Using the coded packet, NC-STP can generate any original packets if only one packet of this group is lost. To achieve the same goal, the DS-TP has to retransmit each packet, while NC-STP only needs to transmit the coded one. If $k(k \geq 2)$ packets in a group are lost, NC-STP needs to retransmit only $k - 1$ packets. Because when these $k - 1$ packets are received, the rest can be generated as well. For example, if $x = 0.25$, which means one out of four packets is corrupted on average, NC-STP transmits one coded packet every three original packets (see Fig. 2).

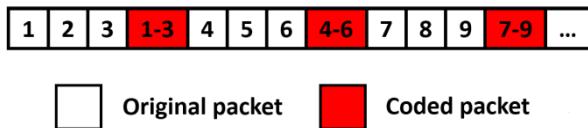


Fig. 2. Example packet transmission sequence

3.2 Details of the NC-STP Protocol

The operation process of the NC-STP will be described in detail in the rest part of this section. The initial value of PER x can be set by previous transmit experience. In the transmit process, the sender side can compute the value of x depending on the acknowledgement information from the receiver side. In this study, we consider that the PER is fixed during the transmit process to simplify the analysis.

The main symbols used throughout the rest of the paper are included in Table 1. Table 2 (a) and (b) are two tables maintained and used in receiver side, recording information of the received original packets and coded packets.

Table 1. Symbols

Symbol	Meaning
x	Link error rate
P_i	Original packet
C_i	Coded packet
T	File size
r_i	Number of retransmit packets during i th round
n	Number of rounds
R	Ratio of packets transmitted in total to the file size.
a_i	Number of packets lost during the i th round in DS-TP
w_i	Number of packets transmitted during the i th round in NC-STP

Table 2.

(a) T_o (Table of original packets)

Original Packet	Coded Packets Involved
P_1	C_1, C_6, \dots
P_2	C_1, C_7, \dots
.....
P_i	C_i, C_j, \dots
.....

(b) T_c (Table of coded packets)

Coded Packet	Original Packets Involved
C_1	P_1, P_2, \dots
C_2	P_4, P_5, \dots
.....
C_i	P_i, P_j, \dots
.....

Sender procedure:

The sender always transmits the first packet in the sending queue, and then moves it to the end of the queue. Every time it has transmitted $\frac{1}{x} - 1$ original packets, it generates a coded packet using the previous $\frac{1}{x} - 1$ original ones and sends it. When the sender receives an ACK, it deletes the ACKed packet from the sending queue. Keep sending packets in the sending queue until the queue is empty.

Receiver procedure:

1) When receiving an original packet P_i , add it to the original-queue, send back an ACK, and do JUDGE (P_i). Check table T_o and T_c (see Table 2 (a) and (b)) to see whether there are any coded packets (represented by C_j) in T_c that will cause no more packets decoded and generated, or, more precisely, whether every original packet involved in C_j is already in the original-queue. If so, delete such coded packets in T_c, T_o and coded-queue. Then delete P_i in T_o.

2) When receiving a coded packet C_i , add it to the coded-queue, and check table T_o and T_c to see if there is only one original packet involved in C_i is not in the original-queue (can be generated). If so, generate such packet and do the receiver procedure again. If not, send back ACK of one of the lost packets involved in C_i , add those original packets (represented by P_j) involved in C_i that are not ACKed into T_o. If P_j is already in T_o, add C_i into its Coded Packets Involved.

JUDGE (P_i):

Check T_o and T_c to see whether the original packet will cause a new packet to be generated. To be more precise, if among all original packets involved in C_i (C_i is the coded packet involved in P_i), there is only one packet that is not in the original-queue. If so, decode it and do receiver procedure again.

4 Theoretical Evaluation

In order to simplify the theoretical evaluation, some modifications are made to the NC-STP. We define a round to be the end-to-end transmission of a specific amount of data. A round starts when a packet is sent out from the sender side and ends when all the ACKs are received. During each round, the sender sends all original packets in the sending-queue and coded packets as well. Since packets that were ACKed had been deleted from the sending-queue, those packets still in the queue are all unACKed. We also make assumptions that the link PER remains fixed during the file transfer and ACKs are sent back to the sender side without lost, which means that all acknowledgement information are sent back to the source side successfully.

4.1 DS-TP and Simplified NC-STP

According to the operational properties of DS-TP, the sender side will transmit all original packets and redundant packets during the first round, or, to be more precise, a redundant packet is transmitted every $\frac{1}{x} - 1$ packets. Let r_1 be the number of packets that are retransmitted during the first round, then $r_1 = T / (\frac{1}{x} - 1)$. That is to say, r_1 packets are transmitted twice and $T - r_1$ packets are transmitted only once. We assume that a_1 packets are lost during the first round (and need to be retransmitted during the second round).

$$a_1 = (T - r_1) * x + r_1 * x^2 \quad (1)$$

Substituting r_1 into Eq. (1), we get that:

$$a_1 = T * x * (1 - x) \quad (2)$$

Generalizing Eq. (2), we assume that during the n th round, the DS-TP sender will need to transmit a_n packets, where

$$a_n = T * x^n * (1 - x^n) \quad (3)$$

The file transfer is complete, once the following equation holds:

$$T * x^n * (1 - x^n) < 1 \quad (4)$$

$$n_{DSTP} = \log_{x*(1-x)}(x * (1 - x))^n = \log_{x*(1-x)} 1/T = \frac{\ln 1/T}{\ln x*(1-x)} \quad (5)$$

Some simplifications are made to the NC-STP in order to calculate the theoretical number of rounds for completing a file transmission. The simplified NC-STP is quite similar to NC-RTP, so we use the theoretical evaluation of NC-RTP for reference. In NC-RTP, the sender side transmits all the original packets and one redundant coded packet every $1/x - 1$ original packets during the first round.

Let $y = 1/x$, then the whole file is divided into $T/(y - 1)$ parts. In one part, if zero or only one packet is lost (including original and coded packets), it needs no retransmission. If $k(k \leq y)$ packets are lost, only $k - 1$ packets are needed to be retransmitted.

Let p_k represents the probability of k packets retransmission in a single part ($k + 1$ packets are lost).

$$p_k = C_y^{k+1} * x^{k+1} * (1-x)^{y-k-1} \quad (6)$$

Let $E(k)$ represents the expectation of k , which is the number of packets needs to be retransmitted in a single part.

$$E(k) = \sum_{k=1}^y k * p_k = \sum_{k=1}^y k * C_y^{k+1} * x^{k+1} * (1-x)^{y-k-1} \quad (7)$$

Let $k + 1 = j$, we can get

$$E(k) = \sum_{j=2}^y j * C_y^j * x^j * (1-x)^{y-j} - \sum_{j=2}^y C_y^j * x^j * (1-x)^{y-j} \quad (8)$$

As $\sum_{j=0}^y j * C_y^j * x^j * (1-x)^{y-j} = 1$, $\sum_{j=0}^y C_y^j * x^j * (1-x)^{y-j} = (x + 1 - x)^y$,

$$E(k) = (1-x)^{1/x} \quad (9)$$

As is already mentioned earlier, there are $T/(y - 1)$ parts in the file. Thus, during the first round, $E(k) * T/(y - 1)$ packets need to be retransmitted.

$$w_1 = E(k) * T * (y - 1) = T * x * (1-x)^{1/x-1} \quad (10)$$

Generalizing Eq. (10), we assume that during the n th round, the NC-STP sender will need to retransmit w_n packets, where

$$w_n = T * x^n * (1-x)^{n*(1/x-1)} \quad (11)$$

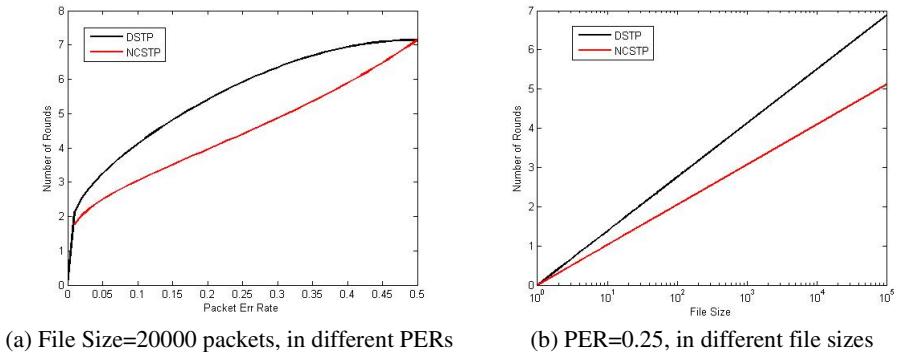
The file transmission is completed, once the following equation holds:

$$T * x^n * (1-x)^{n*(1/x-1)} < 1 \quad (12)$$

$$n_{NC-STP} = \log_{x*(1-x)^{1/x-1}} x^n * (1-x)^{n*(1/x-1)} = \frac{\ln 1/T}{\ln x*(1-x)^{1/x-1}} \quad (13)$$

4.2 Comparison between NC-STP and DS-TP

The Eqs. (5) and (13) are presented together in two figures to compare the performance of DS-TP and NC-STP.

**Fig. 3.** Number of rounds to transmit a file

Results in Fig.3 (a) reveal that, when the PER is smaller than 0.01, performances of DS-TP and NC-STP are almost the same, because both of them help little with few packets lost. But as the PER grows, NC-STP finishes a file transmission in fewer rounds than DS-TP until the PER reaches 0.5, where NC-STP and DS-TP operate in the same way (transmit each packet twice). Fig.3 (b) shows that, the number of rounds grows linearly with the logarithm of File Size in both DS-TP and NC-STP. But in NC-STP, it grows slower, meaning that with the file size increasing, DS-TP will need more and more rounds to complete a transmission than NC-STP.

Our theoretical evaluation reveal that, NC-STP can complete a file transmission in fewer rounds than DS-TP. Observing the results shown in Fig.3 (a) and (b), we can conclude that NC-STP performs better in dealing with large file transmissions over space links with high PERs. It is noteworthy that, the performance showed in Fig.3 (a) and (b) is just of a simplified NC-STP (i.e. NC-RTP). The real NC-STP can perform even better.

5 Experimental Evaluation

5.1 Simulation Settings

We implement the NC-STP and DS-TP in C++ language and explore their performance over a simple one-hop topology. Obviously, the primary interest is the time required for the whole file to be delivered successfully to the receiver side. To simplify the simulation, we assume that the link rate and RTT are fixed during our experiment. In the chosen topology, we send a file from the source node to the destination node each time and check the number of rounds needed to finish a file transmission. We run the simulation 10 times and calculate the average number of rounds for each protocol.

Table 3. Simulation parameters

Parameter	Value
Link rate (packets per second)	1000
File size (number of packets)	$10, 100, 1000, 2000, 5000, 10^4, 2*10^4, 5*10^4, 10^5$
Packet Error Rate	0, 0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.4, 0.5
RTT (seconds)	100

5.2 Results of the Simulation

Number of Rounds. Using the two simulating C++ programs that mentioned earlier, we can obtain the number of rounds that NC-STP and DS-TP need to transmit a file.

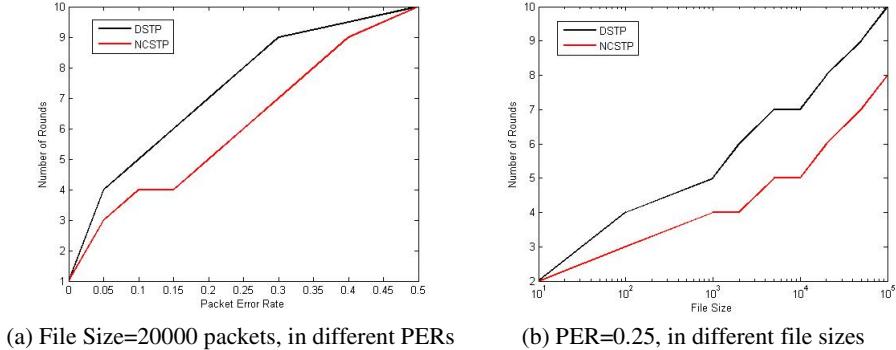


Fig. 4. Number of rounds to transmit a file

Results in Fig.4 (a) and (b) reveal that the experimental results are approximately the same with theoretical evaluation. DS-TP needs more rounds to finish a transmission and with the increasing of file size, the number of rounds grows more rapidly in DS-TP. We can conclude that the NC-STP is more suitable than DS-TP in large file transmission with high PERs.

Packets Ratio R. During a file transmission, the numbers of packets transmitted in total are always larger than the file size because of the redundant packets that the two protocols retransmit. Since the bandwidth of space links is limited, more packets usually means more time to finish a file transmission.

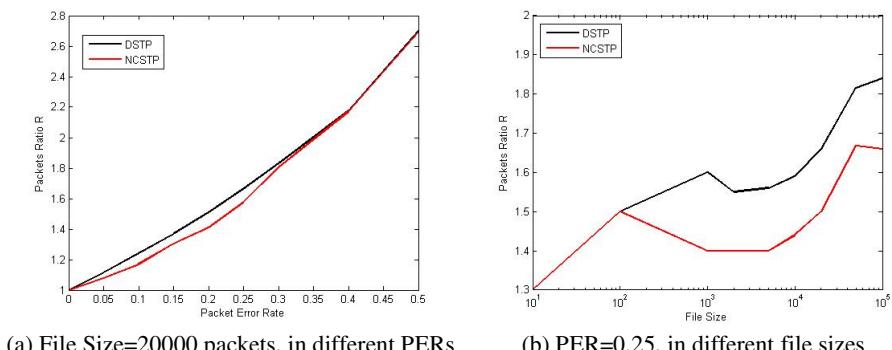


Fig. 5. Packet ratio

The results shown in Fig.5 (a) and (b) reveal that, the packet ratio R of NC-STP is always smaller than that of DS-TP and it is also revealed in Fig.5 (b) that with the file size increasing, the packet ratio R of DS-TP grows sharply than that of NC-STP. Therefore we can conclude that, with limited bandwidth in space links, NC-STP can complete a file transmission faster and perform better than DS-TP in space networks.

Transmission Time Z. Assumption is made that the next round begins when all the ACKs of the present round are sent back to the sender side. In order to obtain the transmission time Z , we just need to add RTT of every round to the time of file transmission. Let n be the number of rounds and v be the link rate.

$$Z = \frac{T}{v} + n * RTT \quad (14)$$

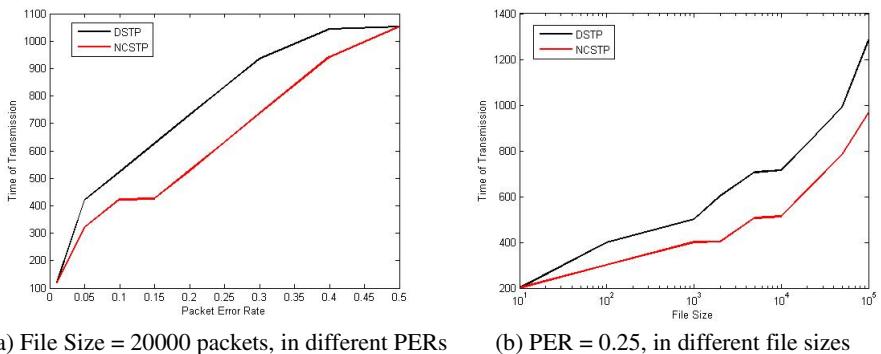


Fig. 6. Transmission time

Fig.6 (a) and (b) show that, the transmission time of NC-STP is smaller than that of DS-TP, which means that NC-STP can transmit a file faster than DS-TP. It can be noticed that Fig. 6 (a) and (b) are similar to Fig. 4 (a) and (b) which is because the time of transmission is highly relevant to the RTT of the transmission links in space DTNs, owing to that RTTs in space links is always very large.

6 Conclusions and Future Works

In this paper, we propose a novel protocol called Network Coding based Space Transport Protocol (NC-STP) by combining network coding with DS-TP. In order to simplify the controlling scheme of DS-TP and transmit files in a continuous manner, NC-STP retransmits coded packets while DS-TP retransmits original ones. Moreover, in the NC-STP, the receiver side only needs to send back ACKs of the received packets as well as generated ones. It's much simpler to control the transmission by ACKs than by both SNACK₁ and SNACK₂.

Our theoretical and experimental evaluations reveal that NC-STP can finish a file transmission faster and transmit fewer packets in total than DS-TP. So NC-STP is more suitable than DS-TP in space networks with high PERs and long propagation delays. NC-STP is also more efficient and reliable in large file transmission.

Although the theoretical evaluation and the simulation results seem very positive, there are still some issues in NC-STP that need to be further investigated. In future works, we will focus on how to react when the ACKs sent back from the receiver side are lost and how to deal with the changing PER under more practical scenarios.

References

1. Akan, O.B., Fang, J., Akyildiz, I.F.: Performance of TCP protocols in deep space communication networks. *IEEE J. Communications Letters* 6(11), 478–480 (2002)
2. Akyildiz, I.F., Akan, Ö.B., Chen, C.: InterPlaNetary Internet: state-of-the-art and research challenges. *J. Computer Networks* 43(2), 75–112 (2003)
3. Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Weiss, H.: Delay-tolerant networking architecture. *RFC4838* (2007)
4. Scott, K.L., Burleigh, S.: Bundle protocol specification. *J. RFC 5050* (2007)
5. Sheets, B.B.P.: Ccsds File Delivery Protocol (CFDP). *J.* (2004)
6. Ramadas, M., Burleigh, S.: Licklider transmission protocol-specification. *J. RFC 5326*, experimental (2008)
7. Samaras, C.V., Tsaooussidis, V., Peccia, N.: DTTP: a delay-tolerant transport protocol for space internetworks. In: Second Ercim Workshop on Emobility, p. 3 (2008)
8. Wood, L., Eddy, W.M., Ivancic, W., McKim, J., Jackson, C.: Saratoga: a Delay-Tolerant Networking convergence layer with efficient link utilization. In: International Workshop on Satellite and Space Communications, IWSSC 2007, pp. 168–172. IEEE Press (2007)
9. Psaras, I., Papastergiou, G., Tsaooussidis, V., Peccia, N.: DS-TP: Deep Space Transport Protocol. In: Proceedings of IEEE Aerospace Conference, Montana, USA (March 2008)
10. Papastergiou, G., Psaras, I., Tsaooussidis, V.: Deep-space transport protocol: a novel transport scheme for space DTNs. *Computer Communications* 32(16), 1757–1767 (2009)
11. Sundararajan, J.K., Shah, D., Médard, M., Mitzenmacher, M., Barros, J.: Network coding meets TCP. In: IEEE INFOCOM, pp. 280–288. IEEE Press (2009)
12. Haoliang, S., Lixiang, L., Xiaohui, H.: A network coding based DTN convergence layer reliable transport mechanism over interplanetary networks. *J. International Journal of Computers Communications & Control* 6(2), 236–245 (2011)
13. Sundararajan, J.K., Jakubczak, S., Médard, M., Mitzenmacher, M.: Barros: Interfacing network coding with TCP: an implementation. *J. arXiv preprint arXiv: 0908.1564* (2009)

Implementing the Matrix Inversion by Gauss-Jordan Method with CUDA^{*}

Ning Tian¹, Longjiang Guo^{1,2,✉}, Meirui Ren^{1,2}, and Chunyu Ai³

¹ School of Computer Science and Technology, Heilongjiang University, China

² Key Laboratory of Database and Parallel Computing, Heilongjiang, China

³ Division of Math & Computer Science, University of South Carolina Upstate, USA
longjiangguo@gmail.com

Abstract. Solving the matrix inversion is an open problem which is often related to scientific computation. Moreover, matrix inverse also has wide applications in social networks. Individuals in social networks are described as nodes, and the similarity among nodes are significant for link prediction. Usually, the problem of calculating similarities among nodes is converted to the problem of matrix inversion. With the increasing of the orders of matrices, traditional sequential algorithms are unable to meet the needs for the short calculation time. Although cluster systems can solve the inversion of large-scale matrices efficiently, the equipment cost and power consumption are very high. This paper proposes a parallel algorithm PA-Gauss, which is based on the Gauss-Jordan method of selecting the main element. CUDA (Computer Unified Device Architecture) of GPU (Graphic Process Unit) is used to implement the proposed algorithm to solve inversions of the real and complex matrices. The experimental results show that the Gauss-Jordan algorithm can save more running time than traditional sequential algorithms and the speedup ratio of PA-Gauss for Real Matrices is 633~100435, and the speedup ratio of PA-Gauss for Complex Matrices is 224~36508. Therefore, the computing time of solving the matrix inversions is reduced significantly.

1 Introduction

Solving the matrix inversion is one of the most common and important operation in linear algebra [1]. It has wide applications in scientific computing [2]. Solving the matrix inversion can directly help to solve the nonlinear programming, optimization, ordinary differential equations. Moreover, matrix inverse also has wide applications in social networks. Individuals in social networks are described as nodes, and the similarity among nodes are significant for link prediction. Usually, the problem of calculating similarities among nodes is converted to the problem of matrix inversion [3,4].

* This work is supported by Program for Group of Science and Technology Innovation of Heilongjiang Educational Committee under grant No.2013TD012, the Science and Technology Research of Heilongjiang Educational Committee under grant No.12511395.

✉ Corresponding author.

Nowadays, because of its importance and wide applications, the matrix inversion problem becomes one of the main computational tasks of high-performance computing. Moreover, with the development of advanced technologies and the improvement of computing power, the size of matrices which people deal with has been increased dramatically in many fields. Therefore, algorithms which can solve the matrix inversion of large-scale matrices are urgently needed. For some practical problems, the orders of matrices often reach thousands, tens of thousands, or even millions [5]. However, the majority of methods for solving the matrix inversion adopt the sequential methods [6] or parallel methods on cluster systems. The speed of sequential solutions is undoubtedly very slow for large matrices. The speed of cluster systems is much faster than the sequential methods in solving the inverse of matrices. Nevertheless, using cluster systems brings an dramatic increase in equipment costs and energy consumption [7].

In recent years, GPU is already famous for the programming capabilities for the large-scale fast calculations. The CUDA technology proposed by NVIDIA is an outstanding representative of this area. For example, A.A.Aqrabi et al. presented a method using compression for large seismic data sets on modern GPUs and CPUs [8]. J.Barnat et al. designed a new CUDA-aware procedure for pivot selection and implemented parallel algorithms using CUDA accelerated computation [9]. Andrei Hagiescu et al. applied an automated architecture-aware mapping of streaming applications onto GPUs [10].

This paper proposes a parallel algorithm named the Gauss-Jordan algorithm of selecting the main element which is implemented by CUDA on GPU to solve the inverse matrix of the real and complex matrices [11]. The experimental results show that the proposed Gauss-Jordan algorithm can save more running time than traditional sequential algorithm and the speedup ratio of PA-Gauss for Real Matrix is 633~100435, and the speedup ratio of PA-Gauss for Complex Matrix is 224~36508. The contributions of this paper are summarized as follows:

- This paper proposes a parallel algorithm to solve the inverse matrix of the real and complex matrices with CUDA on GPU.
- The paper implements the proposed parallel algorithm on Intel Core i5-760 quad-core CPU, NVIDIA GeForce GTX460 card, and Win7 64-bit operating system. The computing time of traditional sequential algorithms is reduced significantly.

2 Preliminaries

Here we introduce some knowledge about the definitions of the matrix inversion and several methods which solve this problem. For a matrix A which is $n*n$, if there exists another matrix B which is also $n*n$, $A * B = B * A = E$ is established, we called the matrix A is reversible, and the matrix B is the inverse matrix of matrix A , which is notated A^{-1} . There are many methods which are commonly used to solve inverse matrix. The definition method is applicable to any reversible matrix, but it has large amount of computation when the orders of matrix are quite large. Using accompanied matrix method has the large

amount of computation, and usually it is applicable to seek low-level matrix inversion. Elementary transform and block matrix are other two methods of matrix inverse. The Gauss–Jordan of selecting the main element occupies a small storage space, and it has small amount of computation, high-speed computation. The biggest advantage is generating results of high precision. For different methods, the time complexity is different. Such as the time complexity of definition methods is $O(n^3)$. Block matrix is $O(n^3)$. Using elementary transform is $O(n^3)$. Accompanied matrix is $O(n + 2)$. The time complexity of selecting main element Gauss–Jordan is $O(n^3)$. In summary, Gauss–Jordan of selecting main element is the most widely used, effective, and reasonable method. However, all the tests of the algorithm are sequential programming implementations, the speed of sequential solutions undoubtedly is very slow for large matrices. Because of GPU’s excellent floating-point calculation capabilities, large memory bandwidth, and relatively low price, it plays a significant role in many application fields. Hence, in this paper we proposes and implements a parallel algorithm with CUDA which is called the Gauss–Jordan algorithm of selecting the main element to solve the matrix inverse for the real and complex matrices.

3 Gauss–Jordan Algorithm

3.1 Sequential Gauss–Jordan Algorithm

Gauss–Jordan Algorithm for the Real Matrix. The basic idea of Gauss–Jordan method for real matrix is: when k is from 0 to $(n - 1)$, we do the following several steps:

1. We select the element which has the maximum absolute value from the lower right corner sub-matrix which starts from the k th row and the k th column. Record the row number and the column number. Then we switch the element to the position of the main element by switching rows and columns.
2. $a_{k,k} \leftarrow 1/a_{k,k}$.
3. For j is from 0 to $(n - 1)$, and j is not equal to k , $a_{k,j} \leftarrow a_{k,j} * a_{k,k}$.
4. For i and j are from 0 to $(n - 1)$, and i and j are not equal to k , $a_{i,j} \leftarrow a_{i,j} - a_{i,k} * a_{k,j}$.
5. For i is from 0 to $(n - 1)$, and i is not equal to k , $a_{i,k} \leftarrow -a_{i,k} * a_{k,k}$.

Finally, according to the information recorded of switched rows and columns in the whole process of selecting the main element, we do the recovery. The principles of recovery are as follows: in the whole process of selecting the main element, the row and column that firstly are switched do the recovery at last. The original switched row is restored with the switched column, and the original switched column is restored with the switched row.

Gauss–Jordan Algorithm for the Complex Matrix. The complex matrix consists of two parts, the real part and the complex part: $A = AR + j*AI$. Its most important function is the complex conjugate operation which is corresponding to the transpose of the matrix, the real matrix cannot finish it. So the

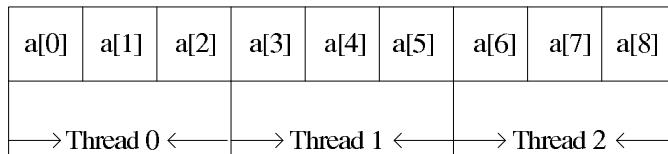
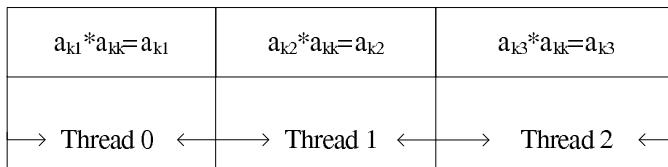
$$A = \begin{bmatrix} 0.236 & 0.247 & 0.257 & 1.267 \\ 1.116 & 0.125 & 0.140 & 0.149 \\ 0.158 & 0.168 & 0.177 & 0.187 \\ 0.197 & 0.207 & 0.217 & 0.227 \end{bmatrix}$$

Fig. 1. The example matrix

computing of the complex matrix has practical significance. The basic idea is similar with the real matrix. We need compute two parts respectively: the real matrix part and the complex matrix part.

3.2 Parallel Gauss-Jordan Algorithm

Algorithm Description Of Gauss-Jordan For Real Matrix Suppose matrix A is an $n * n$ matrix. So we need 2^x threads and allocate m threads for per block. Here we let m is not less than n . Here $x \leftarrow \log_2(n - k)$, because we suppose that the numbers of our matrix are the power of 2, that is the length of the array is 2^x . There are $(2^x)/m$ blocks. For the matrix shown in Fig.1, n is 4, k is 0, then we need to compute the maximum absolute value from the lower right corner sub-matrix which starts from the row 0 and the column 0, that is the maximum absolute value of $(n - k - 1)(n - k - 1) = 3 * 3 = 9$ elements.

**Fig. 2.** The thread work structure of example matrix**Fig. 3.** The thread work structure of the third step of example matrix

Here we use three threads to compute the maximum absolute value of nine elements. Thread 0 finishes elements from zero to two, thread 1 is from three to five, thread 2 is from six to eight. After computing all the nine elements, we get

three elements in the Fig.2. At last, we use thread 0 to compute the maximum absolute value of the three elements. That is also the maximum absolute value of the nine elements. For the third step, we use $(n - 1) = 3$ threads to compute $a_{k,j} \leftarrow a_{k,j} * a_{k,k}$, every thread finishes $a_{k,j} \leftarrow a_{k,j} * a_{k,k}$. The remaining two steps are similar. Fig.3 and Algorithm 1 show the details of performing the orthogonal similarity transformation.

The kernel function of the Gauss-Jordan algorithm of selecting the main element for solving the matrix inversion of the real matrix is shown in Algorithm 2.

Algorithm 1. Element_Maxvalue($a[], n$)

Input: The array $a[]$ is used to stored the matrix elements, the matrix order is n **Output:** The maximum absolute value of array c is f_m , the row number is is and the column number js .

```

1:
2: ThreadID  $\leftarrow$  blockidx.x * BLOCKSIZE + threadidx.x
3:  $x \leftarrow \log(n - k)$ ,  $s \leftarrow (2^x)/2$ 
4: if (ThreadID < n) then
5:   we use  $(n-k-1)$  thread to compute the maximum absolute value of  $(n-k-1)$  elements, every
   thread finish  $(n-k)$  elements, and the row coordinate is  $is$ , the column coordinate is  $js$ ,
6: end if
7: if (ThreadID = 0) then
8:   we find the maximum absolute value of  $n$  elements, which is the maximum absolute value of
    $(n-k-1)*(n-k-1)$  elements using one for cycle.
9: end if
10:  $f_m \leftarrow c[0]$ ,  $m \leftarrow \text{rowindex}[0]/n$ 
11:  $is \leftarrow \text{rownumber}$ ,  $js \leftarrow \text{columnnumber}$ 
```

Algorithm Description of Gauss-Jordan for Complex Matrix. We use similar method to store the elements of the complex matrix. The kernel function is described in Algorithm 3.

4 Experimental Results and Analysis

4.1 The Time Complexity of Sequential Algorithm

The time complexity of one loop is studied. The time complexity of selecting the element of the maximum absolute value from the lower right corner sub-matrix is $O(n - k)$. For switching the element to the main element of the position by switching row and column, the time complexity is $O(n)$. So, the time complexity of the first step is $O((n - k) * n)$. For the third step of the sequential algorithm: $a_{k,j} \leftarrow a_{k,j} * a_{k,k}$, the time complexity is $O(n - 1)$. The time complexity of computing the $a_{i,j} \leftarrow a_{i,j} - a_{i,k} * a_{k,j}$ in the forth step is $O((n - 1) * (n - 1))$. For the final step of the sequential algorithm: $a_{i,k} \leftarrow -a_{i,k} * a_{k,k}$, the time complexity is $O(n - 1)$. At last we do the recovery, which is similar with the first step, the time complexity is $O(n - k)$. In summary, the total time complexity of the sequential algorithm is $O((n - 1) * (n - 1))$.

Algorithm 2. Real_Matrix_Inversion($a[]$, n)

Input: The array $a[]$ is used to stored the matrix elements, the matrix order is n , the iteration parameter is k ; Output: The inversion matrix A^{-1} .

```

1: 
2:  $ThreadID \leftarrow blockIdx.x * BLOCKSIZE + threadIdx.x$ 
3:  $k \leftarrow 1$ ,  $fm \leftarrow 0$ 
4: for  $i = 0$  to  $n - 1$  do
5:   Call kernel function: Element_Maxvalue( $a[ ]$ ,  $n$ )
6:   if ( $fabs(fm) = 0$ ) then
7:     if  $is! = k$  then
8:       if  $ThreadID < (n - 1)$  then
9:          $u \leftarrow k * n + ThreadID + 1$ ,  $v \leftarrow is * n + ThreadID + 1$ 
10:         $D_t[ThreadID] \leftarrow a[u]$ ,  $a[u] \leftarrow a[v]$ ,  $a[v] \leftarrow D_t[ThreadID]$ 
11:      end if
12:    end if
13:    if  $js! = k$  then
14:      if  $ThreadID < (n - 1)$  then
15:         $u \leftarrow (ThreadID + 1) * n + k$ ,  $v \leftarrow (ThreadID + 1) * n + js$ 
16:         $D_t[ThreadID] \leftarrow a[u]$ ,  $a[u] \leftarrow a[v]$ ,  $a[v] \leftarrow D_t[ThreadID]$ 
17:      end if
18:    end if
19:    if  $ThreadID < (n - 1)$  then
20:      if  $ThreadID! = k$  then
21:         $u \leftarrow k * n + (ThreadID + 1)$ 
22:         $a[u] \leftarrow a[k * n + (ThreadID + 1) * a[l]$ 
23:      end if
24:    end if
25:    for  $i = 0$  to  $n - 1$  do
26:      if  $i! = k$  then
27:        if  $ThreadID < (n - 1)$  then
28:          if  $ThreadID! = k$  then
29:             $u \leftarrow i * n + ThreadID + 1$ ,  $a[u] \leftarrow a[u] - a[i * n + k] * a[k * n + ThreadID + 1]$ 
30:          end if
31:        end if
32:      end if
33:    end for
34:    if  $ThreadID < (n - 1)$  then
35:      if  $ThreadID! = k$  then
36:         $u \leftarrow (ThreadID + 1) * n + k$ ,  $a[u] \leftarrow -a[u] * a[l]$ 
37:      end if
38:    end if
39:  end if
40: end for
41: for  $k = n - 1$  to  $0$  do
42:   if  $js! = k$  then
43:     if  $ThreadID < (n - 1)$  then
44:        $u \leftarrow k * n + ThreadID + 1$ ,  $v \leftarrow js * n + ThreadID + 1$ 
45:        $p \leftarrow a[u]$ ,  $a[u] \leftarrow a[v]$ ,  $a[v] \leftarrow p$ 
46:     end if
47:   end if
48:   if  $is! = k$  then
49:     if  $ThreadID < (n - 1)$  then
50:        $u \leftarrow i * n + k$ ,  $v \leftarrow i * n + is$ 
51:        $D_t[ThreadID] \leftarrow a[u]$ ,  $a[u] \leftarrow a[v]$ ,  $a[v] \leftarrow D_t[ThreadID]$ 
52:     end if
53:   end if
54: end for

```

Algorithm 3. Complex_Matrix_Inversion($ar[]$, $ai[]$, n)

Input: The array $ar[]$ $ai[]$ is used to stored the matrix elements, the matrix order is n , the iteration parameter is k ; Output : The inversion matrix AR^{-1} , AI^{-1} .

```

1: 
2:  $ThreadID \leftarrow blockidx.x * BLOCKSIZE + threadidx.x$ 
3:  $k \leftarrow 1$ ,  $fm \leftarrow 0$ 
4: for  $i = 0$  to  $n - 1$  do
5:   Call kernel function: Element_Maxvalue( $a[ ]$ ,  $n$ )
6:   if ( $fabs(fm) = 0$ ) then
7:     if  $is! = k$  then
8:       if  $ThreadID < (n - 1)$  then
9:          $u \leftarrow k * n + ThreadID + 1$ ,  $v \leftarrow is * n + ThreadID + 1$ 
10:         $D_t[ThreadID] \leftarrow ar[u]$ ,  $ar[u] \leftarrow ar[v]$ ,  $ar[v] \leftarrow D_t[ThreadID]$ 
11:         $D_t[ThreadID] \leftarrow ai[u]$ ,  $ai[u] \leftarrow ai[v]$ ,  $ai[v] \leftarrow D_t[ThreadID]$ 
12:      end if
13:    end if
14:    if  $js! = k$  then
15:      if  $ThreadID < (n - 1)$  then
16:         $u \leftarrow (ThreadID + 1) * n + k$ ,  $v \leftarrow (ThreadID + 1) * n + js$ 
17:         $D_t[ThreadID] \leftarrow ar[u]$ ,  $ar[u] \leftarrow ar[v]$ ,  $ar[v] \leftarrow D_t[ThreadID]$ 
18:         $D_t[ThreadID] \leftarrow ai[u]$ ,  $ai[u] \leftarrow ai[v]$ ,  $ai[v] \leftarrow D_t[ThreadID]$ 
19:      end if
20:    end if
21:    if  $ThreadID < (n - 1)$  then
22:      if  $ThreadID! = k$  then
23:         $u \leftarrow k * n + (ThreadID + 1)$ 
24:         $p \leftarrow a[k * n + (ThreadID + 1) * ar[l]$ 
25:         $q \leftarrow ai[u] * ai[l]$ 
26:         $s \leftarrow (ar[u] + ai[u]) * (ar[l] + ai[l])$ 
27:         $ar[u] \leftarrow p - q$ 
28:         $ai[u] \leftarrow s - p - q$ 
29:      end if
30:    end if
31:    for  $i = 0$  to  $n - 1$  do
32:      if  $l! = k$  then
33:         $v \leftarrow i * n + k$ 
34:        if  $ThreadID < (n - 1)$  then
35:          if  $ThreadID! = k$  then
36:             $u \leftarrow k * n + ThreadID + 1$ ,  $w \leftarrow i * n + ThreadID + 1$ 
37:             $p \leftarrow ar[u] * ar[v]$ ,  $q \leftarrow ai[u] * ai[v]$ 
38:             $s \leftarrow (ar[u] + ai[u]) * (ar[v] + ai[v])$ 
39:             $t \leftarrow p - q$ ,  $b \leftarrow s - p - q$ 
40:             $ar[w] \leftarrow ar[w] - t$ ,  $ai[w] \leftarrow ai[w] - b$ 
41:          end if
42:        end if
43:      end if
44:    end for
45:    if  $ThreadID < (n - 1)$  then
46:      if  $ThreadID! = k$  then
47:         $u \leftarrow (ThreadID + 1) * n + k$ ,  $p \leftarrow ar[u] * ar[l]$ ,  $q \leftarrow ai[u] * ai[l]$ 
48:         $s \leftarrow (ar[u] + ai[u]) * (ar[l] + ai[l])$ 
49:         $ar[u] \leftarrow q - p$ ,  $ai[u] \leftarrow p + q - s$ 
50:      end if
51:    end if
52:  end if
53: end for
54: for  $k = n - 1$  to  $0$  do
55:   if  $js! = k$  then
56:     if  $ThreadID < (n - 1)$  then
57:        $u \leftarrow k * n + ThreadID + 1$ ,  $v \leftarrow js * n + ThreadID + 1$ 
58:        $D_t[ThreadID] \leftarrow ar[u]$ ,  $ar[u] \leftarrow ar[v]$ ,  $ar[v] \leftarrow D_t[ThreadID]$ 
59:        $D_t[ThreadID] \leftarrow ai[u]$ ,  $ai[u] \leftarrow ai[v]$ ,  $ai[v] \leftarrow D_t[ThreadID]$ 
60:     end if
61:   end if
62:   if  $is! = k$  then
63:     if  $ThreadID < (n - 1)$  then
64:        $u \leftarrow i * n + k$ ,  $v \leftarrow i * n + is$ 
65:        $D_t[ThreadID] \leftarrow ar[u]$ ,  $ar[u] \leftarrow ar[v]$ ,  $ar[v] \leftarrow D_t[ThreadID]$ 
66:        $D_t[ThreadID] \leftarrow ai[u]$ ,  $ai[u] \leftarrow ai[v]$ ,  $ai[v] \leftarrow D_t[ThreadID]$ 
67:     end if
68:   end if
69: end for

```

4.2 The Time Complexity of Parallel Algorithm

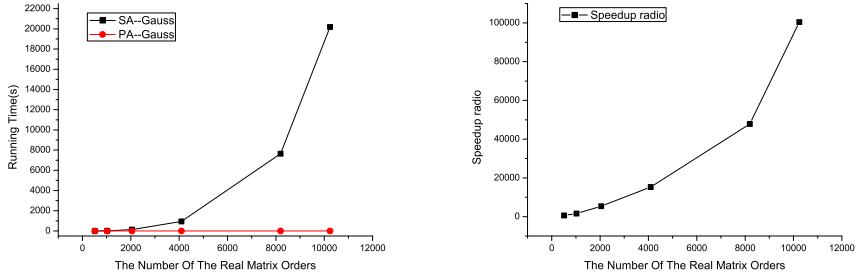
The first part of the first step of the parallel algorithm is similar with the sequential algorithm, the time complexity is $O(n - k)$. Then we switch the element to the position of the main element by switching row and column, which is done by n threads in parallel, the time complexity is $O(1)$. So the time complexity of the first step is $O(\log(n - k - 1))$. The third step of the parallel algorithm is to use $n - 1$ threads to implement $a_{k,j} \leftarrow a_{k,j} * a_{k,k}$, the time complexity is $O(n - 1)$. We use $n - 1$ threads to implement $a_{i,j} \leftarrow a_{i,j} - a_{i,k} * a_{k,j}$, the time complexity is $O(n - 1)$. Then we need $n - 1$ threads to implement $a_{i,k} \leftarrow -a_{i,k} * a_{k,k}$. The time complexity is $O(n - 1)$. At last we also do the similar recovery, which is done by n threads in parallel, the time complexity is $O(1)$. In summary, the total time complexity of the parallel algorithm is $O(n - 1)$.

4.3 Experimental Results

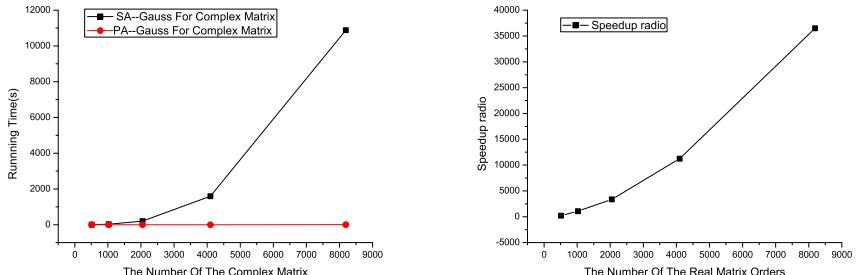
Experimental Results of the Real Matrix. In our experimental environment, we use Intel Core i5-760 quad-core CPU, NVIDIA GeForce GTX460 card, and Win7 64-bit operating system. The data of the matrix are randomly generated with a random function. Our environment of compiling and running is Visual Studio 2010. In the first experiment, we test the running time of the sequential algorithm and parallel algorithm when the size of real matrix is 512×512 , 1024×1024 , 2048×2048 , 4096×4096 , 8192×8192 , and 10240×10240 , respectively. The results are shown in Fig.4a. It can be seen that the running time of the sequential algorithm increases with the order of the matrix; however, the running times of parallel algorithm do not increase obviously when the number of matrix order increases. Overall, the parallel algorithm has quite shorter running time compared with the sequential algorithm. So the running time performance of the parallel version is very satisfactory due to the fact that we implement the most part of computation in parallel, and all the parts in parallel are time-consuming calculation. Therefore, the overall running time in parallel is quite short compare with sequential implementation. Fig.4b show the speedup ratio according to the running time of the Fig.4a. It can be seen that as the size of matrix increases, the speedup ratio increases quickly. And the maximum of the speedup ratio of PA-Gauss for real matrix has reached 100435.

Experimental Results of the Complex Matrix. In the second experiment, we evaluate the running time of the sequential algorithm and parallel algorithm when the size of complex matrix are 512×512 , 1024×1024 , 2048×2048 , 4096×4096 , and 8192×8192 , respectively. The results are shown in Fig.5a. It can be also seen that the parallel running time has been decreased significantly and obviously.

Fig.5b shows the speedup ratio according to the running time of the Fig.5a. It can be seen that as the size of matrix increases, the speedup ratio increases sharply. The maximum of the speedup ratio of PA-Gauss for complex matrix has reached 36508. So our algorithm obtains an impressive speedup ratio, and



(a) Real matrix order vs. running time. (b) Real matrix order vs. speedup ratio.

Fig. 4. Running time and speedup ratio while matrices are real

(a) Complex matrix order vs. running time. (b) Complex matrix order vs. speedup ratio.

Fig. 5. Running time and speedup ratio while matrices are complex

does not add too computational costs obviously. Furthermore, the speed of traditional sequential algorithms are very slow which are unable to meet the needs of applications. Our proposed algorithm overcomes this problem as well.

5 Conclusion

According to the characteristic of CUDA, this paper proposes a parallel algorithm, Gauss-Jordan. Gauss-Jordan is implemented by CUDA (Computer Unified Device Architecture) on GPU (Graphic Process Unit) to solve the inverse matrix of the real and complex matrices. The proposed algorithm solves the problem without high computational costs such as using cluster systems and the slow speed of traditional sequential algorithms. The new algorithm also provides a new way to solve the inverse matrix of the real and complex matrices. In addition, the experimental results show that the Gauss-Jordan algorithm of selecting the main element can save more running time than traditional sequential algorithms, and the speedup ratio of PA-Gauss for Real Matrix is 633~100435 and the speedup ratio of PA-Gauss for Complex Matrix is 224~36508.

References

1. Nash, J.C.: Compact Numerical Methods for Computers: Linear Algebra and Function Minimisation, 2nd edn. Adam Hilger, Bristol (1990)
2. Brini, A., Marino, M., Stevan, S.: The uses of the refined matrix model recursion. *Journal of Mathematical Physics* 52(5), 291–315 (2011)
3. Chakrabarti, S.: Dynamic personalized pagerank in entity-relation graphs. In: 16th International Conference on World Wide Web (WWW), pp. 571–580. ACM, New York (2007)
4. Tong, H., Faloutsos, C., Koren, Y.: Fast direction-aware proximity for graph mining. In: 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), pp. 747–756. ACM, New York (2007)
5. Foo, S.L., Silvester, P.P.: Finite Element Analysis of Inductive Strips in Unilateral Finlines. *IEEE Microwave Theory and Techniques* 41(2), 298–304 (1993)
6. Jodr, L., Law, A.G., Rezaizadeh, A., Watson, J.H., Wu, G.: Computations for the Moore-Penrose and Other Generalized Inverses. *Congress. Numer.* 80, 57–64 (1991)
7. Press, W.H., Flannery, B.P., Teukolsky, S.A., Vetterling, W.T.: Numerical Recipes in FORTRAN: The Art of Scientific Computing, 2nd edn. Cambridge University Press, Cambridge (1992)
8. Aqrabi, A.A.: Three Dimensional Convolution of Large Data Sets on Modern GPUs. Norwegian University of Science and Technology (2009)
9. Barnat, J., Bauch, P., Brim, L., Ceska, M.: Computing Strongly Connected Components in Parallel on CUDA. In: 25th IEEE International Symposium on Parallel and Distributed Processing (IPDPS), pp. 544–555. IEEE Press, New York (2011)
10. Hagiescu, A., Huynh, H.P., Wong, W., Goh, R.S.M.: Automated architecture-aware mapping of streaming applications onto GPUs. In: 25th IEEE International Symposium on Parallel and Distributed Processing (IPDPS), pp. 467–478. IEEE Press, New York (2011)
11. Ben-Israel, A., Greville, T.N.E.: Generalized Inverses: Theory and Applications. Wiley-Interscience, New York (1977)

Operator Scale Out Using Time Utility Function in Big Data Stream Processing^{*}

Mahammad Humayoo¹, Yanlong Zhai^{1, **}, Yan He²,
Bingqing Xu¹, and Chen Wang¹

¹ School of Computer Science, Beijing Institute of Technology, Beijing, China 100081
ylzhai@bit.edu.cn

² Science and Technology on Complex Systems Simulation Laboratory, Beijing, China

Abstract. Many important big data applications require real-time processing of arriving data with high scalability, especially some IoT applications in where devices generate infinite data and environments are intrinsically volatile. Most of current Stream Processing Systems(SPS), like Storm or S4, often show an insufficient scalability as the architecture is based on static configurations. Although considerable research and industry effort has been invested on scale out of operators in SPS, most of them focus on how to scale out different type of operators based on an on-demand infrastructure. Few of them consider when and which operators should be scale out, as improper scale out may introduce extra overhead to the system. In this paper, we present a novel approach for finding bottleneck operator at run time and scale out only bottleneck operator. An algorithm is designed to find out bottleneck operator based on time utility function(TUF) model. The algorithm utilizes utility profit, utility penalty and utility threshold to evaluate the utility accrual of a run-time operator. With the rewarding of early completions and penalizing of missing deadline, the algorithm will scale out the operator when the utility accrual below the threshold. Experimental results show that our time-aware utility accrual approach can exactly identify and efficiently scale out the bottleneck operator at run time in data stream processing system.

Keywords: Stream processing, Big data, Scalability, Utility accrual.

1 Introduction

Big data is a fast emerging topic among both industry and academia, it is featured by 3Vs: Volume, Variety and Velocity. Volume is size of data. Variety is different type of data industry generating i.e. structured, semi-structured and unstructured. Velocity is the speed data is generating. The main challenge for big data is that how to extract required information within given time limit.

* This work is supported by National 863 Programme(No 2013AA01A212) "Kernel Software and System for Intelligent Cloud Service and Management Platform".

** Corresponding author.

Therefore, several big data processing tools emerge, like Hadoop[1] and Storm [2]. Hadoop is mostly used for off-line data processing, whereas Storm is adequate for on-line stream process. Nowadays, more data-intensive applications and technologies require online massive data processing instead of traditional store-then-process system with minimum latency[3]. For example, WSN applications; web companies such as Facebook, LinkedIn and Twitter execute daily data mining queries to analyze their latest web logs[4]; online marketplace providers such as eBay and BetFair run sophisticated fraud detection algorithms on real-time trading activity[5]; telecommunication companies require to detect fraud in real time is in the range of thousands user per second[6]. There is high demand of predictability, resource efficiency and scalability of Stream Processing Engine(SPE) because data load vary frequently and result required with minimal delay.

A stream processing system can be modeled as a query in SPE with several data stream. A query is defined as a direct acyclic graph where each node is an operator and edges define data flows. Typical query operators of SPEs are analogous to relational algebra operators and can be classified as stateless or stateful [7]. Stateless operators (e.g., Map, Union, and Filter) do not keep state across tuples and perform their computation solely based on each input tuple. Stateful operators (e.g., Aggregate, Join, and Cartesian Product (CP)) perform operations on sequences of tuples. Because of the infinite nature of the data stream, stateful operators perform their computation on sliding windows of tuples defined over a period of time or as a fixed number of tuples [6].

Existing SPEs, such as Apache S4 [8] and Twitter Storm, do not have mature mechanism to support run time scale out of bottleneck operators. Some previous works either they scale out the whole query or some fixed partition of the query[6], or they investigate the approaches on how to scale out stateful and stateless operators[9, 19–22]. But none of these researches explain how do they identify the bottleneck operator or what is the method to identify bottleneck operators? Our main focus of this research is to exactly pinpoint bottleneck operator based on run-time facts using utility accrual. Based on these primitives mentioned above, we propose an operator scale out approach using Time Utility Function(TUF) for real-time data stream processing. In our approach we use TUF based on a task model similar to the profit and penalty model introduced by Kumar V et al. [10] to improve the resource utilization of cloud computing applications. We believe that, to improve the performance of any computing system, it is important to not only measure the profit when completing a job in time, but also account for the penalty when a job is aborted or discarded. Note that, before a task is aborted or discarded, it consumes system resources including network bandwidth, storage space, and processing power, and thus can directly or indirectly affect the system performance[13]. If a job is deemed to miss its deadline with no positive semantic gain, a better choice should be one that can detect it and discard it as soon as possible. For illustrative purpose, consider a following example given below.

Figure 1 shows the query of a stream processing application. Data source is time-based windows input stream. In this case the window size is 60 sec. During

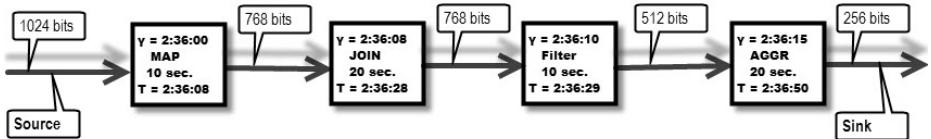


Fig. 1. stream processing

one window (60s) the operator may receive certain amount of data to process. The quantity of data may vary during each window size due to various factors like device generating more data, etc. There are four operators in this query to process incoming tuples: Map, Join, Filter and Aggregate. The execution environment is described by several factors, like incoming data in bits $\rho(t)$, data arrival time(γ_i), start time to process data(T_i) and best possible deadline (D_i), etc. An Operator processes its fraction of data and forwards its output to next operator. The size of the output data may be increased or decreased after the processing of data by an operator. When new data arrive to each operator, SPE must check the load (bottleneck) status of the operator using time utility function to see whether the operator becomes bottleneck if processing current data under certain factors because bottleneck jeopardizes performance of system. If any one of operator is found as bottleneck, its interrupt data transmission to other operators and contaminates the performance of non-bottleneck operators because of operator Interdependence. So we must share its processing load among set of new partitioned operators thus it avoids adding further load to operator, which is already overloaded[6, 9]. Scale out operator in advance is being the icing on the cake because we prevent misuse of resources on recovery of failed operator. Our prognostic scheme discovers the bottleneck operator in advance and scale out it before it becomes real bottleneck which also boosts the performance of system.

Remainder of the paper is organized as follows: Section 2 describes the models we used in the paper and formulate the problem formally. Section 3 presents experiment and evaluation. Related works are discussed in Section 4 and we present the conclusions in Section 5.

2 Time-Aware Operator Scale Out

2.1 System Model

Data Stream Model. A stream S is an infinite series of tuples $s \in S$. A tuple $s = (t, \gamma, \rho)$ has a logical timestamp t , γ is a tuples arrival time to operator for processing and a size of tuples ρ . The timestamp $t \in \mathbb{N}^+$ is assigned by a monotonically increasing logical clock of an operator when a tuple is created in a stream. Tuples in a stream are ordered according to their timestamps. Logical timestamps is used to make provision for handling data that is late or delayed, missing, or out-of-sequence[14]. We create tuples from infinite stream S based

on time-based windows. Therefore, stream $S = \{s_1, s_2, \dots, s_n\}$, γ_i represent their particular arrival time and ρ_i represents their specific size.

Operator Model. $O = \{o_1, o_2, \dots, o_n\}$ is the set of operators, where $o_i \in O$ represents an operator which process incoming tuples. An operator o accepts input streams S , processes their tuples s i.e. $\{s_1, s_2, \dots, s_n\}$ and produce output streams \overline{S} . For ease-of-presentation, we consider that an operator takes a single input stream and emits a single output stream.

Execution of Task. In this paper, we assume a single sequence of arrived tuples. Let Γ denote task of operators o . The act of processing incoming tuples s by operators o is called task of operators. Operator tasks $\Gamma = \{\tau_1, \tau_2, \dots, \tau_n\}$, with τ_i defined using the following parameters:

- $[B_i, W_i]$: The best case execution time and the worst case execution time of τ_i ;
- D_i : The relative deadline of τ_i ;
- $f_i(t)$: The probability density function for the execution time of τ_i ;
- $G_i(t)$: The profit TUF, which represents the profit accrued when a task is completed at time t . We assume $G_i(t)$ is a non-increasing unimodal function before its deadline, i.e. $G(t_i) \geq G(t_j)$ if $t_i \leq t_j$ and $G_i(t) = 0$ if $t \geq D_i$;
- $L_i(t)$: The penalty TUF, which represents the penalty suffered when a task is discarded or aborted or exceeded deadline at time t . We assume $L_i(t)$ is a non-decreasing unimodal function before its deadline, i.e. $L(t_i) \leq L(t_j)$ if $t_i \leq t_j$, and a task is immediately discarded once it missed its deadline;
- $\rho_i(t)$: Size of tuple arrives to operators for processing;
- $c_i(t)$: Cpu utilization during execution of task τ_i ;
- $m_i(t)$: Memory utilization during execution of task τ_i .

As shown above, an operator execution task is associated with both a utility gain function and a utility penalty function with function value varying with time. Therefore, while executing a task has a potential to gain profit, it also has a possibility to face a penalty if it misses its deadline. The system performance is therefore calculated by its total utility gain minus utility penalty.

2.2 The Operator Runtime Utility Function

The execution time of an operator could not be known in advance. Therefore it is not sure if executing the task will lead to missing of deadline or not. The execution time depends to a great extent upon the work load and the assigned resources of the operator. To satisfy the real-time requirement of the system, we must try to make every operator finish the task in time. Accordingly, the operator who is going to be the bottleneck of the query needs to be scaled out. To help make the decision of scaling out an operator, we use a mathematical formula as metric, i.e. the expected accrued utility. Given an execution task of operator τ_i with tuples arrival time γ_i to operator for processing, assume that

the start time of the task τ_i is T . Then the expected profit ($\bar{G}(T)$) to execute τ_i can be described as an Expected Utility Gain Formula:

$$\bar{G}(T) = \int_{B_i}^{D_i - (T_i - \gamma_i)} G_i(t + (T_i - \gamma_i)) f_i(t) \rho_i(t) c_i(t) m_i(t) dt \quad (1)$$

Similarly, the expected loss ($L_i(T)$) to execute τ_i can be described as:

$$\bar{L}(T) = L_i(D) \int_{D_i - (T_i - \gamma_i)}^{W_i} f_i(t) \rho_i(t) c_i(t) m_i(t) dt \quad (2)$$

Therefore, the expected accrued utility ($\bar{U}_i(T)$) to execute τ_i can be described as:

$$\bar{U}_i(T) = \bar{G}(T) - \bar{L}(T) \quad (3)$$

2.3 The Operator Runtime Utility Threshold

A operator can be bottleneck or chosen for scale out when $\bar{U}_i(T) < 0$, which means that the probability to obtain positive gain is smaller than that to incur a loss. By considering some hinder factors, we can further limit the operator scale out by imposing a threshold (δ) to the expected accrued utility, i.e. an operator is bottleneck or can be chosen for scale out if

$$\bar{U}_i(T) \leq \delta \quad (4)$$

We call δ as the expected utility threshold.

2.4 The Operator Runtime Utility Critical Point

Furthermore, since the task execution time of operator is not known a prior, suppose operator starts processing of stream tuples but Operator is taking long time to process. It means that operator has bottleneck or some problem so we need to decide whether to continue or abort the execution of a task for scale out operator. The longer we execute the task, the closer we are to the completion point of the task. At the same time, however, the longer the task executes the higher penalty the system has to endure if the task cannot meet its deadline. To determine the appropriate time to abort a task for scale out, we employ another metric, i.e. the critical point.

Let operator's task τ_i starts its execution at T . Then the potential Profit at $\tilde{T} > T$ (i.e. $\tilde{G}(\tilde{T})$) can be represented as the Expected Potential Utility Gain Formula:

$$\tilde{G}(\tilde{T}) = \int_{\tilde{T} - T_i}^{D_i - (T_i - \gamma_i)} G_i(t + (T_i - \gamma_i)) f_i(t) \rho_i(t) c_i(t) m_i(t) dt \quad (5)$$

Similarly, the potential loss at $\hat{T} > T$ (i.e. $\tilde{G}(\hat{T})$) can be represented as the Expected Potential Utility Penalty Formula:

$$\tilde{L}(\hat{T}) = L_i(D) \int_{D_i - (T_i - \gamma_i)}^{W_i - \hat{T}} f_i(t) \rho_i(t) c_i(t) m_i(t) dt \quad (6)$$

Therefore, the expected accrued utility at $\hat{T} >$ (i.e. $\tilde{U}_i(\hat{T})$) can be represented as:

$$\tilde{U}_i(\hat{T}) = \tilde{G}(\hat{T}) - \tilde{L}(\hat{T}) \quad (7)$$

We can make $\tilde{U}_i(\hat{T}) = 0$ and solve for t_0 . Then when executing task τ_i to time t_0 , the expected profit equals its expected loss. We call t_0 as the critical point for executing task τ_i . Due to the non-increasing nature of G_i , $\tilde{U}_i(\hat{T})$ is monotonically decreasing as t increases. Therefore, it is not difficult to see that the continuous execution of τ_i beyond the critical point will more likely bring a loss rather than a positive gain [10].

2.5 Bottleneck Operator Identification

The SPE calculate runtime utility gain $\Rightarrow G_i(t)$ and runtime utility loss $\Rightarrow L_i(t)$ using equation 1 and 2 respectively. See the evaluation part for details of generating input parameters.

Algorithm 1 is executed to examine operator status whenever new tuple arrives to operator o for processing. First, the SPE takes input parameters (line 1). It then calculates utility gain $\Rightarrow G_i(t)$ and utility penalty $\Rightarrow L_i(t)$ of every arrived tuples for each operator using for loop (line 2, 3, 4). The runtime utility accrual $\Rightarrow U_i(t)$ for each operator is calculated using equation 3 in line 5. The runtime utility accrual $\Rightarrow U_i(t)$ is compared with threshold value δ to determine status of operator (line 6) using equation 4. If statement of line 6 is true, it finds bottleneck operator in line 7.

Algorithm 1. Expected accrued utility algorithm to find out bottleneck operators

- 1: **Input:** Let $\{\tau_1, \tau_2, \dots, \tau_k\}$ be the operators tasks to process incoming tuples s, let $\gamma_i, i = 1, \dots, k$ represent tuples specific arrival times. Let current time be t, and expected time to start processing incoming tuples be T. Let the expected utility threshold be δ .
 - 2: **for** $i = 0 \rightarrow k$ **do**
 - 3: Calculate gain $\Rightarrow G_i(t)$
 - 4: Calculate loss $\Rightarrow L_i(t)$
 - 5: Calculate Utility Accrual $\Rightarrow U_i(t) \equiv G_i(t) - L_i(t)$
 - 6: **if** $U_i(t) \leq \delta$ {Utility Accrual is less than required threshold value} **then**
 - 7: Found **Bottleneck** operator .start scale out process.
 - 8: **end if**
 - 9: **end for**
-

3 Experiment and Evaluation

In this section, we evaluate our operator scale out approach with respect to time, load and threshold value. We first evaluate utility accrual ($\bar{U}_i(T)$), utility gain ($\bar{G}_i(T)$) and utility loss ($\bar{L}_i(T)$). Then we evaluate critical point and finally we evaluate $\bar{U}_i(T)$, $\bar{G}_i(T)$, $\bar{L}_i(T)$ against load.

3.1 Evaluation Setup

The test cases in our experiments are randomly generated. The followings are the details:

- Parameters B, W, and D are randomly generated such that they are uniformly distributed within interval of [1, 10], [30, 60], and [40, 50], respectively.
- The execution time of an operator is assumed to be evenly distributed between interval of [B, W] i.e. $f_i(t) = 1 \div (W_i - B_i)$.
- G, L were assumed to be linear functions, i.e. $G(t) = -ag^*(t - D)$ in the range of [0, D] and $L(t) = al^*t$. The gradient for G(t) and L(t), i.e. ag and al were randomly chosen from the interval of [4, 10] and [1, 5], respectively.
- Operator execution Task release times intervals follow the exponential distribution with $\lambda = 5$.
- The utility threshold δ is set 13075.579. This is median value of four operators. For each operator we run our experiment 60 times and then take median of generated value. There are four median values, each for one operator. Finally we again take median value of these four operator median value and we get 13075.579.
- $\rho_i(t)$: Size of stream tuples are generated randomly in the range of [128, 1024] KB.
- $c_i(t)$: Cpu utilization is generated randomly in the range of [0, 1].
- $m_i(t)$: Memory utilization is also generated randomly in the range of [0, 1].

Each experiment was run 60 times and we report averaged measurements for more accuracy.

3.2 Evaluation Result

Figure 2 shows accrued utility, accrued profit, as well as the accrued penalty against tuples processing time of operator. It is shown that accrued utility $\bar{U}_i(T)$ and accrued profit $\bar{G}_i(T)$ are gently decreasing while accrued penalty $\bar{L}_i(T)$ is gradually going up when execution time of operator is steadily increasing. This is because of longer the execution of task, closer to completion of task, but longer the execution time means more system resources utilization, like cpu usage, memory usage[13], etc., which means more penalty. So if execution time of an operator exceed threshold value or critical point, it means that the operator is becoming a bottleneck and needs to be scaled out. It is worthless to continue execution after exceeded threshold value because it contributes to reduction of gain.

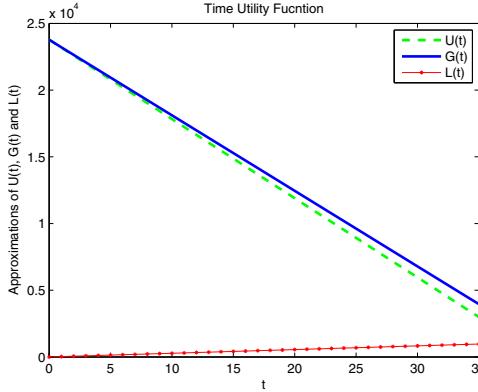


Fig. 2. $\bar{U}_i(T)$, $\bar{G}_i(T)$, $\bar{L}_i(T)$ against time t

Figure 3 below shows the critical point. The critical point is a point where accrued profit $\bar{G}_i(T)$ is equal to accrued penalty $\bar{L}_i(T)$. We can see from the figure that along with the execution of a task on an operator, the utility gain $\bar{G}_i(T)$ is decreasing rapidly, whereas the utility penalty is increasing steadily. After the critical point, accrued penalty $\bar{L}_i(T)$ is always greater than accrued profit $\bar{G}_i(T)$. Therefore, there is no intelligent sense to continue execution of operator after the critical point, because it contributes to increase accrued utility loss only. Thus we must stop execution of current operator and scale out running bottleneck operator. We take the following value of different parameters from randomly generated. $D = 40$, $w = 48.267$, $B = 9$, $ag = 4$, $al = 5$, $m = 0.040$, $c = 0.580$ and $t = 30$ sec., exponential distribution with $\lambda = 5$ and exponential distribution parameter $x = 59$. We get utility gain $\bar{G}(T) = 750.215$ and $\bar{L}(T) = 750.215$. We can see from the value that $\bar{G}(T)$ is equal to $\bar{L}(T)$. The critical point occurs at $t = 30$ with above parameters.

Below Figure 4 plot accrued utility as well as the accrued profit against load. Figure 4 shows that $\bar{U}_i(T)$ and $\bar{G}_i(T)$ are greater than zero during initial load between 100 to 400. During this load resource utilization is less so accrued penalty $\bar{L}_i(T)$ is also less compare to accrued gain $\bar{G}_i(T)$. From that load onwards the accrued utility $\bar{U}_i(T)$ and accrued gain $\bar{G}_i(T)$ have been dramatically declining because of the following reason. First load is increasing continuously and second execution time is prolonged. Thus growing load and long execution time contribute to more resource utilization, which mean greater accrued penalty $\bar{L}_i(T)$. Greater accrued penalty $\bar{L}_i(T)$ means less accrued utility $\bar{U}_i(T)$ and accrued gain $\bar{G}_i(T)$. Figure 4 demonstrates this behaviour quite clearly. So we must scale out operator whenever accrued gain $\bar{G}_i(T)$ is equal to accrued penalty $\bar{L}_i(T)$ (critical point) otherwise it may cause operator to become bottleneck.

Fig.5 demonstrates how to find bottleneck operator for scaling out. This is the evaluation result of Fig.1. For this experiment, we set randomly generated value for time t between 0 and 60. We give data input size $\rho_i(t) = 1024KB$,

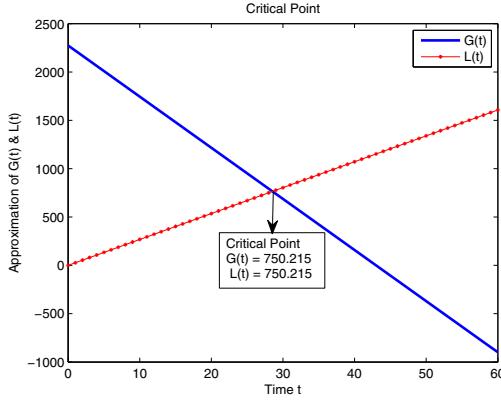


Fig. 3. Find out critical point by approximation of $\bar{G}_i(T)$, $\bar{L}_i(T)$

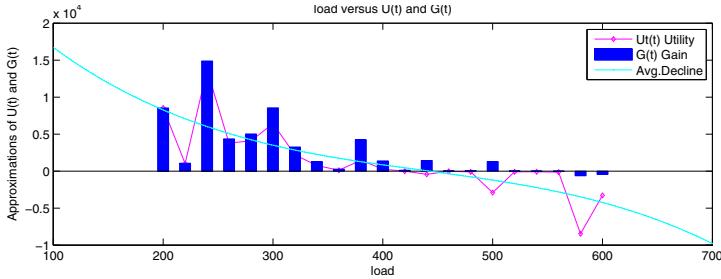


Fig. 4. Approximation of $\bar{U}_i(T)$, $\bar{G}_i(T)$ against load when operator processing stream tuples

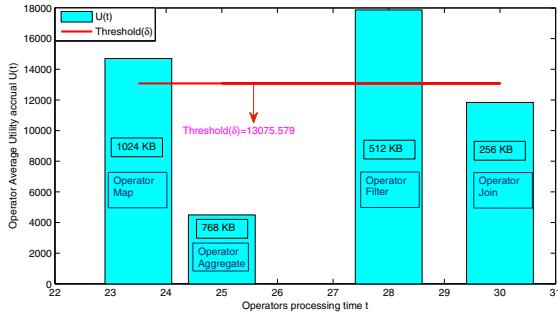


Fig. 5. Average $\bar{U}_i(T)$ against load when operator processing stream tuples

768KB, 512KB and 256KB to cross ponding operators Map, Join, Filter and Aggregate. We run experiment for each operator 60 times and calculate the total utility accrual $\bar{U}_i(T)$. There is 60 $\bar{U}_i(T)$ value for each operators. Then we take median of 60 $\bar{U}_i(T)$ value for each operator. Therefore, we get Average

$\bar{U}_i(T)$ values 14706.677, 11837.935, 17873.025 and 4497.558 to correspondent operators Map, Join, Filter and Aggregate. Similarly we also take median of time for each operators, we get average time 23.5 sec, 30 sec, 28 sec and 25 sec to corresponding operators Map, Join, Filter and Aggregate. We have threshold (δ) value is 13075.579. Thus, According to our algorithms if utility accrual ($\bar{U}_i(T)$) is less equal to threshold(δ) value, it means that this operator has bottleneck and must scale out. So in our example utility accrual($\bar{U}_i(T)$) value of Join and Aggregate operators are 11837.935 and 4497.558 which are less than threshold($\delta = 13075.579$). It means that these two operators Join and Aggregate have bottleneck, we must scale out them as soon as possible.

4 Related Work

Offline and Online Framework: Twitter Storm [2] doesn't support run time scale out and doesn't maintain operator state. Additionally it doesn't have method to identify bottleneck operator in advance because of its stateless behavior. S4 [8] is a scalable distributed SPE that does not use windowing. State information in S4 is continuously maintained but stale data are periodically purged to free memory. It also lacks of dynamic scale out approach and doesn't talk about how to identify bottleneck operator. MapReduce [1] is offline, big batch processing tool in cluster environment. In contrast we are interested in online, fast and real time processing environment. Daewoo Lee et al. [15]. Proposed Large-scale incremental processing with MapReduce named HadUP. HadUP detects and computes the change of datasets at a fine-grained level using a deduplication-based snapshot differential algorithm (D-SD) and update propagation. It means that they use last result to compute next result. But this method is also offline processing and we are interested in online processing.

Elasticity: There are some exist SPEs which provide both scale in and scale out or only one of them. Gulisano et al. [6] describe how to partition the state of specific stateful operators such as join and aggregate for scale out. Each SC periodically monitors incoming load and resource utilization to decide elasticity (scale in and scale out). They don't consider utility gain factor when task is completed within its deadline and utility penalty when task is aborted or not completed within its deadline. They also scale out non-bottleneck operator along with bottleneck operator. In addition, they don't find bottleneck operator in advance. In contrast we identify bottleneck operator in advance based on Utility accrual approach (gain and loss)[10] and scale out only bottleneck operator. Our focus is on bottleneck operator and scale out not scale in. Fernandez et al. [9] presents an integrated approach for scale out and failure recovery by exposing state management of stateful operators. SPS performs checkpoint, backed up, restored and partitioned operation on operator state. The SPS supports dynamic scale out of operators when fault tolerant occur. However they don't mention how they find bottleneck operator to scale out at any time. They assume that if operator failed, they scale out using their policy.

Utility Accrual or Time Utility Function(TUF):Kumar et al. [10] presents a novel utility accrual scheduling algorithm, it is used for scheduling the real-time cloud computing services which accounts for not only the gain by completing a real-time task in time but also the cost when discarding or aborting the task. The most unique characteristics of this approach is that, different from traditional utility accrual approach that works under one single Time Utility Function (TUF), which have two different TUF, a profit TUF and a penalty TUF associated with each task at the same time. To model the real-time applications for cloud computing, that need not only to reward the early completions and also to penalize the missing abortions or deadline misses of real-time tasks. Their scheduling algorithm carefully chooses highly profitable tasks to execute, aggressively removes tasks that potentially lead to large penalty, and judiciously allows preemptions. Our paper is also based on same idea[10].But their works focus on scheduling the real-time cloud computing services and task execution and our research is focus on detection of bottleneck operator and scale out only bottleneck operator in data stream processing. The PP-aware model and scheduling paradigm are first proposed by Yu et al. [16]. In this paper, a task model considers both profit and penalty while executing a task. According to this paper, task is associated with a pair of unimodal time functions, representing system accrued profit when a task is completed before its deadline, or accrued penalty if otherwise. Therefore, one utility function cannot accurately represent both the profit and penalty information when executing a task. Our approach is different from it. First, we use profit TUF and penalty TUF separately, and our focus is on detection of bottleneck operator and scale out only bottleneck operator in data stream processing and their focus is on scheduling the real-time cloud computing services and task execution.

5 Conclusion

We presented a prognostic scheme that can discover bottleneck operator in stream processing applications in advance. With randomly generated parameter and attributed value, we calculated expected gain and loss of each operator when processing certain amount of data. Based on expected gain and loss value we calculate the total utility accrual for each operator. Our algorithm finalizes the operator which is candidate for scale out depending on utility accrual and threshold value. Our experimental results illustrate the effectiveness of our solution in finding an ideal bottleneck operator for scaling out under present existing facts. The work on operator management can be extended in a few directions. One direction for future work is to provide scale in at run time. Another direction is to address fault tolerant of stream processing systems.

References

1. <http://hadoop.apache.org>
2. <http://storm.incubator.apache.org>

3. Babcock, B., et al.: Models and issues in data stream systems. In: Proceedings of the Twenty-first ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. ACM (2002)
4. Russell, M.A.: Mining the Social Web: Data Mining Facebook, Twitter, LinkedIn, Google+, GitHub, and More. O'Reilly Media, Inc. (2013)
5. Parikh, N., Sundaresan, N.: Scalable and near real-time burst detection from e-commerce queries. In: Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM (2008)
6. Gulisano, V., et al.: Streamcloud: An elastic and scalable data streaming system. *IEEE Transactions on Parallel and Distributed Systems* 23(12), 2351–2365 (2012)
7. Abadi, D.J., et al.: Aurora: a new model and architecture for data stream management. *The VLDB Journal the International Journal on Very Large Data Bases* 12(2), 120–139 (2003)
8. Neumeyer, L., Robbing, B., et al.: S4: Distributed Stream Computing Platform. In: ICDMW (2010)
9. Castro Fernandez, R., et al.: Integrating scale out and fault tolerance in stream processing using operator state management. In: Proceedings of the 2013 International Conference on Management of Data. ACM (2013)
10. Kumar, V., Palaniswami, S.: Exploiting Resource Overloading Using Utility Accrual Approach for Parallel Data Processing in Cloud
11. Wu, H., Ravindran, B., Jensen, E.D.: Utility accrual scheduling under joint utility and resource constraints. In: 2004 Proceedings of the Seventh IEEE International Symposium on Object-Oriented Real-Time Distributed Computing. IEEE (2004)
12. Kuno, H.: Surveying the e-services technical landscape. In: Second International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS 2000. IEEE (2000)
13. Liu, S., Quan, G., Ren, S.: On-line scheduling of real-time services for cloud computing. In: 2010 6th World Congress on Services (SERVICES-1). IEEE (2010)
14. Stonebraker, M., Tintemel, U., Zdonik, S.: The 8 requirements of real-time stream processing. *ACM SIGMOD Record* 34(4), 42–47 (2005)
15. Lee, D., Kim, J.-S., Maeng, S.: Large-scale incremental processing with MapReduce. *Future Generation Computer Systems* (2013)
16. Yu, Y., et al.: Profit and penalty aware (pp-aware) scheduling for tasks with variable task execution time. In: Proceedings of the 2010 ACM Symposium on Applied Computing. ACM (2010)
17. Bulut, A., Singh, A.K.: A unified framework for monitoring data streams in real time. In: Proceedings of the 21st International Conference on Data Engineering, ICDE 2005. IEEE (2005)
18. Bartal, Y., et al.: Multiprocessor scheduling with rejection. *SIAM Journal on Discrete Mathematics* 13(1), 64–78 (2000)
19. Zaharia, M., et al.: Discretized Streams: Fault-tolerant streaming computation at scale. In: Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles. ACM (2013)
20. Gedik, B., et al.: Elastic scaling for data stream processing. *IEEE Transactions on Parallel and Distributed Systems* PP(99), 1 (2013)
21. Backman, N., Fonseca, R., Cetintemel, U.: Managing parallelism for stream processing in the cloud. In: Proceedings of the 1st International Workshop on Hot Topics in Cloud Data Processing. ACM (2012)
22. Gedik, B.: Partitioning functions for stateful data parallelism in stream processing. *The VLDB Journal*, 1–23 (2013)

A New Channel Allocation Scheme for Vehicle Communication Networks

Jing Xu, Wei Li, Zan Ma, and Shuo Zhang

University of Science and Technology of China, Anhui, China 230027
`{jxu125,weili011,sa612135,zshuo}@mail.ustc.edu.cn`

Abstract. In roadway networks, the timely, reliable, and high-throughput transmission is particularly important to vehicles, e.g., for roadway safety warning applications. However, it is difficult to achieve these goals at the same time in vehicle-to-vehicle communications due to mobility, interference, etc. In this paper, we tackle this issue and propose a new channel allocation scheme based on OFDM(Orthogonal frequency-division multiplexing). Our design can achieve highly reliable transmission through dynamically allocated interference free channels demanding on timeliness, and high throughput through secondary channels for information transmission insensitive to timeliness. In our evaluation study, the results show that our scheme can provide a guarantee for reliable and high-throughput transmission.

Keywords: vehicle networks, channel allocation, reliability.

1 Introduction

With the increasing demand on high-data-rate wireless communication services, the bandwidth allocation design is expected to accommodate more users and support higher data rate on the guarantee of the quality of service. OFDMA is one of such communication systems. However, most existing OFDMA schemes are centralized and meet difficulties to satisfy users' requirements in vehicle networks. In a typical vehicle network, the topology of the network is changing rapidly all the time. Therefore, it is imperative to provide a dynamic and distributed channel allocation scheme rather than the centralized ones.

In this paper, the proposed channel allocation scheme allows each node to share parts of the channels with others never appearing in their link interference sets. Through this way, we can increase the number of available channels implicitly with little coordination among vehicles. In our design, different channel is allowed to choose better sub-channel for information transmission and to access to different sub-channel to avoid interference. Note that after a node selects one sub-channel for exclusive usage in its neighbor set, there still remains a large amount of channels unused. Based on this observation, we further propose a greedy design to utilize the remaining channel resources using OFDMA.

The rest of this paper is organized as follows: In Section 2, we briefly survey the related work about OFDM. The channel allocation algorithm is proposed

in Section 3. Section 4 try to list some of the theorem to be clear about the performance of our scheme. Section 5 provides the simulation results and Section 6 concludes the paper.

2 Related Work

OFDMA system has been studied for a long time. [1] proposed a simple greedy algorithm and proved that its much better than ribbon OFDMA. [2] raised a theoretical optimal allocation scheme and achieved a sub-optimal result on simulation. However, this algorithm doesn't take the fairness among users into consideration. There is another channel allocation algorithm considering fairness with low complexity—BABA+ACG[3]. It calculates an estimation of essential sub-carriers and allocates them to each user after adjustment.

Both the algorithms mentioned above are based on MA (margin adaptive). [4] proposes a sub-carrier allocation scheme based on RA guidelines. This scheme can maximize the throughput of the system and guarantee a fixed ratio of the speed of each user. Nonetheless, it needs a large amount of computing resource in bit allocation. Someone has improved this algorithm by combining sub-carriers and power and proposed a sub-optimal algorithm which can simplify the bit allocation process[5].

Under normal assumption, [6] proposes a progressive greedy algorithm which can be divided into two parts. The first part is BABS to get the number of sub-carriers by average channel gain and the ratio that users need[7]. The second part is ACG algorithm. It chooses a pair of sub-carrier and the corresponding user which can maximize its channel gain. If the user doesn't get enough sub-carrier, he will be allocated the sub-optimal carriers until there is none left. MAO algorithm proposed by Wong mentioned above gives out theoretical optimal result. However, its complexity is difficult to adopt and it neglects the fairness. BABS+ACG simplifies the process, but it needs cycling iteration to calculate the number of sub-carriers users need and the problem of fairness isn't improved[8,9]. All these schemes mentioned above work in a centralized manner. They lack the ability to support distributed vehicle communication networks.

3 Channel Allocation Algorithm

3.1 Vehicle Network Model

In this section, we briefly introduce the basic network model and some underlying assumptions.

We model the vehicle communication network as a MR-MC(multi-radio multi-channel) network consists of $|V|$ nodes, where there are N orthogonal frequency wireless channels, denoted as k_1, k_2, \dots, k_N . Each node has Q multi-input and multi-output antennas. And we suppose $Q \leq N$.

For the channels available to each node, the N channels can be divided into *primary channels* and *secondary channels*. We can use a N -dimension vector

\vec{c}_u to denote the label and division of a channel for a node u , where value 1 represents *primary channel* and value 0 represents *secondary channel*[10]. For example, $\vec{c}_u = (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)'$ represents that channel k_1, k_4, k_8, k_{10} are *primary channel* for node u , and the rest are *secondary channel* for node u .

Generally, a node tends to use the channel close to it rather than the *secondary channel*. And we suppose that the number of *primary channel* of a node is less than the number of *secondary channel*. For simplicity, suppose the channel code for each node is unique.

In our work, the vehicle network is modeled as an undirected graph $G(V, E, C)$, where V represents the vertex set and E represents the edge set. Each node has a channel coding, and all the channel coding of the vehicle network can be described as a matrix C with the size $N*|V|$. Each column of matrix C represents the code word of a node. For example, the $u - th$ column represents the code word \vec{c}_u of node u .

We assume that a data packet from node u to v needs to be acknowledged that it has been received by sending ACK from node v to u . $N_1(u)$ denotes nodes which are one hop away from node u , and $N_2(u)$ denotes nodes which are two hops from node u , it is obvious that $u \notin N_1(u), u \notin N_2(u)$. In this paper we adopt the protocol interference model. For a node $u \in V$, we represents the interference set of node u as $\mathcal{N}(u)$. If the transmission of node $v \in V$ interfere u with the signal receiving, then v is an interference node of u , we have $v \in \mathcal{N}(u)$. In protocol interference model, $\mathcal{N}(u)$ represents the nodes within two hops away from u , then $\mathcal{N}(u) = N_2(u)$. So it will generate conflicts and interferences if nodes within two hops use the same channel. This is the basic rule of our algorithm and allocation plan. Our objective is to ensure the channel used by a node is disjoint with its interference set.

3.2 Superimposed Code

In this part, we will simply introduce *superimposed code*, then combine *superimposed code* (s,1,N) (also *s-diajunctcode*) with the channel allocation of MR-MC network[11].

Suppose $N, t, s, L \in Z$ satisfies $1 < s < t, 1 \leq L \leq t - s, N - 1$, for a given binary matrix X with size $N \times t$, the $i - th$ column of X $X(i) = (x_1(i), x_2(i), \dots, x_N(i))'$ represents a binary code word numbered i . This kind of code word corresponds to a channel coding vector of a node in our later channel assignment. The boolean sum of $X(1), X(2), \dots, X(s)$ is

$$Y = \bigvee_{i=1}^s X(i) = X(1) \bigvee X(2) \bigvee \dots \bigvee X(s)$$

It is also a binary code word $Y = (y_1, y_2, \dots, y_N)',$ where for $j = 1, 2, \dots, N$:

$$y_i = \begin{cases} 0, & \text{if } x_j(1) = x_j(2) = \dots = x_j(s) = 0, \\ 1, & \text{otherwise,} \end{cases}$$

And for code word Y and Z , we call Y covers Z if $Y \bigvee Z = Y$.

A (s, L, N) SC word code (also called *superimposed – code*), where N represents the length of a word code, s represents strength, its characteristics is that the boolean sum of any s word code set in \mathcal{X} will not cover over $L - 1$ code word of its complementary set. The SC code where $L = 2$ also called $s - disjunct$ code. We can get $G(V, E, C)$ if we append matrix C with $s - disjunct$ code to a corresponding graph $G(V, E)$, where each code word of matrix C corresponds to the availability channel condition of this node[10].

3.3 Algorithm Design

The timeliness of information transmission is vary essential in the vehicle network especially, which also means that the reliability of signal transmission must be ensured first. In our protocol interference model, to ensure a node without interference we must try our best to make its two-hop neighbors to use different channels to deliver messages. The core of our channel allocation scheme is to choose the channel that is not used by its interference set for each node. To meet the requirement of both the reliability and high throughput, our scheme can be divided into two parts:

- **I:** Each node chooses its primary channel (a channel without interference to send some essential and necessary information).
- **II:** Each node chooses available channels by priority with distributed system for OFDMA.

The specific channel allocation scheme is presented in Algorithm 1: \mathcal{X} represents the superimposed code set of all nodes, $AvailableCH(u)$ means node u 's available channel set, $R(u)$ represents the forecast throughput of node u , $Rate(u)$ is on behalf of node u 's the average speed of sending message, $Priority(u)$ shows u 's priority to choose channel, $NumCh(u)$ represents the channel number u needs according to its situation, $ChEstimate(u)$ is the channel-estimation vector node u make for all its available channels, $N_1(u)$ means u 's one-hop neighbor and $\mathcal{N}(u)$ represents u 's neighbors within two hops.

This allocation scheme is a reasonable solution based on a vehicle network in which all the nodes are distributed. The main idea is dividing all the available channels into two parts: One is a primary channels $CH_1(u)$, which can not be selected by nodes adjacent within two hops. This channel is the first level to ensure sending important information and some control signals in our algorithm. The other part is a set of available channels $CH_2(u)$ for each node according to the rule, which can be used directly to make the OFDMA or further to divide the sub-channels and realize the multi-carrier OFDMA. After the partition, each node can choose a proper channel according to the packet's character or application can select the better channel to meet its requirement themselves. In brief, packets with high real-time requirements can be sent in $CH_1(u)$, and much quantity in the $CH_2(u)$.

Now, we focus on the acquirement of $CH_1(u)$ and $CH_2(u)$. The algorithm consists of two parts:

I: Each node transmits its network ID to its neighbor node, and then forward the ID it received to its neighbor, thus each one has all the ID number about the neighbor in two-hop distance. (To avoid the broadcast storm, too much noise and just try to send message within two-hop distance, each node can decide whether the ID message is from the source node or transmitted by others by judge if the ID number is among its neighbor after receiving IDs. Here we send information directly to $\mathcal{N}(u)$ instead of the broadcasting process details.)

After getting the $\mathcal{N}(u)$, each node u can calculate its $CH_1(u)$ set by the boolean operation with $\mathcal{N}(u)$ and u 's s-disjunct code. The $CH_1(u)$ is primary channel to u , but secondary to the $\mathcal{N}(u)$. It could be proved that when $s \geq |\mathcal{N}(u)|$, $BoolSum(\mathcal{X}(\mathcal{N}(u)))$ will not be covered by $\mathcal{X}(u)$, which means there exists at least one row in \mathcal{X} that $\mathcal{X}(u) = 1$ but all $\mathcal{X}(\mathcal{N}(u)) = 0$, so $CH_1(u)$ exists surely.

Algorithm 1. A distributed wireless channel allocation scheme for vehicle networks

Input: The initial information of each node u : C , $ChEstimate(u)$, $N_1(u)$, $NumCh(u)$, $R(u)$, $Rate(u)$.

Output: Each node u chooses its primary channel $CH_1(u)$ to send important information and the channel set $CH_2(u)$ to deliver large amounts of packets.

step 1: Each node broadcasts its ID and forward the received neighbor ID once, thus everyone will get the $\mathcal{N}(u)$.

step 2: $\forall u \in V, CH_1(u) =$

$Channels(BoolSum(\mathcal{X}(\mathcal{N}(u) \cup \{u\}))) \oplus BoolSum(\mathcal{X}(\mathcal{N}(u)))$

▷ find the primary channels for u , and secondary channels for $\mathcal{N}(u)$, then choose one to be the $CH_1(u)$.

step 3: $\forall u \in V, AvailableCH(u) = C -$

$\sum_{v \in (\{u\} \cup \mathcal{N}(u))} CH_1(v)$. (C represents the whole channel set)

step 4: $\forall u \in V, Priority(u) = \frac{R(u)}{Rate(u)}$, and send it to their $\mathcal{N}(u)$.

step 5: $\forall u \in V, Sort(Priority(v)), v \in (u \cup \mathcal{N}(u))$, thus we can get each node u 's priority order $Seq(u)$ among the nodes in $\mathcal{N}(u)$.

step 6: $Token = 1$;

step 7: $\forall u \in V$, if $Seq(u) == Token : CH_2(u) =$ the highest $NumCh(u)$ channels on the value of $Estimate(u)$ among the $Available(u)$.

if $|CH_2(u)| < NumCh(u)$

then $Priority(u)$ Add endif

$Token = Token + 1$ endif.

step 8: if there exists any node u which has not been involved in the allocation scheme, turn to step 7;

else break;

II: Now each node need to calculate some information which will be used later. First, they have to confirm their own available set to make OFDMA: just cut the primary channels of their own as well as their interference neighbour set

$\mathcal{N}(u)$'s form the whole giant channel set (neighbor's primary channels can be gotten by computing themselves or form neighbor's broadcast). After that, each node compute its own priority among $\{u + \mathcal{N}(u)\}$ ($Priority(u)$) and the channel number u perhaps need($NumCH(u)$). the $Priority(u)$ can be computed by the ratio of $R(u)$ and $Rate(u)$, which suggests that the user with more quantity messages to send and lower send speed should get the higher priority (Make every node can transmit its information evenly to guarantee the fairness). Each node send its own $Priority(u)$ to $\mathcal{N}(u)$, and $NumCH(u)$ can be gotten from the *BABS* algorithm or just by fuzzy processing with the $R(u)$.

The node u needs to sort the $Priority$ of u and $\mathcal{N}(u)$ and take notes each sequence as $Seq(u)$ after receiving the priority from $\mathcal{N}(u)$. $Seq(u)$ shows the sequence for node u to choose the channel among $\mathcal{N}(u)$. It's strictly related with the $Priority(u)$, which guarantees the fairness of the principle of channel allocation.

For each node, we set a global variable $Token = 1$, then all the nodes which satisfy the condition $Seq(u) = Token$ start to make a decision to select the highest $NumCh(u)$ channels on the value of $Estimate(u)$ among the $Available(u)$, and make this as $CH_2(u)$. Each node broadcast the $\mathcal{N}(u)$ and the receiver v begin to adjust the $Available(v)$. The adjustment operation is just cut the $CH_2(u)$ from $Available(v)$ and then make the $Token$ add one. So until every node has been allocated the required channels.

We must notice that there may exist one node whose available channel set is empty (It means the quantity of message this node need to send is small, and with high transmission speed, thus it's reasonable for the node to send packets through the $CH_1(u)$). We make a compensation that add a appropriate constant on its priority, which leads to that node can get better channels with high opportunity in the next allocation process after the network topology changes.

4 Performance Analysis

To be clear about the performance of our assignment, We try to give some conclusion theoretically as follows.

Lemma 1. *If $s \geq |\mathcal{N}(u)|$ and $\mathcal{N}(u)$ is the complete set of interferers of u for any node, the $CH_1(u)$ exists surely.*

Proof. Since \mathcal{X} is an s-disjunct code, *BoolSum* ($\mathcal{X}(\mathcal{N}(u))$) dose not cover $\mathcal{X}(u)$, which means that there exists at least one row in \mathcal{X} at which $\mathcal{X}(u)$ has the value 1 and all $\mathcal{X}(\mathcal{N}(u))$ have the value 0. Therefore the conclusion $CH_1(u) \neq \emptyset$ holds.

Lemma 2. *If the channel set u 's first choice $CH_1(u) \neq \emptyset$, then u has no interference with its two-hop neighbor $\mathcal{N}(u)$.*

Proof. Given that $CH_1(u) \neq \emptyset$, node u picks a channel $\alpha \in CH_1(u)$. And we know that form lemma 1 in the \mathcal{X} , on the α th row,

$$\mathcal{X}(\alpha, u) = 1, \text{but } \mathcal{X}(\alpha, \mathcal{N}(u)) = 0 \quad (\forall v \in \mathcal{N}(u))$$

In other word, the channel α is primary to u , and secondary to $\mathcal{N}(u)$. So node u can pick up a channel α from $CH_1(u)$, which will not be in interference with $\mathcal{N}(u)$.

Theorem 1. *If $CH_1(u) \neq \emptyset$ holds for $\forall u \in V$ and $\mathcal{N}(u)$ is the complete set of interferers of u in the network $G(V; E)$, the communications with $CH_1(u)$ can be guaranteed interference free in the network.*

Proof. The theorem holds from Lemma 1 and Lemma 2.

Theorem 2. *The proposal assignment based on the above algorithm can guarantee the instantaneity of each node to send real-time information.*

Proof. For each node u , it can always pick the $CH_1(u)$ as the one to send significant information. We only need to proof that any node in the its interference set won't use same one as follows. We pick the channel $\alpha \in CH_1(u)$ as the selected one for simplicity:

\forall node $v \in \mathcal{N}(u)$, the channel it might use must be in either $CH_1(v)$ or $AvailableCH(v)$. On the one hand, it could be proved that $CH_1(u) \cap CH_1(v) = \emptyset$ by the definition of CH_1 on our allocation scheme. Therefore $\alpha \notin CH_1(v)$. On the other hand, as our algorithm, $AvailableCH(v) = C - \sum_{w \in (\{v\} \cup \mathcal{N}(v))} CH_1(w)$. And $v \in \mathcal{N}(u)$, so $u \in \mathcal{N}(v)$, which means $u \in W$, then $CH_1(u) \cap AvailableCH(v) = \emptyset$. Therefore no one node in $\mathcal{N}(u)$ will use the channel α . In other word, node u can pick the $CH_1(u)$ without any interference at any time, which means can the instantaneity is guaranteed.

Generally, On our scheme, To choose one better primary channel on the first step, for a node, which is influence most crucial for the nodes' performance. We then briefly try to make an analysis on the network's performance which choose the primary channel at the Super-imposed Code we provided. There is no doubt that if each node could choose the channel with highest estimated value as the primary one, then all the nodes do the best. Before discussion, we need two premise: $K \geq |\mathcal{N}(u)|$, and $s \geq |\mathcal{N}(u)|$; thus the first step to choose channel could work successfully, and it's a reasonable assumption and can be easy to satisfy.

Theorem 3. *If the condition each node u has its exclusive best channel $B(u)$ and mutually disjoint. Then there must be one assignment solution to make sure that all node can get its best.*

Proof. It could be proved that there exists one simple but effective scheme which could achieve the goal: just make each node select the channel with highest estimated value among its available channel set. In fact, given a node u , it selects the $B(u)$, and $B(u)$ has the maximum value when node u make the channel estimation on the whole channel set. u can always get the $B(u)$ unless the channel $B(u)$ has been chosen by another node v ($v \in \mathcal{N}(u)$) at the same time. Hence there is $B(u) = B(v)$ as the scheme, which contradicts with the premise. In other word, every node can get its exclusive best channel. which proved our proposition is tenable.

This conclusion reflects in our algorithm:Under the given premise on the 3,node u just need to choose the channel with maximum estimated value after computing the candidate channel set $Channels(BoolSum(\mathcal{X}(\mathcal{N}(u) \cup \{u\})) \oplus BoolSum(\mathcal{X}(\mathcal{N}(u)))$,then it could get its best primary channel.

Of course the premise of3 can be always satisfied.Hence we need to make another analysis and estimation of network performance on an universal condition.

Theorem 4. *Each node u chose the channel according to its own like, and there are K channels totaly.The maximum number of nodes' neighbor is $\mathcal{N}(u)$.When $K \geq \mathcal{N}(u)$ holds,the probability of each node get its own best is $\frac{K(K-1)\cdots(K-\mathcal{N}(u))}{K^{\mathcal{N}(u)+1}}$.*

Proof. Because each node u only is related to its $\{\mathcal{N}(u)\}$ on the first choose step.We might as well to simplify the model, and just to focus on the selection process among one local independent set $u \cup \mathcal{N}(u)$.The node u is random and arbitrary,Hence the original problem can be converted into a reasonable,simple problem of combination and can be described as follows:

There are N people who would select items from a set of size K ,and it conflicts when the same item gets to be multiple selected.we need to compute the probability of system without conflict.

Answer: N people try to choose in-order:When computes the chose option number without conflict,first person have K options, and the next only have $(K - 1)$ options,Hence it totally counts to $K(K - 1)\cdots(K - N + 1)$;As for the whole choose way including the conflict:Each person can chose K .The goal probability is $\frac{K(K-1)\cdots(K-N+1)}{K^N}$.

Corresponding to the original problem, N people represents the set $\{u \cup \mathcal{N}(u)\}$ of size $\mathcal{N}(u) + 1$.The item set represents the channel set of size K .Hence the probability that each node chose its best channel is $\frac{K(K-1)\cdots(K-\mathcal{N}(u))}{K^{\mathcal{N}(u)+1}}$.

Actually,we make a statistics about the real probability on the Section 5.In our experiment, $K = 13,\mathcal{N}(u) = 4$,so the probability $\frac{K(K-1)\cdots(K-\mathcal{N}(u))}{K^{\mathcal{N}(u)+1}} = 41.59\%$.The practical result is 40%,which proves our conclusion is correct and realistic.

Sometimes,we don't have to be restricted to the only best channel,when the condition relieves:each node could chose another channel $B_2(u)$ if the best channel $B_1(u)$ has been chosen.It can be formalize as a complete matching on a special bipartite graph as 1:Each node among the set N has two sides,while the Node of set K doesn't need to. It's a complicated problem to compute the probability that the bipartite graph have the complete matching.But we can get some perfect result if we add some little restriction on the K set.

- **I:**If we can make sure that for each node in set K ,the degree d of node holds for $d \leq 2$,then it could be proved that the complete matching exists.

Proof. Given that $d \leq 2$ holds,we can just make a complete matching with some little steps as follows:

①: First to find out all the nodes in set K and only have one side connected to nodes in N to compose a subset \hat{K} and the corresponding subset \hat{N} (it's the nodes which are linked by red line in our example .Fig.1).Make these nodes in \hat{N} match the nodes in \hat{K} .Each node in \hat{K} links to one node in \hat{N} ,and each node in \hat{N} has at least one link or even more with \hat{K} .Hence the match is easy to be made.

②:After the matching in first step,then we could remove all the nodes in set \hat{K} or \hat{N} from the whole node set.and then cut off all the lines which are linked with any node in set \hat{K} or \hat{N} .Also,if the node in K has no side,it's nothing important with our matching,it should be removed at the same time.

③:There may be some new node with one side because of the lines' cut.And we need to repeat the work in ①,② until there are no node in K which has one side.In other word.All the nodes in K and N have two links with the node in the other set.It's easily to be proved that they form a series of circle,and obviously easy to make a matching in a circle(in our example .Fig.1,it's only need to select any two line which are not adjacent from the circle with blue lines).Hence the goal has achieved.

- **II:** In fact, we can make alternative relax on the restriction:If the degree d_i of each node i in the K ,satisfy the equation: $d_i > 0$.The matching always exists too.(The proof is like above)

We make some useful work like above to provide some theoretical proof on the realistic performance on our algorithm. To sum up,the selection scheme could make our user to get pretty good channel on the whole to send important information and also offer enough channels for them to improve services on demand.which could make a better optimization of resource allocation to a extent.

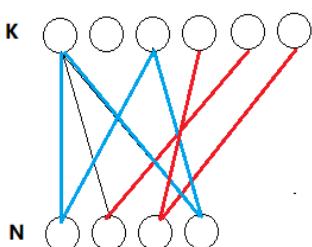


Fig. 1. A particular bipartite graph

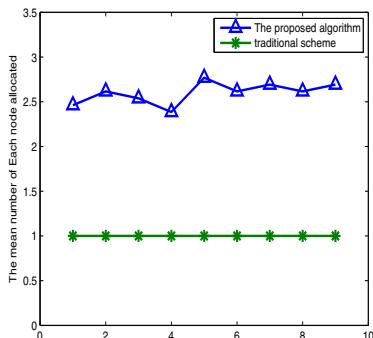


Fig. 2. The average number of wireless channel reused

5 Simulation Results

We simulate the channel allocation scheme mentioned above on MatLab platform. We compare this scheme with the original solution mainly on the number of repeated used channel and the system's ability to prove the advantages and improvements.

In the process of simulation, We ignore details of transmission process and the status of channels to focus on the effect of our scheme (In fact, we still have made the implementation of a typical OFDM system to guarantee the completeness). Because the fairness of each user must be ensure, the status (channel estimation, forecast throughput) of each node and the topology (the distribution and the contact between the various nodes) of the whole network are all randomly generated with the given requirements, which ensures the universality of our results.

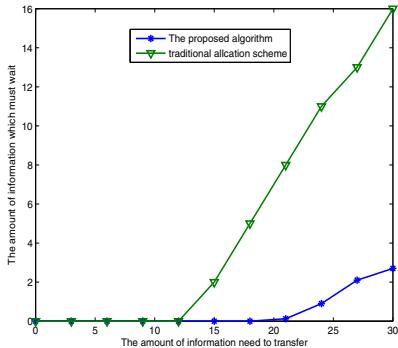


Fig. 3. The change about the queue length of the network node under load gradually to increase

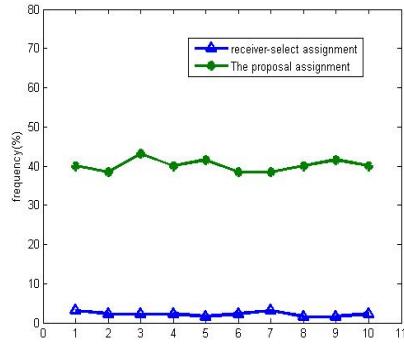


Fig. 4. The probability of each node chose its best channel

In the protocol interference model, a node will not be interfered when transmitting messages if and only if there is no neighbor within two-hop distance using the same channel as that it's using. If we apply the multiplexing on those nodes without interference, the number of channels can be used on the whole network will be greatly increased. In the traditional OFDMA solution, each node monopolizes its own channels. We compare the number of channel multiplexing in our simulation (as shown in Fig.2) and it is obviously that the traditional scheme of a single node monopolize a single channel is of great disadvantage. The new scheme takes 13 channels as example and it shows that each channel is reused about 2.5 times generally, which means that we can increase the throughput capacity of network greatly without any increase in bandwidth and cost of the whole system.

While measuring a network system, it is indispensable to check the performance of system with a heavy load to make sure the reliability and stability of

our results. Fig.3 has embodied the performance of traditional algorithm well and the proposed scheme in the state of network load gradually to increase. We use the sum of the length of each node's waiting queue when this node can't send all its packets with all the allocated channels to measure the ability of robustness under heavy load .It apparently shows that the waiting queue will begin to appear when the number of load is bigger than 13 (We take the packet number that a channel can quickly send out alone as the unit "1") by the traditional scheme. And the length of queue increases quickly, when the number of the load is up to 30 or so, the length of waiting queue has reached 16, exceeded the node number, which means each node now is waiting to send packets but all the wireless channels are occupied. In other words, the network has almost supersaturated and even paralyzed. In contrast to the original solution, the network that take proposed allocation scheme will not have any waiting queue until the load is heavy and still be of strong capacity of load, while the network with traditional scheme has already been paralyzed.

In addition to the obvious advantages mentioned above, the fairness of our new algorithm also cannot be ignored: A node with a large amount of information to send and slow sending speed can be allocated more channel resources, thus it could reduce the waste of channel resources by the optimization of the matching of the whole channel resources. In addition, the cost of base station brought by the centralized allocation and the disadvantages such as waiting delay of the process of gathering whole information and analysis can be avoided by the distributed allocation solution better.

Our assignment is based on the "Sender-select",and some others have proposed the "Receiver-select"[12].They allocate each node one channel for receiving, and then any other who want to communicate with it must send the packets on the channel the receiver selected.Thus every node only need to listen its own channel.It greatly reduced the receiver's workload.But on the contrary,the delivery process is getting more complicated.There are exists several disadvantages which is not with our algorithm such as switch delay,channel collision and the cost to send control information in all channel.

To evaluate the rationality of our allocation,we make a comparison between our scheme and the "Receiver-Select" on the probability of each node chose its best one(see the Fig 4).In the "Receiver-Select" scheme,the value is less than 10%.But in our scheme, the average probability of each node chose the best channel(the channel which has the max channel estimate value with the node)is about 40%(the theoretical probability could be calculated with the theorem4 and the value 41.59% is very close to 40%),which means half the node can use the best channel to send information.In other word,we can improve the load capacity and Qos through our scheme to optimize the channel allocation.

6 Conclusion

This paper proposes a distributed fair channel allocation scheme to realize reliable and high throughput transmission. In the proposed channel allocation

design, we can ensure realtime message transmission in a reliable way with little interference, on the other hand, we achieve high throughput through dynamic priority based channel allocation with OFDMA. and we have proved some theorem to explain why our scheme could performance better. In our future work, we will combine MIMO technology with OFDMA.

References

1. Edfors, O., Sandell, M., Van de Beek, J.-J., Wilson, S.K., Borjesson, P.O.: Ofdm channel estimation by singular value decomposition. *IEEE Transactions on Communications* 46(7), 931–939 (1998)
2. Hwang, T., Yang, C., Wu, G., Li, S., Ye Li, G.: Ofdm and its wireless applications: a survey. *IEEE Transactions on Vehicular Technology* 58(4), 1673–1694 (2009)
3. Kivanc, D., Li, G., Liu, H.: Computationally efficient bandwidth allocation and power control for ofdma. *IEEE Transactions on Wireless Communications* 2(6), 1150–1158 (2003)
4. Minn, H., Bhargava, V.K.: An investigation into time-domain approach for ofdm channel estimation. *IEEE Transactions on Broadcasting* 46(4), 240–248 (2000)
5. Wahlgqvist, M., Olofsson, H., Ericson, M., Ostberg, C., Larsson, R.: Capacity comparison of an ofdm based multiple access system using different dynamic resource allocation. In: *IEEE 47th Vehicular Technology Conference 1997*, vol. 3, pp. 1664–1668. IEEE (1997)
6. Edfors, O., Sandell, M., Van de Beek, J.-J., Wilson, S.K., Ola Borjesson, P.: Ofdm channel estimation by singular value decomposition. In: *IEEE 46th Mobile Technology for the Human Race, Vehicular Technology Conference 1996*, vol. 2, pp. 923–927. IEEE (1996)
7. Gupta, P., Kumar, P.R.: The capacity of wireless networks. *IEEE Transactions on Information Theory* 46(2), 388–404 (2000)
8. Rohling, H., Brüninghaus, K., Grünheid, R.: Comparison of multiple access schemes for an ofdm downlink system. In: *Multi-Carrier Spread-Spectrum*, pp. 23–30. Springer (1997)
9. Petropulu, A., Zhang, R., Lin, R.: Blind ofdm channel estimation through simple linear precoding. *IEEE Transactions on Wireless Communications* 3(2), 647–655 (2004)
10. Xing, K., Cheng, X., Ma, L., Liang, Q.: Superimposed code based channel assignment in multi-radio multi-channel wireless mesh networks. In: *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, pp. 15–26. ACM (2007)
11. Kautz, W., Singleton, R.: Nonrandom binary superimposed codes. *IEEE Transactions on Information Theory* 10(4), 363–377 (1964)
12. Kyasanur, P., Vaidya, N.H.: Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. *ACM SIGMOBILE Mobile Computing and Communications Review* 10(1), 31–43 (2006)

Throughput Prediction-Based Rate Adaptation for Real-Time Video Streaming over UAVs Networks

Tongqing Zhou, Haidong Zhang, Ming Xu, and Yingwen Chen

College of Computer, National University of Defense Technology, China
`{zhou tongqing, zhang haidong, xuming}@nudt.edu.cn, csywchen@gmail.com`

Abstract. Real-time video streaming is extensively used in UAVs networks for battlefield surveillance, disaster relief, etc. The available throughput of the multi-hop networks varies a lot with the movement of UAVs. To guarantee the video's quality and continuity, rate adaptation mechanism should be used to choose the appropriate transmission rate according to the varying throughput. In this paper, we propose a novel proactive prediction-based adaptation algorithm to avoid disruptions and provide high quality for real-time streaming over UAVs networks. We show that available throughput varies periodically with UAVs' mission-related movement. Then we set a prediction range with the knowledge of periodicity gained from the measurements of a training. The raw prediction is further calibrated with reactive estimation of buffered video time to precisely guide the adaptation. Simulation results show that our scheme maintains a continuous playback with a high quality and significantly shorten the start-up delay compared with two constant bit-rate schemes.

Keywords: UAVs networks, knowledge-based prediction, rate adaptation.

1 Introduction

Unmanned Aerial Vehicles(UAVs) networks have been playing increasingly important roles in many areas such as disaster relief, wide area sensing and battlefield surveillance [1]. In these scenarios, UAV nodes act as either information collectors or relays, communicating with each other jointly to deliver the critical data to home station with cost efficiency.

Real-time video streaming is especially valuable among all the data collected, because it provides users with explicit and intuitive descriptions of the area they care for. For example, in tactical networks, one can envision the captured video to facilitate mission management. Nevertheless, the stringent end-to-end latency requirement of real-time video is hard to guarantee. In practical, either video continuity or video quality needs to back off, since the wireless connections among UAV nodes are bandlimited and time-varying, considering the inevitable topology changes over time. As video interruptions degrade user experience significantly, a key challenge rises that how we could get rid of video freezes and shorten start-up delay while still guaranteeing high video quality.

To fulfill this purpose, the bit-rate of video streaming should adapt to the variation of wireless link quality, which demands for the guidance under throughput prediction. Existing works typically perform prediction based on reactive measurements, e.g. Round Trip Time(RTT) [2], Segment Fetch Time(SFT) [3] and simply realtime throughput [4]. For example, [4] predicts the available throughput¹ according to the average throughput achieved in the past several video segments. Though it does make sense when large TCP traffics steadily occupy the same path in a stable environment [5], things are quite different in real-time video streaming scenarios where the achieved throughput is often capped by video generating rate, so that it cannot predict available throughput explicitly. Hence, available bandwidth could be underestimated, which is likely to mislead bit-rate adaption, thus achieving limited video quality. Moreover, the existing schemes are ill-suited to the frequently variation of multi-hop wireless links that UAV works on.

In this paper, we propose a novel scheme to perform video rate adaptation for real-time streaming among UAVs, which enables high utilization of available throughput and makes use of the periodicity knowledge to overcome the frequently throughput variation. Our scheme involves two components, knowledge-based prediction and adaptation with calibration, carried out separately in a training stage and a transmission stage. With a same reconnaissance route, we show that the two stages experience a similar periodic variation, thus making a proactive prediction possible. Our major contributions are:

1. We introduce a proactive training to analyze the variation of available throughput caused by mission-related movement and conclude its periodicity. A prediction range is set based on the several periods' measurements in the training.
2. We propose a method for the estimation of buffered video time, generating an calibration parameter to perform a reactive tweak on the raw prediction.
3. We design an adaptation algorithm based on the prediction to smoothly match the available throughput.

To the best of our knowledge, our prediction method is the first to adopt the periodic throughput variation of UAVs networks to guide video rate adaptation. Moreover, the traditional buffered video time estimation is enhanced in our adaptation algorithm. Experiments show that our scheme successfully maintains an uninterrupted playback with a much shorter start-up delay than two constant bit-rate(CBR) schemes, and achieves a higher video quality.

The rest of the paper is organized as followed: Section 2 describes the relevant work. Knowledge-based throughput prediction and video rate adaptation algorithm are described in Section 3 and Section 4 respectively. Simulation results based on ns3 and discussion are presented in Section 5. We conclude the paper with summary in Section 6.

¹ Throughout the paper we use available throughput to refer to the maximum rate a given flow would achieve at a given point in time.

2 Related Work

Throughput prediction is vital for video rate adaptation as an essential guidance. In [5], throughput predictors for a broad class of applications are analyzed and summarized. And they classify TCP throughput prediction techniques into two categories: Formula-Based (FB) and History-Based (HB). These methods are extensively used in adaptation algorithm. In [2], [3] and [8], FB prediction is presented by analyzing measured parameter RTT, SFT and loss rate. In [4] and [6], HB prediction is proposed to detect fluctuation and take adaptation in real-time. We argue that both the two categories can be regarded as reactive prediction, because the characteristics demanded by FB and previous information demanded by HB are all obtained in real-time. Reactive throughput prediction is often capped by the real-time video's output rate. Thus the capacity would be underestimated which misleads the bit-rate adaptation to a lower level than expected, in other words, video could be transmitted in a higher quality. Our prediction scheme is performed based on the analysis of UAVs' mission-related movement in a training stage before the real-time transmission, which avoids the influence of video output on throughput prediction.

Haakon et al implement a location-based bandwidth-lookup service for bit-rate planning in [7]. They measured bandwidth in real environment, and plan quality adaptation based on the measurement and intermittently collected GPS positional data. In [9], authors propose a location-based model to predict the performance of TCP over a varying ground-to-UAV wireless link. Despite the attractiveness, the estimation process calls for frequently interaction between base station and mobile node which brings down the good throughput, and impacts the real-time transmission, especially for the multi-hop transmission in UAVs networks.

3 Knowledge-Based throughput Prediction

In UAVs networks, a group of mobile nodes jointly communicate with each other to extend communication range. In practical applications, the UAVs play either the role of collector or relay to fulfill a mission. Typically, the collector node would be scheduled to move in a predefined route to obtain acquired data from the ground. The requisite movement result in significantly variation of the available throughput. Ideally, the collector would know the throughput's behavior in advance to take corresponding adaptation for video bit-rate.

Fig. 1 presents a scenario of earthquake surveillance, in which three UAVs facilitate a wireless chain network to transmit the collected real-time video back to the home station. We find that the variation of throughput is periodic with UAVs' repeatedly surveillant movement. Hence, the knowledge of periodicity can be used to benefit the prediction of throughput. A proactive training stage is added before transmission starts to observe and analyze the variation of available throughput in a multi-hop UAV link with the collector regularly moves. Note that the available throughput would experience a similar periodic variation during

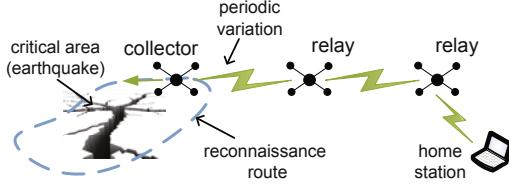


Fig. 1. The collector UAV repeatedly moves in the reconnaissance route to collect real-time information from the critical area. The repeatedly surveillance behavior results in periodic variation of the available throughput provided by the 3-hop-chain network.

video transmission. We introduce a continuous TCP bulk flow from the collector to home station to monitor the variation of available throughput.

We use time series analysis method to prove the existing and conclude the variation period. Let $TP = \{tp_i | 1 \leq i \leq n\}$ be the measured throughput during the t_m long stage, and the sampling interval of throughput is I which equals to t_m/n . Interval I should be appropriately chosen to enable a timely adaptation. The variation frequencies of throughput is organized as

$$F = \{f_i | 0 < f_i \leq 1/I, 1 < i \leq n\} \quad (1)$$

where element f_i denotes a variation frequency. Range of f_i and i decide that the variation period is larger than I and no bigger than t_m . Using Fourier transform, the intensity of each frequency component can be denoted as $P_i = S_i^2 + C_i^2$, where

$$S_i = \sum_{j=1}^n (tp_j - tp_m) \cdot \sin(2\pi \cdot k_j \cdot f_i), \quad (2)$$

and

$$C_i = \sum_{j=1}^n (tp_j - tp_m) \cdot \cos(2\pi \cdot k_j \cdot f_i) \quad (3)$$

tp_m denotes the mean value of the measured throughput, and $k_j = j$. Theoretically, P_i reflects the probability that throughput varies in frequency f_i . Therefore, frequency f_p related to the peek intensity value P_{max} presents the maximum probability for measured throughput to vary with.

The period of throughput's variation, denoted as T , divides the training stage into $N = \lfloor t_m/T \rfloor$ periods, where T equals to $1/f_p$. Hence, there would be T/I intervals in one period. Based on the division, we calculate the average throughput and minimum throughput for each interval in one period. We have,

$$TP_{avg} = \{tp_i^{avg} | tp_i^{avg} = \frac{\sum_{j=1}^N tp_{i+T \cdot j}}{N}, i \in [1, T/I]\}, \quad (4)$$

and

$$TP_{min} = \{tp_i^{\min} | tp_i^{\min} = \min_{0 \leq j \leq N-1} \{tp_{i+T \cdot j}\}, i \in [1, T/I]\} \quad (5)$$

tp_i^{avg} and tp_i^{min} refer to the average and minimum throughput for the i -th interval. During a real-time video transmission, we gain on the average results to seek high video quality, and gain on the minimum ones to avoid the influence of unwanted fluctuations. Hence, TP_{avg} and TP_{min} act as the upper bound and lower bound of the prediction for one period, respectively.

4 Rate Adaptation Algorithm

In this section, an effective video rate adaptation algorithm is proposed in which we adapt the bit-rate to appropriate levels based on prediction repeatedly after a specific interval. By doing this, we aim to (i) minimize the start-up delay while keeping a continuous video playback and (ii) maximize the quality of video. Meanwhile, we estimate the buffered video time on sender-side to tweak the raw prediction results of the training. The flowchart of our adaptation algorithm is shown in Fig. 2. In the flowchart, we use t_{ad} to represent the adaptation interval, while tp_i and tp_{i+1} denote the predicted throughput for the current and next interval respectively. It is important to note that t_{ad} should be appropriately chosen to provide timely adaptation and a relatively smooth quality switch is maintained by taking multi-subsequent-predictions into account at one time. The adaptation process is explicitly described in the subsequent sections.

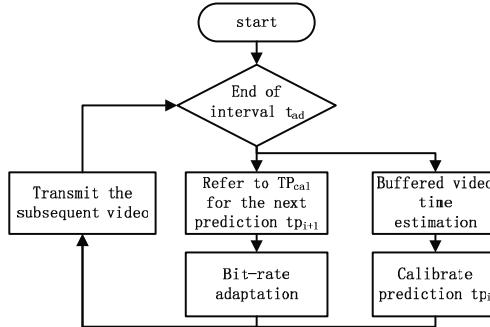


Fig. 2. Flowchart of the proposed prediction-based adaptation algorithm

4.1 Buffered Video Time Estimation

As shown in Fig. 2, we estimate the buffered video time at the end of each adaptation interval t_{ad} . The estimation acts as an evaluation for the prediction performance of the previous interval, and will be provided to the calibration step as a control parameter. Meanwhile, buffer level(buffered video time) is also used to indicate whether the playback is continuous or sometimes interrupted.

We propose a novel scheme to estimate the buffered video time on the sender side instead of collecting the measurement from the receiver side. Overhead on fetching feed-back information is avoided by doing so. During the continuous

transmission, we record the sent bytes M_i^s for the i -th sending interval of a period, and calculate the received bytes of receiver M_i^r based on the sequences of TCP ack segments. The value of M_i^s and M_i^r have no direct relationship with each other as throughput varies. If the sending bit-rate is higher than the current throughput, some resident bytes which represents the bytes un-received will generate. We denote this part of data as M_{res}^i . And the value of M_{res}^i decreases as the adaptation algorithm switch the bit-rate down below the available throughput, then we have,

$$M_i^{res} = \begin{cases} M_i^s - M_i^r & i = 1 \\ M_{i-1}^{res} - (M_i^r - M_i^s) & i > 1 \end{cases} \quad (6)$$

At the end of interval i , say $t_i^{(e)}$, the sent bytes is no smaller than the received bytes, so the resident bytes satisfy $M_i^{res} \geq 0$.

Assume that t_i^r is the length of video received during adaptation interval t_{ad} . t_i^r is consist of previously and currently received video pieces which have different bit-rate levels, thus we have,

$$t_{i+1}^r = \frac{M_i^{res}}{br_i} + \frac{M_{i+1}^r - M_i^{res}}{br_{i+1}} \quad (7)$$

where br_i is the selected video bit-rate during interval i . Then, the reference buffered time can be estimated as,

$$t_{i+1}^{buf} = t_i^{buf} - (t_{ad} - t_{i+1}^r) = t_{su} - \sum_{j=1}^{i+1} (t_{ad} - t_j^r) \quad (8)$$

where t_{su} denotes the start-up accumulation(delay), and t_i^{buf} indicates the buffer level at $t_i^{(e)}$. We emphasize that t_{su} is needed for that t_i^r happens to be smaller than the consumed length of time during the transmission.

4.2 Throughput Prediction Calibration

Results of the proactive training set the variation range of throughput prediction as $[TP_{avg}, TP_{min}]$. If we simply take TP_{avg} as the available throughput, a high video quality could be achieved while video freezes would occur. On the contrary, if we carefully adapt the bit-rate based on TP_{min} , no interruption occurs but the video quality stays low. Taking a compromise between the two bounds, we dynamically estimate the available throughput by introducing the reference buffer level as a control parameter, and derive the calibrated prediction $TP_{cal} = \{tp_i^{cal} | 1 \leq i \leq T\}$.

Specifically, we propose a weighted average method for the calibration,

$$tp_i^{cal} = \alpha_i \cdot tp_i^{avg} + (1 - \alpha_i) \cdot tp_i^{\min} \quad (9)$$

where tp_i^{cal} is the prediction for the available throughput during the i -th interval in a period, and α_i denotes the related weight. By tweaking parameter α_i , the

value of tp_i^{cal} is dynamically changed in range $[tp_i^{\min}, tp_i^{avg}]$. After an adaptation interval, we increase α_i with an increment Δ_i within the given range unless the buffered time's reduction during that interval goes beyond a threshold level t_f . Then we decrease α_i with Δ_i . The increment Δ_i related to α_i equals to $W/(tp_i^{avg} - tp_i^{\min})$, where W is assumed to be the gap between two bit-rate levels. Thus, every adjustment of α_i is sufficient for a level switch of bit-rate.

Hence, the available throughput can be predicted as a succession of throughput period, in which the prediction performance of last period directly influence current prediction TP_{cal} . The advantage of dynamically calibrating the prediction compared to simply using the average or the minimum version is that it tweaks the proactive prediction with reactive information to adapt to the actual situation.

4.3 Bit-Rate Adaptation

Bit-rate adaptation process is performed based on the calibrated throughput prediction. After each adaptation interval, we refer to TP_{cal} to analyze the relationship between current bit-rate and prediction value for the subsequent interval, which can be categorized into three situations: 1) $tp_{i+1}^{cal} > br_i + W$, 2) $br_i < tp_{i+1}^{cal} < br_i + W$ and 3) $tp_{i+1}^{cal} < br_i$.

We set $br_{i+1} = br_i$ in situation 2) because br_i remains to be the best appropriate level. In situation 1), switch-up operation is expected to promote a high quality. We propose a selective switch-up scheme to adapt the bit-rate, in which the predicted available throughput for the next $r(r \geq 2)$ intervals are all picked for comparison. The scheme avoids instantaneously switch-up by detecting the probably throughput spikes. Thus, a switch-up is adopted only if $tp_{i+2}^{cal}, \dots, tp_{i+r}^{cal}$ also satisfies situation 1). And the corresponding bit-rate is set as

$$br_{i+1} = \max\{br_j^{level}, br_j^{level} \leq \min\{tp_{i+1}^{cal}, \dots, tp_{i+r}^{cal}\}\} \quad (10)$$

where br_j^{level} refers to an accomplishable bit-rate level, and note that tp_{i+1}^{cal} would be updated at the end of the subsequent adaptation interval. Otherwise, bit-rate would stay unchanged for the next interval to maintain adaptation stability. For situation 3), switch-down operation should take place to avoid a buffer reduction which may lead to video interruption. In this situation, an aggressive switch-down is preferred to set the bit-rate level with equation 10. The selective process is maintained by taking longer prediction into account to benefit smooth adaptation, while the aggressive action is adopted based on the next interval's prediction. We point out that the proposed algorithm avoids adaptation caused delay by cautiously adapting to the prediction. Thus we only need to calibrate the prediction when unexpected delay is detected.

The minimum throughput version in period T reflects the available throughput related to a specific situation, in which some random interference or loss happen to occur. The algorithm starts by selecting tp_1^{\min} as the prediction for available throughput to minimum start-up delay, calibration coefficients are therefore set as 0. For the subsequent periods, we perform selective switch-up

and aggressive switch-down as mentioned above to maximize the quality while maintaining a continuous play.

5 Experimental Evaluation

5.1 Experiment Environment

We implemented our knowledge-based prediction scheme and rate adaptation algorithm in ns3 [10]. A chain topology with 3 nodes was used in the simulations. The nodes act as the collector UAV, the relay UAV and the home station, respectively. They fell into a line at the beginning of the simulation, and the initial distance between any two adjacent nodes was set to 100m. During the mission, the collector moves in a predefined reconnaissance route repeatedly to collect acquired data from assumptive critical area. We used a log distance propagation model to simulate the wireless channel. All the nodes were configured to utilize IEEE 802.11g physical layer.

We performed the simulation process in two stages, that is, a training stage and a video transmission stage. The two stages last for 200s and 1000s, respectively. The BulkSender application in ns3 was adopted to generate a continuous TCP flow during the training stage, in which we analyzed the periodicity of variation and calculated two prediction bounds. Meanwhile, a real-time video streaming application was designed to carry out during the video transmission stage, in which our algorithm was evaluated and two CBR schemes were also performed for comparison.

In the simulation, we set both the sampling interval I and the adaptation interval t_{ad} to 2s, and the start-up time accumulation t_{su} was set to 5s. Note that t_{ad} was set to its minimum value to enable a timely adaptation. And the stability is maintained by the adaptation scheme with smooth parameter r set to 2. Calibration coefficient α_i for each interval in a period was initially set to 0. And we denoted the reduction threshold t_f to 0.3s. Finally, the adopted bit-rates were 500, 550, ..., and 1000kbit/s with the level gap W set as 50.

5.2 Result and Discussion

Firstly, we carried out a simulation to evaluate the efficiency of the proposed available throughput prediction scheme. Based on the measurements in proactive training, the prediction scheme firstly analyzes the periodicity, the results is shown in Fig. 3. As mentioned above, the intensity for frequency f_i reflects the probability that throughput varies with f_i . Then we have $T = (1/f_4) \cdot I = 50s$, where f_4 is the frequency related to the maximum intensity. Hence, we can divide the training stage into $200/T$ periods. For each interval in a period, we calculate both its average value and minimum value of all the periods. Fig. 4 shows the throughput prediction results TP_{avg} and TP_{min} , which set the upper and lower bound for latter calibration.

Fig. 5 shows the calibrated throughput prediction with a comparison to the available throughput. During a period, the predicted throughput at a given time

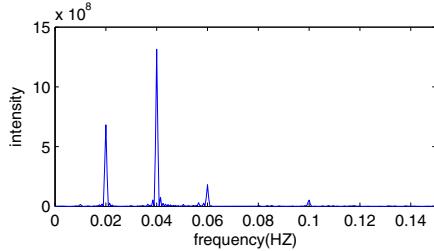


Fig. 3. Intensity as a function of throughput variation frequency

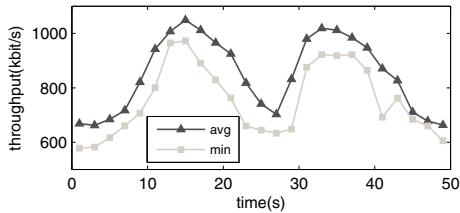


Fig. 4. The prediction bound TP_{avg} and TP_{min} in one period

point i is calibrated to a higher value each time tp_i^{cal} successes to cover the actual capacity. And it decreases when $tp_i^{cal} > tp_i^a$ is satisfied, thus causing the reduction of buffered time to go beyond the threshold t_f . Specifically, the calibration process is performed based on coefficient α , which is periodically tweaked with the buffered time. We take α_{12} and α_{21} related to the 12-th and 21-th interval of the period as examples to present the adjustment of α , the results are shown in Fig. 6. Their increments Δ_{12} and Δ_{21} are 0.3 and 0.2 respectively. We point out that TP_{cal} successfully fits the available throughput by dynamically tweaking between the two prediction bounds TP_{avg} and TP_{min} .

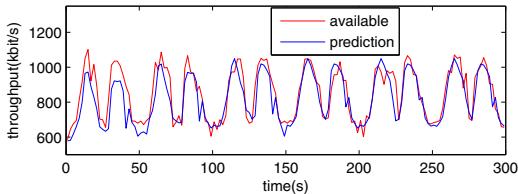


Fig. 5. Calibrated prediction TP_{cal} and available throughput TP_a

Fig. 7 shows the adaptation results of our proposed algorithm, where we only present the first 300s of bit-rate adaptation. During the transmission, adaptation algorithm dynamically choose a bit-rate level below the upper limit set by

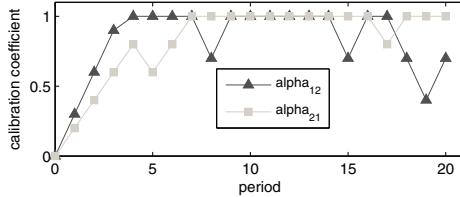


Fig. 6. Adjustment of coefficient α_{12} and α_{21} during the 20 periods long transmission

TP_{cal} . Bit-rate is cautiously switched up to achieve high video quality while maintaining adequate stability by taking next 2 intervals' prediction into account. And it is promptly switched down to avoid adaptation caused delay. The reference buffer level fluctuates as mismatch between available throughput and bit-rate occurs. A behavior of reduction indicates that video bit-rate exceeds the current throughput, which causes the length of received video less than the transmission time. On the other hand, buffer level raises or stays still when the link capacity successfully covers the current bit-rate, thus the new generated bytes and the residual bytes are both received to make up the time consumption. We remark that no buffer underflow occurs, and the minimum buffered time is around 2.5s.

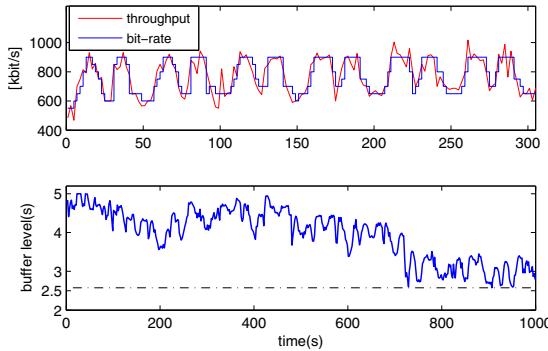
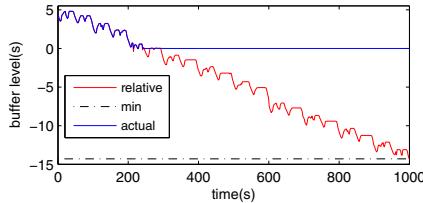
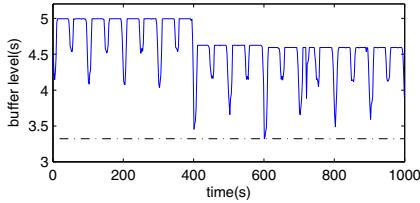


Fig. 7. Measured throughput, video bit-rate and buffer level

Fig. 8 and Fig. 9 show the observation of buffer level for two other runs, which are a high CBR scheme and a low CBR scheme. We set the bit-rate 750kbit/s for the former and 650kbit/s for the latter, introducing a span of 2 bit-rate levels. Note that both the actual buffer level and the relative buffer level are presented in Fig. 8. The relative level is used here to show the length of surplus video time when the buffer level is above 0, and it reflects the length of video that have suffered a disruption when the buffer exhausts. We point out that

**Fig. 8.** Buffer level, cbr=750kbit/s**Fig. 9.** Buffer level, cbr=650kbit/s

buffer underflows happen because it is unable for an CBR scheme to forecast any variations of available throughput.

Table 1. Average bit-rate and relative delay in 3 schemes

Scheme	Average bit-rate(kbit/s)	Relative delay(s)
1	789	2.5
2	750	19.5
3	650	1.7

The detailed comparisons between our adaptation algorithm and the CBR schemes are presented in Table 1, wherein both the average bit-rate and relative delay are concluded, and scheme 1, 2, 3 refer to the proposed algorithm, the high CBR scheme and the low CBR scheme, respectively. Average bit-rate is used because it represents the average quality of the video streaming. And we use relative delay to represent a specific start-up delay level with which no interruption would happen during the transmission. It is important to note that relative delay fairly reflects one's performance on real-time. As a conversion between start-up accumulation and minimum buffer level, relative delay can be calculated as $t_{su} - t_{min}^{buf}$, where t_{min}^{buf} represents the minimum buffer level experienced(e.g., 2.53s for scheme 1). Intuitively, the proposed algorithm achieves a relative delay of 2.5s, almost 8 times shorter than what scheme 2 exhibits, and promotes an even higher average bit-rate. Compared to scheme 3, scheme 1 brings a rise in bit-rate of almost 3 levels, while maintaining a basically same

relative delay (only 0.8s larger). As to continuity, neither the proposed algorithm nor the low CBR scheme incurs an underflow, while the high CBR scheme suffers continuous underflow after around 200s. The proposed algorithm successfully maintains a continuous play of real-time video with a high quality, while introducing the minimum start-up delay.

6 Conclusion

In this paper, we propose a novel throughput prediction method for video bit-rate adaptation performed during real-time video streaming. The advantage of the proposed knowledge-based prediction method compared to schemes used in existing rate adaptation works is that our method is carried out during a proactive training to get rid of the video generating rate's throttle on reactive measurements. And we dynamically calibrate the prediction results with the reactive control of sender-side buffer level estimation. Moreover, an aggressive switch-down and selective switch-up scheme is used to avoid interruption, promote video quality and smooth the adaptation. Simulation results show that the proposed algorithm efficiently maintains a continuous play of real-time video with a minimum start-up delay and provides a relatively higher quality.

References

1. Zhao, W., Ammar, M., Zegura, E.: A message ferrying approach for data delivery in sparse mobile ad hoc networks. In: Proc. of ACM International Symposium on Mobile Ad hoc Networking and Computing (2004)
2. Thapliya, R., Hu, C.: AdapComm: a bandwidth allocation methodology for multimedia applications in wireless networks. In: Proc. of ACM SIGCOMM (2013)
3. Liu, C., Bouazizi, I., Gabbouj, M.: Rate adaptation for adaptive HTTP streaming. In: Proc. of the Second Annual ACM Conference on Multimedia Systems (2011)
4. Tian, G., Liu, Y.: Towards agile and smooth video adaptation in dynamic HTTP streaming. In: Proc. of the 8th International Conference on Emerging Networking Experiments and Technologies (2012)
5. He, Q., Dovrolis, C., Ammar, M.: On the predictability of large transfer TCP throughput. In: Proc. of ACM SIGCOMM (2005)
6. Miller, K., Quacchio, E., Gennari, G., et al.: Adaptation algorithm for adaptive streaming over HTTP. In: Proc. of IEEE Packet Video Workshop, PV (2012)
7. Riiser, H., Endestad, T., Vigmostad, P., et al.: Video streaming using a location-based bandwidth-lookup service for bitrate planning. ACM Transactions on Multimedia Computing, Communications, and Applications, TOMCCAP (2012)
8. Wu, D., Hou, Y.T., Zhu, W., et al.: On end-to-end architecture for transporting MPEG-4 video over the Internet. IEEE Transactions on Circuits and Systems for Video Technology (2000)
9. Kung, H.T., Lin, C.K., Lin, T.H., et al.: A location-dependent runs-and-gaps model for predicting TCP performance over a UAV wireless channel. In: Proc. of IEEE MILCOM (2010)
10. Network simulator ns-3, <http://www.nsnam.org/>

Table-Driven Bus-Based Routing Protocol for Urban Vehicular Ad Hoc Networks

Tabouche Abdeldjalil, Fan Li*, Ruiling Li, and Xin Li **

School of Computer Science, Beijing Institute of Technology, Beijing, 100081, China

Abstract. Vehicular Ad Hoc Networks (VANETs) have attracted increasing interest over the past decade, but the design of an efficient routing method for VANETs is still a challenging task. Via analyzing characteristics of urban VANETs (such as the heterogeneous vehicular types and the impact of traffic lights), we believe that buses can be used as the mobile backbone of VANETs to aid data transmissions. In this paper, we propose a table-driven bus-based routing protocol to lighten the control of packet delivery and reduce the average delay. Simulation results demonstrate a significant improvement in terms of delivery ratio and average delay over traditional routing protocols.

1 Introduction

Recently, vehicular networking has gained a lot of interest from automobile industry, governments, and academic research community [1–3]. In vehicular ad hoc networks, moving vehicles are considered as mobile nodes in the network and they are connected to each other via wireless links when they are within the communication ranges of each other. There are two modes of communication in VANETs: *vehicle to infrastructure* (V2I) and *vehicle to vehicle* (V2V) communications. V2I represents the communication between the on-board units (OBUs) on vehicles and an pre-deployed infrastructure (usually via road side units, RSUs); while V2V represents the communication between OBUs of vehicles [4]. Routing is one of the most fundamental issues in VANETs, which aims to find efficient paths to transmit data packets among OBUs and RSUs.

In this paper, we study how to perform efficient routing in an urban VANET and propose a topology-based routing approach (BB-Rt), which utilizes buses as the mobile backbone. This method is motivated by the characteristics of urban VANETs and effects that buses have on urban environments. Buses, this specific type of vehicles, are characterized by (1) the lower speed compared to regular cars, (2) the considerable number of buses in city scenario, and (3) the regularity

* Corresponding author.

The work of F. Li is partially supported by the National Natural Science Foundation of China under Grant No. 61370192 and 60903151, and the Beijing Natural Science Foundation under Grant No. 4122070.

** The work of X.Li is partially supported by the National Natural Science Foundation of China under Grant No. 61300178.

of the route. We have adopted the MI-VANET architecture [5], where buses and cars represent two different tiers in the network. Our proposed routing method aims to choose a path with the smallest number of nodes, by considering buses as a mobile backbone of the network. Three important benefits have been gained: reducing the average end-to-end delay, increasing the packets delivery ratio, and reducing the number of nodes on a selected route to the destination in a city environment. Compared to the classical Ad hoc On Demand Distance Vector (AODV) routing protocol [6] , which suffers from long connection setup duration and heavy control overheads, our approach lightens the control of packet delivery and improves the overall routing perform in an urban environment. Via extensive NS-2 simulations with traffic generated by MOVE mobility model [7] over a real road map in Beijing city, there are significant improvements in delivery ratio and average delay for the proposed method over AODV.

2 Related Works

Routing in VANETs has been the key issue of VANET research for a decade. There are many different types of VANET routing protocols. Usually they can be categorized into three groups: *topology based*, *position based*, *delay tolerant network (DTN) based*. There are also hybrid approaches [8–10] where multiple routing schemes are combined together. For general VANET routing protocols, please refer to [1,2]. Here, we only briefly survey recent methods which use buses to forward data packets.

In [11], Shanghai BUSNET is proposed. It is based on the modeling of a time-space mode by using some specific information about bus networks, like bus schedule, bus line information, etc. The BUSNET approach is similar to the hybrid DTN routing in VANETs [12,13] and assumes to have a regular number of buses on street which is not guaranteed in the real environment. [14] focuses on modifying and enhancing the AODV routing protocol [6] and proposes a Bus AODV (BAODV). The BAODV chooses the route with the less number of buses but it consumes extra bandwidth caused by the periodic beaconing. In both proposed approaches, the network nodes are only buses, which could debase the scalability of the routing protocol, and other transportation do not participate in the forwarding of messages. In [20], Buses are deployed in all roads acting as intermediate nodes, but it mainly studies the multicast capacity of bus-assistant VANETs.

In MI-VANET architecture [5], the buses play the role of a mobile backbone for data delivery. A two-tier VANET architecture called MI-VANET was proposed where the buses constitute a mobile backbone for message dissemination:

- Each bus is equipped with two wireless interfaces. The first one (low tier) is dedicated to communicate with the standard cars. The second one (high tier), with larger transmission range on another channel, is dedicated to the inter-buses communication.
- Standard cars constitute the low tier of MI-VANET architecture. When the node wants to send message, it has to register on a bus. This method is called

MIRG (Mobile Infrastructure Registering) register on the nearest bus, after that it sends the packet to this bus. The forwarding of packets will be assured by the use of the high tier wireless devices.

In MI-VANET, the proposed routing mechanism is a position based approach and it assumes that vehicles are uniformly distributed on the road and each bus has a digital street map including bus line information. In this paper, our proposed approach is based on this architecture, but the routing is a topology based approach.

3 Characteristics of Urban Traffics

To study and simulate the vehicles movement in urban environment, we should analyze the characteristics and statistics related to the vehicular traffics:

- The first remarkable point, when we observe the vehicles movement in a big cities, is the influence of traffic lights on the vehicle movement. The red traffic light stops vehicles movement, which leads to the network disconnection. When the traffic light turns green, these vehicles will continue to move together and in the same direction like a cluster.
- The second point is the velocity of vehicles on roads; a higher number of vehicles are moving in the day scenario and a lower number at night.

In this work, we choose a small area in Beijing as a real environment and there are some specifics of the Beijing's road traffic:

- According to Beijing Traffic Management Bureau [15], in Beijing, ordinary cars represent about 80% of all motor vehicles, and buses represent less than 20%. We also mentioned here that the route of bus is more regularity, and the speed is slower compared with taxis and private cars, which is easy to establish communication links.
- To study the character of bus line, we choose a road segment in the real area (i.e., Wan Liu East Rd Haidian District, Beijing) which has 7 bus lines. And the interval time between the departure of each bus line is about 15 minutes. As in each road there are two directions, the average time between two adjacent buses is about $15/7/2 = 1.07$ minutes. Another simple experiment, where we take randomly 10 buses, shows that the highest speed of buses is about $50km/h$. The experience also shows that due to the frequently bus stops and traffic lights, the average speed is only about $15km/h$. By taking these two features into consideration, we conclude that the average distance between buses in Beijing is not very long. And buses could assure a good connectivity in a bus-based network.

4 The BB-Rt Routing Approach

In this paper, we propose a table-driven based routing approach which uses buses as the mobile backbone to forward the message, called BB-Rt(Bus Based Routing), which has three steps:

4.1 Neighbor Discovery

The neighbor discovery mechanism is based on the sending of *Hello_Packets* over the broadcast medium, these packets are broadcasted periodically and the nodes inside the transmission range of the sending node are able to hear this *Hello_Packet* and register the sending node as neighbor. A TIMEOUT value is associated with each neighbor and recorded in the node's table. If the node does not receive any *Hello_Packet* from a particular neighbor within the TIMEOUT period, this neighbor will be removed from the list.

4.2 Information Dissemination

In this step, a Link State Packet (LSP) which contains neighbor link information will be sent to other nodes in the network. Two main functions can be presented:

1- Handle the LSP integrity: After the node generates a new LSP, it must transmit it to all the nodes over the broadcast medium. The node received the packet then transmits it to all its neighbors except the one from which the packet was sent. Because each node retains the most recently generated LSP from other nodes, this node can recognize when it receives a duplicate LSP.

2- Updating interval: The process of updating is assured periodically and when it detects a link change and each node broadcasts its outgoing links to all other nodes through a Link State Packets (LSP). These LSPs are flooded to all the other nodes in the network. As each node receives this information, it updates its view of the network.

4.3 Routing Method

Once the node has a table of LSPs, an algorithm is proposed to compute the shortest path from source to destination. This algorithm is inspired by planning methods used in the field of artificial intelligence [16, 17].

The details of the used algorithm are presented. For this aim we define four rules that will be used in the route selection.

Rule 1. If two nodes N_1 and N_2 have the same linkage and their Link State tables are similar, we delete one of the two nodes, which will lighten the Link State table of the source node, as shown in Fig. 1.

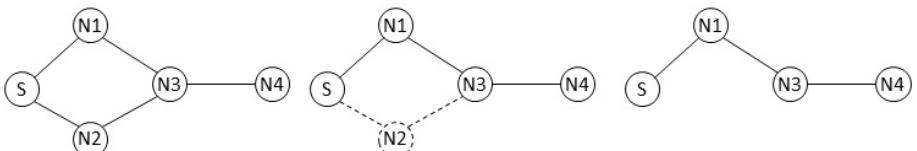


Fig. 1. N_1 and N_2 have the same linkage, the suppression of the node N_2 will lighten the LS table of the node S

Rule 2. As shown in Fig. 2, if the nodes presented in the LS table of one node are also presented in the LS table of another node, the first one could be deleted since it doesn't bring any new route.

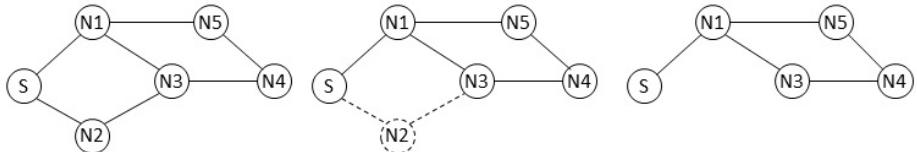


Fig. 2. LS table of N_2 is included in N_1 's LS table, N_2 will be deleted

Rule 3. A node will be deleted from the LS table if we can generate its LS table from a combination of other node's LS tables. As shown in Fig. 3, N_2 can communicate with N_5 and N_6 , these two nodes could be reached through N_1 and N_3 . So, the suppression of the N_2 will not affect the routing.

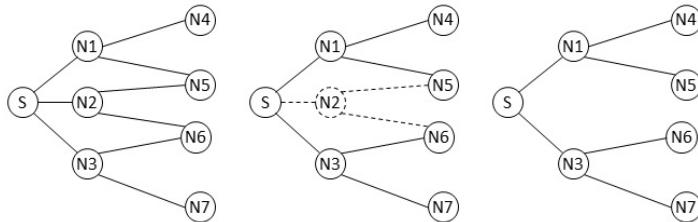


Fig. 3. N_5 and N_6 could be reached through N_1 and N_3 , the suppression of the N_2 will not affect the routing

Rule 4. A node will be automatically deleted from LS table if it has just one link and this will lighten and facilitate the routing. As shown in Fig. 4, N_2 will be deleted from LS table of the source because it has just one link, in other words, it does not participate in the routing mechanism.

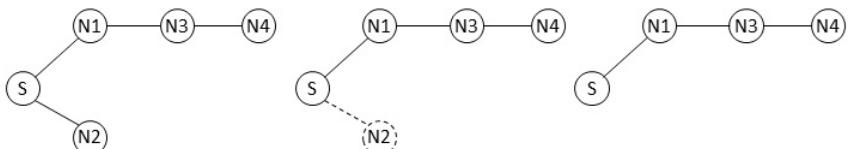


Fig. 4. N_2 does not participate in the routing, so it is deleted from LS table of S

Algorithm 1. BB-Rt: Bus Based Routing Approach

Input: S: Source node. D: Destination node. N: LS table of S.
Output: Rt_Tab : Route table.

```

1: W = N , C =  $\emptyset$ , Path_length = 0 , Rt_Tab [0] = S
2: if D  $\in$  N then
3:   while D  $\notin$  Rt_Tab do
4:     for each node  $N_k$  in W do
5:       if  $N_k$  is a neighbor of  $N_j$  /  $N_k \notin$  Rt_Tab and  $N_j \in$  Rt_Tab then
6:         C = C  $\cup$  { $N_k$ }
7:       end if
8:     end for
9:     W = W - C
10:    for each  $N_k$  in C do
11:      C = C -  $N_k$ 
12:      if  $N_k$  could not be deleted by Rule 1, Rule 2 and Rule 3 then
13:        Add  $N_k$  to Rt_Tab, Path_length++
14:      end if
15:    end for
16:  end while
17:  i = Path_length
18:  while i > 0 do
19:    if  $N_i$  could be deleted from Rt_Tab then
20:      Update Rt_Tab by deleting  $N_i$ 
21:    end if
22:    i --
23:  end while
24: else
25:   Error, No Route
26: end if

```

The Computation Algorithm. Based on the above four definite rules, we present the method in Algorithm 1.

Our approach is table based routing, because it keeps paths information between any pair of nodes in a table. It is based on the principle of shortest path algorithms. Each node updates its routing table if the network topology changes. The computation mechanism requires in worse case a $O(N^2)$ steps to get a route. However, in the simulation, the number of computation steps is much fewer than $O(N^2)$.

5 Evaluation

5.1 Simulation Model

We use version 2.35 of the NS-2 simulator [18] in our experiments. The simulation area is based on real map about 4km by 3km area of Haidian District in Beijing, China, as shown in the Fig. 5. There are 100 to 400 vehicles traveling on the roads, communication radius of cars is set to 250m and 400m for buses. We

use MOVE (Mobility model generator for Vehicular networks) [7] to generate the mobility model, based on the open source SUMO (Simulation of Urban Mobility) [19].

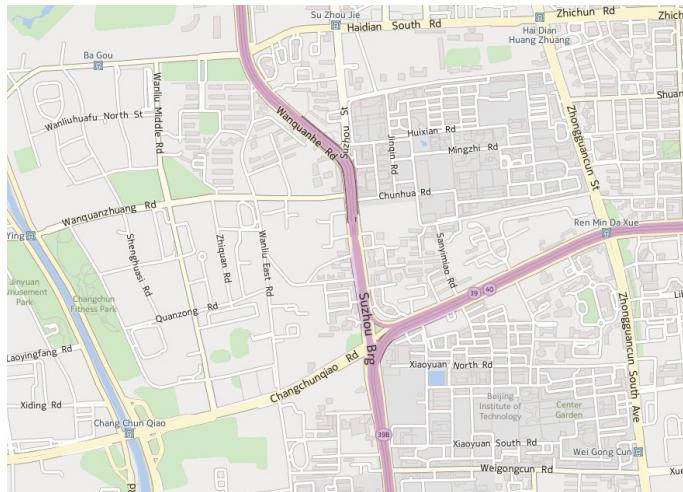


Fig. 5. Map: A 4km by 3km area of Haidian District in Beijing, China

The simulation parameters are set in Table 1. In all experiments, we compare the performance of the Bus-Based routing (BB-Rt) with AODV (denoted as Car-AODV). For the comparison, we also introduce Car-RT (i.e., car to car Routing), in which all vehicles are treated equally. This means bus has only one interface and all nodes participate in packet forwarding. For each method, we run the simulation for 50 times and report the average.

Table 1. Table of simulation parameters

Environmental parameters	Used Values
Experimental area	4 × 3 Km
The number of vehicles	100 - 400
Percentage of buses	5%, 10%, 20%
Wireless communication radius for Cars	250m
Wireless communication radius for Buses	400m
Vehicle velocity	0-20 m/s
The number of the source node	10%
Packet size	512 bytes
Sending rate	128 bps
Simulation time	100 s

To evaluate the performance of the proposed approach, we use the following three metrics:

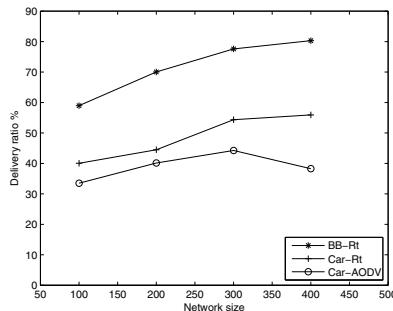
- **Delivery ratio:** It presents the level of delivered data to the destination, which is represented as a percentage of packets that are successfully delivered to a destination compared to the number of packets sent by the source.

- **Average delay:** The average time taken by a packet to be successfully forwarded to the destination. It also includes the delay of the route discovery process and the queuing in data packet transmission.

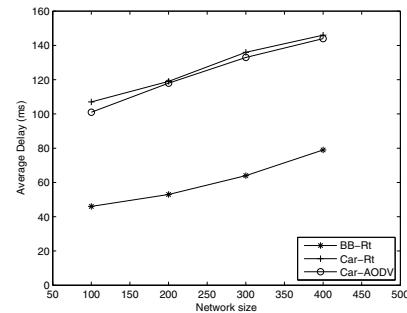
- **Average path length:** The average number of nodes that participate to forward packet from the source to the destination, and only the data packets that successfully delivered to destinations are counted.

5.2 Simulation Results of BB-Rt Compared with Car-Rt and Car-AODV

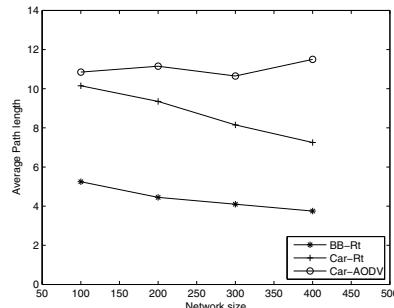
Simulation Results with Different Network Size. As shown in Fig. 6a, BB-Rt achieves the highest packet delivery ratio. AODV incurs a highest data loss



(a) Delivery Ratio



(b) Average Delay



(c) Average Path Length

Fig. 6. Performance comparison among BB-Rt, Car-Rt and Car-AODV with different network size

rate, because simple topology-based strategy without taking urban environment characteristics into account is not suitable for VANET. After considering some urban environment characteristics in VANET, we consider buses as backbone of the network, 15 – 35% more packets can be received. The delivery ratio becomes higher values when the density of the network increases, because the average speed of vehicles decreases in traffic jam scenario, which makes the topology changing slower; this feature promotes the use of a bus-based approach.

As shown in Fig. 6b, the BB-Rt presents the lowest delay compared to the other protocols. The delay is reduced by more than 50%. The main reason is that the buses have larger communication range compared to the others. In addition, the packet control overhead of BB-Rt is small, because only the buses have to send packets. We also observe that the average delay increase from 46 ms with 100 nodes to 79 ms with 400 nodes. This can be explained by the relationship between node density and transmission delay in large-scale wireless ad hoc networks in general and VANETs is one of these networks.

Fig. 6c demonstrates that BB-Rt has shorter route length than AODV route. The improvement is about 20% in average by using Car-Rt, and more than 50% by using BB-Rt. Changes in amount of nodes in network do not intensively

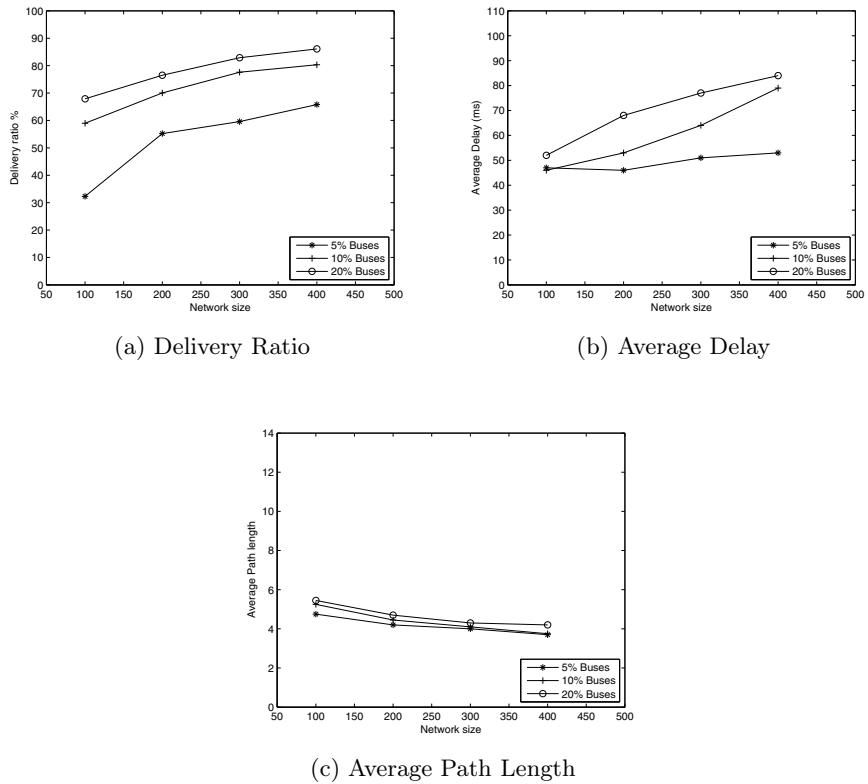


Fig. 7. Performance of BB-Rt with different percentage of buses

influence the efficiency of our proposed approach. The less number of hops in BB-Rt is due principally to the fact that only buses participate in the forwarding of packets compared to the Car-Rt and the Car-AODV where buses and cars participate together and are treated equally in this process.

Performance of BB-Rt with Different Percentage of Buses. The percentage of buses in Beijing is about 10% to 20% of vehicles on the roads. In this section we compare the performance of our approach with different percentage of buses; 5%, 10% and 20%. The average speed of buses is about 15km/h.

Fig. 7 shows that a low percentage of buses on roads influence the performance of our approach, where buses are considered as a mobile backbone of the network. As mentioned above, in real city scenario the percentage of buses on roads is about 10% and the simulation results show that with this percentage of buses we got acceptable results.

Performance of BB-Rt with Different Transmission Ranges of Buses. In this section, we compare the performance of BB-Rt with different transmission range of buses (i.e., 250m, 400m and 500m). Fig. 8 shows the influence of the

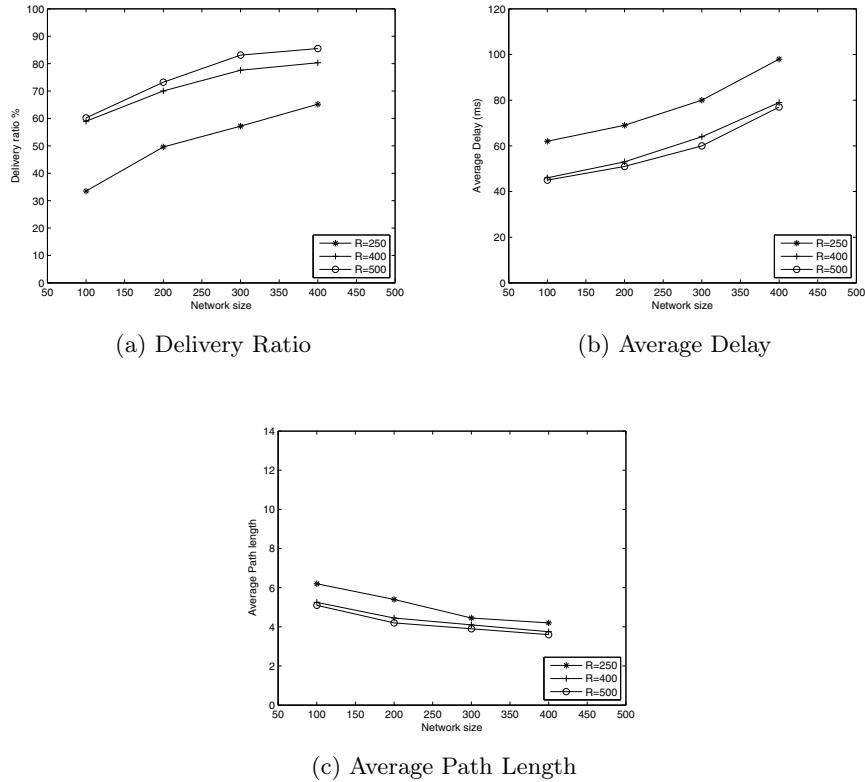


Fig. 8. Performance of BB-Rt with different transmission range of buses

transmission range. With the transmission range of bus is set to 400m, we got acceptable results. We assume that the buses are powerful and can support communication devices with a large transmission range.

6 Conclusion

The proposed bus-based routing protocol (BB-Rt) has been designed to choose a path with the smallest number of nodes, by considering buses as the mobile backbone of the network. This gives three important benefits: reducing the end-to-end delay in network, increasing the packets delivery ratio and reducing the number of nodes on a selected route in the city environment.

The simulation experiments show that BB-Rt protocol outperforms AODV and works well in various traffic situations including the variation of both transmission range and the percentage of buses on roads. With larger transmission range and smaller percentage of buses BB-Rt could generate acceptable results.

References

1. Trivedi, H., Veeraraghavan, P., Loke, S., Desai, A., Singh, J.: Routing mechanisms and cross-layer design for vehicular ad hoc networks: A survey. In: 2011 IEEE Symposium on Computers & Informatics (ISCI), pp. 243–248. IEEE (2011)
2. Li, F., Wang, Y.: Routing in vehicular ad hoc networks: A survey. IEEE Vehicular Technology Magazine 2(2), 12–22 (2007)
3. Papadimitratos, P., La Fortelle, A., Evenssen, K., Brignolo, R., Cosenza, S.: Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Communications Magazine 47(11), 84–95 (2009)
4. Booysen, M.J., Zeadally, S., van Rooyen, G.-J.: Survey of media access control protocols for vehicular ad hoc networks. IET Communications 5(11), 1619–1631 (2011)
5. Luo, J., Gu, X., Zhao, T., Yan, W.: Mi-vanet: A new mobile infrastructure based vanet architecture for urban environment. In: 2010 IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), pp. 1–5. IEEE (2010)
6. Perkins, C., Belding-Royer, E., Das, S., et al.: Rfc 3561-ad hoc on-demand distance vector (aodv) routing. In: Internet RFCs, pp. 1–38 (2003)
7. Karnadi, F.K., Mo, Z.H., Lan, K.-C.: Rapid generation of realistic mobility models for vanet. In: IEEE Wireless Communications and Networking Conference, WCNC 2007, pp. 2506–2511. IEEE (2007)
8. Cheng, P.-C., Weng, J.-T., Tung, L.-C., Lee, K.C., Gerla, M., Haerri, J.: GeoDTN+NAV: A hybrid geographic and dtn routing with navigation assistance in urban vehicular networks. In: MobiQuitous/ISVCS (2008)
9. Li, F., Zhao, L., Fan, X., Wang, Y.: Hybrid position-based and dtn forwarding for vehicular sensor networks. International Journal of Distributed Sensor Networks (2012)
10. Zhao, L., Li, F., Wang, Y.: Hybrid position-based and dtn forwarding in vehicular ad hoc networks. In: 2012 IEEE Vehicular Technology Conference (VTC Fall), pp. 1–5. IEEE (2012)

11. Sede, M., Li, X., Li, D., Wu, M.-Y., Li, M., Shu, W.: Routing in large-scale buses ad hoc networks. In: IEEE Wireless Communications and Networking Conference, WCNC 2008, pp. 2711–2716. IEEE (2008)
12. Vahdat, A., Becker, D., et al.: Epidemic routing for partially connected ad hoc networks. Technical report, Technical Report CS-200006, Duke University (2000)
13. Park, H.-S., Jang, J.-H., Lee, S.-H., Kim, J.-D.: Position-based dtn routing in metropolitan bus network. In: 2012 International Conference on Systems and Informatics (ICSAI), pp. 1449–1453. IEEE (2012)
14. Al-Janabi, S.T.F., Yaseen, Y.S., Askwith, B.: The bus ad hoc on-demand distance vector (BAODV) routing protocol. In: Proc. of Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, PGNet 2012 (2012)
15. Beijing Traffic Management Bureau, <http://www.bjtggl.gov.cn>
16. Ben Hassine, A., Matsubara, S., Ishida, T.: A constraint-based approach to horizontal web service composition. In: Cruz, I., Decker, S., Allemand, D., Preist, C., Schwabe, D., Mika, P., Uschold, M., Aroyo, L.M. (eds.) ISWC 2006. LNCS, vol. 4273, pp. 130–143. Springer, Heidelberg (2006)
17. Sheshagiri, M., DesJardins, M., Finin, T.: A planner for composing services described in daml-s. Web Services and Agent-based Engineering-AAMAS 3, 1–5 (2003)
18. The Network Simulator - ns-2, <http://www.isi.edu/nsnam/ns>
19. Krajzewicz, D., Hertkorn, G., Rössel, C., Wagner, P.: Sumo (simulation of urban mobility). In: Proc. of the 4th Middle East Symposium on Simulation and Modelling, pp. 183–187 (2002)
20. Huang, Y., Guan, X., Cai, Z., Ohtsuki, T.: Multicast capacity analysis for social-proximity urban bus-assisted vanets. In: 2013 IEEE International Conference on Communications (ICC), pp. 6138–6142. IEEE (2013)

Vehicular Ad Hoc Networks: Architectures, Research Issues, Challenges and Trends

Wenshuang Liang¹, Zhuorong Li¹, Hongyang Zhang¹,
Yunchuan Sun², and Rongfang Bie^{1,*}

¹ College of Information Science and Technology, Beijing Normal University, China

² School of Economic and Business Administration, Beijing Normal University, China

{lws, lsr, hongyang}@mail.bnu.edu.cn, {yunchuan, rfbie}@bnu.edu.cn

Abstract. Vehicular Ad hoc Networks (VANETs) have been quite a hot research area in the last few years. Due to its unique characteristics such as high dynamic topology and predictable mobility, VANETs attract so much attention from both academic and industry. In this paper, we provide an overview of the main aspects of VANETs from a research perspective. This paper starts with the basic architecture of networks, then discusses two critical technologies: routing, as well as security and privacy, and ends up with the analysis on challenges and future trends of VANETs.

Keywords: Vehicular Ad hoc Networks, Routing, Security and Privacy, Challenges and Trends.

1 Introduction

Recently, with the development of vehicle industry and wireless communication technology, Vehicular Ad hoc Networks are becoming one of the most promising research fields.

VANETs which use vehicles as mobile nodes is a subclass of Mobile Ad hoc Network (MANET) to provide the communication among nearby vehicles and between vehicles and nearby roadside equipment [1], but apparently differs from other networks by its own characteristics. Specifically, the nodes (vehicles) in VANETs are limited to road topology while moving, so if the road information is available, we are able to predict the future position of a vehicle; what's more, vehicles can afford significant computing, communication and sensing capabilities as well as provide continuous transmission power themselves to support these functions [2].

However, VANETs also come with several challenging characteristics, such as potentially large scale and high mobility. Nodes in the vehicular environment are much more dynamic because most cars usually are at a very high speed and change their position constantly. The high mobility also leads to a dynamic network topology, while the links between nodes connect and disconnect very often. Besides, VANETs have a potentially large scale which can include many participants and extend over the entire road network [2].

* Corresponding author.

It is precisely because of both these unique attractive features and challenging characteristics that VANETs could draw the attention of both industry and academia.

Therefore, several articles have tried to summarize the issues about vehicular networks. For example, In [3][4], the authors discuss the research challenges of routing in VANETs, and summarize and compare the performance of routing protocols; While, Hartenstein, H et al. present an overview on the communication and networking aspects of VANETs and summarizes the current state-of-the-art at that time[5]; Maxim Raya et al. address the security of VANETs comprehensively, provides a set of security protocols as well[6]; in [7], the authors propose a taxonomy of a large range of mobility models available for vehicular ad hoc networks. These articles are all overview specific research areas in VANETs. In addition, others papers like [8] provide comprehensive overview of applications, architectures, protocols and challenges in VANETs, especially introduces VANETs projects and standardization efforts in different regions (i.e. USA, Japan and Europe); Saif et al. provide a detailed information for readers to understand the main aspects and challenges related to VANETs, including network architecture, wireless access technologies, characteristics, applications, and simulation tools[9].

Compared with these current articles, this paper adds the introduction of layered architecture for VANETs so that the summary of network architecture is more completely. Also, we organize the overview of the vehicular ad hoc networks in a novel way. That is we introduce the VANETs from the research perspective in the paper, including some current critical technologies, which do good to the progress of VANETs. Moreover, we provide a more comprehensive analysis on VANETs research challenges and future trends, beneficial for further systematic research on VANETs. In summary, this paper covers basic architecture, critical technologies of VANETs, and provides an overall reference on VANETs.

The rest of this paper is organized as follows. Section 2 first introduces the vehicular Ad Hoc networks architecture, including network components, communication types and layered network architecture. Then in Section 3, we discuss two aspects of VANETs research issues: routing, as well as security and privacy. Section 4 provides an analysis on VANETs research challenges and future trends. Finally, concludes the paper in Section 5.

2 Architecture

This part describes the system architecture of Vehicular Networks. We first introduce the main components of VANETs architecture from a domain view. Then, we explain their interaction and introduce the communication architecture. Besides, we provide a presentation of the layered architecture for VANETs.

2.1 Main Components

According to the IEEE 1471-2000 [10,11] and ISO/IEC 42010 [12] architecture standard guidelines, we are able to achieve the VANETs system by entities which

can be divided into three domains: the mobile domain, the infrastructure domain and the generic domain[13].

As is shown in Fig. 1, the mobile domain consists of two parts: the vehicle domain and the mobile device domain. The vehicle domain comprises all kinds of vehicles such as cars and buses. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smart phones.

Within the infrastructure domain, it includes two domain: the roadside infrastructure domain and The central infrastructure domain. The roadside infrastructure domain contains roadside unit entities instantiated like traffic lights. The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers[13].

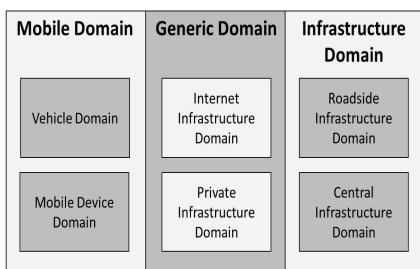


Fig. 1. VANETs System Domains

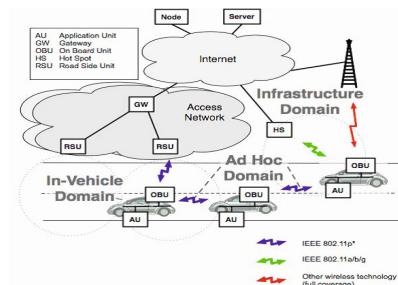


Fig. 2. C2C-CC reference architecture [15]

However, the development of VANETs architecture varies from region to region. In the CAR 2 X Communication System which is pursued by the CAR 2 CAR Communication Consortium, the reference architecture is a little different. CAR 2 CAR Communication Consortium (C2C-CC) is the major driving force for vehicular communication in Europe and published its “manifesto” in 2007. This system architecture comprises three domains:in-vehicle, ad hoc, and infrastructure domain.

As show in Fig. 2, the in-vehicle domain is composed of an on-board unit (OBU) and one or multiple application units (AUs). The connections between them are usually wired and sometimes wireless. While, the Ad-hoc domain is composed of vehicles equipped with OBUs and road-side units (RSU). An OBU can be seen as a mobile node of an Ad Hoc network, RSU is a static node likewise. An RSU can be connected to the Internet via the gateway; RSUs can communicate with each other directly or via multi-hop as well. There are two types of infrastructure domain access, RSU and hot spot (HS). OBUs may communicate with Internet via RSUs or hot spots. In the absence of RSUs and hot spots, OBUs can also communicate with each other by using cellular radio networks (GSM, GPRS, UMTS, WiMAX, and 4G) [2].

2.2 Communication Architecture

Communication types in VANETs can be categorized into four types. The category is closely related to VANETs components as described above. Fig. 3 describes the key functions of each communication type [16].

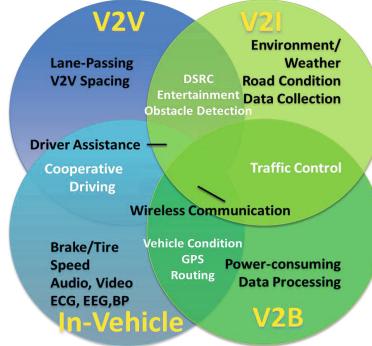


Fig. 3. Key functions of each communication type

In-Vehicle Communication, which is more and more necessary and important in VANETs research, refers to the in-vehicle domain. In-vehicle communication system can detect a vehicle's performance and especially a driver's fatigue and drowsiness, which is critical for driver and public safety.

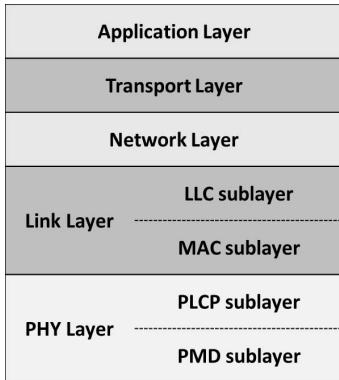
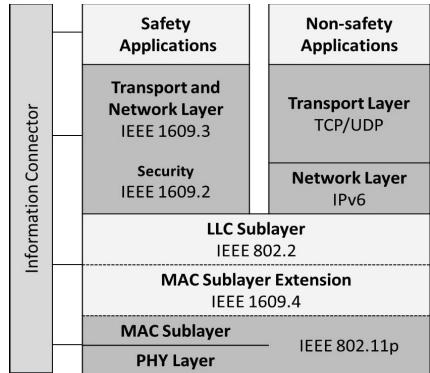
Vehicle-to-Vehicle (V2V) Communication can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-Road Infrastructure (V2I) Communication is another useful research field in VANETs. V2I communication enables real-time traffic/weather updates for the driver and provides environmental sensing and monitoring.

Vehicle-to-Broadband Cloud (V2B) Communication means that vehicles may communicate via wireless broad band mechanisms such as 3G/4G. As the broad band cloud may include more traffic information, monitoring data, as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

2.3 Layered Architecture for VANETs

The Open Systems Interconnection (OSI) model is well-known to most readers, which groups similar communication functions into one of seven logical layers [17]. The session layer and presentation layer are omitted here, and a given layer can be further partitioned into sublayers in this architecture, as illustrated in Fig. 4[18].

**Fig. 4.** OSI reference architecture**Fig. 5.** Layered architecture for DSRC

VANETs architectures differ from region to region, thus the protocols and interfaces are also different among them. Fig. 5 illustrates the protocol stack for dedicated short-range communication (DSRC) in the US. DSRC is specifically designed for automotive use and a corresponding set of protocols and standards [18]. The US FCC has allocated 75MHz of spectrum for DSRC communication, from 5.850 GHz to 5.925 GHz [18]. Different protocols are designed to use at the various layers, some of them are still under active development now. The IEEE 802.11p, an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), is focused primarily on the PHY layer and MAC sublayer of the stack. IEEE 1609 is a higher layer standard based on the IEEE 802.11p. IEEE 1609 represents a family of standards that function in the middle layers of the protocol stack to flexibly support safety applications in VANETs. While non-safety applications are supported through another set of protocols. In particular, network layer services and transport layer services for non-safety applications are provided by three quite stable protocols: IPv6, TCP and UDP [11,18,19].

3 Research Issues

This part is a brief introduction to two aspects of VANETs research issues: routing, as well as security and privacy. Firstly, we discuss the classification of routing protocols. then the state of the art security and privacy are discussed.

3.1 Routing

In VANETs, wireless communication has been a critical technology to support the achievement of many applications and services. However, due to the characteristics of VANETs such as high dynamic topology and intermittent connectivity, these existing routing algorithms in MANETs are not available for

most application scenarios in VANETs. Thus researchers spare no effort to improve existing algorithms as well as design new ones, so that the communication reliability can be ensured. Depending on the number of senders and receivers involved, routing approaches can be divided into three types: geocast/broadcast, multicast, and unicast approaches.

- **Geocast/broadcast:** With the requirement of distributing messages to unknown/unspecified destinations, the geocast/broadcast protocols are necessary in VANETs. In [21], the authors review the current message broadcast protocols on vehicular networks, such as a spatially aware packet routing algorithm, SADV, FROV and a multi-hop broadcast protocol. Likewise, Omprakash et al. present an overview on Geocast Routing(GR) and categorize GR into two groups namely urban and highway based on traffic environment, such as CAGR, VDLA, FPBR and IPSA.[22].
- **Multicast:** Multicast is necessary to communications among a group of vehicles in some vehicular situations, such as intersections, road blocks, high traffic density, accidents and dangerous road surface conditions. In [21], the authors categorize the multicast protocols into two main types. One is topology-based approaches, such as ODMRP, MAODV and GHM. The other is location-based approaches, such as PBM, SPBM, LBM, as well as RBM and IVG. Besides, Dr.Parminder Singh evaluates the performance of some Multicast routing protocols like ODMRP and ADMR [46].
- **Unicast:** Researchers investigate the unicast communication protocols for VANETs in three ways: (1) greedy: nodes forward the packets to their farthest neighbors towards the destination, like Improved Greedy Traffic-Aware Routing (GyTAR), (2) opportunistic: nodes employ the carry-toward technique in order to opportunistically deliver the data to the destination, like Topology-assist Geo-Opportunistic Routing, and (3) trajectory based: nodes calculate possible paths to the destination and deliver the data through nodes along one or more of those paths, like Trajectory-Based Data Forwarding (TBD) [23].

3.2 Security and Privacy

Nowadays more and more intelligent onboard applications may store lots of personal information and vehicular tracks are available electronically, the problem of security and privacy has become an emerging hot research field in VANETs. Security and privacy are two of the critical fundamental problems which have to be solved before vehicular network communications among vehicles or between vehicles and infrastructures can be deployed. Otherwise, the reliability, dependability and user acceptance of the VANETs system is likely to be low, because attackers may manipulate messages or track the itineraries of vehicles[25,26]. In addition, in [47], the authors analyze some possible attacks in VANETs, such as data trust attack and replay attack.

There has been significant interest and progress in the field of security and privacy over the last few years. The majority of researchers have been focusing

on the vehicular communication system, which is a promising approach to facilitate road safety, traffic management, and message dissemination for drivers and passengers[20]. In general, security architecture and vehicular communication are receiving increasing attentions from academia and industry. In [29], the authors describe the security architecture using different viewpoints, such as the functional layer view, the organizational/component view, the reference model view and the information centric view. In [30], the authors present a novel security architecture focusing primarily on securing the operation of the wireless part of the vehicular communication system and on enhancing the privacy of its users. Security vehicular communication draws more attention relative to architecture, such as secure communication schemes and algorithms[26,31]. Raya et al. present a communication scheme, which entities would like to establish a share session key if they need to securely communication for a long time. This scheme pays much attention on safety-related applications, but the non-safety-related applications are neglected [6,33]. In [31], the authors present an advanced secure communication scheme based Raya and Hubaux's scheme, which extends its session key to be using in non-safety-related applications. In [32], the authors discuss many security solutions that have been proposed in detail, such as VPKI, CA and the group signature.

4 Challenges and Future Trends

Based on the previous discussion of VANETs, we can see that VANETs is a fantastic self-organizing network for the future intelligent transportation system (ITS). Although researchers have achieved much great progress on VANETs study, there are still some challenges that need to be overcome and some issues that need to be further investigated, e.g., communication, security, applications, stimulation, verification, and services, etc.[16,34].

4.1 Top Challenges

Compared with Mobile Ad Hoc Network (MANET), the specific features of VANETs require different communication paradigms, approaches to security and privacy, and wireless communication system [35]. For example, network connections may not be stable for a long time period. In order to improve the performance of communication, researchers have investigated the efficient use of available infrastructure, such as road side units and cellular networks. Although, many specific challenges of VANETs have been overcome, we believe that many key research challenges have only partially been solved [35]. Thus, researchers need to do deeper work to solve these challenges. In the following discussion we will summarize the key challenges.

- **Fundament Limits and Opportunities.** Surprisingly little is known about the fundamental limitations and opportunities of VANETs communication from a more theoretical perspective [36]. We believe that avoiding accidents and minimizing resource usage are both important theoretical research challenges.

- **Standards.** The original IEEE802.11 standard cannot well meet the requirement of robust network connectivity, and the current MAC parameters of the IEEE802.11p protocol are not efficiently configured for a potential large number of vehicles [16]. Thus, researchers may do more work about standards.
- **Routing Protocols.** Although researchers have been presented many effective routing protocols and algorithms such as CMV (Cognitive MAC for VANET) and GyTAR (Greedy Traffic Aware Routing), the critical challenge is to design good routing protocols for VANETs communication with high mobility of vehicles and high dynamic topology [34].
- **Connectivity.** The management and control of Network connections among vehicles and between vehicles and network infrastructure is the most important issue of VANETs communication [37]. Primary challenge in designing vehicular communication is to provide good delay performance under the constraints of vehicular speeds, high dynamic topology, and channel bandwidths [38].
- **Cross-layer.** In order to support real-time and multimedia applications, an available solution is to design cross-layer among original layers [38]. In general, cross-layer protocols that operate in multiple layers are used to provide priorities among different flows and applications. In [35,40], the authors address the importance of cross-layer design in VANETs after analyzing the performance metrics.
- **Cooperative Communication.** In [37], the authors consider the VANETs as a type of cloud called Mobile Computing Cloud (MCC), and in [16], the authors present a broadband cloud in vehicular communication. Thus, the cooperation between vehicular clouds and the Internet clouds in the context of vehicular management applications has become a critical challenge to researchers.
- **Mobility.** Mobility that is the norm for vehicular networks makes the topology change quickly. Besides, the mobility patterns of vehicles on the same road will exhibit strong correlations [40]. In [33], the authors address that mobility plays a key role in vehicular protocol design and modeling.
- **Security and Privacy.** Frank et al. present many solutions that come at significant drawbacks and the mainstream solution still relies on 'key-pair / certificate / signature'[41]. For example, key distribution is a key solution for security protocols, but key distribution poses several challenges, such as different manufacturing companies and violating driver privacy [40]. Besides, tradeoff the security and privacy is the biggest challenge under the requirement of efficiency.
- **Validation.** It is not only necessary to assess the performance of VANETs in a real scenario but also to discover previously unknown and critical system properties. Besides, validation has become more and more difficult under the wider range of scenarios, Onur Altintas et al. present can use Field Operational Tests (FOTs) to solve this problem, but conducting meaning FOTs is a challenge like a large and complex system with technology components [37].

Thus, considering the characteristics of high mobility and high dynamic topology, these challenges discussed above are still needed to do more research work to solve them.

4.2 Future Trends

As the society is more and more intelligent, the potential value of VANETs is unpredictable with safety and entertainment applications. New vehicle applications have recently emerged in several areas ranging from navigation safety to location aware content distribution, commerce and games [37]. Thus, the VANETs need to continue to explore and study, and we believe that there must be more applications and research results in the future. For instance, we consider the routing protocols and algorithms in VANETs. The DSRC technology is proposed to provide a communication link between vehicles and road side beacons [42], and the evolution of DSRC is also discuss in [43], the trends of DSRC are better channel interleaving and channel coding, more flexibility in channelization, and better MAC congestion control protocols. It is advanced to apply such DSRC to VANETs. We now discuss some possible future trends of VANETs in three aspects including architecture, algorithm and application, which we called 3A.

Architecture: In the future, a main research issue of vehicular networks focuses on designing an integrated system architecture that can make use of multiple different technologies (e.g. IEEE 802.11p DSRC, WAVE, ITS G5, Wi-Fi, or 3G/4G) and heterogeneous vehicular networks [37]. Besides, in order to the deployment of the FOT mentioned above, researchers need to design a large scale and complex system architecture which should cooperate with different partners and manufacturers [13]. Thus, the reliable and flexible system architecture is one of the main research trends.

Algorithm: Although these existing algorithms have been provided some solutions with these data dissemination problems in VANETs, it is still difficult to examine their performance and security because of these features of VANETs mentioned above. For example, due to the non-persistent network connections, the end-to-end communication path may not exist. In [44], the authors present that the opportunistic routing algorithm can solve this problem with the carry-forwarding pattern. So the advanced algorithms should be designed with the low communication delay, the low communication overhead and the low time complexity.

Application: Due to requiring continuous awareness of the road ahead, safety applications is still the key research trend in the mobile vehicular environment. Moreover, the authors find no applications followed these VANETs application guidelines after studying the most popular vehicular applications in the Android marketplace [45]. So, researchers should do more work about applications' standards and security, and investigate the question "how to use model checking to automatically explore whether these applications meet the standards".

5 Conclusion

In this paper, we first introduce the vehicular networks architecture, including network components, communication types and layered network architecture. Then we discuss two critical technologies in VANETs research issues: routing, as well as security and privacy. Finally, we provide an analysis on VANETs research challenges and future trends.

This paper introduces the vehicular ad hoc networks from the research perspective, covers basic architecture, critical technologies of VANETs, and provides a comprehensive reference on vehicular Ad Hoc networks.

Acknowledgement. This research is sponsored by National Natural Science Foundation of China (61003225, 61171014, 61272475 and 61371185), the Fundamental Research Funds for the Central Universities (2012LYB46, 2013NT57) and by SRF for ROCS, SEM.

References

1. Sivasakthi, M., Suresh, S.R.: Research on vehicular ad hoc networks (VANETs): An Overview. *Journal of Applied Sciences and Engineering Research* 2(1), 23–27 (2013)
2. Moustafa, H., Zhang, Y.: Vehicular networks: techniques, standards, and applications. CRC Press (2009)
3. Li, F., Wang, Y.: Routing in Vehicular Ad Hoc Networks: A Survey. *Vehicular Technology Magazine*, 12–22 (2007)
4. Su, X.: A Comparative Survey of Routing Protocol for Vehicular Sensor Networks. In: 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), pp. 311–316 (2010)
5. Hartenstein, H., Laberteaux, K.P.: A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communications Magazine*, 164–171 (2008)
6. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. *Journal of Computer Security* 15(1/2007), 39–68 (2006)
7. Harri, J., Filali, F., Bonnet, C.: Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy. *IEEE Communications Surveys & Tutorials* 11(4), 19–41 (2009)
8. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., Weil, T.: Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Survey & Tutorials* 13(4), 584–616 (2011)
9. Al-Sultan, S., Al-Door, M.M., AlBayatti, A.H., Zedan, H.: A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications* 37, 380–392 (2013)
10. Maier, M.W., Emery, D., Hilliard, R.: Software architecture: Introducing IEEE standard 1471. *IEEE Computer* 34(4) (2001)
11. Maier, M.W., Emery, D., Hilliard, R.: ANSI/IEEE 1471 and systems engineering. *Systems Engineering* 7(3) (2004)

12. Emery, D., Hilliard, R.: Every architecture description needs a framework: Expressing architecture frameworks using ISO/IEC 42010. In: Proc. Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture, WICSA/ECSA (2010)
13. Kosch, T., Schroth, C., Strassberger, M., Bechler, M.: Automotive Internet-working (2012)
14. Lysaker, N.: Vehicular Networks: Techniques, Standards, and Applications. Auerbach Publications (2009)
15. CAR 2 CAR Communication Consortium Manifesto (2007),
http://elib.dlr.de/48380/1/C2C-CC_manifesto_v1.1.pdf
16. Faezipour, M., Nourani, M., Saeed, A., Addepalli, S.: Progress and challenges in intelligent vehicle area networks. Communications of the ACM 55(2) (2012)
17. http://en.wikipedia.org/wiki/OSI_model
18. Hartenstein, H., Laberteaux, K.: VANET-Vehicular Applications and Inter-Networking Technologies. Wiley (2010)
19. http://en.wikipedia.org/wiki/IEEE_802.11p
20. Emmelmann, M., Bochow, B., Kellum, C.: Vehicular Networking Automotive Applications and Beyond. Wiley (2010)
21. Yang, J., Fei, Z.: Broadcasting with Prediction and Selective Forwarding in Vehicular Networks. International Journal of Distributed Sensor Networks (2013)
22. Kaiwartya, O., Kumar, S.: Geocast Routing: Recent Advances and Future Challenges in Vehicular Ad Hoc Networks. In: Internation Conference on Signal Processing and Integrated Networks (SPIN), pp. 291–296 (2014)
23. Wahid, A., Yoo, H., Kim, D.: Unicast geographic routing protocolsfor inter-vehicle communications: a survey. In: Proceedings of the 5th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks, PM2HW2N 2010, pp. 17–24. ACM, New York (2010)
24. Kim, D., Cano, J.C., Wang, W., De Rango, F., Hua, K.: Data Disseminations in Vehicular Environments. International Journal of Distributed Sensor Networks (2013)
25. Dötzer, F.: Privacy Issues in Vehicular Ad Hoc Networks. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 197–209. Springer, Heidelberg (2006)
26. de Fuentes, J.M., Gonzlez-Tablas, A.I., Ribagorda, A.: Overview of security issues in Vehicular Ad-hoc Networks (2010)
27. Sivasakthi, M., Suresh, S.R.: Research on vehicular ad hoc networks (VANETs): An Overview. Journal of Applied Sciences and Engineering Research 2(1), 23–27 (2013)
28. Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., Shen, X(S.): Security in Vehicular Ad Hoc Networks. IEEE Communications Magazine (2008)
29. Gerlach, M., Festag, A., Leinmuller, T., Goldacker, G., Harsch, C.: Security Architecture for Vehicular Communication
30. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.-P.: Secure Vehicular Communication Systems: Design and Architecture. IEEE Communications Magazine (2008)
31. Wang, N.-W., Huang, Y.-M., Chen, W.-M.: A novel secure communication scheme in vehicular ad hoc networks. Journal of Computer Communications 31(12), 2827–2837 (2008)
32. Samara, G., Al-Salihy, W.A.H., Sures, R.: Security Issues and Challenges of Vehicular Ad Hoc Networks (VANETs). In: 4th International Conference on New Trends in Information Science and Service Science (NISS), pp. 393–398 (2010)

33. Raya, M., Hubaux, J.P.: The Security of Vehicular Ad Hoc Networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks, pp. 11–21 (2005)
34. Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS) status, results, and challenges (2012)
35. Dressler, F., Kargl, F., Ott, J., Tonguz, O.K., Wischhof, L.: Research Challenges in Inter-Vehicular. Karlsruhe Institute of Technology (2010)
36. Hartenstein, H., Heijenk, G., Mauve, M., Scheuermann, B., Wolf, L.: Working Group on Fundamental Limits and Opportunities. Karlsruhe Institute of Technology (2010)
37. Altintas, O., Dressler, F., Hartenstein, H., Tonguz, O.K.: Inter-Vehicular Communication - Quo Vadis, vol. 3(9), pp. 190–213. Karlsruhe Institute of Technology, KIT, Dagstuhl Reports (2014)
38. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., Weil, T.: A Survey and Tutorial on Requirements, Architectures, Challenges. In: Gerla, M., Kleinrock, L. (eds.) Vehicular Networks and the Future of the Mobile Internet, Computer Networks (2011)
39. Sommer, C., Tonguz, O.K., Dressler, F.: Adaptive Beaconing for Delay-Sensitive and Congestion-Aware Traffic Information Systems. In: 2nd IEEE Vehicular Networking Conference (VNC 2010), pp. 1–8. IEEE, Jersey City (2010)
40. Parno, B., Perrig, A.: Challenges in Securing Vehicular Networks (2009)
41. Kargl, F., Buttyan, L., Eckhoff, D., Schoch, E.: Working Group on Security and Privacy. Karlsruhe Institute of Technology, KIT (2011)
42. Cseh, C.: Architecture of the Dedicated Short-Range Communications (DSRC) Protocol (1998)
43. Wu, X., Subramanian, S., Guha, R., White, R.G., Li, J., Lu, K.W., Buccheri, A., Zhang, T.: Vehicular Communications Using DSRC Challenges, Enhancements, and Evolution. IEEE Journal on Selected Areas in Communications/Supplement 31(9), 399–408 (2013)
44. Wang, S., Liu, M., Cheng, X., Li, Z., Huang, J., Chen, B.: Opportunistic Routing in Intermittently Connected Mobile P2P Networks. IEEE Journal on Selected Areas in Communications, 369–378 (2013)
45. Lee, K., Flinn, J., Giuli, T.J., Noble, B., Peplin, C.: AMC: Verifying User Interface Properties for Vehicular Applications. In: Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services, pp.1–12 (2013)
46. Singh, P.: Comparative study between Unicast and Multicast Routing Protocols in Different Data Rates Using VANET. In: International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT), pp. 278–284 (2014)
47. Kim, Y.K., Kim, I.: Security Issues in Vehicular Networks. In: International Conference on Infromation Networking (ICON), pp. 468–472 (2013)

Empirical Study on Spatial and Temporal Features for Vehicular Wireless Communications

Yingwen Chen¹, Ming Xu¹, Pei Li², and Bin Zhang³

¹ College of Computer, National University of Defense Technology,
Changsha, Hunan 410073, China

² College of Information Systems and Management,
National University of Defense Technology, Changsha, Hunan 410073, China

³ Beijing Institute of Systems Engineering, Beijing 100101, China
csywchen@gmail.com, {xuming,peili}@nudt.edu.cn, zhangbinndu@sina.cn

Abstract. Traditional networking technologies based on static topology analysis are not sufficient to the dynamic Vehicular Ad hoc Network. Understanding the network dynamics caused by vehicle mobility is very important for routing protocol design and algorithm optimization. This paper explores the spatial and temporal features based on two real taxi-trace datasets. It reveals that the whole topology of VANETs consists of a large number of small-sized connected components. When the communication range is greater than a threshold, a large proportion of vehicles will connect to a largest connected component, which covers the most part of the downtown region of the city both in on-peak hour and off-peak hour. Based on the analytical results, we propose several design philosophies and new research issues for VANETs.

Keywords: Wireless Communications, Spatial Temporal Analysis, Connected Component, VANETs.

1 Introduction

Vehicular Ad hoc Networking, shorten as VANET, is one kind of new technology for Intelligent Transportation Systems and Smart Cities. By using Dedicated Short Range Communications radios, vehicles can not only exchange messages directly with vicinity nodes but also communicate with other nodes through a number of intermediate nodes.

Since the nodes have capability of communicating with each other, VANETs can provide a number of potential applications with highly diverse requirements. Three major classes of applications possible in VANET are safety oriented, convenience oriented and commercial oriented[5]. Safety applications include immediate collision warning, forward obstacle detection and avoidance, emergency message dissemination and so on. Convenience applications can provide route maps with real-time traffic jams and accident conditions to help the drivers to find the shortest path in terms of time consumption. Commercial applications can provide Internet access, as well as communication between passengers in cars

in the same vicinity, allowing the passengers to surfer the Internet, watch online movies, and even play games.

To support information diffusion in VANETs, two kinds of network architectures are proposed. One is called Vehicle-to-Vehicle(V2V), in which vehicles can communicate when they locate in the communication range of each other. The other one is called Vehicle-to-Roadside(V2R) or Vehicle-to-Infrastructure(V2I) or Vehicle-to-Wayside(V2W), which is a cellular-like system. The roadside infrastructure is used as a basestation and it may dominate the communication in its communication range.

In V2V VANETs, vehicles are equal and information diffusion can be achieved by adopting MANET routing protocols. However, it is well known that moving vehicles result in a disconnected network topology[14], thus different kinds of carry-and-forward strategies[14][4][8] have been proposed to support intermittent connected networks. Carry-and-forward strategy is effective but not efficient, because the source might delay the forwarding until it meets the destination even though there is a routing path between them. It is shown that the packet forwarding delay caused by carry-and-forward can be several orders-of-magnitude longer than that caused by multi-hop forwarding over a connected network[7]. Consequently, we should figure out when and where the vehicles are connected and can be reached for routing purpose.

In V2R VANETs, the roadside infrastructure is usually more powerful than vehicles. To reduce system construction cost and improve communication efficiency, the deployment of roadside infrastructures should also be well studied. Intuitively speaking, the roadside infrastructures are better setup at those spots with poor V2V connectivity.

However, the moving vehicles bring a lot of uncertainty for infrastructure deployment. No one knows whether the connectivities of vehicles are depending on the locations of the city; or whether there is any difference between on-peak hours and off-peak hours. Therefore, connectivity and time variance of network topology should be examined.

This paper is to reveal the understanding of spatial and temporal dynamics of VANETs based on two real taxi-trace datasets collected from San Francisco, USA and Shenzhen, China. The analysis results are suppose to provide new guidelines for VANETs design and protocol optimization. The main contributions of this paper are as follows:

(1) We find that by adopting a reasonable communication range, a large number of vehicles are connected as a main component of the whole network.

(2) We analyze the location dependency of the largest connected component of the whole network. We find that most part of the downtown region of the city can be covered by the largest connected component of the VANET no matter in on-peak hours or off-peak hours.

(3) According to the spatial and temporal features that we have found, we propose several design philosophies and new research issues for VANETs.

The rest of the paper is organized as follows: Section 2 briefly summarizes the related work; Section 3 describes the definitions used in spatial and temporal

analysis for VANETs; Section 4 introduces the two taxi-trace datasets and presents the spatial and temporal discoveries as well as their implications for VANET design and protocol optimization. Finally, Section 5 concludes the article.

2 Related Work

With the broadcast feature of wireless channels, a VANET is always modeled by a unit disk graph, in which two vertices are connected if their distance is below a fixed threshold. By adopting this assumption, percolation theory can be used to analyze the connectivity of VANETs. For example, quantitative relationships among network connectivity, vehicle density, and transmission range are derived in [9].

When considering more realistic constraints of VANETs such as non-uniform and non-Poisson distributions, or non-ideal environments with fading/shadowing impact, Miorandi et al.[11] proposed an equivalent $GI|D|\infty$ queuing model to analyze the connectivity of one-dimensional ad hoc networks. Their results claim that no connectivity can be obtained in condition of channel randomness. Based on the equivalent $GI|D|\infty$ model, the node isolation probability and the average size of connected components can be estimated in one dimensional case. For one-dimensional VANETs, Zhuang et al.[17] also derived the exact expression for the average size of the connected components and their size distribution.

Furthermore, to analyze message propagation in two-dimensional traffic networks, the authors in [17] extended their model to calculate lattice connectivity probability for all the blocks in a district. In real traffic, most vehicles are travelling in a co-directional way. Abuelela et al. [4] found that co-directional traffic is inherently partitioned into connected components and provided an analytical expression of the expected size of those connected components. By exploring the co-directional feature and the existence of connected components, the authors in [4] also designed an Opportunistic Packet Relaying protocol (OPERA) for packet delivery over disconnected VANETs.

In recent years, complex network and network science[6] related concepts are widely adopted in many research domains. Monteiro et al.[12] decomposed the synthetic dynamical topology of VANETs into snapshots and calculated macro parameters of the network such as the node degree distribution, the clustering coefficients, the average shortest path length, and so on, for each topology snapshot.

Based on the abstracted information from network science, a new efficient broadcasting protocol called UV-CAST has been proposed. To further explore the dynamics of VANETs in a completely new way, more analysis[10][13] based on real and realistic simulated traces have been carried out in terms of many other kinds of complex network metrics. Literature [10] makes a thorough investigation of both micro-scale and macro-scale metrics including node degree, lobby index, link duration, network diameter, closeness centrality, betweenness centrality, number of communities, clustering coefficients, and so on. Similar to

[10], literature [13] conducts node-level and network-level analysis including node degree, network assortativity, betweenness centrality, and so on. Besides these, literature [13] also analyzes connected components' dynamics when the number of vehicles and communication ranges vary.

Generally speaking, literatures [9]-[17] explore VANETs' topology based on theoretical connectivity models. These models are useful in discussing the critical conditions or the connectivity boundary. But these theoretical models still rely on strong assumptions, which are very difficult to achieve in real cases. For example, the model in [9] requires a uniform distribution of the vehicles. However, it has been proved not to be true in real mobility scenarios[16]. Literatures [6]-[13] provide new methods to explore VANETs' topology based on network science models. Literatures [10] and [13] also analyze topology evolving by addressing the time-variant size of the connected components. However, their investigations have not considered the coverage area of the connected components. Different from the current work on VANETs' topology analysis, we conduct our research work based on two real taxi traces and propose a new metric to measure the location dependency of the largest connected component of the VANET.

3 Definitions

By adopting the Unit Disk Graph[3] model, VANETs topology can be abstracted as a non-directional graph tagged with timestamps. For better explanation, we first introduce some annotations for related definitions.

3.1 Network Model

The traditional static graph model in describing a network is $G = \langle V, E \rangle$, where V represents the nodes and E represents the connections between the nodes. However, the VANET is dynamic and the topology is evolving due to the movement of the vehicles. Therefore, the topology of VANET can be expressed by a timestamped graph $G(T) = \langle V, E, T \rangle$, where V represents all the vehicles, E represents the links between two vehicles, of which the Euclidean distance is smaller than the wireless communication range R , and T is the timestamps.

3.2 Routing Path

Routing in network is just to find a path in a given topology. We firstly define the routing path in a simplified static case. In a given timestamp t , the topology of VANET is $G(t) = \langle V_t, E_t, t \rangle$. There is a non-empty sub-graph of $G(t)$, denoted as $P(t) = \langle V'_t, E'_t, t \rangle$. Assume $V'_t \subseteq V, E'_t \subseteq E, n = |V'_t|, V'_t = \{v_{a1}, v_{a2}, \dots, v_{an}\}$. $P(t)$ is called a *Path* if and only if there exists $\sigma : V'_t \rightarrow V'_t; \sigma(v_{ai}) = v_i (i = 1, \dots, n)$, s.t. $E'_t = \bigcup_{j=1}^{n-1} (v_j, v_{(j+1)})$. Note that v_1 and v_n are called the two ends of the path at timestamp t . The path from v_1 to v_n can be denoted as Equation 1.

$$P_{v_1}^{v_n}(t) = \{v_1 \xleftarrow{t} v_n\} \quad (1)$$

The *length* of the path is $|V'_t|$, which is n . Note that, there are probably more than one path from v_1 to v_n in $G(t)$. Therefore, the *distance* from v_1 to v_n is defined as the shortest path from v_1 to v_n in $G(t)$. Meanwhile, there might be more than one shortest path from v_1 to v_n in $G(t)$ as well.

In a general case, routing path may pass through several timestamps. Without loss of generality, assuming the routing path from v_1 to v_n passes through a non-descending timestamp set $T_s = \{t_j | j=1^m\}$, then we have Equation 2.

$$P_{v_1}^{v_n}(T_s) = \bigcup_{j=1}^m (P_{v_{t_j1}}^{v_{t_jn}}(t_j)) = \bigcup_{j=1}^m \{v_{t_j1} \xleftarrow{t_j} v_{t_jn}\} \quad (2)$$

where $v_1 = v_{t_11}, v_n = v_{t_m n}$.

In VANET, data packets should be forwarded along the routing path in a consecutive way if the former node is connected to the latter node. However, if one node is not in the communication range of the next hop at a certain timestamp, the data packets should be buffered at this node until next timestamp comes when the consecutive two nodes on the path are connected to each other. Therefore, Equation 2 must fulfill the following requirement.

$$v_{t_k n} = v_{t_{(k+1)} 1} = V'_{t_k} \cap V'_{t_{(k+1)}} \quad (k = 1, \dots, m - 1) \quad (3)$$

3.3 Connected Component

The *Connected Component* at timestamp t is a non-empty sub-graph of network $G(t)$, in which there exists at least one path for any two vertices. That is, the *Connected Component* that node v_i is connected with at timestamp t can be denoted as Equation 4.

$$CC(t) = \bigcup_{v_i, v_j \in V_t} \{v_i \xleftarrow{t} v_j\} \quad (4)$$

As is mentioned in section 1, packets are forwarded much faster in a multi-hop way than that in a carry-and-forward style if the source node and the destination node are in the same connected component. Therefore, the performance of the routing strategy can be greatly improved if there are enough stable connected components in VANETs. We will analyze both the number and size of the connected components in Section 4.2.

3.4 Location Dependency

The location of the connected component is also important for network design. If the connected component is location dependent, in another word, if the vehicles always form the connected component in a specified region, we do not need to place roadside infrastructures in this region anymore. In order to measure the location dependency, we need the locations of all the vehicles in the connected component. For a given connected component $CC(t)$,

let $\Lambda_{CC(t)}$ represents the coordinate set of all the vehicles in $CC(t)$. Then we have $\Lambda_{CC(t)} = \{(x_{v_i}, y_{v_i}) | v_i \in V_{cc(t)}\}$. Let $\underline{X} = \min_{v_i \in V_{cc(t)}}(x_{v_i})$, $\underline{Y} = \min_{v_i \in V_{cc(t)}}(y_{v_i})$, $\overline{X} = \max_{v_i \in V_{cc(t)}}(x_{v_i})$, $\overline{Y} = \max_{v_i \in V_{cc(t)}}(y_{v_i})$. The rectangle covers $CC(t)$ can be defined as Equation 5.

$$\Gamma_{CC(t)} = [(\underline{X}, \underline{Y}), (\overline{X}, \overline{Y})] \quad (5)$$

where $(\underline{X}, \underline{Y})$ is the bottom left coordinate of rectangle $\Gamma_{CC(t)}$, and $(\overline{X}, \overline{Y})$ is the top right coordinate of rectangle $\Gamma_{CC(t)}$. In a consecutive timestamp set $T_s = \{t_j | j=1^m\}$, we denote the region that can cover vehicles in connected component at **any** timestamp in T_s as $\Psi = \bigcup_{j=1}^m \Gamma_{CC(t_j)}$, and denote the region that can cover vehicle in connected component at **all** timestamp in T_s as $\Omega = \bigcap_{j=1}^m \Gamma_{CC(t_j)}$. Assume the function $\delta()$ is used to calculate the area of a region, the location dependency factor of $CC(T_s)$ can be calculated by Equation 6.

$$\xi_{CC(T_s)} = \frac{\delta(\Omega)}{\delta(\Psi)} = \frac{\delta(\bigcap_{j=1}^m \Gamma_{CC(t_j)})}{\delta(\bigcup_{j=1}^m \Gamma_{CC(t_j)})} \quad (6)$$

It is obvious that $0 \leq \xi_{CC(T_s)} \leq 1$. $CC(T_s)$ is more location dependent when the value of $\xi_{CC(T_s)}$ is larger. The Location dependency of the connected components will be discussed in Section 4.3.

4 Dataset Analysis and Implications

This section we will analyze the spatial and temporal features of VANETs by using the concept of connected component other than using the individual node. Based on the discoveries, we will also present our suggestions for network design and optimization.

4.1 Taxi-Trace Dataset

As is shown in Table 1, we have collected two datasets of real taxi traces. One dataset contains GPS coordinates of more than 533 taxis collected in 20 days in San Francisco Bay area, USA[15] (SF for short). The other dataset contains GPS coordinates of 13,799 taxis in 9 days in Shenzhen, China (SZ for short). Most of the coordinate-update frequencies of SF dataset vary from 30 seconds to 60 seconds, and the SZ dataset has the coordinate-update frequency of about 30 seconds. Each vehicle has an individual trace file, in which the coordinates together with the timestamps are saved.

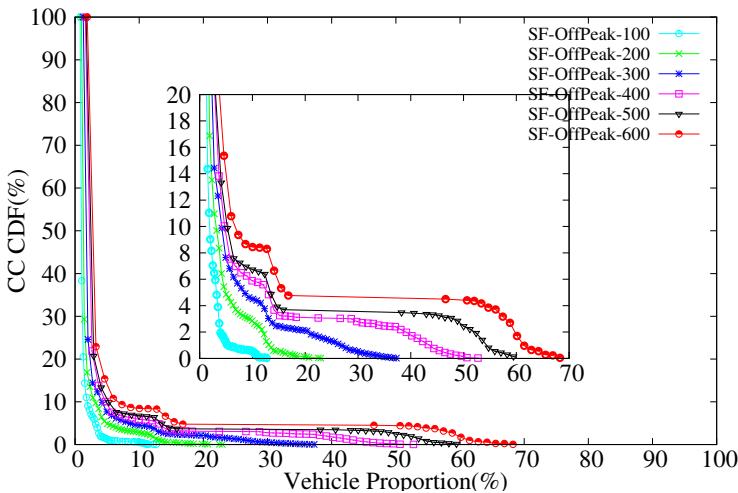
To capture the evolving features of network topology, we use linear interpolation to generate consecutive time synchronized coordinates with coordinate-update frequency of 30 seconds. To find the difference between topologies both in on-peak hour and off-peak hour, we select two observation intervals. One is from 1:00 am to 2:00 am, and the other is from 7:00 am to 8:00 am. To explore the variance according to different communication ranges, we choose six communication ranges from 100 meters to 600 meters.

Table 1. Taxi trace datasets. Brief summary of taxi traces for analysis.

	Taxi traces in San Francisco, USA	Taxi traces in Shenzhen, China
Vehicle quantity	533	13,799
Record duration	20 days	9 days
Update frequency	30s to 60s	30s
Taxi features	Timestamp, latitude, longitude, occupy status	Timestamp, latitude, longitude, occupy status, velocity, angle
File size	91MB compressed file	1.06GB compressed file

4.2 Size Distribution of Connected Components

Firstly, we take a look at the size distribution of the connected components, which is illustrated by Figure 1 to Figure 4. The x-axis is the fractions of the vehicles in the connected components, which is the size of the connected components divided by the total number of vehicles. The y-axis is the cumulated distribution of connected components. From the figures we can learn that most connected components are with very small size. However, the largest connected component contains a large number of vehicles. Larger communication range can enlarge the size of the connected components and hence slightly increase the fraction of big connected components. Comparing Figure 1 with Figure 2 and Figure 3 with Figure 4, we can conclude that the size distribution of the connected components is independent of the peak hours.

**Fig. 1.** Size distribution of CCs in SF during off-peak hour

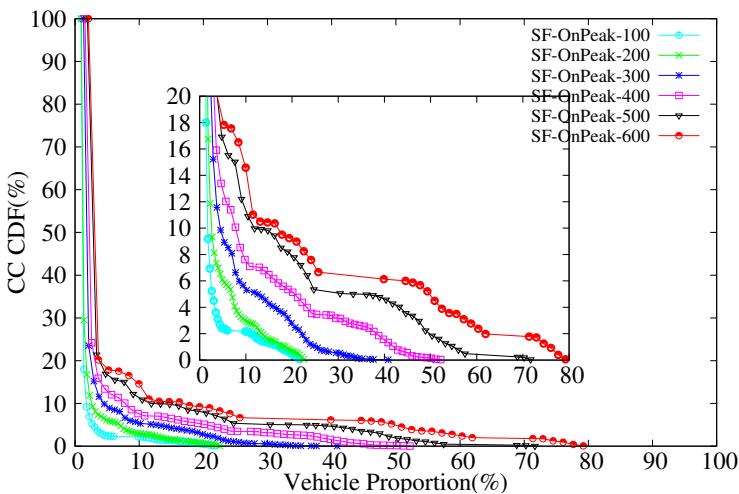


Fig. 2. Size distribution of CCs in SF during on-peak hour

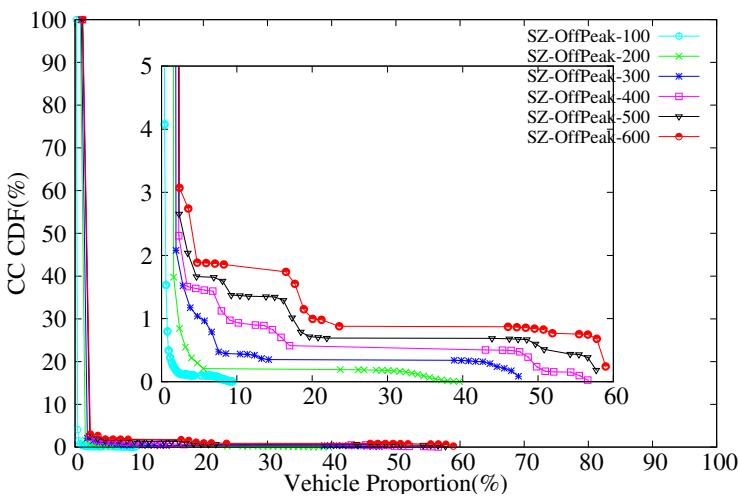


Fig. 3. Size distribution of CCs in SZ during off-peak hour

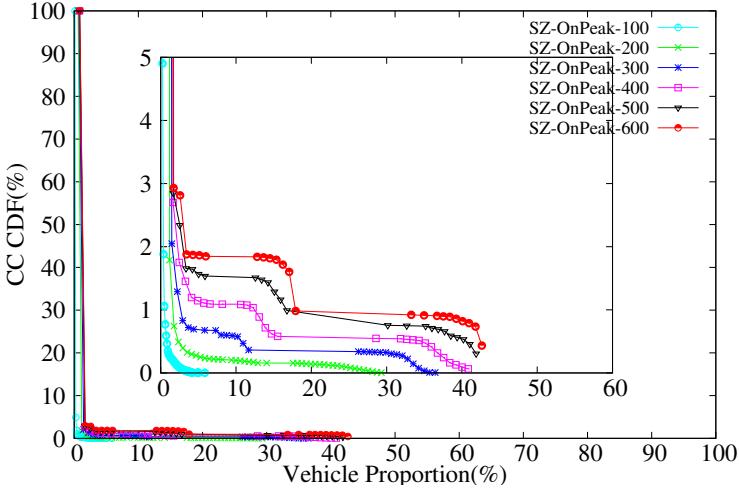


Fig. 4. Size distribution of CCs in SZ during on-peak hour.

Remark 1. Although the whole topology of the VANET is broken into a large number of small-size connected components, the largest connected component can cover a large number of vehicles. As Figure 2 shows, during the on-peak hour, the largest connected component in San Francisco even contains up to 70%-80% vehicles. Therefore, if the largest connected component keeps stable, we can make use of this feature by keeping important information on the vehicles in the largest connected component and design strategies to forward the information with the largest connected component.

4.3 Location Dependency of Connected Components

We study the location dependency of the largest connected component by calculating the location dependency factor defined in section 3.4. The results are given in Figure 5 and Figure 6. It is shown that the communication range is a critical parameter for the location dependency factor. The largest connected component covers a specific region when the communication range is large enough. In the two datasets we use, the communication range should be larger than 400 meters if we need the location dependency feature of the largest connected component. In more specified cases, when the communication range is 600 meters, we can get the results with $\delta(\Psi) \approx 56.24\text{km}^2$, $\delta(\Omega) \approx 12.21\text{km}^2$ in SF dataset and $\delta(\Psi) \approx 525\text{km}^2$, $\delta(\Omega) \approx 252\text{km}^2$ in SZ dataset. It is reported that the areas of downtown region both in San Francisco and in Shenzhen are 12.25km^2 [1] and 412km^2 [2] respectively. That means when the communication range is large enough, the largest connected component is just located in the downtown region.

As is defined in Section 3.4, $\delta(\Omega)$ is a non-increasing function according to the size of connected component, and $\delta(\Psi)$ is a non-decreasing function according

to the size of connected component. Therefore, with the same communication range, location dependency factor in on-peak hour is smaller than that in off-peak hour since the largest connected component contains more vehicles in on-peak hour. However, there is a contradiction in Figure 5. That is because for unknown reasons, some of the vehicles did not successfully record their coordinates at a regular frequency (every 30-60 seconds). These vehicles are deleted from the

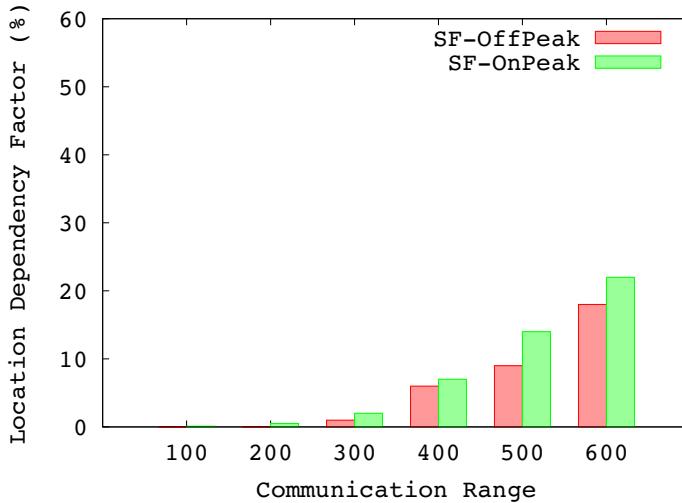


Fig. 5. Location dependency factor of largest CCs in SF

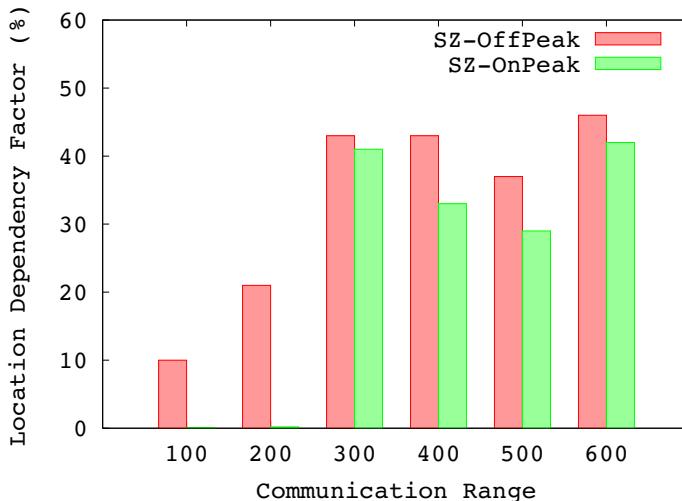


Fig. 6. Location dependency factor of largest CCs in SZ

topology due to the interpolation errors. Thus, in San Francisco case, the largest connected component contains less vehicles in on-peak hour than in off-peak hour.

Remark 2. The location dependency of the largest connected component contributes to two aspects in network design. One benefit is that we do not need to deploy roadside infrastructure to the spots where the connected component forms, because the connectivity can be maintained by the connected component. The other benefit is that vehicles in the downtown region should use multi-hop forwarding strategy rather than carry-and-forward strategy, since vehicles in this region have large probability to be connected to the largest connected component.

5 Conclusions

In this paper, we analyzed the spatial and temporal dynamics of VANETs based on two real taxi-trace datasets. We found that the whole topology of VANETs consists of a large number of small-sized connected components, however, the largest connected component among them contains a large proportion of vehicles. The performance of the routing protocol might be improved by using the largest connected component. Furthermore, by adopting a reasonable communication range, the largest connected component has the feature of location dependency, which is very useful to roadside infrastructure deployment and multi-hop packet forwarding. However, how to efficiently tracking the largest connected component in a distributed way; how to design new network architecture and routing protocols are still open research problems and they are left as our future work.

Acknowledgments. This paper is partially funded by National Natural Science Foundation of China under grant No.61003304, 61105124, and China Scholarship Council under grant 2011611534, 201206115013.

References

1. Manet driven by sf cab trace, <http://zjie.net/manet/cabtrace.php>
2. Shenzhen introduction, <http://en.wikipedia.org/wiki/Shenzhen>
3. Unit disk graph, <http://en.wikipedia.org/wiki/Unitdiskgraph>
4. Abueela, M., Olariu, S., Stojmenovic, I.: Opera: Opportunistic packet relaying in disconnected vehicular ad hoc networks. In: 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2008, pp. 285–294. IEEE (2008)
5. Bai, F., Elbatt, T., Hollan, G., Krishnan, H., Sadekar, V.: Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective. In: Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet), pp. 1–25 (2006)
6. Barabasi, A.L.: Network science. Philosophical Transactions of The Royal Society 371(1987), 1–3 (2013)

7. Jeong, J., Guo, S., Gu, Y., He, T., Du, D.H.: Tsf: Trajectory-based statistical forwarding for infrastructure-to-vehicle data delivery in vehicular networks. In: 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 557–566. IEEE (2010)
8. Jianbin, J., Yingwen, C., Ming, X., Gu, Y.: Improving the estimation of residual delay based forwarding method in opportunistic vehicular networks. In: 2012 9th International Conference on Ubiquitous Intelligence Computing and 9th International Conference on Autonomic Trusted Computing (UIC/ATC), pp. 79–86. IEEE (2012)
9. Jin, X., Su, W., Wei, Y.: A study of the vanet connectivity by percolation theory. In: 2011 IEEE Consumer Communications and Networking Conference (CCNC), pp. 85–89. IEEE (2011)
10. Louloudes, N., Pallis, G., Dikaiakos, M.D.: The dynamics of vehicular networks in urban environments. arXiv preprint arXiv:1007.4106 (2010)
11. Miorandi, D., Altman, E.: Connectivity in one-dimensional ad hoc networks: a queueing theoretical approach. *Wireless Networks* 12(5), 573–587 (2006)
12. Monteiro, R., Sargent, S., Viriyasitavat, W., Tonguz, O.K.: Improving vanet protocols via network science. In: 2012 IEEE Vehicular Networking Conference (VNC), pp. 17–24. IEEE (2012)
13. Naboulsi, D., Fiore, M.: On the instantaneous topology of a large-scale urban vehicular network: The cologne case. In: Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 167–176. ACM (2013)
14. Naumov, V., Gross, T.R.: Connectivity-aware routing (car) in vehicular ad-hoc networks. In: INFOCOM 2007, 26th IEEE International Conference on Computer Communications, pp. 1919–1927. IEEE (2007)
15. Piorkowski, M., Sarafijanovic-Djukic, N., Grossglauser, M.: Crawdad trace set epfl/mobility/cab. Downloaded (February 2009), <http://crawdad.cs.dartmouth.edu/epfl/mobility/cab> (v. February 24, 2009)
16. Piórkowski, M., Sarafijanovic-Djukic, N., Grossglauser, M.: A parsimonious model of mobile partitioned networks with clustering. In: First International Communication Systems and Networks and Workshops, COMSNETS 2009, pp. 1–10. IEEE (2009)
17. Zhuang, Y., Pan, J., Cai, L.: A probabilistic model for message propagation in two-dimensional vehicular ad-hoc networks. In: Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking, pp. 31–40. ACM (2010)

Schedule Algorithms for File Transmission in Vehicular Ad Hoc Networks

Chao Wang^{1,*}, Maya Larson², Yingwen Chen^{3,*}, and Xiumei Fan⁴

¹ School of Computer Science, Beijing Institute of Technology,
Beijing, P.R.China, 100081

² Department of Computer Science, The George Washington University,
Washington D.C., USA, 20052

³ College of Computer, National University of Defense Technology,
Changsha, Hunan, P.R.China, 410073

⁴ The School of Automation and Information Engineering,
Xi'an University of Technology, Xi'an, Shanxi, P.R.China, 710048

{wangchao.andy,csywchen}@gmail.com, maya_email.gwu.edu, xmfan@bit.edu.cn

Abstract. The development of vehicular ad-hoc networks has lead to several new services, such as instant messages, multi-media videos and large data transmissions. These applications have altered the pattern of data transmissions on VANETs to include larger volumes of data with different file sizes. Unstable links in vehicular networks are common due to channel fading and because of the vehicle moving, file transmissions are vulnerable to link interruption. How to utilize the limited link duration to transfer more files of different sizes successfully is a significant problem. Currently, the common practice to schedule file transmissions is a First In First Out (FIFO) mechanism defined in the DSRC (Dedicated Short Range Communication) standard. The algorithms presented in this paper show significant performance improvements. We proposed two algorithms, one based on transmission times and one based on due times. Both algorithms solve this problem by dynamically scheduling the file transmitting sequence according to selected criteria. Simulation results show that our algorithms significantly improve performance compared with FIFO mechanism for the transmission success rate and the network throughput.

Keywords: VANETs, schedule, file transmission, different sizes.

1 Introduction

A Vehicular Ad hoc Network (VANET) is defined as a set of vehicles communicating with peer-to-peer (P2P) wireless network techniques. It is composed of road side units (RSU) and onboard units (OBU) which are equipped with Global Position System (GPS) devices. The original purpose of VANETs was to provide safety information and services such as collision avoidance and traffic jam prediction. As VANET technology matures, additional applications have

* Corresponding author.

become possible, such as audio cell phone services, navigation information, instant messaging services, and video stream services. These emerging services are increasing the complexity of VANETs to the point where more sophisticated algorithms are necessary.

As described in the DSRC standard [1], larger files should be fragmented into small data packets then transmitted to destination nodes. All the fragmented packets must be reassembled at the destination node. When packets are lost, due to link interruptions while transmitting, nodes either resend the missing packet or drop the entire file. Attempting to send a file when the transmission processing time exceeds the link duration time will result in a failed transmission and waste bandwidth. Intuitively, we should avoid transmitting large files that are difficult to finish and transmit files with higher success probability. This transmitting schedule problem is significant in improving network performance.

This paper presents a solution to the file scheduling problem, defined as follows. Several files to different destinations are in a node's sending queue simultaneously. The problem is how to schedule the file transmission sequence, with the purpose of maximizing selected metrics measuring network performance. In our paper, we will call this problem as scheduling problem. In our work, we first prove that, the scheduling problem is an NP-Complete problem. Then we propose two algorithms, one based on transmission times and one based on the due times. These algorithms provide an approximate upper bound solution to this problem.

The remainder of this paper is organized as follows: Section 2 provides an overview of existing work on this topic. Section 3 presents the mathematical foundations of our algorithms. Section 4 presents the proof that the scheduling problem is NP-complete and describes the two algorithms in detail. Section 5 conducts simulations to analyze the algorithms and show improved performance. At last, we conclude and give future work in Section 6.

2 Related Literature

Generally, the data scheduling problem in VANETs is viewed at two levels, the packet level and the file level. The packet level schedule has been researched extensively with most of them focus on the network layer and MAC layer. In one example, the packet delay and loss probability have been investigated by [2].

A much smaller amount of research has focused on file level schedules. Macroscopically, from the perspective of the whole network, the schedule problem has been investigated by [14]. This paper proposed an algorithm to predict vehicle-platoons and an algorithm to strategically replicate data to buffers for redistribution. Microscopically, [8] has analyzed transmissions at the node level, proposing a mechanism to avoid transmission failures at each node. The algorithms in this paper cancel files that cannot be transmitted successfully, which reduces wasted transmissions, but it does not optimize the remaining files for network performance. Furthermore, the mechanisms in this paper are used mainly on infrastructure-less highways, and may not fit city scenarios.

Our work extends previous research in two directions. First, it can be applied to city scenarios and presents scheduling algorithms that optimize network performance. It is based on the link duration estimation work, such as [6] and [13]. These works considered several factors that affect the link duration time between two vehicles. These factors include vehicle velocity, driving direction, street map data and traffic light states. These works developed mechanisms that analyze these factors to estimate the link duration time.

Second, our work frames transmission scheduling as a make-span problem. The make-span problem has been researched for almost a century, and many scheduling algorithms have been proposed in [3] [9] [10]. But existing scheduling algorithms in the make-span problem cannot be applied directly to VANET scenarios because there are more constraints. We extend existing work on this topic by applying techniques from make-span problems to design algorithms that can improve performance in VANETs.

3 System Model

In this section, we introduce our main idea and then describe the mathematical model. We also present the assumptions and terminologies.

3.1 Main Idea

In this paper, we focus on the scheduling problem of how to sequence files to maximize network performance given the following assumptions:

- A node would like to send several files to different neighbors
- All files in the network have the same priority but different sizes
- All the wireless communications are in the same wireless channel (only 1 of the 7 channels in the DSRC standard is used)

Two centralized algorithms are proposed, one based on transmission time and one based on due time. We apply make-span techniques to schedule the files in an optimizing sequence for transmission. The metrics used to measure network performance are the rate of successfully transmitted files and network throughput (bits/second). Our algorithms are solutions that maximize these metrics.

3.2 Problem Definition

We define a set of nodes V in a vehicular ad-hoc network.

- $V = \{V_1, \dots, V_Q\}$: A node set V with Q nodes in the network.

The set of all files on V is defined as F . At any time instance, a node V_i may have a subset of files queued for transmission. A file F_{mn} has a source node V_m and a destination node V_n . Formal notation follows:

- $F = \{F_{mn} | m \in (1, \dots, Q), n \in (1, \dots, Q) \text{ and } m \neq n\}$

- $m \neq n$ means a node cannot send a file to itself
- $F_{mn} \neq F_{nm}$ as the first one is from V_m to V_n with the other opposite

For each file transmission, there are four time definitions:

1. $R_{F_{mn}}$ Release time: the instance when the file is released or when V_m and V_n come into each other's communication range
2. $D_{F_{mn}}$ Due time: the instance when a file is due or when V_m and V_n will leave each other's communication range
3. $S_{F_{mn}}$ Start time: the instance when the file start to transmit
4. $P_{F_{mn}}$ Transmission processing time: the length of time necessary to complete the transmission at current transmission rates

When V_m and V_n come into each other's communication range, F_{mn} is released. If the channel is idle, the source node V_m will establish a connection to the destination node V_n and start to transmit the file F_{mn} at start time $S_{F_{mn}}$. After a length of processing transmission time $P_{F_{mn}}$, the file will be received by V_n at a time instance t equal to $(S_{F_{mn}} + P_{F_{mn}})$. The due time $D_{F_{mn}}$, is a time instance when the connection between them will be interrupted. If $S_{F_{mn}} + P_{F_{mn}} > D_{F_{mn}}$, then the transmission of file F_{mn} will be unsuccessful. We use $U_{F_{mn}}$ to mark this case, shown in Formula 1.

$$U_{F_{mn}} = \begin{cases} 1, & S_{F_{mn}} + P_{F_{mn}} > D_{F_{mn}} \\ 0, & S_{F_{mn}} + P_{F_{mn}} \leq D_{F_{mn}} \end{cases} \quad (1)$$

We use the notation $F_{mn}(t)$ to designate whether a file is currently in transmission at time t . When $F_{mn}(t) = 1$ the file is in transmission, when $F_{mn}(t) = 0$ it is not. This is shown formally in Formula 2.

$$F_{mn}(t) = \begin{cases} 1, & S_{F_{mn}} \leq t \leq \min\{S_{F_{mn}} + P_{F_{mn}}, D_{F_{mn}}\} \\ 0, & \text{other} \end{cases} \quad (2)$$

We define the neighbors within range of node V_i at time t as $N_i(t)$.

$$N_i(t) = \{V_m | m \in (1, \dots, Q) \text{ and } R_{F_{im}} \leq t \leq D_{F_{im}}\} \quad (3)$$

The schedule problem is defined as follows. Given a set of start times $S = \{S_{F_{mn}} | F_{mn} \in F\}$ and $|S| = |F|$, the following conditions should be satisfied.

1. For $\forall F_{mn} \in F$, then $R_{F_{mn}} \leq S_{F_{mn}}$, this means every file should start to be sent after it has been generated.
2. For $\forall V_i \in V$ and $\forall t \in (0, +\infty)$, then $\sum_{m=1}^Q F_{mi}(t) + \sum_{n=1}^Q F_{in}(t) \leq 1$, this means any node in the network can only be in one status (sending, receiving or idle).
3. For $\forall F_{mn} \in F$ and $\forall t \in (0, +\infty)$,
if $F_{mn}(t) = 1$, then the following results hold:
 - (a) for $\forall V_i \in (N_m(t) - V_n)$, $\sum_{p=1}^Q F_{pi}(t) = 0$
 - (b) for $\forall V_i \in (N_n(t) - V_m)$, $\sum_{p=1}^Q F_{ip}(t) = 0$,

this means if node V_m is sending files to V_n , the neighbors of V_m except V_n cannot be in receiving status and the neighbors of V_n except V_m cannot be in sending status to avoid channel collision.

For any start time set S we can calculate the number of unsuccessful transmissions $NU = \sum_{F_{mn} \in F} U_{F_{mn}}$. Therefore, our problem is to find a proper start time set S , that minimizes NU .

4 Scheduling Algorithm

In this section, we first prove that the scheduling problem for each node is NP-complete. Then we use a greedy approach to design two centralized algorithms.

4.1 Proof

Problem Context: Consider each node individually. At any time instance, there are k files (indexed as $1, 2, \dots, k$) in the node's transferring queue, each file i has a release time r_i , a due time d_i , and a transmission processing time p_i . Each node computes a transmission schedule to minimize the number of unsuccessful transmissions, defined as Θ . To frame this as a decision problem, we ask if there is a solution with the number Θ no more than δ . We abbreviate this problem as MFTS, Minimum Failure Transmission Scheduling.

Theorem 1. *MFTS problem is NP-complete.*

Proof. First, we prove that the MFTS problem is in the NP class. We can choose a permutation of the n files and computer the file completion time to check whether this permutation can satisfy the threshold δ . This testing phase can be finished in the Polynomial time and thus the MFTS problem is a member of NP class.

Next, we prove that the MFTS problem is NP-hard by reducing the subset sum problem to our problem. The subset sum problem is that, given a set of positive integers $\{a_1, a_2, \dots, a_t\}$ and an integer x , (here $A = \sum_{i \in T=\{1, 2, \dots, t\}} a_i$ and $x < A$), whether there exists a subset $S \subset T$ such that $\sum_{i \in S} a_i = x$ [7].

Here we reduce the subset sum problem to our problem. Construct a MFTS problem with file number $k = t + 1$. For each file $i (i \in T)$, $r_i = 0$, $p_i = a_i$ and $d_i = A + 1$. For file k , $r_k = b$, $p_k = 1$ and $d_k = x + 1$. Set $\delta = 0$. For each answer S to subset sum problem, $\sum_{i \in S} a_i = x$. This answer can be used as an input for MFTS problem and we can get $\Theta = 0$. Therefore, the unsuccessful transmission $\Theta \leq \delta$. For each answer S to MFTS problem, $\Theta = \delta = 0$, thus $\sum_{i \in S} p_i = x$. Obviously, S is a correct answer to the subset sum problem that $\sum_{i \in S} a_i = x$ holds.

Therefore, the MFTS problem is NP-hard. Since the MFTS problem is both in NP class and is NP-hard, it is NP-Complete.

4.2 Transmission Time Based Centralized Algorithm

This section presents our first algorithm based on transmission time and is shown in Algorithm 1. This algorithm inputs files from the whole network centrally. All the global information is shared by every node and all the transmissions are scheduled globally. Every node maintains its own file queue at any time t . For each file, the node will compute whether the file can be transmitted before the due time and if not, marks the file as cancelled. These steps are shown in Algorithm 1 from line 1 to line 8.

Next, we use a greedy approach to interleave each node's queue into one centralized list. Every node appends its files to a public list S . Then the list is reordered in the ascending order of the transmission time of each file in S . Smaller files will be sent earlier. Larger files should be delayed, even when they come into the node's queue earlier. Since small files have shorter processing times, more files will be completed. This part is shown in Algorithm 1 from line 9 to 11.

If two files in S have the same transmission time, they are reordered by ascending due times. This is shown in Algorithm 1 from line 12 to line 16.

This algorithm will optimize for the highest number of successful file transmissions in S and obeys the rules defined in Section 3.

Algorithm 1. Transmission Time Based Centralized Algorithm

Input:

Files in the queue of each node V_m : $F_m = \{F_{mn} | n \in (1, \dots, Q) \text{ and } m \neq n\}$

Properties for each file F_{mn} : $P = \{P_{F_{mn}}\}, D = \{D_{F_{mn}}\}$

Current time t

Output:

File sending sequence: $S = [S_0, S_1, \dots, S_i, \dots] (S_i = F_{mn})$

```

1: for node  $V_i$  from  $V_1$  to  $V_Q$  do
2:   for File  $F_{in}$  in  $F_i$  do
3:     If  $t + P_{F_{in}} > D_{F_{in}}$  then
4:        $F_i = F_i - F_{in}$ 
5:     end if
6:   end for
7:    $S = S + F_i$ 
8: end for
9: for node  $V_i$  from  $V_1$  to  $V_Q$  do
10:   Insert  $F_{im} \in F_i$  to  $S$  in ascending order of  $P$ ,  $P = \{P_{F_{in}} | F_{in} \in S\}$ 
11: end for
12: for  $\forall F_{ab}, \forall F_{pq}$  in  $S$  do
13:   if  $P_{F_{ab}} = P_{F_{pq}}$  then
14:     Sort  $F_{ab}$  and  $F_{pq}$  in ascending order according to  $D_{F_{ab}}$  and  $D_{F_{pq}}$ 
15:   end if
16: end for

```

4.3 Due Time Based Centralized Algorithm

The first part of this algorithm is similar to the one above. The files that cannot be successfully transmitted are canceled from each node's queue. This is shown in Algorithm 2.

The second step is different. The files are sorted in the ascending order of the due time of each file in list S . In this design each node will transmit files first on the links which will be interrupted the soonest. This will result in more files transmitted before their due times.

If two files in have the same due time, they are reordered by their ascending transmission times, as shown in Algorithm 2 from line 12 to line 16.

Algorithm 2. Due Time Based Centralized Algorithm

Input:

Files in the queue of each node V_m : $F_m = \{F_{mn} | n \in (1, \dots, Q) \text{ and } m \neq n\}$
Properties for each file F_{mn} : $P = \{P_{F_{mn}}\}, D = \{D_{F_{mn}}\}$
Current time t

Output:

File sending sequence: $S = [S_0, S_1, \dots, S_i, \dots] (S_i = F_{mn})$

```

1:   for node  $V_i$  from  $V_1$  to  $V_Q$  do
2:     for File  $F_{in}$  in  $F_i$  do
3:       If  $t + P_{F_{in}} > D_{F_{in}}$  then
4:          $F_i = F_i - F_{in}$ 
5:       end if
6:     end for
7:      $S = S + F_i$ 
8:   end for
9:   for node  $V_i$  from  $V_1$  to  $V_Q$  do
10:    Insert  $F_{im} \in F_i$  to  $S$  in ascending order of  $D$ ,  $D = \{D_{F_{in}} | F_{in} \in S\}$ 
11:   end for
12:   for  $\forall F_{ab}, \forall F_{pq}$  in  $S$  do
13:     if  $D_{F_{ab}} = D_{F_{pq}}$  then
14:       Sort  $F_{ab}$  and  $F_{pq}$  in ascending order according to  $P_{F_{ab}}$  and  $P_{F_{pq}}$ 
15:     end if
16:   end for

```

4.4 Further Details

This section provides further details on how the due time and transmission processing time are computed.

File Due Time. Reference [6] and [13] have shown that, the link duration time can be estimated according to the vehicle velocity, the map, the driving direction, and the traffic light period. So it is possible to calculate for each node. As this is not the kernel part in our scheduling problem of this paper, we make the assumption that the link duration time is known beforehand. Therefore, the due time can also be got from the link duration time.

File Transmission Processing Time. Intuitively, the file transmitting time can be calculated from the file size divided by the transmission rate. However, in practice the transmission rate is always changing according to the DSRC standard, shown in Table 1. The physical layer operations of vehicular ad-hoc networks are specified in DSRC standard, which adopts OFDM mechanism and works with four modulation schemes(BPSK, QPSK, 16-QAM and 64-QAM) and three coding rate ($1/2$, $2/3$ and $3/4$). With the channel environment changing, such as Signal Noise Ratio(SNR), nodes choose a proper modulation scheme and a coding rate which lead to a proper data transmission rate. In this paper, we choose the same way to calculate the data rate as [5] [8]. Then the transmission time is always changing with the data transmission rate.

Table 1. DSRC Data Transmission Rate and SNR Threshold

SNR Threshold (dB)	5	6	8	11	15	20	25	N/A
DataRate(Mbps)	3	4.5	6	9	12	18	24	27

5 Simulations

5.1 Simulation Setup

This section presents our simulation scenario, including network topology, file generator and communication details.

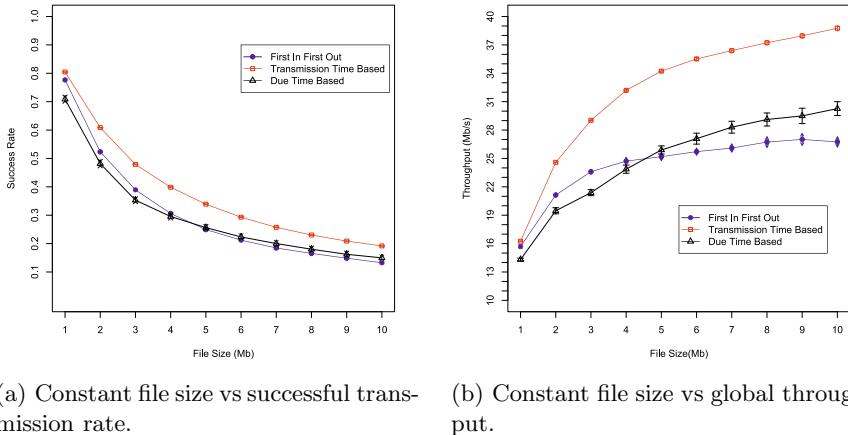
Network Topology. We choose a data set from Cologne, Germany, a typical middle-sized European city. All the node traces are generated from SUMO using Cologne street maps, as shown in [11]. We randomly choose a square space with dimensions $1000\text{m} \times 1000\text{m}$ for 2 minutes. In this square space, there are 123 nodes. We run 100 iterations then compute the average success rate and the throughput.

File Generator. When two nodes come within range of each other, they each generate a file. The file is transmitted at the start time designated in the centralized queue. We analyzed two different size distributions: First, we run the simulation ten times, in each run the files have the same size (from 1Mb to 10Mb). In the second, we distributed the files in a Pareto distribution with a mean file size of 5Mb. In [4] [12], statistical analysis of network flows shows that file sizes follow the Pareto distribution. The Pareto shape parameters range from 1.2 to 2.1. The higher shape parameter models cases where files are more concentrated around the mean file size (smaller variance). The lower shape parameter models cases with larger variances.

Communication Details. We use the methodology from [8] to calculate vehicle data rates. We use the same parameters, but different communication ranges (100m, 150m, 200m, 250m and 300m). The same functions and parameters are used to compute the data transmission rates for any communication range. We compare our scheduling algorithms to the FIFO mechanism as defined in DSRC.

5.2 Simulation Result

In Figure 1, with the file size increasing, the rates of successful transmission for all the three algorithms are decreasing. Since the time window that two vehicles are located in each other's vicinity is very limited, large files may not be transmitted. Although the success rates decline, the network throughputs increase mainly due to larger file sizes. But the transmission time based algorithm performs better than the others, considering both the success rate and the throughput. Therefore, sending files with smaller transmission time first leads more files to be sent successfully which also results in a larger throughput. The due time based algorithm performs worse than DSRC while the file size is less than 5Mb. Although all files have the same size, their transmission durations may be large due to the channel fading and the distance between the source vehicle and the destination vehicle. For small files, the due time based algorithm may start to transmit them while they are far away or going to be out of the communication range. In this case, the transmission may cost more time and prevent other files of short transmission time to be sent. When the files become larger, the due time based algorithm performs better. The FIFO mechanism may suffer from link interruptions, while transmitting files, more seriously than the due time based algorithm.

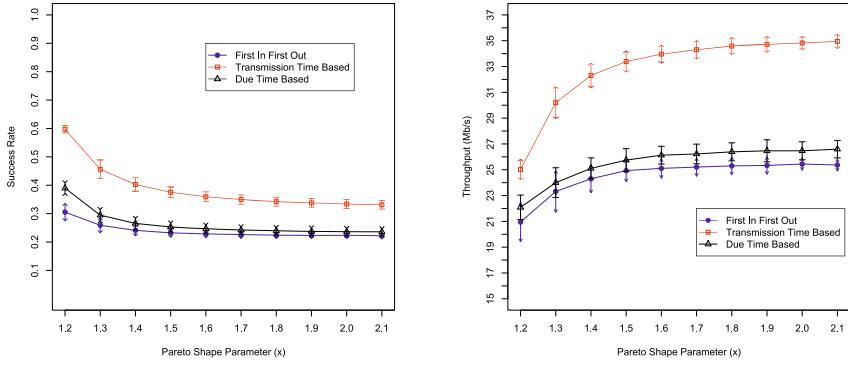


(a) Constant file size vs successful transmission rate.

(b) Constant file size vs global throughput.

Fig. 1. Constant File Size

Figure 2 indicates that, when the file size follows the Pareto distribution, with the shape parameter increasing, the success rates of all the algorithms decline and their throughputs increase. A smaller shape parameter leads to a larger variance, which means there are many smaller files and many larger files coexisting in the network. Then the transmission time based algorithm will transmit more files than the other two algorithms and most of the successfully transmitted files are small files. The due time based algorithm in this scenario always performs better



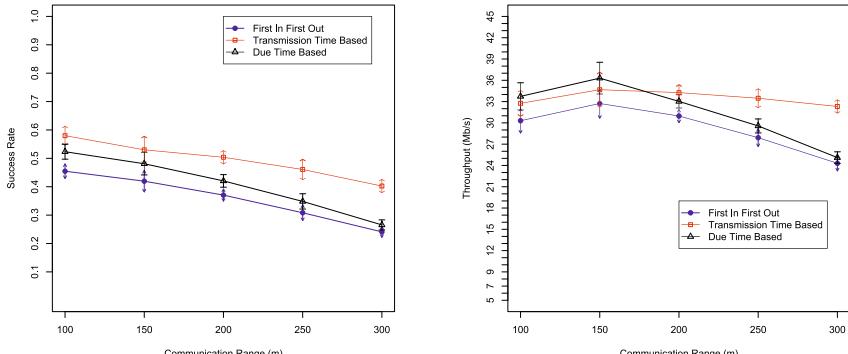
(a) Pareto distribution file size vs successful transmission rate.

(b) Pareto distribution file size vs global throughput.

Fig. 2. Pareto Distribution File Size

than FIFO, in terms of the success rate and the throughput. In this scenario, the due time based algorithm can transfer more files than FIFO, before links break down. Larger files that are hard to be transmitted successfully in FIFO mechanism can also be transmitted in due time based algorithm.

Figure 3 describes the effect of transmission range on the success rate and the throughput. It is shown that a larger communication range leads to a declined success rate. Under a larger communication range, each node may have more neighbors. More files are generated to be sent in our scenario, however, few of them can be successfully transmitted. But the network throughput indicates a



(a) Communication range vs successful transmission rate.

(b) Communication range vs global throughput.

Fig. 3. Different Communication Range

special trend. When the communication range is smaller than 200m, from the mean values and the standard deviations, all the algorithms are almost the same, because their error bars show several overrides. Under a smaller communication range, each node has less neighbors, therefore, less files are to be transmitted. Besides that, these files contain larger files, that cannot be finished, so most of the files left would be transferred, no matter whether they are scheduled. But for larger communication range, more files need to be scheduled, so the contention is more serious and the throughputs of them fall down.

6 Conclusion

Vulnerable links in VANETs are significantly affected by vehicle moving, channel collision, and channel fading. Whether a file can be transferred entirely is dependent on the link duration and the transmission time. Our work investigates how to make more files to be transmitted successfully when many files of different sizes are observed in a node's sending queue. This schedule problem is proved to be an NP-Complete problem and two scheduling algorithms are proposed to provide a upper bound of performance. In the future, according to the upper bound of the network, distributed algorithms are encouraged to be designed, which can be utilized in practice vehicular ad-hoc network. This paper doesn't consider the fairness of the scheduling algorithms, which should be considered as a metric in the future work.

Acknowledgments. This work is supported by Projects of Major International (Regional) Joint Research Program NSFC(No.61120106010), Natural Science Foundation of China (No.61272509), Beijing Natural Science Foundation (No. 4132049), National Natural Science Foundation of China under grant No.61003304, China Scholarship Council under grant 201206115013, and China Scholarship Council under grant 201206030047.

References

1. IEEE standard for information technology— local and metropolitan area networks— specific requirements— part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), pp. 1–51 (2010)
2. Bai, F., Stancil, D.D., Krishnan, H.: Toward understanding characteristics of dedicated short range communications (dsrc) from a perspective of vehicular network engineers. In: Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking, pp. 329–340. ACM (2010)
3. Briand, C., Ourari, S.: Minimizing the number of tardy jobs for the single machine scheduling problem: Mip-based lower and upper bounds. RAIRO-Operations Research 47(01), 33–46 (2013)

4. Castro, E., Fonseca, I.E., Kumar, A., Alencar, M.S.: A packet distribution traffic model for computer networks. In: The International Telecommunications Symposium, ITS (2010)
5. Cheng, L., Henty, B.E., Stancil, D.D., Bai, F., Mudalige, P.: Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band. IEEE Journal on Selected Areas in Communications 25(8), 1501–1516 (2007)
6. Hu, M., Zhong, Z., Zhu, H., Ni, M., Chang, C.Y.: Analytical modeling of link duration for vehicular ad hoc networks in urban environment. In: Proceeding of the Tenth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications. pp. 61–70. ACM (2013)
7. Lenstra, J.K., Rinnooy Kan, A., Brucker, P.: Complexity of machine scheduling problems. Annals of Discrete Mathematics 1, 343–362 (1977)
8. Luan, T.H., Sherman Shen, X., Bai, F.: Integrity-oriented content transmission in highway vehicular ad hoc networks. In: 2013 Proceedings IEEE INFOCOM, pp. 2562–2570. IEEE (2013)
9. Michael, R.G., Johnson, D.S.: Computers and intractability: A guide to the theory of np-completeness. WH Freeman & Co., San Francisco (1979)
10. Moore, J.M.: An n job, one machine sequencing algorithm for minimizing the number of late jobs. Management Science 15(1), 102–109 (1968)
11. Naboulsi, D., Fiore, M.: On the instantaneous topology of a large-scale urban vehicular network: the cologne case. In: Proceedings of the Fourteenth ACM International Symposium on Mobile Ad hoc Networking and Computing. pp. 167–176. ACM (2013)
12. Pustisek, M., Humar, I., Bester, J.: Empirical analysis and modeling of peer-to-peer traffic flows. In: The 14th IEEE Mediterranean Electrotechnical Conference, MELECON 2008, pp. 169–175. IEEE (2008)
13. Viriyasitavat, W., Bai, F., Tonguz, O.K.: Dynamics of network connectivity in urban vehicular networks. IEEE Journal on Selected Areas in Communications 29(3), 515–533 (2011)
14. Zhang, Y., Cao, G.: V-pada: Vehicle-platoon-aware data access in vanets. IEEE Transactions on Vehicular Technology 60(5), 2326–2339 (2011)

Joint Neighbor Discovery and Contention Relationship Inference in Wireless Networks

Guanbo Zheng¹ and Rong Zheng²

¹ Department of Electrical and Computer Engineering, University of Houston, USA

² Department of Computing and Software, McMaster University, Canada

Abstract. In this paper, we investigate the problem of joint neighbor discovery and contention relationship inference in wireless networks with multiple broadcast domains. In contrast to existing work, we represent neighboring relationship as ternaries $\{1, 0, \delta\}$ based on the strength of the received signal. An active ternary inference algorithm is proposed that utilizes decentralized randomized schedules to infer neighboring and contention relationships through *mixed signal* at the receiver nodes. Simulation studies show that the proposed algorithm outperforms an Aloha-like algorithm in neighbor discovery time, and can achieve high accuracy in determining the relationship.

1 Introduction

Neighbor discovery and contention relationship inference are two corner stones of operating and managing wireless networks. Neighbor discovery identifies communicating peers in proximity, while contention relationship characterizes whether multiple transceiver pairs can transmit concurrently without severely degrading the respective packet delivery. For static networks, the two procedures are typically carried out in the bootstrapping phase. In semi-stationary networks, periodical discovery is needed. In both cases, fast and accurate neighbor discovery and contention relationship inference are instrumental in many resource management decisions such as channel and spectrum allocation, power control, routing and scheduling.

Given the importance of the two problems in wireless networks, unsurprisingly, there exists vast literature addressing them. Existing approaches can be classified utilizing multiple criterion, namely, passive vs. active, deterministic vs. randomized, and whether information from multiple transmissions is incorporated. Passive approaches rely on opportunistic listening to learn about a node's neighbors, or relative timing between transmitting frames to infer contention relationship [1–4]. While passive approaches do not introduce additional signalling or messages in the network, due to their opportunistic nature, the inference process tends to be lengthy. Among approaches that utilize active transmissions or probes, one central question is when and which sets of nodes will be transmitting and receiving. Active approaches using a deterministic schedule [5–7] typically require a central coordinator and nodes take turns in transmission. In contrast, in

randomized approaches [8–11], nodes follow decentralized randomized schedules. Another distinction among existing work is the treatment of multiple concurrent transmissions. Randomized neighbor discovery protocols [8,9,12,13] that assume single packet reception at the receiver, aim to devise a good schedule that trades off collision probabilities and total discovery time – essentially a channel access problem. Multiple packet reception in neighbor discovery has been considered in [10, 11] where at most K concurrent transmissions can be decoded. A fundamentally different approach that departs from the assumption of single packet reception in neighbor discovery is proposed by Luo and Guo, which uses binary group testing [14–16]. In [14–16], neighboring relations are associated with binary variables. Binary observations at receivers are then modeled as OR mixtures as the result of the transmission schedule and the neighbor relations.

In this work, we investigate joint neighbor discovery and contention relationship inference, whilst most existing work focuses on one of the two problems. We propose an *active* algorithm, called *the ternary inference algorithm*, that utilizes *decentralized randomized* schedules to infer the neighboring and contention relationships through *mixed signal* at the receiver nodes. In contrast to [14, 16], we represent neighboring relationship as ternaries $\{1, 0, \delta\}$ based on the strength of the received signal. A procedure akin to group testing is devised to infer the neighbor and contention relationship. A t -tolerance variant is further introduced to improve the robustness to observation errors. We analyze the sources of errors in both schemes, and evaluate the impact of network size, and other parameter settings. The simulation results demonstrate the superior performance of the proposed algorithm in terms of completion rate and accuracy.

The rest of this paper is organized as follows. The key notations and network models are presented in Section 2. In Section 3, we present the ternary inference algorithm. Simulation study is given in Section 4 followed by conclusion and future work in Section 5.

2 Network Model and Problem Statement

2.1 Network Model

We consider a multihop wireless network consisting of N nodes. During the phase of neighbor discovery and contention relationship inference, time is divided into equal-length slots. The slot boundary is assumed to be synchronized. Each node follows a randomized on-off schedule alternating between transmitting and receiving modes. The randomized schedule is calculated using a pseudo random generator seeded by the node's ID (assumed to be unique) and a parameter q common to all nodes.

Let the length of the discovery phase to be L . The activity of a node n at time t is denoted by $s_n(t)$, $n \in \{1, \dots, N\}$, $t \in \{1, \dots, L\}$, where

$$s_n(t) = \begin{cases} 1, & \text{transmitting mode} \\ 0, & \text{receiving mode} \end{cases}, \quad (1)$$

and the node's activity follows the i.i.d Bernoulli distribution with $P(s_n(t) = 1) = 1 - P(s_n(t) = 0) = q, \forall n, t$.

The set of transmitting nodes at time t , denoted by $T(t)$, can be written as: $T(t) = \{n : s_n(t) = 1, n \in \{1, \dots, N\}\}$; Similarly, the set of the receiving nodes at time t is written as $R(t) = \{n : s_n(t) = 0, n \in \{1, \dots, N\}\}$. At time t , the collection of $s_n(t), \forall n$ is called a test, denoted by $s(t)$.

The observation of a receiver node n at time t is denoted by $y_n(t)$. We assume the following *ternary model* where $y_n(t)$ takes values in $\{0, 1, \delta\}$:

$$y_n(t) = \begin{cases} 1, & \text{signal decodable} \\ \delta, & \text{signal observed but undecodable} \\ 0, & \text{no signal observed} \end{cases} \quad (2)$$

Additionally, depending on whether the received signal is decodable, $z_n(t)$ gives the set of IDs decoded.

The neighbor relationship between any two nodes n and m , $n, m \in \{1, \dots, N\}$, denoted by $x(n, m)$, is given by,

$$x(n, m) = \begin{cases} 1, & m \text{ is a neighbor of } n \\ \delta, & n \text{ can sense the carrier from } m \\ 0, & m \text{ is not a neighbor of } n \end{cases} \quad (3)$$

Note that $x(n, m)$ is not necessary the same as $x(m, n)$, namely, we can account for asymmetric relationships. The determination of $x(n, m)$ depends on the received signal quality at node n from m , in terms of the signal-to-noise (SNR) ratio. We employ two thresholds Γ_1 and Γ_2 corresponding to the decoding threshold and carrier sensing threshold, respectively. When the SNR is above Γ_1 , the transmitted signal can be successfully decoded, while the transmitted signal can be detected but not decoded if the SNR is between Γ_1 and Γ_2 .

The link contention relationship is denoted by $c(n, m; k)$, $n, m, k \in \{1, \dots, N\}$, namely, whether transmitter k interferes with link $m \rightarrow n$,

$$c(n, m; k) = \begin{cases} 1, & m \rightarrow n \text{ is interfered by } k \\ 0, & m \rightarrow n \text{ is not interfered by } k \end{cases} . \quad (4)$$

In other words, $c(n, m; k) = 1$ if the packet transmission from node m cannot be successfully decoded if node k transmits concurrently. The key notations used in this paper are summarized in Table. 1.

2.2 Problem Statement

The objective of neighbor discovery and contention relation inference is to determine $x(m, n)$ and $c(n, m; k)$ given $y_n(t), t = 1, 2, \dots, L, n = 1, 2, \dots, N$ using as few number of tests L as possible. Note that L is not fixed a prior. Additional tests will be conducted if the percentage of inferred values or the confidence is below a certain threshold.

Table 1. Notations

L	the number of tests
N	the number of nodes in the network
t	the t -th time slot, where $t \in \{1, \dots, L\}$
n, m, k	the $n/m/k$ -th node, where $n, m, k \in \{1, \dots, N\}$
$s_n(t)$	the activity of node n at time i
\mathcal{S}	$\{s_n(t) n \in \mathcal{N}, t = 1, 2, \dots, L\}$
$T(t)$	the set of transmitting nodes at time t
$R(t)$	the set of receiving nodes at time t
\mathcal{T}	$\{T(t) t = 1, 2, \dots, L\}$
\mathcal{R}	$\{R(t) t = 1, 2, \dots, L\}$
$y_n(t)$	the observation at node n at time t
\mathcal{Y}	$\{y_n(t) n \in \mathcal{N}, t = 1, 2, \dots, L\}$
$z_n(t)$	the IDs decoded at node n at time t
\mathcal{Z}	$\{z_n(t) n \in \mathcal{N}, t = 1, 2, \dots, L\}$
$T(t), R(t)$	The set of transmitting and receiver nodes in time t
$x(n, m)$	the neighbor relationship if m is a neighbor of n
\mathcal{X}	$\{x(n, m) n, m \in \mathcal{N}\}$
$c(n, m; k)$	the link contention relationship if $m \rightarrow n$ is contended by transmitter k
$O(n, m; k)$	the outcome of $m \rightarrow n$ interfered by transmitter k
Γ_1	decoding threshold
Γ_2	carrier sensing threshold

3 Ternary Inference Model and Algorithm

In this section, we first introduce the observation model and then present the ternary inference approach.

3.1 Modeling the Observations

We define the ternary operators \wedge and \vee that are analogous to logical AND and OR for binary variables.

Table 2. The Ternary Operators AND and OR

(a) Ternary AND \wedge				(b) Ternary OR \vee			
	1	0	δ		1	0	δ
1	1	0	δ	1	1	1	1
0	0	0	0	0	1	0	δ
δ	δ	0	δ	δ	1	δ	δ

Since the observations $y_n(t)$ is the mixture of signal from all transmitters in $T(t)$, we need to first derive the observation as the result of two concurrent transmitters. Let $O(n, m; k)$ be the observation on node n with respect to m when both m and k are transmitting. It is easy to show that $O(n, m; k)$ satisfies Table 3.

Table 3. The observation on link $m \rightarrow n$ due to transmitters m, k

Cases	$x(n, m)$	$x(n, k)$	$c(n, m; k)$	$O(n, m; k)$	ID(n,m;k)
1	1	1	1	δ	\emptyset
2	1	1	0	1	{m}
3	1	δ	1	δ	\emptyset
4	1	δ	0	1	{m}
5	1	0	0	1	{m}
6	δ	1	1	δ	\emptyset
7	δ	1	0	δ	\emptyset
8	δ	δ	1	δ	\emptyset
9	δ	δ	0	δ	\emptyset
10	δ	0	0	δ	\emptyset
11	0	1	1	0	\emptyset
12	0	1	0	0	\emptyset
12	0	δ	1	0	\emptyset
14	0	δ	0	0	\emptyset
15	0	0	0	0	\emptyset

For example, when $x(n, m) = 1$, $c(n, m; k) = 1$, $O(n, m; k) = \delta$ as the transmission from m cannot be decoded by n due to the interference from k in Case 1 and 3. On the other hand, $x(n, m) = 1$, $x(n, k) = 1$, $c(n, m; k) = 0$, $O(n, m; k) = 1$ implies successive cancelation is possible to decode the transmission from m (as indicated in the ID field).

With $O(n, m; k), \forall m, k \in T(t)$, we can now compute $y_n(t)$ as,

$$y_n(t) = \bigvee_{m \in T(t)} \left(\bigwedge_{k \in T(t), k \neq m} O(n, m; k) \right). \quad (5)$$

The inner \bigwedge operations give the observation with respect to transmitter m on n from all other nodes in $T(t)$ as potential interferers. The outer \bigvee is due to the fact that by definition a successful transmission from any transmitter will result in decodable packets at the receiver. The set of decoded IDs at node n is given by,

$$z_n(t) = \bigcup_{m \in T(t)} \left(\bigcap_{k \in T(t), k \neq m} ID(n, m; k) \right). \quad (6)$$

Consider the example of $T(t) = \{m, k\}$. Clearly, we have

$$y_n(t) = O(n, m; k) \vee O(n, k; m), \quad (7)$$

and

$$z_n(t) = ID(n, m; k) \cup ID(n, k; m). \quad (8)$$

3.2 Inference Algorithm

Given the collection of tests \mathcal{S} and the observations \mathcal{Y}, \mathcal{Z} , the proposed inference algorithm proceeds in two steps: First, it performs neighbor discovery to obtain \mathcal{X} using \mathcal{Y} and \mathcal{S} . Next, it resolves the contention relationship \mathcal{C} from $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ and \mathcal{S} .

Algorithm 1. Ternary Neighbor Discovery

Input : Node Activity \mathcal{S} , Observation \mathcal{Y} , Sets of TX and RX nodes \mathcal{T} and \mathcal{R}
Output: Neighbor Relationship \mathcal{X}

```

1 begin
2   Set  $flag = 1$ ;
3   while  $flag = 1$  do
4     for  $t = 1$  to  $L$  do
5       if  $y_n(t) = 0, n \in R(t)$  then
6         |  $x(n, m) \leftarrow 0, \forall m \in T(t)$ ;
7       end
8       if  $y_n(t) = \delta$  and  $|T(t)| = 1, n \in R(t)$  then
9         |  $x(n, m) \leftarrow \delta, \forall m \in T(t)$ ;
10      end
11      if  $y_n(t) = 1, TX ID m decoded, n \in R(t)$  then
12        |  $x(n, m) \leftarrow 1$ ;
13      end
14      if  $y_n(t) > 0$  and  $|T(t)| \geq 2, n \in R(t)$  then
15        if exist  $x(n, m) < y_n(t), m \in T(t)$  then
16          | remove  $m$  from  $T(t)$ ;
17          if  $|T(t)| = 1$  then
18            |  $flag \leftarrow 1$ , Break;
19          else
20            |  $flag \leftarrow 0$ .
21          end
22        end
23      end
24    end
25  end
26 end

```

Neighbor Discovery. The neighbor discovery algorithm is presented in Algorithm 1. For every test $t = \{1, \dots, L\}$, we evaluate the observation $y(t)$ on all the receiver nodes in $R(t)$. If the observation at a receiver n is zero, all the concurrent transmitter nodes are flagged non-neighbor to n . In the case of multiple concurrent active transmitters, the observation may be a mixture, which can be resolved if we know the neighbor relationship of a subset of transmitter nodes in the mixture. Algorithm 1 iterates through all tests and every pair of nodes until either no further improvement can be made or all entries in \mathcal{X} have been resolved.

t-tolerance neighbor discovery To increase the robustness of neighbor discovery in presence of measurement errors, we introduce a *t*-tolerance algorithm. The basic idea is that each inferred relationship needs to be *independently* verified by *TOL* tests. The tolerance factor *TOL* tradeoffs reliability and the total number of tests to complete neighbor discovery. Due to space limits, we omit the pseudo code of the algorithm.

Algorithm 2. Contention Relationship Inference

Input : Node Activity \mathcal{S} , Observations \mathcal{Y} and \mathcal{Z} , Neighbor Relationship \mathcal{X} ,
Sets of TX and RX nodes \mathcal{T} and \mathcal{R}

Output: Contention relationship \mathcal{C}

```

1 begin
2   Set flag = 1;
3   while flag = 1 do
4     for t = 1 to L do
5       if  $y_n(t) = 0, n \in R(t)$  then
6         |  $c(n, m; k) \leftarrow 0, c(n, k; m) \leftarrow 0, \forall m, k \in T(t);$ 
7       end
8       if  $y_n(t) = 1, n \in R(t)$  then
9         |  $c(n, m; k) \leftarrow 0, \forall m \in z_n(t), k \neq m \in T(t);$ 
10      end
11      if  $y_n(t) = \delta, n \in R(t)$  then
12        if  $|T(t)| = 2$  then
13          | Find  $c(n, m; k)$  and  $c(n, k; m)$  using  $x(n, m)$ ,  $x(n, k)$  and
14            |  $y_n(t), \forall m, k \in T(t)$ , using (7), (8) and Table 3;
15        else
16          | Find  $O(n, m, k)$  and  $O(n, k, m)$  using available
17            |  $x(n, m), x(n, k), c(n, m; k), c(n, k; m), \forall m, k \in T(t)$  and
18            | Table 3;
19          if  $O(n, m, k) = 0$  then
20            | remove m from  $T(t)$ ;
21          else if  $O(n, k, m) = 0$  then
22            | remove k from  $T(t)$ ;
23          end
24          if exist  $|T(t)| = 2$  then
25            | flag  $\leftarrow 1$ , Break;
26          else
27            | flag  $\leftarrow 0$ .
28          end
29        end
30      end

```

Contention Relationship Inference. We observe that if $x(n, m) \in \{\delta, 0\}$, the knowledge of $c(n, m, k)$ has little utility since we cannot decode the data from m to n even in absence of any other transmitters. Thus, we limit the inference to links that can support successful direct communication. From Table 3, it is easy to see that when $x(n, m) = 1$ (the shaded rows), if $O(n, m; k)$ is known, $c(n, m; k)$ can be uniquely determined. In fact, $c(n, m; k) = 0$ if $O(n, m; k) = \delta$, and $c(n, m; k) = 0$ if $O(n, m; k) = 1$. Therefore, it suffices to infer $O(n, m; k)$ for $n, m, k \in \mathcal{N}$ from $y_n(t), z_n(t), \forall n \in T(t), t = 1, 2, \dots, L$.

From (5) and (6), we note that if $m \in z_n(t)$, $\bigwedge_{k \in T(t), k \neq m} O(n, m; k) = 1$, which implies that $O(n, m; k) = 1, \forall k \in T(t), k \neq m$. In other words, a decodable message yields the contention relationship of many links. On the other hand, if $m \notin z_n(t)$, $\bigwedge_{k \in T(t), k \neq m} O(n, m; k) = 0$. The mixture can only be solved when we have sufficient number of known $O(n, m; k)$'s.

In Algorithm 2, when there are only two concurrent transmitter nodes in a test, the contention relationship can be computed directly as evident from (7) and (8). In the case of multiple concurrent transmitters, $O(n, m; k)$ will be inferred recursively. Finally, from $O(n, m; k)$ and Table 3 we can determine $c(n, m; k)$.

3.3 Analysis of Errors

The ternary interference model makes assumptions regarding the superposition of signals at a receiver. In particular, multiple strong signals always add up to an even stronger signal; while the aggregates of multiple weak signals remain to be weak. In practice, these assumptions may not hold. Consider a quantized linear superposition model satisfying

$$\tilde{y}_n(t) = \begin{cases} 1, & \sum_{m \in T(t)} h_{mn} \tilde{x}_m(t) \geq \Gamma_1 \\ \delta, & \Gamma_2 \leq \sum_{m \in T(t)} h_{mn} \tilde{x}_m(t) < \Gamma_1 \\ 0, & \sum_{m \in T(t)} h_{mn} \tilde{x}_m(t) < \Gamma_2 \end{cases}, \quad (9)$$

where $\tilde{y}_n(t)$, $\tilde{x}_m(t)$, h_{mn} are respectively, the aggregated received signal at n , the transmitted signal from node m , and the channel gain from m to n (including antenna gains).

Two types of observation errors in the ternary model are possible: If the linear superposition model gives the observation 0 (or δ), while our ternary model observed δ (or 1), it is called a *false positive error*. This may occur when multiple strong signals cancels out. On the other hand, if the linear superposition model decides δ (or 1) but our ternary model decides 0 (or δ), it is called a *false negative error*. This may occur when multiple weak signals aggregate. The two sources of errors may lead to misidentification of the neighboring and contention relationships.

To see the impact of parameter Γ_1 and Γ_2 on two sources of errors, we conduct simulations by putting N nodes in a 2-D plane with the following parameters:

The parameters are chosen in consistent with the IEEE 802.15.4 transceivers. In the experiments, scheduled transmitters send a ‘1’ bit modulated using BPSK

Table 4. Simulation setup

PHY parameters	Values
Path Loss	3
Center Freq	2.4 GHz
Transmit power	1mW
Noise floor	-102dBm
Channel model	AWGN
Active probability q	0.2
Node density	1000/ Km^2

and carrier frequency 2.4GHz. The received signal is subjected to propagation delay between the transmitters and receivers.

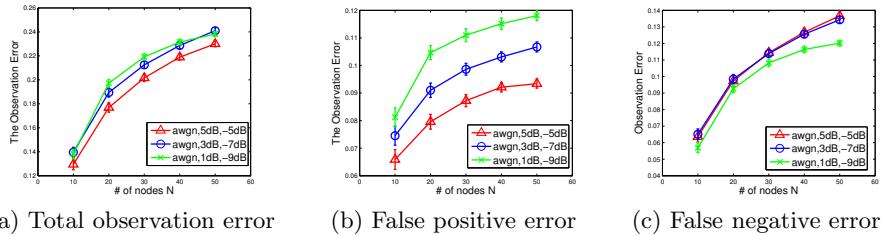


Fig. 1. Observation error rate of the ternary model with respect to the linear superposition model with $L = 200$, and 95% confidence.

Figure 1 shows the observation errors of the ternary model with respect to the linear superposition model. A total of $L = 200$ random tests are conducted. The observation errors are computed as the discrepancy ratio in the observations between the two models. From Figure 1, we observe that the false positive and negative errors are comparable both increasing with more number of nodes in the network. Increasing the thresholds Γ_1 and Γ_2 reduces the false positive errors, and increases the percentage of false negative errors as expected.

4 Performance Evaluation

In this section, we evaluate the performance of the ternary inference approach using simulations. The same simulation setup as in Section 3.3 is used.

4.1 Completion Rate

Fig. 2 shows the percentage of inferred neighboring and contention relationships as a function of the number of tests, called *completion rates*. Completion rate measures how fast the discovery phase takes. In the experiments, we vary the

tolerance level TOL and the number of nodes in the network by keeping the node density constant. For neighbor discovery, we compare it against an Aloha-like approach where each node randomly becomes active with probability q , and inference is possible only when 1) there is only one transmitter in the network, or ii) in the case of multiple transmitters, the observation $y_n(t) = 0$ for some nodes.

Fig. 2(a) shows the completion rates of neighbor discovery for the two algorithms. The completion rate increases when the number of tests increases as expected. Increasing the number of nodes in the network decreases the completion rate. Compared to ‘‘Aloha’’ model, our proposed binary model can achieve higher completion rate. For example, when $N = 30$, Aloha requires close to 600 tests to have a close to 100% completion rate, whilst our proposed inference algorithm only takes 200 tests. Fig. 2(b) shows the completion rates of neighbor discovery with respect to the number of tests under different tolerance levels. We observe that, increasing the tolerance decreases the completion rate as expected, but improves the reliability of decision significantly (Fig. 3(d)). Fig. 2(c) shows the completion rates of contention relationship inference with respect to the number of tests. Compared to Fig. 2(a), the link contention inference process is significantly slower. This is because the number of link contention relationships is in the order of $O(N^3)$.

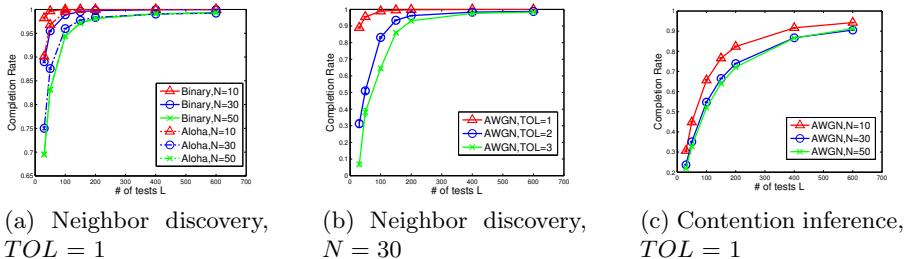
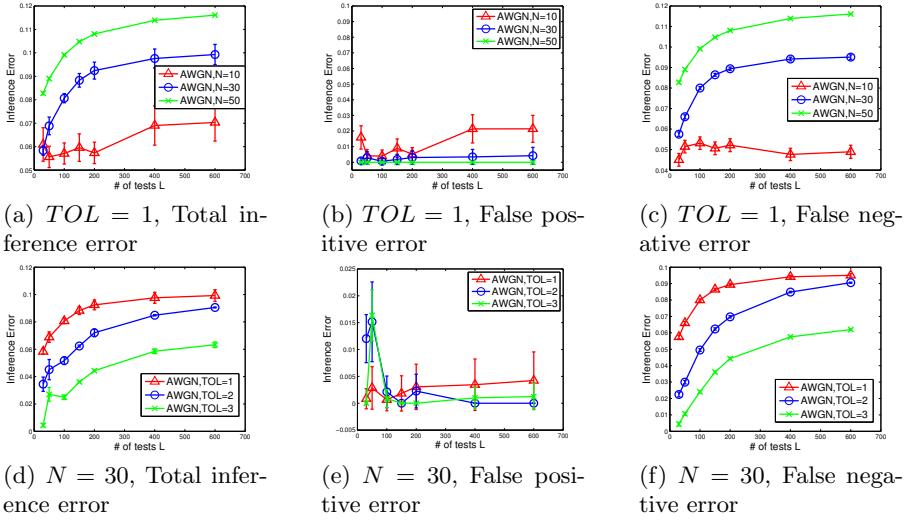


Fig. 2. Completion rate with $\Gamma_1 = 3dB$, $\Gamma_2 = -7dB$. In (a), an Aloha-like algorithm is compared to the ternary algorithm.

4.2 Inference Error Rate

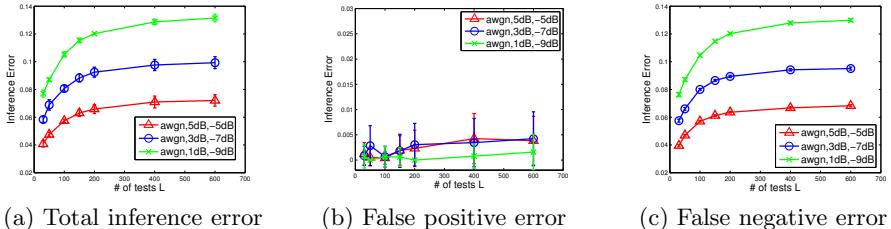
Fig. 3–4 show the total inference error rates, false positive and false negative error rates using the ternary model with respect to the ground truth. In the experiments, we vary the number of the number of tests, tolerance levels TOL , and the threshold values Γ_1 and Γ_2 . In computing the inference errors, we only account for the nodal and link relationships that have been determined thus far.

From Fig. 3, we observe that as the number of tests increases, the inference error rates increase and eventually level off. This can be attributed to more observation errors (Fig. 1) affecting the correctness of inferences. Increasing the number of nodes in the network decreases the false positive errors (Fig. 3(b)), but

**Fig. 3.** Inference error rate with $T_1=3\text{dB}$, $T_2=-7\text{dB}$, and 95% confidence

increases the false negative errors (Fig. 3(c)), which has a net effect of increased inference errors (Fig. 3(a)).

The inference error rate as the function of the SNR thresholds T_1 and T_2 is evaluated in Fig. 4. As a direct consequence of increased observation errors (Fig. 1), larger thresholds result in smaller inference errors.

**Fig. 4.** Inference error rate with different threshold values, $TOL=1$, $N = 30$, and 95% confidence

5 Conclusion

In this paper, we consider the problem of joint neighbor discovery and contention graph inference in wireless networks, which are fundamental building blocks in resource management. Compared to Aloha-like neighbor discovery schemes, the novelty of the proposed ternary inference algorithm lies in the exploitation of mixed signal at the receiver nodes. The simulation results demonstrate the

superior performance of the proposed algorithm in terms of completion rate and accuracy.

There are a number of issues that need to be resolved as part of our future work. First, we will devise an analytic model for the completion rate and inference errors. Second, adaptive randomized schedules will be explored that vary the active probability q . Third, we will investigate the impact of loose synchronization on inference errors and propose more robust mechanisms.

References

1. Jang, K.: Passive online inband interference inference in centralized WLANs. Technical Report 916, USC (2010)
2. Shrivastava, V., Rayanchu, S., Banerjee, S., Pagaginnaki, K.: PIE in the sky: Online passive interference estimation for enterprise wlans. In: USENIX (2011)
3. Yang, J., Draper, S., Nowak, R.: Learning the interference graph of a wireless network (2012), <http://arxiv.org/abs/1208.0562>
4. Chhetri, A., Zheng, R.: WiserAnalyzer: A passive monitoring framework for WLANs. In: IEEE MSN (2009)
5. Ahmed, N., Smarta, S.K.: A self-managing architecture for thin access points. In: ACM CoNEXT (2006)
6. Keshavarzian, A., Uysal-Biyikoglu, E., Herrmann, F., Manjeshwar, A.: Energy-efficient link assessment in wireless sensor networks. In: IEEE INFOCOM (2004)
7. Niculescu, D.: Interference map for 802.11 networks. In: ACM SIGCOMM Conference on Internet Measurement, IMC (2007)
8. Dutta, P., Culler, D.: Practical asynchronous neighbor discovery and rendezvous for mobile sensing applications. In: ACM SenSys (2008)
9. Kohvakka, M., Suhonen, J., Kuorilehto, M., Kaseva, V., Hännikäinen, M., Hämäläinen, T.D.: Energy-efficient neighbor discovery protocol for mobile wireless sensor networks. Ad Hoc Network 7(1), 24–41 (2009)
10. Zeng, W., Vasudevan, S., Chen, X., Wang, B., Russell, A., Wei, W.: Neighbor discovery in wireless networks with multipacket reception. In: ACM MobiHoc (2011)
11. You, L., Zhu, X., Chen, G.: Neighbor discovery in peer-to-peer wireless networks with multi-channel MPR capability. In: IEEE ICC (2012)
12. Angelosante, D., Biglieri, E., Lops, M.: A simple algorithm for neighbor discovery in wireless networks. In: IEEE ICASSP, vol. 3, pp. 169–172 (2007)
13. Neighbor discovery in wireless networks: A multiuser-detection approach. Physical Communication 3(1), 28–36 (2010)
14. Luo, J., Guo, D.: Neighbor discovery in wireless ad hoc networks based on group testing. In: IEEE Allerton (2008)
15. Luo, J., Guo, D.: Compressed neighbor discovery for wireless ad hoc networks: the rayleigh fading case. In: IEEE Allerton (2009)
16. Zhang, L., Luo, J., Guo, D.: Neighbor discovery for wireless networks via compressive sensing. CoRR, vol. arXiv:1012.1007 (2012)

An Improved Approximation Algorithm for the Shortest Link Scheduling Problem in Wireless Networks under SINR and Hypergraph Models*

Cui Wang¹, Jiguo Yu^{1, **}, Dongxiao Yu², and Baogui Huang¹

¹ School of Computer Science, Qufu Normal University,
Ri-zhao, Shandong, 276826, P.R. China

{wangcui6600,hjbaogui}@163.com, jiguoyu@sina.com, yu@mail.qfnu.edu.cn

² Department of Computer Science, The University of Hong Kong
Pokfulam, Hong Kong, China
dxyu@cs.hku.hk

Abstract. Link scheduling is a fundamental problem in wireless ad hoc and sensor networks. In this paper, we focus on the shortest link scheduling(SLS) under SINR and hypergraph models, and propose an approximation algorithm GeoSLS by using geometric links for better performance than GOW* proposed by *Blough, Resta and Santi*(2010). For the average length of scheduling, GeoSLS decreases $1/m$ compared with GOW*, where $m = \lfloor 4p + (\Delta_{max} - 4) \cdot (1-p) \rfloor$ is the expected number of the links in the set V returned by HyperMaxLS and $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V . In the worst, ideal and average cases, the ratios of time complexity of our algorithm GeoSLS to GOW* are $O(\Delta_{max}/\bar{k})$, $O(1/(\bar{k} \cdot \Delta_{max}))$ and $O(\Delta_{max}/(\bar{k} \cdot m))$, respectively, where $1 < \bar{k} < \Delta_{max}$ is a constant called the SNR diversity of instance G .

Keywords: Wireless Networks, Shortest Link Scheduling, Approximation Algorithm, Hypergraph Model, SINR.

1 Introduction

During the past two decades, wireless and sensor networks have been applied in various areas. Compared to a wired network, a wireless network has a fundamental property of sharing the common (radio) communication channels. Therefore, the links will inevitably interfere with each other as they transmit simultaneously. Due to the inherent interference property of wireless networks, one of the major challenges is to decrease interference and maximize the throughput of the network by appropriate scheduling strategy. Link scheduling is an important approach to decrease interference among the transmission links and enhance the

* The work is supported by NNSF of China for contract(61373027, 11101243) and NSF of Shandong Province for contract(ZR2012FM023).

** Corresponding author.

throughput of the network. According to the purpose of scheduling, link scheduling problem in a wireless network can roughly be classified into two cases, single-slot scheduling(One-Slot Scheduling) and the shortest link scheduling(SLS). The former is also known as the maximum independent set(MISL) or maximum link scheduling problem(MaxLSP). That is, for a given set of links, we need to compute the largest possible subset of links that can be scheduled simultaneously without conflicts. The latter is to schedule all the links in the minimum slots.

In wireless networks, interference model plays a very important role in the design of algorithms. The performance of a designed algorithm under different interference models may have great differences. Roughly speaking, interference models can be classified into the graph-based models and the physical interference model. The graph-based models are in essence binary interference models. This implies that the transmission from the sending node s to the receiving node r is successful if and only if r is within the transmission range of s , and within the interference range of r , there is no other concurrent transmission links. As the graph-based models are simple, easy to abstract, many scheduling algorithms in the previous works such as [1] [2], are proposed based on graph-based models. However, the graph-based models are too idealistic, and ignore the cumulative interference. There must exist gaps compared with the actual application environment. In [3], Gupta and Kumar first proposed Signal-to-Interference-plus-Noise-Ratio (SINR) model, this is a kind of physical interference model. Under SINR, the transmission from the node s to the node r is successful if and only if the SINR value of receiver r is greater than a certain threshold. Thus, the interference is no longer a binary interference, all the links in the network have to be considered. In other words, even if the transmission from a far node may also interfere or even prevent the successful transmission of the current node.

It is difficult to design algorithms under the SINR, a global interference model. Li *et al.* proposed a new interference model called the hypergraph model in [4] [5]. This model is different from the hypergraph proposed in [6]. The hypergraph model considers the cumulative interference, which is more accurate than the traditional binary graph models. Unlike the global SINR model, the hypergraph model has locally graphic structures, which can achieve a systematic trade-off between the interference approximation accuracy and user coordination complexity during scheduling [5]. As an application of the hypergraph model, Li *et al.* gave a simple distributed scheduling algorithm for single-slot link scheduling problems. They obtained a lower bound stability region for any maximal scheduler, proved that the interference approximation accuracy of hypergraph model in random networks, and showed that hypergraphs with small hyperedge sizes can model the interference accurately.

In this paper, we mainly focus on the design of SLS algorithm under the SINR model and hypergraph model. The main idea of the algorithms comes from the approximation algorithm in [4] [7]. Firstly, since the hypergraph model can limit the interference of link around itself, the interference from far links can be negligible. Then, we give an improved the algorithm GeoSLS by referring to the ideas of GOW* in [7], and prove the schedule length of the GeoSLS is

$O(\Delta_{max})$ in the worst case in which the links in each division cell S must be sequentially scheduled, where Δ_{max} is maximum number of the receivers in the partitioned cells. The average length of the scheduling is $\Theta(\Delta_{max}/m)$, where $m = \lfloor 4p + (\Delta_{max} - 4) \cdot (1 - p) \rfloor$ is the expected number of the links in the set V returned by HyperMaxLS and $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V . Compared with the algorithm GOW* in [7] whose scheduling length is $O(|C_0| + \Delta_{max})$, where $|C_0|$ is number of links in the C_0 class in which the link must be sequentially scheduled. In the worst case, the length of our algorithm GeoSLS decreases by C_0 , and the average length of scheduling decreases by $1/m$. In the worst case, ideal case and the average case, the ratios of the time complexity of our algorithm to the GOW* are $O(\Delta_{max}/\bar{k})$, $O(1/(\bar{k} \cdot \Delta_{max}))$ and $O(\Delta_{max}/(\bar{k} \cdot m))$, respectively. Constant $1 < \bar{k} < \Delta_{max}$ is called the SNR diversity of instance G .

The rest of this paper is organized as follows. In Section 2, we summarize the related works. In Section 3, we introduce interference models. In Section 4, we present the improved algorithm. And Section 5 concludes the paper.

2 Related Works

A major challenge for link scheduling problem is the wireless interference which limits the link transmission in parallel. Graph-based interference models usually are well understood, due to its simplicity and abundant results of graph theory. Many effective approximate algorithms, such as maximal scheduling and the longest queue first (LQF) scheduling have been proposed [1]. In [8], Moscibroda *et al.* proposed an approximation algorithm which does not require the node location information, and the running time of the algorithm is $O(n)$, where n is the number of links in the network. In [9], Afek *et al.* presented a distributed algorithm for link maximal independent set, which is only necessary to estimate the total number of nodes in the network. However, the graph-based models have also been regarded as a rigorous model which oversimplifies the interference constraints in wireless networks, since it does not take into account the cumulative effect of interference.

Unlike the graph-based models, the physical SINR model can accurately describe the interference in wireless networks. The link scheduling algorithms under the physical interference model are more accurate than the graph-based models. In [10], Goussevskaia *et al.* firstly proved that computing a SLS under the $SINR$ was NP-hard, and gave an $O(g(L))$ -approximation algorithm, where $g(L)$ indicates the link length density in the network. In [11], Pei and Kumar proposed a fast distributed algorithm under the SINR model, whose running time is $O(g(L) \log^c m)$, where $c = 1, 2$ and 3 for different problem instances, and m is the number of links. In [12], based on capacity maximization algorithm, Kesselheim gave an $O(\log^2 n)$ -approximation algorithm for latency-minimization problem. In [13], Halldórsson *et al.* proved a distributed $O(\log n)$ - approximation algorithm has best ratio when compared with centralized algorithms. In [14], Wan *et al.* proposed a polynomial $O(\beta \ln \alpha)$ -approximation algorithm for SLS with

power control under SINR, where α is the independence number, β is the power density. In [15], Kompella *et al.* addressed the SLS problem under SINR model in wireless networks as a cross layer optimization problem, and considered the parameters of link layer, physical layer, and dynamic power in order to get a viable matching. Efficient scheduling algorithms under the SINR model has been widely recognized, however, low-complexity scheduling is still far from being solved. This is because the global interference, *i.e.*, the transmission of any link will be received by other links in the network as the interference, the link weakens its own communication quality. This means that the scheduling algorithms under the SINR model have to coordinate all the links in the network, which makes it very difficult to design the distributed algorithms.

In [4] [5], Li *et al.* proposed hypergraph model based on the graph-based and SINR models, and pointed out that the hypergraph model can combine the advantages of both graph-based models and the SINR model while avoiding their drawbacks. Namely, the hypergraph model can emulate cumulative interference constraints as “hyperedge”, where each “hyperedge” is a set of links that are not allowed to transmit simultaneously. Thus, the hypergraph model can avoid the defects of graph-based models which overlook the cumulative interference. Moreover, since a major portion of the total interference is caused by only a few nearby transmitting links in special wireless networks, the hypergraph can approximate the SINR locally with very good accuracy. Therefore, the hypergraph model can restrict the interference to local. In this paper, we design an SLS algorithm GeoSLS under the hypergraph model and SINR model.

3 Interference Models

Let $L = \{l_1, l_2, \dots, l_n\}$ denote the set of links, where each link l_i represents a communication request from a sender s_i to a receiver r_i , $d_{mn} = d(s_m, r_n)$ denote the Euclidean distance between two nodes s_m and r_n . Thus, the length of link l_j is d_{jj} . We use the path loss model as energy consumption model. That is,

$$P_{r_j}(s_i) = \frac{P}{d_{ij}^\alpha}. \quad (1)$$

where P is the transmission power, the path-loss exponent $2 < \alpha < 6$ is a constant, and $P_{r_j}(s_i)$ is the received power of the signal from s_i to r_j . We adopt the physical interference model, in which a node r_i successfully receives the message from a sender s_i if only if the following condition holds

$$SINR(r_i) = \frac{P_{r_i}(s_i)}{N + I_{r_i}} = \frac{P_{r_i}(s_i)}{N + \sum_{l_j \in W \setminus l_i} P_{r_i}(s_j)} = \frac{P/d_{ii}^\alpha}{N + \sum_{l_j \in W \setminus l_i} P/d_{ji}^\alpha} \geq \beta. \quad (2)$$

where N is the ambient noise, I_{r_i} is the sum of the interference power experienced by a receiver of link l_i , W is the set of concurrently scheduled links in the same

slot, and $\beta \geq 1$ represents the threshold value, *i.e.*, the minimum SINR required for the message to be successful received. We call a transmission set W is valid if the SINR of any transmitting link in W satisfies (2).

A hypergraph interference model is a hypergraph $H = (L, \varepsilon)$, where L is the link set, and ε is the set of hyperedges such that each hyperedge $e = (\{l_{i_1}\}, \{l_{i_2}, l_{i_3}, \dots, l_{i_{k-1}}\}) \in \varepsilon$ consists of a subset of links, in which the links are not allowed to transmit together [4]. For any two link sets $S, T \subseteq L$, $e = (S, T) \in \varepsilon$ if and only if it satisfies [5]

(1) When the links in $S \cup T$ are scheduled all the links in S fail and none of T fails.

(2) If any link in $S \cup T$ is removed, no failure occurs if only the remaining links are scheduled.

The condition (1) is validity, and (2) is minimality. For instance, the set of links $\{\{1\}, \{2, 3\}\}$ is a hyperedge, and while the set $\{\{1\}, \{2, 3, 4\}\}$ can not form a hyperedge.

4 The Approximation Algorithm for SLS

In this section, we give the shortest link scheduling algorithm GeoSLS with a better performance by improving the algorithm GOW* in [7].

In order to understand the differences between algorithm GeoSLS and GOW*, we first review the main implementation of algorithm GOW*. GOW* is based on the idea of partitioning links into SNR classes $C_0, C_1, \dots, C_{\lfloor \log_{1+\epsilon}(P/\beta N) \rfloor}$, with the property that C_i is the set of link l_i such that $(1 + \epsilon)^k \leq \text{SNR}(l_i) < (1 + \epsilon)^{k+1} \beta$, where $\epsilon \geq \frac{1}{\beta}$. GOW* sequentially schedule all the links in class C_0 . Then, for each class C_i , where $i \geq 1$, it is defined that a proper square cell partitioning of the deployment region. Cells are 4-colored in such a way that no two adjacent cells have the same color. Finally, links are greedily scheduled in successive slots, with the property that only links with the same color whose receivers are in different cells are assigned with the same slot.

The differences between algorithm GeoSLS and GOW* are as follows.

Firstly, algorithm GeoSLS uses the geometric links, the outer **for** loop (4-5) of the algorithm GOW* in [7] can be omitted. Then, we divide the network deployment region and set the size of cells at the beginning of the algorithm only once since the links are not classified. Secondly, we can set the size of cells at the beginning of the algorithm, and the deployment region does not need to be repeatedly divided and colored. So compared with GOW*, our algorithm can greatly reduce the time complexity. Finally, the “black links” in [7] must be sequentially dispatched since the SNR values of them are exactly β . Thus, we consider the “black link” as a special case by putting the black link into the set M . In fact, we assume that the lengths of links in the network are geometric proportion, which means $|M| = 1$.

We improve the way of choosing the links in GOW*, and select multiple links instead of only one link in GOW*. We expect to choose as many links at each time slot as possible. Therefore, the number of slots for scheduling all links will be decreased, and the scheduling length will be reduced accordingly.

The algorithm has to call a sub-algorithm HyperMaxLS in order to schedule all the links in the minimum slots. Now, we describe GeoSLS with pseudo-codes.

An Approximation Algorithm for SLS (GeoSLS)

Input: A set L containing n geometric links that the shortest length and the longest length are D and D_n , respectively.

Output: A feasible schedule S_1, S_2, \dots, S_t .

1. Partition network deployment region into squares of width $\mu \cdot D$ and 4-color the squares such that no two adjacent squares have the same color
 2. **for** $j=1, 2, 3$ and 4
 3. **repeat**
 4. For each square A of color j , in which the links compose the set L' , implement the algorithm HyperMaxLS on the set L' , S' is the set V returned by algorithm HyperMaxLS; $L' = L' \setminus S'$; $L_j = L_j \cup S'$
 5. $t = t + 1$; $S_t = L_j$
 6. **until** all the links in selected squares are scheduled
 7. **return** S_1, S_2, \dots, S_t
-

We assume that the lengths of links in the network are geometric proportion, and the length of the shortest link in the network is D , i.e., $D = d_{ii}$, and the length of the longest link is $D_n = D \cdot q^{n-1}$, where $1 < q < 2$ is the common ratio of the lengths of links. Divide the deployment region into square cells of width $\mu \cdot D$, where constant μ is defined as $\mu = 2 \cdot (q^{n-1})^{\lceil \frac{8|k|\beta(\beta+\tau)(\alpha-1)}{\tau(\alpha-2)} \rceil^{\frac{1}{\alpha}}}$, the constant $\tau > 0$, $|k| = \Delta_{max} + 1$ is the upper bound of the links in the set V returned by HyperMaxLS, and Δ_{max} is the maximal number of receivers in a cell [7].

Next, we give a simple and intuitive scheduling algorithm HyperMaxLS, in which we collect the links from a given set of links. Firstly, we choose any link as the key link, and find out the hyperedge which contains the most links. Then, according to the definition of “active hyperedge”, a hyperedge $e_i = (\{l_i\}, \{l_{i_1}, l_{i_2}, \dots, l_{i_{k-1}}\}) \in \varepsilon$ with respect to link l_i is “active” if all links in e_i except l_i are scheduled in [4] [5], the algorithm HyperMaxLS can find out the maximal set of feasible scheduling by forming the “active hyperedge” for each link. The description of HyperMaxLS in pseudo-codes is as follow.

Maximal links schedule under Hypergraph model (HyperMaxLS)

Input: A set L' of links located arbitrarily in the Euclidean plane.

Output: A maximal set of feasible links.

1. **Each** link in L' synchronously implement the pseudo-code; $\varepsilon = \phi$; $V = \phi$
 2. Chose any link $l_i \in L'$ and $l_j \in L' \setminus l_i$; $S_i = \{l_i\}$; $T_i = \phi$
 3. **while** ($L' \neq \phi$)
 4. $T_i = T_i \cup l_j$
 5. **if** (any element in $\varepsilon \in S_i \cup T_i$) ;
 6. **else if**(S_i is invalid)
 7. **if** (T_i is valid)
 8. $e_i = S_i \cup T_i$ will join the ε
 9. **end if**
 10. **else if** (T_i is valid)
 - /* in order to compensate for the deprived links in the line 15 */
 11. $T_i = T_i \cup l_j$
 12. **end if**
 13. **end if**
 14. **end if**
 15. $T_i = T_i \setminus l_j$
 16. $L' = L' \setminus l_j$
 17. **end while**
 18. **return** $V = \arg \max_{T_i \in e_i \in \varepsilon} |T_i|$
-

We call the set S_i is valid(feasible), if each link l_i in the set S_i satisfies

$$\frac{P/d_{ii}^\alpha}{N + \sum_{j \in e_i \setminus \{l_i\}} P/d_{ji}^\alpha} \geq \beta + \tau. \quad (3)$$

The set T_i is valid(feasible), if each link l_j in the set T_i satisfies

$$\frac{P/d_{jj}^\alpha}{N + \sum_{k \in T_i \setminus l_j} P/d_{kj}^\alpha} \geq \beta + \tau. \quad (4)$$

where $e_i = S_i \cup T_i$ in (3) and (4), arbitrarily small constant $\tau > 0$.

We next prove the correctness and the time complexity, determine the scheduling length of the algorithm GeoSLS.

Theorem 1. *The set V constructed by algorithm HyperMaxLS is feasible.*

Proof. According to the definition of the hyperedge that all links in the set T_i can be scheduled together, the set V is feasible. Moreover, the algorithm can confirm that each SINR value of links in the set T_i is greater than $\beta + \tau$. Therefore, the set V is feasible.

Theorem 2. *The schedule computed by algorithm GeoSLS is feasible under the SINR model.*

Proof. We assume that the maximum interference experienced by the link l_i in the set V is I , namely, $\frac{P/d_{ii}^\alpha}{N+I} \geq \beta + \tau$. Now, we calculate the upper-bounded of the total interference I_r contributed by the links in the cells except S and experienced by the link l_i which receiver in a cell S . The inner frame contains 8 cells, the second frame contains 16 cells, and in general the h^{th} frame will contains $(2h+1)^2 - (2h-1)^2 = 8 \cdot h$ cells. The generic receiver contained in the h^{th} frame will be at least $(2h-1)\mu D$ apart from r_i . Considering the minimum distance between r_i and a sender relative to frame h is $(2h-1)\mu D - D_n = D_n((2h-1)\mu/q^{n-1} - 1)$. Thus, the total interference I_r experienced by r_i can be bounded by

$$I_r < \sum_{h=1}^{\infty} \frac{8P|k|\cdot h}{D_n^\alpha((2h-1)\mu/q^{n-1}-1)^\alpha}. \quad (2.1)$$

$$\leq \frac{8P|k|}{D_n^\alpha} \sum_{h=1}^{\infty} \frac{h}{(1/2)^\alpha((2h-1)\mu/q^{n-1})^\alpha}. \quad (2.2)$$

$$= \frac{8P|k|(q^{n-1})^\alpha}{(1/2)^\alpha D_n^\alpha \mu^\alpha} \sum_{h=1}^{\infty} \frac{h}{(2h-1)^\alpha}. \quad (2.3)$$

$$\leq \frac{8P|k|(q^{n-1})^\alpha}{(1/2)^\alpha D_n^\alpha \mu^\alpha} \sum_{h=1}^{\infty} \frac{1}{h^{\alpha-1}}. \quad (2.4)$$

$$\leq \frac{8P|k|(q^{n-1})^\alpha}{(1/2)^\alpha D_n^\alpha \mu^\alpha} \cdot \frac{\alpha-1}{\alpha-2}. \quad (2.5)$$

where (2.2) follows because $x-1 > x/2$ for $x > 2$ and indeed $(2h-1)\mu/q^{n-1}$ is always greater than 2, and (2.5) follows from on Riemanns zeta function.

Sequentially, we need to prove that any link l_i in the set V returned by HyperMaxLS is valid after being experienced the interference I_r . That is,

$$\frac{P/d_{ii}}{N+I+I_r} \geq \beta. \quad (5)$$

In order to prove that (5) holds, we may prove $\frac{N+I+I_r}{P_{r_i}(s_i)} \leq 1/\beta$. Note that, $P_{r_i}(s_i) = P/d_{ii}^\alpha$, we have,

$$\begin{aligned} & \frac{N+I+I_r}{P_{r_i}(s_i)}. \\ &= \frac{N+I}{P_{r_i}(s_i)} + \frac{I_r}{P_{r_i}(s_i)}. \\ &< \frac{1}{\beta+\tau} + \frac{8P|k|(q^{n-1})^\alpha}{(1/2)^\alpha D_n^\alpha \mu^\alpha} \cdot \frac{\alpha-1}{\alpha-2} / P_{r_i}(s_i). \\ &= \frac{1}{\beta+\tau} + \frac{P \cdot \tau}{D_n^\alpha \beta (\beta+\tau)} / P_{r_i}(s_i). \\ &\leq \frac{1}{\beta+\tau} + \frac{\tau}{\beta+\tau}. \\ &= \frac{1}{\beta}. \end{aligned}$$

Therefore, $\frac{P/d_{ii}}{N+I+I_r} \geq \beta$. The schedule given by GeoSLS is feasible.

Note. If the lengths of links in the network are equal, then $\mu = 2 \cdot [\frac{8|k|\beta(\beta+\tau)(\alpha-1)}{\tau(\alpha-2)}]^{\frac{1}{\alpha}}$, we can also prove that the algorithm is correct.

Theorem 3. *The time complexity of algorithm HyperMaxLS is $O(\Delta_{max})$.*

Proof. The maximum number of receivers in a cell is Δ_{max} , which means the maximum number of links in the set L' is Δ_{max} . Each node in the set L' synchronously execute of the algorithm. In the process of implementation, the remaining links except the selected link need to determine whether it is continue to join a set T_i or not until all links are checked. Then the algorithm returns the set V . Therefore, the time complexity of HyperMaxLS is $\Delta_{max} - 1$, i.e., $O(\Delta_{max})$.

Theorem 4. *Algorithm GeoSLS can complete in $O(n \cdot C_0 \cdot \Delta_{max}^2)$. In the ideal case, the complexity of GeoSLS is $O(n \cdot C_0)$. The average time complexity of the algorithm is $O(n \cdot C_0 \cdot \Delta_{max}^2/m)$, where $m = [4p + (\Delta_{max} - 4) \cdot (1 - p)]$ is the expected number of the links in the set V returned by HyperMaxLS, $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V and C_0 is the maximum number of cells in a partitioning of the deployment region in the line 1 of algorithm GeoSLS.*

Proof. The deployment region is divided into square cells and all the cells have been 4-colored. For each of the four colors considered, all the cells of current color are scanned $O(C_0)$ times. The time complexity of the algorithm HyperMaxLS is $O(\Delta_{max})$. In the worst case, we have to select only one link in each cell since any two links in a cell are not scheduled together. Therefore, choosing the links in a cell from the first to the last have to execute $O(\Delta_{max})$ times, then the **repeat-until** loop up to n . Thus, time complexity of the algorithm GeoSLS is $O(n \cdot C_0 \cdot \Delta_{max}^2)$. In the ideal case, the **repeat-until** loop up to $[n/\Delta_{max}]$ times since all the links in one unit can be scheduled simultaneously, so the time complexity of the algorithm GeoSLS is $O(n \cdot C_0)$. Moreover, we assume that the number of links scheduled together in a cell is 4 with probability $0 < p < 1$ since the hypergraph with 4 hyperedges has a better approximation [5]. Therefore, the expected number of the links in the set V returned by HyperMaxLS is $m = [4p + (\Delta_{max} - 4) \cdot (1 - p)]$. Thus, the time complexity of GeoSLS is $O(n \cdot C_0 \cdot \Delta_{max}^2/m)$. The time complexity of GOW* is $O(n \cdot \bar{k} \cdot \#c \cdot \Delta_{max})$, where $\#c$ is the maximum number of cells in a partitioning of the deployment region, and constant \bar{k} is called the SNR diversity of instance G . In this paper, we consider $1 < \bar{k} < \Delta_{max}$ since we mainly select the links in one cell and $1 < q < 2$. In the worst case, ideal case and the average case, the ratios of the time complexity of our algorithm to the GOW* are $O(\Delta_{max}/\bar{k})$, $O(1/(\bar{k} \cdot \Delta_{max}))$ and $O(\Delta_{max}/(\bar{k} \cdot m))$, respectively.

Theorem 5. *The upper bound of the scheduling length computed by algorithm GeoSLS is $O(\Delta_{max})$. The average length of the scheduling is $\Theta(\Delta_{max}/m)$, where $m = [4p + (\Delta_{max} - 4) \cdot (1 - p)]$ is the expected number of the links in the set V returned by HyperMaxLS and $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V .*

Proof. Theorem 2 shows that links whose receivers are in different cells with the same color can be scheduled simultaneously. Firstly, we consider a link from node s to node r in the cell S , and assume that r is exactly at the border of s 's maximum transmission range, *i.e.*, the SNR at node r is exactly $\beta + \tau$, therefore, there are only one link in the cell S is scheduled in one slot. So, all links in the cell S must be sequentially scheduled. The length of scheduling all the links in the cell S is Δ_{max} . Then multiply the color's number, the upper bound of the scheduling length computed by GeoSLS is $4 \cdot \Delta_{max}$. Secondly, there are more two links in the cell S are scheduled simultaneously, in ideal case, all links in S can be scheduled together. Thus, the length of the scheduling computed by GeoSLS is $O(1)$. Moreover, we assume that the excepted number of links in the set V returned by HyperMaxLS is $m = \lfloor 4p + (\Delta_{max} - 4) \cdot (1 - p) \rfloor$, where $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V . So the average length of scheduling all the links is $\Theta(\Delta_{max}/m)$.

5 Conclusion

In this paper, we present a link schedule algorithm GeoSLS under the SINR and hypergraph models, prove that the upper bound of the scheduling length constructed by the algorithm GeoSLS is $O(\Delta_{max})$, the average length of scheduling is $\Theta(\Delta_{max}/m)$, where $m = \lfloor 4p + (\Delta_{max} - 4) \cdot (1 - p) \rfloor$ is the expected number of the links in the set V returned by HyperMaxLS and $0 < p < 1$ is the probability of the number of the links scheduled simultaneously in the set V . In the worst case, ideal case and the average case, the ratios of the time complexity of our algorithm GeoSLS to the GOW* are $O(\Delta_{max}/\bar{k})$, $O(1/(\bar{k} \cdot \Delta_{max}))$ and $O(\Delta_{max}/(\bar{k} \cdot m))$, respectively, and $1 < \bar{k} < \Delta_{max}$. We will make further study about the link scheduling problem with non-uniform power under SINR and hypergraph models.

References

1. Chaporkar, P., Kar, K., Luo, X., Sarkar, S.: Throughput and Fairness Guarantees through Maximal Scheduling in Wireless Networks. *IEEE Trans. Inf. Theory.* 54, 572–594 (2008)
2. Dimakis, A., Walrand, J.: Sufficient Conditions for Stability of Longest Queue First Scheduling: Second Order Properties using Fluid Limits. *Adv. Appl. Probab.* 38, 505–521 (2006)
3. Gupta, P., Kumar, P.R.: The Capacity of Wireless Networks. *IEEE Trans. Inf. Theory.* 46, 388–404 (2000)
4. Li, Q., Kim, G., Negi, R.: Maximal Scheduling in a Hypergraph Model for Wireless Networks. In: Proceedings of IEEE International Conference on Communications (ICC 2008), pp. 3853–3857 (2008)
5. Li, Q., Negi, R.: Maximal Scheduling in Wireless Ad hoc Networks with Hypergraph Interference Models. *IEEE Trans. Vehicular Technology.* 61, 297–310 (2012)
6. Sarkar, S., Sivarajan., K.N.: Hypergraph Models for Cellular Mobile Communication Systems. *IEEE Trans. Vehicular Technology* 47, 460–471 (1998)

7. Blough, D.M., Resta, G., Santi, P.: Approximation Algorithms for Wireless Link Scheduling with SINR-Based Interference. *IEEE/ACM Transactions on Networking* 18, 1701–1712 (2010)
8. Moscibroda, T., Wattenhofer, R.: Maximal Independent Sets in Radio Networks. In: *Proceedings of PODC 2005*, pp. 148–157 (2005)
9. Afek, Y., Alon, N., Barad, O., Hornstein, E., Barkai, N., Bar-Joseph, Z.: A Biological Dolution to a Gundamental Distributed Computing Problem. *Science* 331, 183–185 (2011)
10. Goussevskaya, O., Oswald, Y.A., Wattenhofer, R.: Complexity in Geometric SINR. In: *Proceedings of MobiHoc 2007*, pp. 100–109 (2007)
11. Pei, G., Vullikanti, A.K.S.: Brief Announcement: Distributed Algorithms for Maximum Link Scheduling in the Physical Interference Model. In: Aguilera, M.K. (ed.) *DISC 2012*. LNCS, vol. 7611, pp. 407–408. Springer, Heidelberg (2012)
12. Kesselheim, T.: Approximation Algorithms for Wireless Link Scheduling with Flexible Data Rates. In: Epstein, L., Ferragina, P. (eds.) *ESA 2012*. LNCS, vol. 7501, pp. 659–670. Springer, Heidelberg (2012)
13. Halldórsson, M.M., Mitra, P.: Nearly Optimal Bounds For Distributed Wireless Scheduling in the SINR Model. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) *ICALP 2011, Part II*. LNCS, vol. 6756, pp. 625–636. Springer, Heidelberg (2011)
14. Wan, P., Xu, X., Frieder, O.: Shortest Link Lcheduling with Power Control under Physical Interference Model. In: *Proceeding of the Sixth International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2010)*, pp. 74–78 (2010)
15. Kompella, S., Wieselthier, J.E., Ephremides, A., Sherali, H.D.: On Optimal SINR-based Scheduling in Multihop Wireless Networks. *IEEE/ACM Transactions on Networking* 18, 1713–1724 (2010)

MIMO-Aware Spectrum Access and Scheduling in Multi-hop Multi-channel Wireless Networks

Lin Luo¹, Dengyuan Wu², and Hang Liu³

¹ Marvell, Inc., San Jose, CA, USA

clarylin@gmail.com

² Department of Computer Science,

The George Washington University, Washington, DC, USA

andrewwu@gwmail.gwu.edu

³ Department of Electrical Engineering and Computer Science,

The Catholic University of America, Washington, DC, USA

liuh@cua.edu

Abstract. Software defined radios (SDRs) are a promising technology to enable dynamic channel access and sharing. Multiple Input Multiple Output (MIMO) is another radio technology breakthrough for increasing wireless throughput. To obtain the full benefits brought by SDR and MIMO technologies in wireless mesh networks (WMNs), the higher layer mechanisms should exploit their capabilities in a systematic way. In this paper, we propose a Stream Controlled Multiple Access (SCMA) scheme for multi-hop multi-channel WMNs, which is responsible for scheduling links and assigning channels for data transmission and controlling MIMO operation mode in a cross-layer approach. It enables efficient spectrum access and sharing in temporal, frequency, and spatial dimensions, and adapts to varying network conditions. The evaluation results show that the proposed SCMA scheme greatly improve the network performance compared to the traditional schemes.

Keywords: software-defined radio, MIMO, multi-channel wireless mesh networks, scheduling, multiple access.

1 Introduction

Software defined radios (SDRs) are a promising technology to enable dynamic channel access and sharing by allowing flexible configuration of radio transmission parameters in real time and switching from one channel to another. Multiple Input Multiple Output (MIMO) is another radio technology breakthrough for improving wireless network performance. MIMO can provide many types of benefits via multiple antennas and advanced signal processing. A transmitter can concurrently send multiple independent data streams over multiple antenna elements on the same frequency channel to increase throughput, and the receiver is able to separate and decode these data streams based on their spatial signatures. This feature is referred to as spatial multiplexing. In another way, MIMO can realize interference suppression and improve spectrum spatial reuse. A MIMO transmitter can nullify its signal interference to undesired nearby receivers, and a

MIMO receiver can suppress interference caused by undesired nearby transmitters. These benefits can be achieved simultaneously by properly using different MIMO techniques, i.e. controlling MIMO operation mode. For example, spatial multiplexing and interference suppression can be realized together for achieving significant performance gain. Given its potential, MIMO has been adopted in next-generation WiFi, WiMax, and cellular network standards.

SDR and MIMO are expected to greatly enhance spectrum utilization and increase wireless network throughput. Particularly, in multi-hop wireless mesh networks (WMNs), one of the major problems is capacity reduction due to interference among multiple simultaneous transmissions [1]. WMNs can exploit SDR and MIMO to improve their performance. A WMN node can equip with one or more MIMO-enabled SDR interface. To obtain the full benefits brought by SDR and MIMO techniques in multi-channel WMNs, the higher layer mechanisms such as MAC scheduling should exploit their capabilities in a systematic way due to the interdependence. Particularly, a key challenge in the algorithm design is to take into account the interaction of transmission scheduling, allocation of available frequency channels to different radios, and control of MIMO operation mode on each wireless link (also referred to as MIMO stream control). Scheduling concurrent transmissions on different wireless links should consider the interference level of the links that is determined by the resource allocation at the physical layer. The MIMO operation mode selection of a radio link is inter-dependent with channel assignment and other scheduled radio transmissions on the assigned channel in the neighborhood. The conventional channel assignment and scheduling algorithms for non-MIMO networks become inefficient when directly applied to MIMO SDR-based WMNs. In order to take advantage of MIMO and SDR technologies in multichannel WMNs, it is necessary to use a cross-layer approach to design these networks.

Various channel assignment, scheduling, routing algorithms [2, 3] have been proposed for WMNs, but those algorithms did not consider the effects of MIMO. MIMO has been widely studied for single point-to-point link or point-to-multipoint transmission scenarios in physical and link layers [4, 5]. More recently, the throughput gain of MIMO in single-channel WMNs have been investigated [6, 7], however channel assignment is not an issue in those studies.

As far as we know, research on multichannel MIMO WMNs is very limited and only few results are available [8, 9]. In [8], authors formulated an analytical framework and derived the maximum achievable network throughput in multi-channel multi-antenna WMNs as MIMO interference suppression technique is used. In addition, they only considered routing, not scheduling, in their formulation to optimize the total network throughput. [9] enhanced [8] by presenting a mathematical model of routing and scheduling optimization problem, and analyzed and compared the achievable network throughput for several MIMO operation modes with interference suppression and spatial multiplexing. These works mainly focus on theoretical formulation of the optimization problem with an abstract model of the system, and compute the upper bound of achievable throughput. However, how to design algorithms to exploit SDR and MIMO capabilities to improve performance in multi-hop multi-channel WMNs remains an untouched but challenging issue.

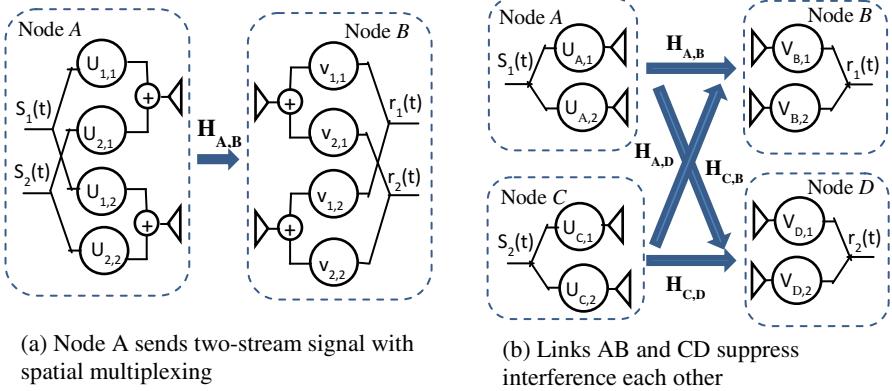
In this paper, we propose a scheme, called Stream Controlled Multiple Access (SCMA), for multi-hop multi-channel WMNs, which is responsible for scheduling links and assigning channels to transmit, and controlling the MIMO transmission mode in a cross-layer approach. In order to maintain network stability, it is desirable that the network layer selects the route of data flows based on long-term expected network conditions. The flow paths are thus not overly sensitive to the instantaneous channel and traffic changes. Therefore, in this work, we assume that routing has been established based on an existing routing protocol [10, 11], and focus on channel assignment, MIMO mode control, and scheduling. The proposed SCMA scheme is able to adapt to channel variations and traffic dynamics to exploit local transmission opportunities and achieve efficient spectrum access and sharing in temporal, frequency, and spatial dimensions. The evaluation results show that the proposed scheme greatly improve the network performance compared to the traditional schemes.

The rest of the paper is organized as follows. In Section 2, we present MIMO background. Section 3 describes the network model. The proposed scheme is presented in Section 4. Performance evaluation is given in Section 5. Finally Section 6 concludes the paper.

2 MIMO Background

MIMO employs multiple antenna elements to offer multiple Degrees of Freedom (DoFs) for communications at a node and to achieve spatial multiplexing and interference suppression. In this section, we briefly explain the basics of MIMO and its benefits. Since MIMO is a broad category containing various techniques, we will mainly focus on introducing Zero-Forcing-Beam-Forming (ZFBF) [5], which is one of the most powerful MIMO techniques.

For ease of explanation, let us first consider a MIMO link and assume that the transmitting node A and the receiving node B are each quipped with two antennas as shown in Fig. 1(a). Two streams, $s_1(t)$ and $s_2(t)$, can be transmitted simultaneously through this MIMO link. Before transmission, precoding can be performed on the two streams by multiplying the stream $s_i(t)$ ($i=1, 2$) with an encoding vector $\mathbf{u}_i = [u_{i,1} \ u_{i,2}]^T$. Therefore, the resulting transmitted signal will be $\mathbf{s}_t(t) = \mathbf{u}_1 s_1(t) + \mathbf{u}_2 s_2(t)$. Each antenna transmits a weighted combination of the original streams $s_1(t)$ and $s_2(t)$. Let $\mathbf{H}_{A,B}$ denote the 2×2 channel matrix between the transmitter A and receiver B. Each entry h_{ij} of $\mathbf{H}_{A,B}$ is a complex channel coefficient along the path from the j th antenna on the transmitter to the i th antenna on the receiver. At the receiver, two separate streams, $r_1(t)$ and $r_2(t)$ can be constructed by weighting the two received signals (one on each antenna) with two decoding vectors $\mathbf{v}_1 = [v_{1,1} \ v_{1,2}]^T$ and $\mathbf{v}_2 = [v_{2,1} \ v_{2,2}]^T$. One can write $r_1(t) = (\mathbf{v}_1^T \mathbf{H}_{A,B} \mathbf{u}_1) s_1(t) + (\mathbf{v}_1^T \mathbf{H}_{A,B} \mathbf{u}_2) s_2(t) + \mathbf{v}_1^T \mathbf{n}$ and $r_2(t) = (\mathbf{v}_2^T \mathbf{H}_{A,B} \mathbf{u}_1) s_1(t) + (\mathbf{v}_2^T \mathbf{H}_{A,B} \mathbf{u}_2) s_2(t) + \mathbf{v}_2^T \mathbf{n}$, where \mathbf{n} is the channel noise. With appropriate configuration of the encoding and decoding vectors, one can ensure $\mathbf{v}_1^T \mathbf{H}_{A,B} \mathbf{u}_2 = 0$ and $\mathbf{v}_1^T \mathbf{H}_{A,B} \mathbf{u}_1 = 1$ to construct $r_1(t)$, and $\mathbf{v}_2^T \mathbf{H}_{A,B} \mathbf{u}_1 = 0$ and $\mathbf{v}_2^T \mathbf{H}_{A,B} \mathbf{u}_2 = 1$ to construct $r_2(t)$. Hence, multiple antennas can be exploited to send multiple streams for increasing throughput with spatial multiplexing.

**Fig. 1.** MIMO transmission

MIMO can also be used to suppress interference. Considering an example in Fig. 1(b), there are two concurrent transmissions: node A → node B and node C → node D, which interfere each other. If each of the nodes is equipped with a single omnidirectional antenna, node C's transmission will interfere with node B's reception, and hence, node B will not be able to successfully receive the signal from node A. Similarly, node D cannot successfully receive the signal from node C under the interference of node A's transmission. However, with MIMO, nodes B and D can successfully receive their desired signals from A and C, respectively, even nodes A and C transmit simultaneously. For illustration purpose, we assume that each node is equipped with two antennas. Node A uses its two antennas to send two weighted copies of its signal $s_1(t)$ to node B, and node C sends two weighted copies of its signal $s_2(t)$ to node D. Let $\mathbf{u}_A = [u_{A,1} \ u_{A,2}]^T$ and $\mathbf{u}_C = [u_{C,1} \ u_{C,2}]^T$ denote the encoding vectors of node A and node C, respectively. The resulting transmitted signal from nodes A will be $\mathbf{s}_A(t) = \mathbf{u}_A s_1(t)$, and the signal from node C will be $\mathbf{s}_C(t) = \mathbf{u}_C s_2(t)$. Let $\mathbf{v}_B = [v_{B,1} \ v_{B,2}]^T$ and $\mathbf{v}_D = [v_{D,1} \ v_{D,2}]^T$ denote the decoding vectors of node B and node D, respectively. Because node B is within the transmission ranges of both A and C, its received signal can be expressed as $r_1(t) = (\mathbf{v}_B^T \mathbf{H}_{A,B} \mathbf{u}_A) s_1(t) + (\mathbf{v}_B^T \mathbf{H}_{C,B} \mathbf{u}_C) s_2(t) + \mathbf{v}_B^T \mathbf{n}$, where $\mathbf{H}_{A,B}$ and $\mathbf{H}_{C,B}$ are the channel coefficient matrices between receiving node B and transmitting nodes A and C, respectively. Similarly, the received signal of node D is $r_2(t) = (\mathbf{v}_D^T \mathbf{H}_{A,D} \mathbf{u}_A) s_1(t) + (\mathbf{v}_D^T \mathbf{H}_{C,D} \mathbf{u}_C) s_2(t) + \mathbf{v}_D^T \mathbf{n}$, where $\mathbf{H}_{A,D}$ and $\mathbf{H}_{C,D}$ are the channel coefficient matrices between receiving node D and transmitting nodes A and C, respectively. Because node B has two antennas, its decoding vector \mathbf{v}_B can be chosen to let $\mathbf{v}_B^T \mathbf{H}_{C,B} \mathbf{u}_C = 0$ and $\mathbf{v}_B^T \mathbf{H}_{A,B} \mathbf{u}_A = 1$ so that the interference caused by node C's transmission can be suppressed, and node B receives an interference-free signal from its intended transmitter A. Similarly receiver D can reconstruct the signal from its intended transmitter C by choosing its decoding vector \mathbf{v}_D so that $\mathbf{v}_D^T \mathbf{H}_{A,D} \mathbf{u}_A = 0$ and $\mathbf{v}_D^T \mathbf{H}_{C,D} \mathbf{u}_C = 1$. In addition, transmitter A may select its encoding vector to nullify its interference to node D by ensuring $\mathbf{v}_D^T \mathbf{H}_{A,D} \mathbf{u}_A = 0$. So can node C null its interference to node B. In general, receivers can use their multiple antennas to suppress interferences caused by undesired nearby transmitters while successfully receiving their desired signals [8]. Transmitters can exploit their multiple antennas to

nullify their signals at undesired nearby receivers while ensuring acceptable signal gains at their desired receivers. Thus, with MIMO, the spatial reuse factor of spectrum is improved by letting multiple interfering links transmit simultaneously.

Although the MIMO techniques can provide appealing benefits, several issues need to be carefully considered when employing it. (1) To properly configure the encoding and decoding vectors, both transmitter and receiver should be aware of the instantaneous channel coefficient matrices. This is a common assumption [6, 7, 8, 9]. However even without such assumption, there exist practical estimation techniques that have already been applied in implementations and given fairly good results [12]. In addition, to keep the illustration simple and focused, we assume the channel coefficient matrices are all full rank. (2) The ability of MIMO to enable spatial multiplexing and interference suppression is not unlimited. Fundamentally, the number of concurrent streams that can be scheduled is constrained by the number of antennas, i.e. DoF of the transmitting node. Also, the number of streams a receiver can simultaneously receive is also limited by its number of antennas (DoF) [5]. We will careful consider the nodes' DoFs in scheduling the transmissions in Section 4.

Based on the above discussions, the DoFs of a MIMO radio can be exploited in one of the following three modes: (1) all DoFs are used to send a multi-stream flow of data by exploiting spatial multiplexing; (2) all DoFs are used to suppress the interference which allows multiple concurrent transmissions of multiple radios in a neighborhood; (3) some of DoFs are used to send a multi-stream flow while the others are used to suppress interference. The overall throughput under different MIMO operation modes is different. For the example in Fig. 1, if links AB and CD transmit in a TDMA fashion, that is, link AB active with 2 streams in time slot 1 and link CD active with 2 streams in time slot 2, the total throughput over 2 time slots is different from that as links AB and CD are both active in time slots 1 and 2, each transmitting one stream. This is because the throughput depends on channel matrices, encoding and decoding vectors which are all varying over time and depend on channel frequency. MIMO mode control, that is, arranging the DoFs of each radio (transmitting, receiving or suppressing interference) at a certain time slot, has a great impact to overall network performance.

3 Network Model

We study multi-SDR, multi-channel wireless mesh networks with MIMO links and assume the system is time-slotted. Each mesh node is equipped with one or more SDRs and multiple antennas. With multiple MIMO-enabled SDR interfaces, a node can flexibly access multiple orthogonal channels and transmit multiple MIMO streams on each channel simultaneously. Depending on implementation, multiple MIMO SDR interfaces at a node may share a set of antennas and some radio processing unit to save the cost. Each radio is capable of dynamically switching channels on a per-slot basis and forming MIMO links with neighboring radios if they are assigned on the same channel. We model the WMN network as a directed graph $G = (V, E)$ where V represents the set of nodes and E the set of directed links. If node u can transmit directly to node v , then we represent this by a link, $e = (u, v) \in E$.

We assume there are C orthogonal channels available in the network, numbered from 1 to C . Assume a node $u \in V$ has $N(u)$ SDRs and each SDR can operate on a channel assigned to it in a time slot. We denote by $F(u)$ the set of channels assigned to node u and $|F(u)|$ is the number of channels in $F(u)$ (obviously, $|F(u)| \leq N(u)$). A communication between two nodes u and v is possible only if there is a common channel among the sets $F(u)$ and $F(v)$. Thus we denote by $F(e) = F(u) \cap F(v)$ the set of channels that can be used by a link $e = (u, v)$.

If the transmitting and receiving radios of a MIMO link $e = (u, v)$ are equipped with K_u and K_v antenna elements, respectively, then there can be no more than $K_e = \min\{K_u, K_v\}$ concurrent streams over e on a channel. The receiver v can decode all K_e incoming streams from transmitter u successfully as long as the total number of streams (including the data streams from u and the interference streams from other nearby transmitters) is less than or equal to its number of antennas (DoFs). For ease of exposition, in this paper we assume that each node has K antenna elements.

The traffic and channel conditions on a wireless link may change very fast, for example, during a period of several packet transmissions. In general, the network layer should select the route of data flows based on long-term expected channel and traffic characteristics for network stability. Link layer and physical layer mechanisms account for instantaneous channel variations and traffic dynamics to exploit local transmission opportunities. Therefore, in this paper, we assume that the routing is established for a longer-term use, while channel assignment, scheduling, and MIMO mode control are dynamically adapted to varying channel and traffic conditions.

4 Stream Controlled Multiple Access (SCMA)

In this section, we present a scheme, called Stream Controlled Multiple Access (SCMA), which assigns the channels to radios, decides the set of simultaneous communications on each available channel i , ($i = 1, 2, \dots, C$) in a time slot t , as well as controls the MIMO operation mode of each active link in order to achieve efficient spectrum access and sharing among temporal, frequency, and spatial dimensions. For a time slot t , the SCMA scheme proceeds in two stages: (1) channel assignment for scheduling a set of non-interfering links for transmission on different channels, and (2) link pairing for taking advantage of MIMO mode control to improve performance. In the following, we assume that there are S data flows in the WMN, each propagating along a path from a source to a destination, and the paths of the flows in the network have been determined by a routing mechanism, e.g. AODV [10] or HWMP [11], at the network layer, for system stability.

4.1 Channel Assignment and Scheduling

A mesh node in the WMN can maintain per-flow queues for resource allocation. Consider a flow s passing through a link $e = (u, v)$ from node u to node v . The queue for flow s at nodes u and v are denoted by Q_u^s and Q_v^s , respectively. Let q_u^s and q_v^s denote the amount of data in the queues Q_u^s and Q_v^s , respectively, i.e. queue lengths.

Note that if the destination node of a flow can process packets fast enough, the queue length at the destination node is zero. Each per-flow queue at a node has an associated weight. The weight for queue q_u^s , denoted by w_u^s , is defined as $w_u^s = \max \{(q_u^s - q_v^s)r_e, 0\}$, where r_e is the transmission rate on the link $e = (u, v)$. That is, the per-flow queue weight is set to be the difference between the flow queue length at the current node and the associated flow queue length at the next hop node, multiplied by the data transmission rate between these two nodes. Actually the weight is a link oriented concept as it involves the two end nodes of a link. Let $s \in e$ denote all the flows that go through link e . Then the transmit queue length of link e at node u is $q_u^e = \sum_{s \in e} q_u^s$,

Let Ω denote the set of all link-channel pairs (e, i) , $e = (u, v) \in E$ and $i = 1, 2, \dots, C$, in the multi-channel MIMO WMN. We denote that r_e^i is the transmission rate of link e on channel i when all K DoFs are used for transmitting K MIMO streams with spatial multiplexing. We then define the weight of link-channel pair (e, i) to be $w_{(e,i)} = \sum_{s \in e} \max \{(q_u^s - q_v^s)r_e^i, 0\}$.

The first stage of SCMA is channel assignment and scheduling. We propose an algorithm in which the available channels are assigned to the links in the decreasing order of link-channel pair weights. In single-channel single-antenna networks, the greedy primal-dual algorithm [13] can approximately attain optimal network throughput. Our proposed algorithm extends the greedy primal-dual algorithm to multi-channel MIMO networks and uses it to perform channel assignment and scheduling.

Specifically, the following procedure is performed to assign channels to the links in time slot t .

- 1) Start from an empty schedule $M^i(t)$ for each channel i .
- 2) Search in the link-channel pair set Ω for the link-channel pair (e, i) with the largest weight $w_{(e,i)}$. Add (e, i) to $M^i(t)$, meaning that in the t -th time slot, link e will be scheduled for transmission on channel i . Correspondingly assign channel i to a radio at node u for transmitting and to a radio at node v for receiving, i.e., update $F(u)$ and $F(v)$ to include the newly assigned channel i , $F(u) = F(u) \cup \{i\}$ and $F(v) = F(v) \cup \{i\}$. Remove from the set of Ω the (e, i) pair. Set the new queue length of link e , $q_u^e(t+1) = q_u^e - r_e^i \tau$, where τ is the time slot length and recalculate $w_{(e,i')}, i' \neq i$ using $q_u^e(t+1)$.
- 3) Remove from the set of Ω all link-channel pairs (e', i) , where $e' \in I(e)$ is the set of links that can interfere with link e . Since channel i has been assigned to link e , link e' can no longer use channel i .
- 4) If $|F(u)| \geq N(u)$, which means node u has used up all its radios, then remove from Ω all the link-channel pairs (e'', i'') where e'' is any link incident (i.e. receiving or transmitting) on node u . Similarly, if $|F(v)| \geq N(v)$, remove from Ω all the link-channel pairs incident on v .
- 5) Repeat from step 2 until Ω is empty.

In the channel assignment stage, all effective DoFs on the transmitter and receiver are assumed to be used for the intended transmissions. Therefore, if a link is scheduled on the i th channel, no other links in its neighborhood can operate on the same channel without causing interference to this link. The channel assignment stage results in a

schedule in which interfering links can be active in a time slot only if each of them can be exclusively assigned a distinct channel. Otherwise, they have to be scheduled in different time slots. We refer to such scheduling algorithm as TDMA. By taking advantage of MIMO mode control, we could achieve better performance by scheduling interfering links to be active on the same channel in a time slot, each using partial number of DoFs to transmit and the remaining DoFs for interference suppression. We refer to this latter scheme as SCMA. SCMA adds link pairing stage after channel assignment.

4.2 Link Pairing

Some links are not scheduled in the channel assignment stage because no more channels are available, i.e. some other links in its interference range have higher weights and used up all available channels. If each of the nodes is equipped with multiple radios, an unassigned link represents a link between two nodes each of which has at least one unassigned/unused radio. With MIMO antenna technique, an unassigned link may share a channel with a neighboring link that has been scheduled in the previous channel assignment stage. For an unassigned link e' , we denote an assigned link in its neighborhood as e . If e and e' can both use partial number of DoFs for their respective transmissions and set aside enough DoFs for suppressing interference from the other, then e' can be scheduled in the same slot on the same channel as e . Note that if this happens, e can no longer transmit as many streams as its DoFs which was assumed in the channel assignment stage. MIMO mode control determines which MIMO transmission strategy should be used, letting e transmit with all its DoFs while keeping e' silent, or allowing e' and e transmit simultaneously, each using partial number of DoFs? The answer is whichever generates the better performance. Also if e' and e are both scheduled, how many and which antennas should be selected at each transmitter? The answers to these two questions are determined by the link pairing algorithm, which proceeds as follows.

- 1) All the unassigned links form a set U .
- 2) Search for the unassigned link $e' = (u', v')$ with the largest queue length in the set U .
- 3) On channel i , find a link paring candidate $e = (u, v)$ for link e' . A candidate link e must satisfy the following two conditions: (a) e is the only link within the interference range of link e' that has been scheduled on channel i in the channel assignment stage; (b) link e has not paired with another link.
- 4) If there exists no candidate link on channel i , continue with the next available channel. Otherwise, determine the set of antennas to be used at each transmitter of the two links e and e' . Calculate $w_{(e,i)}^{(A(e),A(e'))} = \sum_{s \in e} \max \{(q_u^s - q_v^s)r_e^{(i,A(e),A(e'))}, 0\}$ and $w_{(e',i)}^{(A(e'),A(e))} = \sum_{s \in e'} \max \{(q_{u'}^s - q_{v'}^s)r_{e'}^{(i,A(e'),A(e))}, 0\}$, i.e. the weights of the link-channel pair (e, i) and (e', i) with $A(e)$ and $A(e')$ being the set of antennas selected at the transmitters of e and e' , respectively, for transmitting data streams. Here $r_e^{(i,A(e),A(e'))}$ and $r_{e'}^{(i,A(e'),A(e))}$ denotes the transmission rates of links e and e' on channel i when the sets of antennas selected by the transmitters of e and e' are $A(e)$ and $A(e')$, respectively. Since

links e and e' interfere each other, their data rates depends on the antenna selections at both the transmitters. The criterion for antenna selection is to jointly optimize the total weight of two links (e, i) and (e', i) , i.e., $\max_{|A(e)|+|A(e')|\leq K} \{W_{(e,i)}^{(A(e),A(e'))} + W_{(e',i)}^{(A(e'),A(e))}\}$. At each transmitter of e and e' , an independent data stream is transmitted from each selected antenna. The total number of transmitted data streams should be less or equal to the DoF, that is, $|A(e)| + |A(e')| \leq K$.

- 5) Perform steps 3 and 4 on each available channel.
- 6) Link e' may find qualifying candidates on multiple channels. Select the most qualifying candidate, i.e., the candidate which results in the largest maximal total weight of the two links, and pair link e' with this selected link (assuming it is e), i.e., scheduling e' and e to transmit simultaneously on the same channel, each using the MIMO antenna mode determined in step 4.
- 7) Assume the selected candidate link e operates on channel i , then link $e' = (u', v')$ also operates on channel i . Assign channel i to node u' and node v' , Update $F(u') = F(u') \cup \{i\}$ and $F(v') = F(v') \cup \{i\}$.
- 8) Add link e' to $M^i(t)$, meaning that in the t -th time slot link e' can be active on channel i using the MIMO antenna mode determined in step 4. Also update the selected pairing link e that has been added in $M^i(t)$ in the channel assignment stage with the new MIMO mode determined in step 4. After pairing, link e may not be able to transmit with K MIMO streams as assumed in the first stage because it has to share the same channel with link e' . The total number of MIMO streams transmitted by link e' and link e should not exceed the DoF K .
- 9) Update the queue length of link e' and link e , $q_u^{e'} = q_u^{e'} - r_{e'}^{(i,A(e'),A(e))} \tau$, and $q_u^e = q_u^e - r_e^{(i,A(e),A(e'))} \tau$ where τ is the time slot length.
- 10) If $|F(u')| \geq N(u')$ which implies node u' has used up all its radios, remove from U , all the links incident on u' . Similarly, if $|F(v')| \geq N(v')$ which implies node v' has used up all its radios, remove from U all the links incident on v' .
- 11) It is possible that link e' cannot find a link to pair with. If so, link e' is not scheduled to transmit in this time slot and removed from the set U .
- 12) Repeat from step 2 until the set U becomes empty.

After the link paring stage, the two interfering links may be active simultaneously on the same channel under the constraint that the total number of streams is not greater than the effective degrees of freedom at respective receivers. In addition, when a link e is schedule to transmit, the transmitter will send the packets belonging to different flows $s \in e$ on link e in a round-robin fashion to allocate equal resource and maintain fairness among the flows sharing the link.

5 Performance Evaluation

In this section, we compare the performance of the proposed SCMA scheme with TDMA scheme under different network scenarios, and unveil the impact of system

parameters to the performance with simulation results. In TDMA, a link uses all the DoFs for transmitting or receiving, and interfering MIMO links either operate in different time slots or on different channels. With SCMA, interfering MIMO links may simultaneously be active on a channel through the proposed link paring algorithm. We consider a channel path loss model with a path loss exponent of 4 in our simulations and assume the channel bandwidth is 10MHz.

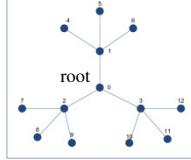


Fig. 2. Tree topology used in simulation

We first consider a tree network with one root node and 12 other nodes as shown in Fig. 2. Tree networks are often used in backhaul WMNs in which the root node is an Internet gateway and the other nodes are mesh routers. The distance between two neighboring nodes on the tree is all 200 meters. We assume each mesh node equipped with only one software-defined MIMO radio capable of switching channels on a per-slot basis and K antennas, and all the mesh radios transmit at a fixed power. We randomly generate channel matrix between each node pair with each of its entries being i.i.d. Gaussian distributed with zero mean and unit variance. We assume there is a traffic flow from each mesh node to the root. For fairness, we seek max-min fairness of all the 12 traffic flows in the network. It is expected that with max-min fairness, the traffic flows sharing a link will be allocated equal resources, that is, equal packet transmission opportunity on the link. We repeat the experiment 100 times for each scenario, each with randomly generated channel matrices. We average the per-flow throughput on the 100 experiments and present the results.

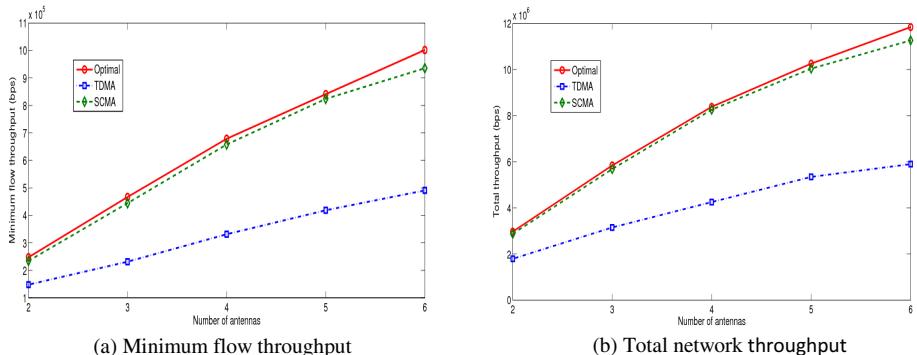


Fig. 3. Minimum flow throughput and total throughput vs. the number of antennas

We first investigate the impact of the number of antennas on the network performance. We vary the number of antennas from 2 to 6 and assume there are two available channels in the network. Fig. 3 shows the achievable total network throughput and minimum flow throughput. We see that SCMA can achieve much larger minimum flow throughput and total network throughput than TDMA. The performance of SCMA is very close to the performance of an ideal case. For the ideal case, we assume that the transmission rate of a link is equivalent to the single point-to-point link capacity in the absence of interference from neighboring transmissions. We also observe that the throughput is nearly a linearly increasing function of the number of antennas.

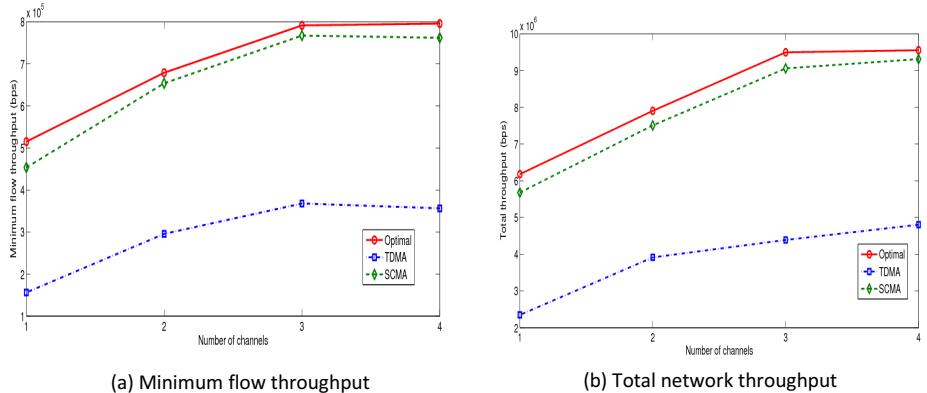


Fig. 4. Minimum flow throughput and total throughput vs. the number of channels

Next we study the impact of number of available channels on network performance. We vary the number of available channels. We present the minimum flow throughput and total network throughput in Fig. 4. As expected, both minimum flow throughput and total network throughput are increasing with the number of available channels. SCMA outperforms TDMA and its performance is very close to the performance of the ideal case.

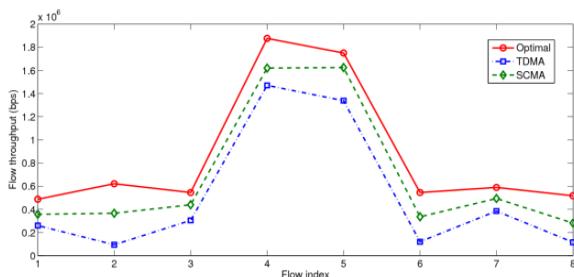


Fig. 5. Per-flow throughput of 20 node random network

Finally we evaluate the performance of TDMA and SCMA in a network with random topology. We randomly place 20 wireless nodes in a square area of $800 \times 800 \text{ m}^2$. We generate 8 data flows with sources and destinations randomly selected. We repeat the experiment 100 times, in each of which channel matrices are randomly generated. The flow throughput for each of the flows averaged over 100 experiments is given in Fig. 5. We observe that SCMA also outperforms TDMA in this scenario. The performance gap between the SCMA and the ideal case is a little bit larger in this random network than in the tree network due to greater impact of interference.

6 Conclusions

In this paper, we proposed a cross-layer scheme, called Stream Controlled Multiple Access (SCMA), for multi-hop multi-channel WMNs, which is responsible for scheduling links and assigning channels to transmit and controlling the MIMO operation mode in every time slot. SCMA enables efficient spectrum access and sharing among temporal, frequency, and spatial dimensions, and adapts to varying network conditions. The evaluation results show that the proposed SCMA scheme greatly improve the network performance compared to the traditional TDMA scheme.

References

1. Gupta, P., Kumar, P.R.: The Capacity of Wireless Networks. *IEEE Transactions on Information Theory*, IT 46(2), 388–404 (2000)
2. Raniwala, A., Chiuh, T.: Architecture and Algorithms for an IEEE 802.11-based Multi-Channel Wireless Mesh Networks. In: IEEE Infocom 2005, Miami (2005)
3. Alicherry, M.R., Bhatia, R., Li, L.: Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks. In: Proc. ACM MOBICOM (2005)
4. Biglieri, E., Calderbank, R., Constantines, A., Goldsmith, A., Paulraj, A., Poor, H.V.: MIMO Wireless Communications. Cambridge University Press (2007)
5. Spencer, Q., Swindlehurst, A., Haardt, M.: Zero-forcing Methods for Downlink Spatial Multiplexing in Multiuser MIMO Channels. *IEEE Trans. Signal Process.* 52(2), 461–471 (2004)
6. Liu, J., Shi, Y., Hou, Y.: A Tractable and Accurate Cross-Layer Model for Multi-Hop MIMO Networks. In: IEEE INFOCOM, New York (2010)
7. Yazdanpanah, M., Assi, C., Shayan, Y.: Cross-Layer Optimization for Wireless Mesh Networks with Smart Antennas. *Computer Communications*, 1894–1911 (2011)
8. Hamdaoui, B., Shin, K.G.: Maximum Achievable Throughput in Multiband Multi-Antenna Wireless Mesh Networks. *IEEE Trans. on Mobile Computing* 9(6), 838–849 (2010)
9. Bansal, M., Trivedi, A.: Cross-Layer Optimization of Multichannel Multiantenna WMNs. *Wireless Pers. Commun.* 71, 1443–1459 (2013)
10. Belding-Royer, E., Perkins, C., Das, S.: Ad Hoc On-Demand Distance Vector (AODV) Routing. In: RFC 3561, Internet Engineering Task Force (2003)
11. IEEE 802.11s Working Group: Mesh Networking. In: IEEE 802.11s Standard (2009)
12. Gollakota, S., Perli, S.D., Katabi, D.: Interference Alignment and Cancellation. In: Proc. ACM SIGCOMM (2009)
13. Stolyar, A.: Maximizing Queueing Network Utility Subject to Stability: Greedy Primal-Dual Algorithm. *Queueing Systems* 50(4), 401–457 (2005)

Minimized Gateway Placement in Hybrid Wireless Network

Hao Wang and Hong Gao

Department of Computer Science, Harbin Institute of Technology,
Harbin, Heilongjiang, China, 150001
whao0218@outlook.com, honggao@hit.edu.cn

Abstract. Heterogeneous wireless networks coexisting in a common area become conventional. Communication between different types of wireless network can only be achieved by utilizing wireless gateways. In this paper, we address the problem of gateway placement for satisfying the bandwidth-requirement of each node by using minimum gateways. This problem can be formulated as a variant of Minimum Geometric Disk Cover problem which has been proved NP-complete. In order to solve our problem, one heuristic gateway placement algorithm and one grid-based greedy algorithm are proposed. The result of simulation demonstrates that the heuristic algorithm can offer a good solution with big probability.

1 Introduction

Due to the rapid development of wireless communication technology, today, wireless network with multi-wireless technology coexisting become familiar [1]. Bluetooth, WiFi, Zigbee, cellular wireless communication technologies have been widely employed by modern wireless devices. These technologies according to its technique features play different role in people's life and in the near future, it is hard to make these technologies unification.

Different wireless communication technologies are complementary but also bring challenges. One of the biggest is these technologies can't make communications mutually. But the requirement of intercommunication is increasingly. To enable every wireless device equip with all these technology is costly and add new wireless technology to existing terminal is almost impossible. Gateway is a device whose basic functions are data distribution and aggregation [2]. Gateway can be designed to communicate with multi-technology wireless network [3][4]. Under this condition, to connect these heterogeneous technologies together, gateways are indispensable.

To achieve better performance in a hybrid wireless network, the placement of gateways must be carefully studied. In wireless mesh network (WMN) [5], gateway placement problem attracts considerable attentions. In WMN, gateway placement application scenario can be described as: The mesh nodes are deployed on the roof of houses in a neighborhood, which serve as access points for users inside the homes and along the roads. All these mesh nodes are fixed and form the mesh network. The mesh

service provider needs to decide where to place the gateway devices to connect the mesh network to the Internet. Since different gateway placement causes different mesh backbone topology and cost, it is important to find optimal gateway placement to minimize the total cost while ensuring the quality of service, e.g., coverage. This application is similar with gateway placement in hybrid wireless network.

Traditional multi-hop wireless network has several problems in modern wireless network. Take an example of people who using wireless devices, it is hard to believe that a person would like to transfer other's packets as well as let his packets be transferred by others. Taking battery and privacy to one's concern, multi-hop is not that convenient and credible.

Gateway placement studies in WMN often consider multi-hop wireless networks [6–8]. And they mainly consider the hybrid network of wired-wireless network [9], hybrid network with two different types of wireless technologies is rarely addressed.

In this paper, we consider a scenario that there is an area, in where randomly located two kinds of wireless nodes equipped with different wireless communication technologies. These two kinds of nodes have the requirement of communication with different type nodes and the internet. Gateways are used to fulfill their communication needs. For quality of service demands, each node must keep in touch with gateways and obtain a regular bandwidth. A gateway has limited capacity of providing bandwidth to the nodes connected to it. All the nodes in this area must be covered by a gateway. We investigate where to place the gateways can minimize the number of gateways placed.

The contributions of our work are as follows:

1. We consider the minimizing gateway placement problem in a hybrid wireless network with two different kinds of wireless communication technologies.
2. We propose a heuristic algorithm and a greedy method to address the problem.
3. Finally, we make simulations to evaluate our method. And the results of simulations demonstrate our method is effective.

The paper is organized as follows. We discuss the related work in Section 2. The network models and some assumptions are given in Section 3. Our problem definition is in Section 4. In Section 5, we propose our two algorithms. Simulation is in Section 6. Conclusions and future work are given in Section 7.

2 Related Work

Bejerano [10] studied gateway placement in multi-hop wireless networks where network nodes were partitioned into minimal number of disjoint clusters that satisfied throughput and delay constraints. Various gateway or backbone nodes placement algorithms were proposed for WMNs [11–13]. However, all the above investigation has been focused on network connectivity of WMNs by selecting a minimum number of fixed positions.

The capacity of hybrid ad hoc networks was investigated in [14-16]. All the above throughput results have been obtained as asymptotic value by assuming that the size of the network goes to infinity. In practice the above assumption can't be satisfied.

3 Model and Assumption

There are three kinds of nodes in our network models. One of them is gateway nodes represented by $G=\{g_1, g_2, \dots, g_k\}$. And the other two are client nodes $A=\{a_1, a_2, \dots, a_n\}$ and client nodes $B=\{b_1, b_2, \dots, b_m\}$. A and B require to communicate mutually, and access to the internet. These communication demands are fulfilled by making client nodes connected with gateways. Gateways are wired connected with each other and access to external network. Every node a_i or b_i is directly connected with the designated gateway node.

Gateway Node Model: The network capacity of each single gateway g_i is W_{ga} bps for nodes A and W_{gb} bps for nodes B . And every gateway node g_i can offer M_a orthogonal channels for nodes A and M_b orthogonal channels for nodes B . All the gateways nodes share the same channels.

Client Node Model: Every node of A and B requires bandwidth of W_a bps and W_b bps, respectively, and they need to keep the connection with its associated gateway node. Communication between two types of nodes can only be realized by connecting them to gateway nodes. As mentioned in 3.1, each node a_i or b_i has the ability to utilize M_a or M_b orthogonal channels, and its transmission range is R_a or R_b respectively. In our paper, we set $R_a \geq R_b$.

Interference Model: Signal from different types of nodes will not interfere mutually. And signal from the same kind of nodes will generate interference only when they are in the same channel. Every node has an interference range. For convenience, let interference range equal to its transmission range. So when $\|a_i - a_j\| < R_a$ ($\|b_i - b_j\| < R_b$) and the two nodes are using the same channel, interference will be caused.

4 Problem Definition

Consider an L meters by W meters area in which nodes $A=\{a_1, a_2, \dots, a_n\}$ and nodes $B=\{b_1, b_2, \dots, b_m\}$ have been random placed. Bandwidth for communication with gateways required by each a_i or b_i is W_a bps or W_b bps. All nodes A take advantage of M_a orthogonal channels to communicate with gateways and nodes B use M_b conflict-free channels for communication. Every gateway g_i can offer W_{ga} (W_{gb}) bps for all the nodes A (B) that connected to g_i . Our object is to select positions to place gateways $G=\{g_1, g_2, \dots, g_k\}$ in order to minimize k and guarantee all the nodes obtain their required bandwidths.

Our problem can be formulated as follows.

Given two sets in the Euclidean plane, set $A=\{a_1, a_2, \dots, a_n\}$ of n points, set $B=\{b_1, b_2, \dots, b_m\}$ of m points. Every point has a location (x_i, y_i) . We wish to select

locations to place a minimum set $G=\{g_1, g_2, \dots, g_k\}$ of k points to cover set A and set B , a_i or b_i is covered by g_i means $\|a_i - g_i\| \leq R_a$ or $\|b_i - g_i\| \leq R_b$, and the number of points of A or B covered by g_i must be less than W_{ga}/W_a or W_{gb}/W_b .

There is an additional restrict of node density on the plane. Because the number of orthogonal channel is limited, when the density of nodes is more than a threshold, the signal of each other node will interfere mutually. The threshold doesn't have to be number of physical channels. There are many techniques to enhance the ability of concurrence wireless communication, such as TDMA or CDMA. These technologies increase the number of actual available channels. We call these channels orthogonal channels. So the threshold can be demonstrated like this: In any circle with a node as center and transmission radius as radius, there can not be more than M_a or M_b , depend on nodes type, nodes. This can be proven easily by using pigeonhole principle.

This problem can be seen as a variant of Minimum Geometric Disk Cover problem which is NP-complete [17]. The Minimum Geometric Disk Cover problem is to find a set of unit disks of minimum cardinality whose union covers a given set of points in the plane, and the disk centers is located at any position in the plane [18].

Obviously our problem is not easier than the Minimum Geometric Disk Cover problem. So at least, our problem is NP-complete.

5 Algorithms

In this section, we propose two methods to determine the locations of gateways.

5.1 Algorithm 1. Farthest Node First Cover(FNFC)

To deal with the asymmetry of nodes distribution, we consider to find an origin of our gateway placement strategy and a direction to move on. The origin in this strategy is one of the farthest two nodes on the plane. And we conduct the gateway placement from the origin to the other one which we call it destination point (DP). In the process of gateway placement, DP is fixed. The strategy will iteratively find the node whose distance to the DP is longest. We call the farthest node the start point (SP).

After SP has been located, we calculate the intersection of two circles. One takes SP as its center, and the other one will take each of the nodes adjacent to SP as its center. Their radiiuses are the transmission radiiuses of the central nodes. If the two circles have two intersections, the one closer to DP will be reserved. When there is only one intersection, it will be reserved. In a few cases that the distance between two centers is shorter than the discrepancy of their radiiuses, there will be no intersection. In this case, we replace the longer radius with shorter one, and calculate their intersection again. In all the intersections we reserved, the one whose distance to the segment (DP, SP) is longest will be selected to arrange a gateway. In accordance with the order of distance to SP , we mark the nodes which can be covered by the gateway. The algorithm repeats above process until all nodes are marked.

Take Fig.1 as example. There are two kinds of nodes on the plane, and they indicated as blue points or red points. Their transmission radius is R_A or R_B . Firstly,

the algorithm finds out the farthest two points on the plan. As shown in the figure, they are point D and point S . We take S as Start Point and D as Destination Point. Then we make circles with S and its adjacent points as center, and their transmission radiuses as radius. Circles with adjacent points as center will intersect the circle with S as center. If the two circles have two intersections, we keep the one with shorter distance to D . Among all the kept intersections, we select point O to arrange a gateway, because O is the nearest point to segment DS . In the next step, depending on their type, nodes in the solid circle will be marked, blue points in the blue circle, red points in the red circle. If the number of nodes $A(B)$ in the circle is more than W_{ga}/W_a (W_{gb}/W_b), we mark the nodes whose distance to point D is farther. And then, the algorithm will take the farthest point to point D among the unmarked as new Start Point. The algorithm repeats this process until all nodes have been marked. The time complexity of FNFC is $O((m+n)^2)$, $n = |A|$ and $m = |B|$.

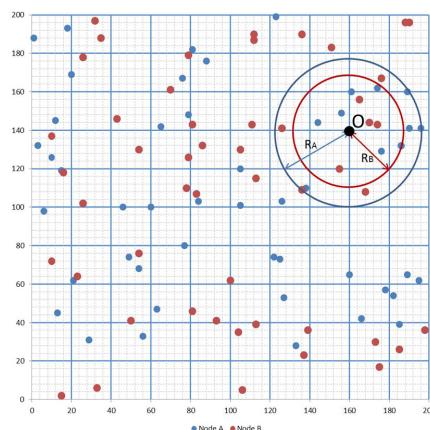


Fig. 1. Demonstration of FNFC: D is DP; S is SP; O is the position to place gateway

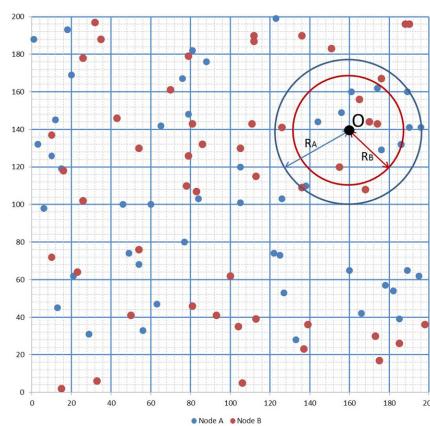


Fig. 2. Demonstration of GBGC: O is the intersection to place gateway

Algorithm 1. FNFC

Input: Node set $N = \{n_i = (x_i, y_i) | 0 \leq i \leq n+m\}$ with transmission radius R_i on Plane P . $N = A \cup B$ $A = \{a_i = (x_i, y_i) | 0 \leq i \leq n\}$ and $B = \{b_i = (x_i, y_i) | 0 \leq i \leq m\}$. R_i is R_a when $n_i \in A$ and R_b when $n_i \in B$. Bandwidth requirement W_a and W_b for a_i and b_i and Gateway bandwidth W_{ga} and W_{gb} for a_i and b_i

Output: $G = \{g_i = (x_i, y_i) | 0 \leq i \leq k\}$

1. Calculate the distance between any two nodes
2. Find the farthest two nodes n_s and n_d
3. Let $SP = n_s$, and $DP = n_d$
4. For all n_i , calculate $\|n_i - n_s\|$; if $\|n_i - n_s\| \leq R_i + R_s$, add n_i to point set Q .
5. Calculate the intersections of circle with n_s as center and circle with each $q_i \in Q$ as center, radius is R_s and R_{qi} . If the intersections do not exist, go to 6; If there is only one intersection $c_{il}(x_{il}, y_{il})$, add c_{il} to point set P ; If there are two intersections $c_{il}(x_{il}, y_{il})$ and $c_{i2}(x_{i2}, y_{i2})$, add the one whose distance to n_d is shorter to point set P .
6. If n_s and q_i belong to different node set and $\|n_s - q_i\| < R_a - R_b$, let R_b be their radius, return to 5.
7. For all nodes in P , calculate $\|p_i - n_d\|$; Let $g_i = p_m$, where $\|p_m - n_d\| = \max \{\|p_i - n_d\|\}$
8. Add n_i , where $\|n_i - g_i\| \leq R_i$, to node set C_A when $n_i \in A$ or C_B when $n_i \in B$.
9. Sort C_A and C_B order by $\|n_i - n_d\|$. Keep the last W_{ga}/W_a and W_{gb}/W_b points in C_A and C_B , remove the other.
10. Mark nodes in C_A and C_B .
11. Check each n_i ; If all nodes are marked, algorithm terminated; Else go to 12
12. Choose the farthest node to DP as new SP from the unmarked nodes; Go to 3.

5.2 Algorithm 2. Grid-Based Greedy Cover(GBGC)

Here we propose a more intuitional method to arrange gateways. We divide the area into grids with diagonal length R_b , so when we place gateways on the intersections, whole area can be covered and no node will be missed. GBGC will try all the intersections to place gateway, and select one where the gateway can cover maximum number of nodes to be the final position. GBGC iterates above process till all nodes have been covered. Fig.2 is an example of how to select an intersection to place gateway. This gateway placement method is much easier to be realized compare to FNFC. So it is a reasonable choice at a quick-deployment situation. The time complexity is $O(k(n+m)^2)$, k is the number of grids.

6 Simulation

In this section, we conduct several simulations to study the performance of FNFC and GBGC. We compare the solutions of FNFC and GBGC under different conditions, and the results shows that FNFC will give better solutions in most case.

6.1 Simulation Setup

We consider an area of 200 meters by 200 meters. Node A and Node B have been randomly placed in this region. R_a is set to 30 meters and R_b is set to 25 meters. And we set $W_{ga}/W_a = 20$, $W_{gb}/W_b = 15$, $Ma = 25$ and $Mb = 20$, if there is no additional statement.

6.2 Results Discussion

In first kind of simulation, we increase the sum of nodes A and nodes B from 100 to 1000, and number of nodes A equals to number of nodes B . As shown by figure 3, gateways generated by FNFC are much fewer than GBGC. And the difference becomes small when nodes number increased. Also, number of gateways generated by FNFC and GBGC both increased along with the growth number of nodes. The velocity of increase is slow down when the amount of nodes become large. This is because as the number of nodes increasing, gateways generated by both algorithms have covered nearly the whole area. In this case, nodes added to the region have great probability to fall in the scopes of gateways already there. It's also the reason why the numbers of gateways generated by two algorithms become closer.

Fig.4 shows the nodes covered rate when we adopting random gateway placement method. We randomly place the same number of gateways generated by FNFC into the area. For each number of nodes, we conduct one hundred times random gateway placement, and calculate the average value of cover rate. When the number of nodes is small, random placement misses a large amount of nodes. Such situation becomes better when the number of nodes increased, since we have placed more gateways. But random placement rarely covers more than ninety percent of nodes.

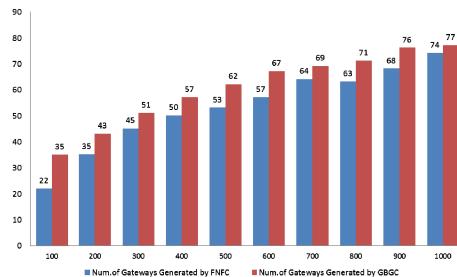
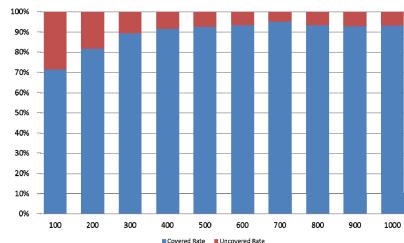
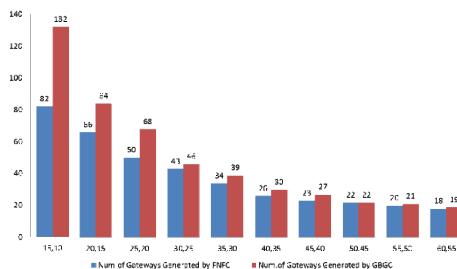
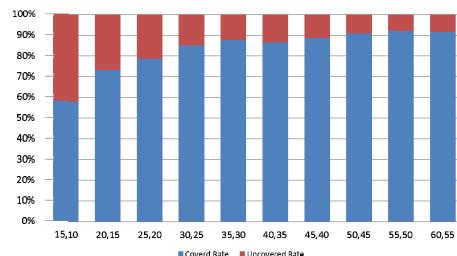
In second kind of simulation, we fix the number of two types of nodes and increase the transmission radius, R_a from 15 meters to 60 meters, R_b from 10 meters to 55 meters. The results is shown in Fig.5.

When the radius is very short, the difference between results of two algorithms is significant. Gateways generated by FNFC are as few as sixty percent of GBGC. With radius rising, numbers of gateways generated by two algorithms become similar. The reason is similar with first kind simulation. As radius growing, arranged gateways will cover most area of the region. Thus the position of each gateway will make less different. Results of randomly placement can also been interpreted, shown in fig.6.

In third simulation, we fix sum of nodes A and nodes B , and change the ratio between nodes A and nodes B , from $A:B = 0:10$ to $A:B = 10:0$. We conduct such simulate to see the algorithm's sensitivity to the difference between W_{ga}/W_a and W_{gb}/W_b . The results is shown in fig.7.

The number of gateways is downtrend, because W_{ga}/W_a is bigger than W_{gb}/W_b . That means one gateway is able to cover more nodes A than nodes B . When number of nodes B declined and number of nodes A increased, fewer gateways are required.

In fourth kind of simulation, we fix the number of nodes A as 150, and so does the number of nodes B . We conduct twenty times of each algorithm with different distributions of nodes in the area. Fig.8 shows the results. From fig.8, we find that distribution has obvious influence on the results of two algorithms. With one of these node distribution, GBGC can achieve nearly the same performance of FNFC. But most of the cases, FNFC is much better than GBGC.

**Fig. 3.** Number of Gateways Generated by FNFC and GBGC**Fig. 4.** Nodes Covered and Uncovered Rate in Random Gateway Placement**Fig. 5.** Number of Gateways Generated by FNFC and GBGC**Fig. 6.** Nodes Covered and Uncovered Rate in Random Gateway Placement

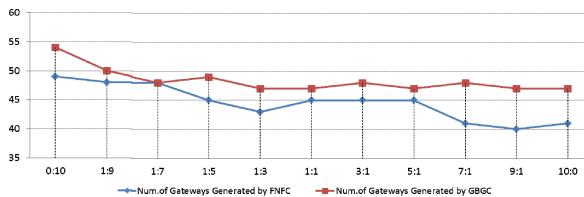


Fig. 7. Gateways generated by two algorithms with different ratio between A and B

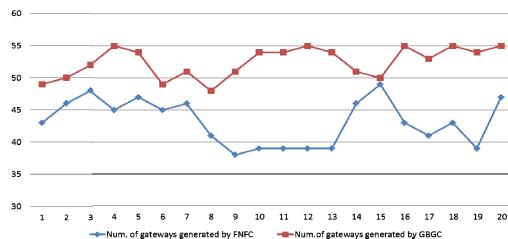


Fig. 8. Results of two algorithms with different nodes distribution

7 Conclusion and Future Work

In this paper, we investigated the minimizing gateway placement problem in hybrid wireless network. We proposed two algorithms to address the problem. The effective of the algorithms has been evaluated by our simulations. Our method can offer a good solution containing a small number of gateways. Actually, the situation will be more complicated. And much more work and analysis need to do to adapt such conditions.

Acknowledgements. This work was partially supported by the National Natural Science Foundation of China (NSFC) under Grant No.61190115, 61033015, the National Science Foundation Distinguished Young Scholars of China under Grant No.61300225.

References

1. Becchetti, L., Delli Priscoli, F., Inzerilli, T., Mahonen, P., Munoz, L.: Enhancing IP service provision over heterogeneous wireless networks: a path toward 4G. *IEEE Communications Magazine* 39, 74–81 (2001)
2. Hwang, K., In, J., Park, N., Eom, D.: Sensor Information Networking Architecture and Applications. *IEEE Personal Communications* 8 (August 2001)
3. Hwang, K., In, J., Park, N., Eom, D.: A design and Implementation of Wireless Sensor Gateway for Efficient Querying and Managing through World Wide Web. *IEEE Trans. on Consumer Electronics* 49 (November 2003)

4. Baird, S., Dawson-Haggerty, S., Myung, D., Gaynor, M., Welsh, M., Moulton, S.: Communicating Data from Wireless Sensor Networks Using the HL7v3 Standard. In: Proceedings of BSN (April 2006)
5. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. *Computer Networks* 47(4), 445–487 (2005)
6. Li, F., et al.: Gateway placement for throughput optimization in wireless mesh networks. *Mobile Networks and Applications* 13(1-2), 198–211 (2008)
7. Jamin, S., Jin, C., Kurc, A., Raz, D., Shavitt, Y.: Constrained mirror placement on the Internet. In: Proc. of IEEE INFOCOM (2001)
8. Chandra, R., Qiu, L., Jain, K., Mahdian, M.: Optimizing the placement of internet TAPs in wireless neighborhood networks. In: Proceedings of the 12th IEEE International Conference on Network Protocols ICNP 2004 (2004)
9. Muthaiah, S.N., Rosenberg, C.: Single gateway placement in wireless mesh networks. In: Proc. of 8th International IEEE Symposium on Computer Networks, Turkey (2008)
10. Bejerano, Y.: Efficient integration of multi-hop wireless and wired networks with QoS constraints. In: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, MOBICOM (September 2002)
11. Srinivas, A., Zussman, G., Modiano, E.: Mobile backbone networks-construction and maintenance. In: Proceedings of the International Symposium on Mobile AdHoc Networking and Computing (MobiHoc 2006), pp. 166–177 (2006)
12. So, A., Liang, B.: Minimum cost configuration of relay and channel infrastructure in heterogeneous wireless mesh networks. In: Akyildiz, I.F., Sivakumar, R., Ekici, E., de Oliveira, J.C., McNair, J. (eds.) *NETWORKING 2007. LNCS*, vol. 4479, pp. 275–286. Springer, Heidelberg (2007)
13. Wang, J., Xie, B., Cai, K., Agrawal, D.P.: Efficient mesh router placement in wireless mesh networks. In: Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems, MASS 2007 (2007)
14. Liu, B., Liu, Z., Towsley, D.: On the capacity of hybrid wireless networks. In: Proc IEEE INFOCOM (2003)
15. Kozat, U.C., Tassiulas, L.: Throughput capacity of random ad hoc networks with infrastructure support. In: Proc. ACM MOBICOM 2003 (2003)
16. Zemlianov, A., de Veciana, G.: Capacity of ad hoc wireless networks with infrastructure support. *IEEE J. Sel. Areas Commun.* 23(3), 657–667 (2005)
17. Fowler, R.J., Paterson, M.S., Tanimoto, S.L.: Optimal packing and covering in the plane are NP-complete, *Inform. Process. Lett.* 12, 133–137 (1981)
18. Acharyya, R., Das, G.K.: Unit disk cover problem. arXiv preprint arXiv:1209.2951 (2012)

Design and Analysis of a Downlink Multi-User MIMO MAC Protocol in WLANs

Chao Guo, Changle Li*, and Huiying Liu

State Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an, Shaanxi, 710071 China
clli@mail.xidian.edu.cn

Abstract. Equipped with multiple antennas, Access Point (AP) can simultaneously communicate with multiple nodes in WLANs, which is called Multi-User Multi-Input Multi-Output (MU MIMO). The traditional IEEE 802.11 Distributed Coordination Function (DCF) protocol cannot take benefit of the multiple simultaneous downlink transmission. Instead, it may be the bottleneck of improving the system performance. Therefore, we propose a Downlink (DL) MU MIMO MAC protocol which extends DCF to the downlink MU MIMO scenario. A Markov chain model is utilized to analyze the performance of the proposed protocol under saturated conditions. By modeling the channel access actions of AP and each node respectively, we can obtain the access delay of AP. We also simulate the proposed protocol in MATLAB. Both the theoretical analysis results and simulation results confirm that the proposed protocol outperforms DCF in terms of the delay and throughput.

Keywords: WLAN, MU, MIMO, MAC, Markov chain.

1 Introduction

To avoid the strong interferences from other networks around using the commonly spectrum such as 2.4GHz and 5GHz, IEEE 802.11ah [1] came into existence, using sub-1 GHz [2] spectrum. IEEE 802.11ah evolved from IEEE 802.11n and 802.11ac to be applied in large scale wireless networks [3, 4]. The 802.11ah specification shall support MU-MIMO feedback structure and protocol as specified in IEEE P802.11ac [5], as an optional feature. The traditional Medium Access Control (MAC) protocols [6, 7] only allow a data transmission in the same time slot, which just improves the communication rate and does not maximize the space multiplexing gain [8].

The research of multi-user MIMO based WLANs is divided into two directions, that is, the uplink transmission [9] and downlink transmission. [10] proposes a MAC protocol with multiuser MIMO techniques with a k-subset round robin policy. A distributed MU MIMO MAC protocol is proposed in [11]. The protocol can be applied to the multi-user scenario with additional timing overhead in its uplink

* Corresponding author.

transmission. The authors of [12] explain the reason why TXOP (Transmit Opportunity) does not support DL MUMIMO transmission. Because the existing rules in EDCA (Enhanced Distributed Channel Access) [13, 14] would not allow the simultaneous transmission of multiple frames belonging to different ACs, which limits the usefulness of the DL MU-MIMO technology.

In this paper, we focus on the extension of DCF to support DL MU MIMO technology. A DL MU MIMO MAC protocol is proposed here, which is applied to the scenario that users have one antenna while AP is equipped with multiple antennas. Therefore, the proposed protocol should consider the selection of packets transmitted simultaneously in the downlink transmission. Another problem is how AP simultaneously reserves the channel with different nodes. Our protocol is proposed by taking the above issues into account. The theoretical analysis and simulation results prove that our protocol can decrease the delay and increase throughput.

The rest of this paper is organized as follows. Section 2 introduces the specific scheme. In Section 3, we utilize a Markov chain to analyze the performance of the proposed protocol in terms of the average access delay. The numerical results of the analysis and simulation are shown in Section 4. Section 5 concludes the paper.

2 The DL MU MIMO MAC Protocol

2.1 Application Scenario

We mainly study the design of downlink Multi-user Multi-Input Multi-Output Medium Access Control (MAC) protocol. We consider the scenario that AP is equipped with multi-antenna, while each node just has an antenna. The application scenario is shown in the Fig. 1.

Assume that there are n nodes and one AP in a single-hop fully-connected network. AP is equipped with M antennas ($M < n$) and each node has one antenna. AP transmits data to n nodes in downlink. In our application scenario, $H = \begin{bmatrix} h_1^T & h_2^T & \dots & h_n^T \end{bmatrix}^T$ is the channel matrix, where $h_i = (h_{i1} \ h_{i2} \ \dots \ h_{iM})$ is used to represent the channel gains from M antennas of the AP to the i -th receiver antenna. AP utilizes RTS to reserve the channel with different nodes so that it can transmit simultaneously M spatial data streams to a maximum of M STAs.

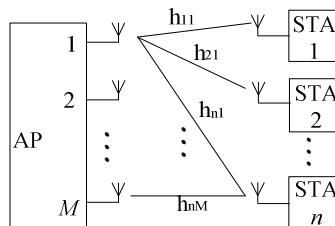


Fig. 1. Application scenario

2.2 Extension of the RTS/CTS Channel Access Method

The proposed MAC protocol extends the RTS/CTS access method of IEEE 802.11 DCF to support DL MU MIMO. The RTS frame in IEEE 802.11 DCF has only one receiver field. Therefore, there is only a single receiving node during each data transmission. To support AP to reserve the channel with multi-node, we modify the frame format of RTS, making it have M receiver fields. Fig. 2 shows the original frame format of RTS, while Fig. 3 illustrates the modified frame format.

Frame Control	Duration	RA	TA	FCS
---------------	----------	----	----	-----

Fig. 2. Original frame format of RTS

Frame Control	Duration	RA ₁	...	RA _M	TA	FCS
---------------	----------	-----------------	-----	-----------------	----	-----

Fig. 3. Modified frame format of RTS

Assume that the packets have the same length. Before AP reserves the channel with different nodes, it should select the packets from the queue for this transmission. Different from the MAC protocol based on 802.11, the proposed MAC protocol can select multi-packet with different destinations. We use the First Come First Served (FCFS) principle to select packets from the queue. When more than one packet for the same destination is selected, we can utilize the packet aggregation [15, 16] technology to solve the problem.

In summary, AP selects packets in order from the queue. If the current packet has the same destination with the packets which have been selected from the queue to transmit, it will be put in the buffer of the according antenna. Continue to select the packets from the queue until there is no packet in the queue or each antenna has packets to transmit.

After selecting packets of this transmission, the destinations can be put in the receiver fields. The next operations are similar to that of IEEE 802.11 DCF, that is, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is adopted to decrease the possibility of collision. Then AP sends RTS including multiple destinations to reserve the channel with different nodes. Nodes respond AP with CTS after SIFS of the channel idle time according to the received RTS. According to the received CTS, AP sends data to the nodes after SIFS. After successfully receiving the data, nodes will simultaneously send ACK to AP. During the process, other nodes which are not the destinations of the RTS from AP will set their Network Allocation Vector (NAV).

2.3 The DL MU MIMO MAC Protocol

In this section, we can give the specific operations of the proposed protocol. The detail operation of the DL MU MIMO MAC protocol can be described as follow.

(1) AP selects packets to M destinations from the queue. That is, each antenna's buffer has more than one packet and different antennas have different destination.

(2) After the selection of packets transmitted, AP transmits RTS with multiple receivers.

(3) After SIFS of the idle channel, AP receives CTS from nodes. If the number of CTS is 0, AP will go into the backoff. Otherwise, AP transmits data to the nodes which respond AP with CTS. The data to nodes which do not respond CTS to AP will continue queuing.

3 Theoretical Analysis

In this section, we use a Markov chain to analyze the performance of the proposed protocol. Assume that: a. the analysis is made under the saturated conditions; b. the times of retransmission are finite; c. the channel condition is considered as ideal; d. The collision probability of a packet is a constant and independent from the retransmission times.

3.1 Markov Chain Model

Here, the time is divided into slots. The backoff time counter of each node or AP is decremented at the beginning of each slot time. So does the transmission of a packet. A bidimensional Markov chain describing the backoff procedure is shown in Fig. 4.

The state $(s(t), b(t))$ indicates at the time t nodes or AP is at the backoff stage $s(t)$ having $b(t)$ as its value of the backoff counter. Assume the maximum backoff stage is m' and retry limit m . When the value of the node's backoff counter is zero, it sends its data. The nodes or AP involved in the collision will enter the next stage. At this moment, if the backoff stage is smaller than, the contention window is doubled. Or else, the contention window is kept as W_{max} .

$P\{i, j_1, k_1 | i, j_0, k_0\}$ shorts for $P\{i, s(t+1) = j_1, b(t+1) = k_1 | i, s(t) = j_0, b(t) = k_0\}$. So the only non null one-step transition probabilities are shown in (1).

$$\begin{cases} P\{i, j | i, j+1\} = 1 & j \in [0, W_i - 2], i \in [0, m] \\ P\{i, j | i-1, 0\} = \frac{p}{W_i} & i \in [0, m], j \in [0, W_i - 1] \\ P\{0, j | i, 0\} = \frac{1-p}{W_0} & j \in [0, W_0 - 1], i \in [0, m-1] \\ P\{0, j | m, 0\} = \frac{1}{W_0} & \end{cases} \quad (1)$$

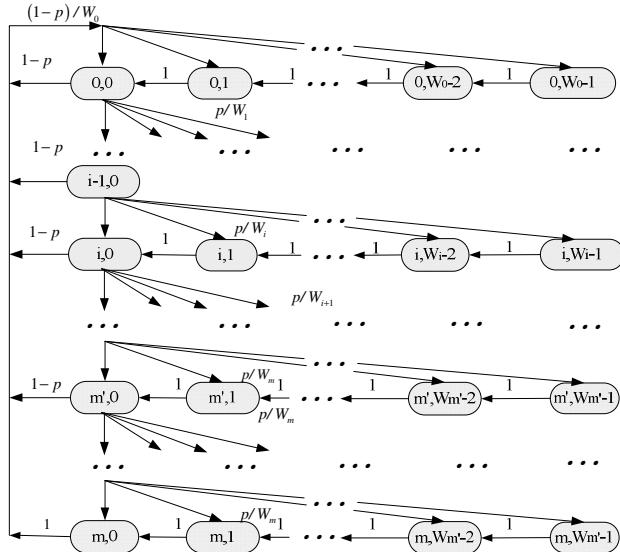


Fig. 4. A Markov chain to model the channel access behavior of AP or a node

The first equation of (1) means that the backoff counter is decremented at the beginning of a slot time. The second equation indicates that the node enters the next stage choosing j as its backoff counter. p is the probability that the node encounters a collision. The third equation shows the fact that the node is back to the minimum backoff stage after a successful transmission. The fourth equation represents the situation that if the node's retransmission times reach the retry limit, the backoff stage will return the stage 0 after the successful and unsuccessful transmission.

$b_{i,j} = \lim_{t \rightarrow \infty} P\{s(t) = i, b(t) = j\}, i \in [0, m], j \in [0, W_i - 1]$ is the stationary probability of the state.

According to the equilibrium equation of the Markov chain, we can obtain a closed-form solution for this Markov chain.

$$b_{i,j} = \frac{W_i - k}{W_i} \cdot b_{i,0} \quad i \in [0, m] \quad (2)$$

$$b_{i,0} = p^i \cdot b_{0,0} \quad i \in [0, m] \quad (3)$$

$$b_{0,0} = (1-p) \sum_{j=0}^{m-1} b_{j,0} + b_{m,0} \quad (4)$$

Let τ be the transmission probability of the STA and let τ_0 be the transmission probability of AP

$$\tau = \sum_{i=0}^m b_{i,0} = \sum_{i=0}^m p^i b_{0,0} = \frac{1-p^{m+1}}{1-p} b_{0,0} \quad (5)$$

$$\tau_0 = \sum_{i=0}^m b_{i,0} = \sum_{i=0}^m p_0^i b_{0,0} = \frac{1-p_0^{m+1}}{1-p_0} b_{0,0} \quad (6)$$

From the viewpoint of a given backoff procedure with retry limit m , we can obtain the relationship between τ, p, τ_0 and p_0 based on the Markov Chain model.

The expression of the collision probability p_0 of AP is:

$$p_0 = 1 - (1 - \tau)^n \quad (7)$$

p indicates the collision probability of a node.

$$p = \tau_0 + (1 - \tau_0) \left[1 - \sum_{m=0}^{M-1} \binom{M-1}{m} \tau^m (1 - \tau)^{M-1-m} \right] \quad (8)$$

According to the normalized condition of Markov chain, the summation of all the stationary probabilities is equal to 1.

$$1 = \sum_{i=0}^m \sum_{j=0}^{W_i} b_{i,j} \quad (9)$$

Substitute (2)-(4) and (7)-(8) into (9), we can get the expression of $b_{0,0}$.

$$b_{0,0} = \frac{2 \cdot (1-2p) \cdot (1-p)}{W \cdot (1-(2p)^{m+1}) \cdot (1-p) + (1-2p) \cdot (1-p^{m+1}) + W \cdot 2^{m'} \cdot p^{m'+1} \cdot (1-2p) \cdot (1-p^{m-m'})} \quad (10)$$

Combined with (5)-(6), the expressions of τ and τ_0 can be obtained.

So we can get a non-linear equation set with τ, p, τ_0 and p_0 as its variables.

p_{s0} is the successful transmission probability of AP.

$$p_{s0} = \tau_0 (1 - \tau)^n \quad (11)$$

3.2 Expressions of the Avarage Access Delay

$E[D]$ is defined as the average access delay. We only calculate the access delay of AP. The expression of $E[D]$ is shown as follow.

$$E[D] = E[X] \cdot E[\text{slot}] \quad (12)$$

where $E[\text{slot}]$ is the length of a slot time, and $E[\text{slot}]$ is the number of slot times AP spending on its backoff procedure. The equations of $E[X]$ and $E[\text{slot}]$ are

$$E[X] = \sum_{j=0}^m d_j \cdot q_j \quad (13)$$

$$E[\text{slot}] = p_{\text{idle}} \cdot \sigma + p_{s0} \cdot L + p_0 \cdot T_c \quad (14)$$

where d_j is the average number of slot times that AP spend in the backoff stage j , q_j is the probability that the packet is successfully transmitted from i.

$$q_j = p_0^j \quad j \in [0, m] \quad (15)$$

$$d_j = \sum_{j=1}^{W_j} \frac{1}{W_j} = \frac{W_j + 1}{2} \quad (16)$$

Substitute (14)-(16) into (13). We can get the access delay's expression $E[D]$.

Due to the multi-packet transmission of AP, the access delay of each packet is assumed as $E[SD]$, which is expressed as follow.

$$E[SD] = \frac{E[D]}{M} \quad (17)$$

4 Simulation and Analysis Results

In this Section, simulation and analysis results are displayed. The comparison of the analysis access delay of the proposed protocol and DCF is shown in Part 4.1. In Part 4.2, we simulate our protocol and DCF in another scenario.

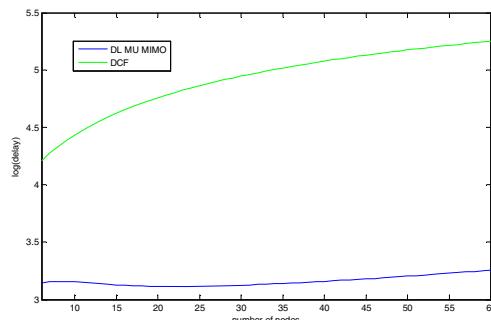


Fig. 5. Comparison curves of the access delay in analysis

4.1 Analysis Results

By the analysis in Section 3, we can obtain the expression of the average access delay for AP. We can get the numerical results of the access delay by substituting the MAC parameters into these equations.

Fig. 5 shows the comparison analysis results between DCF and the proposed MAC protocol. To clearly draw the two delay curves in the same figure, we take log of the delays of the two protocols. When the number of nodes is 30, the delays of the two protocols are 1.3 ms and 5.7 ms respectively. The delay decline rate is 77.1%. Therefore, the results show that the proposed MAC protocol can largely decline the access delay. The reason is that by using multi-antenna AP can transmit packets with different nodes at the same time. In addition, the collision happening condition changes in an uplink transmission. That is, the collision does not happen if the number of nodes simultaneously transmitting is less than the number of AP's antennas. By this way, the collision handling time of the whole network decreases. Therefore, the downlink delay is large decreased.

4.2 Simulation Validation

Besides the analysis results, the proposed protocol is simulated to prove its advantages. There is an AP and n nodes in the network. AP is equipped with 4 antennas and each node has an antenna. The data traffic generation model adopted here is Constant Bit Rate (CBR). Each node has the same packet generation rate as 40 packets/s, while AP's packet generation rate is 160 packets/s. The size of a packet is 250 bytes.

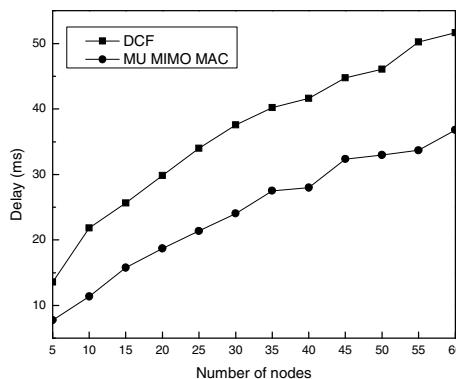


Fig. 6. Delay comparison curves of MU MIMO MAC and DCF in simulation

Fig. 6 shows the simulation delay comparison of the proposed protocol and DCF versus the nodes number. With the increase of nodes, the delays of our protocol and DCF linearly increase. But the delay of our protocol is lower than that of DCF at the same nodes number. When the nodes number is 40, the delays of the proposed protocol and DCF are 27.978 ms and 41.615 ms, respectively. The delay decline rate

is 32.8%. The reason is that AP just can transmit a frame at one time in DCF. So the queuing delay in DCF should be very big. However, in the DL MU MIMO MAC scenario, AP can simultaneously transmit multiple frames. Therefore, the delay is reduced.

Fig. 7 shows the throughput comparison of the proposed protocol and DCF versus the number of nodes. The throughput of our protocol is still higher than that of DCF at the same number of nodes. When the number of nodes is 40, the throughput of the proposed protocol and DCF are 671080 bps and 478100 bps, respectively. The throughput increase rate is 40.3%.

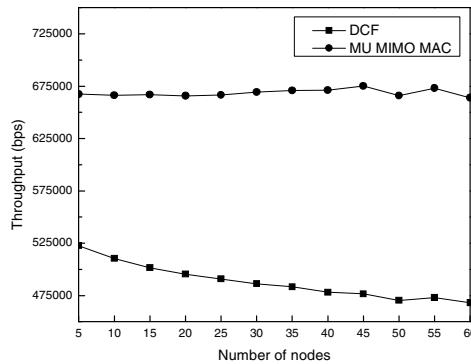


Fig. 7. Throughput comparison curves of MU MIMO MAC and DCF in simulation

5 Conclusion

In this paper, a downlink multi-user multi-input multi-output MAC (DL MU MIMO MAC) protocol was proposed to make full use of the MU MIMO technology. By theoretical analysis and simulation, it proved that the DL MU MIMO MAC protocol could greatly decrease the delay and increase the throughput.

A Markov chain model was utilized to model the channel access actions of AP and each node. The channel access actions of AP and nodes interplayed. We differentiated AP and nodes in the theoretical analysis. The expression of the average access delay for AP was obtained. Both the theoretical analysis results and simulation results confirm that the proposed protocol outperforms DCF in terms of the delay and throughput.

Acknowledgements. This work was supported by National Natural Science Foundation of China (61271176), National Science and Technology Major Project (2013ZX03004007-003) and the 111 Project (B08038).

References

1. Aust, S., Ito, T.: Sub 1GHz Wireless LAN Propagation Path Loss Models for Urban Smart Grid Applications. In: IEEE International Conference on Computing, Networking and Communications, ICNC (2012)
2. 802.11ah-Standard for Information Technology-Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment- Sub 1 GHz License-Exempt Operation
3. Wang, X., Huang, W., Wang, S., Zhang, J., Hu, C.: Delay and Capacity Tradeoff Analysis for Motion Cast. *IEEE/ACM Transactions on Networking* 19(5), 1354–1367 (2011)
4. Wang, X., Fu, L., Hu, C.: Multicast Performance with Hierarchical Cooperation. *IEEE/ACM Transactions on Networking* 20(3), 917–930 (2012)
5. IEEE P802.11ac™/D2.0, Draft Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 5: Enhancements for Very High Throughput for Operation in Bands below 6 GHz
6. Wu, H.: Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement. In: IEEE Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), vol. 2 (2002)
7. Bianchi, G.: Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communications*, 535–547 (2000)
8. Chan, D.S., Berger, T., Lang, T.: Carrier Sense Multiple Access Communications on Multipacket Reception Channels: Theory and Applications to IEEE 802.11 Wireless Networks. *IEEE Transactions on Communications* 61(1) (2013)
9. Zheng, P., Zhang, Y., Liew, S.C.: Multipacket Reception in Wireless Local Area Networks. In: Proc. IEEE ICC 2006, vol. 8, pp. 3670–3675 (2009)
10. Zhao, M., Ma, M., Yang, Y.: Applying Opportunistic Medium Access and Multiuser MIMO Techniques in Multi-Channel Multi-Radio WLANs. *J. Mobile Netw. Appl.* 14(4), 486–507 (2009)
11. Cai, L., Shan, H., Zhuang, W., Shen, X., Mark, J., Wang, Z.: A Distributed Multi-User MIMO MAC Protocol for Wireless Local Area Networks. In: IEEE GLOBECOM 2008, New Orleans, LA (2008)
12. Zhu, C., Bhatt, A., Kim, Y.: MAC Enhancements for Downlink Multi-User MIMO Transmission in Next Generation WLAN. In: Consumer Communications and Networking Conference (CCNC), pp. 832–837 (2012)
13. IEEE 802.11e, Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Std. 802.11e-2005 (2005)
14. Liu, H., Li, C., Hao, S., Cai, X., Li, J.: A Novel Internal Collision Managing Mechanism of IEEE 802.11e EDCA. In: 19th Asia-Pacific Conference on Communications (APCC 2013), Bali, Indonesia (2013)

15. Rajkumar, A., Michael, D.T.: Packet Aggregation for Real Time Services on Packet Data Networks, U.S. Patent U.S. Patent and Trademark Office, No. 7,391,769 (2008)
16. Cha, J.: Performance Comparison of Downlink User Multiplexing Schemes in IEEE 802.11 ac: Multi-user MIMO vs. Frame Aggregation. In: IEEE Wireless Communications and Networking Conference, WCNC (2012)

RLNC in Practical Wireless Networks*

Kyu-Hwan Lee¹, Jae-Hyun Kim¹, and Sunghyun Cho²

¹ School of Electrical and Computer Engineering, Ajou University, Suwon, Korea
`{lovejyoon7, jkим}@ajou.ac.kr`

² Dept. of Computer Science & Engineering, Hanyang University, Ansan, Korea
`chopro@hanyang.ac.kr`

Abstract. In this paper, we investigate random linear network coding (RLNC) in practical wireless networks. First we apply RLNC in the legacy network (wireless LAN mesh network) of multiple unicasts by the global RLNC. In the simulation results, in the system with the global RLNC, the network load and the power consumption is reduced for the simple topologies. However, the global RLNC cannot be applied to practical network by the decoding failure due to the various direction of each flow in the network. In this paper, we also discuss practical issues such as the hidden node problem, the occurrence of coding opportunity, and the RLNC overhead for RLNC in the wireless network.

Keywords: RLNC·network coding·wireless networks·wireless LAN.

1 Introduction

Network coding has attracted interest in many literatures for wireless network systems since it was first introduced in information theory [1]-[4]. It has the potential to yield better throughput and reliability for the network of both unicast and multicast applications. In particular, RLNC is useful to select code in the distributed network. Generally code construction algorithms which are deterministic algorithms require a centralized design based on the topology of the whole network. However, these algorithms are useless in some applications because the network topology could be dynamically changing [5]. The implementation of the centralized design is also uneasy. In RLNC, it can be able to design practical protocol in the distributed network because every coding coefficient is randomly selected. Therefore, many studies deal with RLNC in wireless systems [11]-[16]. However, most of previous works have more theoretical and biased results which may not consider the practical issue in wireless environment. Furthermore, they almost work to create the system for network coding without the compatibility with the legacy system.

* This research was supported by basic Science Research Program Through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(2010-0023326) and the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency (NIPA-2013-(H0301-13-2003)).

To apply RLNC in wireless network, RLNC characteristic is considered as follows:

1. Overhearing: In the wireless network, the packet is conveyed by the wireless medium not the wired line. Therefore, the node which performs the network coding can exploit the broadcast nature. If the node overhears all transmissions, “free-ride” transmission can be achieved by network coding and the broadcast nature of the wireless medium.

2. The coding structure: To get the coding opportunity, the coding structures such as chain topology and X topology exist in the network. In these topologies, “free-ride” transmission can be achieved by overhearing packets. It can yield better throughput in the network.

3. Batch set: In the source of the RLNC, packets are encoded for batch set unit. Therefore, if the intermediate node which performs RLNC does not encode packets which have same batch set, the destination can retrieve its native packet.

4. Application: RLNC is designed for the distributed system of the multicast environments. Therefore, RLNC may appreciate for the multicast application and the intra-session network coding. The intra-session network coding only encodes packets belonging to the same session. However, in the practical wireless network, the unicast application is more used than the multicast application.

In this paper, we investigate the RLNC in practical wireless network. In the legacy system such as IEEE 802.11s, we apply RLNC to the system. We then derive key challenge to apply RLNC in wireless system based on the various results in this paper.

2 Related Works

Network coding is first introduced by Ahlswede *et al.* in 2000. It shows that the capacity of multicast network with network coding can be increased compared with employing traditional routing alone. It is known to achieve the classical max-flow min-cut bound [1]. The studies in [2] and [3] theoretically show that linear coding is enough to achieve the maximum capacity if finite field size of coding coefficient set is longer than theoretically upper bound. Ho *et al.* have proposed RLNC concept in the multicast network [4]. In a node of RLNC a linear combination of incoming packets over finite field with randomly chosen coding coefficient is transmitted to its outgoing links. In the study of Ho *et al.* offers the successful decoding probability in the destination if the finite field size satisfies the given upper bound.

There are many studies on inter-session network coding [6]-[9]. The inter-session network coding is allowed among packets belonging to possibly different sessions. In particular, COPE of Katti *et al.* use XOR network coding and the broadcast nature of the wireless medium to perform the opportunistic listening and the coding. Besides, some works study the intra-session network coding in the wireless network to increase the throughput or offer the reliability [10]-[16]. The intra-session network

coding is restricted to packets belonging to the same session. In particular, MORE of Chachulski *et al.* exploits the opportunistic routing scheme by using RLNC in the packet transmission to give each transmitted packet with the unique information.

Network coding can be used in physical layer [17]-[18]. PNC performs network coding in the wireless radio signal level by combining signals which consist of amplitudes and phase terms [17]. However, the synchronized signal transmission is needed in two senders to perform PNC. In MIXIT, the idea is to code symbols rather than packets [18].

3 RLNC in Wireless LAN

In this section, we investigate whether RLNC can be applied to multiple unicast sessions not the multicast environment although RLNC is suitable for the multicast environment. In wireless systems, multiple unicast applications are more realistic and applicable than multicast applications. This method is called global RLNC in remainder of paper. Therefore, in this paper, we assume that the destination can decode the native packet even if the encoding method in multicast is used and will verify whether assumption is correct. In this paper, we consider a fixed multi-hop wireless network. Ad-hoc on demand vector (AODV) is used as the routing protocol because we consider the compatibility with legacy wireless systems such as IEEE 802.11s [17]-[18]. The maximum number of retransmissions is 4. All of the RLNC function is implemented in the network coding (NC) layer which lies between the IP layer and the MAC layer. Definitions of some terms used in this paper are shown in table 1.

Table 1. Definitions of terms in RLNC

Terms	Descriptions
Native packet	-The original data packet
Coded packet	-The packet after encoding operation (RLNC)
Received packet	-The packet which arrives at its destination node
Forwarding packet	-The packet forwarded by the intermediate node in routing path
Broadcasting packet	-The packet broadcasted by broadcasting node for RLNC
Coding flow	-The flows that are encoded together at a crossover node
Crossover node	-The node that encode packets in same batch set (Global RLNC) -The node which encodes packets of coding flow (Local RLNC)
Broadcasting node	- One-hop predecessor of the crossover node -The node which broadcasts packets to be received by crossover and overhearing nodes
Overhearing node	-One-hop successor of the crossover node -The node which overhears packets from broadcasting nodes and receives packets from crossover nodes

3.1 Operation

Operation of RLNC protocol as shown in fig. 1 is as following:

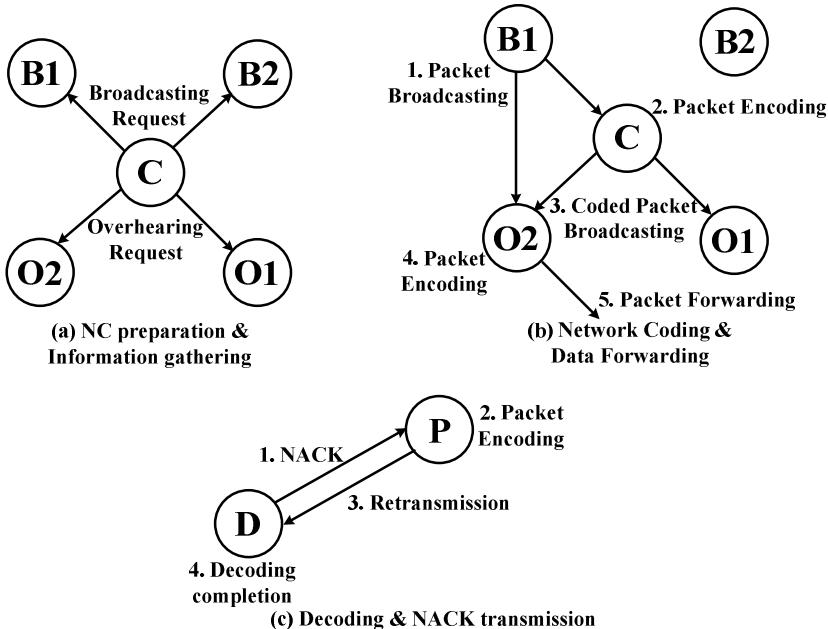


Fig. 1. Operation of global RLNC

-NC preparation & Information gathering: Routing (AODV) is used to select the RLNC set (crossover node, broadcasting node, overhearing node). The condition for RLNC set is that the overhearing node can overhear packets from other broadcasting nodes of coding flows. Routing metric such as hop counts, radio metric, etc can be used [18]. Crossover nodes send the control packet to broadcasting and overhearing nodes respectively.

- Network Coding & Data Forwarding: The crossover and overhearing node generate coded packet from packets of coding flow and packets which are in the same batch set sequence of a retransmission (RTX) buffer. We assume that all nodes can receive most of packet in the same batch set by overhearing and forwarding packets, so that destination nodes may decode its native packet since destination nodes use coded packets, received packets, forwarding packets, and broadcasting packets to decoding. Encoding more packets is a help to make more randomness of the coefficient set, so that the decoding success ratio will increase. Upon receiving packets from broadcasting nodes, the crossover node conducts packet buffering in coding buffer to try getting coding gain. All nodes store received packets, forwarding packets and broadcasting packets in the RTX and the decoding buffer up to timeout to encode and decode packets. Generally most of other researches use the opportunistic coding since the packet buffering can incur the buffering delay. However, the packet

buffering should be needed in RLNC because the encoding and the decoding are only conducted with the same batch set sequence in RLNC. The packet buffering is conducted during sufficient time to receive packets of the coding flow and other same batch set packets.

- Decoding & NACK transmission: If destination nodes do not decode its native packet within certain time, it sends the NACK packet to a previous node. The previous node then generates the coded packet and retransmits it to the destination. If aforementioned assumption is correct, the previous node may generate the coded packet to help decoding in the destination.

3.2 Protocol Validation and Performance Evaluation

We would like to validate the global RLNC protocol and compare the global RLNC gain with the conventional system. First, we look at the performance of simple X topology (crossed with 2 and 3 flows) in terms of the network load and the power consumption in wireless LAN as shown in Fig 2 (2, 3 flow) [21]. We then verify the effectiveness of global RLNC in grid networks. In the grid network simulation, all nodes are set to the promiscuous mode to exploit the broadcast characteristic in the wireless medium. The routing metric is hop counts. Each flow enters the network at different time with the uniform distribution. All flows are constant-bit-rate (CBR) flow with a fixed packet size of 1500byte and an inter-arrival time of 1 second. All flows belong to the same batch set. The batch set sequence increases by one whenever the packet is generated in source nodes. The transmission range is set to 100m. The simulation time is 10minute.

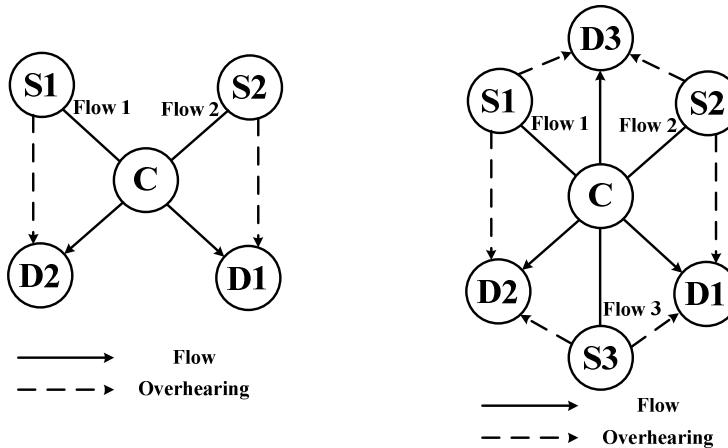


Fig. 2. Simple X topology

1) Simple Topology

Fig. 3 and 4 show the total load and the power consumption in the networks respectively. The load is total number of bits per second (bits/sec) submitted to

wireless LAN layers by all higher layers in all wireless LAN nodes of the network. The quantity of the total load with RLNC decreases as compared with that of the conventional system. It means that RLNC can convey same information by fewer loads than that of the conventional system. In the power consumption, although the RX power consumption increases by the overhearing, The TX power consumption decreases by RLNC. Consequently total power decrease as compared with that of conventional system because TX power has more influential in the wireless LAN system. In this paper to show gain as numerical results, we define the coding gain in the load (G_{load}) and the power consumption (G_{power}) which are load and power consumption quantity we can save by using RLNC, respectively, as

$$G_{load} = 1 - \frac{L_{total,RLNC} (\text{bits/sec})}{L_{total,legacy} (\text{bits/sec})} \quad (1)$$

$$G_{power} = 1 - \frac{P_{total,RLNC} (W)}{P_{total,legacy} (W)}. \quad (2)$$

$L_{total,RLNC}$ and $L_{total,legacy}$ denote the total load in the network of RLNC and the conventional system respectively. $P_{total,RLNC}$ and $P_{total,legacy}$ are the total power consumption in the network of the system with and without RLNC, respectively. G_{load} in the case of 2 and 3 flow scenarios are 25% and 33% respectively. G_{power} in the case of 2 and 3 flow scenarios are 7.47% and 7.6% respectively.

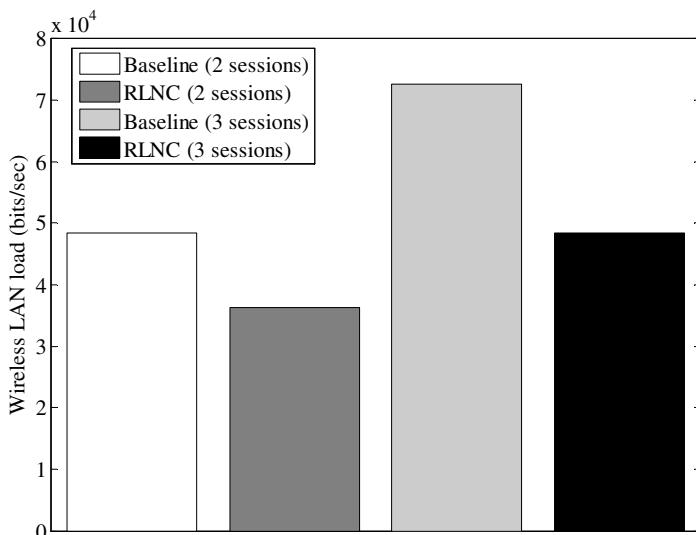


Fig. 3. Total load in simple X topology (bits/sec)

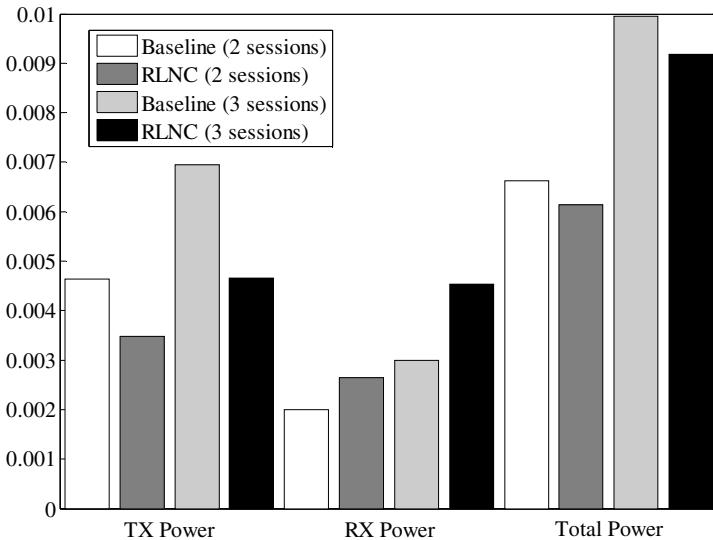


Fig. 4. Total power consumption in simple X topology (W)

2) Grid topology

In the grid topology, we consider 2 scenarios which are 5X5 grid, 7X7 grid to vary the number of nodes. In grid scenarios, the vertical and horizontal distances between two adjacent nodes are 50m. All nodes work as the source node that randomly

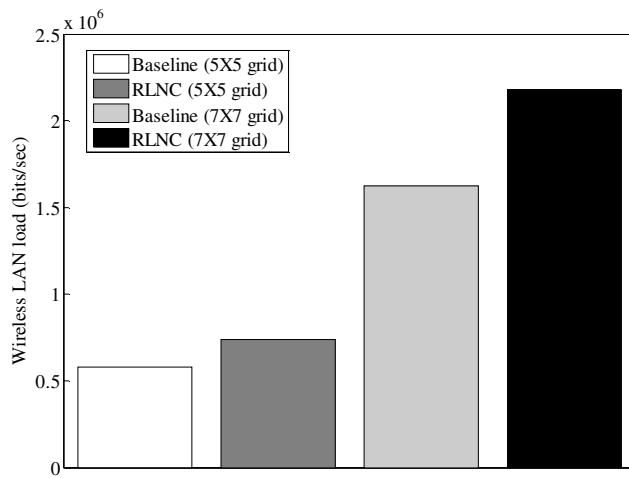


Fig. 5. Total load in grid topologies (bits/sec)

chooses the destination node in the network. Fig. 5 shows the total load in the networks. In grid topology, the total load in RLNC is more than that of conventional system. In destinations, decoding condition is not satisfied although the destination request retransmission up to maximum bound as shown in Table 2. Therefore, the load in network increases as compared with the load in the legacy system. The destination cannot receive sufficient packets to decode its native packets since the direction of each flow in the coded packet is various as shown in Fig. 6. It means that the coding policy of multicast RLNC is not directly applied to the unicast environment and the coding policy should be redesigned for the unicast.

Table 2. Decoding failure in grid topology

Scenario	Decoding failure
5X5 grid	12.04%
7X7 grid	33.22%

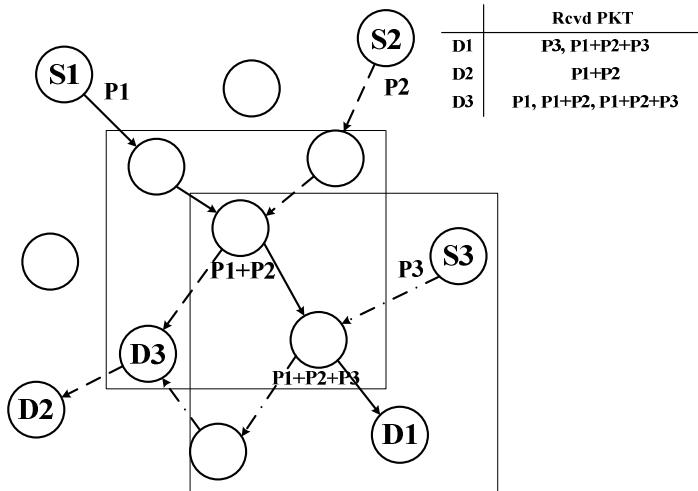


Fig. 6. Description of decoding failure

4 Practical Issues in Wireless Environment

In this section, we deal with practical issues of the RLNC application in the wireless environment. In practical issues, we treat the hidden node problem, the occurrence for the coding opportunity, and the RLNC overhead.

- Hidden node problem: In the case where many nodes sending the packet to bottleneck nodes exist in the distributed network, if they are not within the carrier sense range of each other, it can result in classical hidden node problem. The hidden node problem can be relieved by RTS/CTS in the IEEE 802.11 specification. However, the RTS/CTS scheme is needed for some modification in

the network coding system because the network coding system has to exploit the broadcast characteristic in the wireless medium. Nodes that do not receive the packet work as the sleeping mode by the RTS/CTS procedure, so that the node in sleeping mode cannot overhear other packets for network coding. Therefore, all nodes receiving the RTS packet have to work as the receiving mode instead of the sleeping mode during network allocation vector (NAV).

- Occurrence for the coding opportunity: The coding opportunity is another important factor to affect the performance of RLNC. As described in the previous section, the coding structure such as X topology has to exist in network to get coding opportunity. Therefore, it is required to analyze how many the coding structures in the network to expect the network coding gain.
- RLNC overhead: To apply RLNC in the system, the additive control packets and the overhead in the packet header is needed in the system. There are the control packets to configure the RLNC set and to operate the RLNC system. In the packet header, the coefficient set is needed to encode and decode packets. From the point of view of the packet size, the overhead of the coefficient set is negligible if the data payload is much longer than the packet header including the coefficient set. However, from the point of view of the network, it cannot be negligible since the packet is conveyed by multi-hop in the network.

5 Conclusion

This paper investigates the RLNC for the practical wireless network in various aspects. First this paper investigates whether RLNC can be applied to multiple unicast sessions not the multicast environment. In the simulation results, the network load and the power consumption is reduced for the simple topologies. However, the coding policy of the multicast RLNC is not directly applied to the general unicast environment. The coding policy should be redesigned for the unicast. We also need to find the practical scenario for RLNC. Consequently, additional researches are needed for applying RLNC (network coding) to practical wireless networks as following:

1) Scarce network coding opportunity: the studies such as the network coding aware routing protocol and the construction of the general coding condition are needed for usefulness of RLNC in practical wireless network [22]-[24].

2) Effective Application: the studies on practical scenario for RLNC are needed for practical RLNC. Although RLNC is used in the multicast environment, it can be useless due to monotonous routing path. Furthermore, it is considered to the characteristic for RLNC such as the batch set and the randomness of the coefficient.

3) Minimal overhead: the network coding is not “free-riding”. It can have trade-off between the network load reduction and other performance metrics in the network such as the power consumption. There are overhead such as the control packet and the coefficient set in the packet header. Therefore, these should be considered to design the practical wireless RLNC system.

Until now, RLNC (network coding) may be practically useless in the wireless network due to its limitation of implementation and the unrealistic application. However, if many researches are conducted for practical RLNC (network coding) as aforementioned, RLNC (network coding) will be helpful to general wireless network.

References

1. Ahlswede, R., et al.: Network information flow. *IEEE Transactions on Information Theory* 46, 1204–1216 (2000)
2. Li, S.Y.R., et al.: Linear network coding. *IEEE Transactions on Information Theory* 49, 371–381 (2003)
3. Koetter, R., Medard, M.: An algebraic approach to network coding. *IEEE/ACM Transactions on Networking* 11, 782–795 (2003)
4. Ho, T., et al.: A Random Linear Network Coding Approach to Multicast. *IEEE Transactions on Information Theory* 52, 4413–4430 (2006)
5. Li, S.Y.R., et al.: Linear Network Coding: Theory and Algorithms. *Proceedings of the IEEE PP*, 1–16 (2011)
6. Li, Z., Li, B.: Network coding: The case for multiple unicast sessions. In: Proc. Allerton Conf. (2004)
7. Katti, S., et al.: XORs in the Air: Practical Wireless Network Coding. *IEEE/ACM Transactions on Networking* 16, 497–510 (2008)
8. Rayanchu, S., et al.: Loss-aware network coding for unicast wireless sessions: design, implementation, and performance evaluation. *SIGMETRICS Perform. Eval. Rev.* 36, 85–96 (2008)
9. Jilin, L., et al.: How Many Packets Can We Encode? - An Analysis of Practical Wireless Network Coding. In: The 27th Conference on Computer Communications, INFOCOM 2008, pp. 371–375. IEEE (2008)
10. Wu, Y., et al.: Minimum-energy multicast in mobile ad hoc networks using network coding. *IEEE Transactions on Communications* 53, 1906–1918 (2005)
11. Chachulski, S., et al.: Trading structure for randomness in wireless opportunistic routing. *SIGCOMM Comput. Commun. Rev.* 37, 169–180 (2007)
12. Chou, P.A., Yunnan, W.: Network Coding for the Internet and Wireless Networks. *IEEE Signal Processing Magazine* 24, 77–85 (2007)
13. Fragouli, C., et al.: Wireless Network Coding: Opportunities & Challenges. In: Military Communications Conference, MILCOM 2007, pp. 1–8. IEEE (2007)
14. Koetter, R., Kschischang, F.R.: Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory* 54, 3579–3591 (2008)
15. Tracey, H., et al.: Byzantine Modification Detection in Multicast Networks With Random Network Coding. *IEEE Transactions on Information Theory* 54, 2798–2803 (2008)
16. Swapna, B.T., et al.: Throughput-Delay Analysis of Random Linear Network Coding for Wireless Broadcasting. In: 2010 IEEE International Symposium on Network Coding (NetCod), pp. 1–6 (2010)
17. Zhang, S., et al.: Physical-layer network coding. Presented at the Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, Los Angeles, CA, USA (2006)
18. Katti, S., et al.: Symbol-level network coding for wireless mesh networks. *SIGCOMM Comput. Commun. Rev.* 38, 401–412 (2008)
19. IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), pp. C1–C1184 (2007)

20. IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 10: Mesh Networking. IEEE P802.11s/D12.0, pp. 1–391 (May 2011)
21. Feeney, L.M., Nilsson, M.: Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In: INFOCOM 2001, Proceedings of the IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1548–1557 (2001)
22. Jilin, L., et al.: DCAR: Distributed Coding-Aware Routing in Wireless Networks. *IEEE Transactions on Mobile Computing* 9, 596–608 (2010)
23. Sengupta, S., et al.: Network Coding-Aware Routing in Wireless Networks. *IEEE/ACM Transactions on Networking* 18, 1158–1170 (2010)
24. Guo, B., et al.: Analysis of General Network Coding Conditions and Design of a Free-Ride-Oriented Routing Metric. *IEEE Transactions on Vehicular Technology* 60, 1714–1727 (2011)

Accuracy Evaluation for Sensed Data

Yan Zhang and Hongzhi Wang*

Harbin Institute of Technology, China

{zhangy,wangzh}@hit.edu.cn

Abstract. To address the problem for accuracy evaluation, we propose a systematic method. With MSE, a parameter to measure the accuracy in statistics, we design the accuracy evaluation framework for multi-modal data. Within this framework, we classify data types into three categories and develop accuracy evaluation algorithms for each category in cases of in presence and absence of true values. Extensive experimental results show the efficiency and effectiveness of our proposed framework and algorithms.

Keywords: data quality, accuracy, sensed data.

1 Introduction

With the rapid development of microelectronics, embedded computing techniques, integrated circuits and wireless communication techniques, the Wireless Sensor Networks (WSNs) are rapidly emerging due to their tremendous applications in various areas, such as military defense [12], environment monitoring [9], traffic monitoring [10] etc.

Sensors in WSNs observe and cognize the complicated physical world [8], generating lots of sensed data. Almost all applications of WSNs are dependent on the computation on sensed data. A large number of distributed and energy efficient sensory data processing algorithms have been proposed recently, including the data collection algorithms [1], the sampling based aggregation algorithms [7] and so on. All of these algorithms have high performance in term of accuracy and energy efficiency, and are suitable for the applications of WSNs.

One of the common issues of the aforementioned algorithms is that they assume the sensed dataset sampled by the sensors and transmitted in-network have high quality. However, in practice, sensors acquire the discrete digital data to represent the continuous physical world, incurring errors at very early stage. These errors could be further magnified during the transmission stage since many compression techniques are adopted for the purpose of the energy and space saving. Meanwhile, the vulnerable short-precision sensors, the complicated physical environment, the transmission delay and data packet loss will also lead to the low-quality of sensory data. Therefore, quality ensuring of sensed data is very crucial since the sensor network applications require high quality sensed data.

* Corresponding author.

The low quality of sensed dataset manifests in their incompleteness, inconsistency, inaccuracy and obsoleteness, among which the inaccuracy is the very important one. It will cause that the data computation algorithms return imprecise answers and the users make wrong decisions. Therefore, a method for evaluating the accuracy of sensory data is highly desired. This motivates us to study how to determine the accuracy of the sensory data.

With its importance, the evaluation of accuracy on sensed data brings following technical challenges.

- The sensed data come from multiple sensors with various data schemas. The sensed data contain not only numerical attribute obtained by sensors but also the string or category attributes that describe the environment of the sensors. The accuracy evaluation method should be adapted to all these sensors to assure the widely applications.
- Among the data, different values may describe the same attribute of the same real-world entity. Any of the values may be the true value which should be estimated. Accuracy evaluation should consider the conflicts on values.
- There are various types of attributes. The inaccuracy of different types may be caused by different reasons. As a result, the accuracy of different data types has different definitions. Thus different estimation methods should be designed for different attribute.

Current work seldom consider the estimation of accuracy. Only [13] considers accuracy estimation. However, in [13], only the attributes category type is considered. It means that for a value, in their system, this value can only be considered as a true value or a false value. The type of sensed data may be numerical type such as float.

To address this problem, this paper proposes accuracy estimation methods for sensed data from multiple data sources in different data types. This paper performs following contributions.

- To deal with sensed data, we propose a general framework that is suitable for accuracy evaluation on data in various forms. According to the difference in evaluation method for data in various types, we classify the data types into three classes according to the error computation methods. (Section 2)
- We propose efficient accuracy evaluation algorithms for various data types in two cases of in presence and absence of true values. (Section 3 and Section 4)
- Extensive Experiments are performed to verify the efficiency and effectiveness of proposed methods. Experimental results show that our methods could evaluate accuracy for multi-mode data effectively and efficiently. (Section 5)

2 Framework

Even though sensed data have multiple modes with various schemas, data objects in the data are described with attributes. From the aspect of semantics, the

attributes can describe both involution and extension of data objects. The former includes attributes describing the properties of object and the latter includes attributes describing the relationship between the object and others. From the aspect of representation, an attribute for a data object is a wide concept which includes both the data collected from sensors and those describing the environment. Thus data objects in various modes could be described with a set of attributes. The evaluation of the accuracy of a data set is to evaluate the accuracy of the each data object in the data set and the evaluation of the accuracy of a data object can be a combination of the evaluation of all attributes.

Using attributes as the basic unit of accuracy evaluation does not mean the neglect of the relationships between the attributes. We note that two latent relationships among the attributes will affect the accuracy evaluation. One is *entity relationship*. It means that different attribute value may describe the same attribute of a real-world entity. With entity relationship, during the evaluation, the same attribute with different values shares the same true value. It means that the same attributes of these tuples share the same true value, although they may be different in the table. The other relationship is *source relationship*. It means that some attributes the attributes of different data objects may share the same excepted accuracy. This kind of relationships is led by that different values may come from the same sensor. For example, in a static environment, the accuracy of observations collected from a sensor depends on the fixed accuracy of this sensor.

With above discussion, accuracy evaluation should take attribute as basic unit and consider the relationship between them. Thus the problem is defined formally as follows.

Problem (Accuracy Evaluation). Given a data object set $O=\{o_1, o_2, \dots, o_n\}$ with each data object o_i as a triple (S_i, E_i, A_i) where S_i is the data source ID of o_i , E_i is the ID of the real-world entity described by o_i and $A_i=\{(a_{i1}, v_{i1}), (a_{i2}, v_{i2}), \dots, (a_{ik_i}, v_{ik_i})\}$ is the set of attributes of o_i with each key-value pair (a_{ij}, v_{ij}) representing the value of attribute a_{ij} of o_i is v_{ij} , the accuracy of the data object set O according to the data objects in it is output.

2.1 Classifications of Attributes

The difference computation method for values of a attribute in different type may be different. Since difference computation for values is the basic operation for accuracy computation, we classify the attributes into following three types according to the difference computation method.

- **Measurable Attribute.** The values in such type of attribute are in some total order and can be modeled as some distribution. The difference of values in a measurable attribute is computed with numerical minus. Such attributes include numerical attributes such as the value gathered with instruments.
- **Comparable Attribute.** The values in such type of attribute are not in order and no distribution can be derived from the values. However, the difference between values in such type of attributes can be computed. Such that

the distance between the input value and the true value can be computed. Descriptive attributes in type of string or sequence belong to this type.

- **Category Attribute.** The difference of the value of such attribute cannot be computed. The difference of such attribute can only be marked as “same” or “different”.

Note that from the aspect of difference computation, a category attribute could be treated as a special kind of comparable attribute with the difference function $\text{Diff}()$ as $\text{Diff}(u,v)=1$ if u and v are different. Otherwise, $\text{Diff}(u,v)=0$. Thus we only study measurable and comparable attributes in this paper.

2.2 Accuracy Evaluation Framework

Our method uses accuracy of each attribute as the basic unit and assemble them to describe the accuracy of the whole data set. Since the accuracy of different type of attributes should be evaluate in different methods. We attempt to evaluate the accuracy of attributes according to different data type and combine them.

The framework of the accuracy evaluation includes three phases. (1) The values of attributes are classified according to the type of attributes; (2) the accuracy for each type of attributes is evaluated; and (3) the accuracies in phase 2 are combined.

The first phase extracts attributes from data set and classifies the attributes into different types. For relational database, the values in the same column in each table are in the same type.

In the second phase, from the statistics theory, the accuracy can be estimated as means squared error (MSE) [6]. We use it as the accuracy measure for values in the same attribute. The details of this phase will be described in Section 3 and Section 4 for the cases of presence and absence of true values, respectively.

In the third phase, the average of accuracies of values in different types is computed as the global MSE of data in all types. That is, $accuracy_g = \frac{\sum_{t \in T} |D_t| accuracy_t}{\sum_{t \in T} |D_t|}$, where T is the set of data types, D_t is the set of values in data type t , $accuracy_t$ is the accuracy of data in type t . With $accuracy_g$ as the global MSE, we use $\frac{1}{accuracy_g}$ to describe the global accuracy of the whole data set.

3 Accuracy Estimation with True Values

In statistics theory, mean squared error (MSE) is often used to estimate the accuracy of observations. Thus we use this concept to evaluate the accuracies. The MSE of a parameter θ is described as followings [6].

$$MSE(\hat{\theta}) = E[(\hat{\theta} - \theta)^2] \quad (1)$$

where θ is true value of a parameter and the $\hat{\theta}$ is the observation according to it.

In the case with sufficient information and knowledge, true values could be found with entity resolution [4] and truth discovery techniques [13,3]. Then this formula could be applied directly for accuracy evaluation.

Even in presence of true values, the computation of MSE looks trivial. However, for different data types, the computation of the difference between true value and the value in real data set may be different. We will discuss evaluation methods for data different types with true values, respectively.

In this section, the evaluation involves true values. In order to distinguish true values from the values of attributes in the data set which possibly contain inaccuracy or even false values, in the remaining part of this paper, we use *observation* to refer the value of attributes in data set.

With the true value the MSE is computed as the average of the square of the difference between the observations and the true value. The accuracy for a set of observations is computed as following.

$$MSE(D) = \frac{\sum_{v \in D} Diff^2(t_v, v)}{|D|} \quad (2)$$

where t_v is the true value of v and function $Diff(t_v, v)$ is to compute the difference between t_v and v . For measurable attributes, $Diff(t_v, v) = |t_v - v|$ when $Diff(t_v, v)$ is the difference computation function related to the data type for comparable data type.

4 Accuracy Evaluation without True Values

In the cases without sufficient information for discovering true values, the true value for an attribute is unknown. Thus accuracy evaluation techniques without true values are needed. Here, the accuracy computation is more difficult and the true values have to be estimated with existing observations. With various difference computation methods in different attribute types, the true value computation method is different. Thus we attempt to propose different accuracy evaluation methods in absence of true values for different attribute types in this section. Since

4.1 Measurable Data Type

To evaluate accuracy of values in measurable data type in absence of true values, we formalized the problem into an optimization problem with accuracies and true values as variables. The goal is to choose the true values to minimize the MSE to assure that the accuracy is not underestimated. The value of optimization goal for the solution is the MSE.

Problem Definition. For measurable data type, if it is assumed that the true value of an observation o is T_o and the upper bound of the error between true value and the observation is ϵ_o , then it should satisfy that $|T_o - o| \leq \epsilon_o$. That is, $T_o - \epsilon_o \leq o \leq T_o + \epsilon_o$. Thus, given a set of observation O , the estimation of

minimal bound of the MSE of O can be converted to the following optimization problem.

$$\begin{aligned} \min & \quad \frac{1}{|O|} \sum_{o_i \in O} \epsilon_{o_i}^2 \\ \text{subject to } & T_{o_i} - \epsilon_{o_i} \leq o_i \leq T_{o_i} + \epsilon_{o_i} \quad o_i \in O \end{aligned} \quad (3)$$

where variables include ϵ_{o_i} and T_{o_i} of each o_i .

Note that if some observations are determined to refer to the same attribute of the same object, they share the same true value.

Solutions. This optimization problem is a quadratic programming problem [11] since only the optimization goal contains the quadratic items. The optimization objection can be represented as $R^T QR$, where $R = <\epsilon_1, \epsilon_2, \dots, \epsilon_n>$ and

$$Q = \begin{pmatrix} \frac{1}{|O|} & 0 & \dots & 0 \\ 0 & \frac{1}{|O|} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{|O|} \end{pmatrix}$$

Obviously, Q is positive definite. Therefore, this problem can be solved with ellipsoid method in polynomial time[5].

For the efficiency of computation, some constraints can be merged. Clearly, two constraints $t - o \leq v_1$ and $t - o \leq v_2$ with $v_1 \leq v_2$ could be merged to one constraint $t - o \leq v_1$. Two constraints $v_1 \leq t + o$ and $v_2 \leq t + o$ with $v_1 \leq v_2$ could be merged to $v_2 \leq t + o$.

4.2 Comparable Type

The accuracy computation for values in comparable type is also a optimization problem with the goal as minimizing the total MSE for the same reason as the computation of measurable type but the constraint is different due to the difference computation function is not simply minus.

Problem Definition

Similar as that of measurable type, the estimation of MSE of comparable type can be formalized as following.

$$\begin{aligned} \min & \quad \frac{1}{|O|} \sum_{o_i \in O} \epsilon_i^2 \\ \text{subject to } & Distance(T_{o_i}, o_i) \leq \epsilon_i \quad o_i \in O \end{aligned} \quad (4)$$

where the function $Distance$ is to measure the distance between to values. For example, the edit distance for strings or Jaccard similarity for sets.

Solutions. The function $Distance$ may have various forms. Even for common distance such as edit distance, this optimization problem can hardly be solved by existing numerical programming method [11] since explicit numerical relationship among could not be derived such as edit distance of strings and Jaccard

Algorithm 1. Comparable_MSE($R, \mathbb{O}, \mathbb{S}$)

Input: The set of observations, R ; The partition of observations wrt. corresponding true value, \mathbb{O} ;
 The partition of observations wrt. accuracy, \mathbb{S}

Output: The accuracy of R

```

1: for each  $o_i$  in  $\bigcup_{O \in \mathbb{O}} O$  do
2:    $\epsilon_i = 0$ 
3: while not converge or iteration times smaller than the threshold do
4:   for each  $O$  in  $\mathbb{O}$  do
5:      $T = \arg \min_{t \in O} \left\{ \sum_{o_i \in O} (\max\{Distance(t, o_i) - \epsilon_i, 0\})^2 \right\}$ 
6:     for each  $o_i$  in  $O$  do
7:        $t_i = T; \epsilon_i = |T - o_i|$ 
8:     for each  $S$  in  $\mathbb{S}$  do
9:        $max = \max_{o_i \in S} \epsilon_i$ 
10:      for each  $o_i$  in  $S$  do
11:         $\epsilon_i = max$ 
12: return  $\frac{\sum_{o_i \in R} \epsilon_i^2}{|R|}$ 

```

similarity between sets [2]. To solve this problem, we propose a iteration algorithm to tune the true value and error of each data object iteratively to find the proper values. The pseudo code of this algorithm is shown in Algorithm 1.

The error of each observation is initialized to be 0 (Line 1-2). In the first iteration, for different observations $O=\{o_1, o_2, \dots, o_n\}$ sharing the same true value, the true value T is computed to minimal $\sum_{i=1}^n Distance^2(T - o_i)$ (Line 5 with $\epsilon_i=0$). With the selected value, the true values and errors of each o_i is assigned (Line 6-7). With the consideration of the source relationship, for the observations sharing the same accuracy, the error is the maximal value of the absolute difference between true value and the observation (Line 8-11). With the error ϵ_i of each observation o_i , the true value $T = \arg \max_{t \in O} \left\{ \sum_{o_i \in O} (\max\{Distance(t, o_i) - \epsilon_i, 0\})^2 \right\}$ is selected as following in Line 5 in the following iterations. Then the iteration goes on till converge or reach a given limit.

In total, the time complexity of each iteration is $O(|R|)$, which is linear to the size of data object set.

5 Experimental Results

To verify the effectiveness and efficiency of proposed methods. We perform extensive experiments.

We implemented all algorithm in this paper with C++. All experiments are performed on a PC machine with Intel i5 3450 CPU and 8G main memory.

To test the accuracy, we generate data with different types of data randomly and inject noise randomly to the data. The noise is in uniform distribution. We generate the data with three parameters, the number of true values (#Val), the number of observations sharing the same true value (#Obs) and the possibility that data have error (#Err). The default of #Val, #Obs and #Err are 1M, 4 and 0.1, respectively. For testing the impact of #Val, #Val ranges from 200K

to 1M step by 200M. To test the affect of #Obs, #Obs ranges from 2 to 10 step by 2. We set #Err to be 0.0125, 0.025, 0.05, 0.1, 0.2 and 0.4 to test the impact of #Err.

We perform experiments on efficiency and effectiveness, respectively. We use the trend of accuracy and run time to measure the effectiveness and efficiency, respectively.

5.1 Experimental Results on Measurable Attributes

The experimental results of accuracy evaluation algorithms for measurable attributes are shown in Figure 1. The impacts of #Val on MSE and run time are shown in Figure 1(a) and Figure 1(b), respectively. From the results, #Val has no significant effect on MSE and run time increases polynomially with #Val. Figure 1(c) and Figure 1(d) show the impact of #Obj on effectiveness and efficiency. From the results, #Obj has no affect on MSE for evaluation with true value, while it affects the MSE for the evaluation without true value. While for both of these algorithms, run time is polynomial with #obs. This coincides with the results of values because #Obs also determines the number of variables in the quadratic programming problem. From Figure 1(e) and Figure 1(f), for both algorithms with and without true value, MSE increases with #Err. This shows that MSE represents the ratio of errors effectively and demonstrates the effectiveness of our methods. The efficiency of both of our methods are not affected by #Err. This is because #Err has no affect on the computation of MSE as well as the number of variables and constraints in the quadratic programming problem.

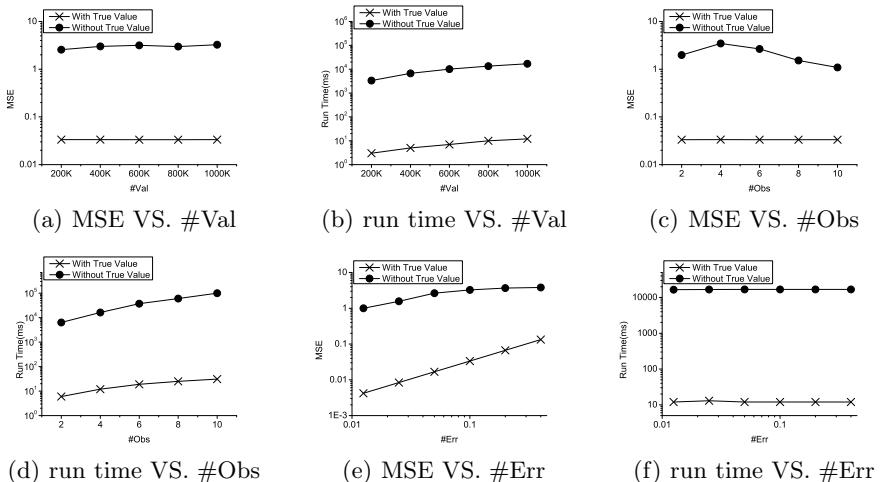


Fig. 1. Experimental Results for Measurable Attributes

5.2 Experimental Results on Comparable Attributes

The experimental results on comparable attributes are shown in Figure 2. From the results, we have following observations. First of all, Figure 2(e) shows that MSE values increase with #Err. It shows that MSE coincides the error ratio that is used to control data accuracy in data generation. From Figure 2(b) and Figure 2(d), our algorithms are polynomial with the data size. A special case is that the run time of algorithm without true value with #Val=600K. This special case is led by a special randomly generated string set that makes the algorithms converge slowly. From Figure 2(f), the run time of the algorithm with true value does not change with #Err while that without true value. For the case without true value, more edit distances should be computed when #Err increases. The last observation is that #Val and #Obs have little impact on the MSE from Figure 2(a) and Figure 2(c). It shows our method for accuracy evaluation for comparable attributes is not affected by the size of data significantly.

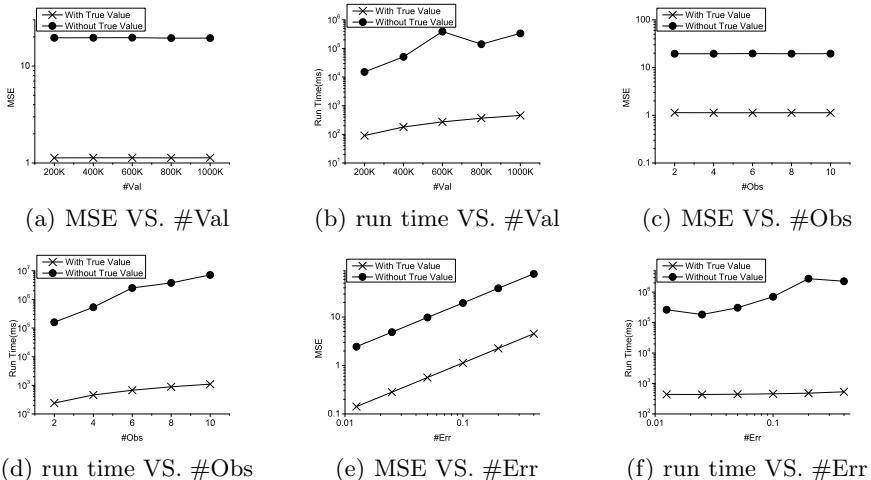


Fig. 2. Experimental Results for Comparable Attributes

Summary of Experiments. From experimental results, we have following results.

1. MSE values increase with error rate in cases of presence and absence of true values. As a result, MSE could represent the accuracy effectively. In the absence of true values, our method could still evaluate accuracy effectively. (Figure 1(e)).
2. Both our algorithm can evaluate algorithm in polynomial time. Thus our algorithms are efficient. (Figure 1(d), Figure 1(b), Figure 2(d), Figure 2(b)).
3. #Val and #Obs have not significant impact on MSE. This shows our evaluation methods are robust. (Figure 1(c), Figure 1(a), Figure 2(c), Figure 2(a)).

6 Conclusions

To evaluate accuracy of sensed data, we use MSE as the measurement. In order to compute the MSE, we classify the attributes in database into three types, measurable, comparable and category. For these three attributes, we design algorithms for MSE estimation for the cases of presence of true values and absence of true values. Experimental results show that our proposed measurements could represent the accuracy effectively and the accuracy evaluation could be accomplished in polynomial time. Future work includes design cloud-based algorithms for accuracy evaluation on massive data set and more experiments on real data.

Acknowledgement. This paper was partially supported by NGFR 973 grant 2012C B316200, NSFC grant 61003046, 61111130189 and NGFR 863 grant 2012AA011004.

References

1. Abadi, D.J., Madden, S., Lindner, W.: Reed: Robust, efficient filtering and event detection in sensor networks. In: VLDB (2005)
2. Elmagarmid, A.K., Ipeirotis, P.G., Verykios, V.S.: Duplicate record detection: A survey. *IEEE Trans. Knowl. Data Eng.* 19(1), 1–16 (2007)
3. Florescu, D., Koller, D., Levy, A.Y.: Using probabilistic information in data integration. In: VLDB, pp. 216–225 (1997)
4. Getoor, L., Machanavajjhala, A.: Entity resolution: Theory, practice & open challenges. *PVLDB* 5(12), 2018–2019 (2012)
5. Kozlov, M.K., Tarasov, S.P., Khachiyan, L.G.: Polynomial solvability of convex quadratic programming. *Doklady Akademii Nauk SSSR* 248
6. Lehmann, E.L., Casella, G.: *Theory of Point Estimation*, 2nd edn. Springer, New York (1998)
7. Li, J., Cheng, S. (ε , δ)-approximate aggregation algorithms in dynamic sensor networks. *IEEE Transactions on Parallel and Distributed Systems* 23(3), 385–396 (2012)
8. Li, J., Cheng, S., Gao, H., Cai, Z.: Approximate physical world reconstruction algorithms in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*
9. Li, M., Liu, Y., Chen, L.: Non-threshold based event detection for 3d environment monitoring in sensor networks. In: ICDCS, p. 9 (2007)
10. Liu, K., Li, M., Liu, Y., Li, X.Y., Li, M., Ma, H.: Exploring the hidden connectivity in urban vehicular networks. In: ICNP, pp. 243–252 (2010)
11. Nocedal, J., Wright, S.J.: *Numerical Optimization*, 2nd edn. Springer, Berlin (2006)
12. Kumar, S.: Sensor information technology for the warfighter. In: Proceedings of the 4th International Conference on Information Fusion, pp. 3–9 (2001)
13. Zhao, B., Rubinstein, B.I.P., Gemmell, J., Han, J.: A bayesian approach to discovering truth from conflicting sources for data integration. *PVLDB* 5(6), 550–561 (2012)

Maximizing Probability of Data Packet Delivery within Deadline

Ran Bi, Hong Gao, and Quan Chen

School of Computer Science and Technology, Harbin Institute of Technology

Harbin, 150001, China

biranhit@gmail.com, {honggao, chenquan}@hit.edu.cn

Abstract. Real-time applications in wireless sensor networks require bounded service latency. There exist many algorithms and routing protocols for efficient data packet delivery. However, previous works set the uniform restriction of retransmissions for the sensor nodes along a deliver path. The method of uniform retransmission threshold is short of taking the link quality and delay requirement into account, which decreases the probability that a packet passes the deliver path within its deadline. This paper first investigates into the problem of computing the optimal retransmission thresholds for relay nodes along a deliver path, such that the summation of the probability that the packet is successfully delivered to the next relay node (or destination node) within its specified deadline is maximized. A distributed greedy algorithm for computing optimal retransmission threshold is provided and the correctness of this algorithm is proved. Experimental results show that the proposed algorithm has better performance in terms of deadline success ratio and real-time ratio.

Keywords: packet delivery, in time, optimal retransmission threshold.

1 Introduction

Real-time applications impose stringent delay requirement on data communication [1–3]. Data delivery delay has been extensively studied in forwarding quality measurement [4–6] and sensor network routing [7–9]. Most of the works focus on investigating the metrics to characterize the forwarding quality or minimizing average path delay. Moreover, existing works set the uniform restriction of retransmissions for the sensor nodes along a deliver path. However, in many cases the retransmission threshold imposes a significant effect on the probability of packet delivery within the specified deadline. The method of uniform retransmission threshold is short of taking the link quality and delay requirement into account, that decreases the success probability of packet transmission over a link of inferior quality. To understand the impact of retransmission threshold on the probability of packet delivery before its deadline, we here give an example, which is illustrated in Figure 1. The number annotating each link is the success probability for a transmission over the link, denoted as p_{suc} , which means that on average it takes $1/p_{suc}$ transmission trials to successfully deliver a packet. The number Δ denotes the delay requirement, which is the deadline divided by once transmission time. If the maximum number of retransmissions for each link is 2, then it is

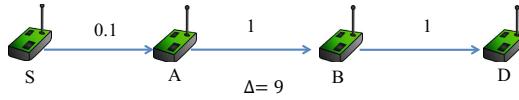


Fig. 1. The impact of retransmission threshold on success probability of packet delivery

easily known that the probability that a packet passes the first link within its deadline is $1 - 0.9 \times 0.9 \times 0.9 = 0.271$. However, if the maximum number of retransmissions for the first link is 6 and the maximum number of retransmissions for others is 0, then the probability that a packet passes the first link within its deadline is $(1 - 0.9^7) \times 1 \times 1 \approx 0.522$. Therefore, the probability that the packet is successfully received by node D within deadline is 0.522, which is almost twice as that of the uniform retransmission method. The approach of uniform retransmission threshold is not optimal for data packet delivery with delay requirement in terms of the probability, that the packet passes the deliver path before its deadline.

To improve the reliability of packet delivery, that a packet is transmitted along multiple paths is widely applied. Therefore, in this paper we focus on computing the optimal retransmission thresholds for the relay nodes along a deliver path, such that the summation of the probability that a packet is successfully delivered to the next relay node (or destination node) within the specified deadline is maximized. To compute the optimal retransmission threshold, a distributed greedy algorithm that can be run on sensor node is developed, which enables the node to adaptively set the optimal retransmission threshold based on the link quality and the remaining time to deadline. The main contributions of the paper are as follows.

- The problem of computing optimal retransmission thresholds for the relay nodes along a delivery path is proposed in this paper. A formal description of the problem is given, and it can be formalized as an integer programming problem.
- A distributed greedy algorithm for computing optimal retransmission threshold is proposed and the correctness of this algorithm is proved. The time complexity of the algorithm is $O(\Delta n)$, and the memory complexity is $O(n)$.
- Simulation experiments are conducted to evaluate the proposed algorithm. Evaluation results show that our algorithm has better performance in terms of deadline success ratio and real-time ratio.

2 Related Works

Data deliver delay is extensively considered in routing metric. The metric of expected transmission count (ETX) was proposed in [10]. ETX measures the expected number of transmissions for successfully delivering a packet over the link, which works well in a homogeneous single-radio environment. Data deliver delay has also been attracted much attention in designing efficient real-time routing protocol. SPEED protocol was proposed in [9], which estimates forwarding delay. Aiming at enabling routing with probabilistic delay bounds in wireless sensing and control (WSC) networks, multi-timescale

adaptation (MTA) routing protocol was proposed in [11], which addresses the challengers of dynamic, uncertain link/path delays in real-time routing. There are plentiful research works that focus on end to end delay analysis in wireless networks. Huang et al. [12] used Chebyshev Inequality for the testing of single-hop real-time satisfiability. A pseudo-polynomial time algorithm optimal-partition-minimum-delay (OPMD) was proposed in [13], which provides an upper bound for probabilistic path delays.

However, previous works set the uniform restriction of retransmissions for the sensor nodes along a deliver path. The method of uniform retransmission threshold is short of taking the link quality and delay requirement into account, which decreases the success probability that a packet passes the deliver path within deadline. To the best of our knowledge, this paper first investigates into the problem of computing optimal retransmission threshold.

3 Greedy Algorithm for Computing Retransmission Threshold

The method of uniform retransmission threshold for the relay nodes along a packet deliver path is deficiency of taking each link quality and delay requirement into account. Therefore, this method enables sensor networks to suffer the low performance in terms of real-time massaging, such as deadline success ratio. In this section, we develop a greedy algorithm for computing the optimal retransmission thresholds for the relaying nodes along a deliver path, such that the summation of the probability that a packet is successfully delivered to the next relay node (or destination node) within the specified deadline is maximized.

3.1 Problem Formulation

Suppose that the end to end path is $P=j_1, j_2, \dots, j_{n+1}$, in which j_1 and j_{n+1} are source node and destination node respectively. Let p_i denote the failure probability for a transmission over link $j_i \rightarrow j_{i+1}$. Then p_i is the probability that a MAC-layer transmission fails due to either collisions or bad channel quality when node j_i forwards a data packet to node j_{i+1} . If K_i is the retransmission threshold of node j_i , then $1 - p_i^{K_i+1}$ is the probability that a packet is successfully delivered to node j_{i+1} by node j_i . To improve the reliability of packet delivery, packets are transmitted along multiple paths. Therefore, we aim at maximizing the summation of the probability that a packet is successfully delivered to the next relay node (or destination node) along the path, subject to the deadline constraint. Let Δ denote the end-to-end delay requirement. For node i , L_i and U_i are used to denote the lower and upper bounds of retransmission threshold respectively. The problem can be formulated as the following integer programming problem.

$$\begin{aligned} & \max \sum_{i=1}^n \left(1 - p_i^{K_i+1}\right) \\ & \text{s.t. } \sum_{i=1}^n (K_i + 1) \leq \Delta \\ & \quad L_i \leq K_i \leq U_i, \\ & \quad K_i \in \mathbb{Z}, i \in \{1, 2, \dots, n\} \end{aligned} \tag{1}$$

Obviously, the value of objective function $\sum_{i=1}^n (1 - p_i^{K_i+1})$ is maximized if and only if the value of $\sum_{i=1}^n p_i^{K_i+1}$ achieves the minimum. For any $i \in \{1, 2, \dots, n\}$, let $k_i = K_i + 1$, $l_i = L_i + 1$ and $u_i = U_i + 1$. Then the aforementioned optimization problem is equivalent to the following integer programming problem.

$$\begin{aligned} & \min \sum_{i=1}^n p_i^{k_i} \\ & \text{s.t. } \sum_{i=1}^n k_i \leq \Delta \\ & l_i \leq k_i \leq u_i, k_i \in \mathbb{Z}, i \in \{1, 2, \dots, n\} \end{aligned} \tag{2}$$

The problem of computing the optimal retransmission thresholds for each relay node along a packet deliver path is defined as follows.

Input:

1. The transmission failure probability set of the nodes along a path, $\{p_1, \dots, p_n\}$.
2. The end-to-end delay requirement Δ .

Output:

Optimal retransmission thresholds k'_1, k'_2, \dots, k'_n , which is an optimal solution to integer programming problem (2).

Based on the above analysis, the key point is to design an efficient algorithm for finding an optimal solution to integer programming problem (2). In the following section, we prove that the optimization problem is solved by a greedy algorithm and the correctness of the proposed algorithm is also provided.

3.2 Correctness of Greedy Algorithm

Lemma 1. For any $i \in \{1, 2, \dots, n\}$, $j \in \{1, 2, \dots, u_i - l_i\}$, if $0 < p_i < 1$, then the following inequalities are hold.

$$p_i^{l_i+j} - p_i^{l_i+j-1} < p_i^{l_i+j+1} - p_i^{l_i+j} < 0 \tag{3}$$

Proof. Let $f_i(x) = p_i^x$, it is easily known that $f''_i(x) > 0$. Therefore, $f_i(x)$ is a convex function and $f'_i(x)$ is an increasing function with respect to x . For any $y > z$, $f'_i(y) > f'_i(z)$ is hold. According to the differential mean value theorem, the following equalities can be derived,

$$f_i(l_i + j + 1) - f_i(l_i + j) = f'_i(\xi) \cdot 1 \tag{4}$$

$$f_i(l_i + j) - f_i(l_i + j - 1) = f'_i(\eta) \cdot 1 \tag{5}$$

in which, $\xi \in (l_i + j, l_i + j + 1)$, $\eta \in (l_i + j - 1, l_i + j)$. Since $f'_i(x)$ is an increasing function, then $f'_i(\eta) < f'_i(\xi)$. It is easily derived that $p_i^{l_i+j} - p_i^{l_i+j-1} < p_i^{l_i+j+1} - p_i^{l_i+j}$. Due to the decreasing of $f_i(x)$, we have $p_i^{l_i+j+1} - p_i^{l_i+j} < 0$. In conclusion, we know that $p_i^{l_i+j} - p_i^{l_i+j-1} < p_i^{l_i+j+1} - p_i^{l_i+j} < 0$. In conclusion, we know that $p_i^{l_i+j} - p_i^{l_i+j-1} < p_i^{l_i+j+1} - p_i^{l_i+j} < 0$. \square

For any $i \in \{1, 2, \dots, n\}$, $j \in \mathbb{Z}^+$, $\lambda_i(j)$ is defined as follows, in which $l_i < u_i$.

$$\lambda_i(j) = \begin{cases} p_i^j - p_i^{j-1} & j \leq u_i \\ \infty & j > u_i \end{cases} \quad (6)$$

Based on Lemma 1, we have $\lambda_i(j+1) > \lambda_i(j)$, for any $j \in [l_i, u_i - 1]$. And it is known that $p_i^{l_i+j} = p_i^{l_i} + \sum_{k=l_i+1}^{l_i+j} \lambda_i(k)$. For any $i \in \{1, 2, \dots, n\}$, we introduce the following sign function.

$$\chi_i(x) = \begin{cases} 1 & x = i \\ 0 & x \neq i \end{cases} \quad (7)$$

Lemma 2. Let $h = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, then $l_1 + \chi_1(h), l_2 + \chi_2(h), \dots, l_n + \chi_n(h)$ is an optimal solution to the following integer programming problem.

$$\begin{aligned} & \min \sum_{i=1}^n p_i^{k_i} \\ & \text{s.t. } \sum_{i=1}^n k_i \leq 1 + \sum_{i=1}^n l_i \\ & \quad l_i \leq k_i \leq u_i, \\ & \quad k_i \in \mathbb{Z}, i \in \{1, 2, \dots, n\} \end{aligned} \quad (8)$$

Proof. It is easily verified that the solution $l_1 + \chi_1(h), l_2 + \chi_2(h), \dots, l_n + \chi_n(h)$ satisfies the constraints of optimization problem (8). For any $i \in \{1, 2, \dots, n\}$, the objective function is decreasing with respect to k_i . Then it is easily derived that the necessary condition of objective function value achieving the minimal is that $\sum_{i=1}^n k_i = 1 + \sum_{i=1}^n l_i$. Suppose that $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution. According to the constraints, we know that $k_i^* \geq l_i$, for $i \in \{1, 2, \dots, n\}$. Then it can be derived that there exist $j \in \{1, 2, \dots, n\}$, such that k_j^* satisfies the following formula.

$$k_j^* = \begin{cases} l_i & i \neq j \\ l_i + 1 & i = j \end{cases} \quad (9)$$

It is easily derived that $\sum_{i=1}^n p_i^{l_i+\chi_i(h)} - \sum_{i=1}^n p_i^{k_i^*} = p_h^{l_h+1} + p_j^{l_j} - p_h^{l_h} - p_j^{l_j+1} = (p_h^{l_h+1} - p_h^{l_h}) - (p_j^{l_j+1} - p_j^{l_j}) = \lambda_h(l_h + 1) - \lambda_j(l_j + 1)$. Since $\lambda_h(l_h + 1) = \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, then $\sum_{i=1}^n p_i^{l_i+\chi_i(h)} - \sum_{i=1}^n p_i^{k_i^*} \leq 0$. In conclusion, $l_1 + \chi_1(h), l_2 + \chi_2(h), \dots, l_n + \chi_n(h)$ is the optimal solution to problem (8). \square

Lemma 3. Let $h = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, if $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to the following integer programming problem, then $k_h^* \geq l_h + 1$, in which Λ is a given positive integer.

$$\begin{aligned}
& \min \sum_{i=1}^n p_i^{k_i} \\
& \text{s.t. } \sum_{i=1}^n k_i \leq \Lambda + \sum_{i=1}^n l_i \\
& \quad l_i \leq k_i \leq u_i, \\
& \quad k_i \in \mathbb{Z}, i \in \{1, 2, \dots, n\}
\end{aligned} \tag{10}$$

Proof. The proof is by induction on Λ . According to Lemma.2, $k_h^* \geq l_h + 1$ is hold, when $\Lambda = 1$. Suppose that when $\Lambda \leq m - 1$, the proposition is hold. We want to prove that when $\Lambda = m$, $k_h^* \geq l_h + 1$ is hold. And the proof is by contradiction. Suppose that $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to problem (10), and $k_h^* < l_h + 1$. According to the constraint, we know that $k_h^* = l_h$. For any $i \in \{1, 2, \dots, n\}$, the objective function is decreasing with respect to k_i . Then it can be known that $\sum_{i=1}^n k_i^* = \Lambda + \sum_{i=1}^n l_i$. Therefore, there must exist $r \in \{1, 2, \dots, n\}$, such that $k_r^* \geq l_r + 1$. We define k'_1, k'_2, \dots, k'_n as follows.

$$k'_i = \begin{cases} k_i^* & i \neq h, i \neq r \\ k_i^* + 1 & i = h \\ k_i^* - 1 & i = r \end{cases} \tag{11}$$

It is easily verified that the solution k'_1, k'_2, \dots, k'_n satisfies the constraints, then it is a feasible solution to optimization problem (10). We can derive that $\sum_{i=1}^n p_i^{k'_i} - \sum_{i=1}^n p_i^{k_i^*} = p_h^{l_h+1} + p_r^{k_r^*-1} - p_h^{l_h} - p_r^{k_r^*} = (p_h^{l_h+1} - p_h^{l_h}) - (p_r^{k_r^*} - p_r^{k_r^*-1}) = \lambda_h(l_h + 1) - \lambda_r(k_r^*)$. Since $\lambda_r(j)$ is an increasing function with respect to j , then $\lambda_r(k_r^*) \geq \lambda_r(l_r + 1)$. Since $\lambda_h(l_h + 1) = \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, then $\lambda_r(l_r + 1) > \lambda_h(l_h + 1)$. Therefore, it can be derived that $\sum_{i=1}^n p_i^{k'_i} - \sum_{i=1}^n p_i^{k_i^*} < 0$, which contradicts the fact that $k_1^*, k_2^*, \dots, k_n^*$ is the optimal solution. In conclusion, it is proved that $k_h^* \geq l_h + 1$. \square

Theorem 1. If $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to integer programming problem (10), then $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to the following integer programming problem, in which $h = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$.

$$\begin{aligned}
& \min \sum_{i=1}^n p_i^{k_i} \\
& \text{s.t. } \sum_{i=1}^n k_i \leq \Lambda - 1 + (l_h + 1) + \sum_{i=1, i \neq h}^n l_i \\
& \quad l_i \leq k_i \leq u_i, i \in \{1, 2, \dots, n\} - \{h\} \\
& \quad l_h + 1 \leq k_h \leq u_h, \\
& \quad k_i \in \mathbb{Z}, i \in \{1, 2, \dots, n\}
\end{aligned} \tag{12}$$

Proof. According to Lemma.3, it can be verified that the solution k_1^*, \dots, k_n^* satisfies the constraints and it is a feasible solution to problem (12). We prove that k_1^*, \dots, k_n^* is an optimal solution by contradiction. Suppose that k'_1, k'_2, \dots, k'_n is an optimal solution to problem (12), and $\sum_{i=1}^n p_i^{k'_i} < \sum_{i=1}^n p_i^{k_i^*}$ is hold. Due to $l_h + 1 \leq k'_h \leq u_h$, we have $l_h \leq k'_h \leq u_h$. Then k'_1, k'_2, \dots, k'_n is a feasible solution to integer programming problem (10). It can be known that k'_1, k'_2, \dots, k'_n is a better solution to problem (10), which contradicts the fact that k_1^*, \dots, k_n^* is an optimal solution. In conclusion, $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to problem (12). \square

Theorem 2. Let $h_1 = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, for any $r \in \{2, \dots, \Lambda\}$, h_r is defined as follows.

$$h_r = \arg \min \left\{ \{\lambda_i(j) | i \in \{1, 2, \dots, n\}, j \in \{l_i + 1, \dots, u_i\}\} - \bigcup_{z=1}^{r-1} \left\{ \lambda_{h_z} \left(l_{h_z} + \sum_{m=1}^z \chi_{h_z}(h_m) \right) \right\} \right\} \quad (13)$$

Then $l_1 + \sum_{r=1}^{\Lambda} \chi_1(h_r), l_2 + \sum_{r=1}^{\Lambda} \chi_2(h_r), \dots, l_n + \sum_{r=1}^{\Lambda} \chi_n(h_r)$ is an optimal solution to integer programming problem (10).

Proof. The proof is by induction on Λ . According to Lemma.2, $l_1 + \sum_{r=1}^{\Lambda} \chi_1(h_r), l_2 + \sum_{r=1}^{\Lambda} \chi_2(h_r), \dots, l_n + \sum_{r=1}^{\Lambda} \chi_n(h_r)$ is an optimal solution, when $\Lambda = 1$. Suppose that when $\Lambda \leq m - 1$, the proposition is hold. We want to prove that when $\Lambda = m$, the proposition is hold. Suppose that $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to problem (10), when $\Lambda = m$. Let $h = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, according to Theorem.1, we know that $k_1^*, k_2^*, \dots, k_n^*$ is an optimal solution to the following integer programming problem.

$$\begin{aligned} & \min \sum_{i=1}^n p_i^{k_i} \\ & \text{s.t. } \sum_{i=1}^n k_i \leq m - 1 + (l_h + 1) + \sum_{i=1, i \neq h}^n l_i \\ & \quad l_i \leq k_i \leq u_i, i \in \{1, 2, \dots, n\} - \{h\} \\ & \quad l_h + 1 \leq k_h \leq u_h, \\ & \quad k_i \in Z, i \in \{1, 2, \dots, n\} \end{aligned} \quad (14)$$

Let $h'_1 = \arg \min \{\{\lambda_i(j) | i \in \{1, 2, \dots, n\}, j \in \{l_i + 1, \dots, u_i\}\} - \{\lambda_h(l_h + 1)\}\}$. For any $r \in \{2, \dots, m - 1\}$, h'_r is defined as follows.

$$h'_r = \arg \min \left\{ \{\lambda_i(j) | i \in \{1, \dots, n\}, j \in \{l_i + 1, \dots, u_i\} - \{\lambda_h(l_h + 1)\}\} - \bigcup_{z=1}^{r-1} \left\{ \lambda_{h'_z} \left(l_{h'_z} + \sum_{m=1}^z \chi_{h'_z}(h'_m) \right) \right\} \right\}.$$

By the induction hypothesis, $l_1 + \sum_{r=1}^{m-1} \chi_1(h'_r), \dots, l_{h-1} + \sum_{r=1}^{m-1} \chi_{h-1}(h'_r), l_h + 1 + \sum_{r=1}^{m-1} \chi_h(h'_r), l_{h+1} + \sum_{r=1}^{m-1} \chi_{h+1}(h'_r), \dots, l_n + \sum_{r=1}^{m-1} \chi_n(h'_r)$ is an optimal solution to problem (14), and the value of

objective function achieves $\sum_{i=1}^n p_i^{k_i^*}$. Therefore, when $\Lambda = m$, we can know that $l_1 + \sum_{r=1}^{m-1} \chi_1(h'_r) + \chi_1(h), l_2 + \sum_{r=1}^{m-1} \chi_2(h'_r) + \chi_2(h), \dots, l_h + \sum_{r=1}^{m-1} \chi_h(h'_r) + \chi_h(h), \dots, l_n + \sum_{r=1}^{m-1} \chi_n(h'_r) + \chi_n(h)$ is an optimal solution to problem (10).

Let $h_1 = \arg \min_{i \in \{1, 2, \dots, n\}} \{\lambda_i(l_i + 1)\}$, and for any $r \in \{2, \dots, m\}$, h_r is defined according to formula (13). It is easily known that for any $i \in \{1, 2, \dots, n\}$, $l_i + \sum_{r=1}^{m-1} \chi_i(h'_r) + \chi_i(h) = l_i + \sum_{r=1}^m \chi_i(h_r)$. In conclusion, for a given positive integer Λ , $l_1 + \sum_{r=1}^{\Lambda} \chi_1(h_r), \dots, l_n + \sum_{r=1}^{\Lambda} \chi_n(h_r)$ is an optimal solution to problem (10). \square

3.3 Greedy Algorithm for Computing Optimal Retransmission Threshold

According to Theorem.1 and Theorem.2, we know that integer programming problem (10) exhibits the optimal substructure and greedy-choice properties. In this section, a greedy algorithm for computing the optimal retransmission threshold is proposed. Suppose that the end to end path is $P = j_1, j_2, \dots, j_{n+1}$, in which j_1 and j_{n+1} are source node and destination node respectively. Let p_i denote the transmission failure probability over link $j_i \rightarrow j_{i+1}$. Suppose that relay node j_i receives a data packet with delay requirement Δ' . The greedy algorithm for computing optimal retransmission threshold runs at sensor node j_i as follows. The retransmission thresholds for nodes j_i, j_{i+1}, \dots, j_n are initialized as L_i, L_{i+1}, \dots, L_n respectively, where L_h is the lower bound of retransmission threshold for node j_h . First, for each $h \in \{i, i+1, \dots, n\}$, compute $p_h^{L_h+2} - p_h^{L_h+1}$. Then, the L_h with the minimum value $p_h^{L_h+2} - p_h^{L_h+1}$ is incremented by one. The above procedures are repeated $\Delta' - \sum_{h=i}^n (L_h + 1)$ times.

4 Performance Evaluation

In this section, experiments have been carried out to evaluate the performance of **greedy algorithm** for computing **optimal retransmission threshold** (GAORT). 100 sensor nodes and the sink are randomly deployed into a region of size $200m \times 200m$ (m for meters) and we assume that the sensors have the same transmission radius. In each simulation, source node and destination node are randomly selected. Each simulation is repeated 100 times and the simulation result corresponds to the average value over 100 times. To the best of our knowledge, existing works(general method) set the uniform retransmission threshold for the sensor nodes and this is the first work that investigates into the problem of computing the optimal retransmission thresholds. To understand the benefits of GAORT method, the comparison with general method is conducted. The first group of experiments is to investigate the deadline success ratio (DSR) of GAORT , in which deadline success ratio is the ratio of packets delivered to the destination before their deadlines. Figure.2(a) shows the comparison of deadline success ratio between the method of GAORT and General Method, in which Δ is computed as the deadline divided by once transmission time. GAORT has better performance in term of deadline

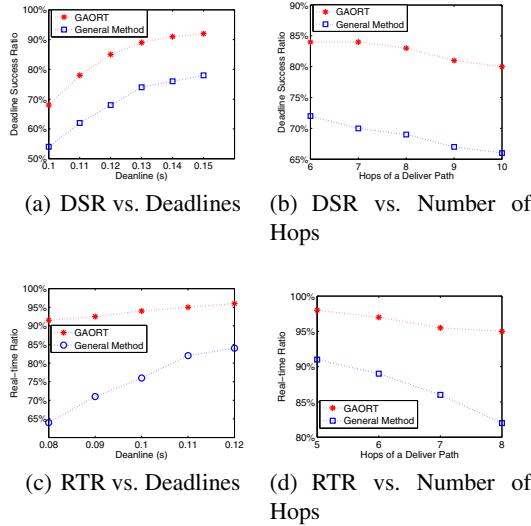


Fig. 2. Effectiveness of GAORT Method

success ratio. Figure.2(b) presents the DSRs under different hops. Since delay requirement and link quality have been taken into account by our algorithm. As expected, GAORT can achieve a higher deadline success ratio. The second group of experiments is to investigate the real-time ratio (RTR) of GAORT, in which real-time ratio is the ratio of packets delivered to the destination before their deadlines among the packets successfully delivered to the destination node. As shown in Figure.2(c), the method of GAORT can reach higher real-time ratio than that of General Method. Figure.2(d) indicates that GAORT has better performance in term of RTR, when the hops of a deliver path vary. The method of GAORT can reduce the deliveries of the packets, that can not meet their delay requirements. Therefore, GAORT improves the real-time ratio and the energy efficiency.

5 Conclusion

There exist many algorithms and routing protocols for efficient data packet delivery. However, previous works set the uniform restriction of retransmissions for the sensor nodes along a deliver path, that ignore the impact of retransmission threshold on the probability of packet delivery before its deadline. This paper first investigates into the problem of calculating the optimal retransmission thresholds for relay nodes along a deliver path, such that the summation of the probability that a packet is successfully delivered to the next relay node (or destination node) within the specified deadline is maximized. A distributed greedy algorithm for computing optimal retransmission threshold is provided and the correctness of this algorithm is proved. Experimental results show that the proposed algorithm has better performance in terms of deadline success ratio and real-time ratio.

Acknowledgement. This work is supported in part by the National Grand Fundamental Research 973 Program of China under grant 2012CB316200, the Key Program of the National Natural Science Foundation of China under grant 61033015,60933001, the Major Program of National Natural Science Foundation of China under grant 61190115, and the National Science Foundation Distinguished Young Scholars of China under grant 61300225.

References

1. Li, Y., Chen, C.S., Song, Y.-Q., et al.: Enhancing Real-Time Delivery in Wireless Sensor Networks With Two-Hop Information. *Transactions on Industrial Informatics* 5(2), 113–122 (2009)
2. Kadri, A., et al.: Wireless sensor network for real-time air pollution monitoring. In: 1st International Conference on Communications, Signal Processing, and their Applications, pp.1–5. IEEE (2013)
3. Liu, G., et al.: Volcanic earthquake timing using wireless sensor networks. In: 12th International Conference on Information Processing in Sensor Networks, pp. 9–102. ACM (2013)
4. Wang, J., Liu, Y., Li, M., et al.: QoF: Towards comprehensive path quality measurement in wireless sensor networks. In: IEEE INFOCOM, pp. 775–783 (2011)
5. Lin, S., Zhou, G., Whitehouse, K., et al.: Towards stable network performance in wireless sensor networks. In: IEEE RTSS, pp. 227–237 (2009)
6. Zhang, H., Sang, L., Arora, A.: Comparison of data-driven link estimation methods in low-power wireless networks. *IEEE Transactions on Mobile Computing* 9, 1634–1648 (2010)
7. Li, H., Cheng, Y., Zhou, C.: Minimizing end-to-end delay: A novel routing metric for multi-radio wireless mesh networks. In: IEEE INFOCOM, pp. 46–54 (2009)
8. Yin, S., Xiong, Y., Zhang, Q., Lin, X.: Traffic-aware routing for real-time communications in wireless multi-hop networks. *Jouranl of Wireless Communications and Mobile Computing* (6), 825–843 (2006)
9. He, T., Stankovic, J., Lu, C., et al.: SPEED: A stateless protocol for real-time communication in sensor networks. In: IEEE ICDCS, pp. 46–55 (2003)
10. De Couto, D.S.J., Aguayo, D., Bicket, J., Morris, R.: A High-Throughput Path Metric for Multi-Hop Wireless Routing. In: ACM MOBICOM, pp. 134–142 (2003)
11. Liu, X., et al.: Taming uncertainties in real-time routing for wireless networked sensing and control. *IEEE Transactions on Smart Grid* 4(1), 288–301 (2012)
12. Huang, X., Fang, Y.: Multiconstrained QoS multipath routing in wireless sensor networks. *Journal of Wireless Networks* (14), 465–478 (2008)
13. Liu, X., Zhang, H., Xiang, Q.: Towards predictable real-time routing for wireless networked sensing and control. In: CPS Week RealWin Workshop (2011)

Model-Based Approximate Event Detection in Heterogeneous Wireless Sensor Networks

Jing Gao and Jianzhong Li*

Department of Computer Science and Technology, Harbin Institute of Technology,
90 West Dazhi Street, P.O. Box 750, Harbin, China
{jinggao,ljzj}@hit.edu.cn

Abstract. Computing and analyzing different types of data generated by a large number of heterogeneous devices have been an important issue demanding prompt solution in the research of Wireless Sensor Networks (WSNs). Due to the restricted computing capability and limited energy of the sensor nodes, this paper investigates the approximate composite event detection problem where composite events are integrated by multi-mode data generated by different types of sensors. Algorithms are proposed to compute the optimal transmitting scheme with minimum cost on the constraint that the confidence of the composite event must exceed the threshold. The optimal transmitting scheme problem is formulated and proved to be NP-complete. A dynamic programming based algorithm which runs in pseudo-polynomial time is presented for simple confidence combination operators, and a 2-approximate algorithm is devised for more complex situation. The experimental results demonstrate the effectiveness and efficiency of the proposed algorithms.

Keywords: Heterogeneous Wireless Sensor Networks, event detection, event model.

1 Introduction

Heterogeneous sensors in wireless sensor networks have different capabilities in terms of communication, computation, sensing and so forth. The application areas of WSNs include national security, environment monitoring, transportation, advanced manufacturing and medical technologies. In many applications the robustness and reliability of the network will be increased by deploying heterogeneous nodes[1]. WSNs with heterogeneous sensors are also one of the key components for cyber-physical systems[2].

Event detection is one of the major tasks in WSNs [3–5]. Most of the traditional event detection techniques aim to detect “simple” event in homogeneous

* This work was supported in part by the Major Program of National Natural Science Foundation of China under grant No. 61190115, the National Basic Research Program of China (973 Program) under grant No. 2012CB316200, and the National Natural Science Foundation of China (NSFC) under grants No. 61033015, No. 60933001 and No. 61100030.

WSNs [6–8]. This “simple” event only involves single-mode data characterizing an aspect of an object or a partial state of the physical world. However, single-mode data cannot describe the complicated phenomena in physical world[9, 10]. For example, in a battlefield surveillance system, light intensity, loud sound, smoke density and high temperature are all necessary information to characterize exploding bomb event. So in this paper we investigate the composite event detection problem in WSNs.

Composite event consisting of several atomic events or multi-mode data may be difficult to detect. Some kinds of data such as multimedia data bring numerous energy and bandwidth consumption during sensing, transmitting and processing. Some types of data can not even be processed by sensor nodes with limited computing capability. Moreover, “event” in WSNs always occurs in small probability. Continuously collecting all the multi-modal data not just causes enormous energy overhead, but most of the data are “useless” since no event occurs in that period. Collecting all the data for event detection is infeasible. Uncertainty is an inherent property for WSNs due to the noises and instability of the devices. Approximation is a natural way to process the sensing data in resource-constrained sensor networks. So in this paper we propose the a model-based approximate event detection technique.

In this paper events are classified into atomic events and composite events. The minimum data reflected the physical world state or the information of the object is defined as atomic event, with only one type of data involved. Several atomic events which satisfy some specific temporal and spatial constraints are composed to generate composite events. The occurrence of a composite event indicates that all the primitive events occur as well as all the constraints are satisfied. The atomic events generated by multi-modal data integrate by predefined pattern of composite event. For example, in a battlefield surveillance system, light sensors, temperature sensors, audio sensors and smoke sensors are deployed in the field of interest to monitor and track explosion event. When a bomb explodes in the monitored area, these four types of sensors can detect anomalies and generate corresponding data. A “bomb explosion” event can be determined by jointly processing all the sensing data.

In order to support approximate event detection, a confidence is attached to every atomic event which can be considered as the possibility of the occurrence of a composite event on condition that atomic event occurs. The occurrence of each atomic event provides support or can be seen as the evidence for the occurrence of a composite event. The confidence of the atomic events can be merged according to predefined rules. When more atomic events are detected, the confidence value of the composite event increases until this confidence exceeds the threshold. This model can process approximate event detection. The “easy” atomic events are handled at first, and meanwhile the confidence of these events is merged as the partial confidence of the composite events. If the partial confidence does not meet the demand of the application, the “complex” atomic events are processed further. It is not necessary to process and analyze the complex data such as multimedia data continuously. On the contrary these complex data just need to

be processed when the event is most likely to occur. A large amount of energy consumption can be saved and the latency of the detection is reduced.

Based on the event model, we study the approximate event detection problem with a confidence constraint. The goal is to decide which atomic event should be transmitted to the base station such that the confidence of the composite event by merging all the received atomic events satisfies the confidence threshold at the same time the total transmitting cost is minimized. We study the optimal transmitting scheme problem and present two algorithms to solve this problem.

The contributions of this paper are as follows.

- The optimal transmitting scheme problem is formulated. The NP-completeness of the problem is analyzed
- An exact algorithm based on dynamic programming technique is presented to solve the optimal transmitting scheme problem, whose time complexity is $O(\Delta k)$ for linear confidence combination operator, where Δ is the confidence threshold and k is the number of types of sensors.
- A approximate greedy algorithm is also proposed with time complexity $O(k \log k)$. The approximation ratio is proven to be 2 for “+” as the confidence combination operator.
- Extensive simulations were conducted to evaluate efficiency and the performance of our algorithms.

The rest of this paper is organized as follows. Related works are presented in Section 2. The preliminaries about event model are described in Section 3. In Section 4, we present the definitions of the optimal transmitting scheme problem and analyze the complexity. In Section 5, an exact algorithm and the approximate algorithm are illustrated and analyzed. We provide the experimental results in Section 6 and conclude the paper in Section 7.

2 Related Works

There are many publications in the literature to study the event detection problem. Different methods are proposed to detect event generated by homogeneous data in [6–8]. Physical world reconstruction methods proposed in [12, 13] with error bound of $O(\epsilon)$ can improve the precision of the event detection. Multi-cast routing technique proposed in [14, 15] can be adopted to collect event data fast and efficiently. In [16] an area query processing method is presented which can detect event area quickly and distributively. But composite event detection technique is not mentioned in all the above methods. Composite event detection problem is discussed and studied in [4, 5] focusing on exact event detection.

3 Preliminaries

In this section we describe the event model. An event in WSNs is an occurrence of a phenomenon of interest during a period of time within monitoring area.

Events consist of atomic events and composite events. Atomic events only involve single-mode data to characterize partial information of the composite event. We use $e(t, s)$ to represent an atomic event, where t is the time that the event occurs. Note that in WSNs time is always discrete. Therefor time-interval can be considered as a collection of time point within the endpoint of the interval. s is the locality that the event occurs. In WSNs we can use the serial number or the id of the device detecting the event to roughly denote the location of the event. e is associated with the constraints of attribute of the sensing data to describe the types of the event. e.g. e_1 is associated with temperature and defined as temperature larger than 25°C. $e_1(t_1, s_1)$ indicates the temperature is larger than 25°C at time t_1 in area s_1 . Composite events are composed by atomic events which satisfy the predefined temporal and spatial constraints. We use $E = \{e_1, e_2, \dots, e_k | T = \{t_1, t_2, \dots, t_k\} \models C(T), S = \{s_1, s_2, \dots, s_k\} \models C(S)\}$ to represent a composite event consisting of k atomic events, where $C(T)$ and $C(S)$ are the sets of temporal and spacial constraints respectively. $T = \{t_1, t_2, \dots, t_k\} \models C(T)$ and $S = \{s_1, s_2, \dots, s_k\} \models C(S)$ mean the k atomic events satisfy the temporal and spacial constraints.

Given a composite event $E = \{e_1, e_2, \dots, e_k\}$, confidence $\delta_1, \delta_2, \dots, \delta_k$ are assigned to each atomic event to support flexible approximate event detection. The confidence of an atomic event satisfies $0 \leq \delta_i \leq 1$ and can be considered as an indication of the occurrence of the composite event. The confidence of an atomic event indicates the possibility of the occurrence of the composite event on condition that the atomic event occurs. We denote \oplus as a combination operator for confidence. The confidence increases with the merging of the atomic events. If all the k atomic events occurs, then the confidence of the composite event is $\delta_1 \oplus \delta_2 \oplus \dots \oplus \delta_k = 1$.

The combination operator for confidence can be defined by the users based on the requirements of the application. There are two kinds of combination operators, linear operator and nonlinear operator. Arithmetic “+” can be set as linear combination operators. Some complex combination rules such as Dempster-Shafer’s rule [17] can be used as nonlinear operator.

The confidence of every atomic event can be assigned by the field experts, or obtained by analyzing and mining the historic data [18]

4 Problem Description

4.1 Problem Formulation

In the event model, suppose the composite event that the system aims to detect consists of k atomic events, and the atomic events are generated by different nodes. The transmitting cost for each kinds of atomic events is c_i . The confidence of the atomic event e_i is δ_i . The user-specified confidence threshold is Δ . The network needs to compute which types of data should be transmitted to the base station so that the event can be detected with the confidence no less than Δ and at the same time the energy cost is reduced to the minimum.

Definition 1 (Transmitting Scheme). A transmitting scheme T for composite event $E = \{e_1, e_2, \dots, e_k\}$ is denoted as $T = \{x_1, x_2, \dots, x_k\}$, where $x_i \in \{0, 1\}$,

$$x_i = \begin{cases} 1 & \text{the data of atomic event } e_i \text{ are transmitted to the base station} \\ 0 & \text{the data don't need to be transmitted} \end{cases}$$

Definition 2. (Optimal Transmitting Scheme Problem (OTS)) Given the cost of each type of atomic event c_1, c_2, \dots, c_k , the corresponding confidence $\delta_1, \delta_2, \dots, \delta_k$ for each atomic event and the total confidence threshold Δ , find a best transmitting scheme $T = \{x_1, x_2, \dots, x_k\}$ such that the confidence of the composite event according to the transmitting scheme is no less than Δ and the transmitting cost is minimized.

$$\min \sum_{i=1}^k c_i x_i \quad (1)$$

s.t.

$$\delta_1 x_1 \oplus \delta_2 x_2 \oplus \dots \oplus \delta_k x_k \geq \Delta \quad (2)$$

$$x_i \in \{0, 1\} \quad (3)$$

$$i = 1, 2, \dots, k \quad (4)$$

4.2 Complexity

Theorem 1. The optimal transmitting scheme problem for approximate event detection is NP-complete when the confidence combination operator “ \oplus ” is “ $+$ ”.

Proof. The OTS problem is clearly in NP since any guessed answer can be tested in polynomial time with “ $+$ ” as the combination operator.

To prove OTS problem is NP-hard, we reduce 0-1 knapsack problem to OTS problem. The 0-1 knapsack problem can be formulated as follows. Let there be n items, where each item i has a value v_i and weight w_i . y_i is the number of copies of the item i , which must be zero or one. The maximum weight that we can carry in the bag is W . Then we want to fill the bag with the most valuable items so that total value is as large as possible,

$$\max \sum_{i=1}^n v_i y_i$$

s.t.

$$\sum_{i=1}^n w_i y_i \leq W$$

$$y_i \in \{0, 1\}$$

The transformation is shown as follows. Let $C = \sum_{i=1}^n w_i$ and $k = n$. Then $\delta_i = \frac{w_i}{C}$. $\Delta = 1 - \frac{W}{C}$. $c_i = v_i$. The OTS problem is

$$\min \sum_{i=1}^k c_i x_i$$

s.t.

$$\sum_{i=1}^k \delta_i x_i \geq \Delta$$

$$x_i \in \{0, 1\}$$

Clearly the above transformation can be done in polynomial time. So the remains to show is that 0-1 knapsack problem is solvable iff the OTS problem has a solution: Let $Y = \{y_1, y_2, \dots, y_k\}$ be the solution to 0-1 knapsack problem. Then we get $X = \{x_1, x_2, \dots, x_k\}$ where $x_i = 1 - y_i$. It is not hard to testify $X = \{x_1, x_2, \dots, x_k\}$ is the solution to OTS problem. The sufficiency can be proved as the same.

By Theorem 1 it can be concluded that the general OTS problem with any legal confidence combination operator is at least NP-complete.

5 Algorithms

In this section we propose two algorithms to solve OTS problem. The dynamic programming algorithm computes the exact solution in pseudo-polynomial time, which is applicable for linear confidence combination operators. The 2-approximate algorithm is proposed based on greedy technique which is suitable for nonlinear and complex confidence combination operators.

5.1 Dynamic Programming Algorithm

We use dynamic programming technique to solve the OTS problem for linear confidence combination operators(e.g. “+”). We define operator “ \ominus ” as the inverse operation of “ \oplus ”, that is $\delta_i = \delta_l \ominus \delta_j$ for $\delta_i \oplus \delta_j = \delta_l$ (e.g. “ $-$ ” is the inverse operation of “ $+$ ”).

Let $m(i, j)$ be the minimum cost when the threshold $\Delta = j$ and the transmitting atomic events are from e_1, e_2, \dots, e_i . Then we obtain the recursive formulation

$$m(i, j) = \begin{cases} \min\{m(i-1, j), c_i\} & \text{if } 0 \leq j \leq \delta_i \\ \min\{m(i-1, j \ominus \delta_i) + c_i, m(i-1, j)\} & \text{if } j > \delta_i \end{cases} \quad (5)$$

And

$$m(1, j) = \begin{cases} c_1 & \text{if } 0 \leq j \leq \delta_1 \\ \infty & \text{if } j > \delta_1 \end{cases}$$

where $m(1, j) = \infty$ means the unsolvable situation.

Algorithm 1. OTS-DP($(\delta_1, \delta_2, \dots, \delta_k), (c_1, c_2, \dots, c_k), \Delta$)

```

1: Initialization  $m(1, j) = c_1$  for  $j = 0$  to  $\delta_1$  and  $m(1, j) = \infty$  for  $j = \delta_1$  to  $\Delta$ 
2: for  $i = 1$  to  $k$  do
3:   for  $j = 0$  to  $\delta_i$  do
4:      $m(i, j) = \min\{m(i - 1, j), c_i\}$ 
5:   for  $j = \delta_i$  to  $\Delta$  do
6:      $m(i, j) = \min\{m(i - 1, j \ominus \delta_i) + c_i, m(i - 1, j)\}$ 
7:    $\Delta_l = \Delta$ 
8:   for  $i = k$  to  $1$  do
9:     if  $m(i, \Delta_l) == m(i - 1, \Delta_l)$  then
10:       $x_i = 0$ 
11:    else
12:       $x_i = 1$ 
13:       $\Delta_l = \Delta_l - \delta_i$ 
14: return  $T = \{x_1, x_2, \dots, x_k\}$ 

```

When the atomic event i is considered, it needs to decide whether to transmit this event or not. According to Eq. 5, the cost $m(i, j)$ equals to the smaller value between the cost achieving by transmitting the event i (e.g. c_i for $j \leq \delta_i$ and $m(i - 1, j \ominus \delta_i) + c_i$ for $j > \delta_i$) and the cost achieving by not transmitting the event i (e.g. $m(i - 1, j)$). The minimum cost of the OTS problem equals to $m(k, \Delta)$.

The dynamic programming algorithm is shown as Algorithm 1.

In Alg. 1, line 1 works as the initialization. Then the recursive formulation is computed(line 2-6). At last the solution is constructed(line 7-13).

Suppose the time complexity of confidence combination operator is α . The time complexity of the Alg. 1 is $O(\alpha\Delta k)$. Since α can be considered as a constant for most linear operator, the time complexity is reduced to $O(\Delta k)$. Because Δ is the part of the input, the Alg. 1 runs in pseudo-polynomial time.

5.2 Greedy-Based Algorithm

The time complexity of Alg. 1 is $O(\alpha\Delta k)$. The complexity of computing confidence combination operator might be great for nonlinear operator(e.g. D-S combination rule). Then Alg. 1 is infeasible when α is large. A greedy-based approximate algorithm is devised for all confidence combination operators.

The greedy-based approximate algorithm is shown as follows.

Alg. 2 first finds all the atomic events with confidence $\delta_i \geq \Delta$ and chooses the one with lowest cost as a candidate C_y (Line 1). Then Alg. 2 greedily chooses the best confidence versus cost ratio $\frac{\delta_i}{c_i}$ with confidence $\delta_i < \Delta$ until the total confidence satisfies the threshold. Firstly, the descending order of confidence versus cost ratio $\frac{\delta_1}{c_1} \geq \frac{\delta_2}{c_2} \geq \dots \geq \frac{\delta_l}{c_l}$ is achieved(Line 2). We define position b as break position if $\sum_{i=1}^{b-1} \delta_i \leq \Delta \leq \sum_{i=1}^b \delta_i$. Then the algorithm obtains another transmitting scheme $T_x = \{1, \dots, 1, 1, 0, \dots, 0\}$ with the first b -th position value of 1 and a total cost C_x (Line 3-10). The algorithm returns the transmitting scheme with lower cost from $\{C_x, C_y\}$ as the final result(Line 11-14).

Algorithm 2. OTS-Greedy $((\delta_1, \delta_2, \dots, \delta_k), (c_1, c_2, \dots, c_k), \Delta)$

```

1:  $Y = \{i | \delta_i \geq \Delta\}$  and  $C_y = \min\{c_i | i \in Y\}$ 
2: sort  $\frac{\delta_i}{c_i}$  with  $\delta_i < \Delta$  and reorder as  $\frac{\delta_1}{c_1} \geq \frac{\delta_2}{c_2} \geq \dots \geq \frac{\delta_l}{c_l}$ 
3:  $\Delta_c = 0$  // current confidence
4:  $C_x = 0$  // total cost
5:  $x_i = 0$ 
6: for  $i = 1$  to  $l$  do
7:   if  $\Delta_c < \Delta$  then
8:      $x_i = 1$ 
9:      $C_x = C_x + c_i$ 
10:     $\Delta_c = \Delta_c + \delta_i$ 
11:   if  $C_x \geq C_y$  then
12:     return  $T_x = \{x_1, x_2, \dots, x_k\}$  and  $C_x$ 
13:   else
14:     return  $T_y$  and  $C_y$ 

```

Theorem 2. Algorithm 2 achieves an approximation ratio of 2 for OTS problem with “+” as confidence combination operator.

Proof. The cost obtained by Alg. 2 is equal to $\min\{C_x, C_y\}$. Let C^* be an optimal cost of the OTS problem. The OTS problem is an instance of integer programming. We can release OTS problem into a fractional programming. Since every solution that is feasible for the OTS instance is also feasible for the respective fractional OTS instance. We have that

$$C_f^* \leq C^*$$

where C_f^* is the respective optimum solution for fractional OTS instance. The respective transmitting scheme of fractional OTS instance is $T_f = \{1, \dots, 1, \alpha, 0, \dots, 0\}$ where $\alpha \in (0, 1]$ at break position. Considering the solution of the integer programming algorithm $T_x = \{1, \dots, 1, 1, 0, \dots, 0\}$

$$C_f^* = C_x - \delta_b + \alpha\delta_b \geq C_x - (1 - \alpha)\delta_b \geq C_x - C_f^*$$

And

$$C_f^* \leq C_y$$

Then we have

$$C_f^* \geq \frac{1}{2} \min\{C_x, C_y\}$$

In total we have

$$\min\{C_x, C_y\} \leq 2C^*$$

The approximate ratio of Alg. 2 is 2.

6 Experiment Evaluation

The effectiveness and efficiency of the proposed algorithms are evaluated through simulations in this section. Several experiments are conducted to compare the performances of the two algorithms. The experiments are carried out on a Windows PC(2.98GHz Intel(R) Core(TM)2 Duo CPU, 2 GB RAM). We use “+” as the confidence combination operator and the confidence of each atomic event is preset.

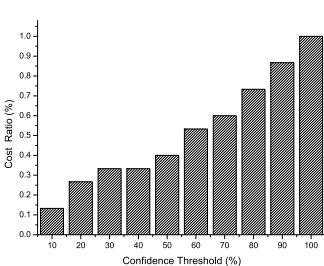


Fig. 1. Cost ratio VS confidence threshold

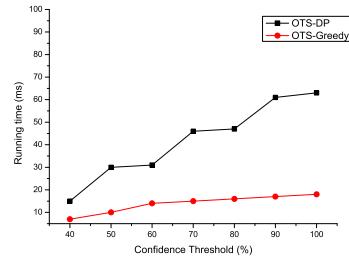


Fig. 2. Running time of OTS-DP and OTS-Greedy

Fig. 1 shows the relationship between cost and confidence threshold. The Y-axis represents the ratio between the cost for current confidence threshold and cost for transmitting all the data. When the confidence threshold increases, more data need to be transmitted to obtain more accurate result. So the cost ratio increases with the confidence threshold.

Fig. 2 depicts the running time between OTS-DP and OTS-Greedy. The running time of both of the algorithm increases with the confidence threshold because more atomic events are considered. OTS-Greedy runs much faster than OTS-DP for simple confidence combination operator. When the confidence combination operator is complex, the running time of OTS-DP increases exponentially.

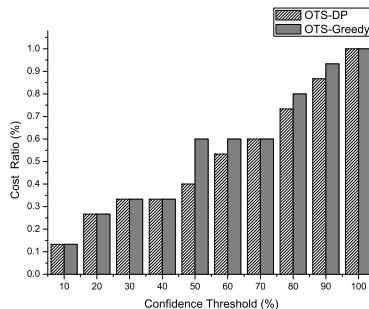


Fig. 3. Cost of OTS-DP and OTS-Greedy

Fig. 3 demonstrates the cost difference between OTS-DP and OTS-Greedy. OTS-Greedy generates the approximate results. The cost of both algorithms increases with the confidence, since more atomic events need to be sent with higher confidence threshold. Both OTS-DP and OTS-Greedy achieve the same confidence with small confidence threshold, because there is an atomic event which can satisfies the confidence threshold. When the confidence threshold grows, the approximate algorithm OTS-Greedy achieves a little bigger cost than that achieved by OTS-DP.

7 Conclusions

Multi-mode data generated by heterogeneous components introduce new challenges for event monitoring in heterogeneous WSNs. The optimal transmitting scheme problem for approximate event detection is investigated and analyzed. The optimal transmitting scheme problem is proved to be NP-Complete. Algorithm OTS-DP is proposed to compute the best transmitting scheme which achieves the minimum cost based on the given confidence constraint for linear confidence combination operator. The approximate algorithm OTS-Greedy is designed for general situation with all kinds of confidence combination operators. The approximate ratio of OTS-Greedy is proved to be 2 for “+” as the confidence combination operator.

References

1. Yarvis, M., Kushalnagar, N., Singh, H., et al.: Exploiting heterogeneity in sensor networks. In: IEEE INFOCOM 2005, vol. 2, pp. 878–890 (2005)
2. Lee, E.A.: Cyber physical systems: Design challenges. In: IEEE International Symposium on Object Oriented Real-Time Distributed Computing, pp. 363–369. IEEE (2008)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., et al.: Wireless sensor networks: a survey. Computer Networks 38(4), 393–422 (2002)
4. Vu, C.T., Beyah, R.A., Li, Y.: Composite event detection in wireless sensor networks. In: IEEE International IPCCC 2007, pp. 264–271. IEEE (2007)
5. Amato, G., Chessa, S., Gennaro, C., et al.: Efficient detection of composite events in Wireless Sensor Networks: Design and evaluation. In: IEEE Symposium on Computers and Communications (ISCC), pp. 821–823. IEEE (2011)
6. Abadi, D.J., Madden, S., Lindner, W.: Reed: Robust, efficient filtering and event detection in sensor networks. In: Proceedings of VLDB, pp. 769–780 (2005)
7. Xue, W., Luo, Q., Chen, L., et al.: Contour map matching for event detection in sensor networks. In: Proceedings of the ACM SIGMOD, pp. 145–156. ACM (2006)
8. Cao, Q., Abdelzaher, T., He, T., et al.: Towards optimal sleep scheduling in sensor networks for rare-event detectionc. In: Proceedings of IPSN, p. 4. IEEE Press (2005)
9. Akyildiz, I.F., Melodia, T., Chowdhury, K.R.: A survey on wireless multimedia sensor networks. Computer Networks 51(4), 921–960 (2007)
10. Akyildiz, I.F., Melodia, T., Chowdury, K.R.: Wireless multimedia sensor networks: A survey. IEEE Wireless Communications 14(6), 32–39 (2007)

11. Chakravarthy, S., Krishnaprasad, V., Anwar, E., et al.: Composite events for active databases: Semantics, contexts and detection. In: VLDB, vol. 94, pp. 606–617 (1994)
12. Cheng, S., Li, J., Cai, Z.: $O(\epsilon)$ -Approximation to physical world by sensor networks. In: INFOCOM 2013, pp. 3084–3092 (2013)
13. Li, J., Cheng, S., Gao, H., et al.: Approximate Physical World Reconstruction Algorithms in Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, doi:10.1109/TPDS.2013.2297121 (to be published)
14. Cai, Z., Chen, Z.Z., Lin, G.: A 3.4713-approximation algorithm for the capacitated multicast tree routing problem. Theoretical Computer Science 410(52), 5415–5424 (2009)
15. Cai, Z., Lin, G., Xue, G.: Improved approximation algorithms for the capacitated multicast routing problem. In: Wang, L. (ed.) COCOON 2005. LNCS, vol. 3595, pp. 136–145. Springer, Heidelberg (2005)
16. Ai, C., Guo, L., Cai, Z., et al.: Processing area queries in wireless sensor networks. In: MSN 2009, pp. 1–8. IEEE (2009)
17. Shafer, G.: A mathematical theory of evidence. Princeton University Press, Princeton (1976)
18. Ho, T.K., Hull, J.J., Srihari, S.N.: Decision combination in multiple classifier systems. IEEE Transactions on Pattern Analysis and Machine Intelligence 16(1), 66–75 (1994)

Structural Health Monitoring Based on RealAdaBoost Algorithm in Wireless Sensor Networks

Zhuorong Li, Junqi Guo*, Wenshuang Liang, Xiaobo Xie, Guangzhi Zhang,
and Shenling Wang

College of Information Science and Technology, Beijing Normal University, China
`{lzs,lws,xiexiaobo,zgz_bnu}@mail.bnu.edu.cn, guojunqi@bnu.edu.cn,`
`wangsl0362@163.com`

Abstract. Since frequent accidents such as bridge collapses have drawn much attention, structural health monitoring (SHM) is considered as a research hotspot in both academic and engineering fields. With the development of wireless sensor networks (WSNs), a large number of sensors have been equipped on architectural or mechanical structures to acquire real-time state data that may imply their health problems, which indicates that data processing is of great significance in WSN-based SHM. In this paper, we propose a SHM scheme by using RealAdaBoost algorithm in a WSN-based environment, in which the RealAdaBoost algorithm is employed here for data classification so as to detect and locate damages of the bridge. Simulation results indicate that the proposed RealAdaBoost algorithm provides better performance than several existing ones employed in SHM scenarios.

Keywords: Structural Health Monitoring (SHM), Wireless Sensor Networks (WSNs), AdaBoost.

1 Introduction

Architectural or mechanical structures around us such as buildings, bridges and aircrafts always suffer from longtime overloading, severe environments and inevitable material aging, which will lead to structural deterioration and damage accumulation. Structural damages can severely affect their working life and may cause vast economic losses and casualties. Consequently, the amount of researches on structural health monitoring (SHM) in recent years has increased rapidly so as to calculate remaining life of engineering infrastructure as well as avoid upcoming danger [1]. The early researches on SHM fields tried to mimic statuses of real structures and received a failed effect due to large complexity of a real-world system [2, 3]. With the development of data processing, this method has been gradually replaced. People tend to collect vibration data of architectural or mechanical structures for their health status evaluation, in which various vibration-based damage detection methods are proposed [4–8].

* Corresponding author.

Wireless sensor networks (WSN), which have made significant strides in the past few years, provide a good choice for structural health monitoring. More and more SHM implementations acquire structural vibration data based on wireless sensors which are equipped on architectural or mechanical structures, where these vibration data can be processed so as to detect structural health problems hidden in them by using intelligent computing [9, 10]. For example, [11] deploys a multi-hop wireless data acquisition system for SHM and conducts a series of experiments on this platform. In [12], Kim Sukun etc. design and implement a WSN system on the south tower of the Golden Gate Bridge for SHM. After sensor data acquisition, transmission, processing and analyzing, structural health problems hidden in raw data can be successfully detected or predicted.

AdaBoost is a popular algorithm in the field of statistical learning and intelligent computing [13, 14]. It has been widely used in areas such as algorithm improvement, feature selection, classification and regression problems. AdaBoost, which has been proved to show outstanding performance among learning algorithms, is a promising candidate for SHM since it can process the collected sensor data with large performance upgrade.

Several works have recently tried to apply the AdaBoost algorithm in structural health monitoring. H. Furuta etc. process digital images of concrete deck based on a neural network algorithm to evaluate the damage condition, in which AdaBoost is applied here to improve performance of neural networks [15]. Dae-won Kim and Michael Philen use signal processing methods combined with AdaBoost algorithm to accomplish classification for the two most frequent damages in metallic structures, namely cracks and corosions [16]. In [17], Yujie Ying etc. apply AdaBoost to select data features of a pressurized pipe for damage recognition. [18] combines fuzzy-neural networks with AdaBoost to recognize the change of structural characteristics. AdaBoost to recognize the change of structural characteristics. However, the existing references seldom use AdaBoost to monitor and locate damages of architectural or mechanical structures by processing wireless sensor data and classifying them into different structural health statuses.

In this paper, we make an attempt to develop a RealAdaBoost algorithm based SHM scheme in an WSN environment. By classifying vibration sensor data into healthy and unhealthy types, the proposed scheme can easily monitor health statuses of architectural structures as well as detect locations of the damage. The purpose of this paper is to show the proposed scheme is more suitable in solving SHM tasks. Also, simulation results demonstrate that RealAdaBoost algorithm provides better performance than other typical algorithms in SHM applications.

The rest of this paper is organized as follows. Section 2 describes the principle of RealAdaBoost algorithm as well as the proposed WSN-based structural health monitoring scheme by using the RealAdaBoost. In Section 3, simulation of the proposed method and performance comparison are given for the purpose of verifying efficiency and accuracy of the proposed SHM scheme. Finally, some conclusions are drawn in Section 4.

2 Methodology

2.1 Architecture of Structural Health Monitoring

In our research, wireless sensors are embedded on architectural or mechanical structures such as bridges. These sensors monitor the state of structures through real-time data acquisition. The sensing data can be sent to database periodically by a certain wireless communication technology such as WiFi, 4G or Zigbee. An SHM module then processes data through intelligent computing and outputs a report about current structural health situation. According to the report, we can take some preventive measures to avoid danger effectively. In general, a WSN-based structural health monitoring for a bridge is showed in Fig. 1.

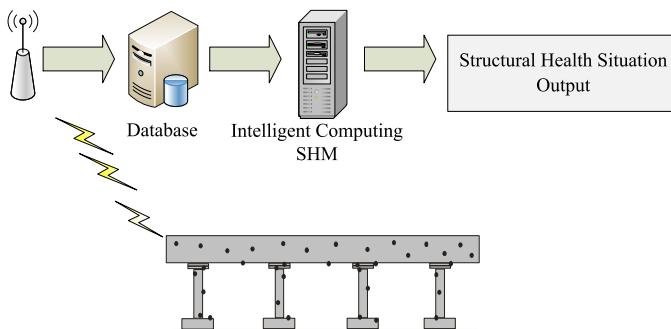


Fig. 1. Architecture of Bridge Structural Health Monitoring

2.2 RealAdaboost

Boosting is a popular statistical learning method that has been widely used in many fields [19]. The main idea of this method is to boost a set of weak learners up to a strong learner. Finding a weak learning algorithm is obviously much easier than that of a strong learning algorithm, so boosting is considered to be an effective method to improve learning algorithms given. Researches on boosting are also growing in number. Among all kinds of existing boosting methods, the most representative one is the AdaBoost algorithm.

AdaBoost, which is short for “Adaptive Boosting”, has been first introduced by Freund Y. and Schapire R.E. in [14]. AdaBoost is an iterative algorithm, in which different weak learners are trained on the same set of weighted training data, and then the prediction results of those weak learners are combined into a weighted sum so as to finally output a strong classifier. The key point of this algorithm is to maintain a weight distribution over the training data. During a training process, the AdaBoost algorithm focuses on examples that are harder to classify by raising their weights. Meanwhile, when the final strong learner is outputted, AdaBoost also raises the weights of those weak learners with higher classification accuracy.

Since original AdaBoost assumes the output of each weak learner is restricted to $[-1, +1]$, Schapire R.E. and Singer Y. then propose a generalization of AdaBoost [20]. This improved AdaBoost algorithm differs from basic AdaBoost in that the weak hypotheses can have range over all of \mathbb{R} , therefore it's called RealAdaBoost.

Algorithm: Real AdaBoost

Input: training set $T = \{(x_i, y_i); i=1, 2, \dots, N\}$ where $x_i \in X \subseteq \mathbb{R}^n$, $y_i \in Y = \{-1, +1\}$

weak learning algorithm **Weak Learner**
specifying number of iterations **Max_Iter**

1. **Initialize** the distribution of training examples weights $D_1(i) = w_{1i} = \frac{1}{N}, i=1, \dots, N$

2. **For** $m = 1, 2, \dots, Max_Iter$ **do**

1) Train a weak learner using distribution D_m and get weak hypothesis

$h_m(x) : X \rightarrow \mathbb{R}$ by the following steps:

a) Partition the set T into disjoint blocks T_1, \dots, T_K

b) **For** $k = 1, 2, \dots, K$ **do**

i. Compute $W_+^k(i) = P(x_i \in X_k, y_i = +1) = \sum_{i: (x_i \in X_k) \wedge (y_i = +1)} w_{mi}$

and $W_-^k(i) = P(x_i \in X_k, y_i = -1) = \sum_{i: (x_i \in X_k) \wedge (y_i = -1)} w_{mi}$;

ii. Set the weak hypothesis on T_k : $h_k(x) = \frac{1}{2} \ln(\frac{W_+^k + \varepsilon}{W_-^k + \varepsilon})$ where ε is a small positive number

iii. Compute the normalization factor: $Z = 2 \sum_k \sqrt{W_+^k W_-^k}$

End for

2) Choose $h_m = \arg \min_{h_k} Z, Z_m = \min_{h_k} Z, k = 1, \dots, K$

3) Update the distribution of weights D_{m+1} : $w_{m+1,i} = \frac{w_{mi}}{Z_m} \exp(-y_i h_m(x_i))$

End for

Output: the final strong learner $H(x) = sign(\sum_{m=1}^M h_m(x))$.

Fig. 2. The RealAdaBoost Algorithm

Fig. 2 describes the pseudocode of a RealAdaBoost algorithm. The input of this algorithm is a training set of N examples where $x_i \in X$ is an instance with n features and $y_i \in Y$ is the class label associated with x_i . Suppose the initial weights of training examples distribute uniformly, each example plays the same

role in this situation, so the first step of this algorithm is equivalent to training a weak learner by using the original training data [13]. Then RealAdaBoost keeps on calling the weak learning algorithm repeatedly in a series of rounds $m = 1, \dots, M$ in which M weak learners with the minimized training error have been trained.

At the m^{th} iteration, the algorithm receives the weak hypothesis h_m associated with a partition of training set T by the following steps. For each subset T_k , let $W_l^k, l = \pm 1$ be the weighted fraction of examples which fall in set T_k with label l . So the normalization factor

$$Z = \sum_i D_m(i) \exp(-y_i h(x_i)) = \sum_k \left(W_+^k e^{-h_k(x)} + W_-^k e^{h_k(x)} \right). \quad (1)$$

It has been proved in literatures that we can minimize training error by minimizing Z on each round of boosting [20]. By analyzing the Eq. 1, it's clear that Z can be minimized to $Z = 2 \sum_k \sqrt{W_+^k W_-^k}$ only when the weak hypothesis $h_k(x)$ on subset T_k satisfies

$$h_k(x) = \frac{1}{2} \ln \left(\frac{W_+^k + \varepsilon}{W_-^k + \varepsilon} \right) \quad (2)$$

where ε is a small positive number as the smoothing factor to bounded both W_+^k and W_-^k between 0 and 1. After receiving K weak hypotheses on the disjoint blocks T_1, \dots, T_K , we choose the weak hypothesis which can minimize Z as h_m at the m^{th} iteration. Then the distribution of weights is updated. The update rule increases the weights of examples on which the hypothesis h_m makes a wrong prediction, namely the “harder” examples [21]. After M iterations, the final hypothesis H is a linear weighted combination of the M weak hypotheses.

The RealAdaBoost as the generalization of AdaBoost algorithm has lots of advantages. It's easy to understand and simple to implement, the classification accuracy is pretty high, it does not need to set parameters, and it's less prone to overfitting than other algorithms. Thus we use RealAdaBoost algorithm to process sensor data for structural health monitoring in this paper.

3 Experiment

In this experiment, we deploy four hundred sensors uniformly and randomly on a bridge, providing a real-time vibration data acquisition. Assume that statuses of architectural or mechanical structure can be divided into two classes: the healthy status and the unhealthy one. Since a small crack may lead to potentially severe structure damage, vibration data collected from such locations should be labeled as “unhealthy”. It can be considered as the healthy status only if there is absolutely nothing wrong with the structure. Therefore, raw vibration data collected by sensors contain both the health and unhealthy statuses. The purpose of our experiments is to distinguish the unhealthy data from the healthy ones so as to monitor locations of potential structure damage. To evaluate feasibility and efficiency of the proposed scheme, we compare RealAdaBoost with several typical learning algorithms in SHM applications.

3.1 Experimental Setting

Data Set. In our experiment, we select 30 different sizes of training sets to train classifiers and testify the performance of these classifiers through independent test sets. The sizes of training sets vary from 100 to 3000. Each training example has 100 features as well as a corresponding label that indicates its health status. So our training set can be represented as $\{(x^{(i)}, y^{(i)}) ; i = 1, \dots, m\}$ where $x^{(i)} = (x_1^i, x_2^i, \dots, x_n^i)$, $y^{(i)} \in \{-1, +1\}$. Label $y = +1$ means the unhealthy data, and $y = -1$ means the healthy data. We run our experiment under 8 dB signal-to-noise ratio (SNR).

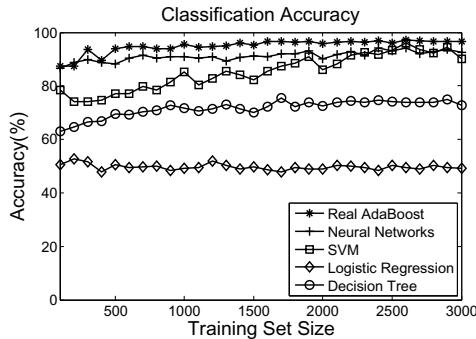
Algorithms for Comparison. We compare the following learning algorithms in our experiment: RealAdaBoost, Logistic Regression (LR), Decision Tree (DT), Neural Networks (NN) and Support Vector Machine (SVM). These methods are all typical learning algorithms that perform well on various classification problems. Note that we use a decision tree algorithm for choosing the weak learners in RealAdaBoost, this kind of AdaBoost is so called “boosting tree”, which has proved to show outstanding performance among statistical learning methods. By simply changing the maximum depth of a decision tree, we can control both the training time and prediction time of the weak learner in AdaBoost.

Evaluation Measures. We use four evaluation measures: Accuracy, Precision, Recall and F1-score. Classification accuracy is the most popular metric to evaluate the performance of classification algorithms. However, the healthy data is far more than the unhealthy data in structural health monitoring scenario, which is called “skewed classes distribution”. In this case, we cannot evaluate an algorithm only by classification accuracy measure. So we use precision and recall measure. Moreover, we also introduce F1-score to evaluate algorithms in order to trade off precision and recall performance.

3.2 Experimental Results

Accuracy. Classification accuracy reflects the percentage of correctly predicted examples in total testing examples. We conduct the experiment on each training set and compare classification accuracy among 5 different algorithms. Fig. 3 illustrates comparison of classification accuracy with the increase of training set size.

As is showed in Fig. 3, the prediction accuracy of each algorithm on test set gradually rises and becomes stable. With the growth of training set size, the RealAdaBoost algorithm finally reaches the accuracy about 96%, while neural networks and SVM achieve about 93% and 92% respectively. Besides, the accuracy of Logistic Regression is around 50% and Decision Tree is 70%. It's obvious that RealAdaBoost is more suitable for an SHM scenarios since it achieves better performance on classification accuracy compared with others.

**Fig. 3.** Comparison of Classification Accuracy

Precision Rate/Recall Rate/F1-score. Precision rate is defined as the percentage of indeed unhealthy examples in the predicted unhealthy data, while recall rate reflects the percentage of predicted unhealthy data in the total unhealthy data. F1-score takes both precision rate and recall rate into accounts, so it can trade off precision and recall rate. F1-score is the harmonic mean of precision and recall:

$$F1-score = 2 \frac{PR}{P+R} \quad (3)$$

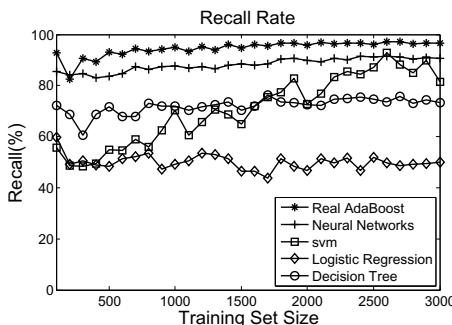
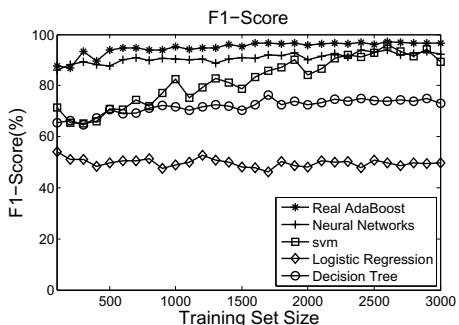
Table 1. Performance in Precision/Recall/F1-score (*No. training examples* = 1000)

	<i>Precision</i>	<i>Recall</i>	<i>F1-score</i>
RealAdaBoost	95.6345	<u>95.0555</u>	<u>95.3441</u>
Neural Networks	93.5345	87.5883	90.0850
SVM	99.7135	70.2321	82.4156
Logistic Regression	48.8000	49.2432	49.0206
Decision Tree	71.2713	71.8466	71.5578

As is showed in Table 1 and Table 2, we calculate these three measures on different sizes of training sets. Although the precision rate of RealAdaBoost is preceded only by SVM slightly, considering that the cost of a false negative is more expensive than that of a false positive in SHM scenarios, the recall rate is accordingly more important than precision rate. All results demonstrate that the recall rate of RealAdaBoost is the hightest one among all of the algorithms. Considering the comprehensive evaluation metric, F1-score of RealAdaBoost algorithm is significantly higher than the others with gradual increase of the training example number. These performance advantages are also confirmed by Fig. 4 and Fig. 5, which illustrate comparison of Recall rate and F1-score with the increase of training set size.

Table 2. Performance in Precision/Recall/F1-score (*No. training examples* = 3000)

	<i>Precision</i>	<i>Recall</i>	<i>F1-score</i>
RealAdaBoost	96.4179	96.6423	96.5300
Neural Networks	94.0024	90.6582	92.2999
SVM	98.7086	81.3165	89.1724
Logistic Regression	49.3421	49.8670	49.6032
Decision Tree	72.6823	73.2380	72.9591

**Fig. 4.** Comparison of Recall**Fig. 5.** Comparison of F1-score

All the experiment results above indicate that RealAdaBoost outperforms LR, DT, NN and SVM in an SHM application.

4 Conclusion

In this paper, we apply a RealAdaBoost algorithm in an environment of wireless sensor networks for structural health monitoring. Hundreds of sensors are equipped on a bridge for real-time sensing and structural data acquisition. RealAdaBoost is used here to classify sensor data so as to detect damages. The feasibility and effectiveness of the proposed method have been verified by theoretical analysis and computer simulation in this paper. Simulation results show that the proposed method performs better in structural health monitoring, compared with some other typical learning algorithms.

Acknowledgement. This research is sponsored by National Natural Science Foundation of China (61003225, 61171014, 61272475 and 61371185), the Fundamental Research Funds for the Central Universities (2012LYB46, 2013NT57) and by SRF for ROCS, SEM.

References

1. Farrar, C.R., Worden, K.: An Introduction to Structural Health Monitoring, New Trends in Vibration Based Structural Health Monitoring, pp. 1–17. Springer, Vienna (2010)
2. Ofsthum, S.C., Wilmering, T.J.: Model-driven development of integrated health management architectures. In: 2004 IEEE Proceedings of the Aerospace Conference (2004)
3. Biswas, G., Mahadevan, S.: A Hierarchical Model-based approach to System Health Management. In: 2007 IEEE Aerospace Conference (2007)
4. Worden, K., Manson, G., Allman, D.: Experimental validation of a structural health monitoring methodology: part I. Novelty detection on a laboratory structure. *Journal of Sound and Vibration* 259(2), 323–343 (2003)
5. Manson, G., Worden, K., Allman, D.: Experimental validation of a structural health monitoring methodology: part II. Novelty detection on a gnat aircraft. *Journal of Sound and Vibration* 259(2), 345–363 (2003)
6. Manson, G., Worden, K., Allman, D.: Experimental validation of a structural health monitoring methodology: part III. Damage location on an aircraft wing. *Journal of Sound and Vibration* 259(2), 365–385 (2003)
7. Xie, X., Guo, J., Zhang, H., Bie, R., Jiang, T., Sun, Y.: Neural-Network based Structural Health Monitoring with Wireless Sensor Networks. In: 9th International Conference on Natural Computation and 10th International Conference on Fuzzy Systems and Knowledge Discovery (ICNC-FSKD 2013), Shenyang, China (2013)
8. Zhang, H., Guo, J., Xie, X., Bie, R., Sun, Y.: Environmental effect removal based structural health monitoring in the internet of things. In: 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS 2013), Taichung, Taiwan (2013)
9. Lynch, J.P., Loh, K.J.: A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring. *The Shock and Vibration Digest* 38(2), 91–128 (2006)
10. Guo, J., Zhang, H., Sun, Y., Bie, R.: Square-Root Unscented Kalman Filtering Based Localization and Tracking in the Internet of Things. Personal and Ubiquitous Computing (PUC), Springer, Digital Object Identifier, DOI (2013), [dx.doi.org/10.1007/s00779-013-0713-8](https://doi.org/10.1007/s00779-013-0713-8)
11. Paek, J., Chintalapudi, K., Govindan, R., Caffrey, J., Masri, S.: A Wireless Sensor Network for Structural Health Monitoring: Performance and Experience. Center for Embedded Network Sensing (2005)
12. Sukun, K., Shamim, P., David, C., et al.: Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks. In: Proceedings of the Sixth International Symposium on Information Processing in Sensor Networks, pp. 254–263 (2007)
13. Freund, Y., Schapire, R.E.: Experiments with a New Boosting Algorithm. In: Proceedings of the Thirteenth International Conference (1996)
14. Freund, Y., Schapire, R.E.: A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting. *Journal of Computer and System Sciences* 55(1), 119–139 (1997)
15. Furuta, H., Hattori, H., Dan, M.: Frangopol: Damage assessment of reinforce concrete bridge decks using Adaboost. In: 3rd International ASRANet Colloquium (2006)
16. Kim, D., Philen, M.: Damage classification using Adaboost machine learning for structural health monitoring. *Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems* (2011)

17. Ying, Y., Harley, J., Shi, J.: Damage Recognition for Structural Health Monitoring, <http://www.cs.cmu.edu/afs/cs/user/bhiksha/WWW/courses/mlsp.fall2010/projects/yjjj.MLSP.pdf>
18. Hattori, H., Gul, M., Catbasand, F.N., Furuta, H.: Structural health monitoring and damage detection using AdaBoost technique. In: Proceedings of the Sixth International IABMAS Conference, pp. 384–391 (2012)
19. Freund, Y., Schapire, R.E.: A Short Introduction to Boosting. Journal of Japanese Society for Artificial Intelligence 14(5), 771–780 (1999)
20. Schapire, R.E., Singer, Y.: Improved Boosting Algorithms Using Confidence-rated Predictions. Machine Learning 37(3), 297–336 (1999)
21. Daum III, H.: Ensemble Methods: A Course in Machine Learning, http://ciml.info/dl/v0_8/ciml-v0_8-ch11.pdf

Probabilistic Threshold Based Monitoring Using Sensor Networks

Ran Bi¹, Hong Gao¹, and Yingshu Li^{1,2}

¹ School of Computer Science and Technology, Harbin Institute of Technology,
Harbin, 150001, China

² Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA
biranhit@gmail.com, honggao@hit.edu.cn, yli@cs.gsu.edu

Abstract. Detecting abnormal events in a monitored area is one of the fundamental applications in Wireless Sensor Networks (WSNs). Accidents and property damage can be avoided if accurate alarms are informed on time. In traditional monitoring strategies, a predefined threshold is given and an alarm is triggered when the sensor reading exceeds this threshold. This Single Threshold based Monitoring (STM) suffers from the inferior quality of sensed data, resulting in many false alarms. This paper proposes a Probabilistic Threshold based Monitoring (PTM) method for WSNs, where an alarm is triggered if the probability of the monitored value being larger than a predefined threshold α is larger than τ . The tight upper bounds of the probability that monitored value is larger than the specified threshold are provided. According to the bounds, probabilistic threshold based algorithms for aggregation monitoring are proposed. Extensive performance evaluation demonstrate the effectiveness of the proposed algorithms. By an extensive experimental evaluation using real dataset, the proposed algorithms outperform the STM method in term of false alarm rate.

1 Introduction

Wireless Sensor Networks (WSNs) attract more and more attention and have been widely applied in many areas, such as transportation, health-care, agriculture, etc. In order to accurately monitor the physical world, many methods on event monitoring have been proposed in WSNs, which can be classified into two categories, instantaneous monitoring [1] and continuous monitoring [2].

The Single Threshold based Monitoring (STM) method is the most popular one to detect abnormal events, in which alarms are triggered if the sensor reading exceeds the specified threshold. However, due to the inferior quality of sensed data, some important alarms may be missed in STM. For example, in greenhouses environment monitoring for blueberry seeding [3], the temperature should be kept between 20°C and 35°C. An alarm is triggered by sensor node equipped on plant, if the sensor reading is larger than 35°C or smaller than 20°C. Because of the error and noise, the sensed data may be 20.5°C at time t , but the actual temperature of plant is 19.5°C. Then no alarm is generated at this moment. Similarly, a false positive alarm is triggered, if the sensed temperature is larger than that of the actual occasion. Therefore, STM is not reliable.

Inferior quality of sensed data caused by inherent low sensitivity to the physical world of sensors [4, 5] incurs higher false alarm rate for STM based method. Compared with STM, a probability threshold involved in Probabilistic Threshold based Monitoring (PTM) method, where an alarm is triggered when the probability that monitored value violates the specified threshold is above a predefined value. For example, suppose the probability threshold is 0.85 for a greenhouse environment monitoring system. The sensed data is regarded as probabilistic data, namely, a random variable $s(t)$, and the sensed data are used to update the probability distribution. According to the probability distribution, we respectively compute $\Pr[s(t) > 35]$ and $\Pr[s(t) < 20]$. An alarm is triggered if either of the them is larger than 0.85. Note that the triggered alarm with high probability implicates that the specified threshold is actually crossed or the node causing measurement error may malfunction.

PTM based monitoring strategies can provide probability guarantees on the triggered alarms, however, estimating the probability distribution requires complicated calculations [6], which is not practical to be carried out on sensors. Due to the aforementioned reasons, we derive an upper bound for the probability and PTM based lightweight algorithms are designed. For example, in greenhouse monitoring, we respectively compute the upper bounds for $\Pr[s(t) \geq 35]$ and $\Pr[s(t) \geq 20]$, denoted by τ_1 and τ_2 . If $\tau_1 < 0.85$, we know that $\Pr[s(t) > 35]$ is smaller than 0.85; if $\tau_2 < 0.15$, we know that $\Pr[s(t) < 20] > 0.85$, then an alarm need be triggered.

To overcome the deficiencies of STM based methods, this paper focuses on designing probabilistic threshold based monitoring strategies in WSNs. The tight upper bound of the probability that monitored value is larger than the specified threshold is derived. According to the upper bound, probabilistic threshold based algorithms for aggregation monitoring is proposed. To the best of our knowledge, this is the first work investigating the problem. The main contributions of the paper are as follows.

- The probabilistic threshold based aggregation monitoring problem is extensively studied. Mathematical methods for computing the tight upper bound of the probability that the aggregation result of monitored area is larger than the specified threshold are provided.
- A probabilistic threshold based algorithm for aggregation monitoring is given and the performance analysis of the algorithm demonstrates low computation cost.
- Simulation experiments are conducted to show the correctness and effectiveness of our algorithms.

2 Related Works

Tang *et al.* [4] designed efficient monitoring methods for distributed probabilistic data threshold monitoring (DPTM). However, probabilistic threshold based monitoring is more challenging in WSNs. The challenges can be summarized as follows.

The probability distribution function(PDF) of sensed data is unknown in WSNs [7]. Since the monitored physical world is unpredictable and dynamics, the underlying distribution of streaming data may not be known in advance. Moreover, it is difficult to directly compute the probability of the aggregate value for noisy sensed data [8]. Amol

et al. [9] extensively studied model based data acquisition in sensor networks. It is assumed that most sensed data are approximated by a Gaussian distribution, however, this assumption is not always meaningful [10]. Although the proposed technique is applicable, it increases the latency of emergency discovery. The centralized approach of PDF updating consumes high communication cost. Therefore, the proposed methods for DPTM are hard to extend in large sensor networks. Moreover, the estimation of probability distribution needs high computation, which cannot be directly applied on sensor node.

3 Probabilistic Threshold Based Aggregation Monitoring

The inferior quality of sensor readings result in high false alarm rate. In this section, we first introduce a formal description of probabilistic threshold based aggregation monitoring. According to the derived upper bounds of probability, a probabilistic threshold based algorithm for aggregation monitoring is proposed.

3.1 Problem Definition

In the rest of this paper, let M denote the number of sensor nodes in the WSN and each sensor node has a unique ID in range of $[1, M]$. $s_i(t)$ denotes the sensed data of node i at time t . Since WSNs are applied for observing the physical world, sup and inf are used to respectively denote the upper and lower bounds of all sensed data. Suppose that $0 \leq s_i(t) \leq sup$, in which $i \in \{1, 2, \dots, M\}$ and $t \in (0, \infty)$. If the sensed data is negative, it can be processed as follows. Let $\hat{s}_i(t) = s_i(t) - inf$, then $0 \leq \hat{s}_i(t) \leq sup - inf$. The initial monitored threshold β is transformed to $\hat{\beta} = \beta - inf$. Due to the uncertainty of sensed data, $s_i(t)$ can be regarded as a random variable. Let μ_i^t denotes the expectation of $s_i(t)$. When the context is clear, the symbols μ_i^t and $\mu_i(t)$ are used interchangeably.

Definition 1. *Probabilistic Threshold based Aggregation Monitoring [4]: Let n be the number of sensor nodes deployed on the monitored area, in which one cluster-head and $n - 1$ member nodes. $S(t) = \sum_{i=1}^n s_i(t)$ denotes the sum of the area at time t . For a given monitored threshold α , a probability threshold τ and time t , an alarm is triggered by cluster-head, if $\Pr[S(t) > \alpha] > \tau$.*

According to the probability distribution of sensed data, computing $\Pr[S(t) > \alpha]$ is alternative. However, achieving the accurate estimation for the probability distribution of physical world is quite tough [6], and existing estimation methods with complicated calculation cannot be directly adopted on the sensor node. Histogram reveals that the data distribution over a long period, thus it is inefficient for time instance threshold monitoring. Setting up to the challenges, a novelty approach for probabilistic threshold based aggregation monitoring is proposed in this section. The main steps of the approach are as follows.

First, according to the sensed data of time t , $s_i(t)$, expectation estimation algorithm runs at sensor node i . Then the node sends the sensed data and its expectation to cluster-head. Since the expectation estimation itself is a challenging research topic, which is

beyond the scope of this paper, then we adopt a weighting technique for expectation estimation [6].

Second, when the cluster-head receives the sensed data and their expectations from all the member nodes, it computes the sum of expectations, denoted by $\mu(t)$. According to $\mu(t)$ and monitored threshold α , the cluster-head computes an upper bound for $\Pr[S(t) \geq \alpha]$, denoted by τ_1 .

Finally, there is no alarm to be triggered if τ_1 is smaller than τ , where τ is the probability threshold. If $\tau_1 > \tau$, we cannot assure whether $\Pr[S(t) \geq \alpha]$ is larger than τ . To avoid triggering an alarm caused by burst noise, we compute the upper bound for $\Pr[S(t+1) \geq \alpha]$. If the upper bound of $t+1$ time instance is smaller than τ , then there is no alarm to be triggered. Otherwise, when the sensed data and its expectation are both larger than α , an alarm needs to be triggered.

Based on the above analysis, the key point of the approach is to calculate a tight upper bound for $\Pr[S(t) \geq \alpha]$. In the following section, the tight upper bounds for $\Pr[S(t) \geq \alpha]$ and $\Pr[S(t) \leq \alpha]$ are proved, respectively. According to the derived upper bounds, probabilistic threshold based algorithm for aggregation monitoring is proposed.

3.2 Estimation for the Upper bound

Lemma 1. *If $x \in [0, 1]$ is a random variable with expectation $E[x] = \mu$, then for any $h \neq 0$, $E[e^{xh}] \leq e^h \mu + 1 - \mu$.*

Proof. Let $f(x) = e^{hx}$, it is known that $f''(x) = h^2 e^{hx}$. Then for any $h \neq 0$, $f''(x) > 0$, therefore $f(x) = e^{hx}$ is a convex function with respect to x . According to the definition of convex function, for any $x_1, x_2 \in \mathbb{R}$, and $\alpha \in [0, 1]$, $f(\alpha x_1 + (1 - \alpha)x_2) \leq \alpha f(x_1) + (1 - \alpha)f(x_2)$ is hold. Since x is a random variable and bounded in $[0, 1]$, then it can be known that $e^{hx} = f(x) = f((1-x) \times 0 + x \times 1) \leq (1-x)e^0 + xe^h$. Therefore the following formula can be obtained.

$$E[e^{hx}] \leq E[(1-x) + xe^h] = e^h \mu + 1 - \mu. \quad (1)$$

□

Theorem 1. *Let $\mu_i(t)$ be the expectation of $s_i(t)$ and $\mu(t) = \sum_{i=1}^n \mu_i(t)$. If $\mu(t) < \alpha$, the following inequality is hold,*

$$\Pr[S(t) \geq \alpha] \leq \exp\{-n\ell(\hat{\mu}(t) + \lambda, \hat{\mu}(t))\}, \quad (2)$$

where $\hat{\mu}(t) = \frac{\mu(t)}{nsup}$, $\lambda = \frac{\alpha - \mu(t)}{nsup}$, and $\ell(x_1, x_2) = x_1 \ln\left(\frac{x_1}{x_2}\right) + (1 - x_1) \ln\left(\frac{1-x_1}{1-x_2}\right)$.

Proof. sup denotes the upper bound of the sensed data. For $i \in \{1, 2, \dots, n\}$, let $x_i(t) = \frac{s_i(t)}{sup}$. Sensed data from different sites are independent [4, 11, 12, 13]. Then $x_1(t), \dots, x_n(t)$ are independent random variables and bounded in $[0, 1]$. Let $X(t) = \sum_{i=1}^n x_i(t)$, $\gamma = \frac{\alpha}{sup}$,

then $E[X(t)] = E\left[\sum_{i=1}^n \frac{s_i(t)}{sup}\right] = \sum_{i=1}^n \frac{\mu_i(t)}{sup} = \frac{\mu(t)}{sup}$. Due to $\mu(t) < \alpha$, we have $E[X(t)] < \gamma$.

The following equality is easily obtained.

$$\Pr[S(t) \geq \alpha] = \Pr\left[\frac{S(t)}{\sup} \geq \frac{\alpha}{\sup}\right] = \Pr[X(t) \geq \gamma] \quad (3)$$

According to Markov's Inequality [14], for any $h > 0$, the following formula can be known.

$$\Pr[X(t) \geq \gamma] = \Pr[e^{X(t)h} \geq e^{\gamma h}] \leq e^{-\gamma h} E[e^{X(t)h}] \quad (4)$$

Since $x_1(t), \dots, x_n(t)$ are independent random variables, then we know that $E[e^{X(t)h}] = E\left[e^{x_1(t)h + \dots + x_n(t)h}\right] = \prod_{i=1}^n E[e^{x_i(t)h}]$. According to Lemma 1, $E[e^{hx_i(t)}] \leq e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}$ is hold, then the following formula can be known.

$$E[e^{X(t)h}] = \prod_{i=1}^n E[e^{x_i(t)h}] \leq \prod_{i=1}^n \left(e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}\right)$$

Based on arithmetic-geometric mean inequality [15], we have

$$\sqrt[n]{\prod_{i=1}^n \left(e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}\right)} \leq \frac{\sum_{i=1}^n \left(e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}\right)}{n}. \text{ Let } \hat{\mu}(t) = \frac{\mu(t)}{nsup}, \text{ obviously}$$

$$\frac{\sum_{i=1}^n \left(e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}\right)}{n} = \frac{1}{n} \left(e^{h\frac{\mu(t)}{\sup}} + n - \frac{\mu(t)}{\sup}\right) = e^h \hat{\mu}(t) + 1 - \hat{\mu}(t), \text{ then we have}$$

$$\sqrt[n]{\prod_{i=1}^n \left(e^{h\frac{\mu_i(t)}{\sup}} + 1 - \frac{\mu_i(t)}{\sup}\right)} \leq e^h \hat{\mu}(t) + 1 - \hat{\mu}(t). \text{ The following formula can be derived.}$$

$$\Pr[S(t) \geq \alpha] \leq e^{-\gamma h} E[e^{X(t)h}] \leq e^{-\gamma h} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$$

To achieve a tight bound, h^* should be an optimal value, such that $e^{-\gamma h^*} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$ achieves the minimum value. Let $y(h) = e^{-\gamma h} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$, and it can be derived that $y'(h) = y(h) \left(\frac{n\hat{\mu}(t)e^h}{\hat{\mu}(t)e^h + 1 - \hat{\mu}(t)} - \gamma\right)$.

Then we can derive that when $h^* = \ln\left(\frac{\gamma(1-\hat{\mu}(t))}{(n-\gamma)\hat{\mu}(t)}\right)$, $y'(h^*) = 0$. It is easily known that when $h > h^*$, $y'(h)$ is positive; when $h < h^*$, $y'(h)$ is negative. Therefore, when $h = h^*$, $y(h)$ achieves the minimum value. Due to $\gamma > n\hat{\mu}(t)$, we know that $\frac{\gamma(1-\hat{\mu}(t))}{(n-\gamma)\hat{\mu}(t)} > 1$, thus h^* being positive satisfies the prerequisite of Markov's Inequality. Therefore, the following formula can be derived.

$$\begin{aligned} \Pr[S(t) \geq \alpha] &\leq e^{-\gamma h^*} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n \\ &= \exp\left\{-n\left(\frac{\gamma}{n} \ln\left(\frac{\gamma n^{-1}}{\hat{\mu}(t)}\right) + \left(1 - \frac{\gamma}{n}\right) \ln\left(\frac{1-\gamma n^{-1}}{1-\hat{\mu}(t)}\right)\right)\right\} \\ &= \exp\left\{-n\ell(\gamma n^{-1}, \hat{\mu}(t))\right\} \end{aligned} \quad (5)$$

Then it is known that $\Pr[S(t) \geq \alpha] \leq \exp\{-n\ell(\gamma n^{-1}, \hat{\mu}(t))\}$. Due to $\alpha > \mu(t)$, there exist $\lambda > 0$ such that $\frac{\gamma}{n} = \frac{\alpha}{nsup} = \frac{\mu(t)+nsup\lambda}{nsup} = \hat{\mu}(t) + \lambda$. In conclusion, we can derive that if $\mu(t) < \alpha$, then $\Pr[S(t) \geq \alpha] \leq \exp\{-n\ell(\hat{\mu}(t) + \lambda, \hat{\mu}(t))\}$, where $\hat{\mu}(t) = \frac{\mu(t)}{nsup}$ and $\lambda = \frac{\alpha-\mu(t)}{nsup}$. \square

Corollary 1. For a given monitored threshold α and a probability threshold τ , suppose that $\mu(t)$ is the expectation of the sum of the monitored area. If $\mu(t) < \alpha$ and $\frac{\alpha}{nsup} \ln\left(\frac{\alpha}{\mu(t)}\right) + \left(1 - \frac{\alpha}{nsup}\right) \ln\left(\frac{nsup-\alpha}{nsup-\mu(t)}\right) \geq \frac{\ln\tau^{-1}}{n}$ are hold, then there is no alarm for the monitored area.

Theorem 2. Let $\mu_i(t)$ be the expectation of $s_i(t)$ and $\mu(t) = \sum_{i=1}^n \mu_i(t)$. If $\mu(t) > \alpha$, then the following formula is hold.

$$\Pr[S(t) \leq \alpha] \leq \exp\{-n\ell(\hat{\mu}(t) - \lambda, \hat{\mu}(t))\} \quad (6)$$

where $\hat{\mu}(t) = \frac{\mu(t)}{nsup}$, $\lambda = \frac{\mu(t)-\alpha}{nsup}$, and $\ell(x_1, x_2) = x_1 \ln\left(\frac{x_1}{x_2}\right) + (1-x_1) \ln\left(\frac{1-x_1}{1-x_2}\right)$.

Proof. The proofs of the theorem is similar as Theorem 1, thus some details will be omitted. Let sup be the upper bound of the sensed data and $x_i(t) = \frac{s_i(t)}{sup}$, for $i = 1, \dots, n$. Then $x_1(t), x_2(t), \dots, x_n(t)$ are independent random variables and bounded in $[0, 1]$. Let $X(t) = \sum_{i=1}^n x_i(t)$ and $\gamma = \frac{\alpha}{sup}$, then $E[X(t)] = E\left[\sum_{i=1}^n \frac{s_i(t)}{sup}\right] = \frac{\mu(t)}{sup}$. Due to $\mu(t) > \alpha$, we have $E[X(t)] > \gamma$. It is easily known that $\Pr[S(t) \leq \alpha] = \Pr\left[\frac{S(t)}{sup} \leq \frac{\alpha}{sup}\right] = \Pr[X(t) \leq \gamma]$. According to Markov's Inequality [14], for any $h < 0$, $\Pr[X(t) \leq \gamma] = \Pr[e^{X(t)h} \geq e^{\gamma h}] \leq e^{-\gamma h} E[e^{X(t)h}]$. Based on the independency of $x_1(t), \dots, x_n(t)$, we have $E[e^{X(t)h}] = E\left[e^{x_1(t)h+\dots+x_n(t)h}\right] = \prod_{i=1}^n E[e^{x_i(t)h}]$. According to Lemma 1, we know that $E[e^{hx_i(t)}] \leq e^{h\frac{\mu_i(t)}{sup}} + 1 - \frac{\mu_i(t)}{sup}$. Therefore, it can be derived that $E[e^{X(t)h}] = E\left[e^{x_1(t)h+\dots+x_n(t)h}\right] \leq \prod_{i=1}^n \left(e^{h\frac{\mu_i(t)}{sup}} + 1 - \frac{\mu_i(t)}{sup}\right)$. Based on arithmetic-geometric mean inequality[15], we have $\sqrt[n]{\prod_{i=1}^n \left(e^{h\frac{\mu_i(t)}{sup}} + 1 - \frac{\mu_i(t)}{sup}\right)} \leq e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)$. Based on the above analysis, the following formula can be derived,

$$\Pr[S(t) \leq \alpha] \leq e^{-\gamma h} E[e^{X(t)h}] \leq e^{-\gamma h} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n \quad (7)$$

where $\hat{\mu}(t) = \frac{\mu(t)}{nsup}$. Similarly, h^* needs to be optimally set, such that $e^{-\gamma h^*} \left(e^{h^*} \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$ achieves the minimum value. Let $y(h) = e^{-\gamma h} \left(e^h \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$, then we know that $y'(h) = y(h) \left(\frac{n\hat{\mu}(t)e^h}{\hat{\mu}(t)e^h + 1 - \hat{\mu}(t)} - \gamma\right)$. Obviously, when $h^* = \ln\left(\frac{\gamma(1-\hat{\mu}(t))}{(n-\gamma)\hat{\mu}(t)}\right)$, $y(h)$ achieves the minimum value. Due to $n\hat{\mu}(t) > \gamma$, h^* being negative satisfies the prerequisite of Markov's Inequality. Then $\Pr[S(t) \leq \alpha] \leq e^{-\gamma h^*} \left(e^{h^*} \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n$ and the following formula can be derived.

$$\Pr[S(t) \leq \alpha] \leq e^{-\gamma h^*} \left(e^{h^*} \hat{\mu}(t) + 1 - \hat{\mu}(t)\right)^n = \exp\{-n\ell(\gamma n^{-1}, \hat{\mu}(t))\}$$

Due to $\alpha < \mu(t)$, there exist $\lambda > 0$, such that $\mu(t) = \alpha + nsup\lambda$. Hence $\frac{\gamma}{n} = \frac{\mu(t)-nsup\lambda}{nsup} = \hat{\mu}(t) - \lambda$, and it is obtained that $\Pr[S(t) \leq \alpha] \leq \exp\{-n\ell(\hat{\mu}(t) - \lambda, \hat{\mu}(t))\}$, in which, $\hat{\mu}(t) = \frac{\mu(t)}{nsup}$, $\lambda = \frac{\mu(t)-\alpha}{nsup}$. \square

Corollary 2. For a given monitored threshold α and a probability threshold τ , suppose that $\mu(t)$ is the expectation of the sum of the monitored area. If $\mu(t) > \alpha$ and $\frac{\alpha}{nsup} \ln\left(\frac{\alpha}{\mu(t)}\right) + \left(1 - \frac{\alpha}{nsup}\right) \ln\left(\frac{nsup-\alpha}{nsup-\mu(t)}\right) \geq \frac{\ln(1-\tau)^{-1}}{n}$ are hold, then an alarm need be generated for the monitored area.

3.3 Probabilistic Threshold Based Algorithm for Aggregation Monitoring

The problem of probabilistic threshold based aggregation monitoring can be defined as follows.

Input:

1. Monitored threshold α and probability threshold τ .
2. The sensed data set $\{s_1(t), \dots, s_n(t)\}$ and the expectation set $\{\mu_1(t), \dots, \mu_n(t)\}$.

Output: Trigger an alarm or not**Table 1.** Notation table

Notation Name	Description
$s_i(t)$	The sensed data by node i at time t
$\mu_i(t)/\mu_i^t$	The expectation of $s_i(t)$
sup	The upper bound of all sensed data
inf	The lower bound of all sensed data
n	The number of sensor nodes in the monitored area
$S(t)$	The sum result of the monitored area, $S(t) = \sum_{i=1}^n s_i(t)$
$\mu(t)$	The expectation of $S(t)$
α	Monitored threshold
τ	Probability threshold

For easy to read, table 1 gives the symbols used in this paper. When the cluster-head receives the sensed data and their expectations from all the member nodes, it computes the expectation of sum, denoted by $\mu(t)$. According to Corollary 1 and Corollary 2, the main idea of probabilistic threshold based algorithm for aggregation monitoring is as follows.

Case 1. $\mu(t) < \alpha$. We compute $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t)}{nsup}\right)$, denoted by τ_t .

a. If $\tau_t \geq \frac{\ln \tau^{-1}}{n}$. According to Corollary 1, we know that $\Pr[S(t) > \alpha] \leq \tau$. Then there is no alarm to be triggered.

b. If $\tau_t < \frac{\ln \tau^{-1}}{n}$. Similar to probabilistic threshold based algorithm for critical point monitoring, the cluster-head sets *Alarm Candidate State*. If $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t+1)}{nsup}\right)$ of $t + 1$ time instance is larger than $\frac{\ln \tau^{-1}}{n}$, then the cluster-head needs not trigger any alarm and sets *Normal State*. If $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t+1)}{nsup}\right)$ of $t + 1$ time instance is less than $\frac{\ln \tau^{-1}}{n}$, two designed strategies are as follows.

I. *Active Strategy*. The cluster-head triggers an alarm and sets *Alarm State*.

II. *Passive Strategy*. If the sum $S(t + 1)$ and its expectation $\mu(t + 1)$ of $t + 1$ time instance are both larger than α , then it triggers an alarm and sets *Alarm State*. Otherwise, no alarm is sent and the state is set *Alarm Candidate*.

Case 2. $\mu(t) > \alpha$. We compute $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t)}{nsup}\right)$, denoted by τ_t .

a. If $\tau_t \geq \frac{\ln(1-\tau)^{-1}}{n}$. According to Corollary 2, we know that $\Pr[S(t) > \alpha] > \tau$. Meanwhile, the cluster-head triggers an alarm and sets *Alarm State*.

b. If $\tau_t < \frac{\ln(1-\tau)^{-1}}{n}$. Since we can't make sure whether $\Pr[S(t) > \alpha]$ is larger than the probability threshold τ . Then the cluster-head sets *Normal Candidate State*. If $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t+1)}{nsup}\right)$ of $t + 1$ time instance is no less than $\ln(1 - \tau)^{-1}$, the cluster-head triggers an alarm and sets *Alarm State*. If $\ell\left(\frac{\alpha}{nsup}, \frac{\mu(t+1)}{nsup}\right)$ of $t + 1$ time instance is smaller than $\ln(1 - \tau)^{-1}$, similarly two strategies are designed as follows.

- I. *Active Strategy.* The cluster-head triggers an alarm and sets *Alarm State*.
- II. *Passive Strategy.* If the sum $S(t+1)$ and its expectation $\mu(t+1)$ of $t+1$ time instance are both larger than α , then it triggers an alarm and sets *Alarm State*. Otherwise, no alarm is sent and the state is set *Normal Candidate*.

Case 3. $\mu(t) = \alpha$. Since the bounds of tail probability fail, for different needs of applications, two strategies are provided.

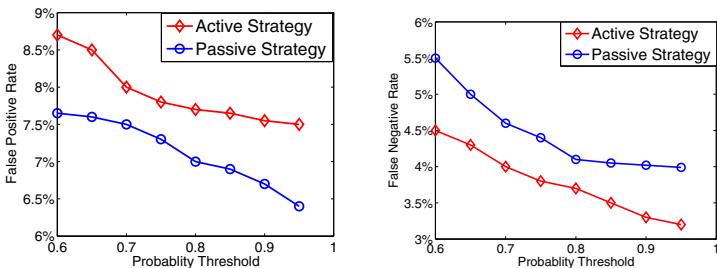
- I. *Active Strategy.* For a given $\varepsilon > 0$, let $\alpha' = \alpha - \varepsilon$, then it checks whether the probability of $S(t) > \alpha'$ is larger than τ and takes the measure proposed in *Case 2*.
- II. *Passive Strategy.* Let $\alpha' = \alpha + \varepsilon$, then it checks whether the probability of $S(t) > \alpha'$ is larger than τ and takes the measure proposed in *Case 1*.

4 Performance Evaluation

To evaluate the performance of the proposed algorithm, experiments have been carried out based on a real data set. The temperature data is used in the experiments. Each simulation is repeated 100 times and the simulation result corresponds to the average value over 100 times. The first group of experiments is to investigate the effectiveness of probabilistic threshold based aggregation monitoring (PTAM) algorithm. Since the equivalence between sum monitoring and average monitoring is obvious, then we evaluate the performance of the proposed algorithm for average monitoring. We compare the active strategy against the passive strategy by running them over T time instances. The relative false positive rate and negative rate are used to measure the proposed strategies. The relative false positive rate is calculated as following, and the relative false negative rate can be computed similarly.

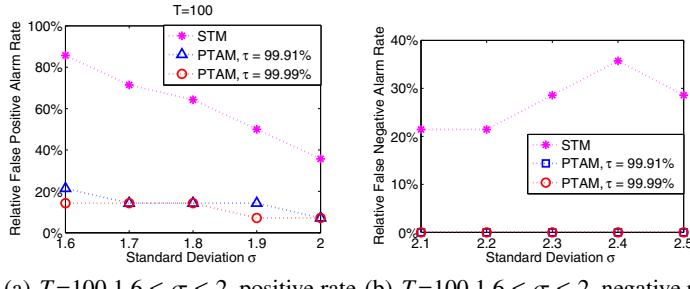
$$\text{Relative false positive rate} = \frac{\# \text{ false positive alarms}}{\# \text{ true alarms among } T \text{ time instances}}$$

As shown in Figure.1(a) and Figure.1(b), both strategies achieve low false alarm rate. Since active strategies more easily trigger alarms than passive strategy, they achieve a higher rate for false positive alarms. The second group of experiments is to compare PTAM algorithm and STM algorithm in terms of false alarm rate. The main idea of



(a) Active strategy vs. passive strategy (b) Active strategy vs. passive Strategy

Fig. 1. Performance of PTAM algorithm

**Fig. 2.**

STM algorithm is that if the sensed data is larger than the specified monitored threshold, an alarm is triggered. Since the measurement error follows the Gaussian distribution $N(0, \sigma)$, in which σ is the standard deviation. Then the comparison between PTAM algorithm and STM algorithm is conducted when the sensed data is influenced by measurement error. As expected, PTAM algorithm has better performance than that of STM algorithm. As shown in Figure.2(a), when the measurement error follows the distribution $N(0, 1.9)$, the relative false positive alarm rate of STM algorithm is higher than 40%, but the rate of PTAM algorithm is bellow 20%, in which the probability threshold is $\tau = 0.9999$. Although the relative false positive alarm rate of STM algorithm and PTAM algorithm is similar, PTAM algorithm has better performance in terms of false negative alarm rate. The above experimental results show that the probabilistic threshold based monitoring algorithm enables the monitoring result with probability guarantee, which decreases the false alarm rate.

5 Conclusion

To overcome the deficiencies of STM, this paper focuses on designing probabilistic threshold based monitoring strategies in WSNs, which can provide guarantees on the probability of triggered alarms. The tight upper bounds of the probability that monitored value is larger than the specified threshold are proved. According to the upper bounds, probabilistic threshold based algorithm for aggregation monitoring is proposed. Performance evaluation demonstrates that the proposed algorithms outperform the STM method in term of false alarm rate.

Acknowledgement. This work is supported in part by the National Grand Fundamental Research 973 Program of China under grant 2012CB316200, the Key Program of the National Natural Science Foundation of China under grant 61033015,60933001, the Major Program of National Natural Science Foundation of China under grant 61190115, and the National Science Foundation Distinguished Young Scholars of China under grant 61300225.

References

- [1] Sukun, K., Shamim, P., Culler, D.: Health monitoring of civil infrastructures using wireless sensor networks. In: Information Processing in Sensor Networks, IPSN 2007, pp. 254–263. IEEE (2007)
- [2] Huang, Z., Wang, L., Yi, K.: Sampling based algorithms for quantile computation in sensor networks. In: Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, pp. 745–756. ACM (2011)
- [3] Chaudhary, D., Nayse, S., Waghmare, L.: Application of wireless sensor networks for greenhouse parameter control in precision agriculture. International Journal of Wireless and Mobile Networks 3(1), 140–149 (2011)
- [4] Tang, M., Li, F., Phillips, J.: Efficient threshold monitoring for distributed probabilistic data. In: 2012 IEEE 28th International Conference on Data Engineering (ICDE), pp. 1120–1131. IEEE (2012)
- [5] Cao, Z., Sutton, C., Diao, Y.: Distributed inference and query processing for rfid tracking and monitoring. Proceedings of the VLDB Endowment 4(5), 326–337 (2011)
- [6] Dehnad, K.: Density estimation for statistics and data analysis. Technometrics 29(4), 495–495 (1987)
- [7] Gaber, M.: Data stream processing in sensor networks. In: Learning from Data Streams, pp. 41–48. Springer (2007)
- [8] Gama, J., Gaber, M.: Learning from data streams: processing techniques in sensor networks. Springer (2007)
- [9] Deshpande, A., Guestrin, C., Madden, S.: Model-driven data acquisition in sensor networks. In: Proceedings of the 30th International Conference on Very Large Data Bases, vol. 30, pp. 588–599. VLDB Endowment (2004)
- [10] Keith Lawrence, H.: Principles of environmental analysis. Analytical Chemistry 55(14), 2210–2218 (1983)
- [11] Huang, L., Garofalakis, M., Joseph, A.: Communication-efficient tracking of distributed cumulative triggers. In: 27th International Conference on Distributed Computing Systems 2007, pp. 54–54. IEEE (2007)
- [12] Sharfman, I., Schuster, A., Keren, D.: A geometric approach to monitoring threshold functions over distributed data streams. ACM Transactions on Database Systems (TODS) 32(4), 23 (2007)
- [13] Kashyap, S., Ramamirtham, J., Rastogi, R.: Efficient constraint monitoring using adaptive thresholds. In: IEEE 24th International Conference on Data Engineering 2008, pp. 526–535. IEEE (2008)
- [14] Mitzenmacher, M., Upfal, E.: Probability and computing: Randomized algorithms and probabilistic analysis. Cambridge University Press (2005)
- [15] Kosaki, H.: Arithmetic–geometric mean and related inequalities for operators. Journal of Functional Analysis 156(2), 429–451 (1998)

Topology-Transparent STDMA Protocol with MIMO Link for Multicast and Unicast in Ad Hoc Networks

Yueyang Song, Changle Li^{*}, Chao Guo, and Yu Zhang

State Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an, Shaanxi, 710071 China
clli@mail.xidian.edu.cn

Abstract. Most of the MIMO MAC protocols are used for either unicast or multicast instead of supporting both simultaneously, which could be a limitation in practical application. Furthermore, SISO-based traditional STDMA could lower the network throughput. So TTS-MIMO is newly designed by exploiting MIMO to raise the network throughput, which could support both unicast and multicast at the same time. By collecting and calculating the cross layer information which could affect the performance of multicast and unicast, the slot allocated to a node is determined dynamically. Utilizing the stream control technology of MIMO and reservation scheme, in the allocated slot, a node sends data packet of unicast or multicast directly, and in the unallocated idle slots, the node reserves the channel or sends data packet of multicast. Finally the simulation results show that the TTS-MIMO outperforms the STDMA in terms of throughput and slot utilization rate, in addition, the system QoS is improved since multicast and unicast are both supported.

Keywords: Ad hoc network, time slot allocation, multicast, unicast, MIMO.

1 Introduction

The self-organizing Ad hoc network is a multi-hop system with wireless transceivers, which can be organized anywhere at any time. It is widely used and becomes the key technology in many fields. MIMO technology at the physical layer has been widely studied and applied. But the advantages of MIMO, such as flexibility and network throughput improvement, can be effectively utilized only by designing upper layer protocols. So, to design better multiple access protocols supporting MIMO for Ad hoc network is studied widely. There are many classes of MIMO MAC protocols [1,2,3,4], such as stream control based [1], encoding based [2] and beam forming based [3]. We just focus on the MIMO MAC protocols based on TDMA.

Spatial Time Division Multiple Access (STDMA) is the extension of TDMA, which is a wireless channel MAC protocol for Ad hoc networks, it enables long distance mobile nodes share the same time slot to improve the throughput of network. There have been many researches on the STDMA protocols which resolve the slot allocation in Ad hoc networks [5,6,7,8,9]. However, these protocols utilize the SISO

* Corresponding author.

technology, which is not able to improve the network throughput. In addition, most of the MIMO MAC protocols are used for either unicast or multicast instead of supporting both simultaneously [10], which could be a limitation in practical application. To overcome these issues, Topology-Transparent STDMA protocol with MIMO links for multicast and unicast in Ad hoc network (TTS-MIMO) is proposed, in which the system QoS is improved since multicast and unicast are both supported. The proposed approach may be applied to large scale wireless networks [11,12] and the network throughput is also improved by exploiting MIMO.

The rest of the paper is organized as follows. Section 2 discusses the network model applied in the TTS-MIMO protocol. The proposed protocol is described in Section 3. In Section 4, we evaluate the network performance of the TTS-MIMO through the simulations. Finally, the conclusion is drawn in Section 5.

2 Network Model

Assuming an Ad hoc network consisting of N nodes [13], where each node can be denoted as $i \in N$. Node i has interference to node j if the SNR on link of node i to node j is greater than or equal to a certain threshold, this character is expressed by formula (1):

$$SNR(i, j) = \frac{P_i}{L_b(i, j)N_r} \geq \gamma_0 \quad (1)$$

In which, the P_i indicates the transmission power of node i , and the path loss of this power reaching to node j is denoted as $L_b(i, j)$, N_r means the effect of the thermal noise. If the link of node i to node j satisfied (1), node i, j allocate in the same contention area. As the nodes in the network are distributed sparsely, so several separated contention areas may exist according to the space.

A network model of 19 nodes is shown in Fig. 1, and area A , B , C are contention areas. Nodes in a same contention area cannot use the same slot to send data, such as node 4, 5, 6 which allocate in area A , while nodes in different contention area can reuse the slot, such as node 7, 10, 14 which belong to area A , C and B , respectively.

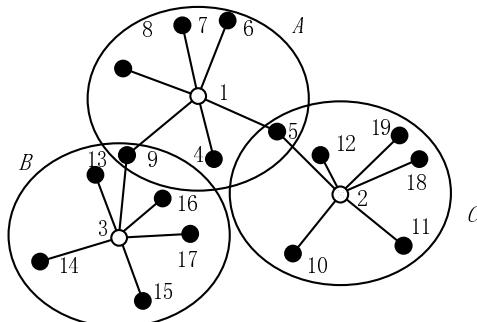


Fig. 1. Network model

In each contention area, like area A , B and C , there is a center node controls the slot allocation in the contention area it allocated. The distance between center node and the other nodes is nearly fixed. In order to reduce the interference, the distance between center nodes in each contention area must reach to a certain value. In Fig. 1, the node 1, 2, 3 are center nodes satisfied the condition.

3 TTS-MIMO Introduction

In the TTS-MIMO protocol, we choose the neighbor nodes density in the network layer and the packet priority in the MAC layer as two factors which can decide the slot allocation, since these two factors are related to the performance of multicast and unicast. Each node sends the neighbor nodes density and data sending packets priority to the center node, then the center node calculates the Q_i according to formula (2). And according to the Q_i , the slot allocated to a node is determined and will change with the topology of network.

$$Q_i = W_{d_i} d_i + W_{p_i} p_i \quad (2)$$

$$(W_{d_i} = \frac{d_i}{\sum_{j=1}^n d_j} , \sum_{i=1}^n W_{d_i} = 1 ; W_{p_i} = \frac{(7-p_i)}{\sum_{j=1}^n (7-p_j)} , \sum_{i=1}^n W_{p_i} = 1)$$

In formula (2), the slot factor Q_i is the sum of weighted d_i and weighted p_i . d_i is the neighbor density of node i and p_i is the packet priority owned to node i , which ranges from 0 to 7, in which 0 represents the highest priority and 7 represents the lowest priority. n means the number of nodes in a same contention area. W_{d_i} means the weighting value of d_i , and the W_{p_i} means the weighting value of p_i . The larger the value of Q_i is, the earlier the time slot is allocated. After finishing slot allocation, for fully utilizing the idle slot, nodes reserve the transmission of unicast or send packet of multicast.

3.1 TTS-MIMO Description

We assume sending node T and receiving node R , each node has M antennas, and the network topology is generated already. CTS packet has three types which are used in three cases respectively:

- (a) The CTS_1 packet is used when a node only receives 1 RTS packet for it without hearing any other packets at the same time. In this case, the receiving node replies a CTS_1 packet to the sending node to inform it to use all antennas for data transmission.
- (b) The CTS_2 packet is used when a node receives l RTS packets for it without hearing any other packets at the same time. In this case, the receiving node replies CTS_2 packets to inform all nodes who send RTS to it that they can use $\lfloor M/l \rfloor$ numbers of their antennas for transmission.

- (c) The CTS_3 packet is used when a node not only receives l RTS packets for it but also hears other packets at the same time. In this case, the receiving node replies the CTS_3 packets to inform all nodes who send RTS packet to it that they can use 1 antenna for transmission.

RTS/CTS/ACK packets are sent by one stream, which is good for avoiding collision. The specific operation procedure is described as follows:

Firstly, each node in the network sends one-hop hello packets periodically to get density information of its neighbor nodes. Then each node sends the density information and the packet priority to the center node, which generates slot factor Q_i , see formula (2). According to the Q_i , center node allocates slots to every node. The more neighbor nodes are and the higher data packet priority of a node has, the larger Q_i is, so the earlier slot will be allocated to the node. We allocate slot by this way is because neighbor density is a factor to decide the performance of multicast, and packet priority is a factor to decide the performance of both multicast and unicast. In other words, the more neighbor nodes are and the higher packet priority of a node has, the earlier the node can send data packet.

```

1.time slot is allocated by center node according to  $Q_i$ ;
2.while(time slot n){
3.    if(n=time slot allocated to node T){
4.        if(unicast) node T sends RTS packet to node R without CSMA/CA;
5.        else node T sends data packet of multicast using M antennas;}
6.    else{
7.        do CSMA/CA;
8.        if(channel is idle){
9.            if(unicast) node T sends RTS packet to node R to reserve channel;
10.           else node T sends data packet of multicast using 1 antenna;}
11.    else node T delays this transmission until next slot;}
12.waits CTS packet;
13.switch(CTS){
14.    case CTS1: node T sends data packet to node R using M antennas;
15.    case CTS2: node T sends data packet to node R using [M/l]antennas;
16.    case CTS3: node T sends data packet to node R using 1 antenna;}
17.waits ACK packet;
18.if(ACK packet is received) this transmission of unicast is successful;
19.else delay this transmission of unicast until next slot;
20.n++;}

```

(a) Operation process of the sending node T

```

1.if(node R received RTS packet only for itself and heard nothing){
2.    if(RTS=1) node R replies CTS1 packet to node T;
3.    else node R replies CTS2 to nodes who send RTS packets to it;}
4.else if(node R heard packet of multicast)
5.    node R gives up replying CTS packet to nodes who send RTS packet to it;
6.else node R replies CTS3 to nodes who send RTS packets to it;
7.if(node R received data packet of unicast successfully)
8.    node R replies ACK packet to node who send RTS packets to it;
9.else
10.   node R gives up replying ACK packet to nodes who send data packet to it;

```

(b) Operation process of the receiving node R

Fig. 2. Operation process of sending and receiving node

Then, in the slot allocated to node T , if the traffic is unicast, the node T sends RTS packet directly, and if the traffic is multicast, node T sends packet of multicast directly using full antennas. In the idle slot unallocated to node T , node T reserves channel to realize unicast or sends data packet of multicast using 1 antenna. According to the different case of receiving CTS packet, sending node selects appropriate number of antennas to send data packets. When a data packet of unicast is received successfully, the receiving node R replies ACK packet to the sending node for confirmation. Otherwise, a failed transmission occurs and the sending node waits retransmission until the next slot. ACK packet is unnecessary in multicast traffic. The operation process of sending node T and of the receiving node R is shown in Fig. 2.

3.2 TTS-MIMO Implementation

We assume the network model has the topology as Fig. 1 shows, and assume all nodes have 4 antennas in the network. We also assume that the nodes within one-hop range are mutual communication and that the nodes within two-hop range are mutual sense. According to Fig. 1, the slot allocation frame structure is shown in Fig. 3. We take the transmission cases in the time slot 1 of the contention area A as a specific instance to analyze operation procedure in the TTS-MIMO, the operation procedure in other contention areas are the same as this instance.

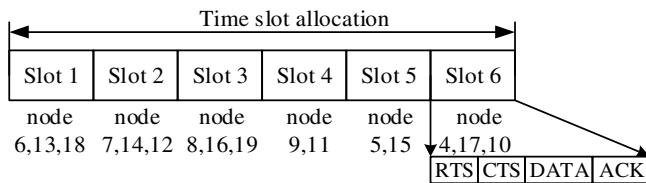


Fig. 3. Slot allocation frame structure

Fig. 4 shows the transmission procedure when the node 6 sends data packet of unicast in the slot allocated to it. Node 6 can directly send RTS packet in the slot 1,

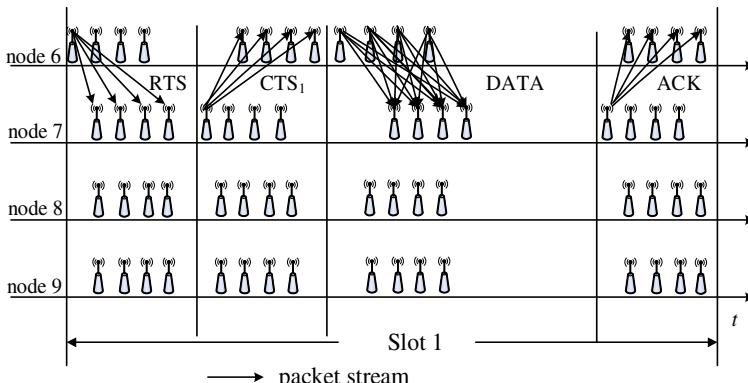


Fig. 4. Node sends data packet of unicast in the allocated slot

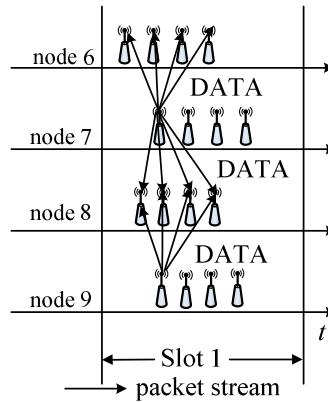


Fig. 5. Node sends data packet of multicast in the unallocated slot

node 7 only received 1 RTS and not heard any other packet transmission. So node 7 replies CTS₁ packet to node 6 to inform node 6 to send 4 data streams. When node 7 received data packet from node 6 successfully, node 7 confirms this transmission by ACK packet. Other nodes will do CSMA/CA at the beginning of the time slot 1 and will keep quiet in the slot 1 without sending packet until the next slot.

Fig. 5 shows the transmission procedure that the node 6 has no data packets to send in the time slot 1 allocated to it. While at the beginning of the time slot 1, if the node 7 and node 9 have data packet of multicast to send, they will do CSMA/CA, and then find the channel is idle, so they send data packet of multicast using 1 antenna respectively. Using 1 antenna for transmission is good to avoid collision.

Fig. 6 shows the transmission procedure that the receiving node has received multiple RTS for it and heard nothing. Node 6 has no data packets to send in the time slot 1 allocated to it, so this slot is idle. At the beginning of the slot 1, node 7, 9 have

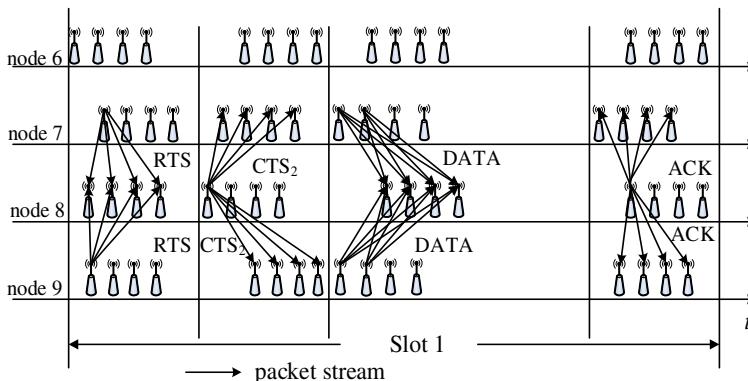


Fig. 6. Receiving node received two RTS packets

data packet of unicast to send to node 8, and then find the channel is idle to make reservation. So node 8 will receive 2 RTS packets and it will reply a CTS₂ packet to the sending node 7, 9 for notifying them to send 2 parallel data streams. This process makes use of the characteristics of the multiple packet reception and interference suppression in MIMO technology, which helps node 8 to receive and separate the data streams from different nodes.

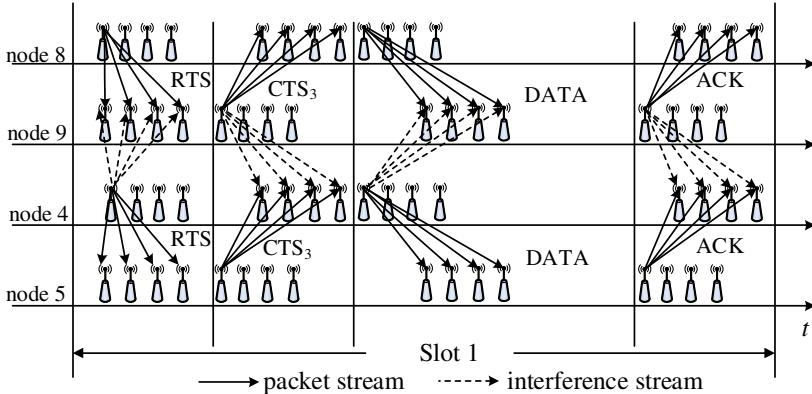


Fig. 7. Receiving node received RTS packet and hear other packet

Fig. 7 shows the transmission procedure that the receiving node has not only received RTS packet for itself but also heard other packets at the same time. In the time slot 1 allocated to node 6, node 6 has no data packets to send, so this time slot is idle. At the beginning of the time slot 1, node 8 and node 4 have data packets to send to node 9 and node 5 respectively, and then find the channel is idle to make reservation. So the node 9 not only receives RTS packet from node 8, but also receives RTS packet from node 4. In order to avoid collision, the node 9 and node 5 send CTS₃ packets to the node 8 and node 4 to notify them to send 1 data stream, respectively.

4 Performance Evaluation

We conduct simulations on the MATLAB to evaluate the performance of the TTS-MIMO. There are 40 transmitters in a contention area and each transmitting stream is 200 bytes in the simulation scenario. The antenna number M is 4. One slot is allowed at most 2 transmission chances. One time slot cycle consists of all slots allocated to nodes in a contention area.

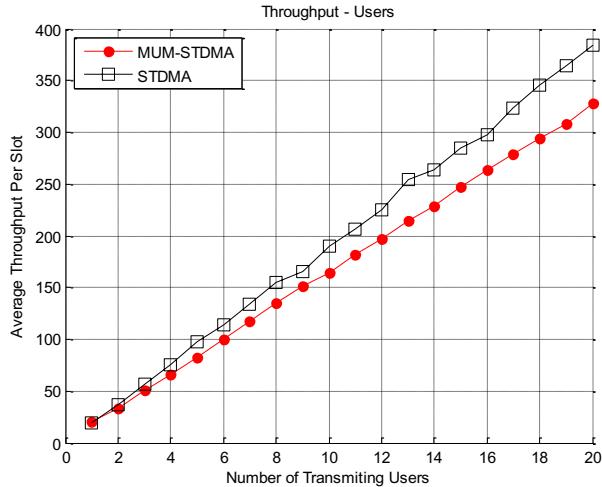


Fig. 8. System throughput when each transmitter has 1 transmission chance

Fig. 8 shows the average throughput (bytes/slot) when each transmitter only has 1 transmission chance. In the STDMA protocol, each transmitter can use 4 antennas to send data packets in their own time slot without any collision. While in the TTS-MIMO protocol, transmitter is allowed to send data packets in the unallocated slot when the slot is sensed to be idle. Therefore, the collision and stream control result in the transmission streams less than 4, and the system average throughput would below that in the STDMA.

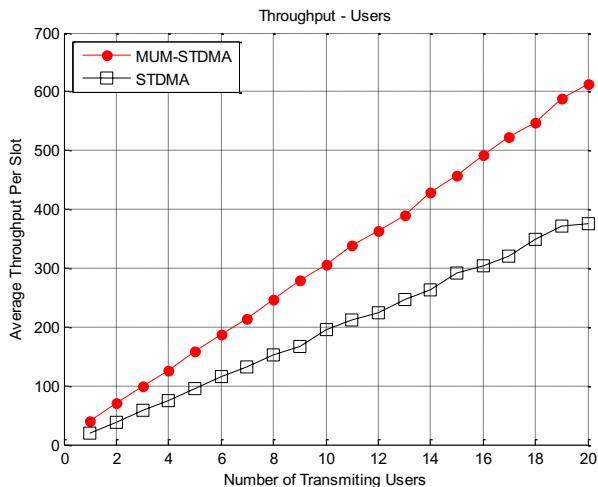


Fig. 9. System throughput when each transmitter has 2 transmission chances

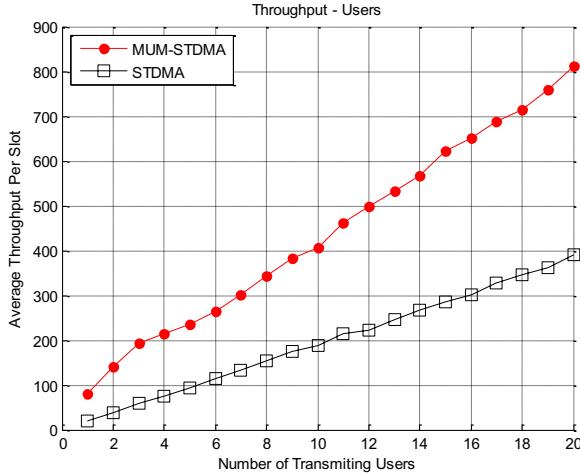


Fig. 10. System throughput when each transmitter has 4 transmission chances

Fig. 9 and Fig. 10 show the average throughput when each transmitter has 2 or 4 transmission chances respectively. The STDMA protocol allocates fixed length of time slot to each transmitter for transmission, idle slots is wasted. While in the TTS-MIMO protocol, transmitter can finish transmission not only in its own slot but also in the idle slot owned to other nodes. Therefore, the TTS-MIMO has higher average throughput.

Fig. 11 shows the corresponding utilization rate of time slots when each transmitter has 1, 2, 4 chances to send respectively. When the chance is 1 or 2, the utilization rate of time slots in the STDMA protocol is higher than that in the TTS-MIMO protocol. This is because the STDMA protocol would finish transmission in u fixed allocated

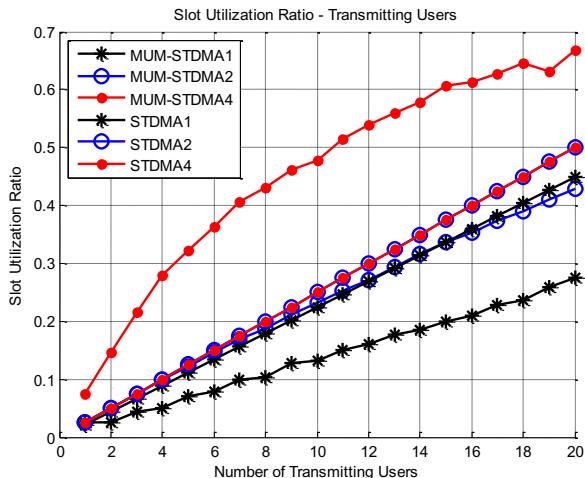


Fig. 11. Slot utilization rate when transmitter has different transmission chance

time slots. While for the TTS-MIMO protocol allowing transmission in the idle time slots through reservation or sending data packets of multicast, nodes can finish the same transmission in v time slots where $v < u$. When the transmission chance of each node is gradually increased, the utilization rate of fixed allocated time slots do not increase in the STDMA protocol, but the TTS-MIMO protocol can make full use of idle time slots to send data packets so as to improve the utilization rate of time slots.

5 Conclusion

Aiming at the practical limitation in most of MIMO MAC protocols, TTS-MIMO is proposed, which could support both unicast and multicast at the same time. Compared to the STDMA, the network throughput is improved by exploiting MIMO technology. The simulation results show that the TTS-MIMO outperforms the STDMA in terms of throughput and slot utilization rate, in addition, the system QoS is improved since multicast and unicast are both supported. Therefore, considering the impact of neighbor nodes density and data packet priority, TTS-MIMO protocol performs better in Ad hoc networks.

There are some future works in TTS-MIMO protocol, such as 1) repeat broadcast slot allocation problem, the same broadcast packet of the node in the intersection of two contention area may send twice so that makes channel slots utilization lower; 2) as for formula (2), it may consider the impact of the current channel conditions in the future work.

Acknowledgements. This work was supported by National Natural Science Foundation of China (61271176), National Science and Technology Major Project (2013ZX03004007-003) and the 111 Project (B08038).

References

1. Sundaresan, K., Sivalumar, R., Ingrain, M.A., et al.: Medium Access Control in Ad hoc Networks with MIMO Links: Optimization Considerations and Algorithms. *IEEE Transactions on Mobile Computing* 3(4), 350–365 (2004)
2. Tan, K., Adrian, J.H., Zhu, H., Candocia, F.M., et al.: A Novel Spectrum Encoding MIMO Communication System. *Wireless Personal Communications* 52(1), 147–163 (2010)
3. Huang, K., Andrews, J.G., Guo, D., Heath, R.W., et al.: Spatial Interference Cancellation for Multiantenna Mobile Ad hoc Networks. *IEEE Transactions on Information Theory* 58(3), 1660–1676 (2012)
4. Park, M., Choi, S.H., Nettles, S.M.: Cross-layer MAC Design for Wireless Networks Using MIMO. In: Proceeding of the IEEE Global Telecommunications Conference, p. 5. IEEE, Piscataway (2006)
5. Rezazade, L., Aghdasi, H.S., Ghorashi, S.A., Abbaspour, M.: A Novel STDMA MAC Protocol for Vehicular Ad hoc Networks. In: International Symposium on Computer Networks and Distributed Systems, pp. 148–151. IEEE, Piscataway (2011)

6. Wu, C., Shuang, X., Liang, H., Di, X.: Design and Implementation of STDMA Slot Allocation Algorithm Based on Strategic Game for Ad hoc Networks. In: Proceeding of the Chinese Control Conference, pp. 4426–4430. IEEE, Piscataway (2011)
7. Li, J., Gong, E., Sun, Z., Li, L., Xie, H.: An Interference Based Distributed TDMA Scheduling Algorithm for Aeronautical Ad hoc Networks. In: International Conference on Cyber-enabled Distributed Computing and Knowledge Discovery, pp. 453–460. IEEE Computer Society, Beijing (2013)
8. Guo, Z.H., Chen, Y.G.: An Optimal Scheduling Algorithm in Spatial TDMA Mobile Ad hoc Networks. In: International Conference on Microwaves, Radar & Wireless Communications, p. 5. IEEE, Piscataway (2010)
9. Yan, Y.C., Li, D.M., Xue, D.: Slot Assignment of Spatial TDMA in Ad hoc Radio Networks Using Fuzzy Set Theory. In: Proceedings of the IEEE 6th Circuits and System Symposium on Emerging Technologies, pp. 497–500. IEEE, Shanghai (2004)
10. Li, J.D., Zhang, G.H., Chen, Y.Y., Li, C.L., et al.: Broadcast Scheduling Algorithms in Multihop Ad hoc Networks with MIMO Links. Journal of Xidian University 33(4), 580–583 (2006)
11. Wang, X., Huang, W., Wang, S., Zhang, J., Hu, C.: Delay and Capacity Tradeoff Analysis for MotionCast. IEEE/ACM Transactions on Networking 19(5), 1354–1367 (2011)
12. Wang, X., Fu, L., Hu, C.: Multicast Performance with Hierarchical Cooperation. IEEE/ACM Transactions on Networking 20(3), 917–930 (2012)
13. Geng, R.: A Cross Layer QoS Design Model for Mobile Ad hoc Networks. In: International Conference on Wireless Communications, Networking and Mobile Computing. IEEE Computer Society, Wuhan (2011)

Secure Device-to-Device Authentication in Mobile Multi-hop Networks

Hyunsoo Kwon¹, Changhee Hahn¹, Daeyoung Kim¹, Kyungtae Kang²,
and Junbeom Hur¹

¹ School of Computer Science and Engineering, Chung-Ang University,
Seoul, Republic of Korea

{khs910504,Mckinsey,rlaeod,jbhur}@cau.ac.kr

² Department of Computer Science and Engineering, Hanyang University,
Ansan, Republic of Korea
ktkang@hanyang.ac.kr

Abstract. In order to deal with drastically increasing mobile traffic these days, device to device connection (D2D) which provides infra-connection's off-loading is getting a lot of attention. However, we observed that most of the current D2D protocols such as Bluetooth and Wi-Fi Direct are not scalable, and vulnerable to main-in-the-middle (MITM) and replay attacks in mobile multi-hop networks. In this paper, we propose novel D2D authentication protocols with a secure initial key establishment using ciphertext-policy attribute-based encryption(CP-ABE) to solve this problem. By exploiting CP-ABE, the proposed scheme allows the communicating parties to mutually authenticate each other and derive the link key in an expressive and secure way in the multi-hop network environment. According to the analysis results, the proposed scheme is secure against MITM and replay attacks in the D2D mobile multi-hop networks.

1 Introduction

A large increase of the smart device brought up significant increase in mobile traffic. According to the study in [1], mobile traffic is going to get 18 times larger for 5 years as of 2011 and also grow 3 times faster than the growth of static IP traffic. Following the trend, device to device (D2D) connection technique receives much attention. Such a technique has an effect of reducing the concentrated traffic of infrastructure because personal smart devices can directly communicate without using a network infrastructure. Also, D2D standardization which supports location-based applications has been developed by several IEEE communication working groups: IEEE 802 and 3GPP. IEEE 802.15.8 working group is now developing PAC(Peer Aware Communication) specification [2] and 3GPP SA is developing ProSe(proximity Service) specification [3], which construct a new mobile ecological system. For example, when a user enters a convenient store, the user can automatically obtain have discount coupons and information about the sale items for the day in real time through a mobile device.

D2D technique is already developed and widely used in the current mobile environment, such as Bluetooth, Wi-Fi Direct. Bluetooth supports authentication between different devices using pre-shared PIN [4]. Wi-Fi Direct protocol has been constructed and on the basis of Wi-Fi. It forms a group composed of a group manager and multiple clients, where each client can do direct communications to the manager [5]. However, in multi-hop network environment where multiple relaying nodes are existing between communicating parties, current D2D protocols cannot guarantee confidentiality or integrity of communications since malicious intermediate nodes can perform man-in-the-middle(MITM) or replay attack during the transmission.

In this paper, we propose a new authentication protocol for D2D communications in a mobile multi-hop network environment. The proposed scheme enables end users to share initial secret keys in a scalable and secure manner by exploiting CP-ABE scheme. Also, we added message integrity code which is generated by PIN and sequence number to enhance security in a mobile multi-hop network.

Our scheme is based on the Bluetooth protocol, but the initial secret key distribution process can be independently designed, the proposed scheme can be used to other D2D authentication protocol such as Wi-Fi Direct. According to the analysis results, the proposed scheme is very efficient and secure against man-in-the-middle attacks and replay attacks in the presence of malicious relaying nodes in a mobile multi-hop networks.

2 Related Work

In this section, we introduce the mobile multi-hop network. Also, we present the authentication process and its security flaws in Bluetooth and Wi-Fi Direct pairing procedures in a mobile multi-hop network.

2.1 Mobile Multi-hop Network

An Ad hoc network [6] features a mechanism that allows multiple nodes to compose a flexible and dynamic network without any infrastructure, such as mesh network [7] and sensor network [8]. Especially when it is composed of mobile nodes, it is called a Mobile Ad-hoc Network(MANET). Since each mobile node maintains a routing table for networks and has capability for the routing information management, those mobile nodes establish networks for communication themselves without infrastructure such as base station or access point [9][10]. In addition, the communication range of each mobile nodes can be extended by relaying it through multiple relaying nodes that are deployed in the middle of communicating parties.

Compared to the direct communication environment, several novel security challenges should be considered in a mobile multi-hop network. The first challenge is the initial key establishment problem. Sharing initial secret keys with all of the different nodes in advance especially in a large-scaled network is impractical due to the limited storage space of mobile devices. And also, malicious relaying nodes can try man-in-the-middle attacks which maliciously change the

message or modify the authentication information that are being sent between mobile nodes. The malicious relaying nodes also can capture previously sent messages en route and perform replay attacks that fraudulently repeats the stored messages in a mobile multi-hop network. Thus, the scalable and secure key management and authentication protocol are very important for secure D2D communications in a mobile multi-hop networks. There have been proposed several protocols addressing this problem in a mobile multi-hop network, [11],[12],[13], however, those schemes only work in a static network structure. Also, existing authentication protocols [14], [15] in MANET exploit Public-Key Infrastructure(PKI) to prove identity of mobile nodes, however, it is not suitable for D2D environment which is fully infrastructureless.

2.2 Bluetooth Pairing

Bluetooth is used for transferring data and short range communication using low power [4]. Bluetooth devices authenticate each other through the pairing process. Pairing checks whether each device is authenticated and if authenticated, it allows the devices to generate a common link key.

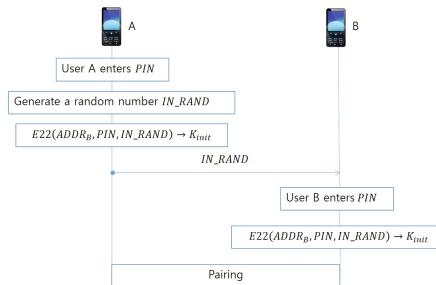


Fig. 1. Bluetooth Pairing

Fig. 1 illustrates the pairing process to generate the link key using the shared PIN. First, the device A, which is a master device, takes PIN from the user, and generates IN_RAND which is a 128 bit random number. Then it generates initial key K_{init} using a hash function E22 on inputs the address of slave device $ADDR_B$, PIN and IN_RAND. K_{init} is used to generate a link key, which is an encryption key for secure communications after the pairing process. After creating K_{init} , A transfers IN_RAND in plaintext to slave device B. After slave device enters the PIN and obtains the K_{init} as master device does, it generates the link key for secure communications afterward.

In order to secure the authentication process, PIN has to be shared between the devices previously. In short distance communication, it may be possible to share the secret information ahead through direct communications among devices. However, in a mobile multi-hop network environment, it is very challenging to share the PIN before which makes the authentication process impossible and vulnerable to replay and MITM attacks [16]. Therefore, in a mobile multi-hop

network environment, it is important to share the PIN safely for mutual authentication. When the PIN is sent as a plaintext through a mobile multi-hop network, intermediate relaying nodes or outside adversaries can steal the information. In addition, using the symmetric encryption for sharing the PIN incurs a scalability problem in key management because when the size of the network is N , the key size results in $O(N^2)$ which makes it difficult to manage them in the network.

2.3 Wi-Fi Direct Pairing

Wi-Fi Direct [5] is on the basis of IEEE 802.11 standard [17]. It enables Wi-Fi devices to connect to each other directly. Wi-Fi Direct guarantees enhanced Quality of Service(QoS) [18] and security mechanisms [19], which are inherited properties from Wi-Fi protocol. A device equipped with Wi-Fi Direct communication capability is called a P2P device. A P2P group consists of a P2P group owner(P2P GO) and Clients.

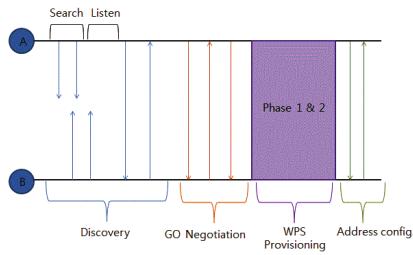


Fig. 2. Wi-Fi Direct Pairing

Fig.2 illustrates the process of Wi-Fi Direct pairing. First in “Discovery” phase, a P2P device alternately switches from “listen” and “search” status to detect whether there are other P2P devices or not. Once the P2P devices are found, they determine the roles of themselves between P2P GO and P2P client using a three-way handshake. This phase is called “GO Negotiation”. In Fig.2, device A illustrates P2P GO and B illustrates P2P Client. Next, in WPS provisioning phase, P2P devices perform mutual authentication and share encryption key. Specifically, the WPS provisioning is composed of Phase 1 and Phase 2. In Phase 1, P2P devices generate and share Master key. Then, using 4-way handshake, they generate link key from the shared Master key in Phase 2.

In one-hop communications, Wi-Fi Direct protocol provides secure authentication in the presence of outside adversaries. However, in a mobile multi-hop network, the authentication protocol cannot guarantee it due to the intermediate relaying nodes that can maliciously forge the messages or perform relay and MITM attacks en route.

3 Secure D2D Authentication Protocol in Mobile Multi-hop Networks

In this section, we propose the D2D authentication protocol that is efficient and secure in a mobile multi-hop network by exploiting attribute-based encryption. The attribute-based encryption provides a scalable and secure way to share initial secret keys among communicating parties.

3.1 Attribute-Based Encryption

Public key cryptosystem can be a promising solution to share initial secret keys between communicating parties in a mobile multi-hop networks. However, public key encryption can be only used in PKI which includes a trusted server for managing certificates. In ad-hoc network, public key encryption is difficult to be used since it is infrastructureless. Attribute-based encryption(ABE) can be a promising solution for scalable and secure key distribution in such an infrastructureless multi-hop environment [20]. ABE is evolved from fuzzy identity-based encryption which is extended on the basis of identity-based encryption [21][22][23]. We suppose w and w' denote independent sets of attributes associated with a ciphertext and a user respectively. Then, in order to decrypt a ciphertext encrypted with w , the overlapped value between user's attribute w' and w has to satisfy beyond a specific predefined threshold. Accordingly, ABE can provide secure communication by only using people's attributes without infrastructure. However, ABE might cause a problem in a certain individual communication because it uses predefined threshold. Therefore, ciphertext-policy attribute-based encryption(CP-ABE) is proposed to fine-grained access control [24]. In CP-ABE, when generating ciphertext, the encryption key is directly generated by sender's access policy, and this allows delicate managing on the receiver whether it can decrypt the ciphertext or not without infrastructure. For instance, an administrator of A school's grade evaluating program can define the access policy for encrypting the data with this policy. ((“workplace: A school” AND “party: B department”) OR “department number: 19253” AND (position > assistant professor)).

3.2 Proposed Scheme

In this section, we propose a device to device authentication(D2DA) protocol which is secure in a mobile multi-hop network environment. The proposed scheme is constructed on the basis of Bluetooth authentication protocol by adding additional initial key sharing process. It enables scalable and secure initial key establishment even in a mobile multi-hop network environment. In addition, the existing Bluetooth protocol is also modified in such a way that it is secure against replay and modification attack by malicious relaying nodes. Even if the proposed scheme is developed on the basis of Bluetooth protocol, it is not limited to Bluetooth protocol, but can be applicable other direct communication protocol, such as Wi-Fi Direct.

Mobile multi-hop network gives 2 possible scenarios: First, a device may need to communicate either with an arbitrary mobile device, or with a specific group composed of multiple devices. Second, a device may need to communicate with a specific device in the group. In consideration of these scenarios, we propose two authentication protocols for each of them, that is D2DA1 and D2DA2 respectively. We assume that the attribute keys are distributed to each device during the initial setup phase before the proposed authentication protocol.

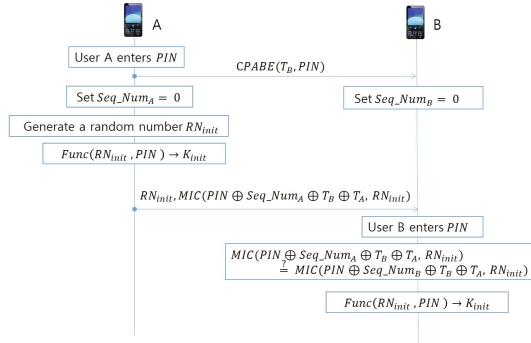


Fig. 3. D2DA1 authentication procedure

D2DA1. In this section, we propose a D2DA1 protocol, which supports device-to-device and device-to-group authentication and communication. As mentioned above, Bluetooth has to share PIN before pairing, however, in a mobile multi-hop network environment, it is difficult to guarantee the confidentiality and integrity of sharing secret information through D2D communication. Therefore, D2DA1 exploits CP-ABE which enables a sender to define an access control policy and enforce it to the encrypted data. Thus, the sender can selectively distribute the PIN to a set of selected receivers in a scalable and secure way. Additional random number and message integrity code (MIC) are adopted in the protocol to enhance integrity and confidentiality of authentication messages. Fig.3 shows D2DA1 authentication procedure.

The protocol progresses as follows:

1. User A enters PIN to device A
2. A → B: $CPABE(T_B, PIN)$

Device A defines access policy T_B with a set of attributes, encrypts PIN under T_B , and sends it to device B. Device A simultaneously resets the Seq_Num to 0 when transferred. Device B also simultaneously resets the Seq_Num to 0 when it receives data from device A. Device A generates 128bits random number. Then it generates initial key K_{init} using hash function $Func$ on inputs RN_{init} and PIN.

3. A → B: $RN_{init}, MIC(PIN \oplus Seq_Num \oplus GI_B \oplus GI_A, RN_{init})$

Device A sends RN_{init} in plaintext and MIC of RN_{init} generated with a key which is XOR of A's Seq_Num, B's device information GI_B , A's device information GI_A , and PIN to device B. Device B decrypts PIN from the ciphertext if a set of attributes of B satisfies the access policy T_B . Then, user B enters the PIN. Finally, B generates MIC of received RN_{init} with a key, that is $PIN \oplus Seq_Num \oplus GI_B \oplus GI_A$. If the MIC from B is equal to MIC from A, B can generate accurate initial key K_{init} using hash function $Func$ on inputs RN_{init} and PIN.

Device-to-group authentication is almost the same as the above protocol except that GI_B is replaced by another group information such as a group ID. After they share the initial secret key, the other procedures for generating link key is the same as Bluetooth protocol.

D2DA2. In this section, we propose a D2DA2 protocol for device-to-device in a specific group. In D2DA2 protocol, we assume that there is a group manager(GM) who manages the group. For example, GO in Wi-Fi Direct plays the role of GM. In the environment where all group member know the PIN and can generate initial key it is impossible for an arbitrary device and a specific device in the group to communicate privately. Therefore, GM is selected for special role to make this authentication and communication possible.

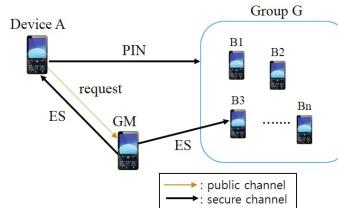
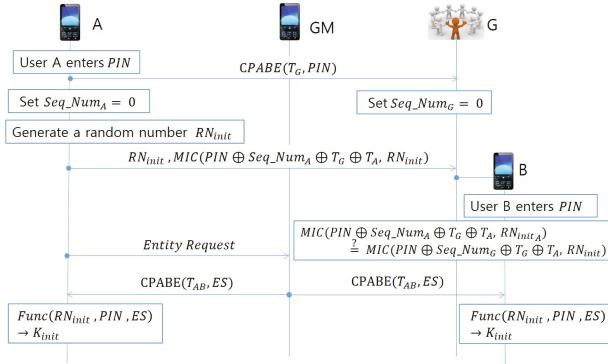


Fig. 4. Key sharing process in D2DA2

Fig.4 shows an example scenario. Suppose that PIN is shared between device A and group B by D2DA1 protocol. When device A wants to communicate with device B3 in group G, GM is selected first with the following strategy. A device that knows locations of each member of the group, but does not belong to the group is selected as GM. If device A sends to GM a request message that A wants to communicate with B3, GM sends encrypted secure information, ES, which can only be decrypted by A and B3. Since, only device A and B3 possess both PIN and ES, they can generate another initial key that others cannot generate. Fig.5 illustrates D2DA2 protocol.

D2DA2 protocol progresses as follows:

1. User A enters PIN to device A

**Fig. 5.** D2DA2 authentication procedure2. $A \rightarrow G: CPABE(T_G, PIN)$

Device A defines access policy T_G with a set of attributes, encrypts PIN under T_G , and sends it to the group G. Device A simultaneously resets the Seq_Num to 0 when transferred. Group G also simultaneously resets the Seq_Num to 0 when it receives data from device A. Device A generates 128bits random number. Then it generates initial key K_{init} using hash function $Func$ on inputs RN_{init} and PIN.

3. $A \rightarrow G: RN_{init}, MIC(PIN \oplus Seq_Num \oplus GI_G \oplus GI_A, RN_{init})$

Device A sends RN_{init} in plaintext and MIC of RN_{init} generated with a key which is XOR of A's Seq_Num, group information GI_G , A's device information GI_A , and PIN to group G. Any group members in G decrypts PIN from the ciphertext if a set of attributes of them satisfies the access policy T_G . Then, group G enters the PIN. Finally, G generates MIC of received RN_{init} with a key, that is $PIN \oplus Seq_Num \oplus GI_G \oplus GI_A$. If the MIC from G is equal to MIC from A, G can generate accurate initial key K_{init} using hash function $Func$ on inputs RN_{init} and PIN.

4. $A \rightarrow GM: Entity\ Request$

Device A sends the request message to GM.

5. $GM \rightarrow A\ and\ B: CPABE(T_{AB}, ES)$

GM encrypts the secret information ES using CP-ABE with access policy T_{AB} that is made of attributes of A and B. GM sends the encrypted GM to A and B. Each device A and B obtain the ES by decrypting the message with their attributes. Then, they generate an initial key, $K_{init} = Func(RN_{init}, PIN, ES)$.

4 Security and Efficiency Analysis

In this section, we analyze the efficiency and security of our proposed protocol. First, we analyze the security against the two main attacks: man-in-the-middle

attack and replay attack. Additionally, we show how the scheme has been enhanced on computation, storage and communication perspectives.

4.1 Security Analysis

Man-in-the-Middle Attack. In D2DA1 scheme, when a sender device transmits the secret information, such as PIN, the device sends it after encrypting it using CP-ABE algorithm. It encures that even if malicious nodes relay the authentication exchanges en route, they cannot obtain any secret information as long as their attributes do not satisfy the access policy embedded in the ciphertext. Thus, end-to-end confidentiality is guarantee against individual or colluding attack of malicious nodes [24]. Therefore, sharing PIN is secure under man-in-the-middle attack. Also, message integrity is preserved due to the adoption of MIC for a random number, which is generated with a securely shared PIN. Thus, the PIN sharing process is secure against outsider adversaries or inside adversaries such as relaying nodes in a multi-hop network.

In D2DA2 scheme, the message exchange procedure between a device and a group for sharing PIN is the same as D2DA1 scheme. However, it adopts additional security parameter, ES. The group manager encrypts ES using CP-ABE with an access policy that can be satisfied by only the communicating parties' attributes and sends it to the communicating devices. It is not possible for another device to decrypts the message and gets the ES. Even though every device in the same group has a PIN, they cannot generate K_{init} without the ES. Therefore, D2DA2 scheme is also secure against man-in-the-middle attack in the presence of the inside attacker.

Replay Attack. In the mobile multi-hop network, replay attack is done by the relay node. In order to prevent the replay attack, we adopt sequential number, Seq_Num. When the PIN is shared, Seq_Num is reset to 0. Every time a device performs the protocol, Seq_Num increases by 1. When a receiver obtains sender's Seq_Num from MIC for RN_{init} , it can know whether the message is replayed or not by comparing its own Seq_Num and sender's Seq_Num. Thus, it is secure under the replay attack.

4.2 Efficiency Analysis

In this section, we compares Bluetooth, D2DA1, D2DA2 protocols in terms of computation, storage and communication.

Computation Cost. Table 1 shows the comparison result of the computation cost. It is categorized into two different phases: communication cost for (1) protocols before PIN establishment(which is Phase 1 in the table) and (2) protocols after PIN establishment(which is Phase 2 in the table). In both of the proposed scheme, compared to the Bluetooth protocol, CP-ABE encryption and CP-ABE

Table 1. Computation cost

		Bluetooth	D2DA1	D2DA2	
Computation	Phase 1			Device	GM
	Phase 2	3P + 6H + 2SE + 2SD	3P + 7H + 3SE + 2SD	3P + 7H + 3SE + 2SD + 2CAD	CAE

P: pseudo random generator, SE/SD: symmetric encryption/decryption

H: hash function, CAE/CAD: ciphertext-policy attribute-based encryption/decryption

decryption are additionally introduced in order to send PIN securely in a mobile multi-hop network.

In Phase 2, computation for MIC generation is required to guarantee message integrity. Even if it adds additional computation cost, message integrity is guaranteed, which cannot be preserved in Bluetooth. In D2DA2 scheme, secret key ES needs to be delivered to communicating parties by GM, which requires one CP-ABE encryption in GM and one CP-ABE decryption in each device.

Even if the CP-ABE computation incurs relatively high cost, it is done once and for all during the initial authentication process for the PIN delivery. Therefore, when a device is authenticated again, the CP-ABE computations need not to be performed afterwards.

Storage Cost. Table 2 shows storage cost of each scheme. A random number, PIN, and device identifier are commonly store in all protocols. In D2DA1 and D2DA2 schemes, however, each device stores Seq_Num. Seq_Num is used to prevent replay attack. D2DA2 scheme requires only the communicating devices to store one more secret key, that is ES, which is used to guarantee more fine-grained access control.

Table 2. Storage cost

	Bluetooth	D2DA1	D2DA2
Storage	IN_RAND, PIN, BD_ADDR(A,B)	PIN, RN_{init} , GI(A,B) Seq_Num	PIN, RN_{init} , ES GI(A,B), Seq_Num

IN_RAND, RN_{init} : random number, PIN: personal identification number

ES: entity secure information, BD_ADDR(A,B), GI(A,B): device identifier, Seq_Num: sequence number

Communication Cost. Table 3 shows the analysis results in terms of communication. In case of Phase 1, the proposed scheme requires additional communication cost for PIN sharing securely. In Phase 2, the proposed schemes require additional communication cost for sending MIC. We note that it is inevitable cost to pay for making the protocols secure against any inside or outside adversaries in a mobile multi-hop network. In the case of D2DA2, additional communication cost is demanded for delivering ES to communicating parties securely, that is 2S_C.

Table 3. Communication cost

		Bluetooth	D2DA1	D2DA2	
Computation	Phase 1			Device	GM
	Phase 2	S_RN	S_RN + S_MIC	S_RN + S_MIC	2S_C

S_RN: random number size, S_MIC: MIC size, S_C: ciphertext size

5 Conclusion

Device-to-device(D2D) communication is getting lots of attention due to its applicability in infrastructureless network environment, such as mobile multi-hop networks. However, current D2D authentication protocols cannot be used in multi-hop networks because they are vulnerable to inside attacks such as man-in-the-middle attack or replay attack by relaying nodes. In this paper, we proposed D2D authentication protocols using CP-ABE to solve the problems with regard to sharing the initial secret information safely under the attacks. Also, the proposed schemes guarantee the integrity of messages by using message integrity code. Even if the proposed schemes are designed on the basis of Bluetooth protocol, our schemes solve the initial key establishment problems and integrity problems in the presence of the inside adversaries in multi-hop networks. Therefore, the proposed schemes can be applicable to the other D2D protocols, such as Wi-Fi Direct.

Acknowledgment. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2012R1A1A1001835 and 2013R1A2A2A01005559).

References

1. CISCO: Cosco Visual Netowking Index: Global Mobile Data Traffic Forecast Update, 2013-2018. White paper (2014)
2. IEEE 802.15 WPAN Task Group8 Peer Aware Communications, <http://www.ieee802.org/15/pub/TG8.html>
3. 3GPP: Feasibility Study on Proximity-based Services. Technical report, 3GPP (2012)
4. Lee, C.: Bluetooth Security Protocol Analysis and Improvements. M.Sc. thesis at San Jose State University (2006), <http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf>
5. Camps-Mur, D., Garcia-Saavedra, A., Serrano, P.: Device-to-Device communications with Wi-Fi Direct: overview and experimentation. IEEE Wireless Commun 20(3), 96–104 (2013)
6. Perkins, C.: Ad Hoc Networking, pp. 1–23. Addison Wesley Professional, Indianapolis (2000)
7. Bruno, R., Conti, M., Gregori, E.: Mesh Networks: Commodity Multihop Ad Hoc Networks. IEEE Communications Magazine 43(3) (2005)

8. Estrin, D., Girod, L., Pottie, G., Srivastava, M.: Instrumenting the world with wireless sensor networks. In: International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001), Salt Lake City, Utah (2001)
9. Kwon, H., Shin, J., Lee, B., Choi, J., Nam, S., Lim, S.: Technical Trends on Mobile Ad Hoc Networks. *Electronics and Telecommunications Trends* 18, 11–24 (2003)
10. Corson, M., Macker, J.: Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC 2501 (1999)
11. Mahmoud, M., Shen, X.: Anonymous and Authenticated Routing in Multi- Hop Cellular Networks. In: IEEE International Conference on Communications, pp. 1–6 (2009)
12. Lee, Y., Lee, H., Lee, G., Kim, H., Jeong, C.: Design of hybrid authentication scheme and key distribution for mobile multi-hop relay in IEEE 802.16j. In: Euro American Conference on Telematics and Information Systems: New Opportunities to Increase Digital Citizenship, (12) (2009)
13. Huang, J., Huang, C.: Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WIMAX Networks against Rogue Base/Relay Stations. In: 2011 IEEE International Conference on Communications, pp. 1–5 (2011)
14. Zhu, X., Xu, S.: A new authentication scheme for wireless Ad Hoc Network. 2012 Information Management, Innovation Management and Industrial Engineering 2, 312–315 (2012)
15. Khalil, I., Bataineh, S., Qubajah, L., Khreishah, A.: Distributed secure routing protocol for Mobile Ad-Hoc Networks. In: 2013 Computer Science and Information Technology, pp. 106–110 (2013)
16. Kügler, D.: Man in the Middle Attacks on Bluetooth. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 149–161. Springer, Heidelberg (2003)
17. IEEE Computer Society LAN MAN Standards Committee: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report. IEEE Computer Society LAN MAN Standards Committee (1997)
18. Wi-Fi Alliance: Quality of Service (QoS) Task Group, Wi-Fi Multi-media(including WMM PowerSave) Specification v1.1 (2005)
19. Wi-Fi Alliance: Wi-Fi Protected Setup Specification, Wi-Fi Alliance Document (2007)
20. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
21. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
22. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
23. Cocks, C.: An Identity Based Encryption Scheme based on Quadratic Residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
24. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy(SP 007), pp. 321–334 (2007)

A New Representation of Photoplethysmography Signal^{*}

Dazhou Li^{**}, Hai Zhao, Sinan Li, and Huanxia Zheng

School of Information Science and Engineering, Northeastern University,
Shenyang, 110819, China
lidazhouzaku@gmail.com

Abstract. In this paper, we study the representation of photoplethysmography (PPG) signal based on a finite Gaussian basis. An iterative optimization scheme is developed for the solution of the optimal representation. When we employ a summation of n ($n < 8$) Gaussian basis to approximate the original PPG signal, we can use a feature vector only including $3n$ parameters of Gaussian basis to represent the original PPG signal, with almost no losses in geometrical shape. In contrast with a thousand samples in time domain, the proposed method can save a lot of resources in processing, transmitting and storing PPG signal in Body Area Networks (BANs).

Keywords: photoplethysmography, Gaussian basis, signal representation.

1 Introduction

PPG signal contains lots of human physiological and pathological information. Analyzing the PPG signal is an important method to diagnosis the status of human health in BANs [1]. Until now, PPG signal has been widely used for the detection of many basic physiological parameters [2], such as blood oxygen [3], heart rate, breath [4] and blood pressure [5]. Besides, it could also reflect some other important cardiovascular parameters, such as atherosclerosis [6]. The recent researches were also focused on the relationship between the PPG signal and physiological models in BANs [7]. It is widely demonstrated that PPG can provide a lot of information about the cardiovascular system and diseases, although its origins and the physiological information hidden in the different components of the PPG signal remain nowadays not fully comprehended [8].

In time domain, the original PPG pulse wave in a period is recorded as a time series comprises of almost a thousand samples with an ordinary sampling rate 1 kHz. Because each sample is not directly linked to the physiological and biochemical property, every simple PPG signal processing operation usually involves a thousand input parameters.

In BANs, many PPG processing, storing, transmission and analyzing applications really require an efficient PPG signal representation to save energy and achieve real time application. The efficiency of the PPG representation is determined by the number

* Project supported by National Science and Technology Support Program of China (No.2012BAH82F04).

** Corresponding author.

of parameters needed to accurately approximate PPG signal. Representations resulting in fewer parameters often yield superior PPG signal processing algorithms. Various signal representations may be formed by selection of different decomposition bases. A particularly interesting decomposition basis is formed by the Gaussian basis. The PPG signal representation corresponding to the Gaussian basis shall be referred to as the Gaussian basis representation. Intuitively, the main advantage of the Gaussian basis is in resulting in optimal simultaneous spatial and frequency resolutions; thus, the Gaussian basis captures abrupt spatial and frequency variations in PPG signal.

In this paper, we study the representation of PPG signal based on a finite Gaussian basis. In Section 2, an iterative optimization scheme is developed for the solution of the optimal representation. In Section 3, several simulation experiments have been used to demonstrate that the Gaussian basis results in a highly efficient method. In section 4, we illustrate Gaussian basis use in the interrogation of PPG signal in order to extract breathing and heart pulse features. Finally, in Section 5, we conclude with a summary and discussion of our results.

2 Representation of PPG Signal

2.1 Physiologic Rationale for the Derived PPG Signal Model

Considering the wave reflection phenomenon [9-11], the PPG waveform can be interpreted as the time-domain summation of a progressive wave traveling downward to the organs and body segments and some regressive waves traveling backwards to the heart form the reflection of peripheral arteries, where the differences between the progressive and regressive components are related to the vascular impedance. The systolic ejection phase of the cardiac cycle is actually a two-stage phenomenon, where the first stage comprises a rapid increase in intraventricular pressure due to the high electric myocardial excitability while the second stage is characterized by a slow decrease in intraventricular pressure due to reduction in excitation. Hence, the complete phase is marked by the presence of two systolic peaks in the PPG signal, which are transmitted to peripheral arteries of the upper extremities as the progressive waveform shape. Thus, the progressive time-domain PPG waveform could be empirically modeled as the summation of two Gaussian functions where each peak represents its respective stage.

As the regressive waves travel backward to acquisition site of the progressive PPG waveform, changes in contour due to the filtering process are reversed and it can be assumed that a very similar contour will be obtained although scaled in amplitude and lagged in time [9]. Because there is not only a reflected wave in the acquisition site of the progressive PPG waveform, the regressive component of the traveling wave was also modeled by the summation of reasonable quantities of Gaussian functions.

Based on the above hypothesis the time-sampled PPG waveform at a fixed arterial site is then represented by summation of the progressive and regressive time-domain pulse waveforms. Since both progressive and regressive time-domain pulse waveforms can be decomposed into a number of Gaussian functions, the PPG signal can be represented by the summation of a certain number of Gaussian functions. An example of an original PPG signal of forefinger for healthy subject aged 30 and the corresponding Gaussian basis representation are depicted in Figs. 1.

2.2 Method of Gaussian Basis Representation

In this paper, we call

$$G(t) = a \cdot e^{-\left(\frac{t-b}{c}\right)^2} \quad (1)$$

a Gaussian basis, where a stands for the amplitude of the each Gaussian pulse waveform, b indicates the location of the Gaussian wave peaks and c indicates the width or ‘duration’ of the Gaussian pulse waveform. In the following section we propose a scheme for the representation of PPG signal based on a finite Gaussian basis.

Let us consider a PPG signal $p(t)$. The finite Gaussian basis $G_i(t)$, for $i = 1, 2, \dots, n$, is defined by

$$G_i(t) = a_i \cdot e^{-\left(\frac{t-b_i}{c_i}\right)^2}, \quad (2)$$

for $i = 1, 2, \dots, n$. Let \mathbf{L} denote the Gaussian basis parameters given by

$$\mathbf{L} = \{(a_i, b_i, c_i), i = 1, 2, \dots, n\}. \quad (3)$$

Finally, the approximation signal $p'(t)$ is defined by

$$p'(t) = \sum_{i=1}^n a_i \cdot e^{-\left(\frac{t-b_i}{c_i}\right)^2}. \quad (4)$$

Observe that the choice of the finite Gaussian basis will be critical in minimizing the approximation error. In the following section we develop a procedure to determine the optimal choice of the finite Gaussian basis.

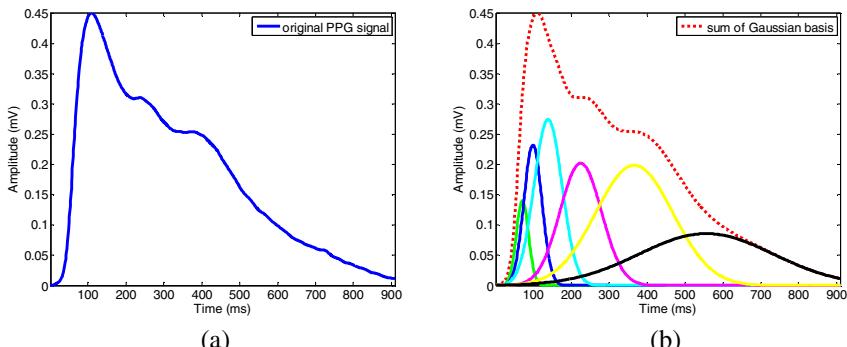


Fig. 1. (a) The original PPG signal of forefinger for healthy subject aged 30; (b) the collection of n Gaussian basis ($n=6$) and the signal formed by the summation of the Gaussian basis

2.3 Optimal Gaussian Basis

Let us denote a collection of N samples of the original PPG signal $p(t)$ by $\mathbf{P} = \{p(t_k), k=1, 2, \dots, N\}$. The optimal Gaussian basis representation is obtained by minimizing the sum of the squared error between samples of the original PPG signal $p(t)$ and the approximation PPG signal $p'(t)$ with respect to the Gaussian basis parameters;

$$R = \arg \min_{\mathbf{L}} \left\{ \sum_{k=1}^{k=N} [p(t_k) - p'(t_k)]^2 \right\}. \quad (5)$$

The solution of Eq.(5) may be derived by solving the system of nonlinear equations obtained by setting $\partial R / \partial \mathbf{L}_i = 0$, for $i = 1, 2, \dots, 3n$, for the unknown Gaussian basis parameters \mathbf{L} . The steepest-descent method [12] is a commonly used approach to the solution of nonlinear minimization problems. The method relies on an iterative procedure and updates the Gaussian basis parameters \mathbf{L} by

$$\nabla \mathbf{R} = -\left\{ \frac{\partial R}{\partial \mathbf{L}_i} \right\}, \quad i = 1, 2, \dots, 3n. \quad (6)$$

The steepest-descent method guarantees convergence, yet it is very slow [13].

An alternative approach is obtained by the modified Gauss-Newton method [14-15]. This method relies on an iterative procedure where a linearization of the approximation signal is obtained from the Taylor expansion; i.e.,

$$\hat{\mathbf{P}}_{\alpha+\beta} = \hat{\mathbf{P}}_\alpha + \mathbf{S}\beta, \quad (7)$$

$$\hat{\mathbf{P}}_\alpha = \{p'(t_k), \quad k = 1, 2, \dots, N\}, \quad (8)$$

$$\mathbf{S} = \left\{ \frac{\partial p'(t_k)}{\partial L_i}, \quad k = 1, 2, \dots, N, \quad i = 1, 2, \dots, 3n \right\}. \quad (9)$$

The Gaussian basis parameters \mathbf{L} are updated by

$$\beta = \{\beta_i, \quad i = 1, 2, \dots, 3n\}. \quad (10)$$

Eq. (5) is now a linear least-squares estimation problem. Setting $\partial R / \partial \beta_i = 0$, for $i = 1, 2, \dots, 3n$, we have

$$\mathbf{A}\beta = \mathbf{B}, \quad (11)$$

$$\mathbf{A} = \mathbf{S}^T \mathbf{S}, \quad (12)$$

$$\mathbf{B} = \mathbf{S}^T (\mathbf{P} - \hat{\mathbf{P}}_\alpha), \quad (13)$$

where \mathbf{T} is the matrix transpose operation.

Finally, the Gaussian basis parameters \mathbf{L} are updated by

$$\gamma = |\beta| \cdot \nabla \mathbf{R} . \quad (14)$$

Thus, the Gaussian basis parameters are updated in the direction determined by the steepest-descent method, and the size determined by the modified Gauss-Newton method.

3 Experimental Results

3.1 Data Acquisition System

A system for continuous acquisition of the PPG waveform was developed and validated previously [16, 17]. The PPG waveforms were acquired by using a photoelectric transducer (HKG-07) connected to a preamplifier with a second order band pass between the characteristic frequencies 1.54Hz and 2.34Hz (-3dB points 1.0 and 3.5Hz). Radial PPG pulse waveform signals were acquired by a 16 bit, 16 single channels, acquisition model USB-6210 (National Instruments, USA).

3.2 The Goodness of Fit

To evaluate the goodness of fit in Gaussian basis representation, we introduce two indexes, Sum of Squares Due to Error (*SSE*) and *R-square* [18].

The first statistic measures the total deviation of the response values from the fit to the response values. A value closer to 0 indicates that the model has a smaller random error component, and that the fit will be more useful for prediction.

$$SSE = \sum_{k=1}^{k=N} [p(t_k) - p'(t_k)]^2 \quad (15)$$

Put another way, *R-square* is the square of the correlation between the response values and the predicted response values. It is also called the square of the multiple correlation coefficients and the coefficient of multiple determinations. *R-square* is defined as the ratio of the sum of squares of the regression (*SSR*) and the total sum of squares (*SST*). *SSR* is defined as

$$SSR = \sum_{k=1}^{k=N} [p'(t_k) - \bar{p}(t_k)]^2 . \quad (16)$$

SST is also called the sum of squares about the mean, and is defined as

$$SST = \sum_{k=1}^{k=N} [p(t_k) - \bar{p}(t_k)]^2 , \quad (17)$$

where $SST = SSR + SSE$. Given these definitions, *R-square* is expressed as

$$R_square = SSR/SST . \quad (18)$$

R-square can take on any value between 0 and 1, with a value closer to 1 indicating that a greater proportion of variance is accounted for by the model.

3.3 Test Result and Analysis

Sixteen subjects were investigated in the study, including ten men and six women with the age between 25 and 30.

In the first session, we select a PPG pulse wave in a period from a male subject, as shown in Fig. 1(a), and we use different number of Gaussian basis to approximate the selected PPG pulse wave. Figs. 2 illustrate the results of *SSE* and *R-square* with the increment of the number of Gaussian basis. It is found that a value, $n = 6$, for the number of Gaussian basis is suitable to represent the selected PPG pulse wave. When $n < 6$, we can get the result $SSE < 0.001795$ and $R\text{-square} > 0.9997$. This shows all the information in the PPG signal can be preserved intact.

In the second session, we analyze 698 PPG pulse waves from the same male subject in the first session. Figs. 3 present the statistics of *SSE* and *R-square* for the variation of the number of Gaussian basis, when we use the different number of Gaussian basis to fit the 698 PPG pulse waves. As clearly observed, the mean of *SSE* and *R-square* both follow the trends in Figs. 2, respectively. Moreover, the variances of *SSE* and *R-square* both decrease with the number of Gaussian basis. As illustrated in Figs. 3, $n = 6$ and $n = 7$ are both reasonable choices, when we adopt the summation of a certain number of Gaussian functions to represent PPG signal.

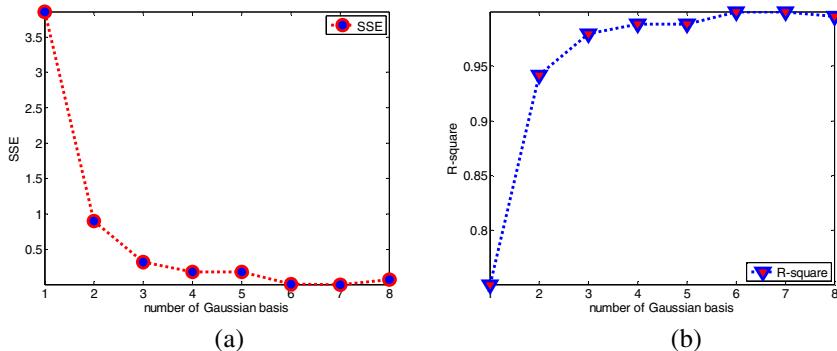


Fig. 2. The goodness of fit for one PPG pulse wave from the male subject

In the third session, we record the PPG signal from every subject in ten minutes. Since there are sixteen subjects in our study, a total of 12714 PPG pulse waves have been processed. Each of the pulse waves is represented by six Gaussian basis, which has proved to be a reasonable choice in the first and second section. In Figs. 4, we present the mean values of *SSE* and *R-square* for every subject, when we employ six Gaussian basis. As illustrated in Figs. 4, the goodness of fit varies with different subjects, all the mean values of *SSE* are less than 0.5 and all the mean values of *R-square* are greater than 0.999. We can see that the methods provided in the paper are satisfactory for different subjects.

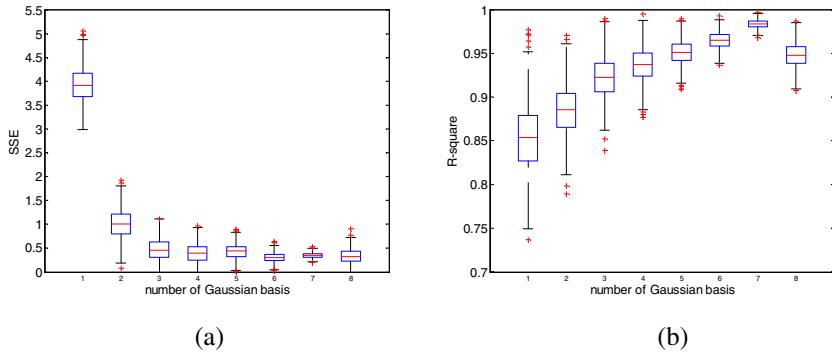


Fig. 3. The goodness of fit for 698 PPG pulse waves from the male subject

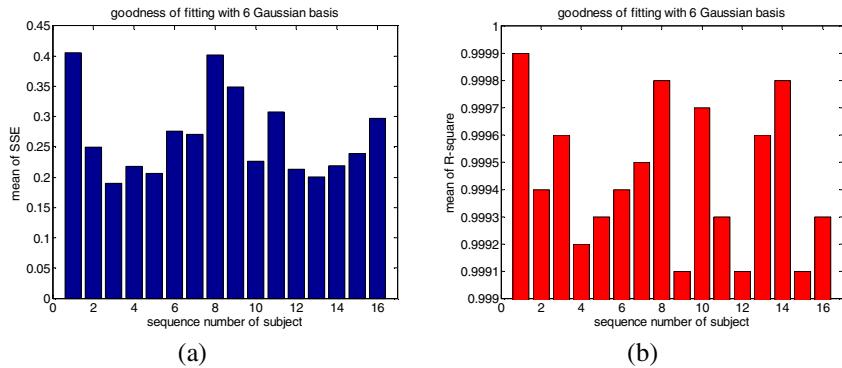


Fig. 4. The goodness of fit for 12714 PPG pulse waves from sixteen subjects

4 Application

After having extracted all Gaussian basis, they can be analyzed further by applying the Hilbert Transform (HT) or processing them in any other suitable way. The combination of Gaussian decomposition of a PPG signal into its Gaussian basis plus residue and a subsequent Hilbert spectral analysis to extract instantaneous frequencies and phases is discussed in the section. The Hilbert transform calculates the conjugate pair of Gaussian basis $G_i(t)$ via

$$H\{G_i(t)\} = \frac{1}{\pi} PV \int_{-\infty}^{\infty} \frac{G_i(\tau)}{t - \tau} d\tau \quad (19)$$

where PV indicates the Cauchy principal value. This way an analytical signal $g_i(t)$ can be defined via

$$g_i(t) = G_i(t) + j \cdot H\{G_i(t)\} = V_i(t) \cdot e^{j\theta_i(t)} \quad (20)$$

with amplitude $V_i(t)$ and instantaneous phase $\theta_i(t)$ given by

$$V_i(t) = \sqrt{\{G_i(t)\}^2 + \{H\{G_i(t)\}\}^2} \quad (21)$$

$$\theta_i(t) = \arctan\left(\frac{H\{G_i(t)\}}{G_i(t)}\right). \quad (22)$$

Each Gaussian basis can now be expressed as

$$G_i(t) = \operatorname{Re}[V_i(t) \cdot e^{j\theta_i(t)}]. \quad (23)$$

PPG signal $p(t)$ can then be expressed as

$$p(t) = \sum_{i=1}^n \operatorname{Re}[V_i(t) \cdot e^{j\theta_i(t)}] + r(t). \quad (24)$$

A Gaussian basis expansion thus provides a generalized Fourier expansion. Note that because

$$\theta_i(t) = \arg(g_i(t)) = \int_{-\infty}^t \omega_i(\tau) d\tau = \int_0^t \omega_i(\tau) d\tau + \theta_i(0) \quad (25)$$

An instantaneous frequency $f_i(t)$ can be obtained as

$$f_i(t) = \frac{1}{2\pi} \cdot \omega_i(t) = \frac{1}{2\pi} \cdot \frac{d\theta_i(t)}{dt}. \quad (26)$$

According to the preceding procedure, an example of a ridge detection method used on a real PPG signal to detect subject breathing rate and heart rate from the ridge associated with subject PPG signal is shown in Fig. 5.

Fig. 5 contains a PPG signal with its associated spectrum plot according to Eq. (19-26). The spectrum in Fig. 5b is plotted in 3-D. Two dominant bands appear in the spectrum: the pulse band and a band associated with subject breathing. These are

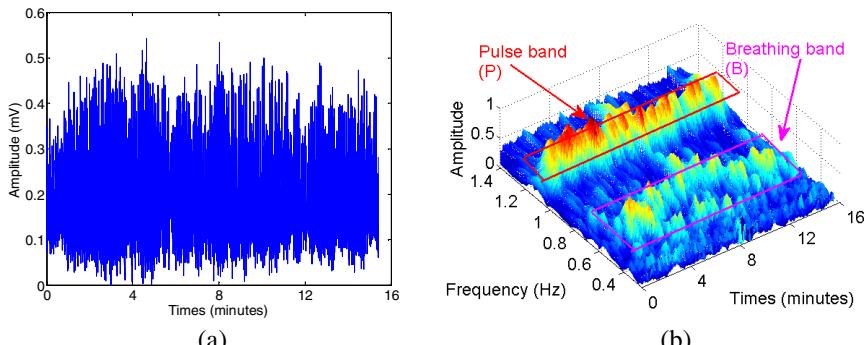


Fig. 5. PPG signal (a) and associated spectrum plot (b) showing respiratory tracing (breathing band) and heart pulse tracing (pulse band)

marked P and B respectively in the plot. In this example we are concerned with the detection the breathing and heart pulse through time and hence here the breathing band and pulse band are the primary bands. The pulse band appears at just over 1.2 Hz, or 72 beats per minute, and the breathing band appears at 0.5~0.6 Hz.

The heart rate derived from our system was compared with that obtained by the ECG monitor. Fig. 6a shows a typical example of dynamic variation in heart rate at rest, and during and after exercise. During the first 4 min. subjects were allowed to rest in a sitting position, and exercise was then performed for 9 min. After exercise, the subject rested, sitting on the bicycle for the remaining 7 min. Heart rates obtained from PPG agreed well with those obtained by ECG at rest and during exercise in this subject. The maximum error of heart rate was 7 beats per minute.

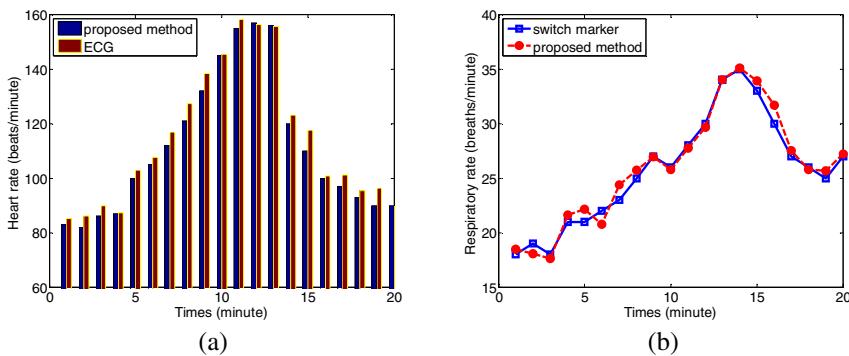


Fig. 6. Comparison of heart rate (a) and respiratory rate (b)

To verify the accuracy of respiratory rate derived from our method, a respiration marker signal was recorded by an observer monitoring the subject's chest movements and activating a small pushbutton switch in synchronization with inspiration (switch depressed) and expiration (switch released). The switch marker signals were processed to derive a manual respiratory rate. The results from the full analysis are presented in Fig. 6b, an average difference of less than 1 breath per minute.

5 Conclusion

In this paper, we studied the representation of PPG signals based on a finite Gaussian basis. Several simulation experiments have been used to demonstrate that the Gaussian decomposition results in a highly efficient method for the representation of PPG signals. We envision the future use of this method for feature extraction, attribute classification and sample clustering in biomedical signal processing field.

Acknowledgments. This work was supported in part by the National Key Technology R&D Program Nos. 2012BAH82F04.

References

- [1] Chen, W., Lei, S., Guo, L., Chen, Y., Pan, M.: Study on conditioning and feature extraction algorithm of photoplethysmography signal for physiological parameters detection. In: Proceedings of the Image and Signal Processing, Shanghai, China, October 15-17 (2011)
- [2] Allen, J.: Photoplethysmography and its application in clinical physiological measurement. *Physiological Measurement* 28(3), 1–39 (2007)
- [3] Kyriacou, P.A., Powell, S., Langford, R.M., Jones, D.P.: Investigation of oesophageal photoplethysmographic signals and blood oxygen saturation measurements in cardiothoracic surgery patients. *Physiological Measurement* 23(8), 533–545 (2002)
- [4] Johansson: Neural network for photoplethysmographic respiratory rate monitoring. *Medical & Biological Engineering & Computing* 41(5), 242–248 (2003)
- [5] Binns, S.H., Sisson, D.D., Buoscio, D.A., Schaeffer, D.J.: Doppler Ultrasonographic, Oscillometric Sphygmomanometric, and Photoplethysmographic Techniques for Noninvasive Blood-Pressure Measurement in Anesthetized Cats. *Journal of Veterinary Internal Medicine* 9(6), 405–414 (1995)
- [6] Usman, S.B., Ali, M.A.B., Reaz, M.M.B., Chellapan, K.: Second Derivative of Photoplethysmogram in Estimating Vascular Aging among Diabetic Patients. In: International Conference for Technical Postgraduates, Kuala Lumpur, Malaysia, December 14-15 (2009)
- [7] Aldrich, T.K., Moosikasuwon, M., Shah, S.D., Deshpande, K.S.: Length-Normalized Pulse Photoplethysmography: A Noninvasive Method to Measure Blood Hemoglobin, vol. 30(10), pp. 1291–1298 (2002)
- [8] Ando, J., Kawarada, A., Shibata, M., Yamakoshi, K., Kamiya, A.: Pressure-volume relationships of finger arteries in healthy subjects and patients with coronary atherosclerosis measured noninvasively by photoelectric plethysmography. *Japanese Circulation Journal* 55(6), 567–575 (1991)
- [9] Quick, C.M., Berger, D.S., Noordergraaf, A.: Constructive and destructive addition of forward and reflected arterial pulse waves. *Am. J. Physiol. Heart Circ. Physiol.* 280(4), 1519–1527 (2001)
- [10] Kelly, R., Hayward, C., Avolio, A., O'Rourke, M.: Noninvasive determination of age-related changes in the human arterial pulse. *Circulation* 80, 1652–1659 (1989)
- [11] Chadwick, R.S., Goldstein, D.S., Keiser, H.R.: Pulse wave model of brachial arterial pressure modulation in aging and hypertension. *Am. J. Physiol. Heart Circ. Physiol.* 251(1), 1519–1527 (1986)
- [12] Fliege, J., Svaiter, B.F.: Steepest descent methods for multicriteria optimization. *Mathematical Methods of Operations Research* 51(3), 479–494 (2000)
- [13] Westwick, D., Kearney, R.E.: Separable Least Squares Identification of Nonlinear Hammerstein Models: Application to Stretch Reflex Dynamics. *Annals of Biomedical Engineering* 29(8), 707–718 (2001)
- [14] Osborne, M.R.: Separable least squares, variable projection, and the Gauss-Newton algorithm. *ETNA. Electronic Transactions on Numerical Analysis* 28(1), 1–15 (2007)

- [15] Yuanjin, Z., Tay, D.B.H., Lemin, L.: Signal extraction and power spectrum estimation using wavelet transform scale space filtering and Bayes shrinkage. *Signal Processing* 80(8), 1535–1549 (2000)
- [16] Zhao, H., Peng, H., Zhu, J., Li, X.: A New Method of Measuring Blood Pressure Indirectly. *Journal of Northeastern University (Natural Science)* 33(2), 191–194 (2012)
- [17] Xu, J., Zhao, H., Sun, P., Yin, Z.: R&D of a Pulse Oximeter Based on WPAN. *Journal of Northeastern University (Natural Science)* 27(7), 747–750 (2006)
- [18] Toutenburg, H., Shalabh: Prediction of response values in linear regression models from replicated experiments. *Statistical Papers* 43(3), 423–433 (2002)

Energy Efficient Social-Based Routing for Delay Tolerant Networks

Chenfei Tian¹, Fan Li^{1,*}, Libo Jiang¹, Zeye Wang¹, and Yu Wang^{2,**}

¹ School of Computer Science, Beijing Institute of Technology, Beijing, 100081, China

² Department of Computer Science, University of North Carolina at Charlotte,
Charlotte, NC 28223, USA

Abstract. Delay Tolerant Network (DTN) is one kind of emerging networks characterized by long delay and intermittent connectivity. Traditional ad hoc routing protocols are inapplicable or perform poorly in DTNs because nodes are seldom fully connected. In recent years, many routing protocols (especially social-based routing) are proposed to improve the delivery ratio in DTNs, but most of them do not consider the load of nodes thus may lead to unbalanced energy consumption among nodes. In this paper, we propose an *Energy Efficient Social-based Routing* (EESR) protocol to reduce the load of nodes while maintaining the delivery ratio within an acceptable range by limiting the chances of forwarding in traditional social-based routing. Furthermore, we also propose an improved version of EESR to dynamically adjust the controlling parameter. Simulation results on real-life DTN traces demonstrate the efficiency of our proposed algorithms.

Keywords: Energy Efficient, Load Balancing, Social-based Routing, Delay Tolerant Networks.

1 Introduction

In delay tolerant networks (DTNs), the end-to-end path does not exist all the time from the current node to the destination node. Thus, routing in DTNs becomes very challenging compared with traditional wireless networks [14]. In recent years, many DTN routing protocols [13, 18] are proposed to leverage the node mobility for packet delivery.

The simplest DTN routing protocol is Epidemic [17], in which whenever a node carrying a message encounters with another node, it copies a replica of the message and forwards the replica to the encountered node. However, such

* Corresponding author.

The work of F. Li is partially supported by the National Natural Science Foundation of China under Grant No. 61370192 and 60903151, and the Beijing Natural Science Foundation under Grant No. 4122070.

** The work of Y. Wang is supported in part by the US National Science Foundation under Grant No. CNS-1050398, CNS-1319915, and CNS-1343355.

flooding-based solution also causes relatively high network overhead. To overcome the shortage of Epidemic routing, many DTN routing protocols limit the number of replicas, such as Spray and Wait [16]. Generally, the delivery ratio of flooding-based strategies is relevant high, but the heavy load of nodes may cause serious congestions in DTNs.

Most of the existing routing protocols adopt “store-carry-forward”, where if there is no connection available, the current node stores and carries the message, and then makes a decision whether to forward the message when it encounters another node. For example, PRoPHET [11] predicts the delivery probability in the future network based on historical contacts, and then decides whether to forward the message. Fresh [3] forwards packets to the encountered node if it meets the destination node more recently than the current node does. Greedy-Total [4] forwards messages to the encountered node if it has a higher contact frequency to all other nodes than v_i does.

To further improve the prediction of future encounters, many social-based routing protocols [12, 18] are proposed. More and more mobile devices in DTNs are used and carried by human beings, so the behaviors of the networks can be better characterized by their social attributes. SimBet [2] is a representative routing protocol for such social-based DTNs. When current node encounters another node, the message is more likely to be forwarded to the node with higher social centrality and more similar with the destination node. Label [7] and Group [10] try to forward the message to the node whose group is the same with the destination node. Bubble Rap [8] forwards the message includes two phases: a bubble-up phase based on global centrality and a bubble-up phase based on local centrality.

All of the above routing protocols focus on improving the delivery ratio without considering the battery usages of the mobile nodes, which could significantly affect the life-time of mobile devices. In this paper, we propose an *Energy Efficient Social-based Routing* (EESR) protocol which aims to reduce the load of nodes in social-based routing by limiting the chances of forwarding at each encounters. We also propose an improved version of EESR (EESR-I) to dynamically adjust the controlling parameter so that the delivery ratio can still be at certain level. The performance of our proposed methods are evaluated through simulations over real-life data traces and compared with other existing social-based routing protocols.

The rest of this paper is organized as follows: Section 2 reviews existing social-based routing methods for DTNs. Section 3 presents the detailed design of the proposed EESR and EESR-I. Section 4 describes simulation results and Section 5 concludes the paper.

2 Related Works

In the previous studies, many routing protocols have been proposed for DTNs. They can be roughly divided into two categories: store-carry-forward strategy and flooding based strategy [13]. For the store-carry-forward strategy, the current

node stores and carries the message, and makes a forwarding decision when encounters another node. For the flooding based strategy, there will be multiple copies of each message in the whole network, such as Epidemic [17]. Though the delivery ratio of flooding-based method is usually high, the multi-copy strategy may greatly increase the loads of nodes and cause serious congestions in DTNs. Since in this paper, we will focus on social-based DTN routing methods, in this section, we briefly review the existing social-based routing methods.

Recently, social-based routing has attracted a lot of attention since most mobile devices (such as smart phones) are now used and carried by people, and the network behaviors can be better characterized by their social attributes. Social-based routing methods aim to carefully choose the relay nodes by choosing a good *social metric* to measure the capability of nodes to deliver the message to the destination. During any encounter, if the encountered node has higher social metric than the current node, the current node will forward its message copy to the encountered node. For example, SimBet [2] uses betweenness centrality and the similarity with destination node as the social metric. Bubble Rap [8] uses global centrality and local centrality to decide whether to forward the message. Gao et al. [5] also utilizes centrality (defined by a cumulative contact probability) and community as the social metrics to design social-based multicast routing protocols. Friendship [1] defines its friendship community as the set of nodes having close friendship (defined by using contact probability) with itself either directly or indirectly. SEBAR [9] introduces social energy (generated by the encounters and shared by communities) to quantify the social ability of forwarding messages to other nodes, which consists of two parts: the reserved energy generated by itself from direct node encounters with other nodes and the reallocated energy gained from its communities.

In this paper, we are committed to reduce the load of nodes in social-based DTNs. It is well-known that the energy of mobile devices is very precious due to the limited capacity of battery. When some nodes run out of energy, it may have a great impact on the performance of the network, especially for sparse networks such as DTNs. Existing social-based routing methods usually choose a node with higher social metric to be the next relay, and they do not consider the energy consumption. In order to save node energy in social-based DTNs, we aim to minimize the number of forwards for message transmission while maintaining acceptable delivery ratio.

3 Energy Efficient Social-Based Routing

In this section, we introduce our proposed *energy efficient social-based routing* (EESR) protocol for DTNs. The aim of EESR is to save the energy consumption by limiting the number of message forwarding. Recall that the message will not be forwarded to the encountered node unless the current node has lower *social metric* than the encountered node. Here, *social metric* (\mathcal{SM}) could be any existing social metrics, such as centrality and similarity in SimBet [2], friendship in Friendship [1], and social energy in SEBAR [9]. The proposed EESR is a

general scheme to reduce the load of each node, and it can be applied to any existing social based routing methods as long as they use social metric per node for relay selection and forwarding decision.

To calculate the social metric value of a node, a social graph is needed to describe the social relationships among nodes. Usually such a social graph is generated from historical contacts [6]. Assume that $V = \{v_1, v_2, \dots, v_n\}$ is the set of nodes in the DTN. Each node can send and receive messages when it encounters another node (the physical distance between them is less than the transmission range of their radios). To generate the social graph, we set a threshold on contact frequency to judge whether there is a close relationship between two nodes in the network. If the number of contact times between two nodes is larger than or equal to the threshold, there is an edge between these two nodes in the generated social graph. The generated social graph contains all nodes and their relations. Given this graph, a variety of social metrics can be calculated and used by our routing algorithms. We use $\mathcal{SM}(v_i)$ to denote the social metric of node v_i .

3.1 EESR: Basic Version

In traditional social-based routing protocols, the messages are forwarded to the encountered nodes with larger social metrics. This may help to achieve higher delivery ratios, but nodes with large social metric values may run out of battery soon due to their heavy load. Therefore, we consider to improve the traditional social-based routing methods by enlarging the social metric of current node v_i to amp_ratio times of the original value. Here, $amp_ratio \geq 1$. Thus, it becomes more difficult for the current node to transfer its message because the encountering node needs to have amp_ratio times higher social metric than that of current node to be chosen as a relay. By doing so, the number of forwarding in the network will be reduced. Naturally, the delivery ratio of the new method decreases, thus we dynamically adjust the amplification ratio amp_ratio according to the *Time to Live* (TTL) of the packet to avoid low delivery ratio. TTL of the packet indicates whether the packet is out-of-dated and when should be discarded. At the beginning, the TTL value of a message is set to a constant TTL_0 . After each hop, the value of TTL will minus one. When TTL is reduced to zero, the message will be discarded.

In EESR, the forwarding happens only when the social metric of the encountered node is amp_ratio times larger than that of the current node. The basic idea of dynamically adjusting amp_ratio is as follows. At the beginning, when TTL is large, EESR puts minimizing the load of nodes as its first priority, thus the value of amp_ratio is set high. However, after several hops, when TTL is reduced to a small value, which means the packet will be discarded soon, EESR puts improving the delivery ratio as its first priority, so the value of amp_ratio should be set small. Therefore, we set

$$amp_ratio = 1 + \frac{ttl}{TTL_0} \cdot \theta,$$

where θ is a predefined constant used to determine the initial value of amp_ratio , and TTL_0 and ttl are the initial TTL value and the current TTL value of the

Algorithm 1. EESR: Energy Efficient Social-based Routing

Node v_i with message M meets v_j which does not hold M .

```

1: if  $v_j$  is the destination then
2:    $v_i$  forwards  $M$  to  $v_j$ 
3: else
4:    $amp\_ratio \leftarrow 1 + \frac{ttl}{TTL_0} \cdot \theta$ 
5:   if  $\mathcal{SM}(v_i) \cdot amp\_ratio \leq \mathcal{SM}(v_j)$  then
6:      $v_i$  forwards  $M$  to  $v_j$ 
7:      $ttl \leftarrow ttl - 1$ 
8:   else
9:      $v_i$  holds the  $M$  and waits for the next encounter
10:  end if
11: end if

```

message, respectively. Note that EESR regresses to the traditional social based routing when $amp_ratio = 1$. Algorithm 1 shows the detailed description of EESR.

Compared with traditional social-based routing methods, EESR aims to reduce the load of nodes. We illustrate an example in Figure 1, which shows the connectivity among nodes from $T = 0$ to 3. The number inside each node represents its \mathcal{SM} value. Assume that node v_1 has a message destined to v_5 . The message will go through v_2 , v_3 , v_4 and reach v_5 eventually by traditional social-based routing. Thus the loads of each node are 1, 2, 2, 2, and 1 respectively. Here, we assume that every time when a message is forwarded from one node to another node, the load of both involving nodes will plus one. In this example, the increase ratio $\theta = 0.5$ and $TTL_0 = 5$. In EESR, v_1 will not forward the message to v_2 at $T = 0$ because $\mathcal{SM}(v_2)$ is not 1.5 times larger than or equal $\mathcal{SM}(v_1)$. The message will be forwarded from v_1 to v_3 at $T = 1$ because $\mathcal{SM}(v_3)$ is 1.5 times larger than $\mathcal{SM}(v_1)$. At $T = 2$, the message will be forwarded to v_4 because $\mathcal{SM}(v_4)$ is 1.4 times larger than $\mathcal{SM}(v_3)$. Here, $amp_ratio = 1 + \frac{4}{5} \times 0.5 = 1.4$. At $T = 3$, the message will be forwarded to the destination node v_5 . Therefore, the packet will go through v_3 , v_4 and reach v_5 with EESR. The loads of each node are 1, 0, 2, 2, and 1 respectively. Overall, the load of v_2 is reduced in this example by EESR. Our simulation results in Section 4 confirm that EESR can reduce the loads of nodes in DTNs.

3.2 EESR-I: Improved Version

If the \mathcal{SM} value of source node is very large, it might be difficult to find a node whose \mathcal{SM} value is amp_ratio times larger than itself except for the destination node. This phenomena could have a great impact on delivery ratio. To prevent it from happening, we design an additional mechanism to further dynamically adjust amp_ratio based on past encounters. When a node encounters more than K nodes whose \mathcal{SM} values are larger than itself, but still does not forward the message (since the \mathcal{SM} values of the encountered nodes are not greater enough

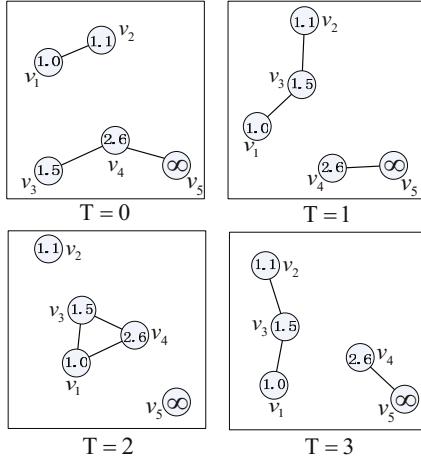


Fig. 1. An example of EESR

than amp_ratio times of the current node), then our method slowly relaxes the forwarding condition by gradually decreasing the value of amp_ratio . In this improved version (denoted by EESR-I), the amplification ratio amp_ratio is dynamically adjusted by: both (1) TTL of the packet and (2) the number of encounter nodes (i.e., $node_counter$ in Algorithm 2) whose \mathcal{SM} values are larger than that of the current node but smaller than amp_ratio times of that. Here, K is the pre-defined threshold for $node_counter$. Algorithm 2 shows the detailed method.

4 Simulations

We have conducted extensive simulation experiments over real-life wireless DTN traces to evaluate our proposed EESR and EESR-I. In our simulations, we use the SimBet utility value [2] as our \mathcal{SM} value per node. Recall that in SimBet routing [2], the message is more likely to be forwarded to the node with high social centrality and more similar with the destination node. The SimBet utility value basically is a weighted value of the centrality and the similarity with the destination node. We compare EESR and EESR-I with the following existing routing methods.

- **Epidemic** [17]: during any encountering, the node copies a replica of the packet and forwards it to any encountered nodes.
- **SimBet** [2]: the packet is only forwarded from node v_i to node v_j if the SimBet utility of node v_j is larger than that of node v_i .
- **FRESH** [3]: the packet is only forwarded from node v_i to node v_j if v_j has met the destination more recently than v_i does.

Algorithm 2. EESR-I: Improved EESR

Node v_i with message M meets v_j which does not hold M .

```

1: if  $v_j$  is the destination then
2:    $v_i$  forwards  $M$  to  $v_j$ 
3: else
4:   if  $\mathcal{SM}(v_i) < \mathcal{SM}(v_j)$  then
5:     node_counter  $\leftarrow$  node_counter + 1
6:     if node_counter  $\geq K$  then
7:       amp_ratio  $\leftarrow 1 + \frac{ttl}{TTL_0} \cdot \theta \cdot \frac{1}{node\_counter - K + 1}$ 
8:     else
9:       amp_ratio  $\leftarrow 1 + \frac{ttl}{TTL_0} \cdot \theta$ 
10:    end if
11:   end if
12:   if  $\mathcal{SM}(v_i) \cdot amp\_ratio \leq \mathcal{SM}(v_j)$  then
13:      $v_i$  forwards  $Msg$  to  $v_j$ 
14:     ttl  $\leftarrow$  ttl - 1
15:     node_counter  $\leftarrow 0$ 
16:   else
17:     node  $v_i$  holds the  $Msg$  and waits for the next encounter
18:   end if
19: end if

```

- **Greedy-Total [4]:** the packet is only forwarded from v_i to v_j if v_j has a higher contact frequency to all other nodes than v_i does.

In all experiments, we compare the performance of each routing method using the following routing metrics.

- *Delivery Ratio:* the average percentage of the successfully delivered packets from the sources to the destinations.
- *Maximum Load:* the largest load of all nodes within a certain period of time.
- *Average Load:* the average load of all nodes within a certain period of time.
- *Average Hops:* the average number of hops during each successful delivery from the sources to the destinations.
- *Average Forwards:* the average number of forwarding times during each delivery (not only limit to successful delivery) from the source to the destination.
- *Average Delay:* the average duration of successfully delivered packets from the sources to the destinations.

We choose InfoCom 2006 trace data [15] to simulate the mobile DTN environment. This trace data includes connections among 78 mobile iMote Bluetooth nodes carried by participants of a student workshop for four days during InfoCom 2006 in Barcelona, Spain. Each record in the data set contains information about the ID of the device who recorded the sightings and the device who was seen. It also contains the starting time and the ending time for a certain contact. The contact information from the first 62 hours is treated as historical data to generate the social graph, then the performance of routing tasks are evaluated

Table 1. Parameters used for EESR and EESR-I

Parameter	Value or Type
Social metric \mathcal{SM}	SimBet Utility
Number of selected nodes	78
Number of routing tasks	6006
Initial value of TTL (TTL_0)	5
Increase ratio θ	0.5
K (Only for EESR-I)	2

over the remaining 30 hours. Each node tries to send a packet to all other nodes. Therefore, we have $78 \times 77 = 6006$ source-destination pairs and routing tasks. Here, we consider single-copy version of all routing methods, where only one copy is allowed within the network for any messages. To generate the social graph, we add an edge between two nodes if their total contact times is greater than one, which is the same as the setting in SimBet. Table 1 summarizes all parameters used in EESR and EESR-I.

4.1 Simulation Results of EESR

Figure 2 demonstrates the performance comparison among EESR and other four existing routing methods. As Figure 2(a) shows, Epidemic has the highest delivery ratio because it offers the upper bound of the delivery ratio that any routing protocol can achieve. The delivery ratio of EESR is not very high, since EESR aims to save the energy by reducing the opportunity of message forwarding. If the \mathcal{SM} value of the source node is large, it will be difficult to find an encountering node whose \mathcal{SM} value is amp_ratio times higher than that of the source node. But EESR has outstanding performance in terms of the maximum and average loads as shown in Figure 2(b) and (c). Note that these two subfigures do not include the results of Epidemic because its maximum load is usually higher than 14,000 and its average load is usually higher than 4,000. Figure 2(e) and (f) indicate that average hops and average forwards of EESR are the smallest among all the methods.

4.2 Simulation Results of EESR-I

We then test the performance of improved version (EESR-I). Figure 3 show the detailed results. Interestingly, EESR-I has very close, even slightly better delivery ratio than that of SimBet, and its average delay is at the similar level with that of SimBet. Although the maximum and average loads of EESR-I increase over time, the load of EESR-I is still much lower than other algorithms. EESR-I still maintains the smallest numbers of hops and forwards. Compared with EESR, the improved version has similar delivery ratio with the original social based routing method while reducing the overall load, number of hops and forwards. The standard deviation of the load for different routing methods are reported

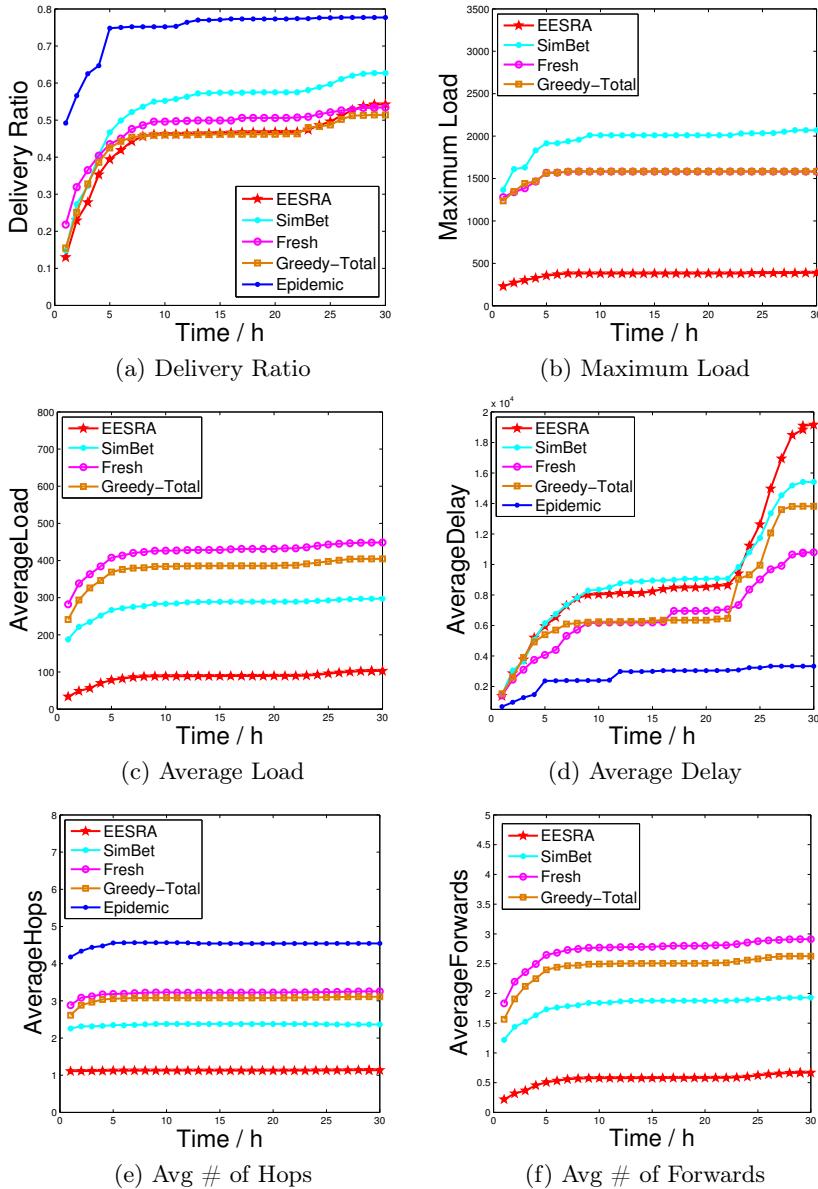


Fig. 2. Simulation Results of EESR over InfoCom 2006 trace data

in Table 2, which demonstrates that our proposed EESR and EESR-I can also limit the variation range of the load. Overall, EESR and EESR-I can reduce the energy consumption while maintaining the similar or even better delivery ratio with the original social based routing. By carefully selecting the parameters, EESR-I can find a balance between load reduction and high delivery ratio.

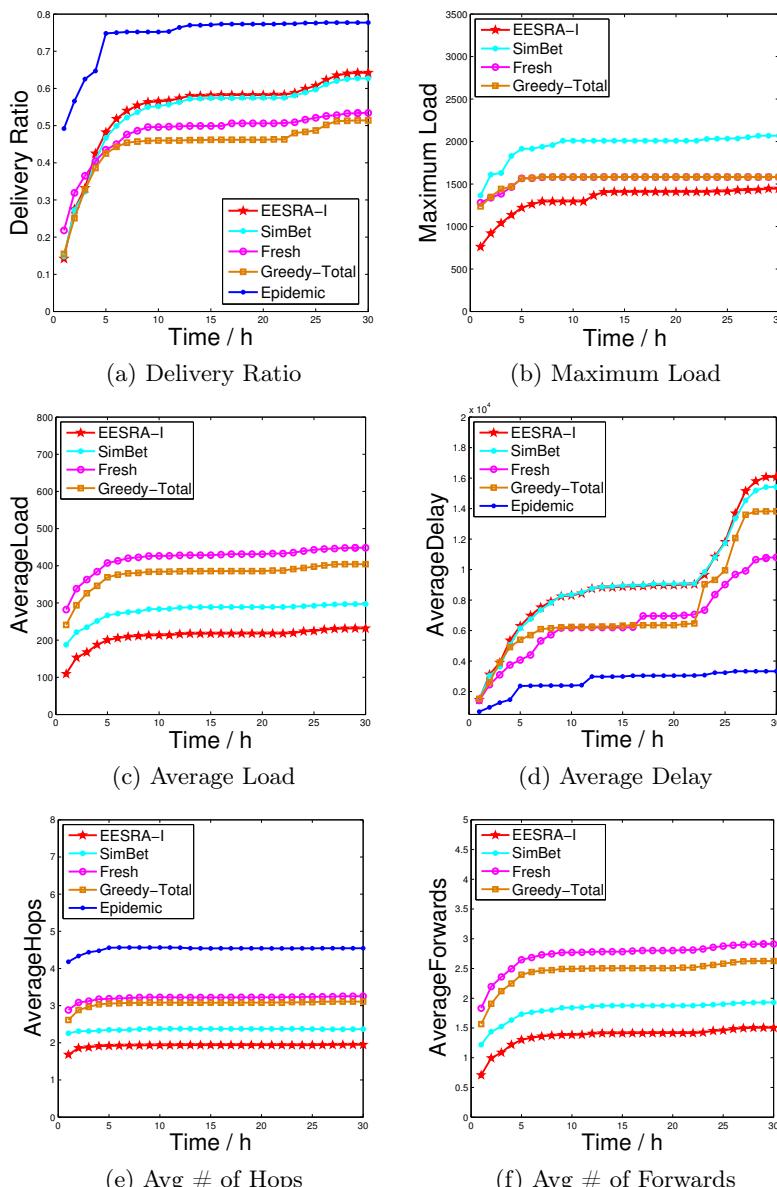


Fig. 3. Simulation Results of EESR-I over InfoCom 2006 trace data

Table 2. Standard Deviation of Loads for Different Routing Methods

Method	Standard Deviation of Load
EESR	64.84
EESR-I	209.95
SimBet	325.97
Fresh	374.85
Greedy-Total	327.16
Epidemic	3,994.94

5 Conclusion

Delay tolerant networks are partitioned wireless ad hoc networks which usually cannot guarantee end-to-end paths between any pair of nodes. Routing in DTNs is a challenging problem. Many social-based routing protocols are proposed to improve the delivery ratio over time, but most of them do not consider the load of nodes. In this paper, we propose an energy efficient social-based routing method to reduce the load of nodes. The proposed general scheme can be applied to any existing social-based routing methods which use social metric per node for relay selection. Simulation results over real-life data traces demonstrate the efficiency of our proposed method.

References

1. Bulut, E., Szymanski, B.K.: Friendship based routing in delay tolerant mobile social networks. In: 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), pp. 1–5. IEEE (2010)
2. Daly, E.M., Haahr, M.: Social network analysis for routing in disconnected delay-tolerant manets. In: Proceedings of the 8th ACM International Symposium on Mobile Ad hoc Networking and Computing, pp. 32–40. ACM (2007)
3. Dubois-Ferriere, H., Grossglauser, M., Vetterli, M.: Age matters: efficient route discovery in mobile ad hoc networks using encounter ages. In: Proceedings of the 4th ACM International Symposium on Mobile Ad hoc Networking & Computing, pp. 257–266. ACM (2003)
4. Erramilli, V., Chaintreau, A., Crovella, M., Diot, C.: Diversity of forwarding paths in pocket switched networks. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, pp. 161–174. ACM (2007)
5. Gao, W., Li, Q., Zhao, B., Cao, G.: Social-aware multicast in disruption-tolerant networks. IEEE/ACM Transactions on Networking (TON) 20(5), 1553–1566 (2012)
6. Hossmann, T., Spyropoulos, T., Legendre, F.: Know thy neighbor: Towards optimal mapping of contacts to social graphs for dtn routing. In: 2010 Proceedings IEEE INFOCOM, pp. 1–9. IEEE (2010)
7. Hui, P., Crowcroft, J.: How small labels create big improvements. In: Fifth Annual IEEE International Conference on Pervasive Computing and Communications PerCom Workshops 2007, pp. 65–70. IEEE (2007)

8. Hui, P., Crowcroft, J., Yoneki, E.: Bubble rap: Social-based forwarding in delay-tolerant networks. *IEEE Transactions on Mobile Computing* 10(11), 1576–1589 (2011)
9. Li, F., Jiang, H., Wang, Y., Li, X., Wang, M., Abdeldjalil, T.: SEBAR: Social energy based routing scheme for mobile social delay tolerant networks. In: Proceedings of the 2013 IEEE International Performance Computing and Communications Conference IEEE (2013)
10. Li, F., Zhao, L., Zhang, C., Gao, Z., Wang, Y.: Routing with multi-level cross-community social groups in mobile opportunistic networks. *Personal and Ubiquitous Computing* 18(2), 385–396 (2014)
11. Lindgren, A., Doria, A., Schelén, O.: Probabilistic routing in intermittently connected networks. *ACM SIGMOBILE Mobile Computing and Communications Review* 7(3), 19–20 (2003)
12. Liu, G., Ji, S., Cai, Z.: Credit-based incentive data dissemination in mobile social networks. In: International Workshop on Identification, Information & Knowledge in The Internat of Things, IIKI 2013 (2013)
13. Liu, M., Yang, Y., Qin, Z.: A survey of routing protocols and simulations in delay-tolerant networks. In: Cheng, Y., Eun, D.Y., Qin, Z., Song, M., Xing, K. (eds.) WASA 2011. LNCS, vol. 6843, pp. 243–253. Springer, Heidelberg (2011)
14. Schurgot, M.R., Comaniciu, C., Jaffres-Runser, K.: Beyond traditional DTN routing: social networks for opportunistic communication. *IEEE Communications Magazine* 50, 155–162 (2012)
15. Scott, J., Gass, R., Crowcroft, J., Hui, P., Diot, C., Chaintreau, A.: Crawdad trace, cambridge/haggle/imote/infocom2006, Downloaded from (2009), <http://crawdad.cs.dartmouth.edu/cambridge/haggle/imote/infocom2006> (v. May 29, 2009)
16. Spyropoulos, T., Psounis, K., Raghavendra, C.S.: Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking, pp. 252–259. ACM (2005)
17. Vahdat, A., Becker, D.: et al.: Epidemic routing for partially connected ad hoc networks. Tech. rep., Technical Report CS-200006, Duke University (2000)
18. Zhu, Y., Xu, B., Shi, X., Wang, Y.: A survey of social-based routing in delay tolerant networks: positive and negative social effects. *IEEE Communications Surveys & Tutorials* 15(1), 387–401 (2013)

Contract Theory for Incentive Mechanism Design in Cooperative Relaying Networks

Yinshan Liu^{1,2}, Xiaofeng Zhong¹, Yang Yan¹, Jing Wang¹, and Walid Saad³

¹ Department of Electronic Engineering, Tsinghua University, Beijing, China

² Dalian Airforce Communication NCO Academy, Dalian, Liaoning, China

³ Electrical and Computer Engineering Department, University of Miami, USA

ys-liu10@mails.tsinghua.edu.cn, {zhongxf,wangj}@tsinghua.edu.cn,

yanyangdavid@gmail.com, walid@miami.edu

Abstract. Multiuser cooperative communication significantly improves the performance of wireless communication networks. One key challenge of multiuser cooperative communication is how to design a cooperative mechanism to incentivize potential relay nodes to help a source node in its data transmission. In this paper, to address this problem, we apply a contract-based *principal-agent* framework to a cognitive-radio-based wireless relaying networks, in which a mobile relay node acts as the principal who designs Incentive Compatible (IC) and Individually Rational (IR) contract items, consisting of a set of rate-price pairs. Subsequently, contract items can be broadcast by a relay to nearby mobile users that want to send data. Once these sources optimally select a relay at the lowest cost and notify the contract items that they are willing to accept, the relay then chooses at least one source for which to provide service. Theoretical analysis and numerical results indicate that this pricing mechanism can lead to a win-win situation in which source nodes get good communication service and relay nodes maximize their own profit that can be used to purchase the relay service of other nodes when needed in the future.

Keywords: cooperative communication, incentive mechanism, relaying networks, contract theory.

1 Introduction

Multiuser cooperative communication has emerged as a promising technique for boosting the performance of wireless networks[1]. The basic premise of cooperative communications is to allow a mobile user to act relay node to help other neighboring mobile user via the short range communication technologies such as Wi-Fi, cellular device-to-device communications, or Bluetooth, among others. The use of relaying has many advantages such as improving the system throughput and coverage as well as enhancing the link rate and reliability. In addition, there is no need to upgrade existing infrastructure in order to install additional relay nodes[2]. However, deploying practical cooperative communication protocols requires overcoming many technical challenges that include reducing

the complexity for cooperation, managing interference, and designing suitable incentive mechanisms to facilitate relaying and cooperation[3, 4, 6, 11, 12].

In recent years, with the advent of highly advanced smartphones, which are capable to simultaneously support multi-mode radio access, including cellular network, Wi-Fi, and Bluetooth, the possibility of cooperative communication at the smartphone level has become more manageable. However, there still remains a need to design low-complexity, distributed cooperative communication mechanisms, which is both challenging and desirable. First, there maybe be a serious problem of signaling overhead, which will increase the cost of operation in a distributed relaying networks. Second, mobile nodes are constrained by limited power and computational resources such as CPUs or batteries. Furthermore, while the use of relaying can improve the data rate of the source user, it can be detrimental to the relay node that must utilize its own power to transmit another node's data. Indeed, due to battery limitations, some mobile nodes may have no incentive to relay the packets of other nodes. Therefore, for such scenarios, distributed incentive mechanisms are necessary to encourage mobile relay nodes to help one another via monetary payments or credits. The mobile relay node can use its earned monetary to purchase the help of other nodes when needed in the future. Thus, it is of interest to develop incentive mechanisms using which all the nodes, sources and relays, can obtain a certain benefit.

The introduction of incentive mechanisms in cooperative networks has attracted attention in the literature [3–7, 9–12]. One popular approach is the use of game-theoretic techniques to introduce distributed pricing mechanisms in cooperative networks[3–6]. However, such approaches are often based on game-theoretic notions such as Nash bargaining that require many rounds negotiation between the nodes which can result in a higher signaling overhead and increased complexity. Another promising approach that has recently been studied is that of contract theory [8]. Contract theory has been used to study economic contracts between service providers as well as issues related to spectrum sharing [9, 10], and relaying [11, 12]. However, in the existing literature such as [11] and [12], building on the relay volunteer their services, the source dominates the trading process and put a price on relay service, resulting in that the source gets the main gain of cooperation, which cannot encourage relay node to provide help.

The main contribution of this paper is to address the problem of cooperative communication using a novel *principal-agent* framework that allows to analyze the monopolistic nonlinear pricing problem, in which a mobile relay node acts as the principal who sets the prices for its service (access rate). The objective of the proposed framework is to maximize the profit of mobile relay nodes. In this respect, we will use the framework of contract theory to formulate Incentive Compatible (IC) and Individually Rational (IR) contracts that can be broadcast by a relay node to nearby mobile users that want to send data. The source nodes will then optimally select a relay at the lowest cost and notify the relay of the contract items that they are willing to accept. Subsequently, the relay will select at least one source for which to provide service. The more payment a mobile relay obtains from its service, the more data service it could purchase when it

becomes a source. Therefore, this mechanism leads to a win-win situation for both source nodes and relay nodes. We analyze the feasibility and optimality of the contract, and derive the best prices assignment and the best transmission time ratio assignment. Numerical results validate the correctness of the theoretical analyses and indicate that the relay is encouraged since it makes most of cooperation gain from the source.

The paper is organized as follows. In Sect. 2, we will first present our system model and contract formulation. In Sect. 3, we design a contract with feasibility and optimality. Section 4 presents the simulation results and analysis. Finally, conclusions are drawn in Sect. 5.

2 System Model

We consider a Cognitive Radio (CR) network that is using the underlay spectrum sharing model shown in Fig.1, which has been studied [13] without considering the two-hop relaying communication. This model consists of CR-enabled mobile stations accessing the communication network via conventional cellular Base Stations (BS). In this network, some mobile bastions (personal devices), acting as source nodes, seek to send data to a far BS with the help of neighboring mobile relays via the BS of the relay. The data will then be forwarded by relay to the ultimate destination of the source. However, the relays have their own data to send and may not be willing to assist the source. Therefore, it is of interest to introduce incentive mechanisms that can encourage mobile devices to relay each others data.

In our underlay sharing model, sources are allowed to adaptively select available spectrum with the guaranty of the Quality of Service (QoS) of the Primary User (PU), improving spectrum utilization effectively. Hence, the maximum transmit

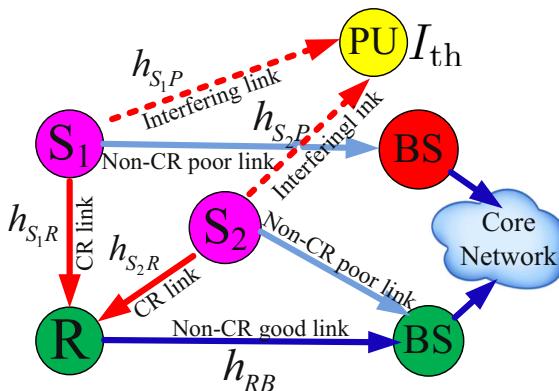


Fig. 1. CR-based hybrid network architecture

power of the sources is limited to $I_{th}/|h_{S_iP}|^2$. So, the sources have different transmission rates:

$$\theta_{S_i} = W \log_2 \left(1 + \frac{I_{th} |h_{S_iR}|^2}{\sigma^2 |h_{S_iP}|^2} \right) . \quad (1)$$

where W is the channel bandwidth, and σ^2 is the noise variance. Without loss of generality, We assume $W = 1$ and σ^2 is identical for all sources.

2.1 Relay Node Model

According to the various values of the sources' capacity, we classify the sources into different type- θ classes. We denote the set of all source types as $\Theta = [\underline{\theta}, \bar{\theta}] \subseteq \mathbb{R}$. The source can obtain its own type by measuring and sensing the wireless environment, while the relay is unaware of the exact type of a particular source before it formulates contract items, consisting of a set of rate-price pairs. This "information" or "knowledge" is private for the source. Nevertheless, we assume the relay has a prior distribution over Θ given by $P(\theta)$ with a continuous density $p(\theta) > 0$. Although the source informs the relay of this private information, the relay has to also consider the cost of receiving and forwarding data, which includes: cost of energy used to receive and forward data, cost of time when receiving and forwarding data, current battery level, as well as other factors.

Since the transmission rate of CR-based link between source and relay is limited due to its transmit power constraint. If the transmission rate is too low, the relay is unwilling to serve source for a long time since the gains from cooperation may be small. In contrast, if it is too high, the relay is unwilling to serve source for a long time because this will reduce its profit (the cost of forwarding data to the BS of relay will increase sharply, e.g., its transmit power must be increased exponentially to increase its data rate by two times under the constant condition of wireless environment). Thus, we define a transmission time ratio, denoted by $q \in Q = [0, 1]$, as the ratio between the transmission time given by the relay and a cooperative slot. The source and the relay negotiate a contract on a pair (q, π) , with time ratio q and a tariff (service price) $\pi \in \mathbb{R}$. The contract is a pair of function $(q, \pi) : \Theta \rightarrow Q \times \mathbb{R}$ that can be viewed as a rule relating the choice of q and π about sources' type θ . Here, we consider two main cost factors: $C(q)$, the cost of time for receiving data, and $G(q\theta)$, the cost of forwarding data with an average transmission rate $q\theta$ bps in a slot. It is easy to see that $C(\cdot)$ and $G(\cdot)$ are non-negative, monotone increasing, and twice differentiable. We further assume that the marginal costs $C'(\cdot)$ and $G'(\cdot)$ are non-decreasing, that is, $C(\cdot)$ and $G(\cdot)$ grow more rapidly at high quantities than they do at small quantities.

Therefore, the *revenue* $R(\theta, q)$ of a relay that is forwarding data with a rate $q\theta$ bps in a slot is given by the difference between the service price and the cost of transmission:

$$R(\theta, q) = \pi(\theta) - C(q) - G(q\theta) . \quad (2)$$

The objective of relay is thus to maximize its revenue in (2).

2.2 Source Node Model

In our model, the source seeks to optimize its data rate. This rate is related not only to the capacity of the source θ , in a slot, but also to the transmission time ratio q allocated by a relay. Thus, we define the *valuation* of a type- θ source for the average transmission rate $q\theta$ bps, denoted by $V(\theta, q)$, as the utility of a source when using a relay's help. We assume $V(\theta, q)$ can simply be given by $f(q\theta)$, where $f(\cdot)$ should be monotonically increasing and concave function. Naturally, the higher the rate that is available to source, the more beneficial it is for the source. However, $f'(\cdot)$, the marginal utility (MU) of the average transmission rate, which reflects the additional satisfaction a source gains from consuming one more unit of average data rate. MU is decreasing with the increase of average transmission rate according to the law of diminishing marginal utility. Here, we can assume that $f(\cdot)$ is given by an α -fair utility function[14]:

$$f(q\theta) = \begin{cases} \omega(1 - \alpha)^{-1}(q\theta)^{1-\alpha}, & 0 \leq \alpha < 1 \\ \omega \log(q\theta), & \alpha = 1 \end{cases} . \quad (3)$$

where ω is the utility level of the source, which represents the source's need for the different applications[7].

2.3 Contracts Formulation

We formulate the problem as a monopolist contract design in which the principal (relay) proposes a contract pair $(q(\theta), \pi(\theta))$ to an agent (source) and, then, the source chooses a unique transmission time ratio $\tilde{q}(\theta)$ and performs a money transfer $\tilde{\pi}(\theta)$ to the relay. In general, $\pi(q(\theta))$ is simply written as $\pi(\theta)$ since $q(\theta)$ is a single-value function. A implementable contract is a set of $(q(\theta), \pi(\theta))$ such that for every type $\theta \in \Theta$, a type- θ source prefers the relaying service with transmission time ratio $q(\theta)$ at the price $\pi(\theta)$ while it does not choose any relaying service with other transmission time ratio at all. Formally, a decision function $q(\theta)$ is *implementable* by a money transfer $\pi(\theta)$ if the IC constraints is satisfied:

$$V(\theta, q(\theta)) - \pi(\theta) \geq V(\theta, q(\tilde{\theta})) - \pi(\tilde{\theta}), \quad \forall \theta, \tilde{\theta} \in \Theta . \quad (4)$$

Equivalently, the contract $(q(\theta), \pi(\theta))$ is implementable.

In addition, due to the selfish and rational nature of the source, a source will never choose a contract that can reduce its utility beyond its *reservation utility* $V(\theta, 0)$. Without loss of generality, we normalize $V(\theta, 0)$ to zero. This property allows to enforce IR on the sources. Formally, we can write the IR constraint as:

$$V(\theta, q(\theta)) - \pi(\theta) \geq 0, \quad \forall \theta \in \Theta . \quad (5)$$

An implementable contract that satisfies the IR constraint is called *feasible*. In other words, a feasible contract must satisfy the IC and IR constraints.

Using the revelation principle, the monopolist's problem can be stated as choosing a pair $(q(\theta), \pi(\theta))$ that solves:

$$\max_{q(\cdot), \pi(\cdot)} \int_{\Theta} [\pi(\theta) - C(q(\theta)) - G(q(\theta)\theta)] p(\theta) d\theta , \quad (6)$$

subject to the IC and IR constraints in (4) and (5).

3 Optimal Contract Design

In this section, we will address the monopolist's problem and analyze the feasibility and optimality of the solution. Furthermore, the best prices assignment and the best transmission time ratio assignment will be derived.

3.1 Social Surplus

The *social surplus*, denoted by $S(\theta, q)$, generated by a relay's selling of service with transmission time ratio q to a type- θ source is defined as the aggregate utilities of both source and relay:

$$S(\theta, q) \stackrel{\Delta}{=} R(\theta, q) + U(\theta, q) = V(\theta, q) - C(q) - G(q\theta) , \quad (7)$$

which reflects the gain from the cooperation between source and relay. Before turning to the analysis of the solution, we define the *first best* solution denoted by $q^{fb}(\theta)$ as the solution of

$$\max_{q(\cdot)} V(\theta, q(\theta)) - C(q(\theta)) - G(q(\theta)\theta) , \quad (8)$$

which would be the optimal decision (i.e., the social optimal transmission time ratio for type- θ) if the relay found the source's type. It is easy to see that $S_{qq}(\theta, q) = V_{qq}(\theta, q) - C''(q) - \theta^2 G''(q\theta) < 0$, $q^{fb}(\theta)$ can be obtained by solving $S_q(q, \theta) = \theta [f'(q\theta) - G'(q\theta)] - C'(q) = 0$ using the implicit function theorem. Thus, the maximum social surplus for each type- θ can be written as $S^{fb}(\theta) = S(\theta, q^{fb}(\theta))$. Here, unlike traditional contract models [8] and [9] in which $q^{fb}(\theta)$ and $S^{fb}(\theta)$ are both monotone increasing with respect to θ , the change trend of $q^{fb}(\theta)$ is such that it firstly increases and then decreases with the increasing of θ as shown in Fig. 2(a) (Sect. 4). Since $q_\theta^{fb}(\theta) = \frac{f'(q\theta) - G'(q\theta) + q\theta[f''(q\theta) - G''(q\theta)]}{C'(q) - \theta^2(f''(q\theta) - G''(q\theta))}$, there exists a stationary point $q\theta = c_0$.

In practice, the social optimal decision may not be adopted by both the source and the relay, whose objectives are always to maximize their own utilities, without considering the social surplus.

The term $G(q\theta)$ in the cost of transmission leads to a non-standard form of the monopolist's problem. Therefore, it must be transformed into a standard form by the method of variable substitution. Making the substitution $\hat{V}(\theta, q) = V(\theta, q) - G(q\theta)$, $\hat{\pi}(\theta) = \pi(\theta) - G(q\theta)$ reduces the monopolist's problem to:

$$\max_{q(\cdot), \hat{\pi}(\cdot)} \int_{\Theta} [\hat{\pi}(\theta) - C(q(\theta))] p(\theta) d\theta , \quad (9)$$

s.t.

- (IC') $\hat{V}(\theta, q(\theta)) - \hat{\pi}(\theta) \geq \hat{V}(\theta, q(\tilde{\theta})) - \hat{\pi}(\tilde{\theta})$, $\forall \theta, \tilde{\theta} \in \Theta$,
- (IR') $\hat{V}(\theta, q(\theta)) - \hat{\pi}(\theta) \geq 0$, $\forall \theta \in \Theta$.

3.2 Feasibility of Contract

Furthermore, as shown in [15, 16], an agent's (source's) utility function $\hat{V}(\theta, q(\theta))$ in the standard monopolist's problem does not satisfy the Spence-Mirrlees Conditions (SMC) or Single Crossing Property (SCP), which implies that $\hat{V}_{q\theta}$ does not change sign for any value of q and θ . So, the local incentive compatibility constraints have to be taken into account. These constraints are equivalent to the monotonicity of the decision variable with respect to the parameter θ . In addition, following [16], we also relax the SMC so as to provide a simple characterization of implementability.

Definition 1. *The relaxing single-crossing or Spence-Mirrlees condition is the constant sign of the cross partial derivative with respect to decision and type:*

$$(CS+) \quad \forall (q, \theta) \text{ in } Q \times \Theta : \hat{V}_{q\theta} > 0,$$

$$(CS-) \quad \forall (q, \theta) \text{ in } Q \times \Theta : \hat{V}_{q\theta} < 0.$$

This implies that the existence of a curve $q_0(\theta)$ dividing the (θ, q) plane into two single-crossing regions, with $V_{q\theta} > 0$ below q_0 and $V_{q\theta} < 0$ above. For notational convenience, we use CS+ and CS- respectively to represent these regions, as we can see in Fig. 2(a) (Sect. 4). Under CS+ (CS-), higher types are associated with higher (lower) marginal valuations of the decision.

Using the implicit function theorem, we can define a unique function $q_0(\theta)$, such that $\hat{V}_{q\theta} = 0$, i.e., $\hat{V}_{q\theta} = f'(q\theta) - G'(q\theta) + q\theta [f''(q\theta) - G''(q\theta)] \stackrel{\Delta}{=} \psi(q\theta) = 0$, so $q_0(\theta) = \psi^{-1}(0)/\theta$, it is easy see that $q_0(\theta)$ is a unique decreasing function.

When $\hat{V}_{q\theta}$ satisfies the relaxing single-crossing condition, one can show that implementability is equivalent to the monotonicity of the quantity assignment function, with increasing under (CS+) or decreasing under (CS-).

Lemma 1. *Let $(q(\theta), \hat{\pi}(\theta))$ be an IC mechanism, then the following condition must be fulfilled:*

1. $\mathcal{V}^q(\theta) := \hat{V}(\theta, q(\theta)) - \hat{\pi}(\theta) = \mathcal{V}^q(\underline{\theta}) + \int_{\underline{\theta}}^{\theta} \hat{V}_{\theta}(\tilde{\theta}, q(\tilde{\theta})) d\tilde{\theta}, \quad \forall \theta \in \Theta ,$
2. $q(\theta)$ is non-decreasing (non-increasing) under CS+ (CS-), i.e., $q_{\theta}(\theta)\hat{V}_{q\theta} \geq 0$.

Proof. The proofs can be found in [16]. □

For the IR' constraint, if $\hat{V}_{\theta} = q(f'(q\theta) - G'(q\theta))$ changes its sign, \mathcal{V}^q in the Lemma 1 has a minimum in the interior of Θ (or at $\underline{\theta}$) depending on q [16]. However, in order to simplify matters, we assume that it is at $\underline{\theta}$. Thus, the IR'constraint needs to be checked only at $\underline{\theta}$ and, since transfer is costly to the principal (relay), IR' must bind at $\underline{\theta}$, i.e., the IR' constraint can be replaced by $\mathcal{V}^q(\underline{\theta}) = 0$. Therefore, the condition in Lemma 1 and $\mathcal{V}^q(\underline{\theta}) = 0$ provide stricter and tighter necessary conditions for the feasible contract.

3.3 Optimality of Contract

Among the possible feasible contracts, our objective is to find an optimal contract. We first derive the best prices for a fixed feasible transmission time ratio

assignment, then we derive the best transmission time ratio assignment for the optimal contract.

Given an implementable mechanism $(q(\theta), \hat{\pi}(\theta))$, there is a non-linear transfer $\hat{\pi}(\theta)$ that implements $q(\theta)$. And

Theorem 1. *Let $(q(\theta), \hat{\pi}(\theta))$ be a feasible contract with the fixed decision variable assignment $q(\theta)$. Then, the unique best price assignment is given by:*

$$\hat{\pi}(\theta) = \hat{V}(\theta, q(\theta)) - \int_{\underline{\theta}}^{\theta} \hat{V}_{\theta}(\tilde{\theta}, q(\tilde{\theta})) d\tilde{\theta} . \quad (10)$$

Proof. By the Lemma 1, for each implementable $q(\theta)$ there exists a unique $\hat{\pi}(\theta) = \hat{V}(\theta, q(\theta)) - \mathcal{V}^q(\underline{\theta}) - \int_{\underline{\theta}}^{\theta} \hat{V}_{\theta}(\tilde{\theta}, q(\tilde{\theta})) d\tilde{\theta}$. Furthermore, according to IR' condition, we have $\mathcal{V}^q(\underline{\theta}) = 0$. Plugging it into the above equation completes the proof. \square

Thus, as the unique best price assignment for the feasible contract $(q(\theta), \hat{\pi}(\theta))$ have been given, we can make a transformation back into terms of $\pi(\theta)$ by making the substitution $\hat{V}(\theta, q) = V(\theta, q) - G(q\theta)$, $\hat{\pi}(\theta) = \pi(\theta) - G(q\theta)$. As a result, we obtain the following corollary.

Corollary 1. *The unique best price assignment for the feasible contract $(q(\theta), \pi(\theta))$ is given by:*

$$\pi(\theta) = V(\theta, q(\theta)) - \int_{\underline{\theta}}^{\theta} [V_{\theta}(\tilde{\theta}, q(\tilde{\theta})) - G_{\theta}(\tilde{\theta}, q(\tilde{\theta}))] d\tilde{\theta} . \quad (11)$$

Theorem 1 suggests that, for any fixed feasible decision variable assignment $q(\theta)$, the best price assignment given by (10) is unique. Therefore, for the monopolist's problem, we plug (10) into the objective function (9) to find:

$$\int_{\Theta} [\hat{\pi}(\theta) - C(q(\theta))] p(\theta) d\theta = \int_{\Theta} \left[\hat{V}(\theta, q(\theta)) - C(q(\theta)) - \int_{\underline{\theta}}^{\theta} \hat{V}_{\theta}(\tilde{\theta}, q(\tilde{\theta})) d\tilde{\theta} \right] p(\theta) d\theta . \quad (12)$$

Integrating by parts, we have $\int_{\Theta} h(\theta, q(\theta)) p(\theta) d\theta$, where $h(\theta, q(\theta)) = \hat{V}(\theta, q(\theta)) - C(q(\theta)) - \frac{1-P(\theta)}{p(\theta)} \hat{V}_{\theta}(\theta, q(\theta))$ is the *virtual surplus*. Thus, we consider the IC' and IR' constraints, and denote $q^{sb}(\theta)$ as the solution which maximizes the following relaxed problem:

$$\max_{q(\cdot)} \int_{\Theta} h(\theta, q(\theta)) p(\theta) d\theta , \quad (13)$$

which can be reduced to a pointwise maximization of the $h(\theta, q(\theta))$. Obviously, $q^{sb}(\theta)$ can be found at the boundary points ($\underline{\theta}$ and $\bar{\theta}$) or at the critical point, i.e., according to Fermat's theorem for stationary points, $q^{sb}(\theta)$ satisfying $h_q(\theta, q^{sb}(\theta)) = 0$ and $h_{qq}(\theta, q^{sb}(\theta)) \leq 0$, for all $\theta \in \Theta$.

If the $q^{sb}(\theta)$ is implementable, then it is the solution of problem (9) subject to IC' and IR' constraints. Otherwise, the monotonicity condition $q_{\theta}(\theta) \hat{V}_{q\theta} \geq 0$ in Lemma 1 is binding. When $q_{\theta}(\theta) \hat{V}_{q\theta} \geq 0$ is binding, one has to respectively perform the *ironing principle* [16] on $q^{sb}(\theta)$ under the region CS+ and CS- to make the infeasible region to be feasible (for a complete analysis of the standard case see in [8]).

4 Simulation Results

We implement the proposed contract in a continuous-type model. The source type θ is distributed with a probability distribution $f(\theta)$ on the interval $[0, 3]$. In our simulations, parameters α and ω of utility function are set to 0.5 and 1, respectively. The cost functions of the relay are defined as $C(q) = 0.5q^{1.2}$ and $G(q\theta) = 0.5(q\theta)^2$. We investigate the optimal contracts in two scenarios which differ from one another in the distribution of type. In case A, all types are uniformly distributed on the $[1, 3]$ with $p(\theta) = 1/3$; in case B, the large type has larger probability than the small type, where $p(\theta) = 2\theta/9$.

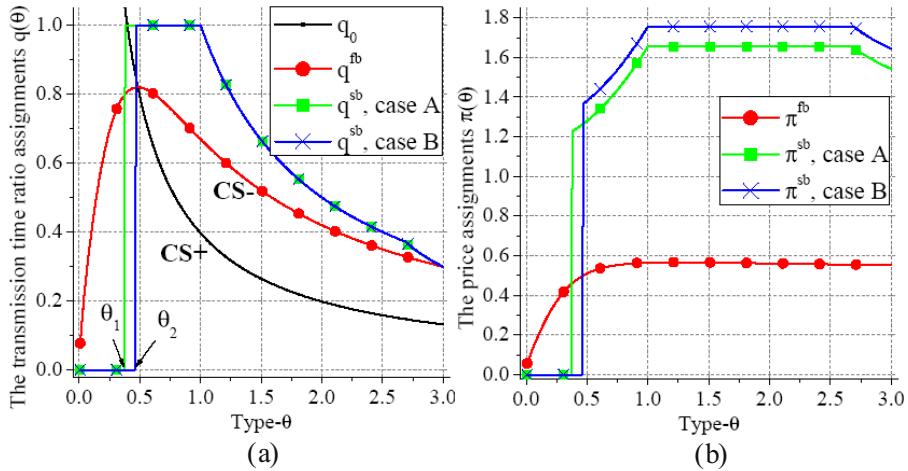


Fig. 2. The transmission time ratio and price assignments in the optimal contracts

Figure 2 presents the transmission time ratio and the best price assignments in the optimal contracts, respectively. In subplot (a), the curve with bold dot represents the social optimal transmission time ratio assignments, i.e., the first best solution q^{fb} , which maximizes the social surplus. The curves with bold square and cross denote the optimal transmission time ratio assignments q^{sb} in the optimal contracts for scenarios A and B, respectively. It can be seen that q^{sb} is non-decreasing (non-increasing) under the region CS+ (CS-), satisfies the second term condition in Lemma 1. Note, for example, in case A, where $q(\theta) = 1$ denote that the transmission time ratio assignments reach the maximum, where $q(\theta) = 0$, i.e., $\theta \in [0, \theta_1]$, denote an aborted trading process; when $\theta \in (\theta_1, 3]$, the transmission time ratio assignment in optimal contract is always more than the social optimal ratio assignment. This can be explained as follows, for the propose of revenue maximizing, the relay will reduce the supply to the lower type source and increase the time assignment to the higher type source. Meanwhile, it charge a much higher price from source. Furthermore, if the probability of lower type sources become smaller, e.g., case B, the relay tends to reduce more supply on the low type sources and charge at higher price from the higher type sources.

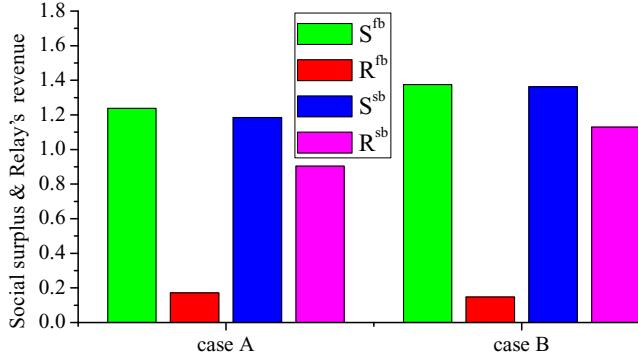


Fig. 3. The social surplus and the revenues of the relay in the optimal contracts

Figure 3 shows the social surplus and the revenues of the relay in the optimal contracts. In this histogram, S^{fb} and R^{fb} denote the social optimal surplus and the revenue of the relay in the social optimal contract, respectively, while S^{sb} and R^{sb} denote the social surplus and the revenue of the relay under the optimal contracts. Clearly, the S^{sb} is only slightly smaller than S^{fb} , which reflects the upper bound of cooperation gain. In Fig. 3, we can see that the relay gains more revenue from the optimal contract, at the expense of social surplus decreasing caused by the dropping out of low type sources.

5 Conclusion

In this paper, we have studied a pricing mechanism for multiuser cooperative communication in a cognitive-radio-based wireless network using a simple principal-agent framework, in which the relay acting as the principal designs contract items and sources act as the agent. The contract items consist of a set of rate-price pairs. we have analyzed the feasibility and optimality of the contract and we have derived the best variable assignment and the best price assignment. The proposed mechanism is simple and requires limited interaction between source and relay. Numerical simulation results have shown that this pricing mechanism can lead to a win-win situation, where the source nodes get good communication service and the relay nodes maximize their own profit. From a social surplus perspective, our results have shown that the social surplus under the optimal contract is close to the maximum social surplus.

Acknowledgments. This work is supported by National Basic Research Program of China (2012CB316000), National Natural Science Foundation of China (61201192), National S&T Major Project (2013ZX03003004-002), International Science and Technology Cooperation Program(2012DFG12010), Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2012D02), and Cooperation Agreement Between THU and SEC.

References

1. Erkip, A., Aazhang, E., Aazhang, B.: User cooperation diversity-Part I: System description and User cooperation diversity-Part II: implementation aspects and performance analysis. *IEEE Trans. on Commun.* 51(11) 1927–1938, 1939–1948 (2003)
2. Vanganuru, K., Ferrante, S., Sternberg, G.: System capacity and coverage of a cellular network with D2D mobile relays. In: *IEEE MILCOM*, Orlando (2012)
3. Huang, J., Han, Z., Chiang, M., Poor, H.V.: Auction-based resource allocation for cooperative communications. *IEEE J. on Sel. Areas in Commun.* 26(7), 1226–1237 (2008)
4. Han, Z., Niyato, D., Saad, W., Basar, T., Hjørungnes, A.: *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*. Cambridge Univ. Press (2010)
5. Huang, J., Palomar, D.P., Mandayam, N.B., Wicker, S.B., Walrand, J., Basar, T.: Game theory in communication systems. *IEEE J. Sel. Areas Commun.* 26(7), 1042–1046 (2008)
6. Wang, B., Han, Z., Liu, K.: Distributed relay selection and power control for multiuser cooperative communication networks using buyer/seller game. In: *26th IEEE International Conference on Computer Commun.*, INFOCOM (2007)
7. Hande, P., Chiang, M., Calderbank, R., Zhang, J.: Pricing under constraints in access networks: Revenue maximization and congestion management. In: *29th IEEE International Conference on Computer Commun.*, INFOCOM (2010)
8. Bolton, P., Dewatripont, M.: *Contract Theory*. The MIT Press (2004)
9. Duan, L., Gao, L., Huang, J.: Contract-based cooperative spectrum sharing. In: *IEEE DySPAN*, pp. 399–407 (2011)
10. Gao, L., Wang, X., Xu, Y., Zhang, Q.: Spectrum Trading in Cognitive Radio Networks: A Contract-Theoretic Modeling Approach. *IEEE J. on Sel. Areas in Commun.* 29(4), 843–855 (2011)
11. Hasan, Z., Jamalipour, A., Bhargava, V.K.: Cooperative communication and relay selection under asymmetric information. In: *IEEE WCNC* (2012)
12. Nazari, B., Jamalipour, A.: Contract design for relay-based cooperative communication with hidden channel state information. In: *1st IEEE International Conference on Commun. in China (ICCC)*, pp. 798–803 (2012)
13. Cai, Z., Ji, S., He, J., Wei, L., Bourgeois, A.G.: Distributed and Asynchronous Data Collection in Cognitive Radio Networks with Fairness Consideration. *IEEE Trans. on Parallel and Distributed Systems.* (99) (2013)
14. Yang, L., Kim, H., Zhang, J.: Pricing-based decentralized spectrum access control in cognitive radio networks. *ACM Trans. on Networking* 21(2), 522–535 (2013)
15. Segal, I.: Lecture notes in contract theory (2010)
16. Araujo, A., Moreira, H.: Adverse selection problems without the Spence-Mirrlees condition. *J. of Economic Theory* 145(3), 1113–1141 (2010)

Object-Oriented Big Data Security Analytics: A Case Study on Home Network Traffic

Kuai Xu, Feng Wang, Richard Egli, Aaron Fives, Russell Howell,
and Odayne McIntyre

School of Mathematical and Natural Sciences

Arizona State University

{kuai.xu,fwang25,regli,agfives,rphowell,ormcinty}@asu.edu

Abstract. Securing and managing home networks has recently become an increasingly challenging task due to the rapid growth of devices, applications and traffic in these networks. This paper presents a novel object-oriented big data security analytics for making sense of traffic data collection from home networks. We extract the source IP addresses from unwanted traffic towards real home networks as *objects of interest*, and subsequently characterize these objects with heterogeneous and streaming data sources including intrusion detection logs provided from distributed firewalls, Internet routing table snapshots from BGP routers, active probing results from open DNS resolver scanning, and IP-to-geographical mapping database. Our preliminary results have revealed a number of important findings and correlations on the *objects of interests* from these diverse and massive data-sets. To the best of our knowledge, this position paper is the first effort to introduce object-oriented perspective to perform security analytics on home network traffic.

1 Introduction

The rapid adoptions of residential broadband and Internet-capable devices in the digital home have driven the exponential growth of home networks traffic. However, many home users do not have the sufficient technical expertise to manage and secure home networks and connected devices, thus leaving many devices compromised by malwares and even controlled by botnets. The rising volume, diversity and heterogeneity of Internet traffic data in distributed home networks has challenged traditional cyber security analytics and forensics analysis that rely on inspecting packet contents and network flow records.

Towards this end, we propose a novel *object-oriented big data security analytics framework* to analyze home network traffic and additional data sources. Rather than randomly analyzing volume, features and distribution of home networks, the framework starts from identifying the *object of interest* and subsequently builds behavior fingerprint and security profiles of these objects. The candidates of objects include IP addresses of home network devices, or IP addresses of Internet attackers, port numbers and applications. In addition, the framework is flexible to support the aggregation of these objects through concept hierarchy.

For example, the framework also can build security profiles for network prefixes or countries.

To demonstrate the ability of the proposed object-oriented security analytics framework, we apply the framework on network traffic collected from five real home networks that deploy our traffic monitoring system [14]. As a case study, we use the framework to extract IP addresses, sending at least one unwanted IP packet towards one of the five home networks, as *object of interests* in this study. For simplicity, we refer to these IP addresses as *attackers*. To build behavior fingerprints and security profiles for these objects, we explore other interesting data-sets including open DNS resolvers, intrusion detection logs, Internet routing tables, IP-to-geolocation database for discovering a rich set of valuable features or dimensions of these *objects*.

The proposed framework will have a variety of applications for network security monitoring and forensic analysis. For example, we could leverage object-oriented security analytics to build security profiles or behavior fingerprints for IP addresses, network prefixes, applications or TCP/IP ports. In addition, we could provide insights of these *objects* to other security analytics tasks, e.g., early detection of worm outbreaks.

The contributions of this paper are two-fold.

- We propose a novel object-oriented big data security analytics that uses object-oriented perspective to make sense of heterogeneous big data from a variety of sources for classifying Internet end hosts and mining anomalous traffic patterns.
- We demonstrate the advantages, simplicity and usage of the proposed framework with the attackers of home network as *objects of interest*, and build behavior fingerprints and security profiles for these objects with a variety of data-sets.

The remainder of this paper is organized as follows. Section 2 presents our proposed object-oriented big data security analytics framework and briefly describes the data-sets used in the study. Section 3 illustrates the results of applying object-oriented big data with home network security as a case study. Section 4 discusses related work, while Section 5 concludes this paper and outlines our future work.

2 Methodology of Object-Oriented Big Data Security Analytics and Data-Sets

2.1 Analytics Framework

Figure 1 shows a schematic diagram to illustrate our proposed object-oriented big data security analytics for making sense of network traffic. Our framework takes into considerations of a variety of heterogeneous data sources such as intrusion detection logs from distributed firewalls, active open DNS resolver scanning,

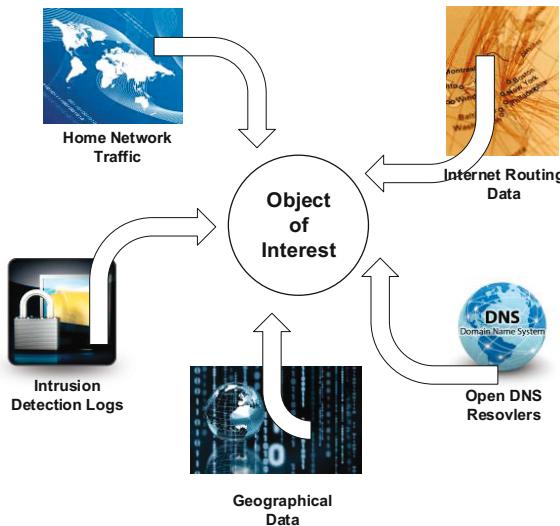


Fig. 1. An object-oriented big data analytics for making sense of home network security data

real-time home network traffic, continuous snapshots of Internet routing tables, and geographic databases of Internet end hosts.

The *object* of interests in the analytics framework could be either *fine-grained* units in IP packets such as IP addresses and port numbers or the *aggregated* units such as network prefixes (a block of IP addresses), autonomous systems (the network of one or multiple prefixes), applications (one or more ports). The framework will allow flexible integration of other data sources including those depicted in the diagram as well as the data-sets not shown, e.g., distributed denial of service (DDoS) packet traces [11] and census and survey of the visible Internet [12,27].

2.2 Data-Sets

In this paper we combine a variety of data sources into the proposed big data security analytics framework. The data include home network traffic, intrusion detection logs, open DNS resolvers, Internet routing information and IP-geographical mapping. Table 1 summarizes the types, units, vantage points, update frequencies, and duration of these data-sets used in this study.

The size of these data used in this study is relatively smaller than those collected from enterprise networks, data center networks, and IP backbone networks. However, the proposed object-oriented approach can effectively extract objects of interests from these data as well and build behavior fingerprints and security profiles for these objects.

Table 1. Description of data-set used in the proposed big-data security analytics framework

Data	Dynamics	Type	Unit	Vantage Point	Update	Durations
netflow	Yes	Flat file	flow	5	5 minutes	2 years
IDS logs	Yes	DB Query	IP	1	daily	12 years
Open DNS Resolvers	Yes	Binary	IP	1	weekly	10 months
BGP	No	Flat file	prefixes	1	N/A	N/A
IP Geolocation	No	DB Query	IP	1	N/A	N/A

3 Home Network Security Analytics

In this section we explore the proposed object-oriented security analytics to make sense of home network traffic collected from five real home networks. Specifically, we use IP as the *object* of interest and analyze a variety of features or dimensions of these objects using other data-sets.

3.1 Big Data in Home Network Traffic

Table 2 illustrates the statistics of network traffic from five home networks which deploy our home network traffic monitoring system [14]. In total, we have observed 66.96 million flows, 2733.02 million data packets, 2301.24 gigabytes of traffic, 502,951 unique source IP addresses, 589,007 unique destination IP addresses, 65,143 unique source port numbers, 65,371 unique destination port numbers, and 111,977 attackers that send unwanted traffic towards these five home networks.

Table 2. Statistics of network traffic from five home networks

network	flows	packets	bytes	duration	srcIP	destIP	srcPort	dstPort	attackers
home 1	10.71M	286.94M	196.21G	5 months	238.09K	313.90K	64564	64720	9,347
home 2	7.77M	512.51M	535.22G	4 months	32.55K	32.09K	64662	64846	6,726
home 3	14.64M	1196.69M	1074.49G	6 months	32.76K	30.25K	64748	64812	10,871
home 4	1.37M	94.54M	74.88G	2 months	15.68K	17.05K	52155	51461	4,945
home 5	32.47M	642.34M	420.44G	3 months	200.99K	213.73K	64502	64660	82,052
total	66.96M	2733.02M	2301.24G	N/A	502.95K	589.00K	65143	65371	111,977

Figure 2 illustrates the data volume of network traffic flows, packets, and flows collected from home network 2 over a 4-month time-span. The basic statistics shows the significant *volume* of home network traffic, while the streams of network flows captures the *velocity* nature of these traffic. The *variety* of these traffic is reflected by the rich set of dimensions or features we could simple observe or derive, such as source IP address, destination IP address, source port numbers, destination port numbers, protocol, packets, bytes, packet-size distribution, flow size distribution, flow duration, packet asymmetry, etc. Thus, home

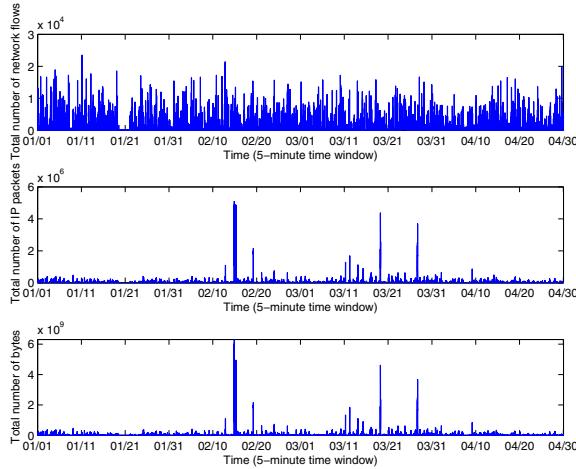


Fig. 2. The data volume of network traffic flows, packets, and flows collected from home network 2 over a 4-month time-span

network traffic carries all the three characteristics of big data: *volume*, *velocity*, and *variety*.

To gain a better understanding on home network traffic, we apply the proposed big-data oriented security analytics to analyze these traffic and integrate with additional data sources. In particular, we will focus on the attackers who send unwanted traffic towards home networks and address the following questions:

- What are these attackers?
- How do they attack distributed home networks?
- Where are they located?
- What networks do they come from?
- Do they also attack other networks?
- Are they also open DNS resolvers?

3.2 Object-Oriented Analytics

Intrusion Detection Logs. We consider each of the attackers captured from home network traffic as an *object*, and query their records from a public intrusion detection databases hosted by DShield [7], which collect intrusion detection statistics from from distributed firewalls [4]. Inspired by a number of recent security studies based on cooperative or collaborative approaches [24,21,10,8], we combine the intrusion detection information as a feature dimension for the IP objects of attackers.

For all 111,977 attacker, we find 3,726 are also included in DShield database. Figure 3 illustrates the distribution of unique IP addresses targeted by these 3,726 attackers based on the unique number of targets they have explored.

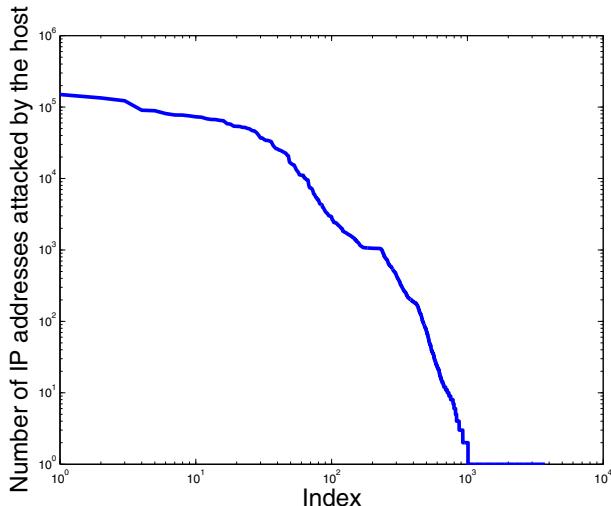


Fig. 3. The distribution of unique IP addresses targeted by aggressive attackers based on querying DShield Internet Storm Center database

Open DNS Resolvers. In recent years, open resolvers have been extensively exploited by attackers in distributed denial of service attacks (DDoS) via DNS reflection attacks, also called DNS amplification attacks, and IP spoofing. Characterizing open resolvers on the Internet becomes an urgent task for stopping such attacks. In this paper, we also collect and analyze a list of open DNS resolvers from Open Resolver Project [20] and correlate with the objects of attackers towards home networks.

For all 111,977 attacker, we find 106,559 are not open DNS resolvers, while 5,418 are open DNS resolvers. By classifying attackers into two groups (non-open DNS resolvers and open DNS resolvers), we find a striking difference between them: the average number of unwanted traffic flows for the first group is 2, while the average for the second group is 32. This finding suggests that these open DNS resolvers discovered from active open DNS probing are likely continuously exploited by many attackers in cyber attacks.

Figure 4 illustrates the distribution of unwanted traffic flows for attackers that are also open DNS resolvers. It is very interesting to see that several attackers aggressively send unwanted packets to distributed home networks in our datasets, while most of them only send a few packets.

BGP Prefixes and Autonomous Systems. Forensic analysis of Internet traffic is always interested in locating the origins of source IP addresses used by attackers. Thus it is important to map their BGP network prefixes and autonomous system numbers (ASNs). In this study, we use a recent BGP routing snapshot for University of Oregon Route Views Project [23] to infer BGP network prefixes and ASNs.

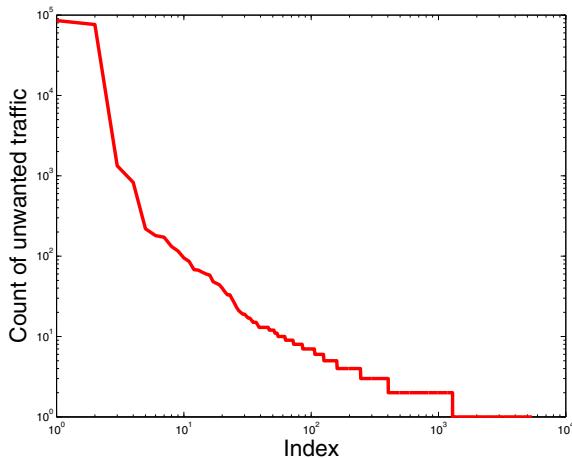


Fig. 4. The distribution of unwanted traffic flows for attackers that are also open DNS resolvers

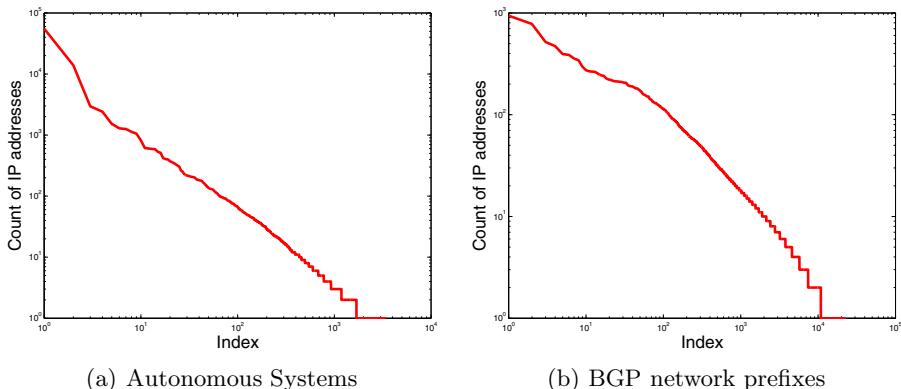


Fig. 5. The distribution of IP addresses for autonomous systems and BGP network prefixes

Figure 5[a][b] illustrate the distribution of IP addresses for autonomous systems and BGP network prefixes, respectively. It is interesting to see that, from both figures, there exist a few prefixes or ASNs that include many attacker IP addresses, while most prefixes or ASNs have a few addresses. Upon close examinations, we find the prefixes and ASNs associated with many attacker IP addresses are mostly broadband network providers suggesting that many home networks contain Internet-capable devices that are compromised or even controlled by attackers.

Geographical Locations In addition of the network origins of attack IP addresses, we also map their geographical locations with MaxMind, an online IP-to-geolocation mapping service. As shown in Figure 6, a few top countries account for the majority of attacker IP addresses, confirming the findings from previous studies. Figure 7 illustrates the top 10 countries with the most number of attackers via Google map where the size of the circles indicates the ranks of the countries. More importantly, we find that the distributions on open DNS resolvers, the country, network prefixes, and ASNs all follows power-law like distributions.

In summary, we demonstrate the capability of object-oriented security analytics to analyze the IP objects and build behavior fingerprints and security profiles of the attackers that explore the vulnerabilities or weakness of home network routers or connected devices. Our preliminary results provide much-needed insights and situation awareness for home users on what is happening in home networks.

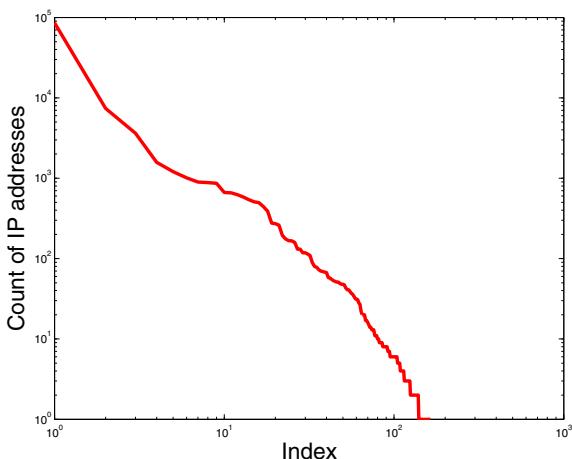


Fig. 6. The distribution of IP addresses across different countries

4 Related Work

The last decade has witnessed the rapid growth of residential broadband and home networks [25]. Securing and managing the increasingly complicated home networks recently become an urgent research topic due to the rising traffic, devices, users and applications [22,15,16,14,9,13,17,18,5,1,28].

The size and diversity of real-time traffic streams from distributed home networks make home network traffic analysis a big data problem [19,3]. Similar to many applications such as social networks and health care, big data analytics and cloud computing have demonstrated their capability of mining important

knowledge from acquiring, processing, and analyzing the unprecedented amount of data [26,6].

The promise of big data leads many security researchers to explore big data tools and techniques to analyze massive, unstructured, diverse and continuous data collected for cyber security and digital forensics [2]. In this paper, we propose an object-oriented big data security analytics to analyze home network traffic as well as integrate with a variety of other data sources such as intrusion detection logs and open DNS resolvers. Our preliminary results illustrate the promise of our framework to effectively build profiles for significant objects of interest in security monitoring and forensic analysis.

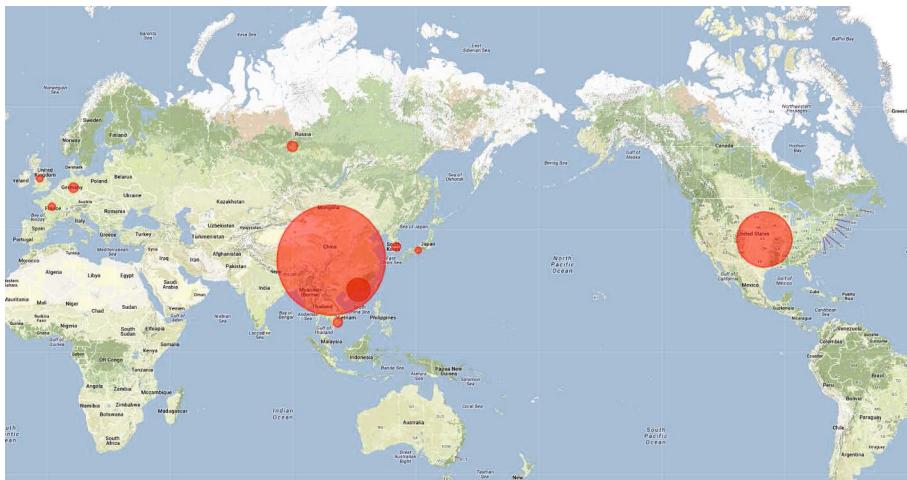


Fig. 7. A Google map of the top 10 countries ranked by the number of attackers extracted from home network traffic

5 Conclusions and Future Work

The growing devices, applications and traffic in the digital homes have challenged the management and security of millions of home networks. In light of the volume, velocity, variety and value of home network traffic, this paper introduces an object-oriented big data security analytics framework to analyze home network traffic data. The framework extracts *objects* of interests from outgoing, incoming and internal home network traffic, and builds behavior fingerprints and security profiles for these objects via analyzing home network traffic as well as correlating with other data sources such as intrusion detection logs, open DNS resolvers, Internet routing tables, IP-to-geolocation mapping database. Our preliminary results have lead to a number of interesting findings from real home network traffic including the distribution of unique IP addresses targeted by aggressive attackers, the distribution of unwanted traffic flows from attackers that

are also open DNS resolvers. Our results also identify the top network prefixes, ASNs and countries of thousands of attackers discovered from home networks traffic, and provide valuable information for network operators and security analysts. Our future work lies in extending the proposed framework to analyze traffic data collected from Internet backbone networks, data center networks and enterprise networks. In addition, we are also in the processing of designing and implementing the framework on top of Hadoop MapReduce and Hadoop distributed file systems (HDFS) and deploying and evaluating the system in real-time.

Acknowledgements. We would like to thank Open Resolver Project and DShield.org for providing the IP addresses of open DNS resolvers and cyber attack statistics, respectively. This work was supported in part by National Science Foundation under the grant CNS #1218212, Arizona State University New College SRCA grants and an NCUIRE team award.

References

1. Anand, A., Gember, A., Akella, A., Sekar, V.: Tracking Semantic Relationships for Effective Data Management in Home Networks. In: Proceedings of ACM SIGCOMM Workshop on Home Networks, HomeNets (September 2010)
2. Cardenas, A., Manadhata, P., Rajan, S.: Big Data Analytics for Security. IEEE Security & Privacy 11, 74–76 (2013)
3. Cuzzocrea, A., Saccà, D., Ullman, J.: Big data: a research agenda. In: Proceedings of International Database Engineering and Applications Symposium, IDEAS (October 2013)
4. Bellovin, S.M.: Distributed Firewalls. Login: Special Issue on Security, 37–39 (November 1999)
5. Dixon, C., Mahajan, R., Agarwal, S., Brush, A., Lee, B., Saroiu, S., Bahl, V.: The Home Needs an Operating System (and an App Store). In: Proceedings of ACM Workshop on Hot Topics in Networks, HotNets (October 2010)
6. McGregor, C.: Big Data in Neonatal Intensive Care. Computer 46, 54–59 (2013)
7. DShield.org: Cooperative Network Security Community - Internet Security, <http://www.dshield.org/>
8. Wustrow, E., Karir, M., Bailey, M., Jahanian, F., Houston, G.: Internet Background Radiation Revisited. In: Proceedings of ACM SIGCOMM Conference on Internet Measurement (November 2010)
9. Feamster, N.: Outsourcing Home Network Security. In: Proceedings of ACM SIGCOMM Workshop on Home Networks (HomeNets) (September 2010)
10. Maier, G., Feldmann, A., Paxson, V., Allman, M.: On Dominant Characteristics of Residential Broadband Internet Traffic. In: Proceedings of Internet Measurement Conference (November 2009)

11. Hussain, A., Heidemann, J., Papadopoulos, C.: A Framework for Classifying Denial of Service Attacks. In: Proceedings of ACM SIGCOMM (August 2003)
12. Heidemann, J., Pradkin, Y., Govindan, R., Papadopoulos, C., Bartlett, G., Bannister, J.: Census and Survey of the Visible Internet. In: Proceedings of ACM Internet Measurement Conference (October 2008)
13. Calvert, K., Edwards, W.K., Feamster, N., Grinter, R.E., Deng, Y., Zhou, X.: Instrumenting Home Networks. In: Proceedings of ACM SIGCOMM Workshop on Home Networks (HomeNets) (September 2010)
14. Xu, K., Wang, F., Gu, L., Gao, J., Jin, Y.: Characterizing Home Network Traffic: An Inside View. In: Proceedings of International Conference on Wireless Algorithms, Systems, and Applications (August 2012)
15. Xu, K., Wang, F., Gu, L., Gao, J., Jin, Y.: Characterizing Home Network Traffic: An Inside View. Accepted by Personal and Ubiquitous Computing 18(4), 967–975 (2014)
16. Xu, K., Gu, L., Wang, F.: Monitoring Home Network Traffic via Programmable Routers. In: Proceedings of IEEE GLOBECOM (December 2013)
17. DiCioccio, L., Teixeira, R., Rosenberg, C.: Measuring and Characterizing Home Networks. In: Proceedings of ACM SIGMETRICS (June 2012)
18. DiCioccio, L., Teixeira, R., Rosenberg, C.: Measuring Home Networks with HomeNet Profiler. In: Proceedings of Passive and Active Measurement Conference (March 2013)
19. Chen, M., Mao, S., Liu, Y.: Big Data: A Survey. Mobile Networks and Applications (January 2014)
20. Open Resolver Project: Open DNS Resolvers, <http://openresolverproject.org/>
21. Katti, S., Krishnamurthy, B., Katabi, D.: Collaborating Against Common Enemies. In: Proceedings of ACM SIGCOMM Internet Measurement Conference (October 2005)
22. Denning, T., Kohno, T., Levy, H.M.: Computer Security and the Modern Home. Communications of the ACM 56(1), 94–103 (2013)
23. University of Oregon: Route Views Project, <http://www.routeviews.org/>
24. Yegneswaran, V., Barford, P., Ullrich, J.: Internet intrusions: global characteristics and prevalence. In: Proceedings of ACM SIGMETRICS (June 2003)
25. Edwards, W., Grinter, R., Mahajan, R., Wetherall, D.: Advancing the State of Home Networking. Communications of the ACM 54(6), 62–71 (June 2011)
26. Tan, W., Blake, M., Saleh, I., Dustdar, S.: Social-Network-Sourced Big Data Analytics. IEEE Internet Computing 17, 62–69 (2013)
27. Cai, X., Heidemann, J.: Understanding Block-level Address Usage in the Visible Internet. In: Proceedings of ACM SIGCOMM (August 2010)
28. Yiakoumis, Y., Yap, K., Katti, S., Parulkar, G., McKeown, N.: Slicing Home Networks. In: Proceedings of ACM SIGCOMM Workshop on Home Networking (August 2011)

SPS: A Novel Semantics-Aware Scheme for Location Privacy in People-Centric Sensing Network

Ziling Wei, Baokang Zhao*, and Jinshu Su

School of Computer Science,
National University of Defense Technology,
Changsha, Hunan, China

wziling1017@gmail.com, {bkzhao, sjs}@nudt.edu.cn

Abstract. With the development of wireless communication technologies, people-centric sensing network which is a newly sensor network provides an opportunity to create intelligence systems. However, location privacy became one of the most serious problems to promote development of people-centric sensing network. Currently, many privacy-preserving techniques for location services focused on obfuscation. However, most of them did not take into account the semantics-aware threat. In this paper, we propose a novel scheme named a novel Semantics-aware scheme for location privacy in People-centric Sensing network (SPS). The original contribution of the paper is a novel scheme for selecting the sensitivity threshold value and protecting location privacy from the obfuscated space generator. Moreover, we evaluate the performance of SPS. The result shows that SPS could resist the semantics-aware threat under a reasonable cost.

Keywords: people-centric sensing network, obfuscation, AHP, privacy.

1 Introduction

With the advancement of computation, storage and wireless communications, a great number of sensors, such as audio, location, and image sensors, are equipped to our PDAs [1]. People-centric sensing network is a kind of network which utilizes these sensors to accomplish the construction of intelligence systems [2]. Nowadays, there are many People-centric sensing network systems, such as, BikeNet [3], CitySense [4], Urban Sensing [5], SenseWeb [6], CarTel [7], and so on. However, there are still some challenges. Privacy is one of the most important problems. In our previous researches, we solved the privacy-preserving in the procedure of data aggregation. In this paper, we focused on the privacy-preserving in the procedure of application. At present, most of applications in PCS based on users' location. Such kinds of applications are usually requested by a PDA [8]. Then, the server response the request based on the client's location. For example, some people are likely to query a request:

* Corresponding author.

which restaurant is the most famous in this city? However, when we request our requirement, the personal location should be transferred to the server. As the server is a third-party and the link of transformation is a kind of open channel, our location information is easily to be leaked. Moreover, personal location data can lead to the inference of sensitive information about individuals, location privacy-preserving in PCS become an important problem. For example, the health status can be inferred from the hospital that one person visited [9] [10].

Personal location data are usually made up of the form (UserID, Loc). UserID represents an individual, and Loc represents the real location of the individual. Therefore, location privacy threat cannot occur until both the UserID and Loc are leaked [11]. That is, in order to preserve the privacy of personal location, the method could be conducted from both UserID and Loc. Currently, there are two main techniques to preserve the personal location, including pseudonym [12] and location obfuscation [13]. Pseudonym focuses on protecting user's identifier UserID. Location obfuscation focuses on protecting user's location Loc.

In this paper, our research focuses on location obfuscation. The reason is that the simple hiding of the identifier cannot sufficient to anonymize requests because identity may be inferred from some other data source. Moreover, some applications may need to have enough identity information for some services. The main idea of location obfuscation is using a careful imprecise region to replace the user's real location. And there are many researches focus on finding available algorithms to generate the imprecise region. These researches achieve a good effect on most cases [14].

However, most of these researches do not consider the geographical knowledge when generating the imprecise region. Therefore, some adversaries may reduce the effect of location obfuscation using semantics-aware threat [15]. At first, we define the meaning of semantic location. Semantic location is the mixture of spatial position and the natural and social attributes of this position. Next, we will take an example to explain the meaning of semantics-aware threat. For example, Bob does not want to let anyone know his health status. Therefore he does not want others to know his position when he is at hospital. If we generate an imprecise region which contains this hospital and a military restricted zone, location obfuscation cannot preserve Bob's location privacy [16]. That is, others can get the real position based on the semantic location.

Maria presented SensFlow algorithm to compute the obfuscated space for solving the semantics-aware threat [17]. At first the user sends his/her real location and the requirement to the obfuscated space generator. Then, the obfuscated space generator generates an obfuscated space based on the real location and sends it to the server. Finally, the server provides the service to the user according to the obfuscated space and the requirement. Through the experimental evaluation, the method can play a key role in semantics-aware obfuscation for location privacy [17][18]. However, the algorithm ignores two problems, including how to select the sensitivity threshold value and protecting location privacy from the obfuscated space generator. This motivates our design of SPS.

The contributions of this paper are summarized as follows:

- We study the threat model in people-centric sensing network, especially the semantics-aware threat. It enables researchers to study the privacy-preserving for location in people-centric sensing network conveniently.
- We present SPS for selecting the sensitivity threshold value and protecting location privacy from the obfuscated space generator. Based on SenseFlow, SPS could provide a sufficient location privacy-preserving service.
- We give the evaluation of SPS. The result of evaluation shows that it can significantly improve the location privacy-preserving under a reasonable cost.

The paper is organized as follows. We provide a brief introduction to SenseFlow algorithm in Section 2. In Section 3, we present our scheme in details. Then, we give the evaluation of SPS in Section 4. Conclusion could be found in Section 5.

2 SensFlow Algorithm

Maria presents SensFlow algorithm to compute the obfuscated space for solving the semantics-aware threat. This algorithm contains three steps. Firstly, it specifies the feature types of semantic location which contains sensitive and unreachable. A position is sensitive when it denotes a set of sensitive places, such as a hospital. A position is unreachable when it denotes a set of places which cannot be accessed by the user, such as a military restricted zone. Then, it defines a metric to quantify how much sensitive an arbitrary location is based on the user's privacy requirements. For example, a space consisting of four regions c_0, c_1, c_2, c_3 ; the set of sensitive types $FT_{sens} = \{ft_0, ft_1, ft_3\}$ and the set of non-reachable types is $FT_{Nreach} = \{ft_2\}$. Table 1 reports how to compute the sensitivity level for a region.

$Area(c, ft)$ represents the area of the region c which affected by the sensitive type ft . $Score(ft)$ represents the degree of sensitivity for a sensitivity type. $Areal_{real}$ represents the real area of the region c . SL_c represents the sensitivity level for each region. The sensitivity level for regions c_0 is calculated as follow [17].

$$SL_{c_0} = \frac{0.5 * 200 + 0.7 * 100 + 0.9 * 0}{400} = 0.425 \quad (1)$$

Table 1. An example about computing the sensitivity level

$Area(c, ft)$	c_0	c_1	c_2	c_3	$Score(ft)$
ft_0	200	0	100	0	0.5
ft_1	100	0	0	50	0.7
ft_2	300	450	200	0	0
ft_3	0	200	100	400	0.9
$Areal_{real}$	400	200	200	500	
SL_c	0.425	0.900	0.700	0.790	

The next step defines the sensitivity threshold value θ_{sens} [19][20]. It represents the level of security. Finally, it divided an area to several obfuscated space. For example, we set $\theta_{sens} = 0.75$. As $SL_{c_1} > \theta_{sens}$ and $SL_{c_0+c_1} < \theta_{sens}$, we should merge c_0 and c_1 to a obfuscated space. Therefore, if a user who being the region c_1 queries a request, the obfuscated space generator will send the obfuscated space $c_0 + c_1$ which contains the user's real location to the service. As the obfuscated space considers the semantic features of a location, it can protect the security of location's privacy from semantics-aware threat [17].

However, SensFlow algorithm ignores two problems, including how to select the sensitivity threshold value and protecting location privacy from the obfuscated space generator. If the sensitivity threshold value θ_{sens} is too large, the performance of privacy-preserving for location is poor. If the sensitivity threshold value θ_{sens} is too little, the quality of applications is poor. The reason is that the more little θ_{sens} , the more large obfuscated space. Therefore, the user's real location is too inaccurate. Another problem is that the obfuscated space generator is a third-party, so we cannot guarantee its security. In SensFlow algorithm, the obfuscated space generator can get the users' real location. Therefore, there is still a big threat. In this paper, we present a scheme to solve these problems.

3 Detail of SPS

In SPS scheme, we focus on two problems, including how to select the sensitivity threshold value and protecting location privacy from the obfuscated space generator. It's easily to know that θ_{sens} should be set by users. For example, for a doctor, a hospital is not a sensitive feature. However, for an ordinary citizen, a hospital is a sensitive feature as it relevant to the health status [21]. Therefore, the users should set θ_{sens} based on them requirements. In order to select the appropriate θ_{sens} , we should balance the security and the quality of service. In SensFlow, if a user queries a requirement for a service, he/she should send the real location to the obfuscated space generator storage. As the obfuscated space generator is a third-party, it is hard to guarantee the security. Therefore, we should take measures to protect the privacy for location when the user queries a requirement. This motivates our design of SPS. The scheme could be divided to three steps.

3.1 Classification

In order to satisfy the requirement of different users, we classify θ_{sens} to five levels, including 0.1, 0.3, 0.5, 0.7, and 0.9. The less θ_{sens} , the more large obfuscated space. On this occasion, the level of security is higher and the quality of services is lower. Then, the obfuscated space generator should divide the whole area to several obfuscated space. Moreover, the obfuscated space generator should storage each obfuscated space's coordinate. For each θ_{sens} , the storage mode could be seen in

Table 2. $Area_1$ is a region. It could be divided to m obfuscated space. x_i^1 and y_i^1 are the i obfuscated space's minimum horizontal ordinate and vertical coordinate. x_i^2 and y_i^2 are the i obfuscated space's maximum horizontal ordinate and vertical coordinate. n_i is a counter. The function of n_i will be explained in Requesting.

It is really hard for an obfuscated space generator to calculate the whole obfuscated space. However, each base station is in charge of each area in people-centric sensing networks. Therefore, each base station could calculate the obfuscated space for the corresponding area. Moreover, the cost of storage space is reasonable.

Table 2. The storage mode

Region	x_0^1	y_0^1	x_0^2	y_0^2	n_0	...	x_m^1	y_m^1	x_m^2	y_m^2	n_m
$Area_1$											
$Area_2$											
...											
$Area_t$											

For example, as shown in Fig. 1, when we set $\theta_{sens} = 0.7$, the region which is specified in Section 2 could be divided to two obfuscated space [17].

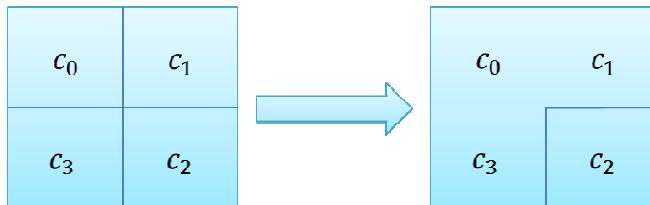


Fig. 1. An example of generating obfuscated space

3.2 Selecting

In this step, we focus on selecting the appropriate θ_{sens} . It based on Analytic Hierarchy Process (AHP). At first, we give a brief introduction about AHP. AHP is a structured technique for organizing and analyzing complex decisions [22]. Based on mathematics and psychology, it was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then. The key of AHP is confirming the three layers, including Goal, Criteria, and Alternatives. In SPS, we could introduce the three layers as follow [23].

- Goal. Selecting the appropriate sensitivity threshold value θ_{sens} .
- Criteria. We consider the requirement for security and quality of service.
- Alternatives. In this layer, it contains the different values of θ_{sens} .

Therefore, the hierarchy is shown in Fig. 2.

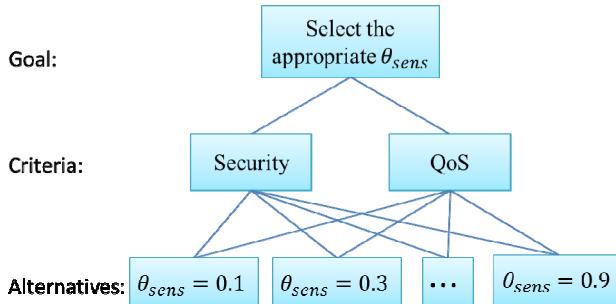


Fig. 2. The hierarchy of SPS

Then, we should establish priorities among the elements of the hierarchy by making a series of judgments based on pairwise comparisons of the elements. For criteria, we can get a decision matrix $A = (a_{ij})_{n \times n}$ based on the pairwise compared scheme. Next, we should extract the relative importance implied by the previous comparisons. At last, we should synthesize these judgments to yield a set of overall priorities for the hierarchy and checking the consistency of the judgments.

As the key of this paper is selecting the appropriate θ_{sens} , we do not introduce the detail of AHP. Based on the general procedure of AHP, it is easily to get the appropriate θ_{sens} .

3.3 Requesting

In order to preserve the privacy for location, the user cannot send the real location to the obfuscated space generator. At first, the user sends a query to the obfuscated space generator. The query uses the following form, $(UserId, \theta_{sens})$. $UserId$ is the user's identifier. θ_{sens} is the user's sensitivity threshold value. It generated by Selecting. When the obfuscated space generator receives the query, it takes out the record which is suitable to θ_{sens} . It is shown as Table 3.

Table 3. A record of obfuscated space generator

Region	x_0^1	y_0^1	x_0^2	y_0^2	n_0	...	x_m^1	y_m^1	x_m^2	y_m^2	n_m
$Area_i$											

As the obfuscated space generator is an untrusted third-part, we could not send the user's real location to the obfuscated space generator for protecting the user's privacy. Therefore, the obfuscated space generator should send the possible obfuscated spaces to users. However, sending all possible obfuscated spaces lead to large overhead, especially the bandwidth consumption. In this paper, we introduce the statistical

learning theory. That is, the number of users in some popular space is larger than the number of users in some unpopular space. Therefore, we could define the priority for different obfuscated space based on the historical information. The value of n_i is used to record the historical information.

Based on the above analysis, the obfuscated space generator chooses four items and sends them to users. The cost of each transmission is decided by the four items and it is reasonable. The four items have the largest value. Each item contains x_q^1 , y_q^1 , x_q^2 , and y_q^2 . After that, the obfuscated space generator sends a data set to the user. The format of the data set is $(id_a, x_a^1, y_a^1, x_a^2, y_a^2, \dots, id_d, x_d^1, y_d^1, x_d^2, y_d^2)$. When the user receives the data set, he/she compare the coordinate of his/her real location and the coordinate of each item in the data set. If there is an item which is satisfying the equation 1, the user sends the corresponding id to the obfuscated space generator. On the contrary, the user sends a message *null* to the obfuscated space generator. If the obfuscated space generator get an id , the corresponding n should be added one and the other three items' n should be subtracted one. Finally, the obfuscated space generator sends the corresponding obfuscated space to the server for services. If the obfuscated space generator get *null*, the four items' n should be subtract one. Then, the obfuscated space generator choose other four items based on n_i .

4 Evaluation

In this section, we evaluate the performance of SPS. The performance contains the security and the efficiency.

4.1 Security Evaluation

In our paper, we assume that the threats contain: (1) there may be the semantics-aware threat (2) the obfuscated space generator could be compromised by adversaries (3) the server could be compromised by adversaries (4) the adversary could eavesdrop all of the communications in the network [25].

For ease of threat, we explain the security features of our scheme.

- There may be the semantics-aware threat. The effectiveness of SensFlow when resisting the semantics-aware threat has been proved. Therefore, SPS can protect the privacy for location from the semantics-aware threat.
- The obfuscated space generator could be compromised by adversaries. In SPS, the user does not send the real location to the obfuscated space generator. Instead, the obfuscated space generator sends the obfuscated space to the user. Therefore, the obfuscated space generator cannot get the user's real location.
- The adversary could eavesdrop all of the communications in the network. According to the previous analysis, the user's real location does not transmit during the whole procedure. Therefore, the adversary cannot get any useful message no matter which links are eavesdropped.

In order to quantitative analysis of the capacity of location privacy preserving, we set a parameter α . The parameter is used to weigh the ratio of each place, such as mountains, hospitals and so on, occurred in obfuscated space. If the insensitive and reachable location occurred more often than the unreachable location, the scheme can protect the location privacy from the semantics-aware threat. We used several areas in Changsha as the original data. Then, we divided these areas to obfuscated space. At last, we count the times of each place occurred in these obfuscated spaces. The results are shown in Table 4.

Table 4. The result of α

The type of places	α	The percentage of area
Mountain	10%	9.6%
Road	21%	10.9%
Hospital	3%	4.7%
Park	18%	8.6%
Market	20%	11.8%
Lake	1%	8.4%
House	18%	30.8%
Others	9%	15.2%

Through questionnaire survey, we could get the rank about the sensitivity level of different places. The order is $\langle Hospital, House, Market, Mountain, Park, Road, Lake \rangle$. Therefore, if the scheme could protect location privacy from the semantics-aware threat, the rate of road, park, and mountain should larger than the real percentage of area. And other types of place should smaller than the real percentage of area. Though the Table 4, the result shows that our scheme suit this trend.

Through the above analysis, SPS is able to meet the security requirements of privacy-preserving for location in people-centric sensing networks.

4.2 Efficiency Evaluation

The efficiency evaluation contains the time complexity, the space complexity, and the cost of transmission.

At first, we evaluate the time complexity. The time complexity is mainly made up of two aspects. The first is caused by AHP. It mainly contains computing the weight of elements. In order to compute the weight of elements, we should compute the equation $W^{(k)} = (a_1^{(k)}, a_2^{(k)}, \dots, a_{n_k}^{(k)})^T = P^{(k)}W^{(k-1)}$. We assume the mumble of rules is n , the mumble of schemes is m . Therefore, the time complexity of matrix multiplication is $O(2mn)$. As the parameters in SPS are constant, the time complexity is acceptable [26]. The other one is caused by SensFlow [17]. We set the number of dividing operations to measure the cost of time. At first, we introduce a factor u which means the percentage of sensitive location. Then, we take some places as examples. And the value of u is different. At last, we count the number of dividing operations. The

results are shown in Fig. 3. The horizontal ordinate is θ_{sens} . Based on the result, we know that the number of operations is no more than 45. Especially, when the θ_{sens} is larger than 0.3, the number of dividing is no more than 25. Therefore, the time complexity of SensFlow is reasonable.

Then, we evaluate the space complexity. The space complexity contains the storage of matrix and the storage of obfuscated space in obfuscated space generator. About the storage of matrix, we assume that there is a $m \times n$ matrix. Therefore, the space complexity is $O(mn/2)$. In SPS, the order of matrix is 2. Therefore, the cost of space can be negligible. About the storage of obfuscated space, we use five different places of Changsha as the original data. Then we calculate the storage capacity. And the result is shown in Fig. 4. The result shows it only cost no more than 4M for each place. For a city, the number of place is about 1000. Therefore, we only cost about 4G. It is reasonable for the obfuscated space generator.

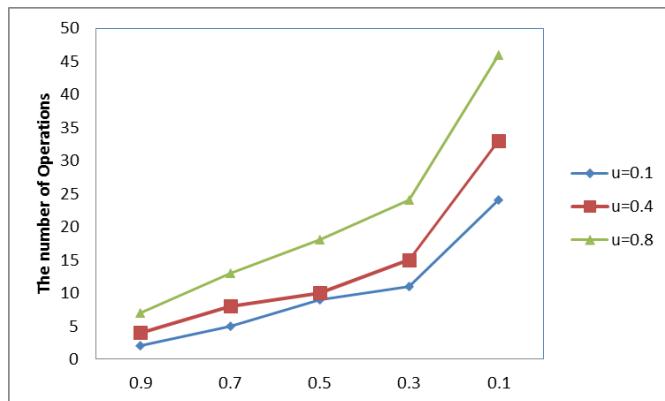


Fig. 3. The number of dividing operations

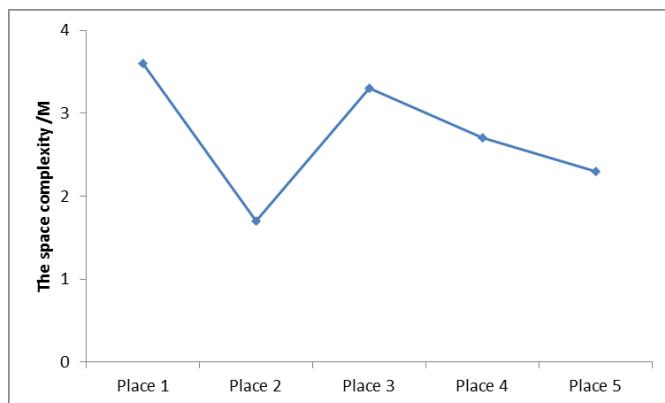


Fig. 4. The space complexity of obfuscated space

Finally, we evaluate the cost of transmission. According to the previous analysis, the number of transmission between the users and the obfuscated space generator decide the cost of transmission. In order to evaluate the number, we use an area of Changsha as an example. Assuming an ordinary citizen, we could set $\theta_{\text{sens}} = 0.5$ as an example. Therefore, there are 23 obfuscated space based on SensFlow algorithm in this area. It could be seen as Fig. 5. And the result about the number of transmission is shown in Fig. 6.

The result shows that the number of users is inversely proportional to the number of transmission. When the number of users reaches to 1000, the number of transmission is close to 1. In reality, the number of users is large enough. For example, the number of users who may use the people-centric sensing networks is more than fifty thousand. Therefore, the cost of communication is reasonable. That is, the user could get the appropriate obfuscated space through about 1 transmission.



Fig. 5. The obfuscated space of this area

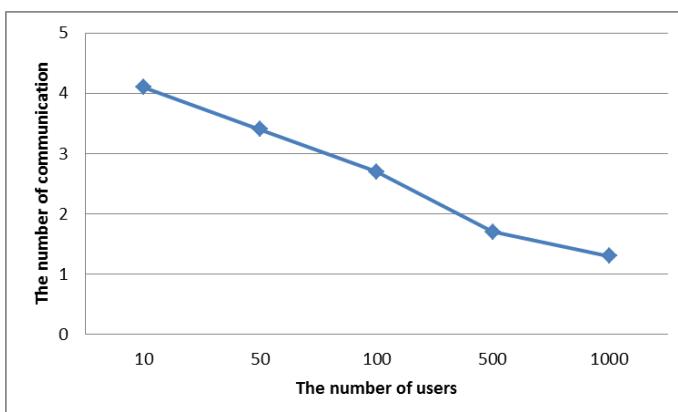


Fig. 6. The average number of transmission

5 Conclusion

We present SPS, a novel Semantics-aware scheme for location privacy in People-centric Sensing network. SPS can support strong user location privacy against the semantics-aware threat. The original contribution of the paper is a novel scheme for selecting the sensitivity threshold value and privacy-preserving for location from the obfuscated space generator. Moreover, we evaluate the performance of SPS. The result shows that SPS could resist the semantics-aware threat under a reasonable cost. We believe a privacy-aware scheme will make People-centric Sensing networks more acceptable, as users are confronted with litter risk to their location privacy.

Acknowledgments. The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No. 2012CB315906; the project of National Science Foundation of China under grant No. 61103189, 61103194, 61103182, 61202488, 61272482; the National High Technology Research and Development Program of China (863 Program) No. 2012AA01A506, 2013AA013505, the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20114307110006, 20124307120032, the program for Changjiang Scholars and Innovative Research Team in University (No.IRT1012), Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province(“network technology”); and Hunan Province Natural Science Foundation of China (11JJ7003).

References

1. Abdelzaher, T., et al.: Mobicopes for human spaces. *IEEE Pervasive Computing* 6(2), 20–29 (2007)
2. Campbell, A.T., et al.: The rise of people-centric sensing. *IEEE Internet Computing* 12(4), 12–21 (2008)
3. Eisenman, S.B., et al.: BikeNet: A mobile sensing system for cyclist experience mapping. *ACM Transactions on Sensor Networks (TOSN)* 6(1), 6 (2009)
4. Welsh, M., Bers, J.: CitySense: an urban-scale sensor network. In: Harvard Graduate School of Design, pp. 164–165. Lars Müller Publishers, Zurich (2010)
5. Mun, M., et al.: PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. In: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services. ACM (2009)
6. Microsoft Research Sense Web project (2007), <http://research.microsoft.com/nec/senseweb/.website> (visited March 2013)
7. Crepaldi, R., et al.: Illinois vehicular project, live data sampling and opportunistic internet connectivity. In: Proceedings of the Third ACM International Workshop on Mobile Opportunistic Networks. ACM (2012)
8. Schiller, J., Voisard, A. (eds.): Location-based services. Elsevier (2004)
9. Gokul, S.: Location Dependent Query Processing. Diss. Cochin University of Science and Technology (2011)

10. Morris, J., et al.: An Architecture for Location and Location Privacy in Internet Applications (2011)
11. Mascetti, S., et al.: Providenthider: An algorithm to preserve historical k-anonymity in lbs. In: Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM 2009. IEEE (2009)
12. Lu, R., et al.: Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology* 61(1), 86–96 (2012)
13. Brush, A.J., Krumm, J., Scott, J.: Exploring end user preferences for location obfuscation, location-based services, and the value of location. In: Proceedings of the 12th ACM International Conference on Ubiquitous Computing. ACM (2010)
14. Quercia, D., et al.: Spotme if you can: Randomized responses for location obfuscation on mobile phones. In: 2011 31st International Conference on Distributed Computing Systems (ICDCS). IEEE (2011)
15. Sheth, A., Ilarri, S., Mena, E.: Semantics in Location-Based Services. *IEEE Internet Computing* 15(6), 0010–14 (2011)
16. Basu Roy, S., Chakrabarti, K.: Location-aware type ahead search on spatial databases: semantics and efficiency. In: Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data. ACM (2011)
17. Damiani, M.L., Silvestri, C., Bertino, E.: Semantics-aware obfuscation for location privacy. *Journal of Computing Science and Engineering* 2(2), 137–170 (2008)
18. Le, T.T.B., Dang, T.K.: Semantic-aware obfuscation for location privacy at database level. In: Mustofa, K., Neuhold, E.J., Tjoa, A.M., Weippl, E., You, I. (eds.) *ICT-EurAsia 2013. LNCS*, vol. 7804, pp. 111–120. Springer, Heidelberg (2013)
19. Xu, T., Cai, Y.: Feeling-based location privacy protection for location-based services. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 348–357. ACM (2009)
20. Wang, Y., Xu, D., He, X., et al.: L2p2: Location-aware location privacy protection for location-based services. In: 2012 Proceedings IEEE INFOCOM, pp. 1996–2004. IEEE (2012)
21. Che, Y., et al.: SALS: semantics-aware location sharing based on cloaking zone in mobile social networks. In: Proceedings of the First ACM SIGSPATIAL International Workshop on Mobile Geographic Information Systems. ACM (2012)
22. Ishizaka, A., Labib, A.: Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications* 38(11), 14336–14345 (2011)
23. Saaty, T.L., Vargas, L.G.: How to Make a Decision[M]//Models, Methods, Concepts & Applications of the Analytic Hierarchy Process, pp. 1–21. Springer, US (2012)
24. Wang, L., Chu, M.T.: On the global convergence of the high-order power method for rank-one tensor approximation. North Carolina State University (2013) (preprint)
25. Wei, Z., Zhao, B., Su, J.: PDA: A Novel Privacy-Preserving Robust Data Aggregation Scheme in People-Centric Sensing System. *International Journal of Distributed Sensor Networks* 2013 (2013)
26. Saaty, T.L.: Analytic hierarchy process. *Encyclopedia of Operations Research and Management Science*, pp. 52–64. Springer, US (2013)

A Novel Resource-Efficient Privacy Amplification Scheme: Towards Ground-Satellite Quantum Key Distribution Post-processing

Zhenning Zhang, Chunqing Wu, Baokang Zhao^{*}, and Bo Liu

School of Computer, National University of Defense Technology, Changsha, China
{yuyinning, liub0yayu}@gmail.com,
{wuchunqing, bkzhao}@nudt.edu.cn

Abstract. Quantum key distribution (QKD) provides the intrinsically unconditional secure method to generate and transfer cryptographic keys based on laws of quantum mechanics. The introduction of QKD technology in satellite communications has changed the way to understand them, permitting secure and reliable global communications. In a real-life situation, however, ground-satellite QKD needs to handle a critical issue: the problem of on-board resource insufficiency. Privacy amplification (PA) determining the final key rate is a significant procedure in QKD post-processing. Though fast Fourier transform (FFT) technology can expedite PA procedure, it costs more computing and storage resources. With a novel division and aggregation scheduling (DAS) policy, we made some modifications to FFT implementation and proposed a resource-efficient PA scheme (called as DAS-FFT PA), which efficiently reduces the resource overhead of implementing overall PA module. Our experimental results demonstrate and confirm that our proposed scheme fulfills the expected target.

Keywords: satellite communications, free-space quantum key distribution, resource-efficient privacy amplification, division and aggregation scheduling.

1 Introduction

Security and privacy are important concerns in wireless communications and particularly so in satellite communication systems [1,2], where eavesdropping can be easily performed because of the broadcast nature of satellites. Quantum Key Distribution (QKD) [3,4] technology, based on the laws of quantum mechanics, can establish unconditional security keys between communication parties. Since proposal of the first practical QKD protocol: the so-called BB84 protocol presented by Bennett and Brassard in 1984 [3], this area has spurred a number of activities both theoretically and experimentally. There have been significant progresses for practical free-space QKD [5,6,7,8,9,10,11,12],[15], such as utilizing free-space quantum

* Corresponding author.

communications with satellites and ground stations to achieve long-distance QKD has been theoretically studied and experimentally proven feasible [13,14][17], which forms a solid basis for QKD based wireless communication security. Unfortunately, the feasibility of ground-satellite QKD over free-space paths might be considered problematic due to the high resource overhead of implementing QKD.

Privacy amplification (PA) [18] is a symmetric procedure in QKD post-processing which have to be performed by both ground station and satellite. Involving the same amount of computation on the satellite as on the ground, PA could potentially create a bottleneck on the satellite. After the information reconciliation step, Alice and Bob share the error-corrected key. Since some information might have been leaked out to the Eve during error correction, the error-corrected key is only partially secure. Then a procedure called as privacy amplification is employed to reduce the partial information about the key leaked to eavesdropper. By applying a so-called two-universal hash function to the partially-secure key, PA produces a provably secure key. Majority research employs Toeplitz matrices [19] as two-universal hash functions and conducts PA procedure with linear feedback shift register (LFSR) structures [20]. Tsurumaru suggests a further optimization that we can speed up Toeplitz multiplication by applying fast Fourier transform (FFT) technology [21]. Comparing with previous implementations, this method is faster as it runs in time $O(n \lg^n)$. With limited computing and memory resource, however, speeding up PA procedure by FFT processor is still a huge challenge.

In this paper, we focus on the resource overhead of the realization of PA. A novel resource-efficient PA scheme with limited resource is designed and incorporated into QKD post-processing, which allows efficient computing. Utilizing DAS, PA is divided into several subtasks with the same operation. All the similar subtasks can be processed by the single dedicated processing unit and then reusing the dedicated processing unit can save hardware resource. We implemented our scheme in real QKD system, the RT-QKD system [22,23], which is an evolution of CLIP system [24]. The experimental results show that this implementation with a decrement in resource overhead is quite efficient as well.

The organization of the paper is as follows. We give a brief introduction to ground-satellite QKD and PA including one of its high performance realization in Section 2. In Section 3, we describe the DAS strategy and use it to derive a simple but optimal divide-and-conquer scheme of PA: DAS-FFT PA scheme. We present the performance evaluation of DAS-FFT PA scheme in Section 4. Conclusions can be found in Section 5.

2 Preliminaries

2.1 Ground-Satellite QKD

QKD could in principle provide intrinsically unconditional security, compared with any of classical private communication methods that derive their security from the perceived intractability of certain problems in number theory, or from the physical

security of the distribution process [3]. Researchers have demonstrated that QKD can be performed over multi-kilometer distances of optical fiber [25]. Currently, the maximum distance for fiber-based QKD is around an order of 100km [26,27]. This distance almost reaches its limit due to huge photon loss, noise of available single photon detector, and the optical fiber's decoherence effect [12]. Fortunately, this limit could be overcome by introducing ground-satellite QKD [6]. Compared with fiber-based QKD [25,26,27], ground-satellite QKD could provide the most appealing solution for much longer distance.

There have been significant theoretical progresses for feasibility of ground-satellite QKD, along with some preliminary experimental tests. It is demonstrated by Hughes et al. the feasibility of practical free-space QKD over a 10 km path in daylight and at night [5]. In the meantime, the first experimental quantum entanglement distribution over 13 km is presented [6]. More recently, Zeilinger etc. reported the successful experimental implementation of a free-space BB84 quantum key distribution over a distance of 144km [8,9,10], which reveals a fact that atmospheric turbulence has little effect on free-space link.

These experiments have accelerated the application of free-space QKD in security and privacy of satellite communications and thus secret keys can be established between any two wireless nodes. The utility of the free-space QKD would greatly enhance the security and privacy of satellite communications. In the near future, we believe that this will bring a revolution in the scope of satellite communications security and privacy.

2.2 Privacy Amplification

After the Error Correction [28], Alice and Bob share the error-corrected key W . However, W is not unconditional safe, since some information might have been leaked out to the Eve. Privacy amplification is employed to reduce the information leaked to the eavesdropper as much as possible and is a procedure which needs to be performed by both Alice and Bob. It consists of applying a specific two-universal function to the error-corrected key W to produce a provably secure key R whose length is l .

Two-universal hash functions [12] are employed in PA. Since the resources are limited, major considerations for the choice of hash function are the computational complexity and the classical communication overhead. Toeplitz matrices [19] are in fact two-universal hash functions and we employ the Toeplitz matrices construction.

Toeplitz matrices have constant diagonals. A binary Toeplitz matrix A has elements $a_{i,j} \in \{0,1\}$ such that

$$a_{i,j} = a_{m,n} \quad (1)$$

for

$$\forall(i, j, m, n) : m - i = n - j . \quad (2)$$

A Toeplitz matrix can be written in the following form:

$$H = \begin{bmatrix} h_l & h_{l+1} & \cdots & \cdots & \cdots & \cdots & h_{n+l-2} & h_{n+l-1} \\ h_{l-1} & h_l & \ddots & & & & h_{n+l-3} & h_{n+l-2} \\ \vdots & h_{l-1} & \ddots & \ddots & & & \vdots & \vdots \\ h_2 & \vdots & \ddots & h_l & h_{l+1} & & & h_{n-2} \\ h_1 & h_2 & \cdots & h_{l-1} & h_l & h_{l+1} & \cdots & \cdots & h_{n-1} \end{bmatrix}_{l \times n} \quad (3)$$

Since Toeplitz matrices can be defined by expressing only the first row and first column, we can describe a Toeplitz matrix using only an array of $(n+l-1)$ -bits. Then we can define a hash function which uses Toeplitz matrices.

2.3 FFT-Based Implementation of PA Scheme

Tsurumaru suggests a further optimization whose main idea is converting Toeplitz matrix multiplication into multiplication of polynomials: the Toeplitz matrix product should be corresponding polynomial product. Then we could quickly multiply two polynomials of degree-bound n in time $O(n \lg^n)$ [21] with both the input and output representations in coefficient form.

The FFT algorithm is a significant improvement on the Discrete Fourier Transform (DFT) with respect to computational complexity. However, implementing a FFT engine with multiple butterfly units still costs a lot of resource. Due to finite-size effects, the error-corrected key has to be kept above a certain value (on the order of 10^5) and it costs a great amount of hardware to implement the logical circuits which was something we did not want to assume. Moreover, the larger scale of PA, the more number of sampling points needs to be stored and operated in the FFT engine, thus, increased the computational complexity of the implementation.

PA is a symmetric procedure which needs to be performed by both parties. Thus, a great amount of work has gone into reducing its complexity. As mentioned above, majority research about implementing PA focusing on improving the final key generation rate, however, implementing a resource-efficient PA scheme in ground-satellite QKD systems has been more and more significant. Based on Division and Aggregation Scheduling (DAS) policy and FFT technology, we proposed and implemented a novel resource-efficient privacy amplification (PA) scheme (called as DAS-FFT PA). The advantage of the proposed scheme is that we can achieve almost the same performance with much less resource overhead.

3 The Proposed Resource-Efficient Privacy Amplification Scheme

Divide-and-conquer [29] is a useful strategy for designing resource-efficient algorithms. Applying this strategy, the problem is recursively subdivided into

relatively independent components, then we can operate on them in turn. By reusing the implemented single FFT processor, the space overhead reduced.

In this section, we begin by providing some notations which will be used later. Then, we give the detailed description of the proposed resource-efficient PA scheme based on DAS and FFT.

3.1 The Description of Proposed Scheme

We assume the security key string before PA is W whose length is n and the Toeplitz matrix used for PA is H whose length is $n+l-1$. The final secure key we gain after PA is called R .

The proposed DAS-FFT PA Scheme consists of the following five phases: conversion, division, multiplication, aggregation, inverse conversion.

Conversion. Create coefficient representations of H and W as degree-bound Mk and Nk polynomials by adding high-order zero coefficients. That is

$$H \rightarrow H(x) = \sum_{i=0}^{Mk-1} h_i x^i \quad (4)$$

$$\text{where } h_i = \begin{cases} 0/1 & i \in [0, n+l-2] \\ 0 & i \in [n+l-1, Mk-1] \end{cases} \text{ for } i \in N,$$

$$W \rightarrow W(x) = \sum_{j=0}^{Nk-1} w_j x^j \quad (5)$$

$$\text{where } w_j = \begin{cases} 0/1 & j \in [0, n-1] \\ 0 & j \in [n, Nk-1] \end{cases} \text{ for } j \in N.$$

M and N are respectively the number of division groups of $H(x)$ and $W(x)$. $K(=2k)$ is the number of points of per FFT processor.

Division. $H(x)$ is divided into M groups, $W(x)$ is divided into N groups, each for a group of k . That is

$$H(x) = \sum_{m=0}^{M-1} H_m, \quad (6)$$

$$W(x) = \sum_{n=0}^{N-1} W_n. \quad (7)$$

Then

$$H(x)W(x) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} H_m(x)W_n(x). \quad (8)$$

For $\forall H(x)W(x)$,

$$H_m(x)W_n(x) = x^{k(m+n)} Htr_m(x)Wtr_n(x). \quad (9)$$

Define $x^{k(m+n)}$ Aggregation factor, we write that ξ , then

$$H_m(x)W_n(x) = \xi Htr_m(x)Wtr_n(x) \quad (10)$$

for $Htr_m(x)$ and $Wtr_n(x)$ are polynomials of degree-bound k .

Multiplication. Compute $Htr_m(x)Wtr_n(x)$ using the multiplication method for polynomials in point-value form. That is

$$Htr_m(x)Wtr_n(x) \rightarrow Rtr_{m+n}(x). \quad (11)$$

Aggregation. Combine terms with equal powers. That is

$$R_{m+n}(x) = \sum_{p,q} Rtr_{p+q}(x) \quad (12)$$

for $p+q=m+n$.

Thus

$$R(x) = H(x)W(x) = \sum_{j=0}^{M+N-2} x^{kj} R_j(x) \quad (13)$$

Inverse Conversion. Get the final key R by processing l coefficients of $R(x)$ for $n-1 \leq l < n+l-1$. That is $R(x) \rightarrow R$.

3.2 Computational Complexity

We present a scheme based on time-space trade-offs whose goal is to reduce resource overhead. The time complexity of the proposed scheme is $O(klg^k)$ where k is the number of sampling points of FFT operation including $M+N$ times FFT operation, MN times multiplication operation and MN times inverse FFT operation.

Since the scheme contains only same operation like FFT, multiplication and inverse FFT, we can reduce the resource overhead of realization of this scheme by implementing and reusing single dedicated processor with smaller scale. This scheme can be implemented with a smaller FFT processor, which is what we expected. Thus, implementing the application specific processor costs less resources and can be implemented in hardware for better performance.

4 Performance Evaluation

4.1 Experiment Setup

In PA procedure, Hash functions are transmitted through public ground-satellite channels which is distinct from the usual fiber channels. We applied a wireless channel to simulate the public ground-satellite channel whose uplink bit rates is 1Mbps, downlink bit rates is 10Mbps and delay is 50ms. We implemented our schemes based on RT-QKD [7], a real-time QKD system connecting to the quantum communication system which conducts BB84 protocol [10]. Our proposed resource-efficient PA scheme replaces the previous PA module and we will measure the time overhead with different solutions. CLIP [8] provides the weak security keys needed by our distributed PA scheme. Fig. 1 shows the whole experiment environment.

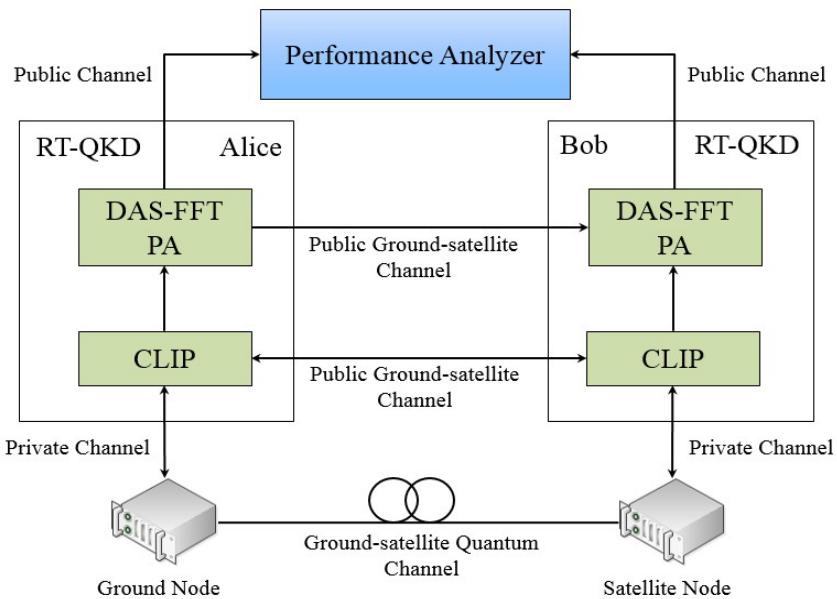


Fig. 1. The experiment environment of the proposed PA scheme

4.2 The Computational Complexity of Different Implementation Scheme

PA can be implemented based on FFT and DAS-FFT as we proposed above. Different implementation of PA leads to different computational complexity, thus we can test how efficient different architecture are.

In this test, we choose 2 and 4 as the numbers of division groups, because these strategies won't take too much time to accomplish a PA process and costs less (little more than 1/2 and 1/4 as we tested) resource overhead. PA based on FFT is also implemented in RT-QKD, thus we can compare them.

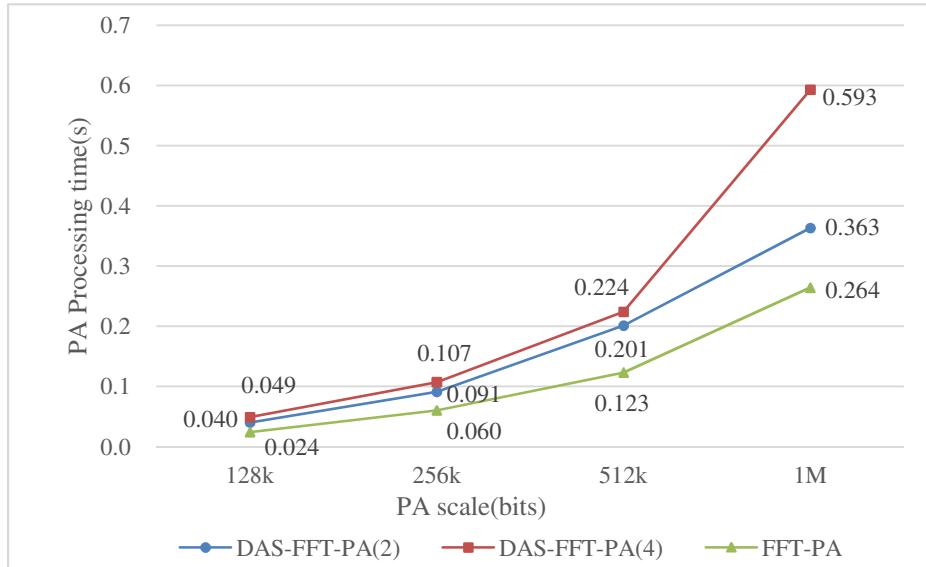


Fig. 2. The PA processing time with PA scale

As shown in Fig. 2, the PA processing time increases with increasing PA scale. With the same PA scale, DAS-FFT PA always costs more time to perform PA than the method based on FFT. And when the PA scale doubled, the DAS-FFT PA processing time increased faster while it needs more time to do DAS. However, when the PA scale is no more than 512k, their computational complexity is quietly similar because the time overhead of DAS is negligible.

4.3 The Effect of Numbers of Division Groups

Various numbers of division groups cost different time overhead to do per PA process. The time complexity of every FFT process is merely $O(n \lg^n)$ and extra time taken to do the division and aggregation scheduling (DAS). And then we think that the more groups divided, the longer time will be taken to process the PA. In this experiment, we focus on the number of groups of DAS which we think has an effect on the time complexity.

As shown in Fig. 3, we can see the processing time of PA with different numbers of division groups. When the number of division groups increased, the PA processing time increased simultaneously. When the PA scale is no more than 512k, the time increment of DAS is indistinctive. But when the PA scale became larger, the PA processing time increased distinctly because of the larger time overhead of DAS with increasing number of division groups. Hence we can achieve almost the same performance with much less resource overhead by dividing the FFT inputs into more groups while the required PA scale is not so large.

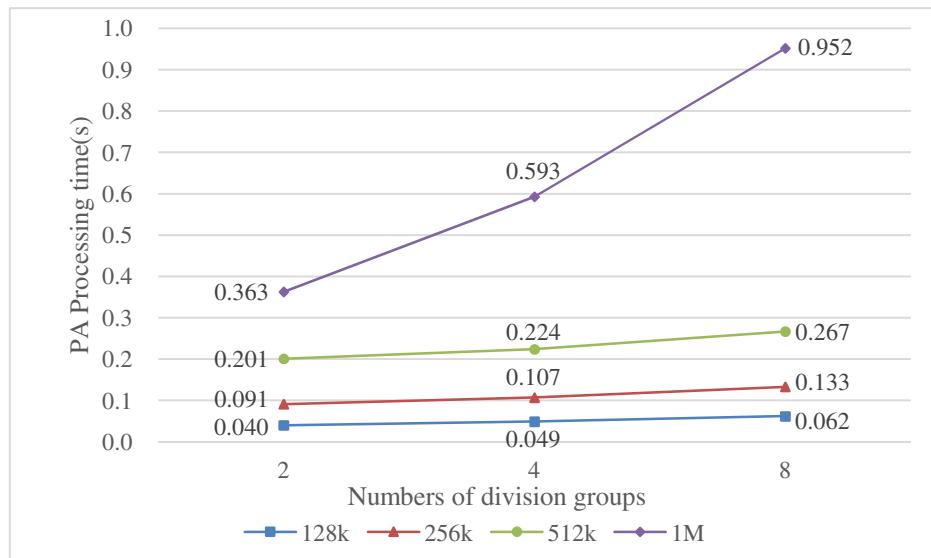


Fig. 3. The PA processing time with different numbers of division groups

5 Conclusion

Since the first experimental demonstrations of ground-satellite quantum key distribution (QKD), researchers have progressively realized that the utility of the ground-satellite QKD would greatly enhance satellites communication security and ground-satellite QKD is predicted to be the critical technology of the next-generation wireless security and privacy. However, with limited resources, the realization of ground-satellite QKD, remained an experimental challenge under real-world conditions. In this paper, based on Division and Aggregation Scheduling (DAS) policy and FFT technology, we proposed and implemented a novel resource-efficient privacy amplification (PA) scheme (called as DAS-FFT PA) in RT-QKD system. The advantage of the proposed scheme is that high computational efficiency can be guaranteed with a low resource overhead by the cost of an increased transfer time for the DAS policy.

Acknowledgment. The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No. 2012CB 315906; the project of National Science Foundation of China under grant No. 61103189, 61103194, 61103182, 61202488, 61272482; the National High Technology Research and Development Program of China (863 Program) No. 2012AA01A506, 2013AA013505.

References

1. Liang, L., Iyengar, S., Cruickshank, H., Sun, Z., Kulatunga, C., Fairhurst, G.: Security for flite over satellite networks. In: WRI International Conference on Communications and Mobile Computing, CMC 2009, vol. 3, pp. 485–491. IEEE (2009)
2. Mahmoud, B., Larrieu, N., Pirovano, A.: An aeronautical data link security overview. In: IEEE/AIAA 28th Digital Avionics Systems Conference, DASC 2009, p. 4-A. IEEE (2009)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175(150), p. 8 (1984)
4. Gisin, N., Ribordy, G., Zbinden, H.: Quantum cryptography. *Reviews of Modern Physics* 74, 145–195 (2001)
5. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics* 4(1), 43 (2002)
6. Peng, C.Z., Yang, T., Bao, X.H., Zhang, J., Jin, X.M., Feng, F.Y., ... Pan, J.W.: Experimental free-space distribution of entangled photon pairs over 13 km: towards ground-satellite global quantum communication. *Physical Review Letters* 94(15), 150501 (2005)
7. Marcikic, I., Lamas-Linares, A., Kurtsiefer, C.: Free-space quantum key distribution with entangled photons. *Applied Physics Letters* 89(10), 101122 (2006)
8. Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., ... Weinfurter, H.: Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* 98(1), 010504 (2007)
9. Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., ... Zeilinger, A.: Entanglement-based quantum communication over 144 km. *Nature Physics* 3(7), 481–486 (2007)
10. Fedrizzi, A., Ursin, R., Herbst, T., Nespoli, M., Prevedel, R., Scheidl, T., ... Zeilinger, A.: High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics* 5(6), 389–392 (2009)
11. Jin, X.M., Ren, J.G., Yang, B., Yi, Z.H., Zhou, F., Xu, X.F., ... Pan, J.W.: Experimental free-space quantum teleportation. *Nature Photonics* 4(6), 376–381 (2010)
12. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. *Reviews of Modern Physics* 81(3), 1301 (2009)
13. Villoresi, P., Jennewein, T., Tamburini, F., Aspelmeyer, M., Bonato, C., Ursin, R., ... Barbieri, C.: Experimental verification of the feasibility of a quantum channel between space and Earth. *New Journal of Physics* 10(3), 033038 (2008)
14. Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G., Villoresi, P.: Feasibility of satellite quantum key distribution. *New Journal of Physics* 11(4), 45017 (2009)
15. Nordholt, J.E., Hughes, R.J., Morgan, G.L., Peterson, C.G., Wipf, C.C.: Present and future free-space quantum key distribution. In: High-Power Lasers and Applications, pp. 116–126. International Society for Optics and Photonics (2002)
16. Rarity, J.G., Tapster, P.R., Gorman, P.M., Knight, P.: Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics* 4(1), 82 (2002)
17. Hughes, R.J., Nordholt, J.E., Mc Cabe, K.P., Newell, R.T., Peterson, C.G.: Ground-satellite quantum communications. In: UQCC 2010, Los Alamos National Laboratory, LANL (2010)

18. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. *IEEE Transactions on Information Theory* 41, 1915–1923 (1995)
19. Gray, R.M.: Toeplitz and circulant matrices: A review. *Foundations and Trends in Communications and Information Theory* 2 (2006)
20. Krawczyk, H.: LFSR-based hashing and authentication. In: Desmedt, Y.G. (ed.) *CRYPTO 1994. LNCS*, vol. 839, pp. 129–139. Springer, Heidelberg (1994)
21. Golub, G.H., Van Loan, C.F.: *Matrix computations*, vol. 3. JHU Press (2012)
22. Liu, B., Liu, B., Zhao, B., Zou, D., Wu, C., Yu, W., You, I.: A real-time privacy amplification scheme in quantum key distribution. In: Mustafa, K., Neuhold, E.J., Tjoa, A.M., Weippl, E., You, I. (eds.) *ICT-EurAsia 2013. LNCS*, vol. 7804, pp. 453–458. Springer, Heidelberg (2013)
23. Liu, B., Zhao, B., Wei, Z., Wu, C., Su, J., Yu, W., ... Sun, S.: Qphone: a quantum security VoIP phone. In: *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, pp. 477–478. ACM (2013)
24. Zou, D., Zhao, B., Wu, C., Liu, B., Yu, W., Ma, X., Zou, H.: CLIP: A Distributed Emulation Platform for Research on Information Reconciliation. In: *2012 15th International Conference on Network-Based Information Systems (NBiS)*, pp. 721–726. IEEE Press, New York (2012)
25. Takesue, H., Nam, S.W., Zhang, Q., Hadfield, R.H., Honjo, T., Tamaki, K., Yamamoto, Y.: Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature Photonics* 1, 343–348 (2007)
26. Stucki, D., Walenta, N., Vannel, F., Thew, R.T., Gisin, N., Zbinden, H., ... Ten, S.: High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics* 11(7), 75003 (2009)
27. Liu, Y., Chen, T.Y., Wang, J., Cai, W.Q., Wan, X., Chen, L.K., ... Pan, J.W.: Decoy-state quantum key distribution with polarized photons over 200 km. *Optics Express* 18(8), 8587–8594 (2010)
28. Sun, S.H., Ma, H.Q., Han, J.J., Liang, L.M., Li, C.Z.: Quantum key distribution based on phase encoding in long-distance communication fiber. *Optics Letters* 35(8), 1203–1205 (2010)
29. Smith, D.R.: The design of divide and conquer algorithms. *Science of Computer Programming* 5, 37–58 (1985)

Protecting Location Privacy Based on Historical Users over Road Networks

Qilong Han, Hongbin Zhao, Zhiqiang Ma, Kejia Zhang, and Haiwei Pan

College of Computer Science and Technology, Harbin Engineering University, Harbin 150001
hanqilong@hrbeu.edu.cn

Abstract. Recently, with the extensive application of the location based services (LBS), more and more location privacy problems have happened. To use LBSs, users must send their location information to service provider, but users' location information is private. The current methods have some flaws, such as in Euclidean space and so on. In this paper, a based historical user dummy generation (BHUDG) scheme is proposed, which can provide location privacy by utilizing density-based clustering method in a real road network environment. We investigate the effectiveness of BHUDG based on extensive simulation study. Simulation results show that our proposed scheme has a better performance.

Keywords: location based services, location privacy, road network, density-based clustering.

1 Introduction

Improvements in sensor and wireless communication technology enable accurate, automated determination and dissemination of a user's or object's position. There is an immense interest in exploiting this positional data through location-based services (LBS). For instance, LBSs could tailor their functionality to the user's current location, or vehicle movement data would improve traffic forecasting and road planning. The application of LBSs is a double-edge sword because it attaches much importance to internet or wireless networks. On the one hand, it gives us convenience; on the other hand, it provides a chance to get the users' privacy illegally, including identity and location information. It will affect the application of LBSs. Therefore, the privacy preserving problem of LBS has become a hot topic in academia and industry.

At present, the research of LBS privacy preserving mostly assumes that the user or object moves in Euclidean space where the direction of movement is unconstrained; however, it is might poor work in a real environment for most of movement objects, such as vehicles, person, etc. moving in road networks. In this paper, we propose a method of moving objects privacy preserving, which anonymize the users' location information in real environment and consider the speed consistency of real users and dummies, at the same time, by analyzing a number of location information of the historical users, the authenticity of dummies is ensured.s

2 Related Work

In this section, we summarize the recent research of location privacy methods with dummies. In [2], Kido, Hidetoshi et al. who are the first to use dummies in protecting location privacy put forward two simple algorithms, which are Moving in a Neighborhood (MN) algorithm and Moving in a Limited Neighborhood (MLN) algorithm. However, by monitoring long-term movement patterns of users, the trajectories of mobile users can still be exposed. In [3], two schemes are proposed, namely, random and rotation pattern, to generate consistent movement patterns in a long run. In random scheme, the start point and the destination of a dummy are firstly selected, and then the dummy moves randomly from the starting point towards the destination. However, without involving factor such as distance deviation, the scheme simply includes more dummies when the privacy requirements are not satisfied. In rotation scheme, a new trajectory is generated for a dummy by rotating the present user trajectory. With proper selection of dummy trajectories, we can minimize the number of dummies so as to satisfy the users' privacy requirements.

In [4], the PAD approach is proposed, which is capable of offering privacy-region guarantees. PAD uses so-called dummy locations that are deliberately generated according to either a virtual grid or circle. However factor such as road network environment is not taken into account.

In [5], a method is proposed to protect the users' location privacy by sending the users' location with dummy locations in real environment, which are determined based on the user's current location. At the same time, movement consistency that includes speed and direction is also proposed to enhance the authenticity of dummies. However, direction consistency is unfeasible in real environment, there are two reasons, firstly, it will be restricted in real road network environment; secondly, if dummy follow direction consistency, the malicious attacker can easily judge which is a dummy. For example, according to the users' queries, server will return the result to the user, and the user is moving in accordance with his own direction, but dummy's and the users' query results may not be the same, so moving in the same direction will leak user privacy.

In [6], the matrix is used to study the real user movement behavior characteristics. In other words, after statistics analysis of user distribution spatial sampling, the distribution matrix and distribution probability matrix is formed. But if the users' privacy demand is very high and the division of the space is very intensive, the matrix may not achieve. The most important is that it sometimes can't find users distribution dense area. We assume that dummies are generated in historical user dense region, solid line area represent historical user in Figure 1 showing an example of distribution. In Figure 1(1), A is the most densely area where historical user distributed, so dummies are generated in A. However, in Figure 1(2) when we change the division of the grid, the result is very different. Visibly, the most intensive is I, and no historical user is found in G, H, J, K, and L. If we generate dummies in these regions, it will violate our assumptions. It seems that the method which combine grid divided and the matrix is not optimal. Due to the deficiencies and disadvantages of the above methods, we adopt the density-based clustering method.

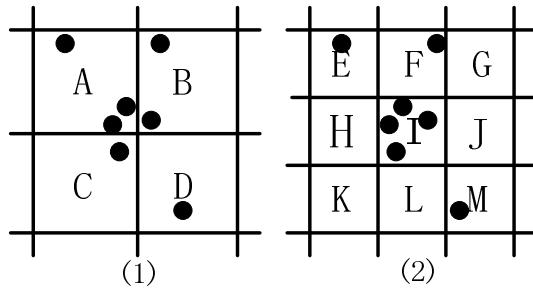


Fig. 1. Division of application space

3 BHUDG Location Privacy Protection Method

3.1 System Architecture of BHUDG Method

This paper proposes the system architecture of the BHUDG method, and it consists of two parts: mobile users and service providers, shown in Figure 2. Mobile user is composed of mobile terminals such as mobile phones with positioning, including a middleware.

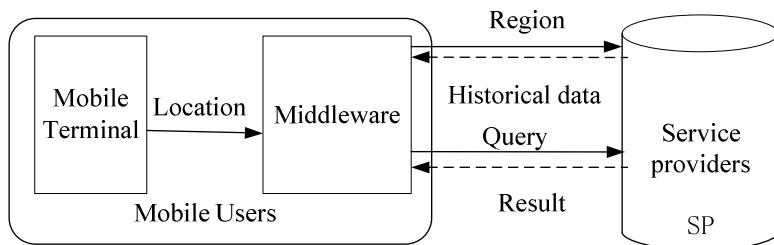


Fig. 2. System architecture of BHUDG method

Mobile terminal transfers location information to the service providers by the middleware, which requires storage and computing functions, and enables the middleware to send fuzzy information including the accurate point to service providers. Then historical location information of the user is returned to the middleware by service provider. Finally, the query results are acquired.

3.2 Related Definition

Definition 1. (The Query) A query Q is represented to a five-tuple $\langle UID, loc, t, Tth, query \rangle$, where UID represents the identifier of the user; loc is a two-tuple $\langle longitude, latitude \rangle$, which represents the latitude and longitude of the location; t represents the moment of the query, Tth represents the query interval threshold, and specified by the user; $query$ is the content of the query that user submits.

Definition 2. (The Privacy Requirement) A privacy requirements PR is represented as a 3-tuple $\langle k, Eps, MinPts \rangle$, where k is anonymous parameter that represents the number of all of users; Eps is neighborhood radius in DBSCAN algorithm; $MinPts$ is neighborhood density threshold in DBSCAN algorithm, the above three parameters are specified by the user.

Definition 3. (The Points of Interest, POI) For the user, POI is a set of potential and relevant points that the user may submit as queries in the road network, such as some service premises, landmark buildings or tourist attractions, etc.

Definition 4. (Security Road Network, SRN) A security road network SRN is represented as $\langle V, E, loc, d_{min}, d_{max} \rangle$, where vertices set V is a set of POI ; edge set E is a set of each connection between adjacent POI ; d_{min} is minimum distance of dummy to the real user; d_{max} is maximum distance of dummy to the real user; Three-tuple $\langle loc, d_{min}, d_{max} \rangle$ represents that generated dummies are in a range of d_{min} to d_{max} .

For example, we assume that $d_{max} = d_1$ and $d_{min} = d_2$, and it is formed a ring area, as shown in Figure 3. The method ensures that the distance from dummies to real user location is not too far away to protect user privacy, nor too near to leak user privacy.

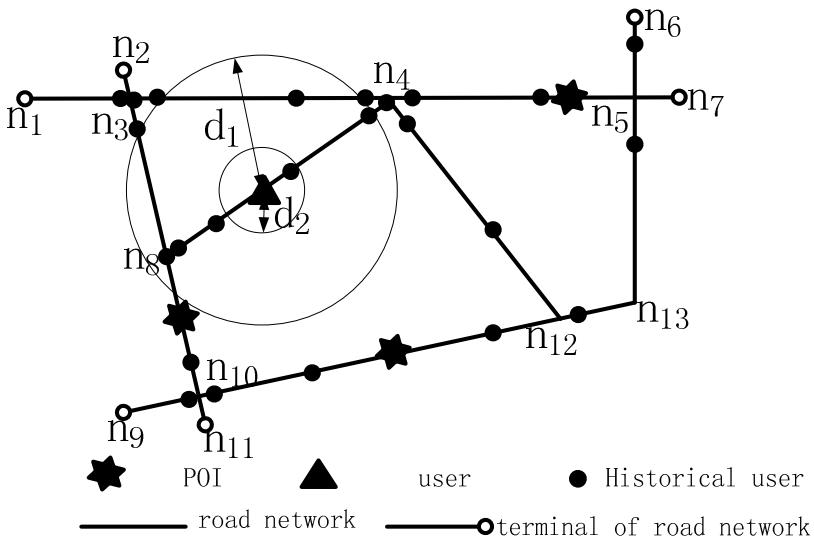


Fig. 3. Security Road Network model

Definition 5. (Speed Consistency) In [5], speed consistency is defined that each dummy continuously moves in almost the same speed as the user. For example, when a user has requested LBS at a certain time and then requests the service again three minutes later, the dummy location more than 10km away from at the previous location is apparent to be a dummy.

3.3 Clustering on the Historical User Location Data

Analyzing the research of previous work, we find the disadvantages of the method combining divided grid and the matrix, so we put forward density-based clustering method to locate dense region in which historical users' distribute. It is rapid and effective to find any shape cluster, moreover it is simple to implement.

We assume that a mobile terminal provides a pre-installed map data. The distribution of users is different in different time, and even at the same time on each road, so the distribution of users is affected by time and geographical condition.

We assume that users submit queries in security road network SRN . Fitly we set corresponding parameters of PR , then use DBSCAN clustering algorithm to find dense regions in which historical user distributed. Finally we get m clusters that are in irregular shape. The number of historical users is N_i in the i -th cluster, anonymous parameters $PR.k$, the number of dummies N_{di} in the i -th cluster, then

$$N_{di} = \frac{N_i \times (PR.k - 1)}{\sum_{i=1}^m N_i}$$

For example, after clustering using DBSCAN algorithm and $PR.k=K$, we get irregular regions, namely A , B and C , and shown in Figure 4. Then the number of dummies that needs to be generated in each region is calculated. N_A , N_B and N_C represent respectively the number of historical users in A , B and C , then

$$N_{dA} = \frac{N_A \times (K-1)}{N_A + N_B + N_C}, \quad N_{dB} = \frac{N_B \times (K-1)}{N_A + N_B + N_C}, \quad N_{dC} = \frac{N_C \times (K-1)}{N_A + N_B + N_C}$$

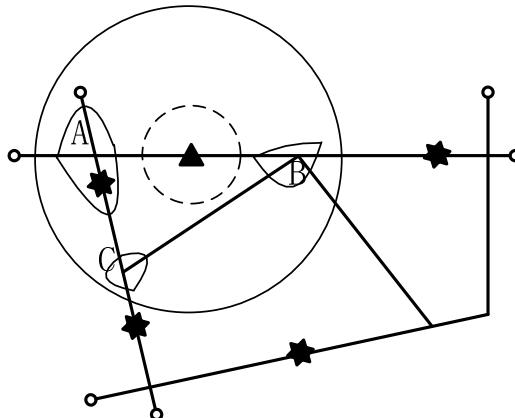


Fig. 4. Clustering on the historical user location data

If we follow the above method, the authenticity of the dummies will be enhanced, and it is difficult for the attacker to distinguish.

3.4 BHUDG Algorithm

Based History User Dummy Generation (BHUDG) mainly improve the direction consistency in [5], and uses the clustering algorithm to get dense regions in which historical user distributed. The main idea of the BHUDG algorithm is that the anonymous server determines the time interval whether is greater than the given threshold T_{th} or not. If the interval is greater than the T_{th} or does not meet anonymous parameter k , anonymous server regenerates dummies on the basis of current location; If not, these dummies are continued to use, but the speed consistency is kept.

Algorithm. BHUDG algorithm

Input: SRN=($V, E, loc, d_{min}, d_{max}$), $Q'=(uid, loc', t', T_{th}', query')$, $Q=(uid, loc, t, T_{th}, query)$, PR=($k, Eps, MinPts$)

Output: Location of real user and dummies

Begin

- (1) position the user's location, and get the location information;
- (2) calculate the user's query interval $\delta=t-t'$;
- (3) if($\delta > T_{th}$)
 - (4) {use DBSCAN clustering algorithm to obtain dense regions in which historical user distributed;
 - (5) generate randomly corresponding number of dummy in each cluster;}
 - (6) else
 - (7) {at time t' calculate the distance D_u that users arrive at the destination, and distance D_i that the i-th dummy arrive at its destination;
 - (8) if(at time $t' D_i > D_u$)
 - (9) {dummies' location is that dummies arrived at the location that meet the speed consistency at time t ;
 - (10) else
 - (11) {they are the destination location of dummies at time t' ;
 - (12) regenerate location of dummies who does not meet the conditions in SRN ;}
 - (13) return location information of all users;

End

4 Experimental Results

4.1 Operating Environment and the Experimental Data

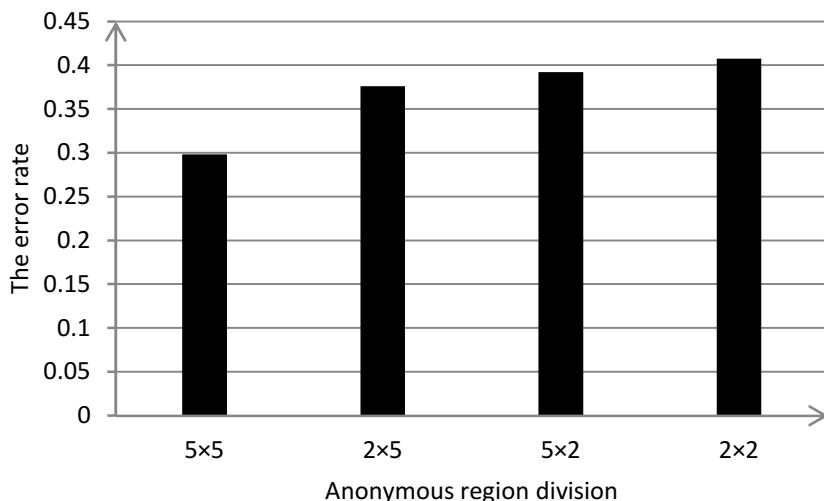
BHUDG is implemented in Java and compiled with MyEclipse7.1. All the experiments are conducted on a Windows XP PC equipped with an Inter dual-core CPU, a 2.66 GHz processor, 2 GB of main memory and 500GB hardware. The default values for each parameter are set as shown in Table 1.

Table 1. Experimental parameters and default values

parameter	default values
$PR.k$	5
d_{max}	6
d_{min}	1
Eps	1
$MinPts$	7

4.2 The Metrics

- The error. It is the probability of unreasonable dummies in detail in the initialization process. We have analyzed the reason in part 2 that can't find dense region in which historical user distribute in the grid. The higher the possibility of unreasonable dummies is, the greater the error is. In our experiment, we divided into 10×10 in the sampling area as the basis.
- The correct rate of movement direction. It is defined as the ratio of the user size according to their destination movement to the total number of all users in the mobile process. We assume that the real user always move in accordance with the direction of the inquiry result. We hope dummies' verisimilitude is as high as possible. Therefore, in a way the correct rate of movement direction indicates the authentic degree of the dummy.

**Fig. 5.** The error of generated dummies

4.3 The Analysis of Result

We have already mentioned that the grid can not accurately identify users dense area in part 2. Along with to dividing diversely 10 m x 10 m sampling experiment area, the error will be different, as shown in Figure 5. When anonymous region division becomes rough, the error becomes high, but even if the area is divided into the same, different error value is got. It follows normal logic, since the more detailed the division is the more reasonable dummies are generated. However, clustering method leads to very higher stability, and smaller errors.

Figure 6 shows the correct rate of movement direction when increasing privacy requirements. When anonymous parameter $PR.k$ is great, the correct rate decreased in the BHUDG method. Since the number dummies increases, the requirement does not increase accordingly, so the BHUDG algorithm is required to regenerate them. Meanwhile, after a comparative analysis with the methods in [5], we found the accuracy of BHUDG method is higher. The results show that our method meet the privacy protection requirement.

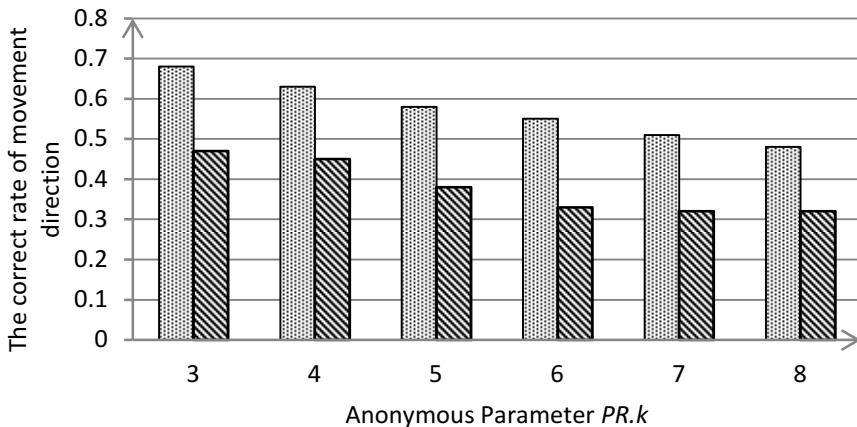


Fig. 6. The correct rate of movement direction

5 Conclusion

Previous location privacy protection studies are rarely based on the road network environment. In this paper, we propose a method to anonymize the user location in real environment. In the initial part, we use clustering method to ensure that dummies are the dense regions in which the historical users' distribute. The experiment shows that our method get higher accuracy rate than the literature [5].

Acknowledgments. This work is supported by the grants from the Natural Science Foundation of China (No. 61370084, 61073182), the Natural Science Foundation of Heilongjiang province (No.F201024), the Fundamental Research Special Funds for the Central Universities (No. HEUCFZ1010, HEUCFZ1305).

References

1. Meng, X., Pan, X.: Location based services privacy-preserving. CCCF 6(6), 16–22 (2010)
2. Kido, H., Yanagisawa, Y., Satoh, T.: Protection of location privacy using dummies for location-based services. In: Proc. of the 21st Int. Conf. on Data Engineering Workshops, pp. 1248–1248. IEEE, Washington (2005)
3. You, T., Peng, W., Lee, W.: Protecting moving trajectories with dummies. In: Proc. of 2007 Int. Conf. on Mobile Data Management, pp. 278–282. IEEE, Mannheim (2007)
4. Lu, H., Jensen, C.S., Yiu, M.L.: PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services. In: Proc. of Int. Workshop on Data Engineering for Wireless and Mobile Access, pp. 16–23. ACM, Canada (2008)
5. Suzuki, A., Iwata, M., Arase, Y., et al.: A user location anonymization method for location based services in a real environment. In: Proc. of the 18th SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems, pp. 398–401. ACM, New York (2010)
6. Liu, H., Wang, T.J., Sun, M., et al.: Location privacy in sparse environment. In: Proc. of 2nd Int. Conf. on Advanced Computer Control (ICACC), pp. 258–261. IEEE, Shenyang China (2010)
7. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proc. of the 1st Int. Conf. on Mobile Systems, Applications, and Services (MOBISYS), pp. 31–42. ACM, New York (2003)
8. Zacharouli, P., Gkoulalas-Divanis, A., Verykios, V.S.: A k-anonymity model for spatio-temporal data. In: Proc. of the IEEE Workshop on Spatio-Temporal Data Mining (STDM), pp. 555–564. IEEE, Istanbul Turkey (2007)
9. Xu, T., Cai, Y.: Exploring historical location data for anonymity preservation in location-based services. In: Proc. of the 27th Conf. on Computer Communications, pp. 547–555. IEEE, Phoenix (2008)
10. Pan, X., Xiao, Z., Meng, X.: Survey of location privacy-preserving. Journal of Frontiers of Computer Science and Technology 1(3), 268–281 (2007)

Towards More Secure Cardholder Verification in Payment Systems

Abdulrahman Alhothaily^{1,2}, Arwa Alrawais^{1,3}, Xiuzhen Cheng¹, and Rongfang Bie⁴

¹ Computer Science, The George Washington University, Washington DC, USA

² General Department of Payment Systems, Saudi Arabian Monetary Agency, Riyadh, KSA

³ College of Computer Engineering and Sciences, Salman Bin AbdulAziz University, KSA

⁴ College of Information Science and Technology, Beijing Normal University, Beijing, China

{*hothaily, alrawais, cheng*}@gwu.edu, rfbie@bnu.edu.cn

Abstract. This paper introduces a new cardholder verification method using a multi possession-factor authentication with a distance bounding technique. It adds an extra level of security to the verification process and utilizes the idea of distance bounding which prevents many different security attacks. The proposed method gives the user the flexibility to add one or more extra devices and select the appropriate security level. This paper argues that the proposed method mitigates or removes many popular security attacks that are claimed to be effective in current card based payment systems, and it can help to reduce fraud on payment cards. Furthermore, the proposed method provides an alternative verification technique and enables cardholders with special needs to use the payment cards and make the payment system more accessible.

Keywords: Cardholder Verification, Contactless Card, Payment System, EMV.

1 Introduction

Contactless card payment is a fast growing method which uses radio-frequency identification (RFID) to make payments. According to Visa Europe, contactless payments were increased by 46% between December 2012 and March 2013, and one in every four Visa cards in the UK is now contactless [1]. In recent years, there has been an increasing interest in contactless card payments in the United States. The number of contactless card payments grew from 58.6 million in 2008 to 140.0 million in 2012 at a compound annual increase rate of 24.31% [17]. Major financial entities offer contactless technology in payment cards around the world. American Express ExpressPay, Mastercard PayWave, PayPass Visa, and ZIP from Discover are examples of payment card projects which use radio-frequency identification technology. Using radio-frequency identification technology, these projects allow the cardholders to wave their credit cards or payment devices in front of contactless point of sale (POS) terminals without any physical contact with the terminals.

The use of radio-frequency identification technology in payments opens up new ways of security attacks. Moreover, it makes contactless payments susceptible to a wide range of RFID related attacks, such as skimming attacks, relay attacks, and cloning attacks. Some of these attacks come from the wrong assumptions when designing the protocols

of contactless payments between a credit card and the point of sale. For example, the EMV (named after Europay, MasterCard and Visa) protocol for contactless payment assumes that it is difficult to conduct card fraud within a range of 10 cm [5] [20]. In addition, relying on a single factor of authentication, such as a credit card, introduces a huge risk for cardholders. When a credit card is lost or stolen, the credit card can be used by an attacker until the cardholder reports the issue to the bank. This scenario happens because many implementations of the credit card verification do not utilize any cardholder verification method, or use weak cardholder verification methods such as signatures that can be easily compromised.

The proposed method in this paper relies on one or more personal RFID devices such as smart watches, smart phones, rings, necklaces, and bracelets. These personal devices are carried by the cardholder most of the time. In addition, they have sufficient computation power, as well as storage capabilities, and thus can be used in designing a new cardholder verification method. The proposed scheme can be extended to give the user the option to set the appropriate security level for different payments. For example, a cardholder can select more devices for higher value transactions, and use fewer RFID devices for lower value transactions. In addition, the proposed method allows the cardholder to replace, add, or remove a registered RFID device.

The rest of the paper is organized as follows. Section 2 briefly overviews the cardholder verification methods recommended by the Europay, MasterCard, and Visa standard, and summarizes other most related research. Section 3 covers the protocol description. Section 4 discusses the security of the protocol, followed by a conclusion drawn in Section 5.

2 Cardholder Verification in EMV and Other Related Research

2.1 Cardholder Verification in EMV

Europay, MasterCard and Visa or EMV is a global standard that was established by Europay, MasterCard, and Visa to be used for credit card and debit card payments [9] [10] [11]. It is widely used in Europe along with Asia, and is expected to be adopted in the United States in the near future. The EMV standard contains a protocol used by point of sale terminals and automated teller machines for authenticating credit and debit card transactions. Based on the EMV protocol, a transaction is divided into three phases [20]:

- A. Card authentication: ensures that the bank did issue the card, and the card details were not altered.
- B. Cardholder verification: ensures the cardholder's eligibility to use the card.
- C. Transaction authorization: ensures that the cardholder's account has enough funds for the transaction.

There are many cardholder verification methods (CVMs) supported by EMV, and implementations of these methods may be different for each country and each issuer [21]. The following are four types of cardholder verification methods introduced by EMV [24]:

1. Online PIN: The PIN is not stored on the EMV card; instead, it is sent to the issuer online for verification. ATM withdrawals using debit and credit cards rely on online PINs to verify the cardholders.
2. Offline PIN: The PIN is stored on the EMV card. During a transaction, the point of sale terminal sends the PIN entered by the cardholder to the card for verification. The card compares the received PIN with the stored one and sends the verification result to the point of sale terminal.
3. Signature: The merchant should ask the cardholder to sign on the receipt or electronic pad. The cardholder verification is achieved by comparing the cardholder's signature with the one at the back of the credit card.
4. No cardholder verification method (CVM): Using this method, there is no verification for the cardholder. The EMV standard allows this method for some cases such as when the point of sale is not equipped with a signature panel and a PIN pad.

All the cardholder verification methods currently in use have advantages and drawbacks. A four-digit Personal Identification Number (PIN) or password is not an optimal cardholder verification method for payment card in the current age. Recent research conducted at The University of Cambridge [3] shows that a thief can use an ATM card once every 11-18 stolen wallets by using the victims' birthdays as passwords. This fact is very alarming since many cardholders carry their identification and driver licenses which contain detailed information about them. In addition, there are many issues with passwords such as the tendency to use the same password everywhere. Other issues include forgetting a password, particularly if it is used infrequently. Furthermore, using PINs as a verification method is not immune against different types of password related attacks. For example, password recovering can be achieved by thermal imaging [26] [18] or direct observation techniques.

Using PINs also suffers from the shoulder surfing attack which is commonly used to obtain sensitive information such as the password [25]. The victim is observed by an attacker using different direct observation techniques. One simple technique is to look over the victim's shoulder to obtain a password. Unfortunately, most of the deployed point of sale terminals in malls, grocery stores and gas stations, do not completely prevent shoulder surfers from obtaining an entered PIN. Shoulder surfers can obtain the PIN because many point of sale terminals are usually located in clear view on counters and gas pumps.

On the other hand, using signatures for cardholder verification does not effectively prevent fraud risks. An attacker or criminal who steals a credit card can sign on behalf of the original cardholder when the point of sale terminal requests a signature. The following are some weaknesses about using signatures as a method for cardholder verification:

- The signature comparison is done manually, and it is seldom that anyone compares the entered signature to the one on the back of the credit card. Even if there is some sort of signature verification, the signature on the back of the credit card could be false.
- When a card is lost or stolen, a malicious and motivated attacker can reproduce a signature that is similar to the one on the back of the credit card after a careful practice.

In general, the PIN cardholder verification method provides much better protection against fraud. Moreover, PIN provides more security when the card is lost or stolen. According to [16] and the debit card fraud data collected by the Federal Reserve Board of Governors, fraud losses due to signature-based transactions represented 13 percent of losses in 2008, while during the same period the PIN based transactions achieved a significantly lower fraud rate of .035 percent, or 3.5 basis points, per dollar volume.

2.2 Most Related Research

The research community also proposed different cardholder verification methods to verify the identity of a cardholder in payment systems. Henniger and Nikolov proposed a new cardholder verification method using biometric on-card verification to be performed on debit or credit cards [13]. To verify the cardholder, they use the handwritten signature verification inside the smartcard chip where the verification is done offline. Breebaart *et al.* [4] studied the advantages and limitations of integrating biometrics in a payment system. Their results indicate that it is unlikely for fingerprints to replace PINs, and they suggested PIN and fingerprint coexist. Nevertheless, according to the authors, the simulation result for co-existence scenario did not provide the claimed advantages of biometric technology such as enhanced security, customer convenience, acceptance, and cost. Ion and Dragovic proposed a protocol using a camera-enabled mobile phone and a previously shared secret with the card to improve cardholder authentication and protect against stolen PINs and cards [14]. For each purchase, the card generates a secure message to be displayed at the point of sale terminal using a visual code. Using a phone's camera, the phone decodes the visual image and computes the response. The response is displayed as a code in the mobile phone. The cardholder enters the displayed code as a PIN at the point of sale, and then the card verifies the inserted code.

Bonneaus *et al.* estimated the distribution of banking PINs by using a survey of 1100 cardholders and a regression model to identify the factors that affect user choices [3]. They found that by guessing PINs based on victims' birthdays, a thief can successfully use an ATM card once every 11-18 stolen wallets. The authors recommended that banks change their policy about PIN selection and move away from customer-chosen in the long term. The authors in [8] and [7] cover different attack scenarios that can be launched against contactless cards that support the offline PIN verification method. In [8], the authors pointed out the dangers of using contactless cards based on the offline PIN verification method. In addition, they introduced an attack scenario to guess a cardholder's PIN without their knowledge by using several accesses to the card. In [7], the authors explained different attack scenarios against verifying the PIN offline on contactless cards. These attacks include denial of service attacks and PIN guessing attacks. The authors also suggested removing the functionality of verifying PINs offline on contactless cards, because it makes contactless cards vulnerable to different attacks.

2.3 Discussions

The existing cardholder verification methods ignore a crucial component from the community. Cardholders with special needs such as blind people, and people with disabled, or missing hands have difficulty entering a PIN or signing a credit card receipt. It is

very important to make the payment system usable by the widest possible community of users by making the cardholder verification method interface accessible.

Accessibility is an important issue to consider when designing a verification method. The proposed cardholder verification method enables handicapped cardholders to use card payments much more easily, while providing a greater level of security. Cardholders with limited or no use of their arms or hands will find using the proposed system advantageous as they will not have to sign a receipt or enter a PIN. In addition, blind people have clear issues in ascertaining their PINs by using current cardholder verification methods. In practice, they have to ask another person to read it. This practice makes the PIN less secure and increases the risk of fraud. On the other hand, our proposed method provides a more friendly design for blind people since it relies on wearable RFID devices that are registered once at the bank. Furthermore, cardholders with dyslexia can have problems in remembering the digits of a PIN in the correct order. Nevertheless, the new verification method resolves this issue. The proposed design makes payment card and cardholder verification more accessible and usable by the widest possible community.

Our contribution is to propose using multi possession-factor authentication with a distance bounding technique. The new cardholder verification method overcomes the current weaknesses of the existing methods of cardholder verification. Using the proposed method, a cardholder would no longer need to remember PINs and keep this number secret. The security analysis of the proposed method shows that it enhances the security of a card payment and prevents various attacks.

3 Protocol Description

The proposed protocol is intended to provide cardholder verification using multi possession-factor authentication and distance bounding technique. When carrying out the proposed scheme, RFID devices to be used for cardholder verification must be registered with the bank. During the registration stage, the user can specify the required number of RFID devices that will be used in the verification process. For each device, the registration terminal generates a shared secret key and stores it on the user device. In addition, the shared secret key should be transferred and stored securely in the bank database. The maximum round trip time for each RFID device has to be measured during the registration process at the registration terminal. For each device, the registration terminal uses a clock to measure the max time T_{max_i} elapsed between sending out a challenge and receiving the response.

In this section, we describe the proposed protocol which consists of seven major steps and involves three main entities: the cardholder, the point of sale, and the bank authentication server. The cardholder carries his credit card and the associated devices. The point of sale is a payment terminal equipped with a card reader and is connected to the issuing bank [19]. The bank issues the credit card to the cardholder and maintains the registered devices used in the cardholder verification process.

The first phase of the protocol is a slow phase, and it includes step 1 to 4. During this phase, the point of sale obtains nonce and identification information and sends them to the bank. The authentication server at the bank fetches the associated keys, then it

Table 1. Abbreviation and Description

Abbreviation	Description
POS	Point of Sale
CC	Credit Card
RD	Registered Device
AS	Authentication Server
m	Number of registered devices
i	$i = 0$ for credit card, $i = 1..m$ for registered devices
ID_i	Device identification number for device i
k_i	Secret Shared key for device i
T_i	Measured round trip time for device i
T_{max_i}	Registered max round trip time for device i
N_i	Nonce generated by device i
Nb_i	Nonce generated by bank for device i
C_1, \dots, C_k	Challenge generated for device i
$R_i^{C_i}$	Reply generated by device i to for challenge C_i

generates a nonce along with a challenge for each registered device and the credit card. The authentication server sends the generated nonces and challenges to the point of sale. The second phase of the protocol is time-critical which involves the point of sale, the registered cardholder devices, and the credit card. Step 5 of the protocol is responsible for this time-critical phase, and it relies on the Haneke and Kuhn protocol [12]. The last phase of the protocol is a slow phase, and it happens between the point of sale and the authentication server at the bank. The goal of this phase is to obtain the verification status and send it to the point of sale. Step 6 to 7 are responsible for this phase.

For better elaboration, we use an example to demonstrate the protocol details. A cardholder has registered an RFID smart watch to be used along with his credit card for the cardholder verification process at the point of sale. Table 1 lists the abbreviations that are used in describing the protocol. Note that we use ID_i , N_i , and NB_i to represent the identity of device i , the nonce generated by device i , and the nonce generated by the bank for device i , respectively. Also note that $i = 0$ refers to the credit card, which makes our description more readable.

Before starting the protocol, the cardholder has to confirm that he wants to pay by performing the following two actions: first, present the credit card and all the registered devices near the point of sale. Second, give the approval by performing a specific action such as pressing a button on one of the registered devices or orally uttering some command.

Note that the second action enhances the security of the payment card and protects cardholders from many attacks such as the skimming attack, as explained in section 4. It can be carried out by either pushing a button or uttering some command, depending on the ability of the cardholder. In the following description, we assume that the cardholder can push a button to give verification permission. After the cardholder's approval, the protocol is ready to start. The steps of the protocol are listed as follows:

1. Cardholder Verification Request

$POS \rightarrow \{CC, RD\}$

In the first step of the protocol, the point of sale sends a verification request message to the cardholder's credit card CC and his registered devices RD . Since the point of sale does not know the exact registered devices, this request should be broadcast to certain (short) distance. The message can also be used to power the credit card and the associated RFID devices.

2. Cardholder Verification Reply

$CC \rightarrow POS : ID_0, N_0$

$RD_1 \rightarrow POS : ID_1, N_1$

\vdots

$RD_m \rightarrow POS : ID_m, N_m$

In the second step, the credit card generates a nonce and replies to the point of sale with the cardholder identification number ID_0 and nonce N_0 . In addition, each RFID device i generates a nonce N_i and replies with its device ID_i to the point of sale. These personal devices need to collaborate to successfully complete the protocol and avoid collisions. The collaboration can be handled during the registration phase by specifying a delay time for each device. Another method to handle collision is to utilize certain collision avoidance protocols (such as those in [22] and [15]) proposed to regulate the responses from multiple RFID tags.

3. Verification Request

$POS \rightarrow AS : m, ID_0, N_0, ID_1, N_1, \dots, ID_m, N_m$

After obtaining the reply messages from the credit card and the associated cardholder devices, the point of sale sends a verification request message using the received information in step 2. The message also contains the number of replied devices, and it is delivered to the bank using a secure connection. We assume that the connection between the point of sale and the bank is encrypted using a standard and strong encryption to protect cardholder sensitive information in transit. It is worth mentioning that encrypting transmissions of cardholder information across public networks is one of the requirements of the payment card industry data security standard, which was designed to increase controls around cardholder information to reduce credit card fraud [23]. Two main conditions have to be verified in order to continue the protocol steps: First, the authentication server at the bank analyzes the request and check whether each ID_i is known or not. Second, the authentication server checks whether the number of replied devices are equal to the number of registered devices. When these two conditions are met, the protocol moves to the next step. Not satisfying one or more of these conditions results in a denial of the transaction, and the authentication server will send a "not verified" message to the point of sale.

4. Verification Request Reply

$AS \rightarrow POS : ID_0, Nb_0, C_1, \dots, C_k$

$ID_1, Nb_1, C_1, \dots, C_k$

\vdots

$ID_m, Nb_m, C_1, \dots, C_k$

The authentication server fetches the associated keys for the cardholder and generates a nonce Nb_i for each device i . It also generates a nonce Nb_0 for the credit card. The generated nonce is different for each registered device and the credit card. In addition, the authentication server generates a random k bit challenge C_1, \dots, C_k for the credit card and each device. The total number of generated challenges has $(m + 1) * k$ bits since we have m registered devices.

The authentication server calculates the reply to device i ($i = 0$ corresponds to the credit card) as follows:

$$R_i = \text{hash}(k_i, N_i || Nb_i),$$

k_i is the secure shared key for device i

N_i is the nonce generated by device i

Nb_i is the nonce generated by the bank for device i

For each RFID device and credit card, the result R_i is splitted into $R_i^0 || R_i^1$. The values are kept at the authentication server for verification status check. The authentication server at the bank sends the generated nonce Nb_i and the challenges C_1, \dots, C_k to the point of sale. Figure 1 covers the first phase of the protocol which includes the steps from 1 to 4.



Fig. 1. The first phase of the protocol (left) and the last phase of the protocol (right)

5. Challenge Response Step

This step builds upon the RFID distance bounding protocol proposed by Hancke and Kuhn [12]. The point of sale sets a timer and sends the nonce Nb_i to the corresponding devices. Each device i , including the credit card ($i = 0$), computes the reply as follows:

$$R_i = \text{hash}(k_i, N_i || Nb_i),$$

k_i is a secure shared key for device i

N_i is the nonce that is generated by device i

Nb_i is the nonce that is generated by the bank for device i

The result R_i is splitted into $R_i^0 || R_i^1$ and loaded into two right-shift registers¹. A single bit challenge $C_j, j = 1, 2, \dots, k$, is transmitted each time by the point of sale to the device i and the device i selects the least significant bit of the shift register, storing $R_i^{C_j}$ as the response. Both registers then shift right one bit position. The point of sale sends in total k challenge bits to device i and it should receive k responses from i . The timer is stopped when the last response is received and the round trip time

¹ Left-shift registers also work but we use right-shift registers to demonstrate the distance bounding technique.

T_i is recorded at the point of sale for device i . This process should be repeated for each registered device and the credit card. At the end of the step, the point of sale will have k response bits plus T_i for each device and then deliver them to the bank for the verification status check. Figure 2 explains the challenge-response step using the Hancke and Kuhn protocol [12].

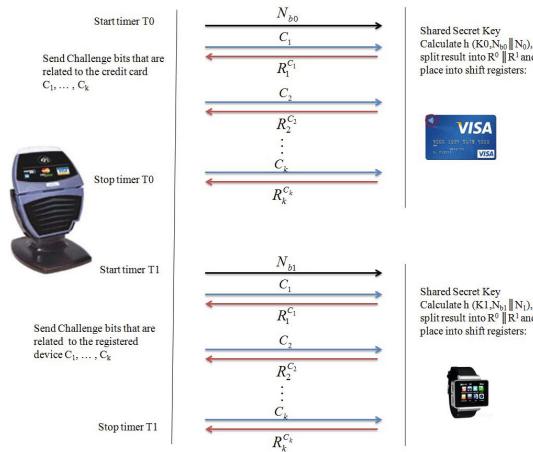


Fig. 2. The critical phase of the protocol using Hancke and Kuhn protocol [12]

6. Check Verification Status

After performing the challenge-response step, the point of sale sends a check verification status message using the received information in step 5 and delivers it to the authentication server at the bank. The message contains the k response bits together with the measured time T_i for the credit card and each associated device.

7. Verification Status Reply

For each RFID device and the credit card, the challenge and response are checked by comparing the computed replies with the received replies at the authentication server in the bank. Moreover, the measured round trip time is compared with the registered maximal round trip time $T_{max,i}$. Algorithm 1 is used to check the verification status at the authentication server for the credit card and each device:

Algorithm 1. Verification Status Check

```

if (calculated  $R_i^{C_i}$  = received  $R_i^{C_i}$ ) AND ( $T_i \leq T_{max,i}$ ) then
    cardholder is verified
else
    cardholder is not verified
end if

```

4 Security Discussion

The design of our cardholder verification protocol improves the security of the cardholder verification process and prevents it from many important security attacks. In this section, we discuss briefly some of the security features of the proposed protocol.

Relay Attacks: The use of the distance bounding protocol proposed by Hancke and Kuhn in step 5 prevents an attacker from launching a relay attack. The attacker can not conduct a distance bounding protocol at the same time between the point of sale from one side, and the credit card with the registered devices from the other side. The point of sale along with the authentication server can detect the relay attack using the measured time for the challenge and response for each registered device in step 5.

Cloning Attacks: Our proposed protocol resists cloning attacks by relying on multi possession-factor authentication. It does not rely on a single factor of authentication since the cardholder can register one or more personal devices. In addition, the use of fresh nonces that are generated by the authentication server and the cardholder's personal devices mitigates the risk of pre-play and cloning attacks in [2].

PIN Related Attacks: It can be clearly seen that the proposed method eliminates many PIN related attacks such as shoulder sniffing, skimming attacks, and direct observation attacks. In addition, the new method protects cardholders from PIN recovering attacks. The cardholder is now prevented from using PINs that can be recovered by using thermal imaging, or by analyzing mechanical vibrations generated after pressing keys [6]. Issues such as using the cardholder's birthday as the PIN, using the same PIN everywhere, or forgetting the PIN are avoided since we rely on personal and wearable devices for cardholder verification.

Signature Related Attacks: By adopting the proposed cardholder verification method, a wide range of signature issues and related attacks can be prevented. Handwriting signatures are susceptible to forgery attacks as an adversary who steals a credit card can sign on behalf of the original cardholder, and it is rare that merchants compare the entered signature to the signature on the back of the credit card. The proposed verification method provides an online and automated verification protocol that mitigates the risk of fraud. Furthermore, it provides a more reliable verification protocol than signature verification since several human factors such as fatigue and some psychological contexts can affect the signature reliability.

Replay Attacks: One important security feature of any cardholder verification protocol is the ability to resist replay attacks. A replay attack occurs when an attacker records a cardholder verification session and replays the verification data at a later point in time. The replayed verification data may be sent to the same point of sale or to a different one. The goal of the replay attack may be impersonation in an attempt to obtain goods without the card being present using the victim's verification data. The use of nonces that are generated by the authentication server with the challenge, and the nonces that are generated by the registered devices together with the credit card ensure that each challenge-response sequence is unique.

5 Conclusion

There is an urgent need for the design of a secure cardholder verification method that can be accessible by a wide range of cardholders. Conventional verification methods suffer from many security attacks and introduce a notable risk for cardholders in addition to issuing banks. Relying on a single factor of authentication, such as a credit card, without verification gives the attacker the opportunity to capitalize on a single point of failure in the verification process. The attacker who steals or clones the credit card can use it for fraud purchases until the bank detects the issue, or the cardholder reports the incident. In addition, using weak cardholder verification methods such as a signature is not the best method to verify the identity of the cardholder, as signatures can be replicated after careful practices.

Various attacks can be prevented in our protocol by using multi possession-factor authentication with distance bounding in the verification process. In addition, the user interaction by uttering some commands or pressing a button on one of the registered devices makes the protocol more secure than conventional cardholder verification methods. The proposed protocol gives the user the option to set the required binding devices. The number of personal devices needs to create a balance between security and convenience. The usability and privacy of the proposed protocol should be further investigated in our future research.

Acknowledgment. Alhothaily acknowledges the scholarship fund from the Saudi Arabian Monetary Agency. Alrawais acknowledges the scholarship fund from the Ministry of Higher Education, Saudi Arabia and the College of Computer Engineering and Sciences, Salman bin Abdulaziz University, Saudi Arabia. This research is also supported by the National Science Foundation of the US under grant CNS-1318872, and the National Natural Science Foundation of China under grant 61171014.

References

1. Atkins, S.: Visa Europe claims growth of 46% in contactless payments in last three months, <http://contactlessintelligence.com/2013/05/21/visa-europe-claims-growth-of-46-in-contactless-payments-in-last-three-months-alone/> (accessed December 02, 2013)
2. Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S., Anderson, R.: Chip and skim: cloning emv cards with the pre-play attack. arXiv preprint arXiv:1209.2531 (2012)
3. Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? the security of customer-chosen banking pins. In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 25–40. Springer, Heidelberg (2012)
4. Breebaart, J., Buhan, I., de Groot, K., Kelkboom, E.: Evaluation of a template protection approach to integrate fingerprint biometrics in a pin-based payment infrastructure. Electronic Commerce Research and Applications 10(6), 605–614 (2011)
5. Ceipidor, U.B., Medaglia, C.M., Marino, A., Sposato, S., Moroni, A.: Kernees: A protocol for mutual authentication between nfc phones and pos terminals for secure payment transactions. In: 9th International ISC Conference on Information Security and Cryptology (ISCISC), pp. 115–120. IEEE (2012)

6. De Souza Faria, G., Kim, H.Y.: Identification of pressed keys from mechanical vibrations. *IEEE Transactions on Information Forensics and Security* 8(7), 1221–1229 (2013)
7. Emms, M., Arief, B., Defty, T., Hannon, J., Hao, F., van Moorsel, A.: The Dangers of Verify PIN on Contactless Cards. *Computing Science*. Newcastle University (2012)
8. Emms, M., van Moorsel, A.: Practical attack on contactless payment cards. In: *HCI 2011 Health, Wealth and Identity Theft* (2011)
9. EMV: Book A: Architecture and General Requirements. EMVCo (2013)
10. EMV: Book B: Entry Point. EMVCo (2013)
11. EMV: Book D: Contactless Communication Protocol. EMVCo (2013)
12. Hancke, G.P., Kuhn, M.G.: An rfid distance bounding protocol. In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, pp. 67–73. IEEE (2005)
13. Henniger, O., Nikolov, D.: Extending emv payment smart cards with biometric on-card verification. In: Fischer-Hübner, S., de Leeuw, E., Mitchell, C. (eds.) *IDMAN 2013. IFIP AICT*, vol. 396, pp. 121–130. Springer, Heidelberg (2013)
14. Ion, I., Dragovic, B.: Dont trust pos terminals! verify in-shop payments with your phone. In: *Proceedings of SMPU*, vol. 8 (2010)
15. Joshi, G.P., Kim, S.W., et al.: Survey, nomenclature and comparison of reader anti-collision protocols in rfid. *IETE Technical Review* 25(5), 285 (2008)
16. King, D.: Chip-and-pin: Success and challenges in reducing fraud (2012)
17. Mathis, R.: Report: Contactless card payments current and forecast analysis to 2017, <http://secureidnews.com/news-item/report-contactless-card-payments-current-and-forecast-analysis-to-2017/> (accessed December 01, 2013)
18. Mowery, K., Meiklejohn, S., Savage, S.: Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. In: *Proceedings of the 5th USENIX Conference on Offensive Technologies*, p. 6. USENIX Association, Berkeley (2011)
19. Nakajima, M.: Payment system technologies and function innovations and developments. *IGI Globale*, Hershey (2011)
20. Ogundele, O., Zavarsky, P., Ruhl, R., Lindskog, D.: Fraud reduction on emv payment cards by the implementation of stringent security features, pp. 252–262 (2012)
21. Ogundele, O., Zavarsky, P., Ruhl, R., Lindskog, D.: The implementation of a full emv smart-card for a point-of-sale transaction. In: *2012 World Congress on Internet Security (WorldCIS)*, pp. 28–35. IEEE (2012)
22. S. Patrick, A., Yung, M. (eds.): *FC 2005. LNCS*, vol. 3570. Springer, Heidelberg (2005)
23. PCI: Payment Card Industry (PCI) Data Security Standard
<https://www.pcisecuritystandards.org/> (accessed December 21, 2013)
24. Sifatullah Bhuiyan, M.: Securing Mobile Payment Protocol based on EMV Standard. Master's thesis, KTH (2012)
25. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: *Proceedings of the Working Conference on Advanced Visual Interfaces*, pp. 177–184. ACM (2006)
26. Zalewski, M.: Cracking safes with thermal imaging,
<http://lcamtuf.coredump.cx/tsafe/> (accessed December 25, 2013)

Fortifying Barrier-Coverage of Wireless Sensor Network with Mobile Sensor Nodes^{*}

Biaofei Xu¹, Donghyun Kim², Deying Li^{1, **}, Joonglyul Lee³, Huaipan Jiang⁴,
and Alade O. Tokuta²

¹ School of Information, Renmin University of China, Beijing, China
deyingli@ruc.edu.cn

² Dept. of Math and Physics, North Carolina Central University, Durham NC, USA

³ Dept. of Computer Science, University of Texas at Dallas, Richardson, USA

⁴ School of Computer Sci. and Tech., Univ. of Sci. and Tech. of China, Hefei, China

Abstract. Recently, the barrier-coverage of wireless sensor network received huge attention thanks to the important applications such as border protection. In practice, sensor nodes are subject to intermittent failure to detect objects within its sensing range due to many reasons. Therefore, a barrier of sensor nodes may exhibit temporal loopholes. In this paper, we investigate the potential of mobile sensor nodes such as unmanned aerial vehicles and human patrols to fortify the barrier-coverage of static wireless sensors. We use a single variable first-order grey model, GM(1,1), based on the intruder detection history from the sensor nodes to determine which parts of the barrier is more vulnerable. Then, we relocate the available mobile sensor nodes to the identified vulnerable parts of the barrier in a timely manner. We show this relocation strategy is optimal in theory. By the simulations, we also evaluate the average performance of our algorithm.

1 Introduction

In the literature, the *coverage* of a *wireless sensor network (WSN)* refers to the quality of the sensor network satisfying a certain surveillance requirement. We say a WSN offers barrier-coverage over an area if the WSN guarantees to detect any object moving into the area. The barrier-coverage model has a wide range of important real-life applications such as border protection and enemy intrusion detection during a war. In practice, sensor nodes intermittently suffer from failures due to many reasons such as inaccurate readings and environmental changes. As a result, a barrier of wireless sensors has a chance to exhibit loopholes which allow some intruder to pass the barrier without being detected. Unfortunately,

* This paper was jointly supported by National Natural Science Foundation of China under grant 91124001, the Fundamental Research Funds for the Central Universities, and the Research Funds of Renmin University of China 10XNJ032. This work was supported in part by US National Science Foundation (NSF) CREST No. HRD-1345219.

** Corresponding author.

in many applications scenarios of barrier-coverage of wireless sensor networks such as enemy intrusion detection in the battlefield, the intruders are intelligent enough to identify such loopholes. Once an intruder identifies a path to penetrate successfully (possibly detected, but not captured), it is likely that the other intruders will try the similar path in the near future. Therefore, in those applications, it becomes very crucial to identify such a trend and accordingly fortify the border security in a timely manner.

In this paper, we assume there is a WSN offering barrier-coverage over an area of interest. In detail, we follow the previous work such as [2, 3] and consider a belt area over which the barrier of sensors is deployed. This is because (a) the belt shape area is easier to handle and (b) a barrier coverage model which is successfully working in the belt area is also applicable to the regions with different shapes such as a ring. We further assume that each sensor node suffers from intermittent failures, whose pattern are not known. However, we can access the statistics of the intruders (fortunately) detected by each sensor node. Under the circumstance, we study how to relocate a set of available mobile sensor nodes (which are much more reliable and physically superior than the cheap ground sensors) to fortify the barrier of sensor nodes against the intruders which may alter their main routes for penetration. Largely, the contribution of this paper has two folds.

- (a) Based on the previous history of the arrival time of intruders detected by each sensor node, we predict the likelihood of intruders being detected by each sensor node in the near future. For this purpose, we adopt a mathematical model known as a single variable first-order grey model, GM(1,1), which has been widely used to predict events which are repeatedly occurring and is known to be highly reliable and efficient for this purpose [4–8].
- (b) Once we identify static sensor nodes which have higher chance to detect intruders, we relocate the available mobile sensor nodes nearby the static sensors so that the area covered by these nodes can be monitored even more thoroughly. Since this should be done in a timely manner, it is necessary to relocate the mobile nodes in a way that the maximum travel distance among the nodes is minimized (i.e. all nodes move concurrently and we would like to minimize the delay to perform the relocation of all nodes). We introduce a new mobile sensor nodes relocation algorithm which tries to satisfy this requirement in a way that a static sensor node with higher chance to detect an intruder will obtain assist from more number of mobile sensor nodes. We also prove our relocation strategy is optimal.

We would like to emphasize that the main contribution of our work is to investigate how to utilize a given set of mobile sensor nodes to fortify the barrier-coverage of static sensors which can be intermittently faulty. We recognize the consideration of the other traditional quality factors of static sensor network such as energy-efficiency is still important in this model. But, we leave how to integrate those mechanisms to improve performance of this hybrid sensor network system as the future work. The rest of this paper is organized as follows. Section 2 introduce some preliminaries. In Section 3, we introduce a new two-phase algorithm

to identify the static sensor nodes to be fortified and to relocate the mobile sensor nodes accordingly. We present the simulation results and make discussions in Section 4. Finally, we conclude the paper in Section 5.

2 Preliminaries and Problem Statement

2.1 Network Model

A barrier coverage model which is successfully working in the belt area is also applicable to the regions with different shapes such as a ring [2, 3]. Therefore, this paper considers a WSN of n static sensor nodes within a two-dimensional rectangular area along with m mobile sensor nodes with limited sensing capability. Throughout this paper, we assume the intruders are moving from the top of the area (outer space) to the bottom (inner space) to trespass, but never circumvent the area (i.e. we are considering a rectangular area whose rightmost side is adjacent to the leftmost side). The static sensor nodes are deployed in the area and already providing barrier-coverage over the bottom region of the area. However, each sensor node suffers from temporal failure due to some reasons and the barrier may exhibit some loopholes. To minimize the loopholes, the mobile sensor nodes are (initially randomly) deployed in the area and will relocate themselves to enhance the quality of the coverage. We follow Saipulla et al. [9] and assume the coordinate (x, y) of each sensor node is known in advance, which can be done using either an on-board GPS unit or any existing localization mechanism. We further assume that the mobile sensor nodes have the knowledge of their locations within the area. Each sensor node has a sensing range r and is capable of detecting any intruder within its sensing region, whose shape resembles a disk with radius r centered at the sensor node. We say an intruder is covered or detected by a static sensor node or a mobile node once the intruder moves into the sensing region of the node [10, 12–14].

2.2 Single Variable First-Order Grey Model, GM(1,1)

This section introduces GM(1,1) which can be used predict the time that the next intruder will arrive at a sensor node based on the history of intruders collected by the sensor node. Suppose we have an initial intruder arrival time sequence measured by the sensor node,

$$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \dots, x^{(0)}(l)\}, \quad (1)$$

where $x^{(0)}(i)$ is the time series data at time i and l is an integer such that $l \geq 4$. Based on the initial time series, we generate a new time-series

$$X^{(1)} = \{x^{(1)}(1), x^{(1)}(2), \dots, x^{(1)}(l)\}, \quad (2)$$

where $x^{(1)}(k) = \sum_{i=1}^k x^{(0)}(i)$ for $k = 1, 2, \dots, l$. The reason to accumulate the measures is to (a) provide the middle message of building a model and (b)

weaken the variation tendency [4]. Then, we need to solve the following first-order differential equation of grey model GM(1,1):

$$\frac{dx^{(1)}(t)}{dt} + ax^{(1)}(t) = b \quad (3)$$

by determining a and b . Here, the (a, b) pair satisfying the equation can be computed by least squares, i.e.

$$(a, b)^T = [\mathbf{X}^T \mathbf{X}]^{-1} [\mathbf{X}^T \mathbf{Y}], \text{ where} \quad (4)$$

$$\mathbf{X} = \begin{pmatrix} -\frac{1}{2}[x^{(1)}(1) + x^{(1)}(2)] & 1 \\ -\frac{1}{2}[x^{(1)}(2) + x^{(1)}(3)] & 1 \\ \vdots & \vdots \\ -\frac{1}{2}[x^{(1)}(n-1) + x^{(1)}(n)] & 1 \end{pmatrix}, \mathbf{Y} = \begin{pmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{pmatrix}$$

Once we obtain the (a, b) pair, we plug them into the differential equation in Eq. (3) and solve it to obtain a GM(1,1) forecast model as follow:

$$\hat{x}^{(1)}(k+1) = [x^{(0)}(1) - \frac{b}{a}]e^{-ak} + \frac{b}{a}, \quad (5)$$

for $k = 1, 2, \dots, n$. Here, $\hat{x}^{(1)}(k+1)$ is the predicted value of $x^{(1)}(k+1)$ at the time slot $k+1$. From this equation, we can obtain the *forecast value* of $\hat{x}^{(0)}(k+1)$ at time $k+1$ as a function of $\hat{x}^{(1)}(k+1)$ and $\hat{x}^{(1)}(k)$, which is

$$\hat{x}^{(0)}(k+1) = \hat{x}^{(1)}(k+1) - \hat{x}^{(1)}(k). \quad (6)$$

In the literature, this model is also referred as “Whole Data GM(1,1) Model”. Note that as we can see from the equations above, its forecast data series is solely dependent on the historical data collected.

2.3 Problem Statement and Our Approach

In this paper, we study how to fortify the barrier of sensors using mobile sensor nodes. In our problem, the intruders are intelligent to detect a part of the sensor barrier which suffers from temporal failure more frequently. Therefore, we assume that a sensor node which fortunately detects larger number of intruders is more likely to be vulnerable. Based on this observation, we measure the vulnerability of each sensor node using GM(1,1) whose only input is the history of intruders collected by the sensor node, and it outputs which sensor node has a better chance to detect intruders in the near future, and thus more vulnerable. Once a set of vulnerable sensor nodes are identified, we relocate the available mobile sensor nodes to assist the vulnerable static sensor nodes such that the maximum travel distance of the mobile sensor nodes is minimized. As a result, this relocated can be achieved in a timely manner.

3 Predict and Fortify: A New Way to Improve Barrier-Coverage Using Mobile Sensor Nodes

In this section, we introduce our two-phase algorithm to dispatch available mobile sensor nodes in a timely manner so that the weak part of the barrier of sensors can be effectively fortified. Let X be the random variable of the number of intruders detected by a barrier of sensors during a certain time period. Clearly, this inter arrival time of intruders can be modeled as a renew process. We use Poisson distribution with parameter $\lambda > 0$ as the probability distribution of the number of intruders since this distribution has been widely adopted to model such a real world random event. Note that the expected value of a Poisson random variable X with parameter λ is λ , i.e. $\lambda = E(X)$.

3.1 Predicting Vulnerability of Static Sensors

Let T_i^k be the time of k_{th} intruder detected by a static sensor node s_i . As we introduced, to apply GM(1,1), we assume that T_i^k is available for any $1 \leq k \leq l$ and $1 \leq i \leq n$ pair, where $l \geq 4$ is the number of intruders detected so far and n is the number of static sensor nodes. Then, using GM(1,1), we obtain \hat{T}_i^{k+1} , which is the predicted time that $k+1_{th}$ intruder (or the first intruder in the next time slot) will arrive at s_i for each i . Then, we compute $\Delta_i = \hat{T}_i^{k+1} - T_i^k$, which is the expected inter arrival time of $k+1_{th}$ intruder. Then, we define we compute the weight of s_i as $W_i = \frac{\lambda}{\Delta_i}$. This equation implies that with larger expected inter arrival time Δ_i , s_i will detect less number of intruders in the next time slot. Therefore, we can determine that a sensor node s_i with higher W_i value is more vulnerable. Let F_i be the number of mobile sensors needed by sensor node s_i . Clearly, the more W_i is, the higher F_i should be. One good equation that we can use is $F_i = \lceil \frac{W_i}{\alpha} \rceil - c$, where α is used to normalize W_i so that $\sum_{\forall i} F_i$ cannot exceed m , the total number of available mobile sensor nodes, and c is introduced to distinguish the group of vulnerable sensors from the rest. For the sake of simplicity, we set $\alpha = 1$, $c = 1$, and proceed.

3.2 Strengthening Barrier with Mobile Sensors

Suppose \mathcal{V} be the set of vulnerable sensor nodes, i.e. $\mathcal{V} = \{s_i | F_i \geq 0\}$, identified by the previous phase. Then, for each sensor node s_i , we would like to (ideally) move at most F_i mobile sensor nodes to assist s_i . Note that we normalized $\alpha = 1$ and $c = 1$, and thus $\sum_{\forall i} F_i \geq m$ may happen. However, our strategy for relocating mobile sensor nodes introduced in this section is a best effort one, and thus it still works. In this section, we assume each mobile node is allowed to move at most \mathcal{D} unit distance through the three steps introduced below. In the following section, we will explain how optimal \mathcal{D} can be found.

- Step 1: Suppose $S = \{s_1, \dots, s_q\}$ is the set of sensor nodes identified to be vulnerable in the previous phase. From S , we first induce S' such that for each $s_i \in S$, we add $s_{(1,1)}, s_{(1,2)}, \dots, s_{(1,F_i)}$ to S' . Let $M = \{u_1, u_2, \dots, u_m\}$

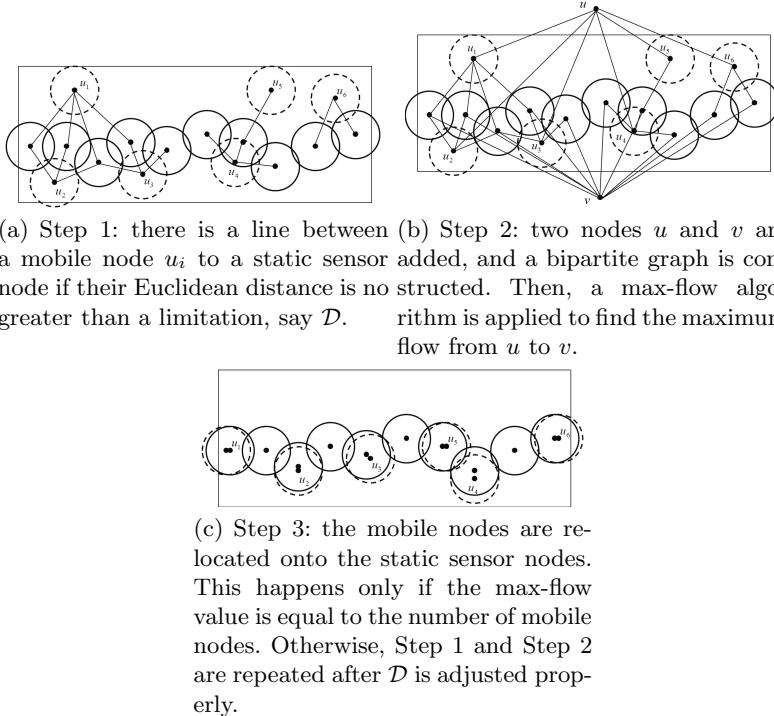


Fig. 1. This figure illustrates how mobile nodes are assigned

be the set of mobile sensor nodes available. Next, we construct the bipartite graph $\mathcal{B} = \{S', M, E\}$, where E will contain an edge between $s_{(a,b)} \in S$ and $u_j \in M$ only if s_a is reachable from u_j if their Euclidean distance is at most \mathcal{D} .

- Step 2: From $\mathcal{B} = \{S', M, E\}$, we construct a new graph $\mathcal{G} = (V_G, E_G)$ such that $V_G = S' \cup M \cup \{u, v\}$ and $E_G = E \cup \{(u, s_{(i,j)}) \mid \text{for all } s_{(i,j)} \in S'\} \cup \{(v, u_i) \mid \text{for all } u_i \in M\}$. Here we assume the capacity of each edge is 1. Then, we apply a maximum flow algorithm such as Ford-Fulkerson[11]) over \mathcal{G} .
- Step 3: Finally, the mobile sensor nodes are assigned in a way that if the maximum flow includes an edge from $s_{(i,j)} \in S'$ to $y \in M$, we assign the mobile sensor node y to s_i . Fig. 1 illustrates how the three steps work.

3.3 Computation of Optimal \mathcal{D}

To find the optimal \mathcal{D} , we utilize binary search. We first compute the distance between every static sensor node and mobile node pair. Suppose $\{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_q\}$ be the list of distinct distances sorted by non-decreasing order. Then, we initially set $\mathcal{D} \leftarrow \mathcal{D}_{\lceil q/2 \rceil}$ and apply our two-phase algorithm introduced in the

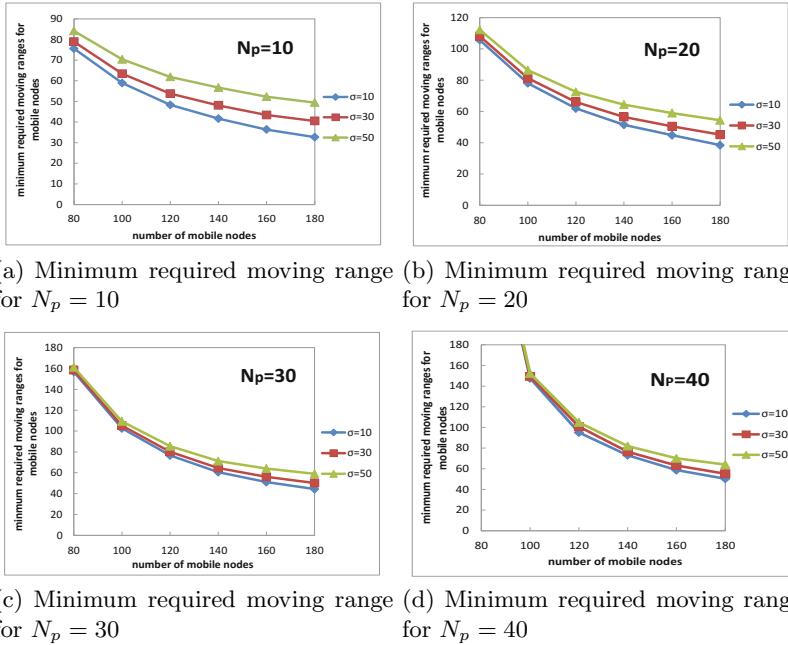


Fig. 2. Performance evaluation of the second phase of the proposed algorithm

previous two steps. If there exists a mobile node m which is not assigned, then we increase \mathcal{D} by setting $\mathcal{D} \leftarrow \mathcal{D}_{\lceil(q+q/2)/2\rceil}$. Otherwise, we decrease \mathcal{D} by setting $\mathcal{D} \leftarrow \mathcal{D}_{\lceil(1+q/2)/2\rceil}$. We keep repeat this until we cannot proceed any further. Then, we will find minimum \mathcal{B} which allows all of the mobile sensor nodes to be assigned. We now prove this strategy results in an optimal solution for this relocation problem.

Theorem 1. *The proposed relocation algorithm with binary search results in an optimal solution.*

Proof. The proof of Lemma 1 is omitted due to space limitation.

3.4 Further Extension with Time Slots

The algorithm described above can be easily implemented in a time slot based system as done by He et al. [1]. That is, we first consider the continuous time domain into a series of time slots with the same length. Then, we assume the time series shown in Eq. (1) are from current time slot. Then, using the first phase of our approach described in this section, we determine the vulnerability of each sensor node in the next time slot. Once decided, we deploy the mobile sensor nodes using the second phase of our approach. At the end of each time slot,

we reanalyze the vulnerability of each sensor node and redistribute the sensor node. One benefit of this time slot based approach against the case without it is that we use relatively new history of intruders only rather than using all of the accumulated history to analyze the vulnerability of each node. Depending on the applications, this can improve the accuracy of the prediction achieved by grey model GM(1,1).

4 Simulation Results and Analysis

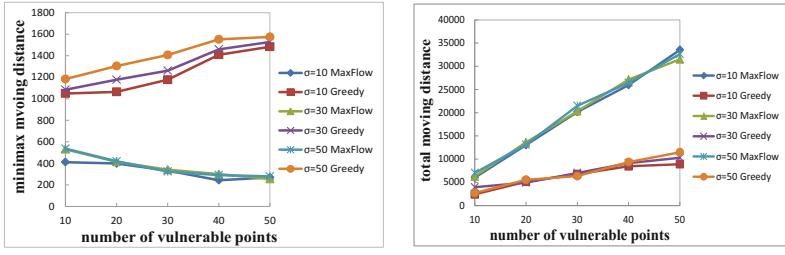
4.1 Performance Evaluation of Mobile Node Relocation Algorithm

In this section, we evaluate the performance of the second phase of our algorithm. We set the number of vulnerable sensor nodes N_p to be 10, 20, 30, and 40. In this simulation, we consider a barrier formed by 100 sensors deployed over a 2000×200 rectangle space. Then, we randomly deploy m mobile sensor nodes along the barriers based on three different random offset variances $\sigma=10, 30$, and 50. Note that with larger variance used, the mobile sensors have a better chance to be located further from the barrier. Under the same parameter setting, we apply our algorithm for 100 instances and compute the averaged value.

Fig. 2 shows the relationship among the number of mobile nodes, the minimum required moving distance of the nodes, and N_p . In Fig. 2(a), N_p is set to 10 and the number of mobile nodes is increased. As we can observe, with more mobile nodes, the mobile node can be completely relocated within less time. We can also observe that with smaller σ value, the travel distance becomes smaller. We can observe the similar trend from Fig. 2(b), Fig. 2(c), and Fig. 2(d). By comparing Fig. 2(a), Fig. 2(b), Fig. 2(c), and Fig. 2(d), we also can learn the effect of σ is constant regardless from the N_p value, which seems natural. On the other hand, with large N_p value, the maximum travel length of mobile sensor nodes for relocation is greater. From this result, to cover all of the vulnerable nodes, a mobile node may need to travel further as the number of vulnerable nodes increase. We believe this is because to assign all of the mobile nodes, some nodes may need to travel very far, and this happens more often if we have more number of vulnerable nodes.

4.2 Performance Comparison of Mobile Node Relocation Algorithm against He et al.'s Strategy [1] for Our Purpose

In [1], He et al. introduced a multiple mobile sensor node relocation algorithm called CSP whose goal is to relocate a group of mobile sensor nodes into a subset of regions based on some probability model to maximize the chance to detect intruders. Therefore, their algorithm also can be used to relocate mobile sensor nodes to solve our problem by replacing our max-flow based algorithm after Step 2 of Phase 2 described in Section 3.2. Note that our algorithm also can be used for their problem. In detail, the CSP algorithm is a greedy algorithm which tries to assign each available mobile sensor to the closest vulnerable point. It assumes



(a) Minimum moving range to monitor all vulnerable points (b) Total moving range to monitor all vulnerable points

Fig. 3. Performance evaluation of mobile node relocation algorithm compare with He et al.'s strategy

that all mobile sensors and vulnerable points are on a straight line, and each vulnerable point is monitored by one mobile sensor. In our scenario, our mobile sensors and vulnerable points are not necessarily on a straight line. However, we can still use the main idea of CSP algorithm. This can be done by iteratively selecting a vulnerable point that has not been assigned any mobile sensor yet, and assign it to the closest available mobile sensor. This process is repeated until all vulnerable points are occupied. Since CSP algorithm assumes the number of available mobile sensor nodes is equal to the number of vulnerable points, so we keep this assumption for a fair comparison.

Fig. 3 show our simulation results. From the figures, we can learn that the min-max distance of the outputs of our algorithm is better than that of He et al's greedy algorithm (greedy). On the other hand, the total distance that the mobile sensor nodes are moving around is larger than that of greedy's. This is due to the difference in the objectives of the algorithms. That is, the goal of our algorithm is to minimize the min-max distance achieved by the mobile sensor nodes while the goal of He et al's greedy algorithm is to minimize the total (average) distance achieved by the mobile sensor nodes. Therefore, our algorithm outperforms He et al's greedy algorithm for our problem.

5 Conclusion

In this paper, we introduce a new paradigm to use mobile sensors to fortify the barrier of static wireless sensors. Our approach is based on GM(1,1) which helps to predict which sensor node has a better chance to detect intruders based on the past record of the intruders detected. We assume that a sensor node has a higher chance to detect an intruder because the intruder consider the area covered by the sensor node is easier to penetrate. Therefore, we deploy available mobile sensor nodes to strengthen the coverage of those sensors. The algorithm that we proposed in this paper also utilizes a binary search approach to minimize the maximum travel length of the mobile sensor nodes, and thus make the relocated done in a timely manner. Our simulation results suggest

some interesting properties of our algorithm, especially about the second phase which concern about the relocation.

References

1. He, S., Chen, J., Li, X., Shen, X., Sun, Y.: Cost-effective Barrier Coverage by Mobile Sensor Networks. In: Proc. of the 31th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM (2012)
2. Chen, A., Kumar, S., Lai, T.H.: Designing Localized Algorithms for Barrier Coverage. In: Proc. of the 13th ACM Annual International Conference on Mobile Computing and Networking, Mobicom (2007)
3. Kumar, S., Lai, T., Arora, A.: Barrier Coverage with Wireless Sensors. In: Proc. of the 11th ACM Annual International Conference on Mobile Computing and Networking, Mobicom (2005)
4. Mao, M., Chirwa, E.C.: Application of Grey Model GM (1, 1) to Vehicle Fatality Risk Estimation. Technological Forecasting and Social Change 73(5), 588–605 (2006)
5. Zhanfeng, Z.: Forecast Model of Logistics on Central Plains area Based on Gray System Theory. Industrial Technology Economy 27(3), 73–76 (2008)
6. Fang, X., Fang, J.: Human Motion Tracking Based on Adaptive Template Matching and GM (1,1). In: Proc. of 2009 International Workshop on Intelligent Systems and Applications, ISA (2009)
7. Xiao, L., Peng, X., Wang, Z., Xu, B., Hong, P.: Research on Traffic Monitoring Network and its Traffic Flow Forecast and Congestion Control Model Based on Wireless Sensor Networks. In: Proc. of the 3rd International Conference on Measuring Technology and Mechatronics Automation, ICMTMA (2009)
8. Soni, S.K., Chand, N., Singh, D.P.: Reducing the Data Transmission in WSNs using Time Series Prediction Model. In: Proc. of IEEE International Conference on Signal Processing, Computing and Control, ISPCC (2012)
9. Saipulla, A., Liu, B., Xing, G., Fu, X., Wang, J.: Barrier Coverage with Sensors of Limited Mobility. In: Proc. of the 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 201–210 (2010)
10. Zhang, H., Hou, J.C.: Maintaining Sensing Coverage and Connectivity in Large Sensor Networks. Ad Hoc Sensor Wireless Network 1(1-2), 89–124 (2005)
11. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms, 2nd edn. MIT Press and McGraw-Hill (2001)
12. Cheng, S., Li, J., Cai, Z.: $O(\epsilon)$ -Approximation to Physical World by Sensor Networks. In: Proc. of the 32nd Annual IEEE International Conference on Computer Communications, IEEE INFOCOM (2013)
13. Cai, Z., Ji, S., Li, J.: Data Caching-based Query Processing in Multi-sink Wireless Sensor Networks. International Journal of Sensor Networks (IJSN) 11(2), 109–125 (2009)
14. Li, J., Cheng, S., Gao, H., Cai, Z.: Approximate Physical World Reconstruction Algorithms in Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, TPDS (2014)

2- m -Domatic Partition in Homogeneous Wireless Sensor Networks*

Lili Jia¹, Jiguo Yu^{1, **}, Dongxiao Yu², and Qingbo Zhang¹

¹ School of Computer Science, Qufu Normal University,
Ri-zhao, Shandong, 276826, P.R. China

{lily_qfnu, qingbozh}@163.com, jiguoyu@sina.com, yu@mail.qfnu.edu.cn

² Department of Computer Science, The University of Hong Kong
Pokfulam, Hong Kong, China
dxyu@cs.hku.hk

Abstract. Due to limited battery power, energy efficiency is an important issue to design efficient protocols in wireless sensor networks, which greatly affects the lifetime of the networks. Fault tolerance is an important approach to design efficient protocols, with which the networks has strong robustness. In this paper, we propose r - m -domatic partition (r - m -DP) problem to design energy efficient fault tolerance. In a wireless sensor network, the r - m -DP problem is to find some disjoint r - m -dominating sets in the network. Based on the uniform clustering, a constant-factor approximation algorithm for 2- m -DP is proposed. To the best of our knowledge, this is the first algorithm for 2- m -DP. The correctness and performance of the algorithm are confirmed by theoretical analysis.

Keywords: wireless sensor networks, domatic partition, energy efficiency, clustering, fault tolerance.

1 Introduction

Wireless sensor networks (WSNs) are multi-hop, self-organizing autonomous networks, without relying on any existing or predefined network infrastructure. And terminal nodes are randomly deployed. WSNs are decentralized distributed systems. Numerous sensors are densely disposed in the monitor region with a random manner. Sensors are used for collecting physical parameters such as light intensity, sound, or temperature. Attention has been paid to WSNs in recent years, which are being widely used in military and civil applications such as battle fields, disaster recoveries, conferences, concerts, environmental detections, health applications and so on.

In WSNs, sensor nodes usually are charged with battery whose energy is limited and placed one-time, which makes it impossible for a second charging. Therefore, energy is an important problem to be considered. In a WSN, finding

* The work is supported by NNSF of China for contract(61373027, 11101243) and NSF of Shandong Province for contract(ZR2012FM023).

** Corresponding author.

a dominating set is generally used for data gathering. While the dominators in the dominating set consume too much extra overheads such as gathering, processing and forwarding data which deplete energy faster than other nodes, and shorten the lifetime of the network. Consequently, it is an important challenge to find a mechanism for balancing energy consumption and prolonging the network lifetime.

Topology control is an important approach to improve the energy efficiency. It includes two basic methods, power control and sleep scheduling [1]. The power control is to change the transmission power of the nodes to reduce the network topology, save energy, and increase the lifetime of the network while preserving connectivity and coverage. However, the approach can not prevent the transmission of redundant information when several nodes are close to each other and may not simplify the network topology enough to make the networks scalable for large deployments. In the hierarchical topology construction approach represented by sleep scheduling [2], a subset of nodes is selected as a communication layer, and only the nodes in the communication layer transmit data, greatly reducing the transmission of redundant information, simplifying the topology of the network, saving the energy for information gathering and filtering, routing and forwarding information required [3-11].

Sleep scheduling is a standard approach for balancing energy consumption, which has been abstracted as the domatic partition problem. Given a graph $G = (V, E)$, a dominating set (DS) of G is a subset of vertices D of V such that each node $v \in V$ is either in D or has a neighbor in D . A r -hop dominating set (r -DS) of G is a subset of vertices D of V such that each node $v \in V$ is either in D or has a r -hop neighbor in D . A domatic partition (DP) (or r -domatic partition (r -DP)) is a partition $\mathcal{D} = \{D_1, D_2, \dots, D_t\}$ of V such that each block D_i of \mathcal{D} is a DS (or r -DS) of G , where t is called domatic number. The domatic partition problem seeks a domatic partition with maximal domatic number. To understand the motivation, suppose that $\mathcal{D} = \{D_1, D_2, \dots, D_t\}$ is a DP of G . By rotating the DSs in DP, the nodes in the network can be dominators alternately. Thus, each node in the network has a chance to become a dominator and then the energy consumption among nodes is balanced and the lifetime of the network is prolonged.

Clustering is a basic and effective method of sleep scheduling. It is a fundamental mechanism to design scalable sensor network protocols. A good clustering imposes a high-level structure on the network. It is easier to design efficient protocols on this high-level structure than that of the individual node. Many efficient protocols have been proposed such as [12-16].

Fault tolerance is necessary for routing since nodes in WSNs which are prone to failures, may have mobility and turn on/off frequently. Thus, it is important to maintain a certain degree of redundancy in a dominating set or a connected dominating set. To improve the fault tolerance of the network, the r -hop m -dominating set (r - m -DS) was proposed. Every node v not in r - m -DS has at least m neighbors within r -hop in D . When selecting dominating nodes, redundancy is achieved by choosing a value for the parameter m greater than one. At the same

time, the distance parameter r allows increasing local availability by reducing the distance to the dominating nodes. Depending on the requirements, problems that require the computation of a DS can be solved by setting the two dominating parameters appropriately.

So far, the r -DP problem and the r - m -DS problem are studied independently. In this paper we combine the two problems into one new energy efficient fault tolerance, r - m -domatic partition (r - m -DP). A r - m -DP of G is a partition $\mathcal{D} = \{D_1, D_2, \dots, D_t\}$ of V such that each block D_i of \mathcal{D} is a r - m -DS of G , where t is called r - m -domatic number (r - m -DN). The r - m -DP problem is to seek a r - m -DP with maximal r - m -DN. It has the following two advantages:

1. By rotating the r - m -DSs in r - m -DP, the energy consumption of the nodes in the network can be balanced and hence the lifetime of the network can be greatly prolonged.
2. If some node of a r - m -DS becomes invalid, other fault-tolerant nodes can also work for data gathering. When $m - 1$ nodes become invalid, the r - m -DS becomes a r -1-DS and there is still a r -hop dominating set for data gathering application.

In this paper, we propose a uniform distributed clustering (UDC) algorithm and obtain a 2- m -DP.

The rest of this paper is organized as follows. Section 2 reviews the existing algorithms for domatic partition and fault tolerant mechanism. Section 3 presents the algorithm for 2- m -DP in detail and the performance by theoretical analysis. Finally, section 4 concludes this paper. We show the results of simulation in the Appendix.

2 Related Work

To save energy consumption and prolong the lifetime of the network, many algorithms for domatic partition are proposed.

In [17], Cardei et al. proposed a centralized algorithm using graph coloring, without providing any bound analysis, to generate a number of disjoint dominating sets in order to reduce energy consumption. To maximize the lifetime of a sensor network, in [18], Islam et al. also used the graph coloring to obtain a domatic partition without any bound analysis.

In [19], applying the graph coloring theory, Feige et al. proposed a centralized algorithm that produces a domatic partition of $\Omega(\delta/\ln \Delta)$ sets. In [20], Moscibroda and Wattenhofer proposed a randomized, distributed algorithm which is an $O(\log n)$ -approximation with high probability in arbitrary graphs. This algorithm is the distributed implementation of the centralized algorithm in [19].

In [21], Pemmaraju and Pirwani proposed a new method of uniform partition and gave three deterministic, distributed algorithms for finding k -domatic partition of size at least a constant fraction of the largest possible $(k - 1)$ -domatic partition for $k > 1$. The first algorithm runs in constant time on unit ball graphs (UBGs) assuming that all nodes know their positions in a global coordinate system. The second algorithm runs in $O(\log n)$ time on UBGs dropping knowledge of global coordinates and instead assuming that pairwise distances between

neighboring nodes are known. The third algorithm runs in $O(\log(\log n))$ time on growth-bounded graphs dropping all reliance on geometric information and using connectivity information only. In [22] Pandit et al. first drove a constant-factor distributed algorithm that can be implemented in $O(\log n)$ rounds of communication in the congest model on unit disk graphs (UDGs).

In [23], Mahjoub and Matula showed that simple topology-based graph coloring can, in practice, not only solve the domatic partition problem in random geometric graphs (RGGs) but also provide $(\delta+1)$ disjoint $(1-\varepsilon)$ dominating sets on a large range of experimented graphs. Later, they carried the study further in [24] by proposing a practical solution to the distributed $(1-\varepsilon)$ dominating sets partition problem that is based on localized graph coloring algorithms.

In [25], Misra and Mandal proposed a domatic partition based scheme for clusterhead rotation on UDGs from the technical application of the uniform partition idea. While, the clusterhead rotation via re-clustering is a global operation which suffers from significant energy overheads when rotation. Later, in [26], Misra and Mandal proposed an efficient rotation scheme using local rotation with the aim of reducing wasteful energy in re-clustering. Followed by these works, in [27], Misra and Mandal studied connected domatic partition (CDP) problem, which essentially involves partitioning the nodes V of a graph G into node disjoint connected dominating sets. They developed a distributed algorithm for constructing the CDP of size at least $\lfloor \frac{\delta+1}{\beta(c+1)} \rfloor - f$, where δ is the minimum node degree of G , $\beta \leq 2$, $c \leq 11$ is a constant for a UDG, and the expected value of f is $\epsilon\delta|V|$, where $\epsilon \ll 1$ is a positive constant, and $\delta \leq 48$. More recently, in [28], Yu et al. proposed a centralized and a distributed constant factor algorithms for domatic partition problem in UDGs.

To improve the fault tolerance of the network, many algorithms are proposed. The connected r -m-DS and k -connected m -dominating set (k -m-CDS) are proposed for fault tolerance.

A connected r -m-DS (r -m-CDS) of G is a r -m-DS and the induced graph of r -m-DS is connected. In [29], Zhang et al. gave two approximation algorithms to compute a minimum r -m-CDS, the first one is a coloring heuristic algorithm to compute a r -m-CDS for UDGs, the other is a greedy algorithm to compute a r -m-CDS for a general graph. In [30], Li et al. also gave two approximation algorithms to compute a minimum r -m-CDS, the first one is constructing an m -DS in the power graph induced by the initial graph, and then extend it into a r -m-CDS, the other one is directly constructing a r -m-DS in the initial graph and then extends it into a r -m-CDS.

A k -m-CDS of G is a vertex subset D of V such that each vertex v not in D is adjacent to at least m vertices in D and the induced graph of D is k -connected. In [31], Dai and Wu proposed four localized k -k-CDS construction protocols, where $m = k$. The first protocol randomly selects virtual backbone nodes with a given probability p_k , where p_k depends on the value of k and network condition, such as network size and node density. The second one maintains a fixed backbone node degree of B_k , where B_k also depends on the network condition. The third protocol is a deterministic approach. It extends the coverage condition, which is

originally designed for CDS construction, to ensure the formation of a k - k -CDS. The last protocol is a hybrid of probabilistic and deterministic approaches. It provides a generic framework that can convert many existing CDS algorithms into k - k -CDS algorithms.

In [32], Wang et al. proposed a 64-approximation centralized algorithm CDSA to construct a 2-connected dominating set, which is only for the case where $k = 2$ and $m = 1$. In [33], Thai et al. proposed a centralized algorithm which requires the input graph to be at least $\max(k, m)$ connected. Firstly, a 1- m -CDS is built and then it is augmented to become a k - m -CDS sequentially. However, this algorithm is not easy to implement due to the difficulty in finding all the k -blocks or k -leaves from a graph.

In [34], Wu et al. proposed a centralized algorithm CGA and a distributed algorithm DDA. The main idea of CGA is to construct a m -dominating set first and then augment the set to be k -connected by adding enough number of connectors. Although CGA can be implemented easily, it cannot guarantee obtaining a k - m -CDS. The main idea of DDA is the same as that of CGA except that DDA builds a 1- m -CDS first. However, a lot of control messages are needed in DDA, which makes the message complexity of DDA very high. Later, in [35], Wu and Li proposed a centralized algorithm ICGA which has the performance ratio that CGA can not provide and a distributed algorithm LDA which has lower message complexity than DDA.

In [36], Shang et al. proposed three centralized algorithms. One is for constructing a 1- m -CDS. Another is for constructing a 2- m -CDS whose basic idea is similar to the work in [31]. The last one first constructs a k -connected k -dominating set for $3 \leq k \leq m$ and then sequentially constructs an maximal independent set(MIS) $m - k$ times. In [37], Shang et al. studied minimum k -connected m -tuple dominating set problem. A k -connected m -tuple DS of G is a vertex subset D of V such that each vertex $v \in V$ is adjacent to at least m vertices in D and the induced graph of D is k -connected. They proposed two algorithms for the cases of $m = 1$ and $m = 2$.

In [38], Tiwari et al. proposed solutions for efficient construction of a fault-tolerant CDS where the nodes have different transmission ranges. Then, they formulated the problem as a k - strongly connected m -dominating and absorbing set problem (k - m -SCDAS). They first proposed two heuristics, one to construct a 1- m -SCDAS and the other one to obtain a k -1-SCDAS in a directed graph, and then combined these two approaches to develop a general construction of k - m -SCDAS.

For other DS and DP related results, one can refer to [39, 40].

3 A 2- m -Domatic Partition Algorithm

3.1 Network Model

We make some reasonable assumptions regarding the network model as follows.

1. There are N sensor nodes that are distributed at random in a square field with area $\|\mathcal{A}\|$.

2. All sensor nodes have the same initial energy and transmission radius R . So the network is homogenous and the graph corresponding to the network is an unit disk graph (UDG).

3. Each sensor node has a globally unique identification id .

3.2 Uniform Clustering-Based Algorithm for 2-m-DP (UC2mDP)

This section presents a uniform clustering-based algorithm for 2-m-DP (UC2mDP). The formation of 2-m-DP is divided into four phases: information collection phase with duration T_1 , clusterhead competition phase with duration T_2 , cluster formation phase with duration T_3 and the coloring phase with duration T_4 . The values of T_1 , T_2 , T_3 and T_4 are estimated and predetermined beforehand.

Phase 1. Information Collection Phase

In this phase, each node broadcasts a *Node_Msg* message with its id . Meanwhile, each node receives the *Node_Msg* from its neighbor nodes. Thus, each node is aware of its degree denoted by d . For each node i , we give the following formula to calculate its waiting time t_i for broadcasting the *Head_Msg* message.

$$t_i = \begin{cases} \frac{D-1}{d} \times \frac{T_2}{2} \times \rho & d \geq D \\ \frac{T_2}{2} + (1 - \frac{d}{D-1}) \times \frac{T_2}{2} \times \rho & d < D \end{cases} \quad (1)$$

Where t_i denotes the waiting time of node i . D is the estimated average number of nodes in one disk with radius R , and its value is preset for $\lfloor \frac{Nr^2}{\|\mathcal{A}\|} \rfloor$, where N is the number of nodes which are distributed in the square field with area $\|\mathcal{A}\|$. ρ is a real value uniformly distributed in $[0.9, 1]$ which is introduced to reduce the probability that two nodes send *Head_Msg* at the same time. It is quite clear that $\frac{D-1}{d} \times \frac{T_2}{2} \times \rho < \frac{T_2}{2} < \frac{T_2}{2} + (1 - \frac{d}{D-1}) \times \frac{T_2}{2} \times \rho$. In the first half period t_i ranging form 0 to $\frac{T_2}{2}$ identifies the clusterheads with large degree. The last half period t_i ranging from $\frac{T_2}{2}$ to T_2 selects the clusterheads among the rest of nodes in the uncovered area.

Phase 2. Clusterhead Competition Phase

In this phase, if a node does not receive the *Head_Msg* when its waiting timer t_i expires, it broadcasts the *Head_Msg* to notify that it will be a clusterhead. Otherwise, it gives up the competition.

Phase 3. Cluster Formation Phase

In this phase, there are three cases for the non-clusterhead nodes joining a cluster.

Case 1. If a non-clusterhead node v only receives *Head_Msg* from only one clusterhead, then it becomes a cluster member of the cluster.

Case 2. If a non-clusterhead node v receives *Head_Msg* from different clusterheads, then it becomes a cluster member of the cluster whose size is currently

less than $\lfloor \frac{\delta}{(c+1)} \rfloor$ (δ is the minimum vertex degree of graph G and c is a constant defined in section 3.3, $c \leq 11$), if such a cluster exists.

Case 3. Otherwise, the non-clusterhead node v becomes a cluster member of the cluster whose clusterhead is closest to v .

When a non-clusterhead node affiliates with a clusterhead, it sends the *Join_Msg* with its *id* and the *id* of the clusterhead. The clusterhead sorts its members according to the sequence of its members affiliating it.

At this time, the first three phases of UC2mDP finish and they are collectively called the uniform clustering phase. The size of any cluster obtained by this phase is at least $\lfloor \frac{\delta}{(c+1)} \rfloor$ (The proof is shown in the following theorem 3).

Phase 4. Coloring Phase

In this phase, each clusterhead successively broadcasts a *Coloring_Msg* to message every m cluster members in the sorted sequence. The message contains the sequence number of sending the message and the *ids* of the m cluster members. The corresponding m cluster members receive the *Coloring_Msg* and color themselves with the sequence number that is also their coloring number. That is, use the sequence number as an assignment of labels to the corresponding m cluster members.

So far UC2mDP finishes and then all the cluster members with the same coloring number consist of a 2- m -DS. It is observed that UC2mDP has the following properties.

1. UC2mDP is a distributed algorithm, and hence it is suitable for large-scale wireless sensor networks.
2. UC2mDP produces the most clusterheads with large degree in the first half period t_i . This ensures that the nodes with relatively larger degree become the clusterheads and hence contributes to bring more nodes together in each cluster.
3. UC2mDP produces the few clusterheads from the rest of nodes in the last half period t_i . This avoids the generation of isolated nodes to guarantee complete coverage.

3.3 Theoretical Analysis of UC2mDP

Theorem 1. There is no other clusterhead in the coverage of each clusterhead.

Proof. According to formula (1), the waiting time t_i of each node almost uniformly distributes in the whole of duration T_2 . Suppose that when some node broadcasts a *Head_Msg*, all of its neighbor nodes can receive the *Head_Msg*, in duration Δt . Obviously, the node would be the only clusterhead in its coverage if its neighbor nodes do not broadcast the *Head_Msg* in the duration Δt . While there would exist multi-clusterheads in the coverage of a clusterhead if multi-nodes broadcast the *Head_Msg* at the same time. Now we discuss the probability that there exist multi-clusterheads in the coverage of a clusterhead.

Since the time t_i of each node for broadcasting the *Head_Msg* uniformly distributes in the whole duration T_2 , the probability that only one node broadcasts the *Head_Msg* in its coverage will fulfill the following inequality:

$$P \geq C_{n_{exp}-1}^0 \left(1 - \frac{\Delta t}{T_2}\right)^{n_{exp}-1}. \quad (2)$$

Where n_{exp} is the expected number of the nodes in the coverage of one node and obviously, $n_{exp} = \lceil \frac{N\pi R^2}{\|\mathcal{A}\|} \rceil$. For a specific wireless sensor network, N and Δt are all constants. For example, assume that $R = 15m$, $\|\mathcal{A}\| = (100 \times 100)m^2$, $N = 100$, $\Delta t = 10ms$ and $T_2 = 10s$, then we can obtain $P \geq 0.994$. This means the probability that multi-nodes broadcast the *Head_Msg* at the same time is rather low. In addition, by extending the duration T_2 or decreasing the cluster radius, we can further guarantee that there is no other clusterhead in the coverage of each clusterhead. \square

Theorem 2. All the clusterheads produced by UC2mDP form a maximal independent set.

Proof. To prove that the produced clusterheads forms a maximal independent set (MIS), we firstly prove that they form an independent set (IS). By theorem 1, there is no another clusterhead in the coverage of each clusterhead. Thus, there is no link between any two clusterheads. Therefore, all the clusterheads form an IS. In the network, each node is either a clusterhead or a cluster member. If we arbitrarily add a cluster member into the IS formed by clusterheads, the independence of the clusterheads is destroyed. Therefore, all the produced clusterheads form a MIS. \square

For a given graph $G = (V, E)$, let $d(u, v)$ to denote the length of the shortest uv -path in G measured by counting the number of edges in the path. The k -neighborhood of v is $N_k(v) = \{u : 0 < d(u, v) \leq k\}$. The cluster with v being its clusterhead denotes as C_v . The maximum size of an IS in $N_2(v) - N_1(v)$ for any node v is a constant c in UDG. The constant c is used in our algorithm, which is given in the following lemma 1:

Lemma 1. For any node v in an UDG, the size of an IS in $N_2(v) - N_1(v)$ is a constant $c \leq 11$, which is the number of 2-hop independent neighbors of v excluding its 1-hop independent neighbors.

The detail proof of Lemma 1 is shown in the reference [27].

Theorem 3. The size of any cluster obtained by UC2mDP is at least $\lfloor \frac{\delta}{(c+1)} \rfloor$, where δ is the minimum vertex degree of graph G , and c is a constant and $c \leq 11$.

Proof. The bound on $c \leq 11$ comes from Lemma 1. It follows from the given construction procedure of the cluster partitions. Consider the worst case. The

waiting time of node v , with the minimum degree δ , expires and it sends $Head_Msg$ to its neighbors. We assume it has the maximum IS (called I) in $N_2(v) - N_1(v)$, the size of which is c ($c \leq 11$). The maximum size of C_v is at most δ , if all its neighbors are closest to itself and the size of each cluster C_u , $u \in I$, is at least $\lfloor \frac{\delta}{(c+1)} \rfloor$. It all can follows from case 2 and case 3 of phase 3. Otherwise, the size of C_v will be $\lfloor \frac{\delta}{(c+1)} \rfloor$, when δ neighbor nodes of v are evenly partitioned to $c + 1$ clusters including cluster v . Case 2 and case 3 of phase 3 ensure that the size of C_v is at least $\lfloor \frac{\delta}{(c+1)} \rfloor$. Therefore, the lower bound of $\lfloor \frac{\delta}{(c+1)} \rfloor$ is always met. \square

Theorem 4. The algorithm UC2mDP produces a 2- m -DP with size at least $\lfloor \frac{\delta}{(c+1)m} \rfloor$, where δ is the minimum vertex degree of graph G , and c is a constant and $c \leq 11$.

Proof. In the coloring phase, m nodes are chosen in each cluster, and then all the chosen nodes consist of a 2- m -DS of G . Since in each cluster, any node can 2-hop reach the other nodes by the clusterhead, and such m nodes are chosen, so they can 2-hop m -dominate the other nodes in the cluster, that is, all the m nodes chosen from every cluster consist of the 2- m -DS of G . By Theorem 3, the cluster size is at least $\lfloor \frac{\delta}{(c+1)} \rfloor$, so we can get at least $\lfloor \frac{\delta}{(c+1)m} \rfloor$ 2- m -DSs, which form a 2- m -DP. \square

4 Conclusion

In this paper, we propose an new energy efficient fault tolerance problem called r - m -domatic partition (r - m -DP), which combines the energy efficiency and fault tolerance. Based on the uniform clustering, we give a constant-factor approximation algorithm for 2- m -DP, which is only for the case where $r = 2$. In the future, we will focus on designing algorithms to break the constraints and make it adaptive to the high density wireless networks.

References

1. Labrador, M.A., Wightman, P.M.: Topology control in wireless sensor networks. Springer Science + Business Media BV (2009)
2. Wu, J., Wu, B., Stojmenovic, I.: Power-aware broadcasting and activity scheduling in ad hoc wireless networks using connected dominating sets. In: Proc. IASTED International Conference on Wireless and Optical Communication, WOC 2002 (2002)
3. Das, B., Bharghavan, V.: Routing in ad hoc networks using minimum connected dominating sets. In: ICC 1997, Montreal, Canada (June 1997)
4. Guha, S., Khuller, S.: Approximation algorithms for connected dominating sets. Algorithmica 20, 374–387 (1998)
5. Wan, P., Alzoubi, K.M., Frieder, O.: Distributed Construction of Connected Dominating Set in Wireless Ad Hoc Networks. In: Proc. IEEE Conference on Computer Communications (INFOCOM), pp. 141–149 (2002)

6. Funke, S., Kesselman, A., Meyer, U., Segal, M.: A simple improved distributed algorithm for minimum CDS in unit disk graphs. *ACM Trans. Sensor Network* 2(3), 444–453 (2006)
7. Wu, J., Dai, F., Yang, S.: Iterative local solutions for connected dominating set in ad hoc wireless networks. *IEEE Transactions on Computers* 57(5), 702–715 (2008)
8. Li, Y., Kim, D., Zou, F., Du, D.: Constructing minimum connected dominating sets with bounded diameters in wireless networks. *IEEE Transactions on Parallel and Distributed System* 20(2), 147–157 (2009)
9. Yu, J., Wang, N., Wang, G.: Heuristic algorithms for constructing minimum connected dominating sets with bounded diameters in wireless networks. In: Pandurangan, G., Anil Kumar, V.S., Ming, G., Liu, Y., Li, Y. (eds.) WASA 2010. LNCS, vol. 6221, pp. 11–20. Springer, Heidelberg (2010)
10. Wu, J.: Extended dominating-set-based routing in ad hoc wireless networks with unidirectional links. *IEEE Trans. Parallel and Distributed Computing* 13(9), 866–881 (2002)
11. Yu, J., Wang, N., Wang, G.: Constructing minimum weakly connected dominating sets for clustering in ad hoc networks. *J. Parallel Distrib. Comput.* 72(1), 35–47 (2012)
12. Han, B., Jia, W.: Clustering wireless ad hoc networks with weakly connected dominating set. *J. Parallel Distrib. Comput.* 67, 727–737 (2007)
13. Yu, J., Qi, Y., Wang, G.: An energy-driven unequal clustering protocol for heterogeneous wireless sensor networks. *Journal of Control Theory and Applications* 9(1), 133–139 (2011)
14. Yu, J., Qi, Y., Wang, G., Gu, X.: A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. *AEÜ - International Journal of Electronics and Communications* 66(1), 54–61 (2012)
15. Yu, J., Qi, Y., Guo, Q., Gu, X.: EADUC: An energy-aware distributed unequal clustering protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks* 2011, Article ID 202145, 8 (2011), doi:10.1155/2011/202145
16. Zhou, X., Wu, M., Xu, J.: BPEC: An Energy-aware distributed clustering algorithm in WSNs. *Journal of Computer Research and Development* 46(5), 723–730 (2009)
17. Cardei, M., Maccallum, D., Cheng, M., Jia, X., Li, D., Du, D.: Wireless sensor networks with energy efficient organization. *Journal of Interconnection Networks* 3(3–4), 213–229 (2002)
18. Islam, K., Akl, S., Meijer, H.: Maximizing the lifetime of a sensor network through domatic partition. In: Proceedings of IEEE Conference on Local Computer Networks (2009)
19. Feige, U., Halldorsson, M., Kortsarz, G., Srinivasan, A.: Approximating the domatic number. *SIAM Journal of Computing* 32(1), 172–195 (2003)
20. Moscibroda, T., Wattenhofer, R.: Maximizing the Lifetime of Dominating Sets. *Parallel and Distributed Processing Symposium* 4, 8–15 (2005)
21. Pemmaraju, S., Pirwani, I.: Energy conservation via domatic partitions. In: Proceedings of ACM MobiHoc, pp. 143–154 (May 2006)
22. Pandit, S., Pemmaraju, S., Varadarajan, K.: Approximation algorithms for domatic partitions of unit disk graphs. In: Dinur, I., Jansen, K., Naor, J., Rolim, J. (eds.) APPROX and RANDOM 2009. LNCS, vol. 5687, pp. 312–325. Springer, Heidelberg (2009)
23. Mahjoub, D., Matula, D.: Employing $(1-\varepsilon)$ dominating set partitions as backbones in wireless sensor networks. In: Proceedings of Workshop on Algorithm Engineering and Experiments, ALENEX 2010, pp. 98–111 (2010)

24. Mahjoub, D., Matula, D.W.: Building $(1 - \varepsilon)$ dominating sets partition as backbones in wireless sensor networks using distributed graph coloring. In: Rajaraman, R., Moscibroda, T., Dunkels, A., Scaglione, A. (eds.) DCOSS 2010. LNCS, vol. 6131, pp. 144–157. Springer, Heidelberg (2010)
25. Misra, R., Mandal, C.: Cluster head rotation via Domatic partition in self-organizing sensor networks. In: Proceedings of the International Symposium of Wireless Pervasive Computing (COMSWARE 2007), pp. 5–7 (January 2007)
26. Misra, R., Mandal, C.: Efficient Clusterhead rotation via domatic partition in self-organizing sensor networks. *Wireless Communications and Mobile Computing* 9(8), 1040–1058 (2009)
27. Misra, R., Mandal, C.: Rotation of CDS via connected domatic partition in ad hoc sensor networks. *Proc. IEEE Transactions on Mobile Computing* 8(4), 488–499 (2009)
28. Yu, J., Zhang, Q., Yu, D., Chen, C., Wang, G.: Domatic partition in homogeneous wireless sensor networks. *Journal of Network and Computer Applications* 37, 186–193 (2014)
29. Zhang, Z., Liu, Q., Li, D.: Two algorithms for connected r -hop k -dominating set. *Discrete Mathematics, Algorithms and Applications* 1(4), 485–498 (2009)
30. Li, D., Liu, L., Yang, H.: Minimum connected r -hop k -dominating set in wireless networks. *Discrete Mathematics, Algorithms and Applications* 1(1), 45–57 (2009)
31. Dai, F., Wu, J.: On Constructing k -connected k -dominating set in wireless network. In: IEEE International Parallel and Distributed Processing Symposium, p. 81a (April 2005)
32. Wang, F., Thai, M., Li, Y.: On the construction of 2-connected virtual backbone in wireless networks. *IEEE Transactions on Wireless Communications* 8(3), 1230–1237 (2007)
33. Wu, Y., Fang, F., Thai, M., Li, Y.: Constructing k -connected m -dominating sets in wireless sensor networks. In: Military Communications Conference(MILCOM 2007), pp. 29–31 (October 2007)
34. Thai, M., Zhang, N., Tiwari, R., Xu, X.: On approximation algorithms of k -connected m -dominating sets in disk graphs. *Theoretical Computer Science* 385(1–3), 49–59 (2007)
35. Wu, Y., Li, Y.: Construction algorithms for k -connected m -dominating sets in wireless sensor networks. In: Proc the 9th ACM International Symposium on Mobile Ad hoc Networking and Computing, Hong Kong, China, pp. 83–90 (2008)
36. Shang, W., Yao, F., Wan, P., Hu, X.: Algorithms for minimum m -connected k -tuple dominating set problem. *Theor. Comput. Sci.* 381(1–3), 241–247 (2007)
37. Shang, W., Yao, F., Wan, P.-J., Hu, X.: Algorithms for Minimum m -Connected k -Dominating Set Problem. In: Dress, A.W.M., Xu, Y., Zhu, B. (eds.) COCOA. LNCS, vol. 4616, pp. 182–190. Springer, Heidelberg (2007)
38. Tiwari, R., Mishra, T., Li, Y., Thai, M.: k -Strongly Connected m -dominating and absorbing Set in wireless ad hoc networks with unidirectional links. In: International Conference on Wireless Algorithms, Systems and Applications, pp. 103–112 (August 2007)
39. Yu, J., Wang, N., Wang, G., Yu, D.: Connected dominating sets in wireless ad hoc and sensor networks - A comprehensive survey. *Computer Communications* 36(2), 121–134 (2013)
40. Du, D., Wan, P.: *Connected Dominating Set: Theory and Applications* (Springer Optimization and Its Applications). Springer (2013)

Barrier Coverage Using Sensors with Offsets*

Haosheng Fan¹, Victor C.S. Lee¹, Minming Li¹, Xiao Zhang¹, and Yingchao Zhao²

¹ Department of Computer Science, City University of Hong Kong

{haoshefan2-c,xiao.zhang}@my.cityu.edu.hk,

{csvlee,minming.li}@cityu.edu.hk

² Department of Computer Science, Caritas Institute of Higher Education, Hong Kong

yczhao@cihe.edu.hk

Abstract. One of the most fundamental tasks of wireless sensor networks is to provide coverage of barrier, which focuses on detecting intruders crossing a specific region. Suppose that all sensors are dropped from an aircraft along a given line interval, and each sensor has circular coverage range of arbitrary radii. Due to the environmental factors, the sensors will be distributed along the deployment line interval with random offsets. We study the barrier coverage problem with line-based offsets deployments by a set of wireless sensors with adjustable coverage ranges. The objective is to find a range assignment with the minimum cost. In this paper, we present a constant-approximation algorithm and two fully polynomial time approximation schemes (FPTASes) for the barrier coverage by using sensors with offsets under a linear cost function on the sensor's range. We also show the performance of the approximation algorithms by experiments.

Keywords: Barrier coverage, wireless sensor networks, approximation algorithm.

1 Introduction

In recent years, there has been increasing development in the field of wireless sensor networks (WSN). WSN consists of a number of wireless sensor nodes, which are characterized by having limited battery power. One of the most important applications in WSN is border surveillance and intrusion detection, such as detecting intruders crossing country borders or boundaries of battlefields.

Barrier coverage [1], differing from covering specific points of targets [2] [3] and entire region [4], focuses on detecting intruders in an attempt to cross a specific region. The performance of barrier coverage depends on sensor deployment schemes. Placing sensors one by one regularly on a straight line interval across the region is the best scheme [1] [5], due to its simplicity and efficiency. However, deploying sensors in a deterministic way is sometimes difficult, such as monitoring boundaries of battlefields. A useful alternative way of distribution is to drop sensors from an aircraft along a given path. Note that the sensors dropping from the air would miss their predetermined positions influenced by potential environmental factors like the wind. Consequently, these sensors will be distributed along the deployment line interval with random offsets.

* This work was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China [Project No. CityU 122512].

In this paper, we consider the scenario where sensors with adjustable ranges are deployed along a line interval, which leads to *line-based normal random offset deployment* (LNRO) [5]. Since the power consumed by a sensor is directly related to its range, a natural question is how to assign the ranges to sensors such that total consumption of power is minimized while the line interval is fully covered.

2 Preliminaries

Formally, we put n sensors $\mu_1, \mu_2, \dots, \mu_n$ in the interval $[0, m]$. Each sensor μ_i is represented by a pair of values (x_i, h_i) where x_i is the horizontal distance from the sensor to the leftmost point of the interval and h_i is the vertical distance from the sensor to the interval. Each sensor μ_i has a transmission radius r_i . We define r'_i as the projection of r_i on the interval and $\mathbf{r}_i = [x_i - r'_i, x_i + r'_i]$ as μ_i 's range. The relationship between r_i and r'_i is showed in Figure 1. We say a sensor μ_i is chosen if $r'_i > 0$. For any point x in $[0, m]$, we say it is covered by sensor μ_i if $|x - x_i| \leq r'_i$.

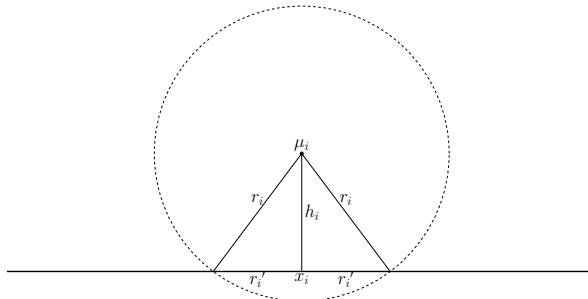


Fig. 1. Each sensor μ_i is represented by (x_i, h_i) where r_i is the radius of μ_i and r'_i is the projection of r_i on the interval

We define $\mathbf{R} = (\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n)$ as a range assignment of interval $[0, m]$ if the whole interval $[0, m]$ is covered by \mathbf{R} . The cost of an assignment \mathbf{R} is defined as $C(\mathbf{R}) = \sum_{i=1}^n r_i^\kappa$ where κ is a positive constant. The main task of this paper focuses on the case when $\kappa = 1$. The assignment with the minimum cost is called the optimal assignment and we use $\mathbf{R}^* = (\mathbf{r}_1^*, \mathbf{r}_2^*, \dots, \mathbf{r}_n^*)$ to denote it.

Due to space limit, we omit some proofs in this version.

3 Related Works

Most of previous studies on WSN coverage assume that each sensor has a fixed-radius disk coverage. In this setting, the coverage of a specific area can be considered as monitoring a fixed number of targets. The problem **Min-Weight Disk Cover** attempts to find a subset of given disks with minimum cost to fully cover all targets. When all

disks have the same radius normalized to one, the problem **Min-Weight Disk Cover** is referred to as **Min-Weight Unit-Disk Cover**. In the last ten years, a sequence of incremental improvements over approximation algorithms for the unweighted variant of **Min-Weight Unit-Disk Cover** were made in [6] [7] [8]. Then, extensive works on constant approximation algorithms for **Min-Weight Unit-Disk Cover** were studied in [9] [10] [11] [12]. Recently, a PTAS for the unweighted variant and a randomized $2^{O(\log^* n)}$ -approximation for the weighted variant were developed [3]. Other variants on disk coverage have been explored in [13] [14] [15].

For the case in which the coverage target is a line segment, it is usually defined as barrier coverage problem. In this direction, various works have been done. If sensors are static, Li et al.[16] studied the problem of covering a line interval by wireless sensors with adjustable ranges, where the sensors were located on the segment, referred to as **Min-Cost Linear Coverage (MCLC)**. The objective is to find a range assignment with the minimum cost in two variants (discrete and continuous) of the problem. On the basis of the algorithm for MCLC, the authors in [17] gave a PTAS with a polynomial cost function on the disks' radii.

When the sensors can move, Czyzowicz et al. [18] studied the coverage problem to minimize the maximum sensor movement. They presented an $O(n^2)$ algorithm to compute the optimal movement of sensors with the same sensing range. Later, Chen et al. [19] improved the complexity to $O(n \log n)$ and came up with an $O(n^2 \log n)$ algorithm with arbitrary sensing ranges. Czyzowicz et al. [20] considered covering a line interval with the aim of minimizing the total movement distance. In terms of maximizing the network lifetime, Bar Noy and Baumer [21] studied the lifetime maximization problem on a line segment by sensors with adjustable ranges. In a recent paper [22], Bar Noy et al. studied the problem of maximizing the coverage lifetime of a barrier by mobile sensors with limited battery powers. They obtained profound theoretical results to maximize the network lifetime on two variants of the problem which are distinguished by whether the sensing radii of sensors can be changed.

Suppose that all sensors are dropped from an aircraft along a given line interval, and each sensor has circular coverage range of arbitrary radii. Due to the environmental factors, the sensors will be distributed along the deployment line interval with random offsets. In this paper, we explore the barrier coverage problem with line-based offsets deployments by a set of wireless sensors with adjustable coverage ranges. Each coverage range of a sensor is a disk centered at that sensor whose radius is decided by the power the sensor chooses. The objective is to find a range assignment with the minimum cost. This optimization problem is defined as **General Min-Cost Linear Coverage problem (GMCLC)**.

4 A Constant-Factor Approximation Algorithm for GMCLC

In this section, we give an approximation algorithm with approximation ratio bounded by a constant. If the context is clear, we also use R to represent the cost of assignment \mathbf{R} . Hence, the cost of the optimal assignment \mathbf{R}^* is R^* . We also define P and Q as the leftmost point and rightmost point on the interval, respectively. We assume $m = 1$ in this section and all sections after unless the value of m is defined explicitly.

In the following, we design an algorithm to approximate R^* .

Our algorithm chooses assignments from two groups of assignments. One group contains all the assignments that only use one sensor to cover the interval. For every sensor μ_i , we calculate its distance to P and Q and denote two distances as $dist(\mu_i, P)$ and $dist(\mu_i, Q)$ respectively. In order to cover the interval, we choose the larger distance from $dist(\mu_i, P)$ and $dist(\mu_i, Q)$ as μ_i 's radius and it is also the cost of the assignment using μ_i only. The other group contains all the assignments that only use two sensors to cover the whole interval. We assume these two sensors are μ_A and μ_B where μ_B is on the right of μ_A . If $x_B - x_A \leq \frac{1}{2}$, we can cover the line interval by letting sensor μ_A cover the line interval on its left and letting sensor μ_B cover the line interval on its right. If $x_B - x_A > \frac{1}{2}$, μ_A must cover the line interval on its left and μ_B must cover the line interval on its right. After that, the “center” of the line interval is still uncovered and its range is $[2x_A, 2x_B - 1]$. This sub-interval must be covered by either μ_A or μ_B or both. The optimal solution occurs when $\angle \mu_A Y P = \angle \mu_B Y Q$ where Y is a point within range $[2x_A, 2x_B - 1]$ if it exists. When $\angle \mu_A Y P = \angle \mu_B Y Q$, the sub-interval is covered by both sensors and we have $\frac{r_A'}{r_B'} = \frac{h_A}{h_B}$. If such point does not exist within the range $[2x_A, 2x_B - 1]$, the optimal solution occurs when either μ_A or μ_B alone covers the sub-interval. Special cases such as μ_A or μ_B is located at the end points of the line interval can be handled in a similar way. Details can be found in Algorithm 1.

```

Input:  $x_A, h_A, x_B, h_B$ 
Output: Minimum cost of the range assignment that chooses  $\mu_A$  and  $\mu_B$ 
if  $x_B - x_A \leq \frac{1}{2}$  then
     $r_A' = x_A$ 
     $r_B' = 1 - x_B$ 
else if  $\frac{h_A}{x_A} > \frac{h_B}{1-x_B}$  and  $\frac{h_A}{2x_B - x_A - 1} \geq \frac{h_B}{1-x_B}$  then
     $r_A' = 2x_B - x_A - 1$ 
     $r_B' = 1 - x_B$ 
else if  $\frac{h_A}{x_A} \leq \frac{h_B}{1-x_B}$  and  $\frac{h_A}{x_A} < \frac{h_B}{x_B - 2x_A}$  then
     $r_A' = x_A$ 
     $r_B' = x_B - 2x_A$ 
else
     $r_A' = \frac{h_A(x_B - x_A)}{h_A + h_B}$ 
     $r_B' = \frac{h_B(x_B - x_A)}{h_A + h_B}$ 
end if
 $cost = \sqrt{r_A'^2 + h_A^2} + \sqrt{r_B'^2 + h_B^2}$ 
return  $cost$ 

```

Algorithm 1. Compute the minimum cost when two sensors are chosen

Among all the assignments using only one or two sensors, we choose the one with minimum cost as the output of our algorithm and denote it as R' .

In order to show the approximation ratio of R' , we first prove a lemma about our algorithm.

Lemma 1. *Given two sensors, the result given by Algorithm 1 is the optimal solution if we only use the sensors given.*

Proof. Assume μ_A and μ_B are the two sensors given and without loss of generality, we assume μ_B is on the right of μ_A . It is obvious that $r_A' \geq x_A$, $r_B' \geq 1 - x_B$ and $r_A' + r_B' \geq x_B - x_A$. Therefore, the interval can be covered by the assignment in Algorithm 1. Next, in the optimal assignment \mathbf{R}^* , we should have $x_A + r_A' = x_B - r_B'$, which means the rightmost point covered by μ_A is also the leftmost point covered by μ_B . If $x_A + r_A' > x_B - r_B'$, there must be at least one sensor in μ_A and μ_B going beyond the boundary of the interval. Without loss of generality, we can assume μ_B is the sensor that goes beyond the boundary of the interval. We can reduce its radius until the leftmost point covered by μ_B is $x_A + r_A'$ or the rightmost point is Q . The cost of assignment decreases and the interval is fully covered. We can adjust the radius of μ_A as well in the same way. Because $r_A' + r_B' \geq x_B - x_A$, $x_A + r_A' = x_B - r_B'$ finally. Then the cost function can be written as $cost = \sqrt{r_A'^2 + h_A^2} + \sqrt{(x_B - x_A - r_A')^2 + h_B^2}$. The cost function becomes a function of r_A' . In order to get the assignment with minimum cost, we can take derivative of the cost function and we have $cost' = \frac{r_A'}{\sqrt{r_A'^2 + h_A^2}} - \frac{x_B - x_A - r_A'}{\sqrt{(x_B - x_A - r_A')^2 + h_B^2}}$. When $cost' = 0$, $\frac{r_A'}{r_B'} = \frac{r_A'}{h_B} = \frac{h_A}{h_B}$. This corresponds to the fourth situation in Algorithm 1 if $r_A' \in (x_A, x_B)$. If such $r_A' < x_A$, then the cost function is always increasing. The minimum value happens when $r_A' = x_A$ and it corresponds to the third case in Algorithm 1. Similarly, the minimum value happens when $r_A' = x_B$ if the optimal $r_A' \geq x_B$ and this corresponds to the second case in Algorithm 1.

Therefore, Algorithm 1 returns the optimal solution as long as two sensors are chosen.

Then we can prove the following theorem.

Theorem 1. *The range assignment \mathbf{R}' given by Algorithm 1 is a $\frac{4}{3}$ -approximation.*

5 Two FPTASes for GMCLC with Linear Cost

In this section, two FPTASes will be designed for the GMCLC problem, where the cost of a sensor with radius r is proportional to r^κ for constant $\kappa = 1$.

5.1 Based on Radius Division

Choosing a small positive constant $\epsilon > 0$, we can define a set of radii

$D_m = \{0, \frac{m}{Kn}, \frac{2m}{Kn}, \dots, \lceil \frac{r_{max}Kn}{m} \rceil \frac{m}{Kn}\}$, where r_{max} indicates the maximum distance from any sensor to any endpoint of the line interval and $K = \lceil \frac{2}{\epsilon} \rceil$. Using the discrete radius given by division, there will be $Kn \cdot \lceil \frac{r_{max}}{m} \rceil + 1$ possible radii for each sensor, defining $n \cdot (Kn \cdot \lceil \frac{r_{max}}{m} \rceil + 1)$ possible radii. We can construct a directed weighted graph G and find the shortest path as in [16]. The graph G has $Kn^2 \lceil \frac{r_{max}}{m} \rceil + n + 2$ nodes. The running time of the algorithm is $O((Kn^2 \lceil \frac{r_{max}}{m} \rceil + n + 2)^2) = O((2 \lceil \frac{r_{max}}{m} \rceil n^2 + n + 2)^2) = O(n^4/\epsilon^2)$. We denote this algorithm as Algorithm RD_{off_line} .

Theorem 2. Let $R^* = \sum_i r_i^*$ be the sum of radii in an optimal solution. Then, for any constant number $\epsilon > 0$, there exists an assignment $\mathbf{R}' = (r'_1, r'_2, \dots, r'_n)$ which can cover the whole line interval with $r'_i \in D_m$ and $R' = \sum_i r'_i \leq (1 + \epsilon)R^*$.

Proof. We can increase radius r_i^* in the optimal solution by at most $\frac{m}{K_n}$ to reach the closest value r'_i in D_m . It is easy to see that the new assignment with radius r'_i for sensor μ_i can cover the line interval. Combining with the fact that $R^* \geq \frac{m}{2}$, we have $R' = \sum_i r'_i \leq R^* + n \cdot \frac{m}{K_n} \leq R^* + n \cdot \frac{m\epsilon}{2n} \leq (1 + \epsilon)R^*$, which proves the theorem.

5.2 Based on Line Interval Division

In this section, before we present another FPTAS for GMCLC, an improved FPTAS will be designed for the MCLC with sensors located on the line interval.

Choosing a small constant $\epsilon > 0$, we divide the line interval with length m into $\frac{2n}{\epsilon}$ sub-intervals (to make the discussion easier, we assume $\frac{2n}{\epsilon}$ is an integer), and each sub-interval $I_j = [\frac{(j-1)\epsilon m}{2n}, \frac{j\epsilon m}{2n}]$. We set $L = \{0, \frac{\epsilon m}{2n}, \frac{2\epsilon m}{2n}, \dots, \frac{k\epsilon m}{2n}, \dots, m, \frac{\epsilon m}{2n} + m, \frac{2\epsilon m}{2n} + m, \dots, 2m\}$ and $L(k) = \frac{k\epsilon m}{2n}$. For any value V in interval $I_j = [\frac{(j-1)\epsilon m}{2n}, \frac{j\epsilon m}{2n}]$, we define $\|V\| = \frac{(j-1)\epsilon m}{2n}$. Then, we can use dynamic programming to find an exact optimal solution in pseudo-polynomial time.

To get the optimal solution, we need to create a table with n rows and $(\frac{4n}{\epsilon} + 1)$ columns. Because the rightmost point covered by the last sensor in the optimal solution may not be the rightmost point of the interval, we calculate the *Cost* function of the assignment that can cover the range up to $[0, 2m]$.

Let function $Cost(i, L(k))$ denote the cost of the optimal assignment that covers exactly the range $[0, L(k)]$ using the first i sensors only.

In order to find the optimal assignment that covers the range $[0, L(k)]$ with only the first i sensors, it is equivalent to finding the optimal assignment that at least covers the range $[0, L(k)]$ with only the i sensors because the rightmost point may not be $L(k)$ necessarily. In order to cover the range, we can either use sensor μ_i or do not use sensor μ_i . In the first case, since we select μ_i , we have two options: using μ_i only or using μ_i and some sensors in the first $i - 1$ sensors. If we use μ_i only, then *Cost* will be $\max(x_i, L(k) - x_i)$. If we use μ_i and some sensors in the first $i - 1$ sensors, we need to use μ_i to cover $L(k)$ because μ_i is the rightmost sensor. Then the range covered by μ_i is $[x_i - (L(k) - x_i), x_i + (L(k) - x_i)]$. And the remaining range $[0, x_i - (L(k) - x_i)]$ must be covered by the first $i - 1$ sensors. The *Cost* in this case can be divided into two parts, which is the minimum cost assignment that at least covers the range $[0, 2x_i - L(k)]$ and the cost that μ_i needs to cover $L(k)$. Each entry in $Cost(i, L(k))$ table records the minimum cost that covers the range $[0, L(k)]$. In order to get minimum cost that covers at least range $[0, L(k)]$, we can select $\min_{k \leq j \leq 4n/\epsilon} Cost(i-1, L(j))$ because the possible rightmost point cannot be greater than $2m$ and must be $L(k)$ at least. Therefore, the total cost is $\min_{\substack{2n\|2x_i-L(k)\| \\ \leq j \leq 4n/\epsilon}} Cost(i-1, L(j)) + (L(k) - x_i) + (2x_i - L(k)) - \|2x_i - L(k)\|$. We add $(2x_i - L(k)) - \|2x_i - L(k)\|$ to guarantee the interval $[\|2x_i - L(k)\|, (2x_i - L(k))]$ can be covered. In the second case where we do not select μ_i , the cost is just $\min_{k \leq j \leq 4n/\epsilon} Cost(i-1, L(j))$.

```

for  $k = 1$  to  $\frac{4n}{\epsilon}$  do
  if  $L(k) = 0$  then
     $Cost(1, L(k)) = 0$ 
  else if  $0 < L(k) \leq 2x_1$  then
     $Cost(1, L(k)) = x_1$ 
  else
     $Cost(1, L(k)) = L(k) - x_1$ 
  end if
end for
for  $i = 2$  to  $n$  do
  for  $k = 1$  to  $\frac{4n}{\epsilon}$  do
    if  $L(k) < x_i$  then
       $Cost(i, L(k)) = \min_{k \leq j \leq 4n/\epsilon} Cost(i-1, L(j))$ 
    else
       $Cost(i, L(k)) = \min\{\min_{k \leq j \leq 4n/\epsilon} Cost(i-1, L(j)), \max\{x_i, L(k) - x_i\}, \min_{\frac{2n\|2x_i - L(k)\|}{\epsilon m} \leq j \leq 4n/\epsilon} Cost(i-1, L(j)) + (L(k) - x_i) + (2x_i - L(k)) - \|2x_i - L(k)\|\}$ 
    end if
  end for
end for
return  $\min_{2n/\epsilon \leq j \leq 4n/\epsilon} Cost(n, L(j))$ 

```

Algorithm 2. Dynamic programming algorithm DP_{on_line} for MCLC

Therefore we have the dynamic programming algorithm DP_{on_line} as shown in Algorithm 2.

The initial value for $Cost(1, L(k))$ is defined as follows.

$$Cost(1, L(k)) = \begin{cases} 0, & \text{if } L(k) \leq 0 \\ x_1, & \text{if } 0 < L(k) \leq 2x_1 \\ L(k) - x_i, & \text{if } L(k) > 2x_1 \end{cases} \quad (1)$$

The cost of the optimal solution is $Cost(n, m)$. The running time of Algorithm DP_{on_line} is $O(n \cdot (\frac{4n}{\epsilon})^2) = O(\frac{n^3}{\epsilon^2})$.

In each iteration, the solution will be increased by at most $(2x_i - L(k)) - \|2x_i - L(k)\|$, which is less than $\frac{\epsilon m}{2n}$ as illustrated in Figure 2.

Theorem 3. Let $R^* = \sum_i r_i^*$ be the sum of radii in an optimal solution. Then, for any constant number $\epsilon > 0$, Algorithm DP_{on_line} is an FPTAS for the MCLC problem with running time $O(\frac{n^3}{\epsilon^2})$ such that $R = \sum_i r_i \leq (1 + \epsilon)R^*$.

Proof. Suppose that $\mathbf{R} = (r_1, r_2, \dots, r_n)$ and $\mathbf{R}^* = (r_1^*, r_2^*, \dots, r_n^*)$ are the solutions produced by Algorithm DP_{on_line} and the optimal solution of the original instance, respectively. Let $R = \sum_i r_i$ and $R^* = \sum_i r_i^*$. The difference between these two values are at most $n \cdot \frac{\epsilon m}{2n} = \frac{\epsilon m}{2} \leq \epsilon R^*$.

Hence, we have $R \leq R^* + n \cdot \frac{\epsilon m}{2n} = R^* + \frac{\epsilon m}{2} \leq (1 + \epsilon)R^*$.

We can extend Algorithm DP_{on_line} to Algorithm DP_{off_line} for the GMCLC problem easily with minor changes. The modified version of the recurrence structure is shown below.

If $L(k) > x_i$,

$$\begin{aligned} Cost(i, L(k)) = & \min\{\min_{2n/\epsilon \leq j \leq 4n/\epsilon} Cost(i-1, L(j)), \sqrt{\max\{x_i, L(k)-x_i\}^2 + h_i^2}, \\ & \min_{\frac{2n\|2x_i-L(k)\|}{\epsilon m} \leq j \leq 4n/\epsilon} Cost(i-1, L(j)) + \sqrt{(L(k)-x_i)^2 + h_i^2 + (2x_i - L(k)) -} \\ & \|2x_i - L(k)\|\}. \end{aligned}$$

Otherwise,

$$Cost(i, L(k)) = \min_{k \leq j \leq 4n/\epsilon} Cost(i-1, L(j))$$

The initial value for $Cost(1, L(k))$ is defined as follows.

$$Cost(1, L(k)) = \begin{cases} 0, & \text{if } L(k) \leq 0 \\ \sqrt{h_1^2 + x_1^2}, & \text{if } 0 < L(k) \leq 2x_1 \\ \sqrt{h_1^2 + (L(k) - x_1)^2}, & \text{if } L(k) > 2x_1 \end{cases} \quad (2)$$

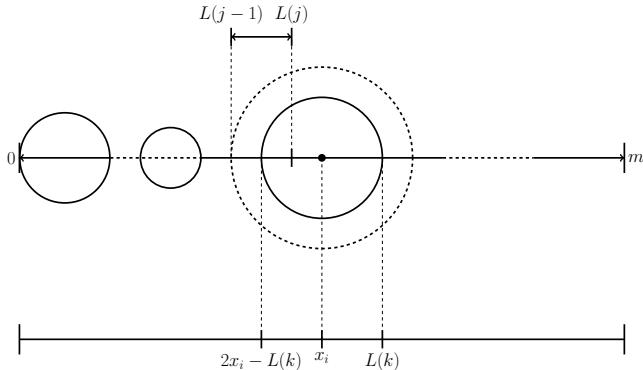


Fig. 2. For each iteration, the sensor μ_i locates in the interval $[L(j-1), L(j))$, the radius of sensor μ_i will be enlarged by at most $\frac{\epsilon m}{2n}$ to meet the rightmost point $L(j-1)$. This will cause at most $\frac{\epsilon m}{2n}$ loss for each sensor.

Theorem 4. Let $R^* = \sum_i r_i^*$ be the sum of radii in an optimal solution. Then, for any small constant $\epsilon > 0$, Algorithm DP_{off_line} is an FPTAS for the GMCLC with running time $O(\frac{n^3}{\epsilon^2})$ such that $R = \sum_i r_i \leq (1 + \epsilon)R^*$.

6 Experiments

In this section, we evaluate the performance of our constant-approximation algorithm with randomly generated sensor positions. Because there is no efficient way to get exact

optimal solutions since the special case when all the sensors are on the line is proved to be NP-hard in [23], we compare our constant-approximation algorithm with the results given by DP_{off_line} . We use R_ϵ to denote the cost of DP_{off_line} with approximation ratio $1 + \epsilon$ and use R to denote the cost of range assignment obtained by our $\frac{4}{3}$ -approximation algorithm. Given each set of sensors with randomly generated positions, we calculate R , R^ϵ and $\frac{R}{R^\epsilon}$. We run several experiments for different ϵ values and maximum sensor height. Let m be the length of the line interval to be covered. Notice that if the average height of sensors is large, the optimal assignment will tend to select a small number of sensors since choosing any sensor will waste quite some cost to cover the vertical distance first. This will make the optimal solution close to our approximation solution. In order to evaluate the performance of our algorithm, we force the maximum height to be small. The computer used to run the experiments has a 2.20 GHz Core i7 processor and 8 GB of memory. The operating system used is Windows 8.

6.1 $\epsilon = 0.1$

In this experiment, we set ϵ to be 0.1, which means we compare our algorithm with a 1.1-approximation algorithm. The number of sensors varies from 1 to 20. We do not select a larger sensor number due to the large time complexity of DP_{off_line} . For every fixed number of sensors, we generate 1000 cases and the positions of sensors are picked randomly in each case. The average ratio is recorded in Figure 3 and Figure 4, where the x-axis represents the number of sensors and the y-axis represents the mean value of $\frac{R}{R_{0.1}}$. Figure 3 shows the result when we force the maximum sensor height to be at most $\frac{1}{2}m$. Figure 4 shows the result when we force the maximum sensor height to be at most $\frac{1}{10}m$. We can find that our $\frac{4}{3}$ -approximation algorithm can achieve very similar performance as DP_{off_line} even though we set the maximum sensor height to be small. However, if we take the time complexity into consideration, our approximation algorithm is much better.

6.2 $\epsilon = 0.05$

In this experiment, we set ϵ to be 0.05, which means we compare our algorithm with a 1.05-approximation algorithm. The number of sensors varies from 1 to 10. We do not select a larger sensor number due to the large time complexity of DP_{off_line} . We choose less number of sensors in this case compared to $\epsilon = 0.1$ case because DP_{off_line} needs more time in the case of $\epsilon = 0.05$. For every fixed number of sensors, we generate 1000 cases and the positions of sensors are picked randomly in each case. The average ratio is recorded in Figure 5 and Figure 6, where the x-axis represents the number of sensors and the y-axis represents the mean value of $\frac{R}{R_{0.05}}$. Figure 5 shows the result when we force the maximum sensor height to be at most $\frac{1}{2}m$. Figure 6 shows the result when we force the maximum sensor height to be at most $\frac{1}{10}m$. Even though we set ϵ to be 0.05, our approximation algorithm can still achieve good performance.

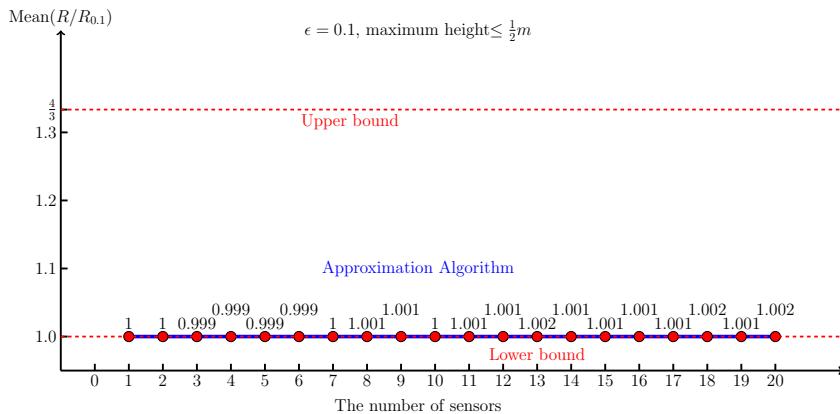


Fig. 3. Comparing our $\frac{4}{3}$ -approximation algorithm with DP_{off_line} when $\epsilon = 0.1$

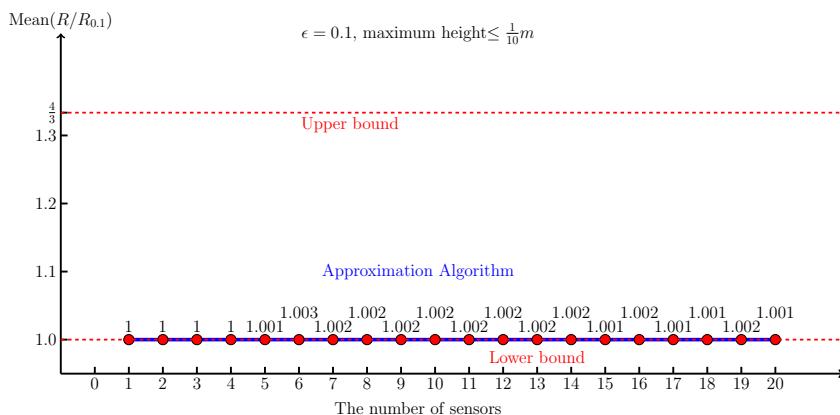


Fig. 4. Comparing our $\frac{4}{3}$ -approximation algorithm with DP_{off_line} when $\epsilon = 0.1$

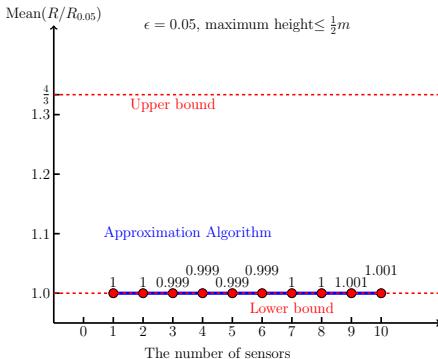


Fig. 5. Comparing our $\frac{4}{3}$ -approximation algorithm with DP_{off_line} when $\epsilon = 0.05$

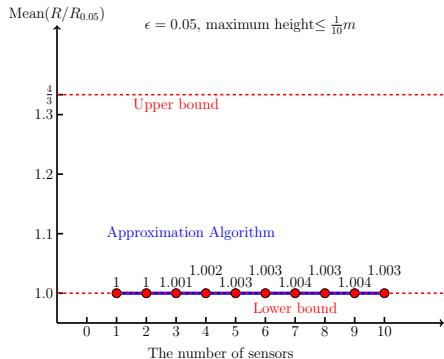


Fig. 6. Comparing our $\frac{4}{3}$ -approximation algorithm with DP_{off_line} when $\epsilon = 0.05$

7 Conclusion

In this paper, we study the barrier coverage problem with line-based offsets deployments by a set of wireless sensors with adjustable coverage ranges. The objective is to find a range assignment with the minimum cost. An approximation algorithm with approximation ratio $\frac{4}{3}$ is presented for GMCLC under a linear cost function on the sensor range. Furthermore, we also designed two FPTASes to solve the optimization problem. Possible future directions are designing and improving the approximation algorithms for the problem with an arbitrary cost function on the sensor radius.

References

1. Kumar, S., Lai, T.H., Arora, A.: Barrier coverage with wireless sensors. In: Proceedings of International Conference on Mobile Computing and Networking, pp. 284–298. ACM (2005)
2. Alt, H., Arkin, E.M., Brönnimann, H., Erickson, J., Fekete, S.P., Knauer, C., Lenchner, J., Mitchell, J.S., Whittlesey, K.: Minimum-cost coverage of point sets by disks. In: Proceedings of Symposium on Computational Geometry, pp. 449–458. ACM (2006)
3. Wan, P.J., Xu, X., Wang, Z.: Wireless coverage with disparate ranges. In: Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 1–8. ACM (2011)
4. Yu, Z., Teng, J., Li, X., Xuan, D.: On wireless network coverage in bounded areas. In: Proceedings of the IEEE Infocom Conference on Computer Communications, pp. 1195–1203. IEEE (2013)
5. Saipulla, A., Westphal, C., Liu, B., Wang, J.: Barrier coverage of line-based deployed wireless sensor networks. In: Proceedings of the IEEE Infocom Conference on Computer Communications, pp. 127–135. IEEE (2009)
6. Călinescu, G., Măndoiu, I.I., Wan, P.J., Zelikovsky, A.Z.: Selecting forwarding neighbors in wireless ad hoc networks. Mobile Networks and Applications 9(2), 101–111 (2004)

7. Narayanappa, S., Vojtechovský, P.: An improved approximation factor for the unit disk covering problem. In: CCCG (2006)
8. Carmi, P., Katz, M.J., Lev-Tov, N.: Covering points by unit disks of fixed location. In: Tokuyama, T. (ed.) ISAAC 2007. LNCS, vol. 4835, pp. 644–655. Springer, Heidelberg (2007)
9. Ambühl, C., Erlebach, T., Mihalák, M., Nunkesser, M.: Constant-factor approximation for minimum-weight (connected) dominating sets in unit disk graphs. In: Díaz, J., Jansen, K., Rolim, J.D.P., Zwick, U. (eds.) APPROX 2006 and RANDOM 2006. LNCS, vol. 4110, pp. 3–14. Springer, Heidelberg (2006)
10. Huang, Y., Gao, X., Zhang, Z., Wu, W.: A better constant-factor approximation for weighted dominating set in unit disk graph. *Journal of Combinatorial Optimization* 18(2), 179–194 (2009)
11. Zou, F., Wang, Y., Xu, X.H., Li, X., Du, H., Wan, P., Wu, W.: New approximations for minimum-weighted dominating sets and minimum-weighted connected dominating sets on unit disk graphs. *Theoretical Computer Science* 412(3), 198–208 (2011)
12. Erlebach, T., Mihalák, M.: A $(4 + \varepsilon)$ -approximation for the minimum-weight dominating set problem in unit disk graphs. In: Bampis, E., Jansen, K. (eds.) WAOA 2009. LNCS, vol. 5893, pp. 135–146. Springer, Heidelberg (2010)
13. Abrams, Z., Goel, A., Plotkin, S.: Set k-cover algorithms for energy efficient monitoring in wireless sensor networks. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 424–432. ACM (2004)
14. Wan, P.J., Yi, C.W.: Coverage by randomly deployed wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)* 14(SI), 2658–2669 (2006)
15. Wang, J., Zhong, N.: Efficient point coverage in wireless sensor networks. *Journal of Combinatorial Optimization* 11(3), 291–304 (2006)
16. Li, M., Sun, X., Zhao, Y.: Minimum-cost linear coverage by sensors with adjustable ranges. In: Cheng, Y., Eun, D.Y., Qin, Z., Song, M., Xing, K. (eds.) WASA 2011. LNCS, vol. 6843, pp. 25–35. Springer, Heidelberg (2011)
17. de Rezende, P.J., Miyazawa, F.K., Sasaki, A.T.: A ptas for the disk cover problem of geometric objects. *Operations Research Letters* 41(5), 552–555 (2013)
18. Czyzowicz, J., et al.: On minimizing the maximum sensor movement for barrier coverage of a line segment. In: Ruiz, P.M., Garcia-Luna-Aceves, J.J. (eds.) ADHOC-NOW 2009. LNCS, vol. 5793, pp. 194–212. Springer, Heidelberg (2009)
19. Chen, D.Z., Gu, Y., Li, J., Wang, H.: Algorithms on minimizing the maximum sensor movement for barrier coverage of a linear domain. In: Fomin, F.V., Kaski, P. (eds.) SWAT 2012. LNCS, vol. 7357, pp. 177–188. Springer, Heidelberg (2012)
20. Czyzowicz, J., et al.: On minimizing the sum of sensor movements for barrier coverage of a line segment. In: Nikolaidis, I., Wu, K. (eds.) ADHOC-NOW 2010. LNCS, vol. 6288, pp. 29–42. Springer, Heidelberg (2010)
21. Bar-Noy, A., Baumer, B.: Maximizing network lifetime on the line with adjustable sensing ranges. In: Erlebach, T., Nikoletseas, S., Orponen, P. (eds.) ALGOSENSORS 2011. LNCS, vol. 7111, pp. 28–41. Springer, Heidelberg (2012)
22. Bar-Noy, A., Rawitz, D., Terlecky, P.: Maximizing barrier coverage lifetime with mobile sensors. In: Bodlaender, H.L., Italiano, G.F. (eds.) ESA 2013. LNCS, vol. 8125, pp. 97–108. Springer, Heidelberg (2013)
23. Fan, H., Li, M., Sun, X., Wan, P.J., Zhao, Y.: Barrier coverage by sensors with adjustable ranges. to appear in ACM Transactions on Sensor Networks

A Distance Ratio-Based Algorithm for Indoor Localization in Wireless Sensor Networks

Xi-ruo Lu, Jian-xin Chen, Xuan-cheng Zhou, Yi Dong, and Liang Zhou

Key Lab of Broadband Wireless Communication and Sensor Network Technology
(Nanjing University of Posts and Telecommunications), Ministry of Education
Nanjing, China, 21003

{xiruolu,cliffezhou,ydong}@outlook.com, chenjx@njupt.edu.cn,
liang.zhou@ieee.org

Abstract. In recent years, compared to GPS which is commonly used in outdoor positioning, an increasing number of RSSI-based algorithms are adopted in indoor positioning. Substantial studies have been conducted for multi-node RSSI localization in wireless sensor networks. Although they are able to reach reasonable accuracy, it still faces some technical challenges. The bandwidth resource, energy consumption, as well as interference, will impact the practical implementation and accuracy of localization. To improve the performance of indoor positioning system, we design a novel ratio algorithm with high accuracy by introducing a relative distance ratio, instead of measuring the practical distance, to decrease the number of variables. Importantly, this method is of low complexity as it just needs three anchor nodes. Experiments on IRIS platform have demonstrated that the proposed algorithm is effective with high accuracy, low power consumption, and low cost.

Keywords: RSSI-based, indoor positioning, ratio algorithm, wireless sensor network.

1 Introduction

With the rapid development of computer and communication systems, the computer network is finding growing applications in modern society. Especially the development of wireless sensor networks (WSNs) has changed our social life considerably. In particular, indoor localization in WSNs will bring immeasurable reform and benefit in the fields of industry, medical treatment and commerce. For instance, intelligent industrial operations can protect employees from contacting the harmful substances or dangerous conditions. Patients can be located to prevent the condition at risk and avoid unnecessary death. In order to reduce the backlog of goods or to prevent goods out of stock, managers can estimate the popularity of the goods by analyzing the amount of customers and their stay time [6] to adjust purchase volume.

Some existing algorithms may yield satisfactory positioning performance, but it is difficult to be applied directly in our daily life. For example, the k -nearest

algorithm needs a considerable number of anchor nodes [7], and the fingerprint algorithm achieves high accuracy at the cost of high-capacity data storage [3]. In addition, it works in a specific environment, and it is necessary to re-update the data module as the environment changes. No matter from any perspective, the cost or the allocation of wireless resource, the demerits of some algorithms make them difficult be applied in practical applications.

Now a natural question arises, is it possible and how can we achieve a general indoor positioning system? Inspired by the idea that one can achieve in some sense tradeoff between accuracy and generality within a certain range of accuracy [10], we propose a ratio algorithm which utilizes relative distance ratio, instead of measuring the practical distance, with decreased number of variables fast and accurate positioning is achieved. As a result, the proposed algorithm, due to its simplicity, can be applied in most of real-world environment with reasonable accuracy without adding extra hardware or bandwidth resource consumption.

This paper is organized as follows. In Section 2, we present a series of works related to the indoor localization. Subsequently, we study and describe the traditional positioning algorithm and obtain a mathematical model between RSSI and distance in section 3. Section 4 designs our positioning system and explains the advantages compared to the traditional algorithm. In Section 5, we verify the proposed algorithm and indicate the optimal positioning range. Finally, we conclude the paper and direct the future work in Section 6.

2 Related Work

Wireless positioning technologies can be briefly divided into two main categories: range-based positioning and range-free positioning [9]. The former measures the distance or angle between the unknown nodes and anchor nodes, and the latter just needs to know the connectivity or topology of the network. Among all these technologies, the most popular ones are: Received Signal Strength Indication (RSSI), Time of Arrival (TOA), Time Difference of Arrival (TDOA) and Angle of Arrival (AOA) [2]. Firstly, we compare them from the aspects of complexity and practicality.

- *RSSI* it has the advantages such as low-power, low-cost, no extra hardware is needed. However, the signal strength values vary on a large scale as it is subjectd to fading and shadowing.
- *TOA* high accuracy can be achieved, but precise clock synchronization makes it difficult to be utilized in large scale deployment.
- *TDOA* accurate positioning is feasible in an ideal environment, but auxiliary ultrasonic module or other hardware is essential. And the ultrasonic propagation distance is another limitation, so it is not suitable for complex environments.
- *AOA* it can provide direction information, but it is susceptible to influence, and needs a large amount of hardware.

The key of TDOA is to determine the difference in propagation time of two kinds of signals, rather than the absolute arrival time which is used in TOA to compute the distance between the unknown and anchor nodes directly. Like other methods, TDOA also needs complex hardware, and it is difficult to apply the algorithm to large-scale scenario. Similarly, AOA can provide better positioning result in free space than RSSI. However, in order to obtain the arrival angles, the quantity and cost of hardware are considerable. Moreover, AOA is not suitable in the complex environment with various obstacles.

As most sensors who have capability of wireless communication can provide RSSI values, it is easy to locate without additional sensors such as ultrasonic [1]. Based on RSSI values, researchers have found new ways for indoor localization. If two unknown nodes share the same or similar RSSI values. We can assume that they lie at the same place or they are close to each other. In this case, the k -nearest algorithm estimates the location of unknown nodes with two phases. Firstly, deploying the anchor nodes with given coordinates uniformly in a specified space and make sure that these nodes broadcast information of their own periodically. Secondly, when the unknown node enters into the space, by comparing the RSSI value between the unknown node and anchor nodes, the gateways search and choose several nodes whose RSSI value are close to the unknown node's, then treat the average of these anchor nodes' coordinate as the estimated location. Since the nodes in a distant place may share the similar RSSI values with unknown node, if the number of anchor nodes is not large enough, the estimation will suffer large errors. Nevertheless, if the quantity of the anchor nodes satisfies the requirement, this algorithm still suffers from the cost problem.

Another widely used method is fingerprint algorithm. The traditional fingerprint method usually includes two phases [8]: training and searching. During the train phase, we divide the fixed space into a number of areas and record the RSSI value of each area. After all measured data of these areas have been recorded, terminals will build a fingerprint database where there is a correspondence between the RSSI values and area. Then, when the terminal senses an unknown node steps into one of these areas, it can obtain the node's RSSI value and gain coordinate by searching the fingerprint database for the matched data. As discussed in [8], this method performs well in terms of accuracy. Nonetheless it underperforms in time consumption and environment adaptability.

Generally speaking, more nodes or complicated algorithms are adopted to achieve high accuracy for positioning. How can we gain higher accuracy with lower cost is of great challenge. To this target, in this paper, we propose a distance ratio-based algorithm of low complexity which can achieve high-accuracy with very few anchor nodes.

3 The Traditional Trilateral Positioning Algorithm

As shown in Fig.1, we assume that $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$ are anchor nodes, and $D(x, y)$ is an unknown node to be located.

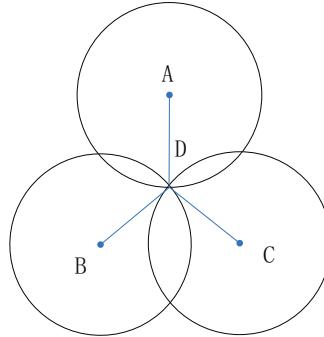


Fig. 1. Theory of trilateral localization

The traditional trilateral positioning algorithm is applied to calculate the position of the unknown node, here we assume the distance between node D and A, B, C are d_1, d_2, d_3 ,

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = d_1^2 \\ (x - x_2)^2 + (y - y_2)^2 = d_2^2 \\ (x - x_3)^2 + (y - y_3)^2 = d_3^2. \end{cases} \quad (1)$$

The coordinate of D can be obtained by (1), which is,

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_1 - x_3) & 2(y_1 - y_3) \\ 2(x_2 - x_3) & 2(y_2 - y_3) \end{bmatrix}^{-1} \begin{bmatrix} x_1^2 - x_3^2 + y_1^2 - y_3^2 + d_3^2 - d_1^2 \\ x_2^2 - x_3^2 + y_2^2 - y_3^2 + d_3^2 - d_2^2 \end{bmatrix}. \quad (2)$$

The traditional trilateral algorithm is based on the measured distance, while the RSSI-based algorithms convert the received signal strength to distance. The theoretical value in free space of RSSI can be expressed as: $RSSI = -(10 \cdot n \cdot logd + A)$ [4], where, radio frequency (RF) parameters A and n are used to denote the operating environment of a sensor network. In an omnidirectional model, the RF parameter A is the received signal strength in dBm at $1m$ away from the transmitting node. If the received signal strength is $-40 dBm$, then parameter A is set to 40 . n denotes the path loss exponent, which indicates the decay rate of signal strength with the increasing of distance between the transmitter and receiver. Experiments show that the decay rate is proportional to $d - n$, where d is the distance between the transmitter and receiver. Fig.2 shows the fitting curve between RSSI and distance in a practical scenario

In the practical scenario, a set of experiments are conducted on IRIS platform. The RSSI value and distance are related by the curve in Fig.2. We found that RSSI is an exponential function of distance with two unknown parameters. But when the distance is larger than $3m$, the signal strength rarely changes. In this paper, $3m \times 3m$ is chosen as the optimal positioning range.

Traditional trilateral algorithm transforms the RSSI value to distance. As the theoretical model $RSSI = -(10 \cdot n \cdot logd + A)$ includes two variables A and

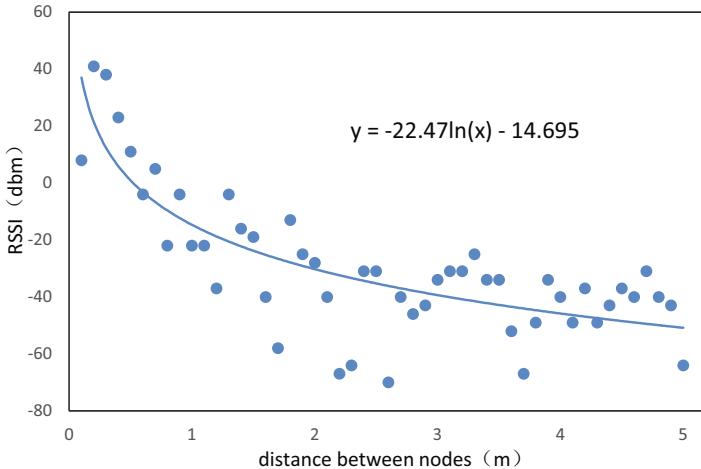


Fig. 2. Fitting curve between RSSI and distance

n , unwanted errors will be introduced if we use their experimental values to calculate the distance directly.

4 Distance Ratio-Based Algorithm

The proposed distance ratio-based algorithm comprises of four parts depicted in Fig.3. Specifically, A , B , C are the anchor nodes with given coordinates, among which $A(1.5, 3)$, $B(0, 0)$, $C(3, 0)$. D is the unknown node, and E is the base station. The terminal receives and processes information. Our system works as follows. Node D broadcasts the message of its own to all the other anchor nodes periodically. The anchor nodes A , B and C receive the signal from D and obtain the signal strength. Then they forward these information to the base station E which forwards the information to terminal for data processing. Finally the terminal who knows the coordinates of anchor nodes in advance calculates the estimated position of the unknown node D using our distance ratio-based algorithm as analyzed below.

The signal strength between A and D , B and D , C and D are assumed to be r_1 , r_2 , r_3 . The length of AD , BD , CD are a , b , c . m represents the parameter $10 \cdot n \cdot \log_e$, and h for parameter $-A$. According to the relationship of distance and signal strength shown in Fig(2),we have,

$$\begin{cases} r_1 = m \cdot \ln a + h \\ r_2 = m \cdot \ln b + h \\ r_3 = m \cdot \ln c + h. \end{cases} \quad (3)$$

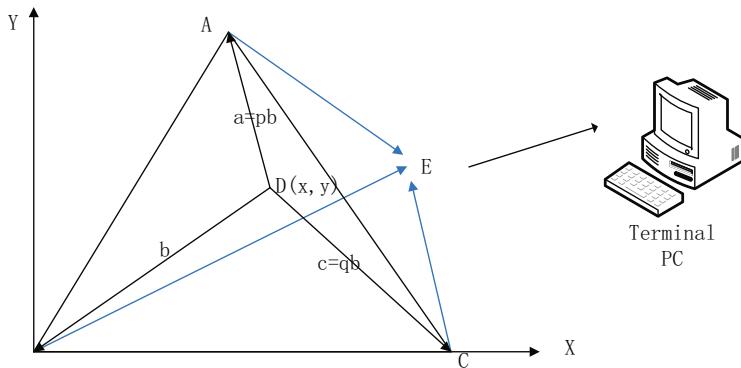


Fig. 3. Coordinate relationship between nodes

As A varies with platform, time and environment, it means that each time we use A to calculate the distance it may be different. But in traditional algorithm, A is a constant. Then we have,

$$\begin{cases} r_1 - r_2 = m \cdot \ln\left(\frac{a}{b}\right) \\ r_3 - r_2 = m \cdot \ln\left(\frac{c}{b}\right). \end{cases} \quad (4)$$

Clearly, Eq.3 contains two variables, but in Eq.4, we just need to calculate m . With the variation of environment and radio signal, the values of signal strength may vary relatively large. But if we use the difference of two signals' strength, part of the interference introduced by the environment and radio signal can be counteracted. Thus, the distance ratio of unknown node to the three anchor nodes can be obtained:

$$\begin{cases} p = \frac{a}{b} = e^{(r_1 - r_2)/m} \\ q = \frac{c}{b} = e^{(r_3 - r_2)/m}. \end{cases} \quad (5)$$

Reasonable layout of anchor nodes can reduce the algorithm complexity. We assume that it is an isosceles triangle and point B as the origin in Fig.3. Then the relationship between the coordinates of node A , B , C , D and variables p , q can be presented as below,

$$\begin{cases} p^2 = \frac{(x-x_1)^2 + (y-y_1)^2}{x^2 + y^2} \\ q^2 = \frac{y^2 + (x_3-x)^2}{x^2 + y^2}. \end{cases} \quad (6)$$

The unknown node's coordinate can be obtained by Eq.6. Proposed algorithm which reduces the amount of variables by calculating the difference of signal strength and obtain the ratio of each distance. Thus, we realize the improvement of traditional trilateral positioning algorithm.

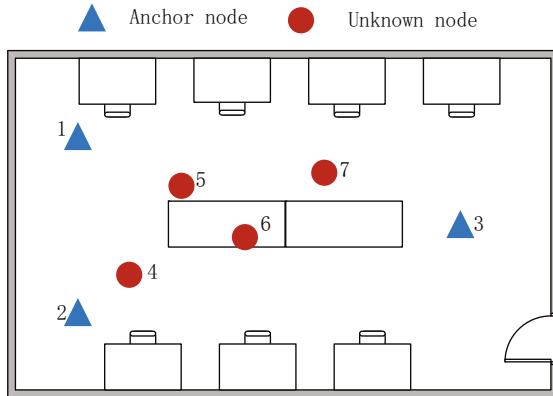


Fig. 4. Layout of positioning environment

5 Experiment Results

5.1 Experiment Environment

We have conducted a set of experiments in a practical scenario as shown in Fig.4. The nodes 1, 2, 3 are anchor nodes with given coordinates. 4, 5, 6, 7 are unknown nodes. In addition to desks shown in fig.4, there are computers, printers, TVs and other furniture in the lab. The nodes 1, 2, 3 in Fig.4 correspond to the vertices of the isosceles triangle in figure.3. So, we can use physical layout of the nodes to reduce the complexity of localization algorithm.

The sensor we use is IRIS [5]. It is a 2.4GHz Mote module used for enabling low-power, wireless sensor networks. Any IRIS node can be connected to the gateway as a base station. The base station collects all the dates from other sensors and forwards them to PC. The sensor node and gateway are shown in fig.5.

5.2 Comparisons

A large number of tests have shown that when the unknown node is very far away or very close to any anchor node [1], the relationship between the signal



Fig. 5. IRIS sensor node and gateway

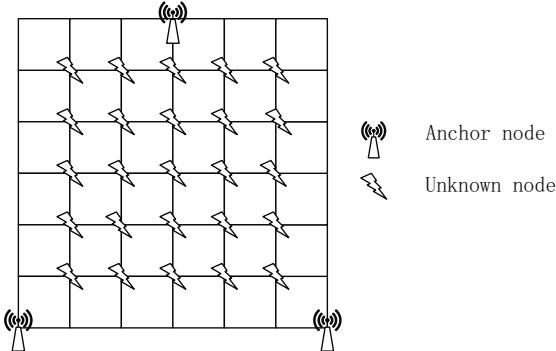


Fig. 6. Layout of nodes

strength and distance will no longer follow the logarithmic relationship shown in Fig.2. In order to further improve the accuracy of three-point positioning, we uniformly distribute the unknown nodes among anchor nodes. Fig.6 investigates the layout of nodes, among which, the locations of the anchor nodes are fixed, and unknown nodes move forward step by step per $0.5m$. As mentioned above, the isosceles triangle layout of anchor nodes can reduce the complexity of the algorithm.

In the same scenario, we use the traditional trilateral algorithm to locate the unknown node. The result is shown in Fig.7. We take $e = \sqrt{(X - X_n)^2 + (Y - Y_n)^2}$ as the error standard, where (X, Y) is the actual coordinate of the unknown node and (X_n, Y_n) is the estimated coordinate. We see that there are many significant errors in traditional trilateral algorithm. Except for these points with significant error shown in Fig.7, there still exists a point whose error is beyond 20 meters but not displayed in the figure.

Although there are still some errors in the proposed algorithm, the number of points with significant error reduces greatly as we reduce the number of unknown parameters. Thus we improve the indoor position system successfully within a certain range of error.

The curve in Fig.7 denotes the difference of the actual coordinates and estimated coordinates. The further the distance from the x-axis the larger the error node produces appears. Fig.7 demonstrates that the improved positioning algorithm is superior to the original trilateral position algorithm, at the same time, we reduce the maximal error from $25m$ to $1.4m$ and 90% of the test results are better than the traditional location algorithm in the same coordinate system.

5.3 The Optimal Positioning Range

To verify the optimal positioning range proposed in Section 3, another experiments were conducted in the same experimental scenario except the coordinate system. Coordinates of the anchor node are node1 $(0, 4)$, node2 $(0, 0)$, node3

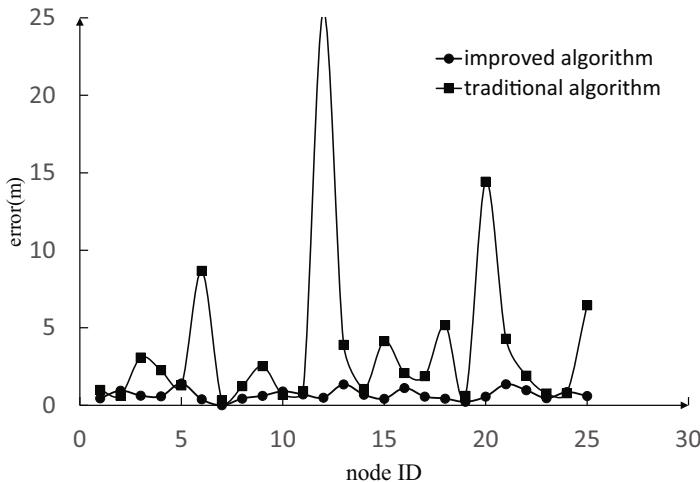


Fig. 7. Comparison of two positioning error

(3.5, 2). The distance from the curve to x-axis represents the difference of the actual coordinates and estimated coordinates.

Fig.2 shows that, with the distance increasing, the relationship curve between the signal strength and distance tends to be horizontal, it means that the signal strength does not change or change little that we can not rely on it to judge the distance between nodes. In Fig.8, by comparing the positioning error of the same place in different coordinate systems, it can come to conclusion that when the positioning range is more than three meters, the error increases significantly.

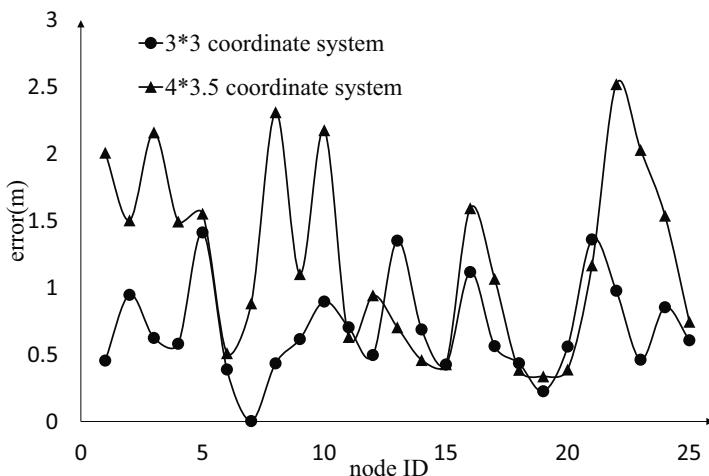


Fig. 8. Positioning error of same coordinate in different coordinate systems

We compare the error in different coordinate systems. The results state the maximal error is more than sixty percent in the $4m \times 3.5m$ coordinate system. In practice, we choose the $3m \times 3m$ coordinate system to achieve the trade-offs between hardware requirements and positioning precision. Of course, there may exist some values between $3m$ and $4m$ which can reach minimum positioning error. In this paper, we choose $3m \times 3m$ as the optimal range.

6 Conclusion

In this paper, we propose a novel positioning algorithm and analyze the positioning error in a practical scenario. The experimental results demonstrated that within a certain range of accuracy reasonable positioning result can be achieved using only three anchor nodes. By introducing the ratio of distance, the proposed algorithm can decrease the positioning error as it reduces the number of variables in distance-RSSI equation. Most of all, the proposed Ratio-based algorithm turns out to be of high accuracy and low complexity. For future work, we can combine this work with the extended kalman filter to further improve the positioning accuracy, availability and portability.

Acknowledgment. This work is supported by the State Key Development Program of Basic Research of China (2013CB329005), National Natural Science Foundation of China (Grant No. 61201165,GZ211018), the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), and Ministry of Education (No. NYKL201306), and Nanjing University of Posts and Telecommunications Foundation (Grant No. NY211032).

References

1. Awad, A., Frunzke, T., Dressler, F.: Adaptive distance estimation and localization in wsn using rssI measures. In: 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools, DSD 2007, pp. 471–478. IEEE (2007)
2. Brchan, J.L., Zhao, L., Wu, J., Williams, R.E., Pérez, L.C.: A real-time rfid localization experiment using propagation models. In: 2012 IEEE International Conference on RFID, pp. 141–148. IEEE (2012)
3. Gogolak, L., Pletl, S., Kukolj, D.: Indoor fingerprint localization in wsn environment based on neural network. In: 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics (SISY), pp. 293–296. IEEE (2011)
4. Instruments, T.: CC2431 data sheet,
<http://www.ti.com/lit/ds/symlink/cc2431.pdf>
5. Instruments, T.: IRIS-XM2110 data sheet,
http://www.dinesgroup.org/projects/images/pdf_files/iris_datasheet.pdf
6. Liu, H., Gan, Y., Yang, J., Sidhom, S., Wang, Y., Chen, Y., Ye, F.: Push the limit of wifi based localization for smartphones. In: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, pp. 305–316. ACM (2012)

7. Saxena, M., Gupta, P., Jain, B.N.: Experimental analysis of rssi-based location estimation in wireless sensor networks. In: 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE 2008, pp. 503–510. IEEE (2008)
8. Yang, Z., Wu, C., Liu, Y.: Locating in fingerprint space: wireless indoor localization with little human intervention. In: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, pp. 269–280. ACM (2012)
9. Zhan, J., Liu, H., Huang, B.: A new algorithm of mobile node localization based on rssi. Wireless Engineering and Technology 2(2), 112–117 (2011)
10. Zhou, L., Hu, R.Q., Qian, Y., Chen, H.H.: Energy-spectrum efficiency tradeoff for video streaming over mobile ad hoc networks. IEEE Journal on Selected Areas in Communications 31(5), 981–991 (2013)

On Effectiveness of Clustering Principles in Maximizing Wireless Sensor Network Lifespan

Xiaohui Kuang¹, Bowen Li^{1,2,*}, and Li Liu¹

¹ National Key Lab of Science & Technology on Information System Security, China

² School of Software and TNLIST, Tsinghua University, China

lbw1225@gmail.com

Abstract. Network lifespan maximization is widely recognized as the most critical issue in wireless sensor networks (WSNs), especially in the reconfiguration-constrained applications such as disaster management, combat field reconnaissance and security surveillance. Clustering is a promising way for saving energy consumption in WSNs, which partitions the large networks into multiple small cells for achieving easier node management and less transmit power waste. Quite a lot of clustering algorithms are proposed in the literature, trying to prolong network lifetime. Diverse clustering principles such as periodical head replacement, cluster size optimization, link quality matching, etc., are proposed, however, without comparative evaluation on their effectiveness. In this paper, we systematically analyze and comparatively evaluate the influencing factors that impact system lifetime of clustered WSNs. Based on the results, we derive several observations, which could be used for guiding energy-efficient clustering algorithms design.

1 Introduction

The rapid technological advances in low-power hardware design have enabled the rapid development of tiny battery-powered sensor nodes which are able to compute, sense and communicate with each other[1]. One of the advantages of wireless sensors networks (WSNs) is their ability to operate unattended in harsh environments in which contemporary human-in-the-loop monitoring schemes are risky, inefficient and sometimes infeasible. Therefore, sensors are expected to be deployed randomly in the area of interest by a relatively uncontrolled means, e.g. dropped by a helicopter, and to collectively form a network in an ad-hoc manner [2]. Given the vast area to be covered, the short lifespan of the large population of battery-operated sensors are expected in most WSNs applications. Designing energy-aware algorithms becomes an critical factor for extending the lifetime of sensors as well as making the WSNs pervasive.

Grouping sensor nodes into clusters, i.e., clustering, has been widely pursued by the research community for achieving efficient network management as well as providing network scalability[3, 4]. Every cluster would have a leader, often referred to as the cluster head (CH). The base station, cluster head and cluster

* Partially supported by CPSF (Grant No: 2013M540951).

members constitute a hierarchical network architecture, which benefits network operation in many ways. On one hand, the hierarchical architecture facilitates the information transmission in the network. e.g., it could localize the route set up within the cluster and thus reduce the size of the routing table stored at the individual node[5]. Also, it conserves communication bandwidth since it limits the scope of inter-cluster interactions to CHs and avoids redundant exchange of messages among sensor nodes [6, 7]. On the other hand, the existence of CHs could further help optimizing the network. For example, the CH could schedule activities in the cluster so that nodes can switch to the low-power sleep mode most of the time and reduce the rate of energy consumption[8]. Moreover, a CH can aggregate the data collected by the sensors in its cluster and thus decrease the number of relayed packets[9].

Plenty of clustering algorithms have been proposed in the literature. The early work consider ad hoc networks[10–12], aiming to generate stable clusters in mobile adhoc networks (MANET). Many of such techniques care mostly about node reachability and route stability, without much concern about critical design goals of WSNs such as network longevity. Recently, a number of clustering algorithms have been specifically designed for WSNs[13–15], with the goal of maximizing networks lifespan. Perhaps the most popular principal is to periodically replace the CHs, thus to keep uniform energy consumption across nodes[13]. Residual energy[14] as well as intra-cluster communication cost[15] are the main concern for head rotation. Meanwhile, other energy consumption related factors such as inter-cluster communication cost, cluster size, re-clustering (or rotation) overhead, etc., are also considered independently in the literatures[16–18]. However, the commonality and differences among these clustering principles in prolonging network lifetime are rarely explored, neither did their effectiveness.

In this paper, we systematically analyze the influencing factors on lifespan of clustered wireless sensor networks, aiming to explore the main attributes on network lifespan extension and the root reason hiding behind. Specifically, we comparatively evaluate the effectiveness of cluster size optimization, link-aware cluster formation and energy-aware rotation on network lifespan extension. The three clustering principles are highly concerned in constructing energy-efficient clustering WSNs recently; however, few attention have been paid on their achievable performance and mutual effect. Our work on one hand could help understanding the components of energy consumption in wireless sensor networks and the principles of existing various clustering algorithms. On the other hand, it answers several critical questions, e.g., what factor should be most concerned, what factor could be compromised when conflict happen, etc., providing guidelines for designing energy-efficient clustering algorithms.

The remainder of this paper is organized as follows. Section 2 analyze the influencing clustering factors on network lifespan, accompanied with a brief summary of related work. The system model and experiment setting are given in Section 3. In Section 4, we comparatively evaluate and analyze the effectiveness of considered clustering principles by extensive simulations. Finally, Section 5 concludes our work.

2 Influencing Factors and Related Work

In a systematic view, there are three ways in prolonging network lifetime: 1) to improve energy efficiency of data transmission; 2) to reduce the volume of total data transmission (as well as overhead); and 3) to balance energy consumption across nodes.

Focusing on one or multiple of above methods, several clustering principles are widely used in existing literatures. Perhaps the most popular principle is *head rotation*, which is firstly developed by LEACH[13]. In LEACH, sensor nodes elect themselves as cluster heads with some probability and broadcast their decisions. The remaining nodes join a cluster, of which the cluster head is closest in terms of the communication energy cost. Then the role of the cluster head is periodically rotated among the nodes to **balance energy consumption**, since cluster heads have the extra burden of performing a long-range transmission to a distant sink node. HEED[14] introduces a variable known as the cluster radius which defines the transmission power to be used for intra-cluster broadcast. The initial probability for each node to become a tentative cluster head depends on its residual energy, and final cluster heads are selected according to the intra-cluster communication cost (*intra-cluster link quality*). Thus, both **energy consumption balancing** and **energy efficiency improving** are considered during dead rotation. Ding et al. [15] have proposed DWEHC to achieve more aggressive goals than those of HEED. In general, the clusters formed by DWEHC is more well-balanced than HEED. Meanwhile, it also achieves significantly lower energy consumption in intra-cluster and inter-cluster communication than HEED.

Proper *cluster size* is critical for **improving energy efficiency of data transmission**. Exploiting small clusters indicates more data are transmitted over longer and more energy consuming CH-BS link, while big clusters results in higher energy consumption of intra-cluster communication. In [13], the designers of LEACH communication protocol calculate the efficient number of clusters, whereby the network will save a huge amount of energy. However, their results solely specify an interval to which the optimal number of clusters belongs. The following protocols such as HEED[14], DWEHC[15] assume that the number of optimal cluster size is available before network deployment, which is impractical in most WSNs applications. Most recently, authors in [16] propose an analytical model to achieve the optimal number of clusters for wireless sensor networks, however, all the analytical results are established in perfect statistical models such as node distribution, energy consumption model, as well as propagation model. In a word, how to derive a proper cluster size is still an open problem. Thus, it is meaningful to evaluate the impact of estimation error of cluster size.

While for data reduction, the most widely applied approach is data fusion[9], in which the CHs gathered sensing data from its members and proceeds data compression so as to reduce the data amount transmitted to sink. Duty cycle is another effective way for saving energy in WSNs[8], which allows nodes turn off radio when it has no data to send/receive. In this paper, we consider both data gathering and duty cycle are used in our networks, while ignoring the detail algorithm, since they are not the main concern of clustering.

In this paper, we are focus on evaluating the main clustering principles, rather than specific clustering protocols, so as to concentrate on the core idea but not algorithm details. Inspired by the above analysis, we opt to explore the factors of *cluster size*, *link quality* and *head rotation*. Note that for the link quality, both the intra- and inter- cluster links are studied in our experiments for exploring the potential benefit, although most clustering algorithms only consider the intra-clustering link quality for CH election.

3 Network Model

3.1 System Model

Network Model. There exists a base station (BS), also known as sink, collecting sensing data from sensor nodes. BS is powerful in computation, communication, storage and energy supply. The sensors are randomly distributed around BS. In this section, we consider the scenario that nodes are capable of communicating with the BS, thus to make the investigation more focused.

Energy Model. The same energy model as the one introduced in [19, 20] is used throughout the paper. Specifically, the transmit and receive energy for a given message with l bits in the distance of d are respectively given by

$$E_{Tx}(l, d) = lE_{elec}^{Tx} + l\varepsilon_{amp}d^k 10^{\frac{\rho}{10}}$$

$$E_{Rx}(l, d) = lE_{elec}^{Rx}$$

where E_{elec}^{Tx} and E_{elec}^{Rx} denote the energy being dissipated to run the transmitters or receivers circuitry, respectively, to send or receive one bit of the data packet. ε_{amp} represents the energy dissipation of the transmission amplifier to convey one bit of the data packet to the receiver node with a distance of $d = 1$ m away, and n is the path loss exponent which is specified by radio propagation model. The parameter ρ indicates the random lognormal shadowing fading caused by obstacles in the propagation path. As it can be seen, the transmitter expends energy to run the radio electronics and power amplifier, while the receiver only expends energy to run the radio electronics.

Link Model. We consider $k = 2$ to approximate signal attenuation as a function of the distance between transmitters and receivers. Commonly, the free space model is used at small distances propagation. We further formulate the link randomness caused by unpredictable obstacles with lognormal shadowing model. Specifically, the additional shadowing caused path loss ρ (in dB) is normal distributed with mean 0 and variance σ .

Data Aggregation Model. We consider that the cluster heads are capable of aggregating their cluster members data signals to produce a single representative signal. Data fusion consumes lE_{DA} nJ/signal for each l -bit input signal, where E_{DA} indicates the prorated cost of aggregation for a single bit. We quantize the compression performance by the parameter λ , where $0 \leq \lambda \leq 1$. Specifically, the

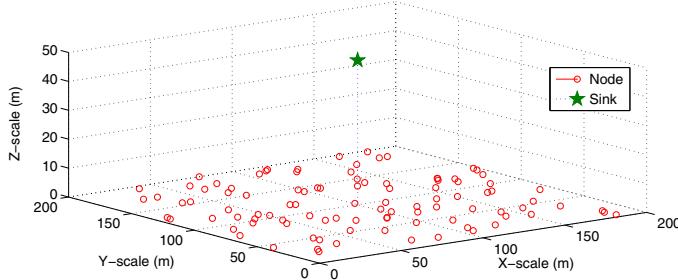


Fig. 1. Experiment scenario

aggregator would output $(1 + \lambda)l$ bits if multiple (≥ 2) l bit packets are input. The nodes are able to turn off radio periodically for energy saving when there was no sending/receiving mission for him.

3.2 Experiment Settings

Simulation Parameters. We consider there are 200 nodes randomly distributed within a $200\text{m} \times 200\text{m}$ square area. The sink (i.e., base station) located in (100, 100, 50)m. The network topology is randomly generated at the beginning of each run. A simple example of experimental scenario is depicted in Fig1. The main parameters used in experiment is presented in Table.1, which are mainly derived from [19, 20].

Clustering Algorithms. As we focus on clustering principles rather than clustering protocol, we use a simple cluster formation approach, i.e., partition the whole $200\text{m} \times 200\text{m}$ square area into multiple small squares with given cluster diameters. Based on the formed clusters, the CHs are determined in following ways:

C0: random CH election- randomly select a node in the cluster as CH and continue work till its battery exhausted, then reselect a CH randomly among the remain nodes.

C1: inter-cluster link based CH election- select the node that would consume minimum energy for transmitting given data to BS, i.e.,

$$\arg \min_{n \in C_i} \left\{ d_{n-bs}^k 10^{(0.1 * \rho_{n-bs})} \right\}$$

where C_i is the i^{th} cluster.

C2: inter-&intra-cluster link based CH election- select the node that would minimize the total energy consumption of nodes in cluster, i.e.,

$$\arg \min_{n \in C_i} \left\{ (1 + \lambda) d_{n-bs}^k 10^{(0.1 * \rho_{n-bs})} + \sum_{m \in C_i, m \neq n} \left\{ d_{m-n}^k 10^{(0.1 * \rho_{m-n})} \right\} \right\}$$

Table 1. Experiment Parameters

Network parameter	Value
Field span	Square: 200m × 200m
Location of BS	(100, 100, 50)m
Number of nodes (N)	200
Packet size (l)	500 bytes
Number of frames per round	1
Energy parameter	Value
Initial energy per node (E_0)	2J
E_{elec}^{Tx}	50 nJ/bit
E_{elec}^{Rx}	50 nJ/bit
ε_{amp}	100 pJ/bit/m ²
Link parameter	Value
Path loss Exponent (k)	2
Lognormal shadowing variance (σ)	4
Aggregation parameter	Value
E_{DA}	5 nJ/bit/signal
λ	0.5

C3: random CH election with rotation- randomly select a node in the cluster as CH periodically rotate the role of CH among the nodes in the cluster.

C4: random CH election with energy-aware rotation- randomly select a node in the cluster as CH periodically reappoint CH as the node with maximum residual energy.

With random CH election **C0**, an example of the clustered network topology in different cluster diameters is shown in Fig.2.

4 Comparative Evaluation on Influencing Factors

We now present the main results of simulations as well as our observations. The results presented in this section are derived with 500 independent runs. While at the beginning of each run, the locations of nodes as well as the lognormal shadowing fading coefficient between nodes are randomly generated.

4.1 Cluster Size

In this subsection, we explore the influence of cluster size on system energy efficiency as well as network lifespan. The cluster diameter is set to be [20 40 50 60 80 100]m. Fig.3 depict the energy consumption of the whole network nodes with respect to cluster size. Note that here the energy consumption value is derived when the all nodes are still alive. It is clear that there exists an optimal

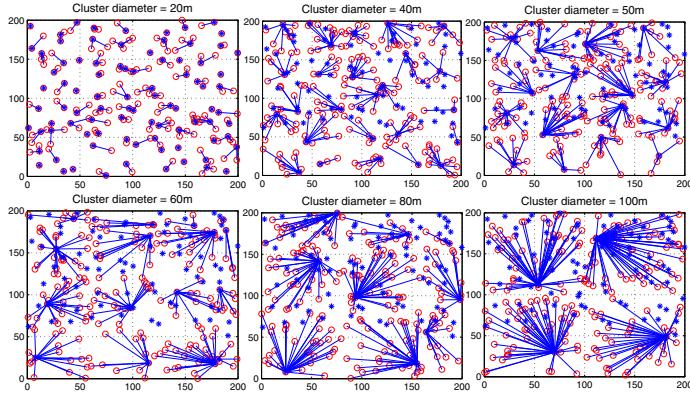


Fig. 2. An example of clustering with different cluster size

size, i.e., 50m in the given scenario. Moreover, we depict the composition of the energy consumption. Firstly, the main part of energy consumption happens in members transmitting packets to heads, as well as heads uploading packets to BS. Secondly, although the energy for data fusion as well as data receiving in heads are increasing with the cluster size, they are much smaller and smoother in changes than that of transmission energy consumption. Finally, as cluster size increases, the uploading energy decreases due to the reduced number of CHs. Meanwhile, the member transmitting energy greatly increased, for the reason of longer intra-communication range.

We further investigate the network lifetime with different cluster size. The definition of network lifetime depends on the specific application. Here we record the whole procedure of network evolution, and depict the following 6 kinds of lifetime with diverse dead rate: 1) the first node dies; 2) 10% of the nodes die; 3) 30% death rate; 4) 50% nodes are dead; 5) 80% death; and 6) all nodes are dead. The results in Fig.4 reveal that the network lifetime with proper cluster size (i.e., 50m in the scenario) would be more than 2 times than with improper cluster size (e.g., 20m in the scenario). The cumulative distribution function of nodes's dead time are presented in Fig.5.

4.2 Link Quality

It is intuitive to improve the energy efficiency by letting more data transmitted over better links. In this subsection, we evaluate the benefit of doing so. In Fig.6, the data fusion, seta receiving in head part are combined into the energy consumption of heads. Compare the curves of **C1** with **C0**. The energy saving mainly comes from the head part. This is reasonable since **C1** selects CH with the consideration on the inter-cluster link quality only. Also, it is observed that when cluster size is up to 100m, the benefit of **C1** over **C0** is negligible. This

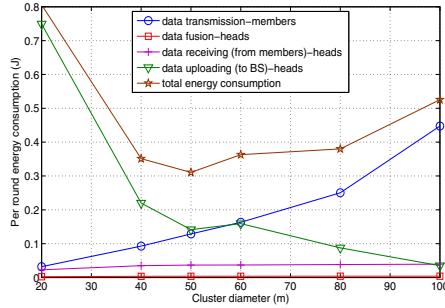


Fig. 3. Components of energy consumption vs. cluster diameter

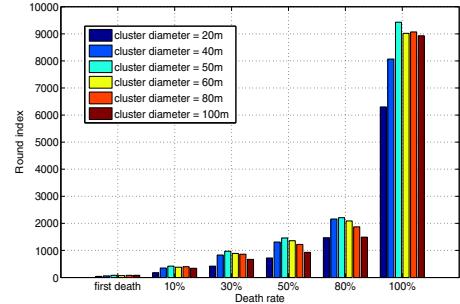


Fig. 4. Lifetime comparison with different cluster size

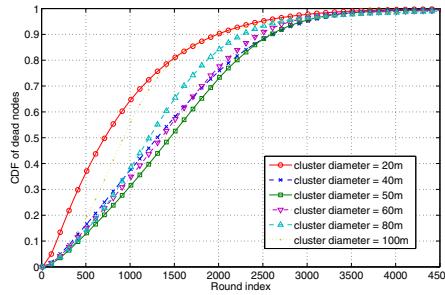


Fig. 5. CDF of dead nodes

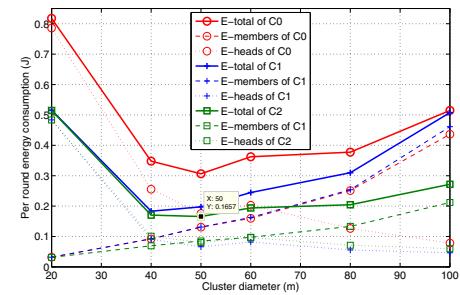


Fig. 6. Energy consumption of C1&C2

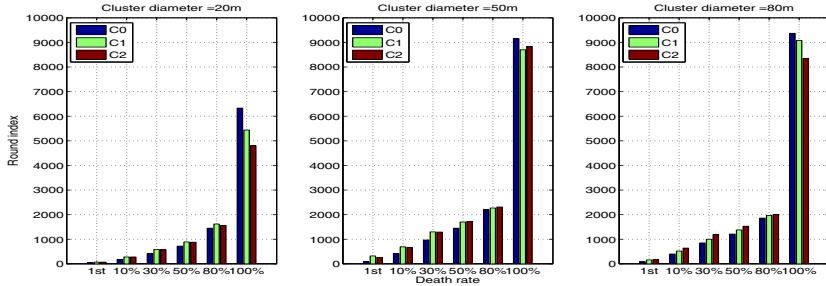
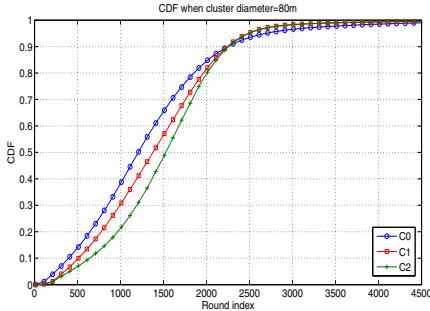
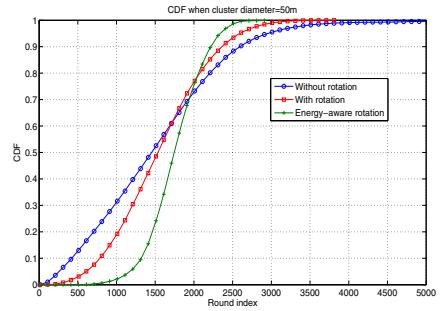
is because the number of heads is too few in this condition. Similar, **C2** further reduce the energy consumption by reducing the members' transmitting power.

Fig.7 depict the lifetime comparison. It is shown that with link consideration, the network lifetime is prolonged in most criteria, except the case of 100% death rate. We guess this is because that, with **C1** or **C2**, the nodes with good link are always die first (due to their duty to be head); while with **C0**, the nodes with good link are capable of being cluster member for a considerable long time, and thus keep alive much longer in the later period. Also, we find that **C2** outperform **C1** very little when cluster size is not so big (e.g., < 80m). This reveals that the inter-communication cost dominates the energy consumption in the scenario. The CDF of dead nodes with cluster size equals to 80m is presented in Fig.8.

4.3 Head Rotation

Here, the head rotation is carried out in two phases: rotation without considering on residual energy and residual energy-aware rotation.

The CDF of death is presented in Fig.9, where both the two kinds of rotation are contained. Compare with the algorithm without rotation, the curves of

**Fig. 7.** Lifetime comparison with link consideration**Fig. 8.** Lifetime CDF of C1&C2**Fig. 9.** Lifetime CDF of C3&C4

rotation-related method are steeper, which indicates that nodes are with more similar deadtime. The lifetime comparison is depicted in Fig.10. It is clearly, that the time of first death is greatly extended. Moreover, the 10%, 30%, even 50% lifetime are prolonged; however, at the cost of shorter lifetime of 80% death and sharply shrank 100% death lifetime.

4.4 Main Results

Finally, we compare the effectiveness of the three clustering principles on lifespan maximization, and derive the designing guidelines.

The CDF curves are presented in Fig.11. The gap between blue and red line indicates the benefit of cluster size optimization; similarly, the red-green gap is the benefit of link-aware clustering, and the red-purple gap is the benefit of energy-aware rotation. This figure tells that: 1) cluster size optimization contributes the main lifetime extension. In other words, engineers should pay more attention on determining the optimal cluster size for WSNs. 2) in the accuracy-sensitive or completeness-sensitive applications, i.e., the system is defined to be alive only when most of nodes are alive, energy-aware rotation is a dominate

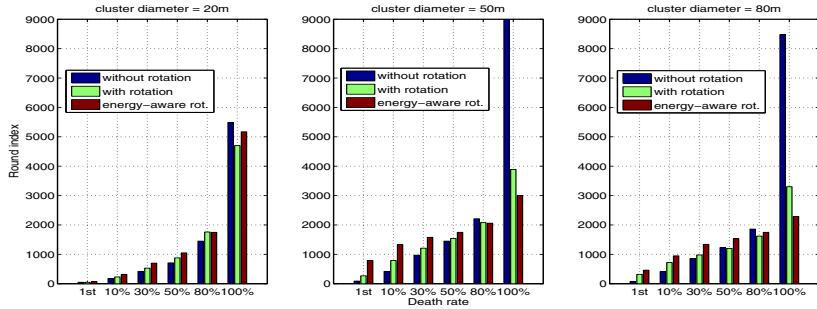


Fig. 10. Lifetime comparison with head rotation

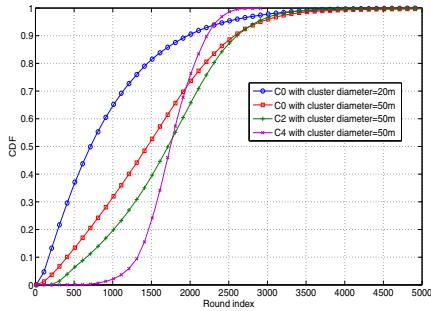


Fig. 11. CDF comparison

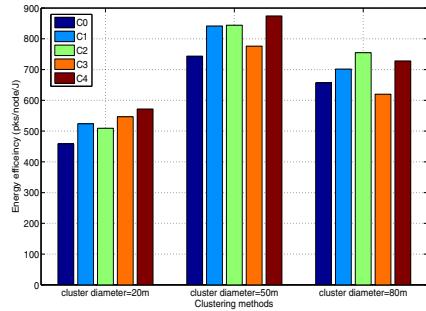


Fig. 12. Energy efficiency

technology for lifetime maximization. Otherwise, for the applications requires coarse long time sensing data, head rotation is worse than useless. 3) link-aware clustering benefits in all kinds of applications.

We further derive the energy efficiency on sensing data transmission of the network whole lifecycle. The energy efficiency is defined as the ratio between “the total transmitted sensor packets” and the total network energy. The results are put in Fig.12. It is worth to note that, although rotation (especially energy-aware rotation) do not choose the good link for data transmission, it achieves high energy efficiency, sometimes even better than link-aware clustering. The magic comes from the node cooperation gain. As energy-aware rotation try to keep alive as many nodes as possible, most nodes are transmitted through CHs. While, for the link-aware method, although it always chooses currently best node to send data, too early node death makes the network more sparse, leading to higher needs on transmit energy.

5 Conclusion

In this paper, we systematically analyze and comparatively evaluate the influencing factors that impact system lifetime of clustered WSNs. We show by

experiments that the cluster size dominate the network lifetime. Moreover, we find that link-aware clustering head selection benefits in all kinds of applications, while the choice of implementing head rotation depends on the application type. Observing that there are little consideration paid on cluster size optimization in existing protocol design, we are now working on developing distributed clustering optimization framework, focusing on adaptively optimizing cluster size without priori knowledge such as node location, density, energy model etc.

References

- [1] Chong, C.-Y., Kumar, S.P.: Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE* 91(8), 1247–1256 (2003)
- [2] Akyildiz, I.F., et al.: Wireless sensor networks: a survey. *Computer Networks* 38, 393–422 (2002)
- [3] Abbasi, I., Younis, M.: A survey on clustering algorithms for wireless sensor networks. *Computer Communications* 30(14–15), 2826–2841 (2007)
- [4] Liu, X.: A survey on clustering routing protocols in wireless sensor networks. *Sensors* 12(8), 11113–11153 (2012)
- [5] Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. *Elsevier Journal of Ad Hoc Networks* 3(3), 325–349 (2005)
- [6] Younis, M., Youssef, M., Arisha, K.: Energy-aware management in cluster-based sensor networks. *Computer Networks* 43(5), 649–668 (2003)
- [7] Jolly, G., Younis, M.: An energy efficient, scalable and collision less MAC layer protocol for wireless sensor networks. *Wireless Communications and Mobile Computing* 5(3), 285–304 (2005)
- [8] Wu, T., Biswas, S.: A self-reorganizing slot allocation protocol for multi-cluster sensor networks. In: *Proceedings of IPSN 2005* (April 2005)
- [9] Dasgupta, K., Kalpakis, K., Namjoshi, P.: An efficient clustering based heuristic for data gathering and aggregation in sensor networks. In: *WCNC 2003*, New Orleans, LA (March 2003)
- [10] Kawadia, V., Kumar, P.R.: Power control and clustering in Ad Hoc networks. In: *Proceedings of IEEE INFOCOM*, San Francisco, CA (March 2003)
- [11] Chatterjee, M., Das, S.K., Turgut, D.: WCA: a Weighted Clustering Algorithm for mobile Ad Hoc networks. *Cluster Computing* 5(2), 193–204 (2002)
- [12] Amis, A.D., Prakash, R., Vuong, T.H.P., Huynh, D.T.: Max-Min D- cluster formation in wireless Ad Hoc networks. In: *Proceedings of IEEE INFOCOM* (March 2000)
- [13] Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: Application specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications* (2002)
- [14] Younis, O., Fahmy, S.: HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks. *IEEE Transactions on Mobile Computing* 3(4), 366–379 (2004)
- [15] Ding, P., Holliday, J., Celik, A.: Distributed energy-efficient hierarchical clustering for wireless sensor networks. In: Prasanna, V.K., Iyengar, S.S., Spirakis, P.G., Welsh, M. (eds.) *DCOSS 2005. LNCS*, vol. 3560, pp. 322–339. Springer, Heidelberg (2005)
- [16] Amini, N., Vahdatpour, A., Xu, W., et al.: Cluster size optimization in sensor networks with decentralized cluster-based protocols. *Computer Communications* 35(2), 207–220 (2012)

- [17] Wang, S.S., Chen, Z.P.: LCM: a link-aware clustering mechanism for energy-efficient routing in wireless sensor networks. *IEEE Sensors Journal* 13(2), 728–736 (2013)
- [18] Gao, T., Jin, R.C., Song, J.Y., et al.: Energy-efficient cluster head selection scheme based on multiple criteria decision making for wireless sensor networks. *Wireless Personal Communications* 63(4), 871–894 (2012)
- [19] Alippi, C., Camplani, R., Roveri, M.: An Adaptive LLC-Based and Hierarchical Power-Aware Routing Algorithm. *IEEE Transactions on Instrumentation and Measurement* 58(9), 3347–3357 (2009)
- [20] Cheng, Z., Perillo, M., Heinzelman, W.: General Network Lifetime and Cost Models for Evaluating Sensor Network Deployment Strategies. *IEEE Trans. Mobile Computing* 7(4), 484–497 (2008)

Predictive Nearest Neighbor Queries over Uncertain Spatial-Temporal Data

Jinghua Zhu, Xue Wang, and Yingshu Li

Department of Computer Science,
Georgia State University, Atlanta GA, USA
jhzhu.ellen@gmail.com

Abstract. Predictive nearest neighbor queries over spatial-temporal data have received significant attention in many location-based services including intelligent transportation, ride sharing and advertising. Due to physical and resource limitations of data collection devices like RFID, sensors and GPS, data is collected only at discrete time instants. In-between these discrete time instants, the positions of the monitored moving objects are uncertain. In this paper, we exploit the filtering and refining framework to solve the predictive nearest neighbor queries over uncertain spatial-temporal data. Specifically, in the filter phase, our approach employs a semi-Markov process model that describes object mobility between space grids and prunes those objects that have zero probability to encounter the queried object. In the refining phase, we use a Markov chain model to describe the mobility of moving objects between space points and compute the nearest neighbor probability for each candidate object. We experimentally show that our approach can filter out most of the impossible objects and has a good predication performance.

Keywords: spatial-temporal data, uncertain data, predictive query, Markov chain, semi-Markov model.

1 Introduction

With the emerging and proliferation of GPS enabled mobile devices and wireless communications, processing and managing spatial-temporal data becomes vital for many location-based services including intelligent transportation, ride sharing and advertising [1]. Predictive queries over spatial-temporal data are proved to be vital in these applications such as nearest neighbor queries, e.g., "find the nearest companions of a moving tourist 1 hour later", range queries, e.g., "find customers who are predicted to be within ten miles of my moving store in the next 30 minutes" and aggregate queries, e.g., "find areas with predictive traffic jam before it happens" [2, 11–15].

However, due to physical and resource limitations of data collection devices like RFID, sensors and GPS, data is collected only at discrete time instants. In-between these discrete time instants, the positions of the tracked moving objects are uncertain. As shown in Fig.1, the trajectory in Fig.1(a) has no uncertainty,

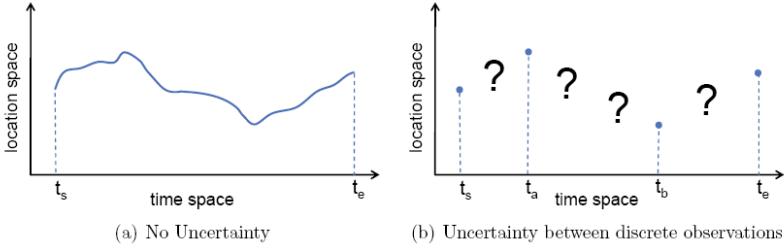


Fig. 1. Trajectory in Space and Time

and the trajectory in Fig.1(b) has uncertainty. Unlike most of the existing works regarding predictive queries that assume the deterministic behavior of object movement, few research works assume uncertainty about these trajectories. Basically, uncertainty deals with stochastic process with respect to object locations and velocities at different time instants. In this paper, we assume that the uncertain movement of an object between consecutive observations can be described by a Markov Chain Model, which captures the time dependencies between consecutive locations. The work in [4] shows that the possible worlds (trajectories between consecutive observations) can be efficiently analyzed and probability query evaluation can be facilitated by integrating pruning mechanisms into Markov Chain matrices. All these are sufficient for the case where there are few queried objects following similar movements; however, if there is a large number of objects in the database, with different movements, especially the query objects are moving as other objects, evaluating a predictive probability spatial-temporal query directly against each object individually would be very expensive. The work in [5] proposes hierarchical index UST tree to bound the uncertain movement of objects. It allows for efficient and effective filtering during query evaluation. However, the storage cost and time cost for UST construction and reconstruction will increase with the number of possible states.

In this work, we exploit the filtering and refining framework to evaluate predictive nearest neighbor queries over uncertain spatial-temporal data. In the filtering phase, a semi-Markov model that describes objects mobility between space grids and prunes those objects that have zero probability to encounter the queried object. In the refinement phase, we use a Markov chain model to describe the mobility of moving objects between space points and compute the nearest neighbor probability for the small amount of candidate objects. The main contributions of our work are as follows:

- We introduce the predictive probability nearest neighbor query (PPNN) over uncertain spatial-temporal data; both the query objects and the common objects are moving randomly in the space.
- We exploit the filtering and refining framework to process the proposed PPNN queries.
- We use a semi-Markov model to describe the object movement between space grids and effectively prune the impossible objects.

- We use a Markov Chain model to describe the object movement between space points and compute the PPNN probability for each candidate object.
- We conduct thorough experimental evaluation of the proposed method to validate its performance.

The remainder of this paper is organized as follows: in Section 2, we discuss the related works about uncertain spatial-temporal queries. Section 3 gives the predictive probability query definition and assumptions. Section 4 and Section 5 introduce the Semi-Markov and Markov model which are used to describe the uncertain movement in two space levels. We describe the PPNN algorithm in Section 6 and evaluate its query performance using real and synthetic data in Section 7. Finally, Section 8 concludes this paper.

2 Related Works

The management of spatial-temporal data has gained increasing interests in many location based applications. A typical aim of these applications is to answer users’ queries such as range queries, nearest neighbor queries and aggregate queries [2, 11–15]. Another important set of location based services focuses on predicative spatial-temporal queries[3][7]. A mobility model is used to predict the coming path of each of the underlying objects and employ the prediction results to evaluate predictive range queries. RangeSearch and KNNSearchBF [7]are introduced to traverse a spatial-temporal index tree to find the nodes that intersect with the query circular region for Range and KNN queries, respectively. A comprehensive technique [8] that employs adaptive multi-dimensional histogram, historical synopsis, and a stochastic method is used to provide an approximate answer for aggregating spatio-temporal queries for the future.

Unlike most of the existing works in predictive queries that assume the deterministic behavior of object movements, few research works assume uncertainty about these movements. To index uncertain motions of a set of moving objects, the Bx-tree[9] is enhanced and two movement inference techniques are introduced to obtain anticipated object locations in a non-deterministic manner. A Spatio-Temporal Prediction tree, STP-tree[10], is introduced to index uncertain movement patterns and to answer predictive queries.

3 Problem Definition

3.1 Assumptions

In this paper, we assume that the given space is divided into L virtual grids $G = \{g_1, g_2, \dots, g_L\}$, where L is a system parameter representing the length of the single grid. At some certain time, one moving object can only be in one grid and there may be multiple moving objects in the same grid. Furthermore, one moving object could stay in a specific grid for a while. We also assume a discrete state space of possible locations $S = \{s_1, s_2, \dots, s_{|S|}\}$ and a discrete time

domain $T = \{0, 1, \dots, n\}$. Thus, a spatial-temporal database D stores quadruples (o_i, t, l_1, l_2) where o_i is a unique object identifier, $t \in T$ is a timestamp and $l_1 \in G$ and $l_2 \in S$ are the grid location and space location of o_i respectively. Each such quadruple corresponds to an observation that o_i has been seen at some location at time t . Let $D = \{o_1, o_2, \dots, o_{|D|}\}$ be a trajectory database containing uncertain $|D|$ moving objects. For each object $o \in D$ we store a set of observations $\Theta^o = \{< t_1, l_1^o(t_1), l_2^o(t_1) >, < t_2, l_1^o(t_2), l_2^o(t_2) >, \dots, < t_{|\Theta^o|}, l_1^o(t_{|\Theta^o|}), l_2^o(t_{|\Theta^o|}) >\}$. We assume that at any timestamp, the grid location of an object is certain, while the space location of an object between two observations is uncertain.

3.2 Predictive Probability Nearest Neighbor Queries

In this paper, we focus on the predictive nearest neighbor query over uncertain moving objects. Both the queried object and the common objects are randomly moving in the space.

Definition 1 (PPNN QUERY). A predictive probability query retrieves all objects $o \in D$ which have a sufficient high probability to be the nearest neighbor of query q at the future timet $\in T$, formally,

$$PPNNQ(D, q, t, \tau) = \{o_i \in D \setminus q, PPNN(D, o_i, q, t) \geq \tau\}$$

where $PPNN(D, o_i, q, t) = P\{\forall o_j \in D \setminus o_i : dist(l_2^i(t), l_2^j(t)) \leq dist(l_2^i(t), l_2^q(t))\}$ and $l_2^i(t)$ is the space location of object o_i at time t , $dist(x, y)$ is a distance function defined on spatial points, typically the Euclidean distance.

4 Semi-markov Model

4.1 Model

We model the mobility of object o between the virtual grids with a time homogenous semi-Markov (G_n^o, T_n^o) with discrete time. The states are represented by the grids $G = \{g_1, g_2, \dots, g_L\}$. An object that moves between two grids transits in the Markov process between the corresponding states. We assume the transition probabilities between states have the Markov memory-less property, meaning that the probability of object o transiting from state G_i^o to $G_i + 1^o$ is independent of state $G_i - 1^o$. Thus, process (G_n^o) is a standard discrete time Markov Chain. The random variable T_n^o represents the time instance of the transition $G_n^o \rightarrow G_{n+1}^o$. The random variable $T_{n+1}^o - T_n^o$ represents the sojourn time of object o in grid n . The associate Semi-Markov model is defined as follows:

$$\begin{aligned} Q_{ij}^o(t) &= P(G_{n+1}^o = j, T_{n+1}^o - T_n^o \leq t | G_n^o, G_1^o, \dots, G_L^o; T_0^o, T_1^o, \dots, T_n^o) \\ &= P(G_{n+1}^o = j, T_{n+1}^o - T_n^o \leq t | G_n^o = i) \end{aligned} \quad (1)$$

Let p_{ij}^o be transition probability that object o moves from grid i to grid j , and $p_{ij}^o = \lim_{t \rightarrow \infty} Q_{ij}^o(t), i, j \in G(2)$. In this paper, we assume that the transition probability p_{ij} are given which can be attained by the history information or given by the experts. Assume $S_i^o(t)$ is the probability that object o will leave

grid i on or before time t . It also indicates the distribution of the dwell time of object o in grid i .

$$S_i^o(t) = P(T_{n+1}^o - T_n^o \leq t | G_n^o = i) = \sum_{j=1}^L Q_{ij}^o(t) \quad (2)$$

$$S_{ij}(t) = P(t_{ij} < t) = \sum_{n=0}^{t-1} P(t_{ij} = n) \quad (3)$$

We assume that the mobility history provides a representative sample from which the sojourn time distribution can be drawn. Then, using the assumption that the dwell time random variables are independent from the embedded state transition process (G_{ij}), we derive

$$\begin{aligned} Q_{ij}(t) &= P(G_{n+1} = j, T_{n+1} - T_n \leq t | G_n = i) \\ &= P(G_{n+1} = j | G_n = i) \cdot P(T_{n+1} - T_n \leq t | G_n = i, G_{n+1} = j) \\ &= p_{ij} \cdot S_{ij}(t) \end{aligned} \quad (4)$$

4.2 Meeting Probability

If we know that an object o is currently in grid i , after t time units, it will be in grid j with probability $\varphi_{ij}^o(t)$. This provides the prediction of object grid location. To determine $\varphi_{ij}^o(t)$, we start with a special case when an object is in grid i and there is no movement between time 0 and t .

$$\begin{aligned} &P(G_t = i | G_0 = i, T_1 \geq t) \\ &= P(T_1 - T_0 \geq t | G_0 = i) \\ &= 1 - S_i(t) \end{aligned} \quad (5)$$

If the object transits at least once between time 0 and t , we consider on time k of the first transition from state i and state r to which the object moves immediately after state i . The process can be formulated as follows:

$$\begin{aligned} &P(G_t = i | G_0 = i, \text{atleastonetransition}) = \\ &\sum_{r=1}^l \sum_{k=1}^{t-1} (Q_{ir}(k) - Q_{ir}(k-1)) \varphi_{rj}(t-k) \end{aligned} \quad (6)$$

Putting them together, we obtain:

$$\varphi_{ij}(t) = (1 - S_i(t)) \varphi_{ij}(0) + \sum_{r=1}^l \sum_{k=1}^{t-1} (Q_{ir}(k) - Q_{ir}(k-1)) \varphi_{rj}(t-k) \quad (7)$$

We note that φ can be computed iteratively. Next, we show how to compute the meeting probability of two moving objects. Assume that the trajectories of moving objects are independent of each other. The probability that objects a and b will meet in grid k at future time t is $m_{ab}^k(t) = \phi_{sa,k}^a(t-t_a) \cdot \phi_{sb,k}^b(t-t_b)$. Here,

sa/sb is the most recent grid location of object a/b at time ta/tb . Then the probability that a and b will meet at any grid at time t is:

$$m_{ab}(t) = \sum_{k=1}^L m_{ab}^k(t) \quad (8)$$

The PPNN algorithm in our paper will use this meeting probability to filter those impossible result objects. We will introduce the filtering process in Section 6 in details.

5 Markov Model

5.1 Uncertain Trajectory Model

The semi-markov model in Section 4 describes the movement of objects between space grids. We can filter the impossible result objects by computing their meeting probability. However, as for the remaining candidate objects, we have to compute their nearest neighbor probability.

We can describe the location of an uncertain moving object at time t as a random variable $o(t)$. Given a time interval $[0, t]$, the locations of moving objects can be represented by a family of correlated random variables, i.e. a stochastic process.

In this paper, we explore the Markov Model as a specific instance of a stochastic process. As introduced in Section 3.1, the state space of the Markov Model is the spatial domain S , and state transitions are defined over time domain T . The Markov chain model is based on the assumption that the position $o(t+1)$ of an uncertain object o only depends on the location $o(t)$ at time t .

The condition probability $M_{ij}^o(t) = P(o(t+1) = s_j | o(t) = s_i)$ (10) is the transition probability of uncertain object o from state i to state j at a given time t . Transition probabilities are stored in a matrix $M^o(t)$, called transition matrix of object o at time t . Let $\mathbf{s}(t) = (s_1, s_2, \dots, s_{|S|})^T$ (11) be the distribution vector of object o at time t , where $\mathbf{s}(t) = P\{o(t) = s_i\}$. Without any further knowledge, the distribution $\mathbf{s}(t+1)$ can be obtained from $\mathbf{s}(t)$ by the following formula $\mathbf{s}(t+1) = M^o(t)^T \cdot \mathbf{s}(t)$ (12).

5.2 Nearest Neighbor Probability

We start by computing the probability that a candidate object o is the NN of query q at time t . Let $J(t)$ be the joint probability matrix of o and o' . $J_{ijk}(t) = P(o(t) = s_i \wedge o'(t) = s_j \wedge q(t) = s_k)$ (13) denotes the probability that at time t object o is in state s_i , object o' is in state s_j and query q is in state s_k . We assume that the movement of uncertain objects are dependent of each other, therefore, matrix $J(t)$ can be computed by $J(t) = \mathbf{s}_o(t) \cdot \mathbf{s}_{o'}(t)^T \cdot \mathbf{s}_q(t)^T$ (14). From this joint probability matrix, we can compute the probability that o is closer to q than o' at time t as follows. We need to define an indicator matrix I :

$$I_{ijk}(t) = \begin{cases} 1, & \text{if } dist(s_i, s_k) \leq dist(s_j, s_k) \\ 0, & \text{otherwise} \end{cases} \quad (15)$$

The indicator matrix $I(t)$ can describe for each state pair, which state is closer to q . Therefore, we can determine the aggregated probability of o being closer than o' by evaluating $H(t) = J(t) \cdot I(t)$. $H(t)$ represents all the possible worlds still satisfying the query predicated at time t , and for each entry $H_{ijk}(t)$, we have to aggregate over all states object o , o' and q can come from the previous time step $t - 1$, as the following formula shows:

$$H_{ijk}(t) = \sum_l \sum_m \sum_n (H_{lmn}(t-1) \cdot M_{li}^o(t-1) \cdot M_{mj}^{o'}(t-1) \cdot M_{nk}^q(t-1)) \cdot I_{ijk}(t) \quad (16)$$

Therefore, (16) can be rewritten as

$$H(t) = (H(t-1) \cdot M^o(t-1) \cdot M^{o'}(t-1) \cdot M^q(t-1)) \cdot I(t) \quad (17)$$

Then the following holds:

$$PPNN(o, q, \{o'\}, t) = \sum_i \sum_j \sum_k (H_{ijk}(t)) \quad (18)$$

Due to the stochastic independence of moving objects, the NN probability of o in the candidate sets CS can be computed as following:

$$PPNN(o, q, CS, t) = \prod_{o' \in CS} PPNN(o, q, \{o'\}, t) \quad (19)$$

6 PPNN Algorithm

In this section, we present the detailed processing algorithm for a PPNN query. In the tracking system, we first maintain for each moving object two models, the Semi-Markov and Markov models as introduced in Section 4 and Section 5. We can construct these models based on the history trajectories. Then we can process a predictive query by employing the PPNN algorithm. Algorithm 1 and algorithm 2 are the pseudocodes summarizing the above process for processing a PPNN query.

PPNN-Filter, by employing the Semi-Markov model and computing the contact probabilities for objects o and q , we can prune a great number of impossible results and get an candidate set CS. As shown in line 3 in Algorithm1, the contact probability is computed according to Formula (9) in Section 4.

PPNN-Refine, by employing the Markov model and computing the NN probability for each object in the candidate set, we can obtain the final objects satisfying the query predicates. As shown in Algorithm 2, given the trajectory database D, the candidate set CS, the future time t_e and the query object q , Algorithm 2 will output the predictive possible nearest neighbor of q . Line 1 and line 2 first generate the indicator matrix for each discrete time stamp from now to the future time t_e . Lines 3 through 9 use a double loop to compute the

Algorithm 1. PPNN_Filter

Input: (1) Uncertain trajectory database D , (2) future query time t , and (3) query object q
Output: Candidate result object set CS

- 1: $CS := \emptyset;$
- 2: **for** each node o in $D - q$ **do**
- 3: Compute $m_{oq}(t) = \sum_{k=1}^L m_{oq}^k(t);$
- 4: **if** $m_{oq}(t) > 0$ **then**
- 5: Insert o into $CS;$
- 6: Return $CS;$

PPNN probability for each candidate object when there is only one object o' in database D . Then in line 10, due to the independence of each object trajectory, we can compute the final NN probability of object o according to Formula (19) in Section 5.

Algorithm 2. PPNN_Refine

Input: (1) Uncertain trajectory database D , (2) future query time te , (3) query object q , (4) candidate query result set CS
Output: query result object set RS

- 1: $RS := \emptyset;$
- 2: **for** $t=0$ to te **do**
- 3: Generate $I(t);$
- 4: **for** each o in CS **do**
- 5: **for** each o' in $CS - o$ **do**
- 6: $J(0) = \vec{s}^{\delta}(0) \cdot s^{o'}(0)^T \cdot \vec{s}^q(0)^T$
- 7: $H(0) = (M^o(0) \cdot M^{o'}(0) \cdot M^q(0)) \cdot I(0);$
- 8: **for** $t=1$ to te **do**
- 9: $H(t) = (H(t-1) \cdot M^o(t-1) \cdot M^{o'}(t-1) \cdot M^q(t-1)) \cdot I(t);$
- 10: $PPNN(o, q, \{o'\}, t) = \sum_i \sum_j \sum_k (H_{ijk}(t));$
- 11: $p = PPNN(o, q, CS, t) = \coprod_{o' \in CS} PPNN(o, q, \{o'\}, t);$
- 12: **if** $p > 0$ **then**
- 13: Insert o into $RS;$
- 14: Return $RS;$

7 Experiment Evaluation

In this section we report on the experimental results on different datasets. We describe the relevant settings in Section 7.1 and present the experimental results in Section 7.2.

7.1 Experimental Settings

We conduct a set of experiments to verify both the effectiveness and efficiency of the proposed solutions, using a desktop computer having an Intel i3-2370 CPU at 2.40GHz and 4GB of RAM. We use the data generator to construct a two dimensional Euclidean state space, consisting of n states. Each of these states is drawn uniformly from the $[0, 1]^2$ square. The space is further divided into L virtual grids. We assume that the mobility history provides a representative sample from which the sojourn time distribution can be drawn. In order to construct a transition matrix, we derive a graph by introducing edges between any point and its neighbors. We then set the transition probability of this entry indirectly proportional to the distance between the two connected vertices.

7.2 Experimental Results

Varying the Number of Grids

We set the number of moving objects to be 10000 in the first experiment and evaluate the filtering capability when varying the number of grids from 100 to 1000. As shown in Fig.2(a), the more the virtual grids, the fewer the candidates left. It means that the filtering capability increases with the number of grids. In fact, the filtering capability will be more obvious when the number of grids is large. However, the computation cost will increase with the number of grids as shown in Fig.2(b). Therefore, there is a tradeoff between the number of grids and the computation cost.

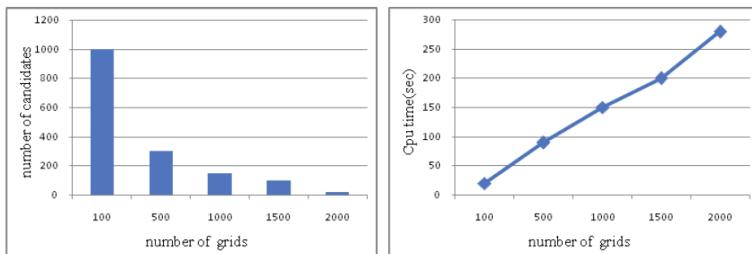


Fig. 2. (a)Filtering capability VS #grids (b)CPU time VS #grids

Varying the Number of Space States

The CPU time increases with the number of states in the refinement phase. However, after the filtering phase, there are only a small number of candidate objects left. Hence, the CPU time will not increase too much with the number of the space states. As shown in Fig.3(a), the CPU time only increases a little when increasing the number of states. As shown in Fig.3(b), the size of the candidate set is relative stable when varying the number of states. It is related to the size of grids.

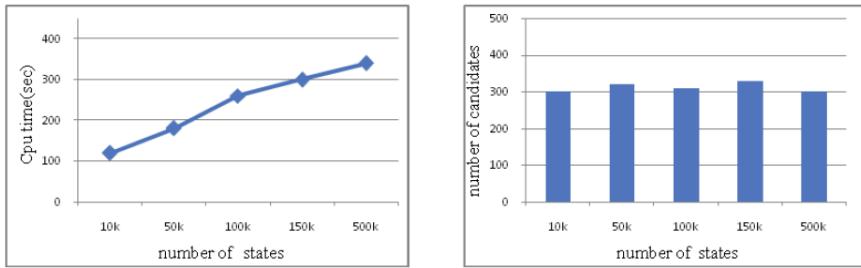


Fig. 3. (a)Filtering capability VS #states (b) CPU time VS #states

Varying the Number of Objects

As shown in Fig.4 and Fig.5, the number of objects leads to a decreasing performance as well. The more objects stored in a database with the same underlying motion model, the more candidates objects are found during the filtering step. This leads to an increasing number of probability calculations during refinement, and hence a higher query cost.

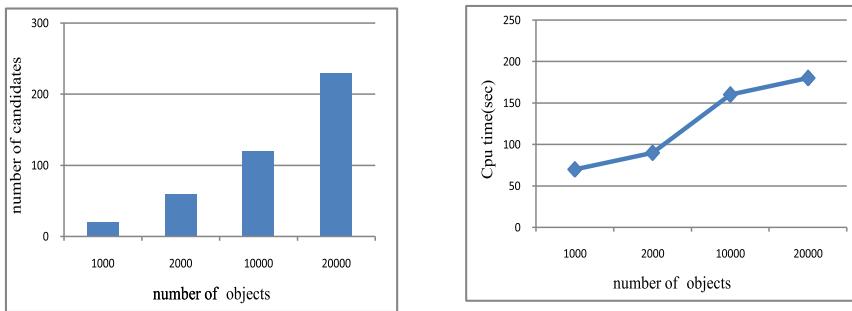


Fig. 4. Filtering capability VS #objects

Fig. 5. CPU time VS #objects

8 Conclusions

In this paper, we address the problem of processing predictive NN queries over uncertain spatial temporal data. We use the Markov chain to model the uncertain movement of objects based on stochastic processes. To cope with the large trajectory database, we exploit the filtering and refinement framework to speed up processing a predictive NN query. In the filtering phase, we divide the space into L virtual grids and model the movement of objects as a Semi-Markov chain. By computing the meeting probability of each object to the queried object, we can prune a large number of non-result objects and obtain a small number of candidate result objects. Then in the refinement phase, we model the movement

of objects as a Markov chain and compute the exact NN probability of the candidate objects. The experimental evaluation shows that our two-level Markov model can effectively describe the movement of objects and can efficiently process a predictive NN query over uncertain spatial-temporal data.

Acknowledgment. This work was supported in part by the National Science Foundation for Young Scholars of China(61100048, 61102105), and the Research Foundation of Harbin for Youth Innovative Talents(2011RFQXG028, 2012RFQXG096).

References

1. Hu, H., Xu, J., Lee, D.L.: A Generic Framework for Monitoring Continuous Spatial Queries over Moving Objects. In: Proceedings of the ACM International Conference on Management of Data, SIGMOD, Maryland, USA, pp. 479–490 (June 2005)
2. Hendawi, A.M., Mokbel, M.F.: Panda: A Predictive Spatio-Temporal Query Processor. In: Proceedings of the ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. ACM SIGSPATIAL GIS, California (2012)
3. Jeung, H., Liu, Q., Shen, H.T., Zhou, X.: A Hybrid Prediction Model for Moving Objects. In: Proceedings of the International Conference on Data Engineering, ICDE, Cancun, Mexico, pp. 70–79 (April 2008)
4. Niedermayer, J., Zufle, A., Emrich, T., Renz, M., Mamoulis, N., Chen, L., Kriegel, H.-P.: Probabilistic nearest neighbor queries on uncertain moving object trajectories. To Appear in the 40th International Conference on Very Large Databases, VLDB (2014)
5. Bian, K., Park, J.M., Chen, R.: A quorum-based framework for establishing control channels in dynamic spectrum access networks. In: MOBICOM, pp. 25–36 (2009)
6. Emrich, T., Kriegel, H.-P., Mamoulis, N., Renz, M., Zufle, A.: Indexing uncertain spatio-temporal data. In: Proc. CIKM, pp. 395–404 (2012)
7. Zhang, R., Jagadish, H.V., Dai, B.T., Ramamohanarao, K.: Optimized Algorithms for Predictive Range and KNN Queries on Moving Objects. *Information Systems* 35(8), 911–932 (2010)
8. Sun, J., Papadias, D., Tao, Y., Liu, B.: Querying about the Past, the Present, and the Future in Spatio-Temporal. In: Proceedings of the International Conference on Data Engineering, ICDE, Massachusetts, USA, pp. 202–213 (March 2004)
9. Zhang, M., Chen, S., Jensen, C.S., Ooi, B.C., Zhang, Z.: Effectively Indexing Uncertain Moving Objects for Predictive Queries. *PVLDB* 2(1), 1198–1209 (2009)
10. Tao, Y., Faloutsos, C., Papadias, D., Liu, B.: 0002. Prediction and Indexing of Moving Objects with Unknown Motion Patterns. In: Proceedings of the ACM International Conference on Management of Data, SIGMOD, Paris, France, pp. 611–622 (June 2004)
11. Cheng, S., Li, J., Cai, Z.: $O(\epsilon)$ -Approximation to Physical World by Sensor Networks. In: The 32rd Annual IEEE International Conference on Computer Communications, pp. 3084–3092

12. Cai, Z., Lin, G., Xue, G.: Improved Approximation Algorithms for the Capacitated Multicast Routing Problem. In: Wang, L. (ed.) COCOON 2005. LNCS, vol. 3595, pp. 136–145. Springer, Heidelberg (2005)
13. Ai, C., Guo, L., Cai, Z., Li, Y.: Processing Area Queries in Wireless Sensor Networks. In: The Fifth International Conference on Mobile Ad-hoc and Sensor Networks
14. Wang, X., Guo, L., Ai, C., Li, J., Cai, Z.: An Urban Area-Oriented Traffic Information Query Strategy in VANETs. In: Ren, K., Liu, X., Liang, W., Xu, M., Jia, X., Xing, K. (eds.) WASA 2013. LNCS, vol. 7992, pp. 313–324. Springer, Heidelberg (2013)
15. Cai, Z., Chen, Z., Lin, G.: A 3.4713-Approximation Algorithm for Capacitated Multicast Tree Routing Problem. Theoretical Computer Science 410(52), 5415–5424 (2009)

The Tempo-spatial Properties of Information Dissemination to Time-Varying Destination Areas in Mobile Opportunistic Networks

Xia Wang¹, Shengling Wang², Wenshuang Liang^{2,*}, Jianhui Huang³,
Rongfang Bie², and Dechang Chen⁴

¹ College of Applied Sciences, Beijing University of Technology, China

² College of Information Science and Technology, Beijing Normal University, China
lws@mail.bnu.edu.cn

³ Institute of Computing Technology, Chinese Academy of Sciences, China

⁴ Division of Epidemiology and Biostatistics,
Uniformed Services University of the Health Sciences, USA

Abstract. Mobile opportunistic networks can enable self-organizing communications in complicated and dynamic scenarios. However, existing work overlooks the tempo-spatial properties of information dissemination to time-varying destination areas in mobile opportunistic networks, which reveal whether such networks can support emerging applications with dynamic dissemination objectives. In this paper, we investigate the tempo-spatial properties of information dissemination across a linear time-varying area boundary with the Brownian motion. Our investigations give the distribution of delivery delay under the one-copy and the multiple-copy forwarding policies, where the former has only one information carrier in the network and the latter has more than one information carrier at the beginning and each delivers a copy of the information to an encountered node with a certain probability. The analytical results demonstrate the power of the multiple-copy forwarding compared to the one-copy forwarding.

Keywords: Mobile opportunistic networks, distribution of delivery delay, time-varying destination areas.

1 Introduction

Mobile opportunistic networks adopt the store-carry-forward policy to disseminate information, making it suitable for self-organizing communications in complicated and dynamic scenarios. Though mobile opportunistic networks come into being a long time before the current large-scale applications appear, people still expect them to support not only novel applications such as mobile commerce services, disaster relief, and social networking and micro-blogging, but also traditional ones such as file sharing and Internet surfing.

* Corresponding author.

To that aim, most research has been focusing on how to make effective forwarding decisions [1–4] to enhance the routing performance in terms of delivery rate and/or delay when the network has severely challenged intermittent connectivity. Meanwhile, some researchers have realized that it is important to understand the fundamental information dissemination properties of mobile opportunistic networks because they provide the answer to what one can expect for optimal performance (e.g. through theoretical bounds) or the guidelines to accelerate the information spread. As a result, analytical results on the performance limits with respect to the propagation speed [5–7], hop-count [8], connectivity [9], and delay-capacity tradeoff [10], have been obtained, which offer insights into the efficiency of data delivery between the source-destination pairs or the network throughput.

However, the above investigations can not reveal the information dissemination properties of mobile opportunistic networks from the spatial and temporal domains at the same time. Nevertheless, such properties are important because they can provide the answer regarding whether mobile opportunistic networks can support emerging applications such as mobile commerce and disaster relief, which may involve time and location sensitive information dissemination [12, 13]. In other words, current research does not reveal the potential of mobile opportunistic networks in supporting emerging applications sensitive to the tempo-spatial properties of information dissemination.

Due to the fact that the intermittent connectivity is inherent to rather than an exception of mobile opportunistic networks, they fall into the category of delay tolerant networks (DTNs). This implies that the applications of mobile opportunistic networks should be delay/disruption tolerant and thus cannot utilize the traditional TCP/IP protocols. Such unusual requirements completely change the solution landscape and make it important to understand the tempo-spatial properties of information dissemination in mobile opportunistic networks.

In [12] and [13], we have investigated the tempo-spatial properties of disseminating information to static destination areas in mobile opportunistic networks with Lévy mobility and Brownian motion models, respectively. In reality, the destination areas may be time-varying. For example, as shown in Figure 1, in an earthquake rescue application, due to the aftershock, the earthquake stricken area continuously enlarges as time goes after the principal earthquake happens. Considering that the help or warning messages should be disseminated to the areas with rescuers or the locations having more efficient resources (e.g. better communication infrastructure) for faster broadcasts over the whole network once they leave the earthquake stricken area, i.e., the destination area is outside the earthquake stricken area, the time variation of the earthquake stricken area determines the time variation of the destination area.

Obviously, it is very important to investigate the tempo-spatial properties of disseminating information to the time-varying destination areas in mobile opportunistic networks for applications such as the one illustrated in Figure 1. This is because such an investigation may help rescuers to deduce the time at which the earthquake happened, evaluate the disaster situation, figure out

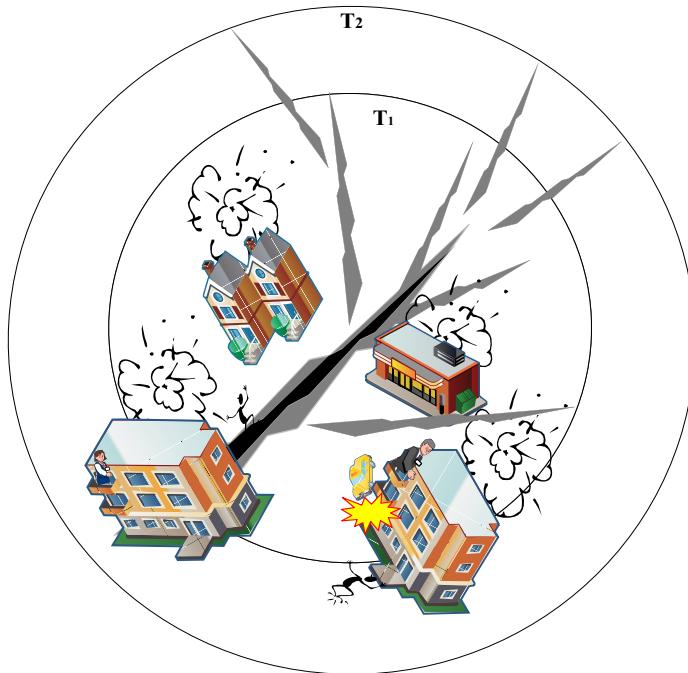


Fig. 1. An earthquake rescue application with a time-varying destination area

whether the rescuers can arrive at the disaster area before the golden window passes, or even to decide how to rescue the affected people.

In fact, such an investigation is not only important to the earthquake rescue application, but also to other emerging applications such as mobile commerce with a dynamic dissemination objective. Regretfully, no such investigation has been taken by existing work, which stimulates us to study the tempo-spatial properties of disseminating information to the time-varying destination areas in mobile opportunistic networks. In this paper, we focus on the problem regarding “how far and how fast the information can be disseminated to the time-varying destination area in mobile opportunistic networks.” It is challenging to find an answer to this problem because both the movement of nodes as well as the destination area are dynamic, making the analytical work very complicated.

As in [13], we employ the Brownian motion model in this paper to characterize the movement pattern of the nodes in the network. This is because the Brownian motion model can be viewed as a limiting case of the random walk mobility model and the Markovian mobility model. As a result, our analytical results based on the Brownian motion model can be easily extended to the random walk and Markovian mobility models.

Our analytical analysis adopts the method from simple to complex. That is, we analyze the one-copy case first, and then the multiple-copy case. In the

one-copy case, only one information carrier exists in the network and the information can be spread to the destination area only when its carrier arrives in there; and in the multiple-copy case, there are more than one information carriers at the beginning who deliver the information with some probability to others contacted opportunistically, and the information can be spread to the destination area as long as one information carrier arrives in there. For simplicity, we consider a liner time-varying destination area in this paper. Assume that the dissemination of the information starts at time 0. We obtain the following results:

1. Before time t , the probability that the information spreads to the liner time-varying destination area is $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^2$ in the one-copy case.
2. The multiple-copy mode can speed up the information spreading. The probability that the information spreads to the liner time-varying destination area before time t is $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^{2C}$, where C is the number of information copies in the network at time t .

The rest of the paper is organized as follows. The related work is presented in Section 2. Sections 3 details our analytical work on the tempo-spatial properties of information dissemination to time-varying destination areas in mobile opportunistic networks. This paper is concluded by Section 4.

2 Related Work

In recent years, most analytical work targeting mobile opportunistic networks mainly studies key metrics affecting information dissemination, including the delivery latency [5, 6, 11], the diameter of the network [8], the network connectivity [9], and the tradeoff of delay-capacity [10].

For example, Jacquet *et al.* [5] provided an upper-bound of the delivery delay between the source-destination pairs that can communicate using any routing algorithm for mobile opportunistic networks. Kim *et al.* [6] introduced a new metric $G_{\alpha,\beta}$ that denotes the time required to guarantee α -completion with a probability β , and developed a new framework to study this metric. Lee and Eun [11] studied the impact of heterogeneous contact dynamics of mobile nodes on the performance of forwarding algorithms in mobile opportunistic networks. They focused on two kinds of heterogeneities: the heterogeneity among node pairs (individual) and the heterogeneity in the underlying environment (spatial). Chaintreau *et al.* [8] defined the diameter of a network to be the number of hops needed to achieve a high proportion of delivery rate using the flooding routing policy under any time constraint and proved that the diameter grows slowly with the network size in a simple random case. Lee *et al.* [9] studied the impact of two processes, i.e. the processes of each user's availability and the mobility-induced contact/inter-contact, on the link-level connectivity. Based on the observation that the occupation probabilities and the first exit time distributions of Brownian and Lévy have a similar structure with respect to the dominating terms, Lee *et al.* [10] analytically derived the delay-capacity tradeoff for the Lévy mobility.

As described above, existing work does not reveal the information dissemination properties of mobile opportunistic networks from the spatial and temporal domains at the same time. Hence, in [12] and [13], we investigated the problem by respectively employing Lévy mobility and Brownian motion to characterize the movement pattern of the nodes in the network. Both investigations are taken from the perspectives of small- and large-scale. From the perspective of small-scale, the distribution of the delivery delay needed by the information to reach a given region is investigated; from the perspective of large-scale, the asymptotic characteristic of delivery delay needed by the information to spread to a region, whose distance to the data source is large enough, is investigated. The small- and large-scale analyses are taken under two kinds of routing policies: the one-copy and multiple-copy cases.

In conclusion, all existing work including our previous study does not investigate the scenario when the destination area is time-varying. On one hand, the time-varying destination area may exist in reality, making studying such a scenario possess practical significance; on the other hand, it is important to study the information dissemination properties of mobile opportunistic networks from the spatial and temporal domains at the same time. This is because such a study can provide the answer regarding whether mobile opportunistic networks can support some emerging applications. Due to the above reasons, in this paper, we study the tempo-spatial properties of information dissemination to time-varying destination areas in mobile opportunistic networks.

3 Our Analytical Work

In this paper, we study the information dissemination properties of mobile opportunistic networks from the spatial and temporal domains at the same time, by answering the question regarding “how far and how fast the information can be disseminated to the time-varying destination areas in mobile opportunistic networks”. let $g(t)$ be a region boundary, where $g(t) : (0, \infty)$ is a continuous function satisfying $g(0+) \geq 0$. The destination area is outside $g(t)$. Then, our problem is to study the distribution of the delivery delay needed by the information to spread outside of $g(t)$.

Because the time-varying area boundary complicates the analytical problem, in this paper, we focus on the linear time-varying case for simplicity. That is:

$$g(t) = \alpha t + \beta,$$

where $\alpha \in \mathbb{R}$, $\beta > 0$. The more complicated area boundaries such as a nonlinear time-varying one will be investigated in our future work.

As described above, our analytical work adopts the method from simple to complex. That is, we will analyze the one-copy case first, and then generalize to the multiple-copy case. The detailed analyses are introduced in the following subsections.

3.1 One-Copy Case

Theorem 1. Let $\{B_t : t \geq 0\}$ be a standard \mathbb{R} -Brownian motion started at zero, and let

$$\tau = \inf\{t > 0 : B_t \geq g(t)\}.$$

Then the probability density function of τ is:

$$f_\tau(t) = \frac{\beta}{t^{\frac{3}{2}}} \varphi\left(\frac{\alpha t + \beta}{\sqrt{t}}\right),$$

where $\varphi(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$.

Proof. To prove this theorem, we use the idea of [14] for reference. In [14], Goran Peskir proved that the distribution of the first-passage time of a strong Markov process X with continuous sample paths satisfies an integral equation over $g(t)$. In our paper, we adopt the main method of the proof in [14], and directly obtain the explicit probability density function of the first-passage time of \mathbb{R} -Brownian motion $\{B_t : t \geq 0\}$ over a linear function $\alpha t + \beta$.

Since

$$\begin{aligned} & P\{B_t \geq g(t)\} \\ &= P\{B_t \geq \alpha t + \beta, \tau \leq t\} \\ &= E[I_{[\alpha t + \beta, \infty)}(B_t) I_{\{\tau \leq t\}}] \\ &= E[E[I_{[\alpha t + \beta, \infty)}(B_t) I_{\{\tau \leq t\}} | \tau]] \\ &= E[I_{\{\tau \leq t\}} E[I_{[\alpha t + \beta, \infty)}(B_t) | \tau]] \\ &= \int_0^t E[I_{[\alpha t + \beta, \infty)}(B_t) | \tau = s] f_\tau(s) ds \\ &= \int_0^t E[I_{[\alpha t + \beta, \infty)}(B_t) | B_s = \alpha s + \beta] f_\tau(s) ds \\ &= \int_0^t P\{B_t \geq \alpha t + \beta | B_s = \alpha s + \beta\} f_\tau(s) ds \\ &= \int_0^t P\{B_t - B_s \geq \alpha(t - s) | B_s = \alpha s + \beta\} f_\tau(s) ds \\ &= \int_0^t P\{B_t - B_s \geq \alpha(t - s)\} f_\tau(s) ds \\ &= \int_0^t P\{B_{t-s} \geq \alpha(t - s)\} f_\tau(s) ds, \end{aligned}$$

where I_A is an indicator function of set A ; that is, if $x \in A$, $I_A(x) = 1$, and if $x \in A^c$, $I_A(x) = 0$. Here, the following facts are utilized: $\forall t > s > 0$, $B_t - B_s$ is independent of B_s , and $B_t - B_s$ has the identical distribution with B_{t-s} .

Let $\Phi(x) = \int_{-\infty}^x \varphi(z) dz$ and $\Psi(x) = 1 - \Phi(x)$. We have

$$\Psi\left(\frac{\alpha t + \beta}{\sqrt{t}}\right) = \int_0^t \Psi(\alpha\sqrt{t-s}) f_\tau(s) ds. \quad (1)$$

Then standard Laplace transform techniques therefore can be applied to solve Eq. (1) yielding the following explicit formula:

$$f_\tau(t) = \frac{\beta}{t^{\frac{3}{2}}} \varphi\left(\frac{\alpha t + \beta}{\sqrt{t}}\right). \quad (2)$$

According to Eq. (2), we get

$$F_\tau(t) = \int_0^t f_\tau(s) ds = \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi\left(\frac{\alpha s + \beta}{\sqrt{s}}\right) ds. \quad (3)$$

In the one-copy case, there is only one copy of the data at any instant of the time in the whole network. Let $\{\mathbb{B}_t^{(1)} : t \geq 0\}$ be a \mathbb{R}^2 - Brownian motion process, denoting the position of the data at time t when it starts at $(0,0)$ at time 0. Let $\mathbb{T}^{(1)}$ be the least time needed by the data to reach the destination area in the one-copy case. Let

$$\mathbb{T}^{(1)} = \inf\{t > 0 : \mathbb{B}_t^{(1)} \in \overline{(-\infty, g(t)] \times (-\infty, g(t)]}\}.$$

Theorem 2. *The distribution of $\mathbb{T}^{(1)}$ satisfies*

$$P\{\mathbb{T}^{(1)} > t\} = [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi\left(\frac{\alpha s + \beta}{\sqrt{s}}\right) ds]^2.$$

Proof. Since $\mathbb{B}_t^{(1)} = (\mathbb{B}_{x,t}^{(1)}, \mathbb{B}_{y,t}^{(1)})$, where $\mathbb{B}_{x,t}^{(1)}$ and $\mathbb{B}_{y,t}^{(1)}$ are x and y coordinates of the data at time t , respectively, and the \mathbb{R} -Brownian motion processes $\{\mathbb{B}_{x,t}^{(1)}\}$ and $\{\mathbb{B}_{y,t}^{(1)}\}$ are *i.i.d*, we have:

$$\mathbb{T}^{(1)} = \min\{\mathbb{T}_x^{(1)}, \mathbb{T}_y^{(1)}\},$$

where

$$\mathbb{T}_x^{(1)} = \inf\{t > 0 : \mathbb{B}_{x,t}^{(1)} \geq \alpha t + \beta\}$$

and

$$\mathbb{T}_y^{(1)} = \inf\{t > 0 : \mathbb{B}_{y,t}^{(1)} \geq \alpha t + \beta\}.$$

Since $\mathbb{T}_x^{(1)}$ and $\mathbb{T}_y^{(1)}$ are *i.i.d* random variables, we have

$$\begin{aligned} P\{\mathbb{T}^{(1)} > t\} &= P\{\min\{\mathbb{T}_x^{(1)}, \mathbb{T}_y^{(1)}\} > t\} \\ &= P\{\{\mathbb{T}_x^{(1)} > t\} \cap \{\mathbb{T}_y^{(1)} > t\}\} \\ &= P\{\mathbb{T}_x^{(1)} > t\} \cdot P\{\mathbb{T}_y^{(1)} > t\} \\ &= (P\{\mathbb{T}_x^{(1)} > t\})^2. \end{aligned}$$

According to (3), we have

$$P\{\mathbb{T}^{(1)} > t\} = [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi\left(\frac{\alpha s + \beta}{\sqrt{s}}\right) ds]^2.$$

In light of Theorem 2, the probability that the information goes out of $g(t)$ before time t is $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi\left(\frac{\alpha s + \beta}{\sqrt{s}}\right) ds]^2$ in the one-copy case.

3.2 Multiple-Copy Case

In this section, we analyze the multiple-copy case. According to [12, 13], when $Q \geq 1$ nodes carrying the same information start from $(0,0)$ at time 0, and the probability for each to deliver the information to the other is $\kappa > 0$, the number of nodes $M(t)$ carrying this information at time t can be easily derived through the classical *susceptible-infected* (SI) model of the epidemic theory.

Let $\tilde{\tau}$ be the delivery delay needed by the information to go out of $g(t)$ using the above multiple-copy routing policy. Also let \mathbb{T} be the delivery delay needed by the information to go out of $g(t)$ in the case that $M(t)$ nodes carrying the same information start from the origin at time 0 and never deliver the information to others, i.e. $\kappa = 0$. According to the analysis of [12, 13], $P(\tilde{\tau} > t) = P(\mathbb{T} > t)$. Hence, by solving $P(\mathbb{T} > t)$, we obtain $P(\tilde{\tau} > t)$. Let $C = [M(t)]$, where $[.]$ is the rounding operation. We have the following theorem.

Theorem 3. Let $\{\mathbb{B}_t^{(i)} : t \geq 0\}, i = 1, 2, \dots, C$, be C i.i.d \mathbb{R}^2 -Brownian motion processes, all of which start at the origin $(0,0)$ at time 0. Let

$$\begin{aligned} \mathbb{T} = \inf \{t > 0 : \mathbb{B}_t^{(1)} \in \overline{(-\infty, g(t)] \times (-\infty, g(t)]}\} \text{ or } \dots \\ \text{or } \{\mathbb{B}_t^{(C)} \in \overline{(-\infty, g(t)] \times (-\infty, g(t)]}\} \end{aligned}$$

Then

$$P\{\mathbb{T} > t\} = [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^{2C}$$

Proof. For $\forall i = 1, 2, \dots, C$, let

$$\mathbb{T}^{(i)} = \inf\{t > 0 : \mathbb{B}_t^{(i)} \in \overline{(-\infty, g(t)] \times (-\infty, g(t)]}\}.$$

Then $\mathbb{T}^{(i)}$, $i = 1, 2, \dots, C$, are i.i.d random variables and

$$\mathbb{T} = \min\{\mathbb{T}^{(1)}, \mathbb{T}^{(2)}, \dots, \mathbb{T}^{(C)}\}$$

Hence, using the result of Theorem 2, we obtain:

$$\begin{aligned} & P\{\mathbb{T} > t\} \\ &= P\{\min\{\mathbb{T}^{(1)}, \dots, \mathbb{T}^{(C)}\} > t\} \\ &= P\{\{\mathbb{T}^{(1)} > t\} \cap \dots \cap \{\mathbb{T}^{(C)} > t\}\} \\ &= P\{\mathbb{T}^{(1)} > t\} \dots P\{\mathbb{T}^{(C)} > t\} \\ &= (P\{\mathbb{T}^{(1)} > t\})^C \\ &= [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^{2C} \end{aligned}$$

Compared to Theorem 2, Theorem 3 shows that the multiple-copy mode can speed up the information spreading. Specifically, the probability that the information goes out of $g(t)$ before time t is $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^{2C}$ in the multiple-copy case.

4 Conclusion

Mobile opportunistic networks adopt the store-carry-forward policy to disseminate information, making them perfectly suitable for self-organizing communications in complicated and dynamic scenarios. However, existing work overlooks the tempo-spatial properties of information dissemination to time-varying destination areas in such networks, which stimulates our investigation. In this paper, we focus on investigating the distribution of the delivery delay needed by the information to go out of a linear time-varying area boundary. Our investigations demonstrate that before time t , the probability of the information spreading to a liner time-varying destination area is $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^2$ in the one-copy case; and $1 - [1 - \int_0^t \frac{\beta}{s^{\frac{3}{2}}} \varphi(\frac{\alpha s + \beta}{\sqrt{s}}) ds]^{2C}$ in the multiple-copy case, which clearly states that the multiple-copy mode speeds up the information spreading. In our future work, we plan to investigate more complicated scenarios such as the non-linear time-varying destination areas to further understand the tempo-spatial properties of information dissemination in mobile opportunistic networks.

Acknowledgement. The authors would like to thank the support from National Natural Science Foundation of China (61171014, 61272475, 61371185, 61202410, 10771010 and 11301015), Beijing Natural Science Foundation (No.1132008, Stochastic Analysis with uncertainty and applications in finance), PHR (No. 201006102), 111 Talent Project Fund of BJUT, P.R. China and the Fundamental Research Funds for the Central Universities(2013NT57) and by SRF for ROCS, SEM.

Note: The opinions expressed herein are those of the authors and do not necessarily represent those of the Uniformed Services University of the Health Sciences and the Department of Defense.

References

- Chen, X., Proulx, B., Gon, X.: Social Trust and Social Reciprocity Based Cooperative D2D Communications. In: MOBIHOC 2013, Bangalore, India (2013)
- Wang, S., Liu, M., Cheng, X., Li, Z., Huang, J., Chena, B.: Opportunistic Routing in Intermittently Connected Mobile P2P Networks. IEEE Journal on Selected Areas in Communications 31(9), 369–378 (2013)
- Wang, S., Liu, M., Cheng, X., Song, M.: Routing in Pocket Switched Networks. IEEE Wireless Communications 19(2), 67–73 (2012)
- Liu, G., Krishnamani, J., Sunderraman, R., Li, Y.: Prediction-based Routing with Packet Scheduling under Temporal Constraint in Delay Tolerant Networks. In: IEEE IPCCC 2013, San Diego, California, USA (2013)
- Jacquet, P., Mans, B., Rodolakis, G.: Information Propagation Speed in Mobile and Delay Tolerant Networks. IEEE Transactions on Information Theory 56(10), 5001–5015 (2010)
- Kim, Y., Lee, K., Shroff, N.B., Rhee, I.: Providing Probabilistic Guarantees on the Time of Information Spread in Opportunistic Networks. In: INFOCOM 2013, Turin, Italy (2013)

7. Jacquet, P., Mans, B., Mühlethaler, P., Rodolakis, G.: Opportunistic Routing in Wireless Ad Hoc Networks: Upper Bounds for the Packet Propagation Speed. *IEEE Journal on Selected Areas in Communications* 51(10), 2867–2891 (2007)
8. Chaintreau, A., Mtibaa, A., Massoulie, L., Diot, C.: The Diameter of Opportunistic Mobile Networks. In: ACM CONEXT, New York, USA (2007)
9. Lee, C.-H., Kwak, J., Eun, D.Y.: Characterizing Link Connectivity for Opportunistic Mobile Networking: Does Mobility Suffice. In: IEEE INFOCOM 2013, Turin, Italy (2013)
10. Lee, K., Kim, Y., Chong, S., Rhee, I., Yi, Y.: Delay-Capacity Tradeoffs for Mobile Networks with Lévy Walks and Lévy Filight. In: IEEE INFOCOM 2011, Shanghai, China (2011)
11. Lee, C.-H., Eun, D.Y.: On the Forwarding Performance under Heterogeneous Contact Dynamics in Mobile Opportunistic Networks. *IEEE Transactions on Mobile Computing* 12(6), 1107–1119 (2013)
12. Wang, S., Wang, X., Cheng, X., Huang, J., Bie, R.: The tempo-spatial information dissemination properties of mobile opportunistic networks with Lévy mobility. In: ICDCS 2014 (2014)
13. Wang, X., Wang, S., Cheng, X., Huang, J., Tian, Z.: The potential of mobile opportunistic networks for information dissemination. submitted to IEEE/ACM Transactions on Networking, TON (2014)
14. Peskir, G.: On integral equations arising in the first-passage problem for Brownian motion. *Journal of Integral Equation Application* 14(4), 397–423 (2002)

Beamforming Design for Cognitive Bidirectional Relay Networks with Imperfect CSI

Ruiqi Xue¹, Meng Zhang¹, Hui Yu¹, Hanwen Luo¹, and Huijiang Zhi²

¹ Department of Electronic Engineering
Shanghai Jiao Tong University, Shanghai, China
{xrq,mengzhang,yuhui,hwluo}@sjtu.edu.cn
² Leadcore Technology Co.,Ltd., Shanghai, China
zhihuijiang@leadcoretech.com

Abstract. Cognitive radio combined with bidirectional relay could greatly improve spectrum utilization. In this paper, we consider a multi-relay cognitive radio network with imperfect channel state information (CSI). Interference to primary users and secondary users' quality of service (QoS) are the main factors considered and optimized. Using semidefinite relaxation (SDR), the optimization problem could be transferred into a convex form and solved. Simulation results validate the effectiveness of our proposed scheme compared to nonrobust one, particularly in ensuring the stability of the system.

Keywords: beamforming; cognitive radio; bidirectional relay; QoS; imperfect CSI; robust.

1 Introduction

In the past decades, point-to-point wireless communication has made great progress, especially with the development of technologies such as multi-input-multi-output (MIMO) technology. In [1], D.Gesbert focuses on space-time coding in MIMO system and E.Telatar studies the capacity of MIMO channels in [2]. Combinations of multiple advanced technologies have increased the capacity of point-to-point communication channels significantly. However, researchers find that besides continuously enhancing channel capacity, other practical technologies are well worth studying when attempting to improve the quality of service (QoS) in a wireless communication system. Among these technologies, relay technology stands out especially in enhancing the coverage and reliability of a wireless communication system. In [3], the authors give a closed-form solution of relay precoding in sense of MSE optimization in a relay network and prove that this solution is optimal. In [4], secrecy transmission in a relay network with presence of an eavesdropper is studied and a joint design scheme is given to enhance the reliability of data transmission.

Later, researchers find that cognitive radio (CR) can be applied to relay networks to solve the spectrum scarcity. CR is a dynamic spectrum access (DSA) technology, where two types of users, primary user (PU) and secondary user

(SU), coexist in a network. PUs are already licensed and occupy certain spectrum. When PUs are idle or there exist unoccupied spectrum, SUs are permitted to access this network but some constraints should be exerted on these SUs, e.g. interference from SUs to PUs and SU QoS requirements. Besides, it has been proved that with some interference mitigation measures, SUs could be allowed to share the spectrum resources with PUs and spectrum efficiency will be further improved [5]. Then in [6], the authors derive the outage probability and the lower bound on symbol error rate (SER) of cognitive transmission in a cognitive relay network.

Conventionally, it takes four time slots to accomplish a data exchange process between two nodes via relaying but two-way relays can compete a data exchange process in two time slots. Therefore, with emergence of new technologies, especially device-to-device (D2D) communication, where user equipments tend to exchange data directly, bidirectional relay has recently drawn great attention since a user device itself could act as a two-way relay. It is promising that CR incorporating with two-way relay would further improve the spectrum utilization [7]. The authors in [8] study a network where PUs exchange data with help of a SU, which acts as a two-way relay and superimposes its own messages along with the primary transmission. A strategy of power allocation and joint design of the primary and secondary precoders is proposed and demonstrated.

In this paper, we consider a spectrum-sharing cognitive bidirectional relay network. Several pairs of PUs and SUs exchange data via a set of single-antenna two-way relays. It is assumed that the channel state information (CSI) is perfectly known at the relay side while users can not obtain perfect CSI, which means there exists channel estimation error in downlink channel. Although pre-coder design with imperfect CSI in cognitive relay network has been studied in [9], we propose a novel optimization strategy towards SU QoS and interference to PUs in a scenario of multiple two-way relays, which is different from [9] where outage performance is the principal problem. With presence of channel estimation error, simulation results verify that our robust scheme outperforms nonrobust scheme particularly in the stability of the system.

The rest of the paper is organized as follows. System model and problem formulation are presented in section 2. Section 3 exhibits our first scheme with sum PU interference minimization and SU QoS constraints. Another scheme with worst case SU QoS optimization and sum PU interference constraint is proposed in section 4. Simulation result and analysis are shown in section 5. Finally, conclusions are drawn in section 6.

Notation: In this paper, we use bold uppercase and lowercase letters denote matrices and vectors, respectively; $(\cdot)^T$, $(\cdot)^H$, denote the conjugate, transpose, conjugate transpose and inverses of a matrix or a vector, respectively; $\mathbf{x} = \text{diag}\{\mathbf{X}\}$ is the vector formed by diagonal elements of the diagonalized matrix \mathbf{X} and $\mathbf{X} = \text{diag}\{\mathbf{x}\}$ is a diagonal matrix whose diagonal elements is from \mathbf{x} ; $Tr(\cdot)$ is the trace of a matrix.

2 System Model and Problem Formulation

When SUs access into a cognitive bidirectional relay network, there already exist multiple primary user-pairs which exchange data through help of multiple single-antenna bidirectional relays as shown in Fig.1. Assume that there's no direct link between users. All PUs and SUs are equipped with single antenna and they exchange messages simultaneously using the same spectrum. We assume that there exist P PUs and S SUs communicating via help of R two-way relays and all these PUs and SUs are paired, which means the j -th PU is exchanging data with the \bar{j} -th ($\bar{j} = P - j$) PU and the i -th SU is exchanging data with the \bar{i} -th ($\bar{i} = S - i$) SU.

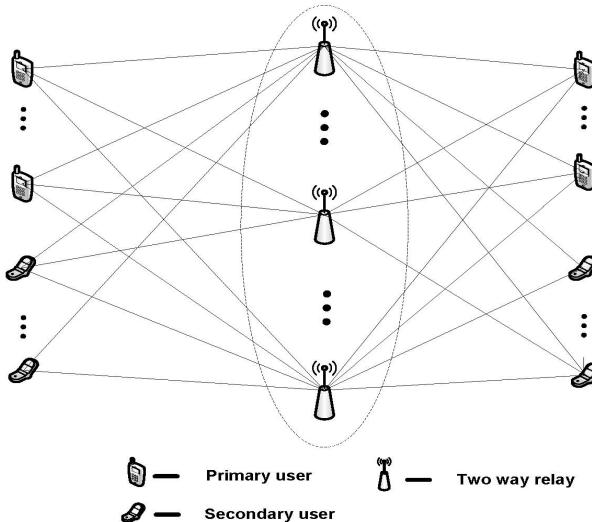


Fig. 1. Illustration of multi-relay multiuser bidirectional cognitive radio networks

In the first timeslot, all P PUs and S SUs will transmit messages to the R relays and the signal received at relays can be expressed as

$$\mathbf{y}_r = \sum_{m=1}^P \mathbf{h}_m^{(p)} p_m + \sum_{n=1}^S \mathbf{h}_n^{(s)} s_n + \mathbf{n}_r, \quad (1)$$

where p_m and s_n are transmitted signal from m -th PU and n -th SU, respectively, with $\mathbf{E}\{s_n s_n^H\} = \sigma_s^2$, $\mathbf{E}\{p_m p_m^H\} = \sigma_p^2$; $\mathbf{y}_r = [y_1, y_2, \dots, y_i, \dots, y_R]$ and y_i denotes the signal received at i -th relay; $\mathbf{h}_m^{(p)} \in \mathbb{C}^{R \times 1}$ represents the equivalent uplink channel between the m -th primary user and relays; $\mathbf{h}_n^{(s)} \in \mathbb{C}^{R \times 1}$ represents the equivalent uplink channel between the n -th secondary user and relays. Besides, $\mathbf{n}_r \in \mathbb{C}^{R \times 1}$ is zero-mean additive Gaussian noise at relays with the covariance

$\sigma_n^2 \mathbf{I}$. The received signal is broadcasted after multiplied by the equivalent relay precoding matrix $\mathbf{F} \in \mathbb{C}^{R \times R}$, $\mathbf{F} = \text{diag}\{f_1, f_2, \dots, f_R\}$, where f_1, f_2, \dots, f_R denote the beamforming factors on each relay node. Thus the transmit signal can be expressed as

$$\mathbf{x}_r = \mathbf{F} \sum_{m=1}^P \mathbf{h}_m^{(p)} p_m + \mathbf{F} \sum_{n=1}^S \mathbf{h}_n^{(s)} s_n + \mathbf{F} \mathbf{n}_r. \quad (2)$$

Then the received signal at the i -th secondary user can be written as

$$y_i^{(s)} = \mathbf{g}_i^{(s)} \mathbf{F} \sum_{m=1}^P \mathbf{h}_m^{(p)} p_m + \mathbf{g}_i^{(s)} \mathbf{F} \sum_{n=1}^S \mathbf{h}_n^{(s)} s_n + \mathbf{g}_i^{(s)} \mathbf{F} \mathbf{n}_r + n_i^{(s)}, \quad i = 1, 2, \dots, S, \quad (3)$$

where $\mathbf{g}_i^{(s)}$ represents the equivalent downlink channel between relays and the i -th secondary user; $n_i^{(s)}$ is the Gaussian white noise at the i -th secondary user with covariance σ_n^2 . Likewise, the receiving signal at the j -th primary user can be presented as

$$y_j^{(p)} = \mathbf{g}_j^{(p)} \mathbf{F} \sum_{m=1}^P \mathbf{h}_m^{(p)} p_m + \mathbf{g}_j^{(p)} \mathbf{F} \sum_{n=1}^S \mathbf{h}_n^{(s)} s_n + \mathbf{g}_j^{(p)} \mathbf{F} \mathbf{n}_r + n_j^{(p)}, \quad j = 1, \dots, P, \quad (4)$$

where $\mathbf{g}_j^{(p)}$ represents the equivalent downlink channel between relays and the j -th primary user; $n_j^{(p)}$ is the Gaussian white noise at the j -th primary user with covariance σ_n^2 . After self-cancellation, the received signal at the i -th secondary user and j -th primary user can be written in the form

$$\tilde{y}_i^{(s)} = \mathbf{g}_i^{(s)} \mathbf{F} \mathbf{h}_{\bar{i}}^{(s)} s_{\bar{i}} + \mathbf{g}_i^{(s)} \mathbf{F} \sum_{m=1}^P \mathbf{h}_m^{(p)} p_m + \mathbf{g}_i^{(s)} \mathbf{F} \sum_{n=1, n \neq i, \bar{i}}^S \mathbf{h}_n^{(s)} s_n + \mathbf{g}_i^{(s)} \mathbf{F} \mathbf{n}_r + n_i^{(s)},$$

$$i = 1, \dots, S, \quad (5)$$

$$\tilde{y}_j^{(p)} = \mathbf{g}_j^{(p)} \mathbf{F} \mathbf{h}_{\bar{j}}^{(p)} p_{\bar{j}} + \mathbf{g}_j^{(p)} \mathbf{F} \sum_{m=1, m \neq j, \bar{j}}^P \mathbf{h}_m^{(p)} p_m + \mathbf{g}_j^{(p)} \mathbf{F} \sum_{n=1}^S \mathbf{h}_n^{(s)} s_n + \mathbf{g}_j^{(p)} \mathbf{F} \mathbf{n}_r + n_j^{(p)},$$

$$j = 1, \dots, P, \quad (6)$$

where $\bar{i} = S - i$ and $\bar{j} = P - j$ represent the index of the user paired with the i -th secondary user and the j -th primary user, respectively.

In a cognitive radio network, when secondary users access a network which already consists of several pairs of primary users served by relays, communication of both PUs and SUs should be guaranteed when designing relay beamforming. To guarantee PUs' service, interference to PUs should be constrained to a certain extent. Meanwhile, limitation on interference to PUs doesn't mean easily reducing SUs' transmitting power because SU's communication should also be

maintained. In this paper, PUs' service is guaranteed by restricting sum interference to PUs and SUs' communication is optimized by maximizing the minimum SU SINR value. Besides, we consider the imperfect CSI condition, where the relays could obtain the full channel information while all users are not able to get perfect CSI. To deal with the problems stated above, a joint beamforming design for all single-antenna relays is given and the scheme can be divided into two categories: sum PU interference minimization with SU QoS constraints and worst case SU QoS optimization with sum PU interference constraints.

3 Sum PU Interference Minimization with SU QoS Constraints

In this section, PUs' QoS is optimized by minimizing sum interference to them. It's obvious that the less interference received by PUs, the better service PUs could obtain but the more tight constraint on SUs' transmission power. Meanwhile, in order to guarantee SUs' basic QoS requirement and to satisfy relays' power requirement, SUs' SINR and sum relay power should also be taken into consideration, with SUs' SINR values above a preset threshold τ and sum relay power below the threshold P_r . The scheme can be expressed as

$$\min_{\mathbf{F}} \sum_{j=1}^P \text{INF}_j^{(p)} \quad (7a)$$

$$\text{s.t. } \|\mathbf{x}_r\|^2 \leq P_r \quad (7b)$$

$$\begin{aligned} \text{SINR}_i^{(s)} &\geq \tau \\ i &= 1, 2, \dots, S \end{aligned} \quad (7c)$$

Here we consider the imperfect CSI condition, where the relays could obtain the full channel information while all users are not able to get perfect CSI and as a consequence, there exists a channel estimation error at users. The channel estimation error is supposed to be norm-bounded, specifically,

$$\mathbf{g}_i^{(s)} = \bar{\mathbf{g}}_i^{(s)} + \Delta \mathbf{g}_i^{(s)}, \|\Delta \mathbf{g}_i^{(s)}\|^2 \leq \epsilon, \quad (8)$$

$$\mathbf{g}_j^{(p)} = \bar{\mathbf{g}}_j^{(p)} + \Delta \mathbf{g}_j^{(p)}, \|\Delta \mathbf{g}_j^{(p)}\|^2 \leq \epsilon, \quad (9)$$

where $\bar{\mathbf{g}}_i^{(s)}$ and $\bar{\mathbf{g}}_j^{(p)}$ are the estimated channels of $\mathbf{g}_i^{(s)}$ and $\mathbf{g}_j^{(p)}$, respectively; $\Delta \mathbf{g}_i^{(s)}$ and $\Delta \mathbf{g}_j^{(p)}$ are the channel estimation error.

The SINR value of the i -th SU can be denoted as (10).

$$\text{SINR}_i^{(s)} = \frac{\sigma_s^2 \|\mathbf{g}_i^{(s)} \mathbf{F} \mathbf{h}_i^{(s)}\|^2}{\sigma_p^2 \sum_{m=1}^P \|\mathbf{g}_i^{(s)} \mathbf{F} \mathbf{h}_m^{(p)}\|^2 + \sigma_s^2 \sum_{n=1, n \neq i}^S \|\mathbf{g}_i^{(s)} \mathbf{F} \mathbf{h}_n^{(s)}\|^2 + \sigma_n^2 \|\mathbf{g}_i^{(s)} \mathbf{F}\|^2 + \sigma_n^2}. \quad (10)$$

To transform the expression of $\text{SINR}_i^{(s)}$ to a convex form, we have the following S lemma.

Lemma 1. Let $f_i(\mathbf{x}) = \mathbf{x}\mathbf{Q}_i\mathbf{x}^H + 2\text{Re}\{\mathbf{x}\mathbf{r}_i\} + d_i$ for $i = 0, 1$, where $\mathbf{x} \in \mathbb{C}^n$ and $(\mathbf{Q}_i, \mathbf{r}_i, d_i) \in \mathbb{H}^n \times \mathbb{C}^n \times \mathbb{R}$ for $i = 0, 1$. Suppose that there exists an $\hat{\mathbf{x}} \in \mathbb{C}^n$ satisfying $f_1(\hat{\mathbf{x}}) \leq 0$. Then, the following statements are equivalent:

1. $f_0(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathbb{C}^n$ satisfying $f_1(\mathbf{x}) \leq 0$.
2. There exists a $t \geq 0$ such that

$$\begin{bmatrix} \mathbf{Q}_0 & \mathbf{r}_0 \\ \mathbf{r}_0^H & d_0 \end{bmatrix} + t \begin{bmatrix} \mathbf{Q}_1 & \mathbf{r}_1 \\ \mathbf{r}_1^H & d_1 \end{bmatrix} \succeq \mathbf{0}. \quad (11)$$

Using Lemma 1, after some mathematical transformation, the SINR constraint can be turned into the form

$$\Delta\mathbf{g}_i^{(s)}\mathbf{Q}_i^{(s)}\Delta\mathbf{g}_i^{(s)H} + 2\text{Re}\{\Delta\mathbf{g}_i^{(s)}\mathbf{r}_i^{(s)}\} + d_i^{(s)} \leq 0, i = 1, 2, \dots, S, \quad (12)$$

where

$$\begin{aligned} \mathbf{Q}_i^{(s)} = & -\sigma_s^2 \mathbf{F} \mathbf{h}_{\bar{i}}^{(s)} \mathbf{h}_{\bar{i}}^{(s)H} \mathbf{F}^H + \tau \sigma_p^2 \sum_{m=1}^P \mathbf{F} \mathbf{h}_m^{(p)} \mathbf{h}_m^{(p)H} \mathbf{F}^H \\ & + \tau \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \mathbf{F} \mathbf{h}_n^{(s)} \mathbf{h}_n^{(s)H} \mathbf{F}^H + \tau \sigma_n^2 \mathbf{F} \mathbf{F}^H, \end{aligned} \quad (13)$$

$$\begin{aligned} \mathbf{r}_i^{(s)} = & -\sigma_s^2 \mathbf{F} \mathbf{h}_{\bar{i}}^{(s)} \mathbf{h}_{\bar{i}}^{(s)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_p^2 \sum_{m=1}^P \mathbf{F} \mathbf{h}_m^{(p)} \mathbf{h}_m^{(p)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} \\ & + \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \mathbf{F} \mathbf{h}_n^{(s)} \mathbf{h}_n^{(s)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} + \sigma_n^2 \mathbf{F} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H}, \end{aligned} \quad (14)$$

$$\begin{aligned} d_i^{(s)} = & -\sigma_s^2 \bar{\mathbf{g}}_i^{(s)} \mathbf{F} \mathbf{h}_{\bar{i}}^{(s)} \mathbf{h}_{\bar{i}}^{(s)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_p^2 \sum_{m=1}^P \bar{\mathbf{g}}_i^{(s)} \mathbf{F} \mathbf{h}_m^{(p)} \mathbf{h}_m^{(p)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} \\ & + \tau \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \bar{\mathbf{g}}_i^{(s)} \mathbf{F} \mathbf{h}_n^{(s)} \mathbf{h}_n^{(s)H} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_n^2 \bar{\mathbf{g}}_i^{(s)} \mathbf{F} \mathbf{F}^H \bar{\mathbf{g}}_i^{(s)H}. \end{aligned} \quad (15)$$

When \mathbf{Y} is a diagonal matrix, $\mathbf{Y}\mathbf{x}\mathbf{x}^H\mathbf{Y}^H = \mathbf{X}\mathbf{y}\mathbf{y}^H\mathbf{X}^H$, where $\mathbf{y} = \text{diag}\{\mathbf{Y}\}$, $\mathbf{X} = \text{diag}\{\mathbf{x}\}$. Let $\mathbf{f} = \text{diag}(\mathbf{F})$, $\mathbf{W} = \mathbf{f}\mathbf{f}^H$, $\mathbf{H}_i^{(s)} = \text{diag}\{\mathbf{h}_i^{(s)}\}$, $\mathbf{H}_j^{(p)} = \text{diag}\{\mathbf{h}_j^{(p)}\}$. Therefore, $\mathbf{Q}_i^{(s)}$, $\mathbf{r}_i^{(s)}$ and $d_i^{(s)}$ in (13), (14), (15) can be rewritten as

$$\mathbf{Q}_i^{(s)} = -\sigma_s^2 \mathbf{H}_{\bar{i}}^{(s)} \mathbf{W} \mathbf{H}_{\bar{i}}^{(s)H} + \tau \sigma_p^2 \sum_{m=1}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} \\ + \tau \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} + \tau \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})), \quad (16)$$

$$\mathbf{r}_i^{(s)} = -\sigma_s^2 \mathbf{H}_{\bar{i}}^{(s)} \mathbf{W} \mathbf{H}_{\bar{i}}^{(s)H} \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_p^2 \sum_{m=1}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} \bar{\mathbf{g}}_i^{(s)H} \\ + \tau \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})) \bar{\mathbf{g}}_i^{(s)H}, \quad (17)$$

$$d_i^{(s)} = -\sigma_s^2 \bar{\mathbf{g}}_i^{(s)} \mathbf{H}_{\bar{i}}^{(s)} \mathbf{W} \mathbf{H}_{\bar{i}}^{(s)H} \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_p^2 \sum_{m=1}^P \bar{\mathbf{g}}_i^{(s)} \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} \bar{\mathbf{g}}_i^{(s)H} \\ + \tau \sigma_s^2 \sum_{n=1, n \neq i, \bar{i}}^S \bar{\mathbf{g}}_i^{(s)} \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} \bar{\mathbf{g}}_i^{(s)H} + \tau \sigma_n^2 \bar{\mathbf{g}}_i^{(s)} \text{diag}(\text{diag}(\mathbf{W})) \bar{\mathbf{g}}_i^{(s)H}. \quad (18)$$

Similarly, the interference received by the p -th primary user can be formulated as

$$\text{INF}_j^{(p)} = \sigma_p^2 \sum_{m=1, m \neq j, \bar{j}}^P \|\mathbf{g}_j^{(p)} \mathbf{F} \mathbf{h}_m^{(p)}\|^2 + \sigma_s^2 \sum_{n=1}^S \|\mathbf{g}_j^{(p)} \mathbf{F} \mathbf{h}_n^{(s)}\|^2 + \sigma_n^2 \|\mathbf{g}_j^{(p)} \mathbf{F}\|^2 \\ \approx \sigma_p^2 \bar{\mathbf{g}}_j^{(p)} \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{F} \mathbf{h}_m^{(p)} \mathbf{h}_m^{(p)H} \mathbf{F}^H + \sigma_s^2 \sum_{n=1}^S \mathbf{F} \mathbf{h}_n^{(s)} \mathbf{h}_n^{(s)H} \mathbf{F}^H + \sigma_n^2 \mathbf{F} \mathbf{F}^H \right) \bar{\mathbf{g}}_j^{(p)H} \\ + 2\sigma_p^2 \text{Re} \left\{ \Delta \mathbf{g}_j^{(p)} \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{F} \mathbf{h}_m^{(p)} \mathbf{h}_m^{(p)H} \mathbf{F}^H \bar{\mathbf{g}}_j^{(p)H} \right. \right. \\ \left. \left. + \sigma_s^2 \sum_{n=1}^S \mathbf{F} \mathbf{h}_n^{(s)} \mathbf{h}_n^{(s)H} \mathbf{F}^H \bar{\mathbf{g}}_j^{(p)H} + \sigma_n^2 \mathbf{F} \mathbf{F}^H \bar{\mathbf{g}}_j^{(p)H} \right) \right\} \\ = \sigma_p^2 \bar{\mathbf{g}}_j^{(p)} \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} + \sigma_s^2 \sum_{n=1}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} + \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})) \right) \bar{\mathbf{g}}_j^{(p)H} \\ + 2\sigma_p^2 \text{Re} \left\{ \Delta \mathbf{g}_j^{(p)} \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} \bar{\mathbf{g}}_j^{(p)H} \right. \right. \\ \left. \left. + \sigma_s^2 \sum_{n=1}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} \bar{\mathbf{g}}_j^{(p)H} + \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})) \bar{\mathbf{g}}_j^{(p)H} \right) \right\}. \quad (19)$$

As it is stated in [10], we can find a upper or lower bound of an expression with norm-bounded variables.

$$\max_{\|\mathbf{x}\| \leq \delta} \mathcal{X}(\mathbf{x}) = \Re(\mathbf{x}^H \mathbf{y}), \quad (20)$$

$$\min_{\|\mathbf{x}\| \leq \delta} \mathcal{Y}(\mathbf{x}) = \Re(\mathbf{x}^H \mathbf{y}), \quad (21)$$

their solutions can be given by

$$\mathcal{X}((\delta/\|\mathbf{y}\|)\mathbf{y}) = \delta\|\mathbf{y}\|, \quad (22)$$

$$\mathcal{Y}(-(\delta/\|\mathbf{y}\|)\mathbf{y}) = -\delta\|\mathbf{y}\|. \quad (23)$$

Therefore, the upper bound of sum interference received by all primary users can be formulated as

$$\begin{aligned} \sum_{j=1}^P \text{INF}_j^{(p)} &\leq \sigma_p^2 \sum_{j=1}^P \bar{\mathbf{g}}_j^{(p)H} \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} + \sigma_s^2 \sum_{n=1}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} \right. \\ &\quad \left. + \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})) \right) \bar{\mathbf{g}}_j^{(p)H} + 2\sigma_p^2 \sum_{j=1}^P \left\{ \sqrt{\epsilon} \left\| \left(\sum_{m=1, m \neq j, \bar{j}}^P \mathbf{H}_m^{(p)} \mathbf{W} \mathbf{H}_m^{(p)H} \bar{\mathbf{g}}_j^{(p)H} \right) \right\| \right\} \\ &\quad + \sigma_s^2 \sum_{n=1}^S \mathbf{H}_n^{(s)} \mathbf{W} \mathbf{H}_n^{(s)H} \bar{\mathbf{g}}_j^{(p)H} + \sigma_n^2 \text{diag}(\text{diag}(\mathbf{W})) \bar{\mathbf{g}}_j^{(p)H} \}. \end{aligned} \quad (24)$$

Besides, in a similar way as stated above, the relay power constraint can be written as

$$\begin{aligned} \|\mathbf{x}_r\|^2 &= \sigma_p^2 \sum_{m=1}^P \|\mathbf{F} \mathbf{h}_m^{(p)}\|^2 + \sigma_s^2 \sum_{n=1}^S \|\mathbf{F} \mathbf{h}_n^{(s)}\|^2 + \sigma_n^2 \|\mathbf{F}\|^2 \\ &= \sigma_p^2 \sum_{m=1}^P \mathbf{h}_m^{(p)H} \text{diag}(\text{diag}(\mathbf{W})) \mathbf{h}_m^{(p)} + \sigma_s^2 \sum_{n=1}^S \mathbf{h}_n^{(s)H} \text{diag}(\text{diag}(\mathbf{W})) \mathbf{h}_n^{(s)} \\ &\quad + \sigma_n^2 \text{Tr}(\text{diag}(\text{diag}(\mathbf{W}))). \end{aligned} \quad (25)$$

Introducing a new variable z as the upper bound of sum PU interference, which can be obtained by (24), the scheme described by (7) can be rewritten as

$$\min_{\mathbf{W}} z \quad (26a)$$

$$\text{s.t. } \sum_{j=1}^P \text{INF}_j^{(p)} \leq z \quad (26b)$$

$$\|\mathbf{x}_r\|^2 \leq P_r \quad (26c)$$

$$\text{SINR}_i^{(s)} \geq \tau \quad (26d)$$

$$\mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) = 1 \quad (26e)$$

where $i = 1, 2, \dots, S; j = 1, 2, \dots, P$. With the rank constraint in (26e), this problem is unfeasible. However, it is studied in [11] that such kind of problem can be solved by firstly dropping the rank constraint. After dropping the rank constrain, problem (26) is a typical SDP problem and can be solved by softwares such as CVX [12]. Then randomization technique can be applied to get the final solution to (7) [13].

4 Worst Case SU QoS Optimization with SSum PU Interference Constraints

In last section, we propose a beamforming design scheme with sum PU interference minimization and SU QoS constraints. In this section, another optimization scheme aiming to optimize SUs' worst SINR is given. Similarly, when we optimize SUs' SINR, the interference faced by PUs should also be restricted. Here we introduce ξ as the upper bound for the sum interference to PUs. Moreover, relay power constraint and channel estimation error are considered as well. Therefore, our second scheme could be expressed as

$$\max_{\mathbf{F}} \min_{i=1,\dots,S} \text{SINR}_i^{(s)} \quad (27a)$$

$$s.t. \quad \|\mathbf{x}_r\|^2 \leq P_r \quad (27b)$$

$$\sum_{j=1}^P \text{INF}_j^{(p)} \leq \xi \quad (27c)$$

Introducing τ as the worst SU SINR value, the scheme stated by (27) can then be rewritten as

$$\max_{\mathbf{F}} \tau \quad (28a)$$

$$s.t. \quad \text{SINR}_i^{(s)} \geq \tau, \quad (28b)$$

$$\|\mathbf{x}_r\|^2 \leq P_r \quad (28c)$$

$$\sum_{j=1}^P \text{INF}_j^{(p)} \leq \xi \quad (28d)$$

Reusing the method mentioned in last section, the optimization problem in (28) could be solved by semidefinite relaxation (SDR). Bisection search is applied in acquiring the final maximized value of SU minimum SINR.

5 Numerical Results and Discussions

In this section, numerical results are given with parameters set as follows: $P = 4, S = 2, R = 6$, which means there are 4 PUs (2 pairs), 2 SUs (1 pair) and 6

single antenna relays; $\sigma_n^2 = 1$; $\sigma_p^2 = \sigma_s^2 = 10\text{dB}$; all channels are Rayleigh flat fading channels with the downlink channel estimation error $\epsilon = 0.001$; relay sum power constraint $P_r = 50\text{dB}$. All simulation results are obtained by 1000 Monte Carlo experiments.

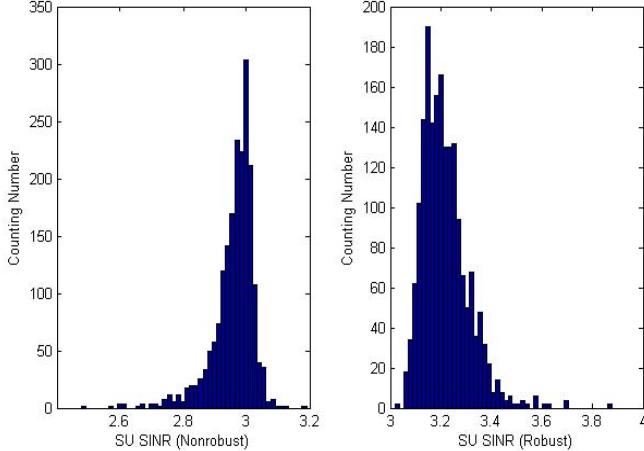


Fig. 2. SU SINR distribution with threshold $\tau = 3$

Fig. 2 shows SU SINR distribution with SU SINR threshold $\tau = 3$, which is the scheme we proposed in section 3. Our robust design is compared with nonrobust scheme which can be obtained by omitting the robust design part of the robust scheme. It can be observed that with channel estimation error, more than half of SU SINR values fall below the preset threshold τ while our robust scheme could guarantee all SU SINR values beyond the threshold. It validates the robustness of our proposed scheme.

Moreover, we study the sum PU interference and average relay power of the robust and nonrobust schemes as can be seen in Fig. 3. We can see from Fig. 3 that sum PU interference and average relay power gradually increase with the growth of threshold τ . This is reasonable as the increase of τ means more relay power is needed to maintain SU QoS and thus cause more interference to PUs. Moreover, in order to achieve the robustness of the system, more relay power is consumed and more interference to PUs is detected. However, the gap between robust and nonrobust schemes is quite small that it could almost be ignored in consideration of the robustness brought to the system.

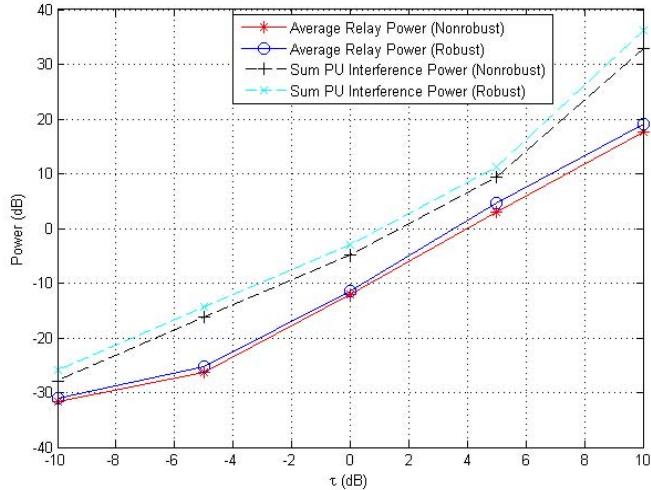


Fig. 3. Sum PU interference power and average relay power vs. SINR threshold

In Fig. 4, the robustness of our proposed scheme in section 4 is demonstrated. Similar to Fig. 2, with sum PU interference threshold $\xi = 10$, the results achieved by our robust scheme perfectly satisfy the sum interference constraint. As a comparison, about half of results acquired by nonrobust scheme violate the sum interference constraint.

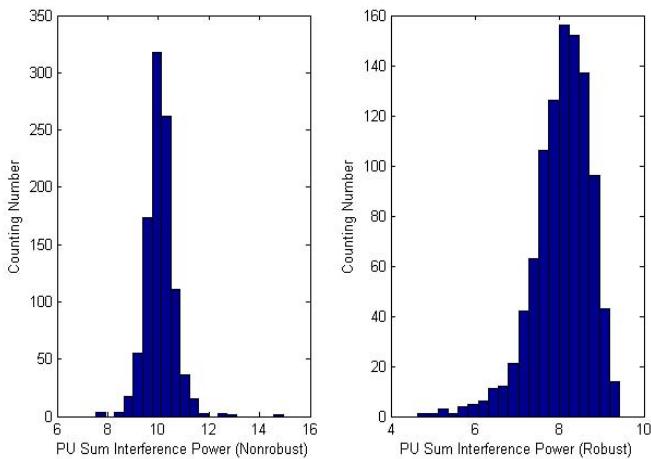


Fig. 4. Sum PU interference distribution with threshold $\xi = 10$

6 Conclusion

In this paper, we focus on a multi-relay cognitive radio network with imperfect CSI in downlink channels. In order to constrain interference to PUs as well as guarantee SU QoS, upper bound of sum interference to PUs and expressions of SU SINR values are derived and relaxed to convex forms through SDR. Simulation results indicate that our robust design can effectively resist the adverse impact of channel estimation error. Norm-bounded error model is considered in this paper while there are some other error models, e.g. channel errors subject to the Beta distribution caused by the limited feedback.

Acknowledgement. This paper is partially sponsored by National Key Project of China (No.2013ZX03001007-004).

References

1. Gesbert, D., et al.: From theory to practice: an overview of MIMO space-time coded wireless systems. *Selected Areas in Communications* 21(3), 281–302 (2003)
2. Goldsmith, A., et al.: Capacity limits of MIMO channels. *Selected Areas in Communications* 21(5), 684–702 (2003)
3. Guan, W., Luo, H.: Joint MMSE Transceiver Design in Non-Regenerative MIMO Relay Systems. *IEEE Communications Letters* 12(7), 517–519 (2008)
4. Xue, R., et al.: Joint design of relay precoding and artificial noise with presence of an eavesdropper. In: International Conference on Communications in China (ICCC), Xi'an, August 12-14 (2013)
5. Goldsmith, A., et al.: Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proceedings of the IEEE* 97(5), 894–914 (2009)
6. Yu, H., et al.: Outage probability and SER of amplify-and-forward cognitive relay networks. *Wireless Communications Letters* 1(4), 219–222 (2013)
7. Liu, J., et al.: Optimal Energy-Efficient Relay Selection and Power Allocation for Cognitive Two-Way Relay Network Using Physical-Layer Network Coding. In: Vehicular Technology Conference (VTC Fall), Las Vegas, September 2-5 (2013)
8. Wang, R., Tao, M., Liu, Y.: Optimal Linear Transceiver Designs for Cognitive Two-Way Relay Networks. *Signal Processing* 61(4), 992–1005 (2013)
9. Zhang, X., et al.: Outage performance study of cognitive relay networks with imperfect channel knowledge. *Communications Letters* 17(1), 27–30 (2013)
10. Chalise, B., Vandendorpe, L.: MIMO Relay Design for Multipoint-to-Multipoint Communications With Imperfect Channel State Information. *IEEE Transactions on Signal Processing* 57(7), 2785–2796 (2009)
11. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge Univ. Press, Cambridge (2004)
12. CVX Research, Inc. CVX: Matlab software for disciplined convex programming, version 2.0 beta (September 2012), <http://cvxr.com/cvx>
13. Huang, Y., Palomar, D.P.: Rank-Constrained Separable Semidefinite Programming With Applications to Optimal Beamforming. *IEEE Transactions on Signal Processing* 58(2), 664–678 (2010)

A Comparative Study on Full- and Half-Duplex Relaying Protocols with Practical Channel Estimates

Youyun Xu and Xiaochen Xia*

Institute of Communication Engineering, PLA University of Science and Technology,
Nanjing, China
yxu@vip.sina.com, tjuxiaochen@gmail.com

Abstract. This paper investigates the performance of cooperative relaying protocols with practical channel estimates. Two relaying protocols, i.e., the full duplex relaying (FDR) protocol and half duplex relaying (HDR) protocol, are considered. The outage probability for both protocols are analyzed and compared in the presence of imperfect channel estimates. The thresholds for residual interference power at the relay that ensure the FDR protocol outperforms the HDR protocol in outage probability are theoretically derived. Simulation results are presented to verify the theoretical analyses. Both analytic and simulation results show that the HDR protocol achieves better performance when the quality of channel estimates is good while the FDR protocol is preferred when the quality of channel estimates is bad.

Keywords: Full duplex relaying, half duplex relaying, outage probability, performance comparison.

1 Introduction

In recent years, relaying has been accepted by several standards such as IEEE 802.11s, IEEE 802.16j and LTE-Advanced as a powerful technique to provide spatial diversity in cooperation systems and extend the coverage of the wireless networks. A large number of existing works on cooperative communications considered the half duplex relaying (HDR) protocols, where the relay transmits and receives in the orthogonal frequency or time [1]-[6]. However, as shown in [7], the HDR protocol doubles the required channels for transmission from source to destination, which induces the spectral efficiency loss.

Full duplex relaying (FDR) protocol is a promising approach to improve the spectral efficiency of cooperative network, which received considerable attentions recently. In FDR protocol, the relay transmits and receives simultaneously at the same frequency and time, but at the cost of a strong echo interference due to signal

* This work is supported by the Jiangsu Province Natural Science Foundation (BK2011002), National Natural Science Foundation of China (No. 61301165 & No. 61371123) and Jiangsu Province Natural Science Foundation for Young Scholar (BK2012055).

leakage between the relay output and input [8]. To mitigate the echo interference in FDR protocol, two approaches have been studied, i.e., 1) passive cancellation techniques which are based on antenna separation or antenna directionality [9], and 2) active cancellation techniques which can be categorized into time-domain cancellation [10] and spatial suppression [11]. Inspired by these literatures, several works have dedicated to the study of FDR protocol. For example, the relay selection strategy for cooperative amplify-and-forward (AF) relaying with multiple full duplex relays has been analyzed in [12]. In [13], the authors have studied the outage performance of decode-and-forward (DF) FDR protocol. A novel block based transmission scheme to achieve the diversity gain for cooperative AF and DF protocols with full duplex relay has been proposed in [14].

However, most of the previous literatures assumed the channel state information (CSI) is perfectly known at all the participated nodes. This assumption is too optimistic in practical wireless networks where the channel estimates are corrupted by mobility, feedback delay and channel estimation error [15], [16]. As a result, it is of great importance to consider the effect of CSI imperfection when evaluating the performances of FDR and HDR protocols.

In this paper, we investigate the performance of FDR and HDR protocols with practical channel estimates in the independent but non-identical Rayleigh fading channels. We assume the channel estimates are only available at the receiver and are degraded by the feedback delay and channel estimation error. The conditional and average outage probabilities for FDR and HDR protocols are derived and compared theoretically. The threshold for residual interference at the relay that ensures the FDR protocol outperforms HDR protocol in outage performance is obtained in closed-form.

The rest of this paper is organized as follow. In the next section, we will describe the system model and present the expression for the received signal-to-interference-plus-noise ratio (SINR). The outage performance for FDR and HDR protocols are analyzed and compared in section 3. Simulation results are presented in section 4 and some conclusions will be drawn in the last section.

2 System Model and Relaying Protocols

Considering the dual-hop AF relaying network which consists a source node S , a destination node D and a relay R , where the source node transmits data to the destination with the assistance of the relay. It is assumed that the direct channel between the source and destination does not exist because the distance between S and D is large or the direct channel is degraded severely by the shadowing or physical obstacles. This assumption corresponds to the scenarios where the relay is used for coverage extension of the network [12],[14]. Let h_{UV} ($UV \in \{SR, RD\}$) denote the channel coefficient between nodes U and V with variance Ω_{UV} . Both h_{SR} and h_{RD} are reciprocal and independent Rayleigh fading. It is assumed that the knowledge of channel estimates is only available at the receiving end of each transmission.

In practical wireless network, due to feedback delay and channel estimation error, the available channel estimates are often imperfect. In this paper, to de-

scribe the impacts of channel imperfection, we use the channel model developed in [17],[18]. Specifically, we use e_{UV} to denote the channel estimation error and use the power correlation coefficient $\rho_{UV} \in [0, 1]$ to characterize the variation between the estimates of h_{UV} and its delayed version (introduced by feedback delay). As a result, the channel coefficient between nodes U and V at time instant t can be modeled as

$$h_{UV}^t = \sqrt{\rho_{UV}} \tilde{h}_{UV}^{t-d} + \sqrt{1 - \rho_{UV}} g_{UV}^t + e_{UV}^t \quad (1)$$

where e_{UV}^t is an independent complex Gaussian random variable (RV) with distribution $e_{UV}^t \sim \mathcal{CN}(0, \Omega_{UV}\sigma_{UV})$. Let \tilde{h}_{UV}^t and \tilde{h}_{UV}^{t-d} denote the channel estimates at time instant t and $t - d$, respectively, with distributions $\tilde{h}_{UV}^t \sim \mathcal{CN}(0, \Omega_{UV}(1 - \sigma_{UV}))$ and $\tilde{h}_{UV}^{t-d} \sim \mathcal{CN}(0, \Omega_{UV}(1 - \sigma_{UV}))$. We use $\sqrt{1 - \rho_{UV}} g_{UV}^t$ to denote the additional error introduced by feedback delay which can be expressed as $\sqrt{1 - \rho_{UV}} g_{UV}^t = \tilde{h}_{UV}^t - \sqrt{\rho_{UV}} \tilde{h}_{UV}^{t-d}$, where g_{UV}^t is an independent complex Gaussian RV with distribution $g_{UV}^t \sim \mathcal{CN}(0, \Omega_{UV}(1 - \sigma_{UV}))$. Note that the parameters σ_{UV} and ρ_{UV} characterize the quality of channel estimates. For example, when $\sigma_{UV} = 0$ and $\rho_{UV} = 1$, the channel estimates are perfect. The quality of channel estimates degrades as σ_{UV} increasing and/or ρ_{UV} decreasing. In the following, we neglect the superscript t and $t - d$ for convenience and use \tilde{h}_{UV} to denote the available channel estimate (i.e., \tilde{h}_{UV}^{t-d}) at the destination.

2.1 Full Duplex Relaying Protocol

In FDR protocol, the relay transmits and receives simultaneously during one time slot. It is assumed that an echo interference cancelation scheme is used at the relay. However, the residual interference exists due to the imperfect cancellation, which is characterized by the residual interference channel with fading coefficient h_{RR} . Since the distribution of h_{RR} is highly related to the employed echo interference cancellation technique, in this paper, we model the squared amplitude of residual interference channel, i.e., $|h_{RR}|^2$ as a gamma variable with mean Ω_{RR} and shape factor m_{RR} [19]. Note that this approach is widely used to model the RV with unknown distribution and the exponential assumption for $|h_{RR}|^2$ used in [12]-[14] can be treated as a special case when $m_{RR} = 1$. The received signals at the relay and destination be expressed as

$$\begin{aligned} y_R^{\text{FDR}} &= \sqrt{E_S} h_{SR} X_S + \sqrt{E_R} h_{RR} X_I + n_R \\ y_D^{\text{FDR}} &= \sqrt{E_R} h_{RD} \beta^{\text{FDR}} y_{R,\tau}^{\text{FDR}} + n_D \end{aligned} \quad (2)$$

where E_S and E_R denote the transmitted powers of source and relay, respectively. X_S denotes the unit-power transmitted symbol of S . X_I denotes the residual interference signal due to the imperfect echo interference cancelation and is modeled as $X_I \sim \mathcal{CN}(0, 1)$ [14]. $n_R \sim \mathcal{CN}(0, 1)$ and $n_D \sim \mathcal{CN}(0, 1)$ denote the additive white Gaussian noises (AWGN) received at the relay and destination, respectively. Let τ denote the processing delay at the relay. $y_{R,\tau}^{\text{FDR}}$ is the received sample at the relay with delay τ . β^{FDR} denotes the normalization factor adopted

at the relay which can be expressed as $\beta^{\text{FDR}} = \frac{1}{\sqrt{E_S|h_{SR}|^2+E_R|h_{RR}|^2}+1}$. Based on (1) and (2), the end-to-end received SINR at D for FDR protocol can be expressed

$$\text{SINR}^{\text{FDR}} = \frac{\phi_{SR}^{\text{FDR}} \phi_{RD}}{\phi_{SR}^{\text{FDR}} + \phi_{RD} + 1} \quad (3)$$

where $\phi_{SR}^{\text{FDR}} = \frac{\gamma_{SR}}{\text{RI} + I_{SR}^f + I_{SR}^e + 1}$ and $\phi_{RD} = \frac{\gamma_{RD}}{I_{RD}^f + I_{RD}^e + 1}$ denote the received SINRs of the S - R and R - D channels, respectively. Here we let $\gamma_{SR} = E_S \rho_{SR} |\tilde{h}_{SR}|^2$ and $\gamma_{RD} = E_R \rho_{RD} |\tilde{h}_{RD}|^2$. Let

$$\begin{aligned} I_{SR}^f &= \mathbb{E} [E_S (1 - \rho_{SR}) |g_{SR}|^2] = E_S \Omega_{SR} (1 - \rho_{SR}) (1 - \sigma_{SR}) \\ I_{RD}^f &= \mathbb{E} [E_R (1 - \rho_{RD}) |g_{RD}|^2] = E_R \Omega_{RD} (1 - \rho_{RD}) (1 - \sigma_{RD}) \end{aligned} \quad (4)$$

denote the average interference powers introduced by the feedback delay on S - R and R - D channels, respectively, where $\mathbb{E}[\cdot]$ indicates the expectation. Let $I_{SR}^e = \mathbb{E} [E_S |e_{SR}|^2] = E_S \Omega_{SR} \sigma_{SR}$ and $I_{RD}^e = \mathbb{E} [E_R |e_{RD}|^2] = E_R \Omega_{RD} \sigma_{RD}$ denote the average interference powers introduced by the channel estimation errors on the S - R and R - D channels. Finally, we use $\text{RI} = E_R |h_{RR}|^2$ to denote the instantaneous residual interference power due to the imperfect echo interference cancelation in FDR protocol.

2.2 Half Duplex Relaying Protocol

In HDR protocol, one time slot is divided into two phases with equal length. The source S transmits at the first phase and the received signal at the relay can be expressed as

$$y_R^{\text{HDR}} = \sqrt{E_S} h_{SR} X_S + n_R \quad (5)$$

The relay scales the received signal y_R with factor β^{HDR} , which can be expressed as $\beta^{\text{HDR}} = \frac{1}{\sqrt{E_S|h_{SR}|^2+1}}$, and sends the scaled signal at the second phase. The received signal at D can be expressed as

$$y_D^{\text{HDR}} = \sqrt{E_R} h_{RD} \beta^{\text{HDR}} y_R^{\text{HDR}} + n_D \quad (6)$$

Based on (1), (5) and (6), the received end-to-end SINR at D for the HDR protocol can be expressed

$$\text{SINR}^{\text{HDR}} = \frac{\phi_{SR}^{\text{HDR}} \phi_{RD}}{\phi_{SR}^{\text{HDR}} + \phi_{RD} + 1} \quad (7)$$

where $\phi_{SR}^{\text{HDR}} = \frac{\gamma_{SR}}{I_{SR}^f + I_{SR}^e + 1}$ denotes the received SINR of S - R channel for HDR protocol.

3 Outage Analysis and Comparison

In this section, we first derive the expressions of outage probabilities for FDR and HDR protocols. Based on the theoretical results, the relative performance of FDR and HDR protocols will be analyzed.

3.1 Conditional Outage Analysis

By definition, the outage event occurs when the mutual information at the destination falls below the target rate R_T , or equivalently, the received SINR at the destination is below the target SINR Υ_T . Note that we have $\Upsilon_T = \Upsilon_T^{\text{FDR}} = 2^{R_T} - 1$ for the full duplex protocol and $\Upsilon_T = \Upsilon_T^{\text{HDR}} = 2^{2R_T} - 1$ for the half duplex protocol. As a result, the outage probability for FDR and HDR protocols can be expressed as

$$\mathcal{P}_{\mathcal{O}}^{\psi}(R_T) = \Pr(\text{SINR}^{\psi} < \Upsilon_T^{\psi}) = 1 - \Pr\left(\frac{\phi_{SR}^{\psi}\phi_{RD}}{\phi_{SR}^{\psi} + \phi_{RD} + 1} > \Upsilon_T^{\psi}\right) \quad (8)$$

where $\psi \in \{\text{FDR}, \text{HDR}\}$.

Proposition 1. *The outage probability for FDR and HDR protocols conditioned on the residual interference at the relay RI can be expressed as*

$$\begin{aligned} \mathcal{P}_{\mathcal{O}}^{\psi}(R_T, \text{RI}) &= 1 - \frac{\delta \text{RI} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \exp\left(-\frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \Upsilon_T^{\psi}\right) \\ &\times \exp\left(-\frac{\delta \text{RI} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \Upsilon_T\right) \sqrt{\frac{4\bar{\gamma}_{SR}\Upsilon_T^{\psi}(\Upsilon_T^{\psi} + 1)}{\bar{\gamma}_{RD}}} \frac{I_{RD}^f + I_{RD}^e + 1}{\delta \text{RI} + I_{SR}^f + I_{SR}^e + 1} \\ &\times K_1\left(\sqrt{4\Upsilon_T^{\psi}(\Upsilon_T^{\psi} + 1) \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \frac{\delta \text{RI} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}}}\right) \end{aligned} \quad (9)$$

where $\delta = 1$ for FDR protocol and $\delta = 0$ for HDR protocol. $\psi \in \{\text{FDR}, \text{HDR}\}$ and $K_1(\cdot)$ denotes the first order modified Bessel function of the second kind [20]. $\bar{\gamma}_{UV}$ ($UV \in \{SR, RD\}$) denotes the mean of γ_{UV} , which can be expressed as $\bar{\gamma}_{SR} = E_S \Omega_{SR} (1 - \sigma_{SR}) \rho_{SR}$ and $\bar{\gamma}_{RD} = E_R \Omega_{RD} (1 - \sigma_{RD}) \rho_{RD}$.

Proof. The proof is similar with that for [21, Eq. 29], and thus is neglect for the sake of brevity. \square

Note that the conditional outage probability for HDR protocol given in the above is actually the average outage probability, since $\mathcal{P}_{\mathcal{O}}^{\text{HDR}}(R_T, \text{RI})$ is independent with RI. The outage performance for FDR and HDR protocols with perfect CSI considered in [2],[12] can be derived by setting I_{SR}^f , I_{SR}^e , I_{RD}^f and I_{RD}^e in (9) to zero.

Proposition 1 can be used to study the effect of instantaneous residual interference RI on the relative performance of FDR and HDR protocols. According to (3) and (8), the conditional outage probability of the FDR protocol is an increasing function of RI, and when the echo interference at the relay is perfectly canceled, the FDR protocol achieves smaller outage probability compared with the HDR protocol. Therefore, there must be a threshold for RI that ensures the FDR protocol outperforms HDR protocol in conditional outage probability, i.e., the FDR protocol outperforms the HDR protocol in conditional outage probability when the instantaneous residual interference power satisfies

$$\text{RI} < \text{RI}_{\text{th}}^{\mathcal{O}} \quad (10)$$

otherwise, the HDR protocol outperforms FDR protocol. Wherein, the threshold $\text{RI}_{\text{th}}^{\mathcal{O}}$ can be expressed approximately as [Appendix]

$$\text{RI}_{\text{th}}^{\mathcal{O}} \simeq \bar{\gamma}_{SR} \left(\frac{I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} + \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \right) \left(\frac{2^{2R_T} - 1}{2^{R_T} - 1} - 1 \right) \quad (11)$$

(11) shows that the condition which ensures the FDR protocol outperforms the HDR protocol becomes relaxed, i.e., the threshold increases, when the average interference powers introduced by feedback delay and channel estimation error increasing (ρ_{UV} decreasing and σ_{UV} increasing, $UV \in \{SR, RD\}$). However, the condition becomes strict when the average interference powers introduced by feedback delay and channel estimation error decreasing (ρ_{UV} increasing and σ_{UV} decreasing, $UV \in \{SR, RD\}$). In this case, more powerful echo interference cancelation technique should be employed at the relay in order to obtain better performance the the HDR protocol. Meanwhile, (11) shows that the condition which ensures the FDR protocol outperforms HDR protocol in conditional outage probability also becomes relaxed when the target rate R_T increases. This result suggests that the FDR protocol is more suitable in the network which requires higher data rate.

3.2 Average Outage Analysis

The average outage performances for FDR and HDR protocols are analyzed in this subsection. Based on the results, the effect of average residual interference on the relative performance of FDR and HDR protocols is studied.

Proposition 2. *The approximate expression of average outage probability for FDR and HDR protocols can be given by*

$$P_{\mathcal{O}, \text{App}}^{\psi}(R_T) = 1 - \Phi \exp \left(-\frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \gamma_T^{\psi} \right) \exp \left(-\frac{I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \gamma_T^{\psi} \right) \quad (12)$$

where $\psi \in \{\text{FDR}, \text{HDR}\}$ and Φ can be expressed as

$$\Phi = \begin{cases} \left(\frac{m_{RR}}{\overline{\text{RI}}} \right)^{m_{RR}} \left(\frac{m_{RR}}{\overline{\text{RI}}} + \frac{\gamma_T^{\text{FDR}}}{\bar{\gamma}_{SR}} \right)^{-m_{RR}}, & \text{FDR protocol} \\ 1, & \text{HDR protocol} \end{cases} \quad (13)$$

where $\overline{\text{RI}} = \mathbb{E}[\text{RI}]$.

Proof. See Appendix. \square

Note that the expression in Proposition 2 can also be obtained by using the SINR upper bounds which are derived by neglecting the term 1 on the denominators of (3) and (7) and using the harmonic-to-min approximation on the resultant expression. Therefore, the expression in Proposition 2 is actually a lower bound of the exact average outage probability.

Similarly, the FDR protocol outperforms the HDR protocol in average outage probability when the average residual interference power satisfies

$$\overline{\text{RI}} < \overline{\text{RI}}_{\text{th}}^{\mathcal{O}} \quad (14)$$

otherwise, the HDR protocol outperforms FDR protocol. Setting

$$1 - \mathcal{P}_{\mathcal{O}, \text{App}}^{\text{FDR}}(R_T) > 1 - \mathcal{P}_{\mathcal{O}, \text{App}}^{\text{HDR}}(R_T) \quad (15)$$

we can obtain an approximate expression for the threshold $\overline{\text{RI}}_{\text{th}}^{\mathcal{O}}$, which can be expressed as

$$\overline{\text{RI}}_{\text{th}} \simeq \frac{\bar{\gamma}_{SR} m_{RR}}{2^{R_T} - 1} \left\{ \exp \left(\frac{2^{2R_T} - 2^{R_T}}{m_{RR}} \left(\frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} + \frac{I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \right) \right) - 1 \right\} \quad (16)$$

From (16), we can see that threshold $\overline{\text{RI}}_{\text{th}}$ is a decreasing function of ρ_{UV} and is an increasing function of σ_{UV} , where $UV \in \{SR, RD\}$.

To get more insight about the effect of the system parameters, in the following, we develop the asymptotic analysis based on the results in Proposition 2.

Proposition 3. *The asymptotic expression of average outage probability for FDR and HDR protocols can be expressed as*

$$\mathcal{P}_{\mathcal{O}, \text{Asy}}(R_T) = \left(\frac{\delta \overline{\text{RI}} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} + \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \right) (2^{\xi R_T} - 1) \quad (17)$$

For the FDR protocol, we have $\delta = 1$ and $\xi = 1$. For the HDR protocol, we have $\delta = 0$ and $\xi = 2$.

Proof. According to [22], the asymptotic expression can be derived by performing McLaurin series expansion on the expression of average outage probability (given in Proposition 2) and neglecting the higher order terms. Therefore, by exploiting the McLaurin series expansion of some elementary functions, one can arrived at the result in Proposition 3.

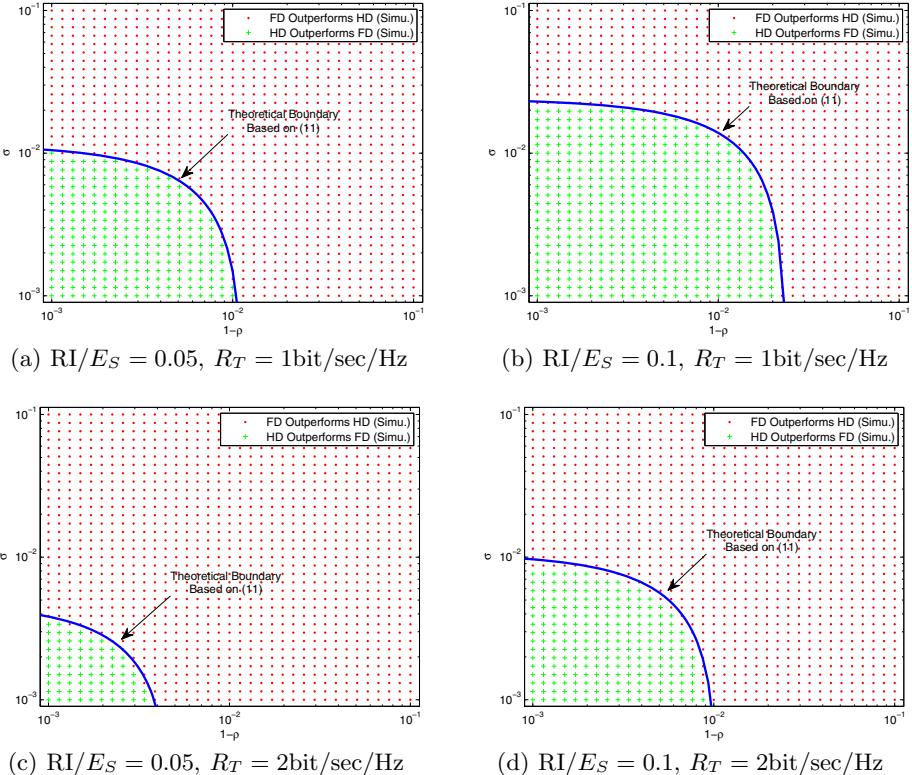


Fig. 1. The region that FDR protocol outperforms HDR protocol in conditional outage probability, where $\rho_{SR} = \rho_{RD} = \rho$, $\sigma_{SR} = \sigma_{RD} = \sigma$, $m_{RR} = 1$, $E_S = E_R = 30\text{dB}$, $\Omega_{SR} = \Omega_{RD} = 1$

From Proposition 3, it is clear that the outage probabilities of both FDR and HDR protocols degrade as the average interference powers introduced by the feedback delay and estimation error, i.e., I_{UV}^f and I_{UV}^e ($UV \in \{SR, RD\}$), increasing. Meanwhile, the outage probability of the FDR protocol is also degraded by the residual interference at the relay due to the imperfect echo interference cancellation, which is characterized by the average interference power $\overline{\text{RI}}$. Moreover, it is interesting that the asymptotic outage performance of FDR protocol is independent with the shape factor of the residual interference channel, i.e., m_{RR} .

Based on Proposition 3, it can be shown that the threshold $\overline{\text{RI}}_{\text{th}}^{\mathcal{O}}$ given by (16) becomes

$$\overline{\text{RI}}_{\text{th}}^{\mathcal{O}} \simeq \bar{\gamma}_{SR} \left(\frac{I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} + \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \right) \left(\frac{2^{2R_T} - 1}{2^{R_T} - 1} - 1 \right) \quad (18)$$

Note that the result is the same with that for instantaneous residual interference given by (11).

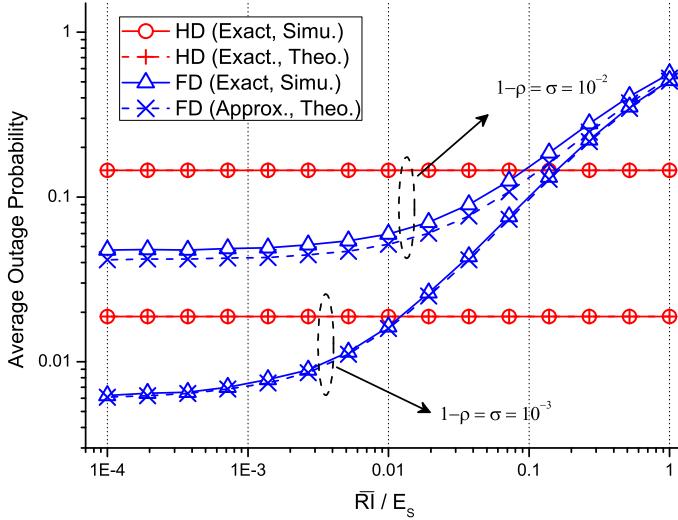


Fig. 2. Outage probability versus \overline{RI}/E_S , where $\rho_{SR} = \rho_{RD} = \rho$, $\sigma_{SR} = \sigma_{RD} = \sigma$, $m_{RR} = 1$, $E_S = E_R = 30\text{dB}$, $\Omega_{SR} = \Omega_{RD} = 1$, $R_T = 1\text{bit/sec/Hz}$.

4 Simulation Results

Fig. 1 shows the region that FDR protocol outperforms HDR protocol in conditional outage probability, where we set $\rho_{SR} = \rho_{RD} = \rho$ and $\sigma_{SR} = \sigma_{RD} = \sigma$. As shown in the figure, for given RI, the FDR outperforms HDR when $1 - \rho$ and σ is large, which corresponding to the scenario where the quality of channel estimates is bad, while the converse is true when the quality of channel estimates is good. Moreover, the region that FDR protocol outperforms HDR protocol decreases as RI increasing and increases as the target rate R_T increasing. This observation coincides with the result obtained by (11). Finally, it is seen that the threshold given by (11) yields region in perfect agreement with the exact region obtained by Monte Carlo simulations.

Fig. 2 depicts the average outage performance of the FDR and HDR protocols as a function of \overline{RI}/E_S , where the exact expression for HDR protocol and approximate expression for FDR protocol are given by (9) and (12), respectively. From the figure, the FDR protocol outperforms the HDR protocol as $\overline{RI}/E_S < 0.015$ and $\overline{RI}/E_S < 0.08$ when $1 - \rho = \sigma = 10^{-3}$ and $1 - \rho = \sigma = 10^{-2}$, respectively. The observation indicates that the condition which ensures the FDR protocol outperforms HDR protocol becomes relaxed as $1 - \rho$ and σ increasing (the quality of channel estimates degrades).

Fig. 3 compares the average outage performances of the FDR and HDR protocols as a function of transmitted power. The exact expression for HDR protocol and approximate expression for FDR protocol are given by (9) and (12), respectively. Again, we can see that the FDR protocol achieves better performance as the quality of channel estimates is bad while the HDR protocol can outperform

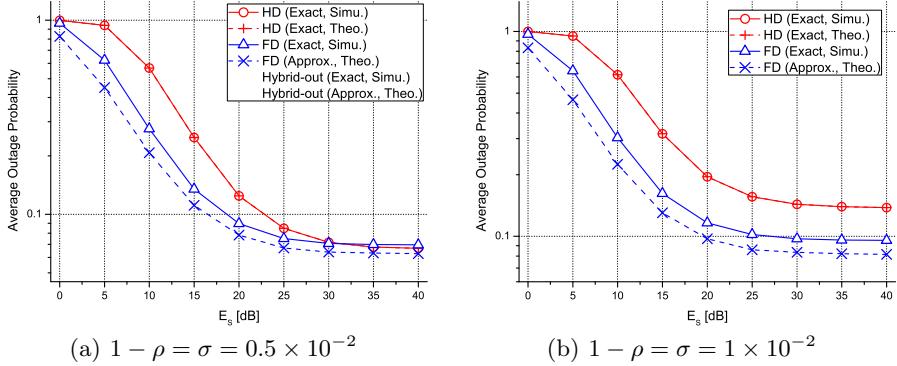


Fig. 3. Average outage probability versus E_S , where $\overline{\text{RI}}/E_S = 3 * 10^{-2}$, $\rho_{SR} = \rho_{RD} = \rho$, $\sigma_{SR} = \sigma_{RD} = \sigma$, $m_{RR} = 1$, $\Omega_{SR} = \Omega_{RD} = 1$, $E_R = 1.5E_S$, $R_T = 1\text{bit/sec/Hz}$

the FDR protocol in the high SNR region as the quality of channel estimates is good. However, we can see that FDR always outperforms HDR in the low-moderate SNR region. This is because we consider the peak constraint for both protocols, i.e., the node is not allowed to double its transmit power in HDR protocol even though it remains silent at the other half of the duration time of one time slot.

5 Conclusion

The effect of channel estimates imperfection on the outage performance for FDR and HDR protocols is investigated in this paper. Our results show that there exists a threshold on the echo interference power at the relay that ensures the FDR protocol outperforms the HDR protocol in outage probability. Furthermore, we show that, for given echo interference power, the FDR protocol achieves the better performance when the quality of channel estimates is bad, while the converse is true when the quality of channel estimates is good.

Appendix

Proof of (11)

The FDR protocol outperforms the HDR protocol in conditional outage probability when $\mathcal{P}_{\mathcal{O}}^{\text{FDR}}(R_T, \text{RI}) < \mathcal{P}_{\mathcal{O}}^{\text{HDR}}(R_T, \text{RI})$, or equivalently,

$$1 - \mathcal{P}_{\mathcal{O}}^{\text{FDR}}(R_T, \text{RI}) > 1 - \mathcal{P}_{\mathcal{O}}^{\text{HDR}}(R_T, \text{RI}) \quad (19)$$

When E_S and E_R are large, we have the following approximation [20, 8.446]

$$K_1(z) \simeq \frac{1}{z} \quad (20)$$

Inserting (20) into (9) and substituting the resultant expression into (19), we can obtain

$$\begin{aligned} & \exp \left(-\frac{\text{RI} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \gamma_T^{\text{FDR}} - \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \gamma_T^{\text{FDR}} \right) \\ & > \exp \left(-\frac{I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \gamma_T^{\text{HDR}} - \frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \gamma_T^{\text{HDR}} \right) \end{aligned} \quad (21)$$

At last, following by some algebraic manipulations, one can arrived at the result in Proposition 2.

Proof of Proposition 2

Inserting the approximation $K_1(z) \simeq \frac{1}{z}$ (when E_S and E_R are large) into (9), the conditional outage probability reduces to

$$\mathcal{P}_O^\psi(R_T, \text{RI}) \simeq 1 - \exp \left(-\frac{I_{RD}^f + I_{RD}^e + 1}{\bar{\gamma}_{RD}} \gamma_T^\psi \right) \exp \left(-\frac{\delta \text{RI} + I_{SR}^f + I_{SR}^e + 1}{\bar{\gamma}_{SR}} \gamma_T^\psi \right) \quad (22)$$

Averaging (22) with respective to the probability density function (PDF) of RI, which can be expressed as

$$f_{\text{RI}}(x) = \left(\frac{m_{RR}}{\overline{\text{RI}}} \right)^{m_{RR}} \frac{x^{m_{RR}-1}}{\Gamma(m_{RR})} \exp \left(-\frac{m_{RR}}{\overline{\text{RI}}} x \right) \quad (23)$$

and using [20, 3.381.4] on the resultant expression, one can obtain the result in (11).

References

1. Laneman, J.N., Tse, D.N.C., Wornell, G.W.: Cooperative diversity in wireless networks: efficient protocols and outage behavior. *IEEE Trans. Inf. Theory* 50, 3062–3080 (2004)
2. Azarian, K., Gamal, H.E., Schniter, P.: On the achievable diversity multiplexing tradeoff in half-duplex cooperative channels. *IEEE Trans. Inf. Theory* 51, 4152–4172 (2005)
3. Ding, Z., Krikidis, I., Rong, B., Thompson, J.S., Wang, C., Yang, S.: On combating the half-duplex constraint in modern cooperative networks: protocols and techniques. *IEEE Wireless Commun. Mag.* 19, 20–27 (2012)
4. Xu, Y., Xia, X., Xu, K., Zhang, D.: On the hybrid relaying protocol for time division broadcasting. To appear in *Trans. Emerging Telecommun. Tech* (2013)
5. Xia, X., Xu, Y., Xu, K., Zhang, D., Li, N.: Outage performance of AF-based time division broadcasting protocol in the presence of co-channel interference. In: *IEEE WCNC 2013*, Shanghai, China (April 2013)
6. Xu, Y., Xia, X., Xu, K., Chen, Y.: symbol error rate of two-way decode-and-forward relaying with co-channel interference. In: *IEEE PIMRC 2013*, London, Britain (September 2013)

7. Kim, S.J., Devroye, N., Mitran, P., Tarokh, V.: Achievable Rate Regions and Performance Comparison of Half Duplex Protocols. *IEEE Trans. Inf. Theory* 57(10), 6405–6418 (2011)
8. Riihonen, T., Werner, S., Wichman, R.: Optimized gain control for single-frequency relaying with loop interference. *IEEE Trans. Wireless Commun.* 8, 2801–2806 (2009)
9. Riihonen, T., Werner, S., Wichman, R.: Mitigation of loopback self interference in full-duplex MIMO relays. *IEEE Trans. Signal Process.* 59, 5983–5993 (2011)
10. Bharadia, D., McMilin, E., Katti, S.: Full duplex radios. In: ACM Sigcomm 2013, Hong Kong, China (August 2013)
11. Chun, B., Jeong, E., Joung, J., Oh, Y., Lee, Y.: Pre-nulling for self-interference suppression in full-duplex relays. In: APSIPA Ann. Summit and Conf., Sapporo, Japan (October 2009)
12. Krikidis, I., Suraweera, H.A., Smith, P.J.: Full-duplex relay selection for amplify-and-forward cooperative networks. *IEEE Trans. Wireless Commun.* 11, 4381–4393 (2012)
13. Khafagy, M., Ismail, A., Alouini, M., Aïssa, S.: On the outage performance of full-duplex selective decode-and-forward relaying. *IEEE Commun. Lett.* 17, 1180–1183 (2013)
14. Krikidis, I., Suraweera, H.A., Yang, S., Berberidis, K.: Full-duplex relaying over block fading channel: a diversity perspective. *IEEE Trans. Wireless Commun.* 11, 4524–4535 (2012)
15. Xia, X., Xu, K., Ma, W., Xu, Y.: On the design of relay selection strategy for two-way amplify-and-forward mobile relaying. To appear in *IET Commun.* (2013)
16. Yang, L., Qaraqe, K., Serpedin, E., Louini, M.: Performance analysis of amplify-and-forward two-way relaying with co-channel interference and channel estimation error. To Appear in *IEEE Trans. Commun.* (2013)
17. Han, S., Ahn, S., Oh, E., Hong, D.: Effect of channel estimation error on BER performance in cooperative transmission. *IEEE Trans. Veh. Technol.* 58, 2083–2088 (2009)
18. Yoo, T., Goldsmith, A.: Capacity and power allocation for fading MIMO channels with channel estimation error. *IEEE Trans. Inf. Theory* 52, 2203–2214 (2006)
19. Cheng, W., Zhang, X., Zhang, H.: QoS driven power allocation over full-duplex wireless links. In: IEEE ICC 2012, Ottawa, Canada (June 2012)
20. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series and Products, 7th edn. Academic Press (2007)
21. Louie, R., Li, Y., Vucetic, B.: Practical physical layer network coding for two-way relay channels: performance analysis and comparison. *IEEE Trans. Wireless Commun.* 9(2), 764–777 (2010)
22. Wang, Z., Giannakis, G.B.: A simple and general parameterization quantifying performance in fading channels. *IEEE Trans. Commun.* 51(8), 1389–1398 (2003)

Identifying Missing and Spurious Interactions in Directed Networks

Xue Zhang¹, Chengli Zhao^{1,*}, Xiaojie Wang¹, and Dongyun Yi^{1,2}

¹ School of Science, National University of Defense Technology,
Changsha, 410073, China

² State Key Laboratory of High Performance Computing,
National University of Defense Technology, Changsha, 410073, China
chenglizhao@gmail.com

Abstract. Recent years, the studies of link prediction have been overwhelmingly emphasizing on undirected networks. Compared with it, how to identify missing and spurious interactions in directed networks has received less attention and still is not well understood. In this paper, we make use of classical link prediction indices for undirected networks, adapt them to directed version which could predict both the existence and direction of an arc between two nodes, and investigate their prediction ability on six real-world directed networks. Experimental results demonstrate that those modified indices perform quite well in directed networks. Compared with Bi-fan predictor, some of them can provide more accurate predictions.

Keywords: link prediction, directed network, local similarity, block model, Bi-fan predictor.

1 Introduction

Network is an effective and efficient tool to describe real-world complex systems[1], such as social, biological, traffic and information systems, where nodes represent individuals, proteins, airports, web pages etc, and links denote the relations and interactions between them. The study of complex networks is an important growing field that attracts lots of attention from different branches of science. While making great efforts to understand the structural features and evolutionary mechanism of networks, scientists gradually realize that the inaccuracy and incompleteness of data sets is a significant obstacle to the research[2, 3]. To address this issue, link prediction algorithms have been adopted to extract the missing information, identify spurious interactions, reconstruct network, and so forth.

The problem of link prediction aims at estimating the likelihood of the existence of a link between two nodes in a given network based on the observed links[4], and it has a wide range of applications in the real world. For example, in online social networks, very likely but not-yet-existent links can be recommended as promising friendship, which can help users in finding new friends; in biological

* Corresponding author.

networks, compared to blindly checking all possible protein-protein interactions, accurate prediction of the most likely existent ones can dramatically reduce the experimental cost; in e-commerce, with the help of recommendation systems, sellers enhance their sales by watching customers' purchases and recommending them other goods in which they may be interested[5]; in security domain, link prediction methods could be used to assist identifying groups of terrorist or criminals[6].

Since the link prediction problem is relevant for various domains, lots of algorithms have been proposed to solve it. The most widely used link prediction indices are the local similarity measures [7–11] e.g., Common Neighbors, Jaccard index, Adamic-Adar index and Resource Allocation index etc, which only require consideration of the local structure of the networks. They are favored for low complexity, low time consumption and relatively high accuracy especially when the network is highly clustered[12].

Algorithm based on statistical inference is another branch in the study of link prediction, in which some organizing principles of the network structure, like hierarchical organizations or community structures, are often presupposed[6, 13, 14]. Using Bayes' theorem, people can infer the underlying structure from observed network and take advantage of the knowledge to reliably identify both missing and spurious interactions. Usually, the performance of this type of method is more accurate and robust, but it has an obvious drawback—the high computational complexity makes it infeasible for large-scale networks.

All the algorithms mentioned above are designed for undirected networks. However, in the real world asymmetric interactions are widespread such as world wide web, food web, neural network, email network, and citation network etc. Unfortunately, there has been little research focusing on how to identify missing and spurious interactions in directed networks. Until very recently, a new mechanism for the local organization of directed networks—potential theory has been proposed[15]. Combining the potential theory with the clustering and homophily mechanisms, Bi-fan structure which consists of 4 nodes and 4 directed links is deduced to be the most favored local structure and could be used directly as a well-performed missing link predictor in directed networks.

In this paper, we focus on the link prediction problem in directed networks. Our contribution is twofold: 1) Instead of proposing a brand-new directed link predictor, we make the best of classical prediction indices of undirected networks. We extend the most representative measures to directed version, to meet the requirement of predicting both the existence and direction of an arc between two nodes. 2) To investigate the performance of these modified indices, we design simulation experiments on six real biological and technological directed networks, the results of which vividly demonstrate their prediction ability.

The reminder of the paper is organized as follows. In section 2, we describe the link prediction problem in directed networks and the standard metric for performance evaluation. Then, we present how the adapted indices work in asymmetric networks and access their prediction ability in section 3 and 4. Finally, the conclusion is drawn in section 5.

2 Problem Description and Evaluation Metric

Given a directed network $G(V, E)$, where V and E are sets of nodes and directed links respectively. Multiple links and self-connections are not allowed. The fundamental task of a link prediction algorithm is to give a rank of all non-observed links in the set $U \setminus E$, where U is the universal set containing all $|V|(|V| - 1)$ possible directed links. The mainstream method is to assign each non-observed link a score, and the one with higher score ranks ahead. The top ranked links are regarded as the most likely missing (or future) interactions.

To evaluate the algorithmic performance, the observed links E is divide into two parts: the training set E^T is treated as known information, while the probe set E^P is used for testing and no information therein is allowed to be used for prediction. Clearly, $E = E^T \cup E^P$ and $E^T \cap E^P = \emptyset$.

We adopt metric AUC[16] (area under the receiver operating characteristic curve) to quantify the prediction accuracy. It evaluates the predictor performance according to the whole list and can be interpreted as the probability that a randomly chosen missing link (i.e., a link in E^P) is given a higher score than a randomly chosen nonexistent link (i.e., a link in $U \setminus E$). Among n independent comparisons, if there are n' times the missing link having a higher score and n'' times they are the same, the AUC value is

$$AUC = \frac{n' + 0.5n''}{n}. \quad (1)$$

Similarly, the link prediction algorithm can also be used to identify spurious interactions. In this case, the task is changed to score all the observed links in E , and rank them in an ascending order, then the top ranked links are suspected as the most likely spurious interactions. To test the algorithmic performance, $E^{T'} = E \cup E^{P'}$ is treated as the “hypothetical observed” links, where $E^{P'}$ is made up of some randomly selected nonexistent links from $U \setminus E$. Now the AUC represents the probability that a randomly chosen spurious link (i.e., a link in $E^{P'}$) is given a lower score than a randomly chosen real link (i.e., a link in E).

In a word, for both predicting missing links and identifying spurious links cases, the higher the AUC value, the better the prediction algorithm works.

3 Directed Link Predictors

In this section, we first review some classical prediction indices for undirected network and present how to extend them to directed version. The basic structural measures for a node i is its neighbors $\Gamma(i)$, which could be defined as $\Gamma(i) = \{j | (i, j) \in E \vee (j, i) \in E\}$. In directed networks, taking the link direction into consideration, $\Gamma_{out}(i) = \{y | (i, y) \in E\}$ is regarded as the set of outgoing neighbors, while $\Gamma_{in}(i) = \{j | (j, i) \in E\}$ represents the group of incoming neighbors.

1) Common Neighbors (CN): The common neighbors refers to the nodes that are connected with both i and j . This measure rests on the fact that two nodes

are more likely to be connected if they share more common friends. In undirected networks, this index is defined as

$$S_{ij}^{CN} = |\Gamma(i) \cap \Gamma(j)|. \quad (2)$$

It is obvious that $S_{ij}^{CN} = (\mathbf{A}^2)_{ij}$, where \mathbf{A} is the adjacency matrix. In directed networks, adjacency matrix $\tilde{\mathbf{A}}$ becomes asymmetric,

$$\tilde{A}_{ij} = \begin{cases} 1 & \text{if there is a directed arc } i \rightarrow j, \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

Then $(\tilde{\mathbf{A}}^2)_{ij}$ equals the number of different two-step paths from i to j ; in other words, $(\tilde{\mathbf{A}}^2)_{ij}$ measures how many “transit nodes” in the network that could forward the message got from i to j . Thus the extension of CN index in directed networks could be naturally defined as

$$S_{ij}^{CN^*} = (\tilde{\mathbf{A}}^2)_{ij} = |\Gamma_{out}(i) \cap \Gamma_{in}(j)|. \quad (4)$$

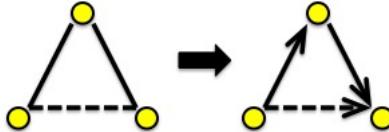


Fig. 1. In undirected networks, CN indices could be interpreted as the number of triadic closure, while in directed networks this index measures the formation of feed-forward structure

2) Preferential Attachment (PA): This is a basic link prediction algorithm corresponding to the preferential attachment phenomena in many real-world networks[17, 18]. The probability that a link will connect i and j is proportional to the number of their neighbors, i.e.,

$$S_{ij}^{PA} = |\Gamma(i)| \times |\Gamma(j)|. \quad (5)$$

Accordingly, in directed networks, the more outgoing neighbors i has and incoming neighbors j attracts, the more likely to build a connection from i to j . So the PA score for an arc $i \rightarrow j$ is given by

$$S_{ij}^{PA^*} = |\Gamma_{out}(i)| \times |\Gamma_{in}(j)|. \quad (6)$$

3) Stochastic Block Model (BM)[13]: Stochastic block model is one of the most general network models, where nodes are partitioned into groups and the probability that two nodes are connected depends only on the groups to which they belong.

In undirected networks, given a block model $M = (P, \mathbf{Q})$, in which P is the partition of nodes into groups and the matrix $\mathbf{Q} = (Q_{\alpha\beta})$ describes the probabilities of the linkage between groups, then the likelihood of the observed network is

$$p(\mathbf{A}|P, \mathbf{Q}) = \prod_{\alpha \leq \beta} Q_{\alpha\beta}^{l_{\alpha\beta}} (1 - Q_{\alpha\beta})^{\gamma_{\alpha\beta} - l_{\alpha\beta}}, \quad (7)$$

where \mathbf{A} is the adjacency matrix, $l_{\alpha\beta}$ is the number of links between nodes in groups α and β , and $\gamma_{\alpha\beta}$ is the maximum number of such links. Using Bayes' Theorem, the reliability of an individual link is

$$\begin{aligned} S_{ij}^{BM} &= p(\mathbf{A}_{ij} = 1 | \mathbf{A}) \\ &= \frac{1}{Z} \sum_{p \in \mathcal{P}} \int_{[0,1]^G} p(\mathbf{A}_{ij} = 1 | P, \mathbf{Q}) p(\mathbf{A}|P, \mathbf{Q}) p(P, \mathbf{Q}) d\mathbf{Q}, \end{aligned} \quad (8)$$

where \mathcal{P} is the space of all partitions, G is the number of distinct group pairs, and Z is a normalizing constant¹.

In directed networks, the interaction between two nodes are no longer reciprocal, which implies that the underlying matrix \mathbf{Q} becomes asymmetric, i.e. $Q_{\alpha\beta}$ determines the probability of nodes in group α linking to the ones in group β , while $Q_{\beta\alpha}$ limits the chance of links from group β to α . $Q_{\alpha\beta}$ and $Q_{\beta\alpha}$ are not necessarily to be the same. In addition, the links of different direction between two groups should be counted separately. Thus, the likelihood of the directed network structure is

$$p^*(\tilde{\mathbf{A}}|P, \mathbf{Q}) = \prod_{\alpha, \beta} Q_{\alpha\beta}^{l_{\alpha\beta}^*} (1 - Q_{\alpha\beta})^{\gamma_{\alpha\beta}^* - l_{\alpha\beta}^*}. \quad (9)$$

Notice that, $l_{\alpha\beta}^*$ now becomes the number of directed arcs from groups α to β , and $\gamma_{\alpha\beta}^*$ is the corresponding maximum number of such links.

$$\gamma_{\alpha\beta}^* = \begin{cases} |\alpha||\alpha - 1| & \alpha = \beta \\ |\alpha||\beta| & \alpha \neq \beta \end{cases} \quad (10)$$

Then by replacing $p(\mathbf{A}|P, \mathbf{Q})$ with $p^*(\tilde{\mathbf{A}}|P, \mathbf{Q})$ in Equation (8), we can easily get the score for the arc $i \rightarrow j$ ²,

$$\begin{aligned} S_{ij}^{BM*} &= p(\tilde{\mathbf{A}}_{ij} = 1 | \tilde{\mathbf{A}}) \\ &= \frac{1}{Z^*} \sum_{p \in \mathcal{P}} \int_{[0,1]^G} p(\tilde{\mathbf{A}}_{ij} = 1 | P, \mathbf{Q}) p^*(\tilde{\mathbf{A}}|P, \mathbf{Q}) p(P, \mathbf{Q}) d\mathbf{Q}. \end{aligned} \quad (11)$$

¹ $Z = \sum_{p \in \mathcal{P}} \int_{[0,1]^G} p(\mathbf{A}|P, \mathbf{Q}) p(P, \mathbf{Q}) d\mathbf{Q}$

² $Z^* = \sum_{p \in \mathcal{P}} \int_{[0,1]^G} p^*(\tilde{\mathbf{A}}|P, \mathbf{Q}) p(P, \mathbf{Q}) d\mathbf{Q}$

Table 1. Some local similarity measures and their corresponding extensions for directed networks

Index	Undirected network	Directed network
Jaccard	$\frac{ \Gamma(i) \cap \Gamma(j) }{ \Gamma(i) \cup \Gamma(j) }$	$\frac{ \Gamma_{out}(i) \cap \Gamma_{in}(j) }{ \Gamma_{out}(i) \cup \Gamma_{in}(j) }$
Hub Promoted	$\frac{ \Gamma(i) \cap \Gamma(j) }{\min\{k(i), k(j)\}}$	$\frac{ \Gamma_{out}(i) \cap \Gamma_{in}(j) }{\min\{k_{out}(i), k_{in}(j)\}}$
Hub Depressed	$\frac{ \Gamma(i) \cap \Gamma(j) }{\max\{k(i), k(j)\}}$	$\frac{ \Gamma_{out}(i) \cap \Gamma_{in}(j) }{\max\{k_{out}(i), k_{in}(j)\}}$
Salton	$\frac{ \Gamma(i) \cap \Gamma(j) }{\sqrt{k(i) \times k(j)}}$	$\frac{ \Gamma_{out}(i) \cap \Gamma_{in}(j) }{\sqrt{k_{out}(i) \times k_{in}(j)}}$
Leicht-Holme-Newman	$\frac{ \Gamma(i) \cap \Gamma(j) }{k(i) \times k(j)}$	$\frac{ \Gamma_{out}(i) \cap \Gamma_{in}(j) }{k_{out}(i) \times k_{in}(j)}$
Sørensen	$\frac{2 \Gamma(i) \cap \Gamma(j) }{k(i) + k(j)}$	$\frac{2 \Gamma_{out}(i) \cap \Gamma_{in}(j) }{k_{out}(i) + k_{in}(j)}$
Adamic-Adar	$\sum_{z \in \Gamma(i) \cap \Gamma(j)} \frac{1}{\log k(z)}$	$\sum_{z \in \Gamma_{out}(i) \cap \Gamma_{in}(j)} \frac{1}{\log k_{out}(z)}$
Resource Allocation	$\sum_{z \in \Gamma(i) \cap \Gamma(j)} \frac{1}{k(z)}$	$\sum_{z \in \Gamma_{out}(i) \cap \Gamma_{in}(j)} \frac{1}{k_{out}(z)}$

Among all the link prediction measures for undirected networks, the above three indices are chosen to be adapted for the following reasons. Firstly, the design philosophies of them are different from each other, and they all have their own advantages. CN index follows the nature intuition and has wide range of applications in practice. PA index reflects the mechanism of rich-get-richer and is superior for its least information requirement, while BM method takes into account network community structures, rests on solid mathematical foundations and returns excellent results. Secondly, those three indices are fairly representative, so their modification methods are enlightening and could be extended to other indices. For example, inspired by the modified CN index, other local similarity measures can also be extended in a similar way. Table 1 illustrates a few common local similarity indices and their corresponding extensions.

To analyze the performance of those modified measures, next we introduce Bi-fan predictor as a comparison index. Bi-fan structure is found to be quite widespread in real world[19] and proven to be a well-performed predictor for directed networks.

4) Bi-fan Predictor[15]: The potential theory is proposed as a microscopic organizing principle for directed networks, which assumes that each directed link corresponds to a decrease of a unit potential and subgraphs with definable

potential values for all nodes are preferred. Combining the clustering and homophily mechanisms with potential theory, it is deduced that Bi-fan subgraph is the most favored local structure in directed networks (see Fig. 2).

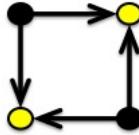


Fig. 2. Bi-fan structure consists of 4 nodes and 4 directed links. All the links are equivalent to each other and nodes are of two different potential—the potentials of two black nodes are a unit higher than that of the yellow ones.

This special structure could be directly used as a link predictor, with the assumption that a link that can generate more Bi-fan subgraphs is more significant and thus of a higher probability to appear. So the Bi-fan index is determined by how many Bi-fan subgraphs that link $i \rightarrow j$ could generate, which can be calculated by

$$S_{ij}^{Bifan^*} = \mathbf{r}_i \left(\sum_s \mathbf{r}_{k_s}^T \right), \quad (12)$$

where $\mathbf{r}_i = (a_{i1}, a_{i2}, \dots, a_{i|V|})$ is the i th row vector of the adjacency matrix $\tilde{\mathbf{A}}$, and \mathbf{r}_{k_s} are the ones that meet the requirement of $a_{k_s j} \neq 0$.

4 Result

4.1 Data Sets

Our experiments are carried out on six real-world directed networks drawn from biological and technological fields. Those networks are pretty representative and often employed in simulation experiments to validate the effectiveness of the proposed scheme. i) FoodWeb1 (FW1)[20]: A network of food web representing the predator-pray relations between 69 species living in Everglades Graminoids during wet season. ii) FoodWeb2 (FW2)[21]: A network of food web consists of 97 species living in Mangrove Estuary during wet season. iii) FoodWeb3 (FW3)[22]: A network of food web consists of 128 species living in Florida Bay during wet season. iv) C. elegans (CE)[23]: The neural network of the nematode worm C. elegans, in which an edge joins two neurons if they are connected by either a synapse or a gap junction. v) Small & Griffith and Descendants (SmaGri)[24]: A citation network to Small & Griffith and Descendants, in which a directed arc from node i to j means i cites j . vi) Political Blogs (PB)[25]: A directed networks of hyperlinks between weblogs on US political blogs.

Table 2. The basic topological features of the six directed networks. $|V|$ and $|E|$ are the number of nodes and links. k_{max}^{in} and k_{max}^{out} are the maximum of in-degree and out-degree of all nodes, $\langle k \rangle$ is the average degree of the network, $\langle d \rangle$ is the average shortest distance between pair nodes, C is the clustering coefficient of the directed networks.

Networks	$ V $	$ E $	k_{max}^{in}	k_{max}^{out}	$\langle k \rangle$	C	$\langle d \rangle$
FW1	69	911	63	44	13.275	0.309	2.168
FW2	97	1492	90	46	15.381	0.261	2.185
FW3	128	2106	110	63	16.453	0.177	2.412
CE	297	2345	134	39	7.896	0.174	3.992
SmaGri	1024	4918	89	232	4.804	0.156	3.242
PB	1222	19021	337	256	15.565	0.219	3.39

For convenience, we eliminate all the loops and multi-edges of the above networks. The basic topological features of these six networks are summarized in Table 2.

4.2 Experimental Results

In this section, we investigate the prediction ability of the indices presented in section 3. Comparisons of algorithms' accuracy are displayed in Fig.3 and Fig.4. Each AUC value is obtained by averaging 100 independent realizations, except for the SmaGri and PB, of which the implementation times is 50.

From Fig.3, we can see that when applied in finding missing links, BM outperforms CN and PA, and works even better than Bi-fan predictor in most networks. The advantage of BM to others is usually remarkable except for network Political Blogs, in which the performance of BM, Bi-fan and PA nearly keep pace with each other. This outcome demonstrates that community structure also plays an important role in directed networks. Compared with other three measures utilizing only the local structure information, BM index which take advantage of the organizing principles of the whole network could get more accurate prediction results.

It is worth noting that PA index, which is regarded as the worst predictor in undirected networks, surprisingly performs quite well in the experiments. It has the third best overall performance among all the indices, especially for network SmaGri in which its result is more accurate than that of Bi-fan predictor. Hence the relatively good prediction ability together with the least information requirement make PA index more competitive in directed networks.

Fig.3 also shows that the prediction accuracy of all four indices decline with the increases of f , but the rate of decrease are varying. Compared with the linear decrease of CN index, the trend of AUC for others is slowly downward until reaches a “turning point”, after which the remaining links in E^T are not enough to infer the underlying structure of network, so the prediction accuracy drops sharply. For example, in all FoodWebs, the prediction accuracy falls dramatically after f reaches 0.75. In network Political Blogs, 0.65 could be regarded as the

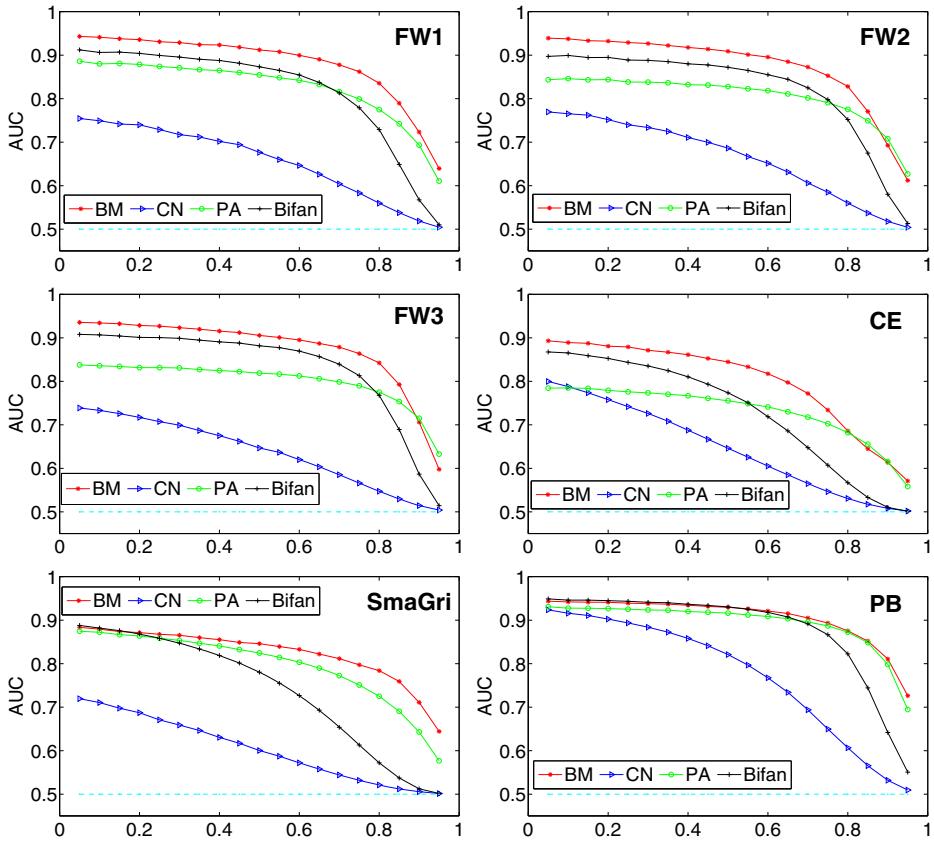


Fig. 3. Prediction results of missing links. The X-axis denotes fraction $f = |E^P|/|E|$, ranging from 0.05 to 0.95 and the interval is set to be 0.05. The cyan dashed line indicates the baseline accuracy when the score of each link is got by pure chance.

“turning point”, before which the AUC values for PA, BM and Bi-fan nearly remain unchanged, but after that the prediction accuracy drops quickly.

As is illustrated in Fig. 4, in identifying spurious interactions, BM and Bi-fan are the two best predictors which are followed by PA, while CN index still has the worst overall performance as before. Note that for each index, different with the results in finding missing links, AUC values in Fig. 4 are relatively high and basically not changed with the increases of f . However, high accuracy is not sufficient for spurious link detection algorithms. If just a few unexpected important links are incorrectly removed, the structural and dynamical properties of the network may change dramatically[26]. So when applied in identifying spurious links, the prediction indices should be evaluated meticulously, however this problem is beyond the scope of this paper.

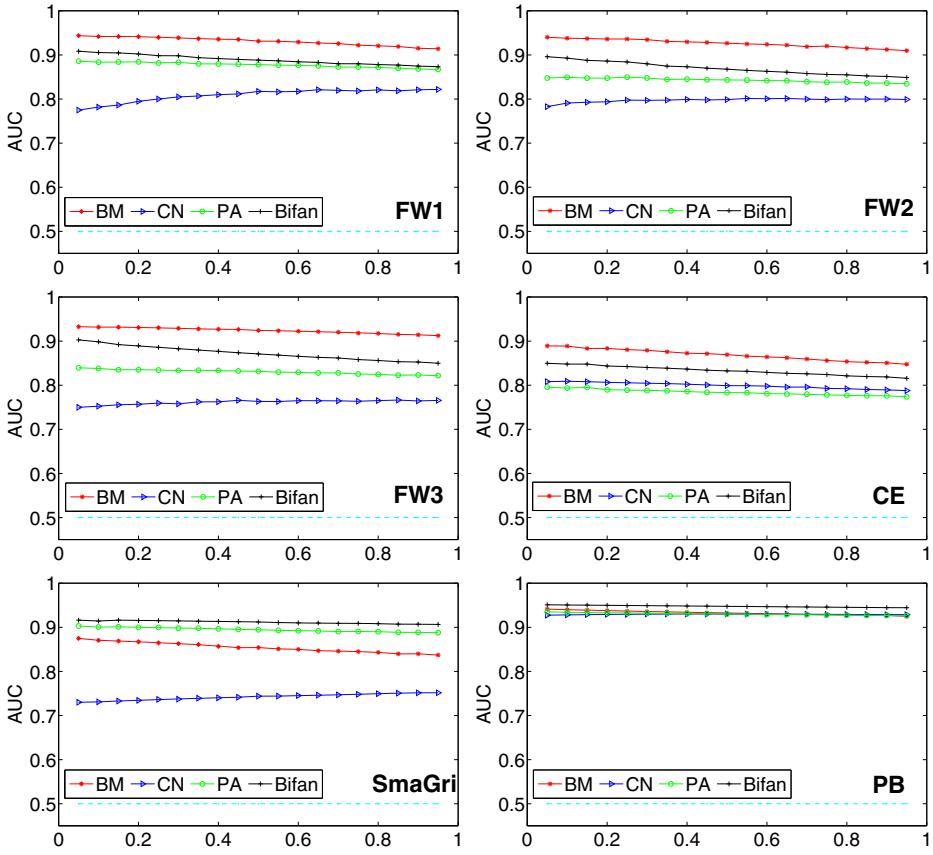


Fig. 4. Prediction results of spurious links. The X-axis stands for fraction $f = |E^{P'}|/|E|$, ranging from 0.05 to 0.95 and the interval is set to be 0.05. The cyan dashed line indicates the baseline accuracy when the score of each link is got by pure chance.

5 Conclusion

This paper studied how to identify both missing and spurious interactions in directed networks. We have showed how to extend classical link prediction indices to directed version, making them able to predict both the existence and direction of an arc between two nodes. Simulation experiments on six real-world directed networks have demonstrated the prediction ability of those modified measures.

The purpose of this paper is not to present a better directed link predictor, but to give an example of how to use the valuable knowledge of undirected networks to solve the problems in directed networks. For directed networks, the direction of links is a double-edged sword. It provides additional valuable information for link prediction, but also leads to greater difficulty—how to determine the direction of the unknown links is a tough problem. The extended CN index made use of the

asymmetric similarity to determine the link direction, while BM benefited from asymmetric likelihood of the linkage between groups. In brief, asymmetry is the key. However, prediction methods based solely on asymmetry is incomplete, and other natures of the directed networks should be taken into consideration. For example, in neural networks and some technological networks, information or resources are often collected by basal nodes, transmitted through directed links and delivered to top nodes eventually. Such kind of macroscopic flow direction may help to determine the unknown link direction.

On the other hand, each prediction index has its own advantages and is suitable for different kind of networks. How to chose the most appropriate algorithm according to the features of the networks is also a question worth studying.

Acknowledgments. The work is supported by Basic Research Project of National University of Defense Technology.

References

- Lin, Y., Duan, X., Zhao, C., Xu, L.: Systems Science: Methodological Approaches. CRC Press, Boca Raton (2013)
- Schafer, J., Graham, J.W.: Missing data: our view of the state of the art. *Psychol. Methods* 7, 147–177 (2002)
- Kossinets, G.: Effects of missing data in social networks. *Soc. Networks* 28, 247–268 (2006)
- Lü, L., Zhou, T.: Link prediction in complex networks: A survey. *Physica A* 390, 1150–1170 (2011)
- Lü, L., Medo, M., Yeung, C.H., Zhang, Y.C., Zhang, Z.K., Zhou, T.: Recommender systems. *Phys. Rep.* 519, 1–49 (2012)
- Clauset, A., Moore, C., Newman, M.E.J.: Hierarchical structure and the prediction of missing links in networks. *Nature* 453, 98–101 (2008)
- Liben-Nowell, D., Kleinberg, J.: The link-prediction problem for social networks. *J. Am. Soc. Inf. Sci. Technol.* 58, 1019–1031 (2007)
- Newman, M.E.J.: Clustering and preferential attachment in growing networks. *Phys. Rev. E* 64, 25102 (2001)
- Jaccard, P.: Étude comparative de la distribution florale dans une portion des Alpes et des Jura. *Bull. Soc. Vaud. Sci. Nat.* 37, 547–579 (1901)
- Adamic, L.A., Adar, E.: Friends and neighbors on the web. *Soc. Networks* 25, 211–230 (2003)
- Zhou, T., Lü, L., Zhang, Y.C.: Predicting missing links via local information. *Eur. Phys. J. B* 71, 623–630 (2009)
- Feng, X., Zhao, J.C., Xu, K.: Link prediction in complex networks: a clustering perspective. *Eur. Phys. J. B* 85, 3 (2012)
- Guimerà, R., Sales-Pardo, M.: Missing and spurious interactions and the reconstruction of complex networks. *Proc. Natl. Acad. Sci. USA* 106, 22073–22078 (2009)
- Zhang, X., Wang, X., Zhao, C., Yi, D., Xie, Z.: Degree-corrected stochastic block-models and reliability in networks. *Physica A* 393, 553–559 (2014)
- Zhang, Q.M., Lü, L., Wang, W.Q., Zhou, T.: Potential theory for directed networks. *PLoS One* 8, e55437 (2013)

16. Hanely, J.A., McNeil, B.J.: The meaning and use of the area under a receiver operating characteristic (ROC) curve. *Radiology* 143, 29–36 (1982)
17. Barabási, A.L., Albert, R.: Emergence of scaling in random networks. *Science* 286, 509–512 (1999)
18. Xie, Y.B., Zhou, T., Wang, B.H.: Scale-free networks without growth. *Physica A* 387, 1683–1688 (2008)
19. Milo, R., Shen-Orr, S., Itzkovitz, S., Kashtan, N., Chklovskii, D., Alon, U.: Network motifs: simple building blocks of complex networks. *Science* 298, 824–827 (2002)
20. Ulanowicz, R.E., Heymans, J.J., Egnatovich, M.S.: Network Analysis of Trophic Dynamics in South Florida Ecosystems, FY 99: The Graminoid Ecosystem. Technical report TS-191-99 (2000)
21. Baird, D., Luczkovich, J., Christian, R.R.: Assessment of Spatial and Temporal Variability in Ecosystem Attributes of the St Marks National Wildlife Refuge, Apalachee Bay, Florida. *Estuarine, Coastal, Shelf Sci.* 47, 329–349 (1998)
22. Ulanowicz, R.E., Bondavalli, C., Egnatovich, M.S.: Network Analysis of Trophic Dynamics in South Florida Ecosystem, FY 97: The Florida Bay Ecosystem. Technical report CBL 98-123 (1998)
23. White, J.G., Southgate, E., Thomson, J.N., Brenner, S.: The structure of the nervous system of the nematode *C. elegans*. *Philos. Trans. R. Soc. Lond. Ser. B* 314, 1–340 (1986)
24. Batageli, V., Mrvar, A.: Pajek datasets website (2006),
<http://vlado.fmf.uni-lj.si/pub/networks/data/>
25. Ackland, R.: (2005), <http://inccsub.org/blogtalk/images/robertackland.pdf>
26. Zeng, A., Cimini, G.: Removing spurious interactions in complex networks. *Phys. Rev. E* 85, 036101 (2012)

Online Auction Based Relay Selection for Cooperative Communications in CR Networks

Tao Jing¹, Fan Zhang¹, Wei Cheng², Yan Huo¹, and Xiuzhen Cheng³

¹ School of Electronics and Information Engineering,
Beijing Jiaotong University, China

² Department of Computer Science,
Virginia Commonwealth University, Richmond VA, USA

³ Department of Computer Science,
The George Washington University, Washington DC, USA
*{tjing, 11120188, yhou}@bjtu.edu.cn, wcheng3@vcu.edu,
cheng@gwu.edu}*

Abstract. In this paper, we propose an online auction based relay selection scheme for cooperative communication in CR networks. Specifically, we design an auction scheme through adopting stopping theory. The proposed scheme ensures that the primary user (PU) can effectively select a CR relay to transmit its packets in a given time bound. Extensive simulations demonstrate that the proposed relay selection scheme can always successfully and efficiently select a proper relay for a PU and can achieve a higher cooperative communication throughput comparing with the conventional schemes.

1 Introduction

Cognitive radio technology has been recognized as a solution for improving the spectrum utilization [1] through opportunistically spectrum access without interfering with the primary communications. Cooperative communication is an emerging technology that has the great potential to increase the throughput between two wireless devices [2] without requiring the support of infrastructure. Intuitively, the integration of these two hot technologies is expected to be a solution for the problems of spectrum scarcity and capacity limitation. In this paper, we particularly target on the scenario where the primary CR users (PU) seek to find a suitable CR relay to help transmit data, so that its end-to-end throughput can be increased and its end-to-end delay can be reduced.

Certainly, this hybrid cognitive-cooperative communication architecture is facing both technical and practical challenges. For instances, the relays should get sufficient incentives for participating in the cooperative communications. In addition, if there are multiple candidate relays, it may be impossible/impractical for the primary user to collect information from all the candidate relays to make a decision of relay selection. The reasons are twofold: (i) The time for collecting information from all the candidate relays may exceed the PU's end-to-end delay tolerance; (ii) The availability of candidate relays may changed during the collecting time as CR links are generally not stable. Therefore, an idea cognitive-cooperative scheme should be able to sufficiently incentive the CR users and select a proper relay in a given time.

To design such a scheme, we conservatively consider to collect a candidate relay information and make the relay selection decision for this candidate relay online so that the collected information is valid and end-to-end delay requirement can be satisfied. In other words, the candidate relays send their information (including its sealed bid for cooperative transmissions) to the PU one by one. After receiving the information from a candidate relay, the PU immediately decides whether to choose this relay for cooperative transmission. Once a relay has been selected, the PU stops considering the rest of the candidate relays and pays the chosen relay a compensation based on its bid. In the paper, we consider the candidate relays as bidders and the PU as a buyer, respectively.

Specifically, we design an online auction based relay selection scheme for cooperative CR communication. The main contributions of this paper are summarized below:

1. we formulate the online relay selection problem as an optimal stopping problem and design an optimal stopping policy, which can guarantee the success of relay selection in a given time while controls the cost of PU for utilizing cooperative communication. To the best of our knowledge, This is the first work to jointly adopt stopping theory and design auction scheme for relay selection in CR networks.
2. We analytically prove the truthfulness of the proposed online auction scheme without requiring any information about bidders behavior. Our proposed online auction scheme is also individual rational. Due to the page limit, we will report our proof in our technical report.
3. Extensive experiments are conducted to study the performance of our online auction scheme. We investigate the impact of several parameters and compare our scheme with the **Optimal Relay Selection (ORS)** scheme, which will look at all the candidate relays for minimizing the PU cost. The results demonstrate that the PU can always select an appropriate relay in the given time and our scheme achieves a higher throughput than ORS with a tiny cost increase.

The rest of the paper is organized as follows. The related work is presented in Section 2. The preliminary knowledge is illustrated in Section 3. In Section 4, we describe the proposed stopping policy and the online auction scheme for cooperative communications. The simulation results are reported and analyzed in Section 5. We conclude our paper in Section 6.

2 Related Work

In this section, we briefly review the most related works to our research in the area of auction based cooperative communications.

In [3], Huang *et al.* treated relay nodes as sellers and source nodes as buyers. Two auction mechanisms have been proposed: the SNR auction and the power auction. In each auction mechanism, each user iteratively updates its bid according to the others' previous bids to maximize its own profit. The existence and the uniqueness of the Nash Equilibrium in a single-relay network has been proven. In networks with multiple relays, the Nash Equilibrium only exists under certain conditions. Zhang *et al.* considered the network scenario where there is a single relay and multiple user nodes in [4].

The authors formulated this problem as a sellers' market competition. A distributed algorithm has been developed to search the Nash Equilibrium. In [5], Wang *et al.* studied the situation of one source node and multiple relay nodes. The authors modeled it as a Stackelberg game which is divided into two levels of hierarchy. The benefits of the source node and relay nodes were jointly considered. In [6], the authors formed a Co-operative Cognitive Radio Network (CCRN) where each primary user (PU) employs a set of appropriate second users (SUs) for relaying the PUs information in an energy-efficiency solution. The relay selection and the parameter optimization had been formulated as two Stackelberg games. Unique Nash equilibrium is achieved and proved for each game. In [7], authors assumed that SUs can make rational choice between co-operation and band leasing. This CCRN model were modeled as a Stackelberg game and analyzed. In [8], the impact of spectrum leasing was studied based on a game-theoretic analysis. The authors first illustrated the significance of the problem with a two-secondary-user game. Subsequently, a n-secondary-user game was studied and analyzed given the occupancy model of primary users. However, none of the above work had considered the truthfulness. As a result, these mechanisms are vulnerable to market manipulation and may produce poor outcome [9].

In [10], the authors considered the problem of cooperative spectrum sensing scheduling in a CR network. The author assumeed that each SU has the freedom to decide whether or not to participate in the cooperative spectrum sensing; If not, the SU can wiretap the decision on channel status made by other SUs. This mechanism strives the balance between conserve the energy for spectrum sensing and brings down the spectrum sensing performance. In [11], Yang *et al.* designed an optimal relay assignment algorithm for cooperative communication. Ref. [12] designed a double auction mechanism for cooperative communication. These two works satisfied the truthfulness requirements. They both need to collect the information from all the source nodes and all the relay nodes, and their the auction mechanisms are performed in a single-round fashion. As a comparison, our approach does not require the information from all relay nodes and the auction is performed in an online manner.

3 Preliminary

In this section, we present our system model and depict the two common economic properties (Truthfulness and Individual Rationality) of an auction.

3.1 System Model

In this paper, we consider a time-slotted system consisted by a pair of primary transmitter (PU) and receiver and a number of R candidate relays. The PU needs to send out a packet within T time slots, and it values the packet by β . The time needed for collecting information from each relay is α time slots. Then, the PU can check at most $M = \lfloor T/\alpha \rfloor$ relays within T . The PU randomly collects information from the R candidate relays one by one. The i th candidate relay X_i has a private true valuation v_i and a bid price b_i for forwarding the packet. When the PU collects the information from X_i , X_i returns its bid b_i . Note that, the bid b_i is valid for α time slots, and each candidate relay bids in a sealed-bid manner. After receiving b_i from X_i , the PU needs to

Table 1. Notations

Notations	Definition
R	Number of candidate relays
T	The delay tolerance for the PU
β	The value of a packet
α	The time needed for checking each relay
M	The maximal number of relays that can be checked within T
X_i	The i th candidate relay
b_i	The bid of X_i
v_i	The private true valuation of X_i
Y_n	Real-valued reward function for checking X_n
$V_n^{(M)}$	Maximum reward at stage n
$E(V_{n+1}^{(M)})$	Maximum expected reward at stage $n + 1$
Z_{M-n}	A equal representation of $E(V_{M-n+1}^{(M)})$

immediately make a decision on whether to select X_i as the relay to transit the packet or continue to check X_{i+1} . Table 1 summarizes the notations used through this paper.

3.2 Economic Properties

Truthfulness. An auction is truthful if revealing the private true value is the dominate strategy for each bidder. This means that no bidder can raise its utility by bidding $b_i \neq v_i$, no matter how others bids. This property can resist market manipulation and ensure the auction fairness and efficiency. In untruthful auctions, a selfish bidder can alter its bid to obtain extra outcome which will benefit itself but hurt the others.

Individual Rationality. An auction is individual rational if a winner (the selected relay) is always paid by no less than its bid and the PU's cost is no more than the value of the packet. This property can ensure that the utility of both the PU and the selected relay are no less than 0. In other words, both the PU and the selected relay have sufficient incentive to participate in cooperative communications.

4 Online Auction Scheme for Relay Selection

In this section, we formulate the relay selection process as an optimal stopping problem and present our proposed scheme in detail.

4.1 Problem Formulation

In the following, we first give a brief introduction of the finite stopping problems, then formulate the relay selection process accordingly.

Definition 1. Finite stopping problems: *Given a sequence of random variables, X_1, X_2, \dots, X_M , and a sequence of real-valued reward functions, $y_0(), y_1(X_1),$*

$y_2(x_1, X_2), \dots, y_M(x_1, x_2, \dots, X_M)$, the objective is to find a n , so that the reward function $y_n(x_1, x_2, \dots, X_n)$ is the maximal. Note that the joint distribution of the random variables and the reward functions are known, and that X denotes the random variable and x denote the value of a random variable, respectively.

In order to maximize the PU's utility, the PU makes each decision by comparing the instantaneous reward of selecting X_i with the expected reward of checking X_{i+1} . Accordingly, we formulate the relay selection process as a sequence of decision problem which is defined based on the theory of optimal stopping [13] below.

According to [14], the PU knows (or can learn) the distribution of the bidding price of the bidders (candidate relays). We assume that there is no collusion among the candidate relays and the bidding price of the candidate relays is independently distributed. In this paper, we particularly assume the bidding price follows the normal distribution with the

mean value μ and the standard deviation σ , i.e. $f(b_i) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(b_i - \mu)^2}{2\sigma^2}}$, where $f(b_i)$ is the probability density function of b_i . Note that, our proposed scheme can be generally applied to any bidding price distribution.

We partition the bidding price range into J intervals so that the price is within a finite-state space. We use S to represent the finite-state space of the the bidding price.

$$S = \{s_1 = 0, s_2, s_3, \dots, s_J = \beta, s_{J+1} = +\infty\}.$$

If the bidding price $b_i \in [s_j, s_{j+1})$, we say that b_i is in state s_j . The probability that b_i is in state s_j ($j = 1, 2, \dots, J$) is :

$$p_j = \int_{s_j}^{s_{j+1}} f(b_i) db_i = \int_{s_j}^{s_{j+1}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(b_i - \mu)^2}{2\sigma^2}} db_i. \quad (1)$$

We use X_n to denote the bidding price of the n th checked candidate relay. As a result, the probability that X_n bid for s_j is:

$$P(X_n = s_j) = p_j, 1 \leq j \leq J, 1 \leq n \leq M. \quad (2)$$

Note that, in order to ensure that the PU's cost is no larger than β , we set $s_J = \beta$ and $s_{J+1} = \infty$.

Considering the fact that the time consumed for checking candidate relays are also valuable to the PU (because the PU can use them to transmit other packets, and the PU has a time limit to transmit a packet), checking more candidate relays should result in less PU's utility. Therefore, we use a decreasing function $f(n) = C^{\frac{n-\alpha}{T}}$ to represent the time's impact, where $C \in (0, 1]$. Accordingly, the PU's real-valued reward function for checking the n th candidate relay is :

$$\begin{aligned} Y_n &= y_n(X_1, X_2, \dots, X_n) = (\beta - X_n) \cdot f(n) \\ &= (\beta - X_n) \cdot C^{\frac{n-\alpha}{T}} \\ &\text{for } 1 \leq n \leq M, C \in (0, 1]. \end{aligned} \quad (3)$$

According to [13], a necessary condition for the existence of optimal stopping rules to solve the problem is that Y_n should satisfy the following two requirements:

$$E\{\sup_n Y_n\} < +\infty. \quad (4)$$

$$\limsup_{n \rightarrow +\infty} Y_n \leq Y_{+\infty}. \quad (5)$$

We have proven that the Y_n defined in (3) satisfies the requirements. Due to the page limit, we will report the proof in our technical report.

4.2 Online Auction Based Selection Scheme

We use $V_n^{(M)}(x_1, x_2, \dots, x_n)$ to represent the maximum reward that could be obtained after checking n candidate relays:

$$\begin{aligned} V_n^{(M)}(x_1, x_2, \dots, x_n) = & \max\{y_n(x_1, x_2, \dots, x_n), \\ & E(V_{n+1}^{(M)}(x_1, x_2, \dots, x_n, X_{n+1}) \\ & | X_1 = x_1, X_2 = x_2, \dots, X_n = x_n)\}. \end{aligned} \quad (6)$$

In the above equation, $y_n(x_1, x_2, \dots, x_n)$ means the instantaneous reward if we stop at stage n , $E(V_{n+1}^{(M)}(x_1, x_2, \dots, x_n, X_{n+1}) | X_1 = x_1, X_2 = x_2, \dots, X_n = x_n)$ represents the expected maximum reward by proceeding to stage $n + 1$. Thus, it is better for the PU to stop checking the next candidate relay when the instantaneous reward is larger than the expected maximum reward. Accordingly, the stopping rule is defined as:

$$\begin{aligned} \text{If: } y_n(x_1, x_2, \dots, x_n) \geq & E(V_{n+1}^{(M)}(x_1, x_2, \dots, x_n, X_{n+1}) \\ & | X_1 = x_1, X_2 = x_2, \dots, X_n = x_n), \end{aligned} \quad (7)$$

The PU stops at stage n (selects the n th candidate relay), otherwise, it continues to check the next candidate relay.

We use the method of backward induction to solve the finite stopping problem under the above stopping rule. Since the PU has to stop at stage M , we first calculate the optimal stopping rule at stage $M - 1$, then conclude the optimal rule at stage $M - 2$, and so on until we get the optimal rule at stage 1. We use Z_{M-n} to represent the maximum expected reward at the $n + 1$ stage, i.e. $Z_{M-n} = E(V_{n+1}^{(M)})$. We define that: $Z_0 = -\infty$. As the bidding price of each candidate relay is independent and identically distributed, the value of the Z_u , $u = M - n$, only depends on the remaining number of steps u . Therefore the valuation of Z_u can be calculated as follows:

$$\begin{aligned} Z_1 &= E\{V_M^{(M)}\} = E\{(\beta - X_M) \cdot C^{\frac{M-\alpha}{T}}\} \\ &= C^{\frac{M-\alpha}{T}} \cdot (\beta - E(X_M)) \\ &= C^{\frac{M-\alpha}{T}} \cdot \beta - C^{\frac{M-\alpha}{T}} \cdot \sum_{j=1}^J s_j \cdot p_j. \end{aligned} \quad (8)$$

When $u \geq 1$, we can get:

$$\begin{aligned} Z_{u+1} &= Emax\{Y_{M-u}, Z_u\} \\ &= \sum_m C^{\frac{(M-u)\cdot\alpha}{T}} \cdot (\beta - s_m) \cdot p_m + \sum_n Z_u \cdot p_n, \end{aligned} \quad (9)$$

where the value of m and n need to satisfy the following condition:

$$\begin{aligned} m &\in \{j \mid C^{\frac{(M-u)\cdot\alpha}{T}} \cdot (\beta - s_j) \geq Z_u, j = 1, 2, \dots, J\}, \\ n &\in \{j \mid C^{\frac{(M-u)\cdot\alpha}{T}} \cdot (\beta - s_j) < Z_u, j = 1, 2, \dots, J\}, \\ m + n &= J. \end{aligned} \quad (10)$$

Once a relay has been selected, the PU needs to calculate its payment to the selected relay. In order to frustrate the selfish candidate relays who bid untruthful, the payment that paid to the winner should be bid-independent. As Z_u is a static-value for each $u \in [1, M]$, we can have the highest bidding price for the checked candidate relay to win at each step. Specifically, at step n , if $y_n(x_1, x_2, \dots, x_n) \geq Z_{M-n+1}$, the winner gets payment p_n , which is calculated as follows:

$$\text{As: } y_n(x_1, x_2, \dots, x_n) = (\beta - p_n) \cdot C^{\frac{n\cdot\alpha}{T}} = Z_{M-n}, \quad (11)$$

$$\text{So: } p_n = \beta - \frac{Z_{M-n}}{C^{\frac{n\cdot\alpha}{T}}}. \quad (12)$$

Algorithm 4.2: Online Auction for Relay Selection

- 1: Start checking from X_1 ;
- 2: **for** $n = 1$ to $M - 1$ **do**
- 3: Compute the reward function y_n and the maximum expected reward Z_{M-n} according to Eq. (3) and Eq. (9), respectively.
- 4: **if** $y_n \geq Z_{M-n}$ **then**
- 5: Choose relay X_n for cooperative communication;
- 6: Calculate payment p_n according to Eq. (12);
- 7: Break;
- 8: **else**
- 9: Continue to check the next candidate relay X_{n+1} .
- 10: **end if**
- 11: **end for**
- 12: Select the relay X_M for cooperative communications and reward it with b_M .

The proposed scheme is described in Algorithm 4.2. When the PU needs to send a packet in a given time, it first calculate M . After checking the n th candidate relay, the PU computes y_n and the expected reward Z_{M-n} . According to the comparison of y_n and Z_{M-n} , the PU makes a decision whether to select X_n for cooperative communication immediately. If the PU does not chose any of the first $M - 1$ candidate relay, it has to select the last candidate relay. Under this worst case, the PU needs to pay b_M . Note

that, the decreasing function $f(n)$ can prevent the happening of the worst case, which has been verified by the simulations. We justify that our proposed online auction base relay selection scheme is both truthful and individual rational. Due to the page limit, the detailed proof will be given in our technical report.

5 Simulations

In this section, we conduct simulations to examine the performance of our proposed online auction mechanism. We assume that the bidding price of each candidate relay follows the normally distribution with the expected value $\mu = 0.5$ and the variance $\sigma = 0.2$. We partition the bidding price into $J = 20$ intervals. We set the time limit for the PU to select a relay is 90 time slots, i.e. $T = 90$. In the following, we study the impact of the parameters such as α and C on the number of observation steps and the reward of the PU, respectively. In order to justify the effectiveness of our scheme, we compare ours with the **Optimal Relay Selection(ORS)** scheme, which has the knowledge of who is the optimal relay that has the maximal PU reward among the M candidate relays. In the ORS scheme, the PU stops after checking the optimal relay. The simulations are conducted under several network scales. Particularly, the M takes the value of 20, 30 and 40, separately. Each reported result is the average of 100 independent instances.

5.1 The Impact of Observation Duration α

In this subsection we set the time efficiency parameter $C = 0.3$. The private value of the packet $\beta = 0.9$. Fig. 1 illustrates the relationship between the number of observation steps and the observation duration α under different network scales. From Fig. 1, we observe that the PU generally stops checking within 6 steps in our scheme. When α changes from 2 to 2.2, there is an obvious decline on the number of observation steps in our scheme. Generally speaking, a larger α results in a smaller observation steps. This is because the cost of checking a candidate relay is large when α is big. Thus, the PU

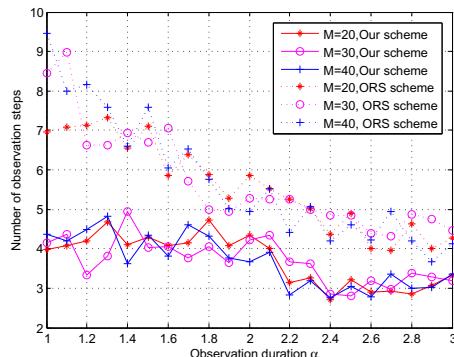


Fig. 1. Average number of observation steps α

intends to find a proper relay as soon as possible. On the other hand, when α is small, the PU may attempt to check more candidate relays to maximize its reward. We also find that the observation steps is always less than M , which indicates that the worst case of choosing the M th relay will not happen. In addition, we can see that the observation steps of ORS is always higher than the corresponding one of ours. It means that our scheme need less time for selecting a cooperative relay.

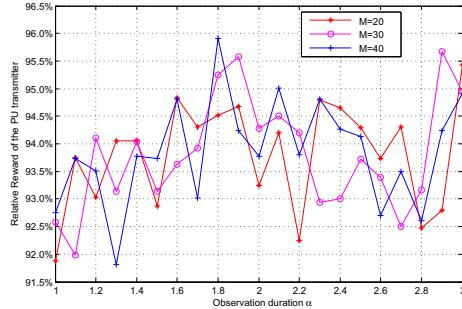


Fig. 2. Relative reward for one packet transmission α

In Fig. 2, we compare our scheme with ORS in terms of reward. Specifically, the reward of our scheme is normalized by the corresponding one of ORS, and we name this ratio as relative monetary reward. Fig. 2 shows the relationship between the relative monetary reward of the PU and the observation duration. According to the results, we find that the relative reward of the PU fluctuates with the checking duration α , but with a small variance (within 4%), and that the relative monetary reward is always higher than 91.5%. Jointly considering the results in Fig. 1, we can conclude that our scheme selects the relay sooner, and the monetary reward for a single transmission is slightly smaller than the one of ORS.

By the time that the PU finds the optimal relay in OSR, the PU in our scheme can finds multiple relays and get rewards via transmitting multiple packets. Therefore, to make a fair comparison in terms of reward, we define the Ratio of monetary reward as the ratio between the total reward obtained in our scheme and the reward of ORS during the same time period. The value of ratio is reported in Fig. 3. From Fig. 3 we find that the ratio monetary reward is always higher than 1. The maximum value can reach 2 when $\alpha = 1$ and $M = 40$. In other words, our proposed scheme can produce higher reward than OSR during the same time period.

5.2 The Impact of Time Efficiency C

In this subsection, we set the observation duration $\alpha = 2$, the private value of the packet $\beta = 0.9$. From Fig. 4, we can see that the PU can stop within six steps in our scheme, and the number of observation steps increases with the increase of C . This is because the impact of C on the reward is big when C is small. Thus, the PU intends to stop as

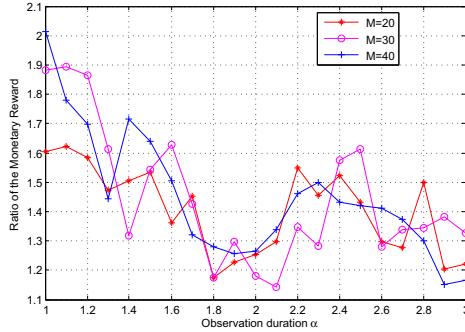


Fig. 3. Ratio of reward during the same time period with α

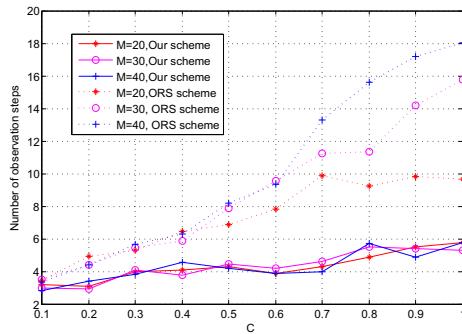


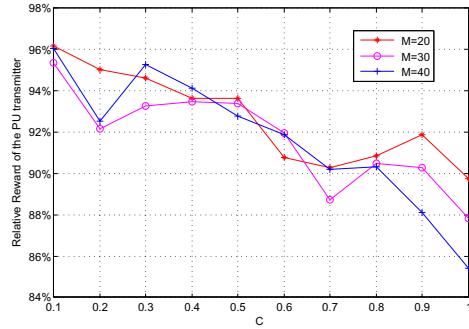
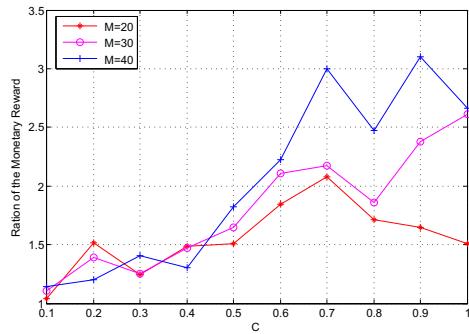
Fig. 4. Average number of observation steps with C

soon as possible at a smaller C . By comparing with the ORS scheme, we can find that the observation steps in our scheme is always less than the corresponding one of ORS.

In Fig. 5, we compare our scheme with ORS scheme in terms of relative reward for one packet transmission under different C . Similarly, the results of our scheme are normalized by the corresponding one of ORS. From Fig. 5, we find that the relative reward decrease with the increase with C . The reason is that the time impact on the reward function is small when C approximate 1. In general, the relative reward is larger than 85%.

Similarly to the ratio results reported in Fig. 3, we report the ratio of reward in Fig. 6 under several C . From Fig. 6 we can see that the ratio of monetary reward increases with the increase of C . The value of the ratio is always larger than 1 and can reach 3 when $M = 40$ and $C = 0.9$. In other words, the reward of our scheme is always higher than the one of ORS scheme during the same time period.

In summary, we can conclude that the PU can always select a relay within 6 observations by our scheme, which is much less than the number of observation steps in ORS. Although the reward of transmitting one packet in our scheme may be slightly smaller

**Fig. 5.** Relative reward for one packet transmission with C**Fig. 6.** Ratio of reward during the same time period with C

than the corresponding one in OSR, the accumulated reward of our scheme is always much larger than the corresponding one of OSR for transmitting multiple packets in a given time period.

6 Conclusion

In this paper, we have designed an online auction based relay selection scheme for cooperative communication in CR networks. Without checking the information from all the candidate relays, the PU can select a desirable relay within a given time limit. Our scheme achieves the property of truthfulness, which assures that all the bidders reveal their true valuations and eliminates the fear of market manipulation. Extensive simulations show that our scheme enables the PU to select a proper relay in a very short time and achieves a higher accumulated reward in a given time period comparing to the OSR scheme.

Acknowledgment. This work was supported by the National Science Foundation under Grant No. CNS-1265311.

References

1. Akyildiz, I.F., Lee, W.Y., Vuran, M.C., Mohanty, S.: Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks* 50(13), 2127–2159 (2006)
2. Laneman, J.N., Tse, D.N., Wornell, G.W.: Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory* 50(12), 3062–3080 (2004)
3. Huang, J., Han, Z., Chiang, M., Poor, H.: Auction-based resource allocation for cooperative communications. *IEEE Journal on Selected Areas in Communications* 26(7), 1226–1237 (2008)
4. Zhang, G., Cong, L., Zhao, L., Yang, K., Zhang, H.: Competitive resource sharing based on game theory in cooperative relay networks. *ETRI Journal* 31(1), 89–91 (2009)
5. Wang, B., Han, Z., Liu, K.R.: Distributed relay selection and power control for multiuser cooperative communication networks using buyer/seller game. In: IEEE INFOCOM, pp. 544–552 (2007)
6. Caoy, B., Mark, J.W., Zhang, Q., Lu, R., Lin, X., Shen, X.S.: On optimal communication strategies for cooperative cognitive radio networking. In: IEEE INFOCOM, pp. 1774–1782 (2013)
7. Roh, H., Jung, C., Lee, W., Du, D.Z.: A stackelberg game for cooperative cognitive radio network with active sus. In: IEEE ICNC, pp. 911–915 (2013)
8. Roh, H., Shao, C., Lee, S., Lee, W., Du, D.Z.: Secondary user games with spectrum leasing market in cooperative cognitive radio networks. In: IEEE INFOCOM DEMO, pp. 2461–2462 (2013)
9. Klemperer, P.: What really matters in auction design. *The Journal of Economic Perspectives* 16(1), 169–189 (2002)
10. Li, H., Cheng, X., Li, K., Xing, X., Jing, T.: Utility-based cooperative spectrum sensing scheduling in cognitive radio networks. In: IEEE INFOCOM, pp. 165–169 (2013)
11. Yang, D., Fang, X., Xue, G.: Hera: An optimal relay assignment scheme for cooperative networks. *IEEE Journal on Selected Areas in Communications* 30(2), 245–253 (2012)
12. Klemperer, P.: What really matters in auction design. *The Journal of Economic Perspectives* 16(1), 169–189 (2002)
13. Ferguson, T.: Optimal stopping and applications,
<http://doi.acm.org/10.1145/1614320.1614325>
14. Kern, S., Müller, S.D., Hansen, N., Büche, D., Ocenasek, J., Koumoutsakos, P.: Learning probability distributions in continuous evolutionary algorithms—a comparative review. *Natural Computing* 3(1), 77–112 (2004)

Channel Selection for Rendezvous with High Link Stability in Cognitive Radio Network^{*}

Zhenhua Han^{1,2}, Haisheng Tan², Yongcai Wang³, and Jipeng Zhou²

¹ School of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu, China

² Department of Computer Science, Jinan University, Guangzhou, China
thstan@jnu.edu.cn

³ Institute for Interdisciplinary Information Sciences, Tsinghua U., Beijing, China

Abstract. Channel selection is a fundamental problem in Cognitive Radio Networks (CRNs). One basic channel assignment problem is *rendezvous*, which investigates how secondary users can establish a connection by selecting a common available working channel in the same time slot. Rendezvous is the prerequisite for communication, which however is challenging especially in a dynamic spectrum environment. Link stability is a key factor that benefits the performance of a wireless network. In this work, we study the dynamic channel selection for rendezvous with high link stability. In the centralized case, we propose an algorithm to make as many secondary users as possible to establish stable links. In the distributed case, we derive a novel fast rendezvous strategy in the two-user scenario based on the local idle time of channels. The strategy can be utilized in asynchronous systems. Extensive simulations show that our algorithms have a higher stability in various environments compared with other rendezvous strategies.

Keywords: Cognitive Radio Networks, Channel Selection Problem, Rendezvous Problem, Link Stability.

1 Introduction

Wireless spectrum is a kind of scarce resource in recent wireless communication. It is widely believed that the cognitive radio (CR) technique will play a key role in solving the spectrum scarcity problem[1]. In a cognitive radio network (CRN), the licensed entities are often called the primary users (PUs), which have absolute priority in accessing the spectrum band. PUs allow the unlicensed secondary users (SUs) to access the licensed band without causing interference to the PUs. Therefore, before communication, secondary users need to sense a wide range of band and choose a free channel as the working channel, which is called *Channel Selection*.

* This work was supported in part by the Fundamental Research Funds for the Central Universities in China, and the National Natural Science Foundation of China Grant 61373125 and 61202360.

In CRNs, to avoid any possible interference to the PUs, we consider the case that SUs are only allowed to use the free channels which are not used by nearby PUs, i.e., in an overlay mode. Due to the existence of the PUs, the available channels for SUs are dynamic over both space and time. SUs at different locations may have different available spectrum. And the available spectrum for SUs may also change with time. One fundamental problem of SUs is how to establish a link with each other by selecting the same available channel to work on in a time slot, which is called *rendezvous*.

Channel selection for rendezvous in cognitive radio networks has attracted great attention in both academics and industry. The outputs can be divided into two groups: centralized and distributed. In a centralized system, secondary users adopt a central controller to help secondary users to build connections[2]. Although such a central controller may achieve high performance in rendezvous, it requires large information exchange overhead, which may not be practical. Some other centralized methods use a dedicated channel, called the Common Control Channel (CCC), to exchange information between users for rendezvous[3–7]. However, these methods have a key drawback that such a free channel used as CCC may be occupied by PUs, and also it may become an easy attack point.

To overcome the above drawbacks, blind rendezvous in a distributed system without any CCC or central controller is preferred. Among distributed strategies, the main group are to utilize channel-hopping (CH) technique [8–12] or a quorum system [7, 13–15]. Most of these methods can achieve low expected time to rendezvous (TTR). However, although they considered the spatial dynamics of the available channels for SUs, they did not take the channel dynamics over time into account.

Link stability is a key factor to determine the performance of a wireless network, particularly for the dynamic channel environment in CRNs. Unstable links mean frequent channel switches. In CRNs, the change of channel availability may cause disconnection between a pair of nodes. The channel selection strategies will also have a great effect on the link stability. In our paper, we focused on designing channel selection approaches to establish stable links for SUs. The main contribution includes:

- Centralized Environment: we proposed a centralized algorithm for multi-user networks to maximize the number of connected links, which will also have a property of improved link stability.
- Distributed Environment: we also derived a distributed rendezvous strategy for two secondary users, which has a low time to rendezvous when two users have a similar spectrum environment. A connected link will also have better stability compared with other exist rendezvous methods. The strategy does not need a global clock.
- We conducted extensive simulations to validate the performance of the above algorithms. Other than the random setting of the available channels for SUs, we set up the channel environment of the SUs based on the behaviors of the PUs. This setting is more close to the environment in practice.

The rest of the paper is organized as follows. We present the network model and the problem definitions in Section 2. We then propose a centralized algorithm to solve stable channel selection problem in Section 3. We also propose a distributed rendezvous strategy for two secondary users in Section 4. Section 5 contains the simulation results, and we conclude our work in Section 6.

2 Network Model and Problem Definitions

2.1 Network Model

We study a cognitive radio network which comprises the following elements:

- $U = \{SP_1, SP_2, \dots, SP_N\}$ is the set of N pairs of secondary users. S_i and D_i , where $i = \{1, 2, \dots, N\}$, are the sets of source nodes and destination nodes respectively;
- $C = \{c_1, c_2, \dots, c_L\}$ is the set of L channels in the network;
- $PU = \{PU_1, PU_2, \dots, PU_M\}$ is the set of M primary users.

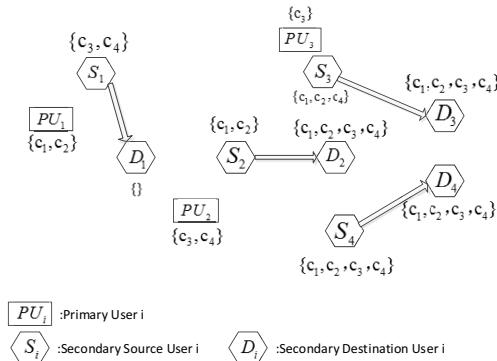


Fig. 1. A cognitive radio network with different available channels to secondary users

As stated before, we consider the network works under an overlay mode, i.e., SUs can only use channels that are free to its nearby PUs. The available channel set for a secondary user u is denoted as A_u . Figure 1 illustrates a scenario of a CRN with PUs and SUs. The whole channel set is $C = \{c_1, c_2, c_3, c_4\}$. The channel set beside a PU indicates its current working channel, while the set beside a SU indicates its available channels. For example, $A_{S_1} = \{c_3, c_4\}$, since S_1 can not use the working channels of PU_1 ; $A_{D_1} = \emptyset$, since all the channels are occupied by its nearby PUs. In this work, we assume that each SU has already known its local available channels through spectrum sensing or accessing to a centralized spectrum resource database. Our work focuses on the selection of an available channel as the working channel for each SU.

2.2 Stable Channel Selection Problem

Two secondary nodes can communicate if and only if they select the same available channel at the same time slot. For the pair SP_i of secondary users, we define

$$x_l^i = \begin{cases} 1, & \text{both two nodes of the pair } SP_i \text{ select channel } c_l \\ 0, & \text{otherwise.} \end{cases}$$

A node can only choose one available channel at each time slot (also called round). We adopt the global interference model, so an available channel can be chosen by only a pair of nodes. In addition, we define *the communication time* of a link is the duration from its establishment on a working channel c to the end of its connection on channel c no matter due to the disconnection of the link or the change of its working channel.

In the centralized case, our main aim is to maximize the number of connected links. The assignment may not be unique. We select the one with the highest stability. At each round, we will re-choose working channels for each SU to achieve the global optimization in maximizing the connected links and the network stability. That is to say, the working channel of a link might be switched to another one even its old working channel is still available. Therefore, in the centralized case we define stability as follow:

- Stability decreases if a secondary link disconnects;
- Stability decreases if a link is still connected but the nodes switch their communication channel to another one.

Let $\beta(i, l)$ denote the stability of channel $c_l \in C$ for secondary pair $SP_i \in U$. There might be various definitions of $\beta(i, l)$. Here, in order to improve the probability that a link remains working on the same channel as long as the channel is available, we propose a definition only based on the network status of the previous round:

$$\beta(i, j) = \begin{cases} 1, & \text{Secondary Pair } SP_i \text{ used channel } c_j \text{ as} \\ & \text{the communication channel in the previous round;} \\ 0, & \text{otherwise.} \end{cases}$$

Based on the above, we can formulate the following the stable channel selection (SCS) problem:

$$\begin{aligned} \max \quad & \left\langle \sum_{l=1}^L \sum_{i=1}^N x_l^i, \sum_{l=1}^L \sum_{i=1}^N x_l^i \beta(i, l) \right\rangle \\ \text{s.t.} \quad & x_l^i \in \{0, 1\}, \quad \forall SP_i \in U, \forall c_l \in C \end{aligned}$$

$$\begin{aligned}
& \sum_{l=1}^L x_l^i \leq 1, & \forall SP_i \in U \\
& \sum_{i=1}^N x_l^i \leq 1, & \forall c_l \in C \\
& x_l^i = 0, & \forall SP_i \in U, \forall c_l \notin A_{S_i} \text{ or } c_l \notin A_{D_i} \\
\text{variables } & \mathbf{x} = \{x_l^i\}.
\end{aligned}$$

In addition, the order of $\langle a, b \rangle$ and $\langle c, d \rangle$ is defined as follows: $\langle a, b \rangle$ is greater than $\langle c, d \rangle$ if and only if $a > c$, or $b > d$ when $a = c$.

In the distributed case, due to the dynamics of the available channels, the rendezvous of two nodes is already challenging. In this work, we investigate the stable rendezvous problem of two SUs, and leave the rendezvous for multiple users as the future work. Once the two SUs achieve rendezvous on a channel c , they will keep on working on this channel until c is occupied by a PU. Therefore, we define the stability in the distributed case as:

- Once two SUs achieve rendezvous, the longer communication time indicates the better link stability.

In every round, both SUs independently choose an available channel and attempt to build connection on this channel. If they choose the same channel, the rendezvous is achieved. Our goal is to design a strategy which can help two SUs to build a stable connection with a short time to rendezvous (TTR).

3 A Centralized Stable Channel Selection Algorithm

In the centralized condition, secondary users adopt a central controller to help them selecting channels. The controller acquires all channel state of SUs before making the assignment. At any time t , we design the Stable Channel Selection Algorithm (Algorithm 1) to achieve the maximum number of connected links with high link stability. The algorithm contains the following steps:

1. Line 1–9: *Construct a weighted directed bipartite graph between the sets secondary user pairs U and channels C .*

We denote the bipartite graph as $G = (V(U, C), E)$. An edge $e_{ij} \in E$ pointing from a node in U to a node in C if and only if channel c_j is available for both nodes of pair SP_i (Figure 2). Then, the channel selection for a time t , denoted as P_t , is a subset of links in E . For example, if $e_{ij} \in P_t \subseteq E$, it means at time t we assign channel c_j to the pair SP_i .

In addition, we set $\beta(i, j)$ as the weight (or cost) of the edge e_{ij} .

2. Line 10–15: *Construct a graph to compute the maximum cost maximum flow, denoted as G_1 .*

We add two virtual nodes N_{source} and N_{sink} to G . N_{source} points to each node in U with cost 0; and each node in C points to N_{sink} with cost 0. We set the capacity of all edges in G_1 to 1.

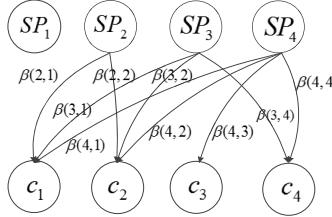


Fig. 2. the constructed bipartite graph based on the scenario in Figure 1

3. Line 16–17: *Compute the channel selection.*

We compute the maximum cost maximum flow in G_1 taking N_{source} and N_{sink} as the source and sink respectively. The edges between nodes U and C whose residual capacity is 0 are the elements of P_t .

Algorithm 1. Stable Channel Selection Algorithm

Input: t, P_{t-1}
Output: P_t

- 1 Initialize a weighted bipartite graph $G = (V(U, C), E = \emptyset)$ and $P_t = \emptyset$;
- 2 **for** $i \in \{1, 2, \dots, |U|\}$ **do**
- 3 **for** $j \in \{1, 2, \dots, |C|\}$ **do**
- 4 **if** channel c_j is open to the source and destination node of SP_i **then**
- 5 **if** $t = 0$ or $e_{ij} \in P_{t-1}$ **then**
- 6 $\beta(i, j) \leftarrow 1$;
- 7 **else**
- 8 $\beta(i, j) \leftarrow 0$;
- 9 Add edge e_{ij} to G with cost $\beta(i, j)$;
- 10 Construct a weighted graph $G_1 = (V \cup \{N_{source}, N_{sink}\}, E)$ based on G ;
- 11 **for** $i \in \{1, 2, \dots, |U|\}$ **do**
- 12 Add edge between N_{source} and SP_i in G_1 with cost 0;
- 13 **for** $i \in \{1, 2, \dots, |C|\}$ **do**
- 14 Add edge between N_{sink} and c_i in G_1 with cost 0 ;
- 15 Set the capacity of all edges in G_1 to 1;
- 16 Compute the maximum cost maximum flow of G_1 with source N_{source} and sink N_{sink} ;
- 17 $P_t =$ All edges between U and C where the residual capacity is 0 when achieving the maximum cost maximum flow;
- 18 **return** P_t ;

The input of Algorithm 1 are the time slot t and the channel selection of the previous slot P_{t-1} . Here, the maximum matching of the bipartite graph G are the maximum connected links at time t . The maximum cost maximum flow

in G_1 guarantees that the cost is maximized with the precondition that the flow is maximized, which can be computed in polynomial time. Moreover, when achieving the maximum flow, the edges P_t , whose residual capacities are 0, form a maximum matching of the bipartite graph G . The cost of an edge e_{ij} is set as $\beta(i, j)$. Therefore, the maximum cost indicates our channel selection P_t also have the maximum stability.

4 Distributed Strategy for 2-User Rendezvous Problem

In a distributed system, a node only knows the available channels of its own. In this section, we propose a novel rendezvous strategy for two secondary users based on the local idle rate of channels.

Let T denote the timeslots counted from the moment that the SU enters the network and $Idle(c)$ denote the total available time of channel c during the T slots. In our method, a node is required to calculate and memorize $Idle(c)$ of every channel from the moment it enters the network. At time T , the largest available probability among all the channels is estimated as $p = \frac{Idle(c_m)}{T}$, where c_m is the channel with the longest available time so far. Figure 3 shows an example of the calculation.

At the first τ timeslots, our strategy just calculate the idle rates of channels and does not try to achieve rendezvous. This is to avoid rendezvous on an unstable channel with insufficient information. After τ slots, we sort all the channels based on their available time so far¹, and the SU will select the working channel based on a geometric distribution probability(Algorithm 2).

Time	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Channel 1	Off	Off	On	On	On	Off	Off	Off	On	On	On	On	Off	Off	Off	Off	Off	On	On	
Idle(c_1)	0	0	1	2	3	3	3	3	4	5	6	7	7	7	7	7	7	8	9	
Channel 2	On	On	On	Off	Off	Off	On	On	On	Off	Off	Off	Off	Off	On	On	On	On	Off	
Idle(c_2)	1	2	3	3	3	3	4	5	6	6	6	6	6	6	6	6	7	8	9	9
p	1	1	1	0.75	0.6	0.5	0.57	0.625	0.667	0.6	0.545	0.5	0.538	0.5	0.467	0.438	0.412	0.444	0.473	0.45

Fig. 3. An example of calculating $Idle(c)$ and p for one SU in the case of two channels (the shadowed grid is the channel c_m which has the longest available time so far)

In our strategy Algorithm 2, since a channel with longer available time will have a higher probability to be selected, a connected link would have a good property of stability. Meanwhile, if two SUs have similar channel environments, their sorted lists of channels will also be similar. Therefore, our strategy makes them tend to select the same available channel, which implies the time to rendezvous (TTR) is small. In practice, two SUs communicating with each other

¹ If two channel c_i and c_j have the same available time so far, i.e., $Idle(c_i) = Idle(c_j)$, then the one with the lower channel ID comes first in the sorted list.

Algorithm 2. Rendezvous strategy for one SU in the distributed case

```

1: Sort all channels in descending order by their available time so far.
2:  $p = \frac{Idle(c_m)}{T}$ , where  $c_m$  is the channel with the longest available time.
3: if  $T > \tau$  then
4:   Choose the  $i$ -th open channel ( $i \geq 1$ ) in the sorted order with possibility
       $\frac{p}{\lambda}(1 - \frac{p}{\lambda})^{i-1}$  ( $\lambda$  is a constant set by the secondary user)
5: else
6:   Do not try any channel
7: end if

```

should be close, which indicates their channel environment should be similar. Our simulations in the next section will verify the performance of Algorithm 2 for both the small TTR and high stability. Moreover, our strategy dose not make use of a global clock between the two SUs, which means it can be adopted in asynchronous systems.

5 Simulation

To analyze the performance of the algorithms in Section 3 and 4, we conduct extensive simulations. In this work, we propose a method to set up the channel environment for SUs based on PUs. Recall that each SU can not make use of the channels occupied by nearby PUs. Therefore, for a primary user PU_i , we define a *dominating range*, denoted as r_i^{dom} . To avoid any interference to PU_i , any SU with a distance equal to or shorter than r_i^{dom} to PU_i can not use the current working channels of PU_i . Furthermore, a Markov model in Figure 4 is adopted to simulate the working channels of the PUs. At a time slot, each channel of PU_i has a probability of α_i to change its state from OFF for SUs (PU_i works on it) to ON for SUs (PU_i does not work on it); similarly, each channel has a probability of β_i to change form ON to OFF.

Based on the above method, we set up two CRN instances with different characteristics: Network 1 and Network 2 (Figure 5 and 6). The parameters are listed in Table 1. In the figures, a red dot represents the location of a PU and the red circle centered at it indicates its dominating range. A blue triangle dot represents the location of a secondary user. Two secondary users connected by a blue line means they are a secondary pair. Initially, the working channels of PUs are set randomly.

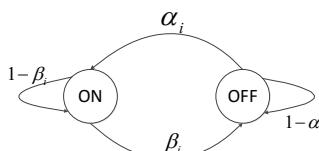
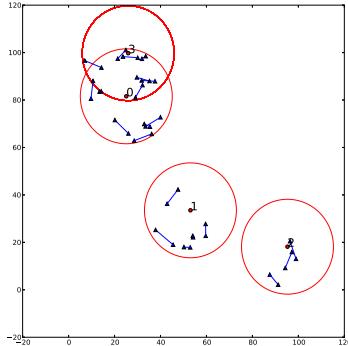
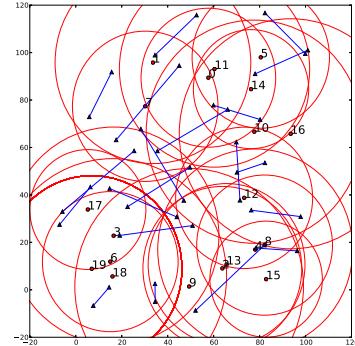


Fig. 4. Markov model of the state of PU_i 's channels

**Fig. 5.** Network 1**Fig. 6.** Network 2

5.1 The Centralized Stable Channel Selection Algorithm

In the centralized condition, the Greedy Channel Selection Algorithm (GCS) in [16] is also implemented for comparison, which directly assigns the channels through computing the maximum bipartite matching in $G = (V(U, C), E)$. The main difference from our method is that we consider the stability of the entire network. Because both methods can achieve the maximum connected links, we only compare the property of stability through calculating switches, disconnections and average communication time of links. One disconnection means a connected link is disconnected. Switches increases by one when a disconnection

Table 1. Settings of two Networks

Settings	Network 1	Network 2	Network 3
Number of Channel	20	30	10 to 100
Number of Primary User	4	20	10
Number of Secondary User	42	40	2
Average value of α	0.3	0.9	0.3
Average value of β	0.8	0.9	0.8
Maximum dominating range of PU	20	50	80
Maximum communicating range of SU	10	40	30

happens or a link changes its working channel. We calculate the above parameters in both Network 1 and 2. We generate the two networks 200 times based on their parameters in Table 1, and run the two centralized algorithms to take the average values as our simulation results. Figure 7 and 8 illustrate the numbers of disconnections at each round in Network 1 and 2 respectively. In network 1, our algorithm has a similar disconnection fluctuation with the GCS because of the simple network structure. In the complex Network 2, our method has a clearly lower numbers of disconnection. Figure 9 and 10 show that our algorithm has lower switches. Figure 11 and 12 indicate the higher average communication time per link of our algorithm. All experiments validate that our algorithm have the better stability than the GCS Algorithm.

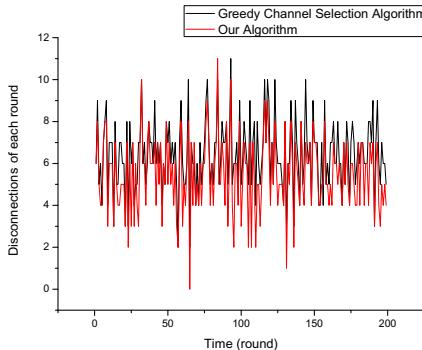


Fig. 7. Disconnections on network 1 at each round

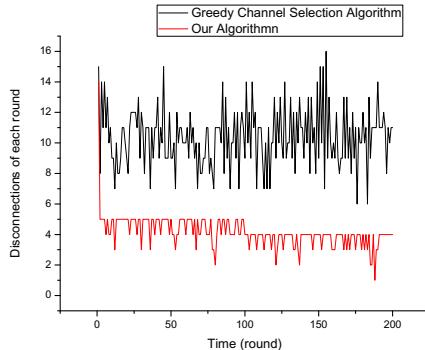


Fig. 8. Disconnections on network 2 at each round

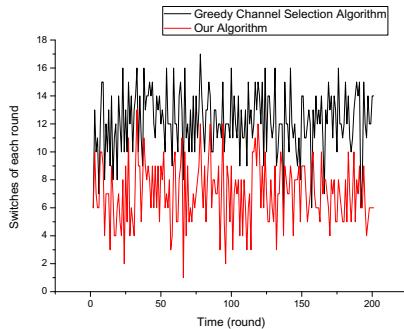


Fig. 9. Switches on network 1 at each round

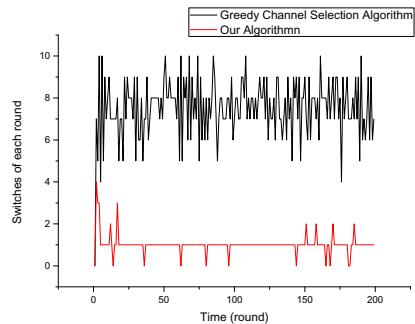


Fig. 10. Switches on network 2 at each round

5.2 The Distributed Strategy

For the rendezvous strategies for two SUs, we will compare our strategy Algorithm 2 with the well-known Jump-stay algorithm in [9] and the random selection. We calculate the link commutation time and expected time to rendezvous

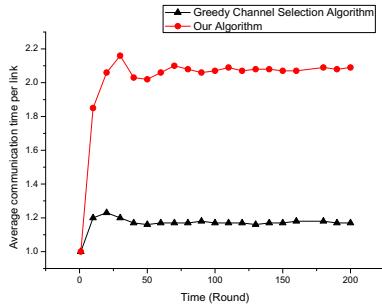


Fig. 11. Average communication time per link on network 1

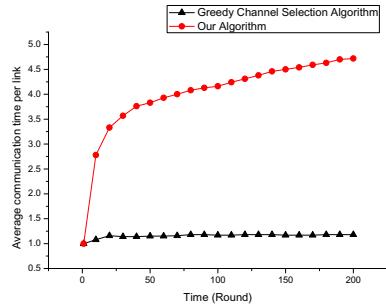


Fig. 12. Average communication time per link on network 2

(ETTR) to evaluate the link stability and rendezvous speeds of the three methods. We generate the network based on the parameters of Network 3 in Table 1. The simulation program will randomly put two SUs on 200 different sets of positions. In one set of position, 400 timeslots are observed, and each algorithm will be repeated for 100 times. We take the average communication time as our results, and the average TTR as the expected TTR (ETTR). It will be regarded as a failure once two nodes can not reach rendezvous within 400 timeslots.

We set that our algorithm will only collect the channel information for the first 30 rounds (i.e., we set $\tau = 30$). Figure 13 shows that our strategy has a higher cumulative communication time after about 60 time-slots than the other methods. Here, cumulative communication time means during the 400 timeslots, once the link is disconnected we establish the link again using the same strategy and sum up the communication times. Figure 14 shows the fact that our strategy has the lowest ETTR for all different cases of the the total number of channels if we neglect the time for collecting the channel information.

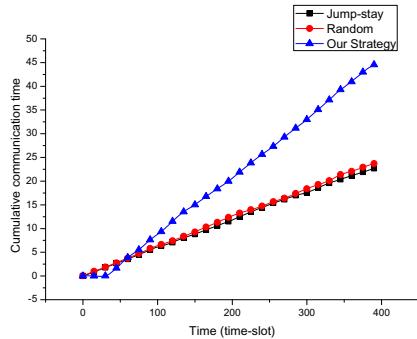


Fig. 13. Cumulative Communication time (number of channels=40)

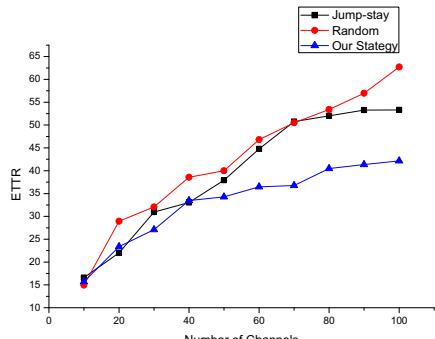


Fig. 14. Expected time to rendezvous

6 Conclusion

In this paper, we investigate the channel selection problem in cognitive radio network with high link stability. We formulate the stable channel selection (SCS) problem under centralized and distributed conditions. For the centralized case, we solve the SCS problem and achieve the maximum number of connected links based on computing the maximum cost maximum flow. The links established also have a good property of stability. For the distributed case, we consider the 2-user rendezvous problem and propose a novel algorithm which utilizes the idle rates of each channel to achieve high network stability. Our rendezvous strategy have a small time to rendezvous and can be adopted in asynchronous environments. Extensive simulations validate our algorithms have higher stability than other methods in most cases. The study of the distributed rendezvous strategies with high link stability for multiple users will be an interesting extension of this work. Future work can also include studying the channel assignment under a more realistic interference model, such as the physical interference models.

References

1. Bahl, P., Chandra, R., Moscibroda, T., Murty, R., Welsh, M.: White space networking with wi-fi like connectivity. *ACM SIGCOMM Computer Communication Review* 39(4), 27–38 (2009)
2. Liang, H., Lou, T., Tan, H., Wang, Y., Yu, D.: On the complexity of connectivity in cognitive radio networks through spectrum assignment. *Journal of Combinatorial Optimization* (2013)
3. Cordeiro, C., Challapali, K., Birru, D., Sai Shankar, N.: IEEE 802.22: the first worldwide wireless standard based on cognitive radios. In: *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 328–337 (November 2005)
4. Jia, J., Zhang, Q., Shen, X.: HC-MAC: A hardware-constrained cognitive mac for efficient spectrum management. *IEEE Journal on Selected Areas in Communications* 26(1), 106–117 (2008)
5. Pérez-Romero, J., Salient, O., Agustí, R., Giupponi, L.: A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation. In: *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 46–54 (2007)
6. Zhao, J., Zheng, H., Yang, G.-H.: Distributed coordination in dynamic spectrum allocation networks. In: *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pp. 259–268 (2005)
7. Bian, K., Park, J.-M., Chen, R.: Control channel establishment in cognitive radio networks using channel hopping. *IEEE Journal on Selected Areas in Communications* 29(4), 689–703 (2011)
8. Gandhi, R., Wang, C.-C., Hu, Y.C.: Fast rendezvous for multiple clients for cognitive radios using coordinated channel hopping. In: *Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 434–442 (2012)
9. Lin, Z., Liu, H., Chu, X., Leung, Y.-W.: Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks. In: *IEEE INFOCOM*, pp. 2444–2452 (2011)

10. Theis, N.C., Thomas, R.W., DaSilva, L.A.: Rendezvous for cognitive radios. *IEEE Transactions on Mobile Computing* 10(2), 216–227 (2011)
11. Azar, Y., Gurel-Gurevich, O., Lubetzky, E., Moscibroda, T.: Optimal discovery strategies in white space networks. In: Demetrescu, C., Halldórsson, M.M. (eds.) *ESA 2011. LNCS*, vol. 6942, pp. 713–722. Springer, Heidelberg (2011)
12. Anderson, E.J., Weber, R.: The rendezvous problem on discrete locations. *Journal of Applied Probability*, 839–851 (1990)
13. Romaszko, S., Mahonen, P.: Grid-based channel mapping in cognitive radio ad hoc networks. In: *IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pp. 438–444 (2011)
14. Romaszko, S., Denkovski, D., Pavlovska, V., Gavrilovska, L.: Asynchronous rendezvous protocol for cognitive radio ad hoc networks. In: Zheng, J., Mitton, N., Li, J., Lorenz, P. (eds.) *ADHOCNETS 2012. LNICST*, vol. 111, pp. 135–148. Springer, Heidelberg (2013)
15. Bian, K., Park, J.-M.: Asynchronous channel hopping for establishing rendezvous in cognitive radio networks. In: *IEEE INFOCOM*, pp. 236–240 (2011)
16. Hou, F., Huang, J.: Dynamic channel selection in cognitive radio network with channel heterogeneity. In: *Global Telecommunications Conference (GLOBECOM)*, pp. 1–6 (December 2010)

Game Theoretic Joint Beamforming and Power Allocation for Cognitive MIMO Systems with Imperfect Channel State Information

Feng Zhao¹, Jiayi Zhang¹, and Rongfang Bie²

¹ Key Laboratory of Cognitive Radio and Information Processing (Guilin University of Electronic Technology), Ministry of Education, Guilin, China
zhao.feng@guet.edu.cn, 297212323@qq.com

² College of Information Science and Technology, Beijing Normal University, Beijing, China
rfbie@bnu.edu.cn

Abstract. This paper considers a spectrum underlay sharing cognitive radio networks composed of multiple primary users (PUs) and multiple non-cooperative secondary users (SUs). With the imperfect channel state information (CSI), our objective is to maximize the total throughput of SUs, while guaranteeing the interference constraints of PUs as well as the peak transmission power constraints of SUs. We formulate the design of the SUs as a non-cooperative game, where the SUs compete with each other over the beamforming weights and transmit power made available by the PUs. Nash equilibrium (NE) is considered as the solution of this game and we analyze the existence and uniqueness of NE. Simulation results show that under the imperfect CSI the proposed algorithm has good performance and can converge to a locally optimal pair of transmission power vector and beamforming vector.

Keywords: Cognitive radio, Multi-input multi-output (MIMO), Game theory, Imperfect channel state information.

1 Introduction

The increasing demand for wireless services has urged researchers to seek an efficiency way of utilizing the scarce radio spectrum. As a novel approach, cognitive radio (CR) has attracted tremendous interests recently. Through spectrum sensing, CR can opportunistically communicate on temporarily idle frequency bands while avoiding interference with licensed PUs [1]. MIMO communications improve the link throughput by sending independent data streams simultaneously over different antennas [2].

MIMO CR networks were recently studied in [3, 4]. A semi-distributed algorithm was proposed in [3] to obtain a locally optimal solution to the SU beamforming problem. When the secondary transmitter has complete, partial, or no knowledge about the channels to the primary receivers, [4] studied the optimal secondary-link beamforming pattern that balances between the SU's throughput and the interference. CR is viewed as a smart technology to allow SUs to flexibly utilize the spectrum

resource licensed to primary users. There are two main spectrum sharing strategies: spectrum sharing overlay and spectrum sharing underlay [5, 6]. In spectrum sharing underlay, the challenge is to maintain the interference to PUs below a tolerable level and null the mutual interference among SUs while maximizing the SUs' quality of service (QoS), the joint beamforming and power allocation technology is considered as an effective technique to solve it. In [7], a joint beamforming and power allocation algorithm for total throughput maximization in CR network was proposed. But in the algorithm, when the number of PUs is large or their transmission power is high, the total throughput of SUs will fall rapidly. The authors of [8] formulated the problem of resource allocation and beamforming as a mixed-integer programming problem. To reduce the computation complexity, a branch and bound method was proposed to find the optimal solution.

However, previous works on CR were largely based on the exploitation of perfect CSI. In practice, the CSI will never be perfect, due to estimation and quantization errors as well as Doppler spread. The authors of [9] considered partial channel state information and channel uncertainties. But it was assumed that the secondary base station can know the perfect CSI for SUs. A bounded region for channel matrices and channel covariance matrices was assumed to be known in [10]. [9, 10] used a type of ellipsoid uncertainty problem to express the bound channel uncertainty.

Uncertainty in game theory has only recently been investigated. In [11], following the worst-case robust theory, the authors took into account the imperfectness of SU-to-PU CSI by adopting proper interference constraints. The existence and uniqueness of the NE of the robust game were studied by relying on the variational inequality theory. A distribution-free robust framework for the rate-maximization game had been proposed in [12], where the authors analyzed the social properties of the equilibrium under varying channel uncertainty bounds for the two-user case. Robust equilibrium in additively coupled games in communications networks had been presented in [13]. The objective was to present a complete analysis of the NE in robust games as compared to that of NE in nominal games with complete information.

In our earlier works, [14] studied the problem of joint beamforming and power allocation in a cognitive MIMO system via game theory, but the CSI is perfect. Different from [14], in this work, we take into account an ellipsoid approximation of the uncertainty in the CSI by the robust interference constraint. [15] considered the problem of joint beamforming and power allocation under perfect and imperfect CSI, but the existence and uniqueness of NE did not study when the CSI is imperfect, and the system model is different from this work. In this paper, under a game-theoretic framework, we study the problem of joint beamforming and power allocation in a cognitive MIMO system with imperfect channel state information. Given the competitive nature of the SUs, we formulate beamforming weights and transmit power among SUs as a strategic non-cooperative game, where each SU competes against the others to maximize his own sum utility under the power constraints and the robust interference constraints. In the non-cooperative game the NE [16] is considered as the solution of this game, the pricing function is the cost of the spectrum. We study the existence and uniqueness properties of the NE and solve the game optimization problem via a second order cone programming method.

The following notations are used in this paper. The capital boldface is used to denote matrices, and the lowercase in boldface denotes vectors. $(\cdot)^H$, $(\cdot)^T$ and $\|\cdot\|$

denote the conjugate transpose operation, transpose operation and Euclidean norm of a vector, respectively.

2 System Model and Problem Statement

We consider a CR network composed of a primary network and a secondary network, coexisting in the same area and sharing the same spectrum, as illustrated in Fig. 1. Suppose that there are M antennas at the secondary base station (SBS) and a single antenna for each SU. Similarly, there is also a primary base station (PBS) to communicate with PUs, and each PU has the maximum interference threshold constraint, both the PBS and the PUs have single antenna. For simplicity of presentation, we assume that the PBS communicates with only one PU with the interference threshold PUs constraint. Let $h_{k,m}$ be channel gain between transmit antenna M and the receiver of SU k . Note $\mathbf{h}_k = [h_{k,1}, h_{k,2}, \dots, h_{k,M}]$, and the channel matrix \mathbf{H} is $\mathbf{H} = [\mathbf{h}_1^*, \mathbf{h}_2^*, \dots, \mathbf{h}_M^*]^*$. Let $\mathbf{g} = [g_{1,p}, g_{2,p}, \dots, g_{K,p}]$ denote the channel gain from the PBS to SU k . Let $\mathbf{w}_k = [w_{k,1}, w_{k,2}, \dots, w_{k,M}]^T$ be the beamforming weight for the SU k , and the beamforming weight matrix can be expressed as $\mathbf{w} = [w_1, w_2, \dots, w_k]$.

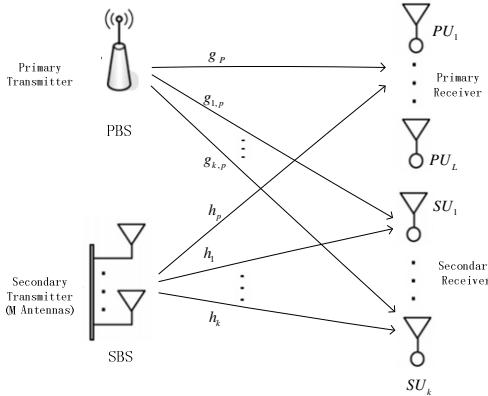


Fig. 1. Cognitive MIMO system model

Therefore the received signal for SU k can be written as

$$y_k = \sum_{i=1}^K \sqrt{p_i} \mathbf{h}_k \mathbf{w}_i x_i + \sqrt{p_p} g_{k,p} x_p + n_k \quad (1)$$

The received signal at the PU receiver is expressed as

$$y_p = \sum_{i=1}^K \sqrt{p_i} \mathbf{h}_p \mathbf{w}_i x_i + \sqrt{p_p} g_p x_p + n_p \quad (2)$$

where $\mathbf{h}_p = [h_{p,1}, h_{p,2}, \dots, h_{p,M}]$ and g_p denote the channel gain from SBS to PU and from PBS to PU, respectively, x_k and x_p are the modulated symbols for SU k and PU, n_k and n_p are the noise random variables with zero-mean and variances σ_k^2 and σ_p^2 , respectively. Therefore, the output signal-to-interference-and-noise ratio (SINR) of the k -th is

$$\text{SINR}_k = \frac{|\mathbf{h}_k \mathbf{w}_k|^2 p_k}{\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |g_{k,p}|^2 p_p + \sigma_k^2} \quad (3)$$

and the interference received by PU from SBS is $\kappa = \sum_{k=1}^K |\mathbf{h}_p \mathbf{w}_k|^2 p_k$, where p_k is the transmit power from SBS to PU and p_p is the transmit power from PBS to PU. The achievable rate of the k -th SU can be expressed as

$$R_k = \log_2(1 + \text{SINR}_k) \quad (4)$$

Therefore, our interest is to maximize the sum-rate of the SUs subject to the individual peak transmission power constraint of each SU, as well as the interference power constraints of PU. The optimization problem can be formulated as follows

$$\begin{aligned} & \max_{p_k, \mathbf{w}} \sum_{k=1}^K R_k \\ & 0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K] \\ & \text{subject to } \sum_{k=1}^K |\mathbf{h}_p \mathbf{w}_k|^2 p_k \leq \kappa_p \end{aligned} \quad (5)$$

where the peak transmission power constraint of k -th SU is denoted by $p_{k,\max}$, and κ_p is the interference threshold constraint.

In practice, however, SBS-to-PU CSI is seldom perfect due to lack of explicit cooperation. To take into account imperfect SBS-to-PU CSI, we adopt the following common imperfect CSI model [17, 18]. The ellipsoidal approximation has the advantage of parametrically modeling complicated data sets and thus provides a convenient input parameter to algorithms. Specifically, a nominal channel $\tilde{\mathbf{h}}_p$, which is a corrupted version of the actual $\hat{\mathbf{h}}_p$ by an error \mathbf{e}_p .

$$\tilde{\mathbf{h}}_p = \hat{\mathbf{h}}_p + \mathbf{e}_p \quad (6)$$

where \mathbf{e}_p belongs to an elliptical uncertainty region D_p defined by the weighted Euclidean norm as

$$D_p = \{\mathbf{e}_p \in \ell : \|\mathbf{e}_p\| \zeta_p \leq \varepsilon_p\} \quad (7)$$

where ζ are given positive weights. The radius ε_p represents the size of the uncertainty region, the larger ε_p is, the more uncertainty there is.

So the optimization problem (5) can be equivalently expressed as

$$\begin{aligned} & \max_{p_k, \mathbf{w}} \sum_{k=1}^K R_k \\ & 0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K] \\ \text{subject to } & \sum_{k=1}^K \left| \left(\hat{\mathbf{h}}_p + \mathbf{e}_p \right) \mathbf{w}_k \right|^2 p_k \leq \kappa_p \end{aligned} \quad (8)$$

3 Game Theoretic Design

Obviously, the optimization problem (8) is non-convex. Thus, even a centralized computation of the globally optimal solution is prohibitively expensive. To develop a distributed algorithm, we reformulate (8) as a non-cooperative game and derive a pricing function for each CR link that guarantees a locally optimal solution.

3.1 Game Formulation

A non-cooperative game is characterized by a set of players, their action/strategy spaces, and corresponding utility/payoff functions. For the system model, the set of the k SUs represents the set of players. The action space is the union of the action spaces of various players, subject to constraints condition in. The action/strategy space for each player is the set of all possible beamforming matrices for the frequency channels. Therefore, a non-cooperative game can be formulated as follows

$$Q = \left\{ \Omega, \left\{ \mathbf{w}_k, p_k \right\}_{k \in \Omega}, \left\{ u_k \right\}_{k \in \Omega} \right\} \quad (9)$$

where $\Omega = \{1, 2, \dots, K\}$ is the set of the k SUs, The strategy of each player includes beamforming weights and transmit power (denoted by \mathbf{w}_k and p_k for the k -th SU, which is non-negative), u_k is the utility function, the utility function can be designed based on the achievable rate, i.e.,

$$\mu_k = \log_2(1 + SINR) \quad (10)$$

3.2 Pricing Policy

By solving the above problem, SUs implicitly interact with each other through their choices. Under some conditions, the game reaches a NE where no user has an incentive to unilaterally deviate from. However, the selfish behavior of SUs may be serious, the resulting NE is often far from the Pareto optimum, and the network throughput can be low. The utility function defined in (10) does not embody the harmful effect of SUs' transmit power to the PU, we can introduce pricing policies as an effective tool into the utility function to qualify such harmful effects. The new utility function with price is defined as

$$\dot{\mu}_k = \log_2(1 + SINR) - F \quad (11)$$

where F is the pricing function.

In this work, pricing has been used to improve the efficiency of a NE of a non-cooperative game. Pricing discourages players from behaving selfishly and incentivizes them to work in a cooperative way. We define the pricing F function as $\lambda p_k \left| \tilde{\mathbf{h}}_p \mathbf{w}_k \right|^2$, where λ is a positive constant and has an effect on reflecting the potential interference to the PU. What's more, in the following discussion, we will show that regardless of how to choose the pricing factor, the Nash equilibrium always exists. The non-cooperative game is formulated as

$$\begin{aligned} & \max_{p_k, \mathbf{w}} \sum_{k=1}^K \mu_k \\ & 0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K] \\ & \text{subject to } \sum_{k=1}^K \left| \left(\hat{\mathbf{h}}_p + \mathbf{e}_p \right) \mathbf{w}_k \right|^2 p_k \leq \kappa_p \end{aligned} \quad (12)$$

Here, each SU competes against the others by choosing its beamforming vector \mathbf{w}_k and transmission power p_k to maximize its own utility function.

3.3 Existence of Nash Equilibria

Given a strategic non-cooperative game, the existence of a NE in pure strategies is not guaranteed, the main difficulty in the analysis of the proposed games is that one cannot compute the best-response mapping of each user. The following theorem guarantees the existence of a NE of the game.

Theorem 1: There exists at least one NE for the non-cooperative game.

Proof: We need to show that [19]

- 1) The action space of each player is convex and compact.
- 2) The utility function μ_k is concave with respect to $\{\mathbf{w}_k, p_k\}_{k \in \Omega}$.

The action space of SUs k is shaped by constraints $0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K]$ and $\sum_{k=1}^K \left| \tilde{\mathbf{h}}_p \mathbf{w}_k \right|^2 p_k \leq \kappa_p$, which define the feasible region of the local optimization problem. It is easy to verify that the Hessians of them are positive definite. Hence, the two constraints are convex. Consequently, the feasible region or action space defined by constraints is the intersection of two convex regions, i.e., the action space of the game convex.

By taking the first derivative of μ_k with respect to p_k and $|\mathbf{w}_k|^2$, respectively, we have

$$\frac{\partial \mu_k}{\partial p_k} = \frac{1}{\ln 2} \frac{|\mathbf{h}_k \mathbf{w}_k|^2}{\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |g_{k,p}|^2 p_p + \sigma_k^2 + p_k |\mathbf{h}_k \mathbf{w}_k|^2} - \lambda \left| \tilde{\mathbf{h}}_p \mathbf{w}_k \right|^2 \quad (13)$$

$$\frac{\partial \mu_k}{\partial |\mathbf{w}_k|^2} = \frac{1}{\ln 2} \frac{p_k |\mathbf{h}_k|^2}{\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |\mathbf{g}_{k,p}|^2 p_p + \sigma_k^2 + p_k |\mathbf{h}_k \mathbf{w}_k|^2} - \lambda p_k \left| \tilde{\mathbf{h}}_p \right|^2 \quad (14)$$

Moreover, by finding the second derivative of μ_k with respect to p_k and $|\mathbf{w}_k|^2$, respectively, we get

$$\frac{\partial^2 \mu_k}{\partial^2 p_k} = -\frac{1}{\ln 2} \frac{|\mathbf{h}_k \mathbf{w}_k|^4}{\left[\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |\mathbf{g}_{k,p}|^2 p_p + \sigma_k^2 + p_k |\mathbf{h}_k \mathbf{w}_k|^2 \right]^2} \quad (15)$$

$$\frac{\partial^2 \mu_k}{\partial^2 |\mathbf{w}_k|^2} = -\frac{1}{\ln 2} \frac{p_k^2 |\mathbf{h}_k|^4}{\left[\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |\mathbf{g}_{k,p}|^2 p_p + \sigma_k^2 + p_k |\mathbf{h}_k \mathbf{w}_k|^2 \right]^2} \quad (16)$$

As $|\mathbf{h}_k \mathbf{w}_w|^4 \geq 0$ and $p_k^2 |\mathbf{h}_k|^4 \geq 0$, it is easy to check that $\frac{\partial \mu_k}{\partial^2 p_k} \leq 0$ and $\frac{\partial \mu_k}{\partial |\mathbf{w}_k|^2} \leq 0$,

hence the overall utility function is concave. Therefore, the game is a concave game, so it always admits at least one NE.

3.4 Uniqueness of Nash Equilibria

By setting the first derivatives to zero, we get

$$p_k = \frac{\frac{|\mathbf{h}_k|^2}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |\mathbf{g}_{k,p}|^2 p_p + \sigma_k^2 \right)}{|\mathbf{h}_k \mathbf{w}_k|^2} \quad (17)$$

$$|\mathbf{w}_k|^2 = \frac{\frac{|\mathbf{h}_k|^2}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K |\mathbf{h}_k \mathbf{w}_i|^2 p_i + |\mathbf{g}_{k,p}|^2 p_p + \sigma_k^2 \right)}{p_k |\mathbf{h}_k|^2} \quad (18)$$

In order to prove that the NE is unique, the key is that the best response function $BR_k(p_k)$ should be a standard function, which fulfills the following axioms [20]:

- 1) Positivity: for all $k \in K$, $BR_k(p_k) > 0$.
- 2) Monotonicity: if $p_k > p_k^*$, then $BR_k(p_k) > BR_k(p_k^*)$.
- 3) Scalability: for all $\eta > 1$, $\eta BR_k(p_k) > BR_k(\eta p_k)$.

Positivity: To ensure the normal operation of the system, the best response function must meet the positivity condition.

Monotonicity: If $p_k > p_k^*$, then $\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 < \sum_{i=1, i \neq k}^K p_i^* |\mathbf{h}_k \mathbf{w}_i|^2$. We can get

$$\begin{aligned}
& \frac{BR_k(p_k) - BR_k(\bar{p}_k)}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 + |g_{k,p}|^2 p_p + \sigma_k^2 \right) \\
& = \frac{\frac{|\mathbf{h}_k|^2}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 + |g_{k,p}|^2 p_p + \sigma_k^2 \right)}{\left| \mathbf{h}_k \mathbf{w}_k \right|^2} \\
& = \frac{\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 - \sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2}{\left| \mathbf{h}_k \mathbf{w}_k \right|^2} > 0
\end{aligned} \tag{19}$$

As a result, the monotonicity property is satisfied.

Scalability: for all $\eta > 1$, we have

$$\begin{aligned}
& \frac{\eta BR_k(p_k) - BR_k(\eta p_k)}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 + |g_{k,p}|^2 p_p + \sigma_k^2 \right) \\
& = \eta \frac{\frac{|\mathbf{h}_k|^2}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - \left(\sum_{i=1, i \neq k}^K \eta p_i |\mathbf{h}_k \mathbf{w}_i|^2 + |g_{k,p}|^2 p_p + \sigma_k^2 \right)}{\left| \mathbf{h}_k \mathbf{w}_k \right|^2} \\
& = \frac{(\eta-1) \left(\frac{|\mathbf{h}_k|^2}{\lambda \ln 2 \left| \tilde{\mathbf{h}}_p \right|^2} - |g_{k,p}|^2 p_p - \sigma_k^2 \right)}{\left| \mathbf{h}_k \mathbf{w}_k \right|^2}
\end{aligned} \tag{20}$$

According to the positive requirement, $\sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 \geq \sum_{i=1, i \neq k}^K p_i |\mathbf{h}_k \mathbf{w}_i|^2 + |g_{k,p}|^2 p_p + \sigma_k^2$,

so $|g_{k,p}|^2 p_p + \sigma_k^2 \leq 0$, we can get $\eta BR_k(p_k) > BR_k(\eta p_k) > 0$. Consequently, the scalability property is satisfied.

In conclusion, we can see that the best response function $BR_k(p_k)$ is a standard function, i.e., it has only one solution. Similarly, when the power allocation strategy is fixed, we can also prove that the best response function $BR_k(\mathbf{w}_k)$ is a standard function.

4 Second Order Cone Programming Solution

In this section, we solve the optimization problem (8) via a second order cone programming solution. We first make some approximation, it is clear that maximizing

is equivalent to maximizing $\sum_{k=1}^K \sqrt{p_k} |\mathbf{h}_k \mathbf{w}_k|$ [9]. By defining $\mathbf{f}_k = \sqrt{p_k} \mathbf{w}_k$, the objective function can be rewritten as $\sum_{k=1}^K |\mathbf{h}_k \mathbf{f}_k|$. Similarly, the interference power

can be expressed as $\sum_{k=1}^K \left| \left(\hat{\mathbf{h}}_p + \mathbf{e}_p \right) \mathbf{f}_k \right|^2 \leq \kappa_p$. Thus, the problem can be transformed

into

$$\begin{aligned} & \max_{p_k, f_k} \sum_{k=1}^K |\hat{\mathbf{h}}_k f_k| \\ & 0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K] \\ \text{subject to } & \sum_{k=1}^K \left(\hat{\mathbf{h}}_p + \hat{\mathbf{e}}_p \right) f_k \leq \kappa_p \end{aligned} \quad (21)$$

Then the above problem can be reformulated as a second order cone program (SOCP) problem, following similar steps in [11]. Defining $\hat{\mathbf{e}}_p = \zeta_p \hat{\mathbf{e}}_p$, the interference constraint is equivalent to $\sum_{k=1}^K \max_{\|\hat{\mathbf{e}}_p\| \leq \varepsilon_p} \left| \left(\hat{\mathbf{h}}_p + \hat{\mathbf{e}}_p \right) f_k \right| \leq \sqrt{\kappa_p}$. Using the triangle inequality and the Cauchy-Schwarz inequality with $\|\hat{\mathbf{e}}_p\| \leq \varepsilon_p$, it follows that

$$\sum_{k=1}^K \left| \hat{\mathbf{h}}_p f_k + \hat{\mathbf{e}}_p \frac{f_k}{\zeta_p} \right| \leq \sum_{k=1}^K \left(\left| \hat{\mathbf{h}}_p f_k \right| + \left| \hat{\mathbf{e}}_p \frac{f_k}{\zeta_p} \right| \right) \leq \sum_{k=1}^K \left(\left| \hat{\mathbf{h}}_p f_k \right| + \varepsilon_p \left\| \frac{f_k}{\zeta_p} \right\| \right) \quad (22)$$

where the equality is achieved when $\hat{\mathbf{e}}_p = \varepsilon_p e^{j\phi_p} \frac{f_k \|\zeta_p\|}{\zeta_p \|f_k\|}$, $\phi_p = \angle \left(\hat{\mathbf{h}}_p f_k \right)$.

So it is equivalent to

$$\sum_{k=1}^K \max_{\|\hat{\mathbf{e}}_p\| \leq \varepsilon_p} \left| \left(\hat{\mathbf{h}}_p + \hat{\mathbf{e}}_p \right) f_k \right| = \sum_{k=1}^K \left(\left| \hat{\mathbf{h}}_p f_k \right| + \varepsilon_p \left\| \frac{f_k}{\zeta_p} \right\| \right) \leq \sqrt{\kappa_p} \quad (23)$$

Note that the arbitrary phase rotation of f_k does not change the value of the objective function or the constraints. Therefore, we can assume that f_k , \mathbf{h}_k , \mathbf{h}_p have the same phase, i.e.,

$$\operatorname{Re}\{\mathbf{h}_k f_k\} \geq 0, \operatorname{Im}\{\mathbf{h}_k f_k\} = 0, \operatorname{Im}\{\hat{\mathbf{h}}_p f_k\} = 0 \quad (24)$$

By combining (21), (23) and (24), the optimization problem can be converted into a SOCP problem as

$$\begin{aligned} & \max_{p_k, f_k} \sum_{k=1}^K |\hat{\mathbf{h}}_k f_k| \\ & 0 \leq p_k \leq p_{k,\max}, \forall k \in [1, K] \\ \text{subject to } & \sum_{k=1}^K \left(\left| \hat{\mathbf{h}}_p f_k \right| + \varepsilon_p \left\| \frac{f_k}{\zeta_p} \right\| \right) \leq \sqrt{\kappa_p} \\ & \operatorname{Im}\{\hat{\mathbf{h}}_p f_k\} = 0 \end{aligned} \quad (25)$$

The joint beamforming and power allocation problem (25) is a convex optimization problem with respect to f_k [15]. This optimization problem is very

difficult to solve, we will resort to numerical simulations to illustrate the convergence property of the sum utility of SUs.

5 Simulations

Computer simulation results are presented to evaluate the performance of the proposed algorithms under Rayleigh flat fading channels in this section. It is assumed that the SBS has imperfect CSI from PU, and the sum utility obtained by a SOCP

approximation algorithm [21] is evaluated. The estimation error is set to $\varepsilon_p^2 = \|\hat{h}_p\|^2$.

For simplicity, we consider the CR network with four SUs and a single PU.

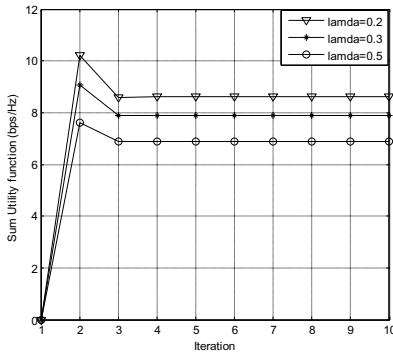


Fig. 2. Sum utility of SUs for different λ

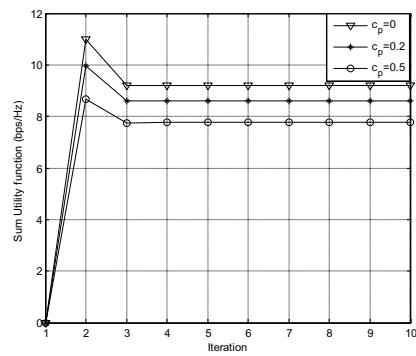


Fig. 3. Sum utility of SUs for different c_p

In the following results, we choose the noise power $\sigma_k^2 = 3e-3W$, the PU transmit power $p_k = 0.1W$, the SU maximum transmit power $p_{\max} = 10W$, the interference threshold $\kappa_p = 100$, respectively. First, in Fig.2 we show the sum utility of SUs versus the pricing factor λ when the interference to PU caused by SUs is restricted, with $c_p = 0.2$. As observed from Fig. 2, the sum utility of SUs decrease as λ increases and can converge to a locally optimal value. In Fig.3, we investigate how the total the sum utility of SUs change with the value of the uncertainty parameter increases, with $\lambda = 0.3$. Clearly, the sum utility of SUs decrease with the value of the c_p increases.

In Fig. 4, the uncertainty parameter is set to $c_p = 0, 0.05, 0.2, 0.5$, respectively. When $c_p = 0$, the CSI is perfect. In addition, the noise power and the interference threshold between SUs and the PU are set to 1. Due to the CSI uncertainty, the sum utility is lower than that under perfect CSI, and as the value of the uncertainty parameter increases, the sum utility becomes less. The sum utility of SUs under imperfect CSI converge with the increase of transmission power constraint of SUs.

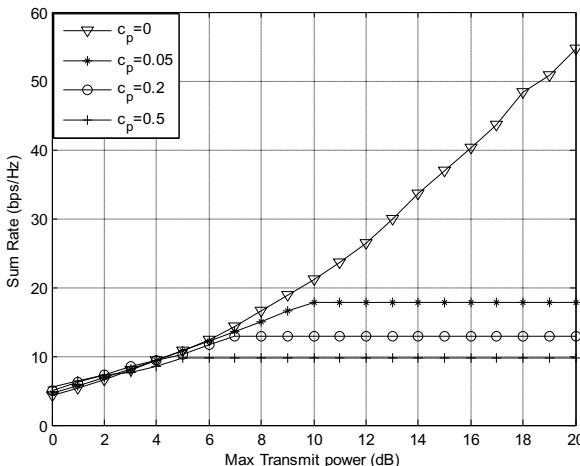


Fig. 4. Sum utility under perfect and imperfect CSI

6 Conclusion

In this paper, we investigate the problem of joint beamforming and power allocation in a cognitive MIMO system via game theory. Subject to the peak transmission power constraints of SUs as well as the interference constraints of PU, a proper utility function with pricing characterizes the transmission of all SUs. Imperfect CSI between the SBS and the PU is considered, and an ellipsoid model was adopted to describe the CSI uncertainty. We study the existence and uniqueness properties of the NE of the game. Simulation results showed the effectiveness of the proposed algorithm and the convergence property of the sum utility of SUs.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (61172055) and the Foundation of Department of Education of Guangxi Province (201202ZD046).

References

1. Mitola, J.: Cognitive radio for flexible mobile multimedia communication. In: Proc. IEEE Int. Workshop on Mobile Multimedia Commun., San Diego, pp. 3–10 (1999)
2. Gesbert, D., Shafi, M., Shiu, D.S., Smith, P.J., Naguib, A.: From theory to practice: an overview of MIMO space-time coded wireless systems. *IEEE J. Sel. Areas Commun.* 21(3), 281–302 (2003)
3. Kim, S.J., Giannakis, G.B.: Optimal resource allocation for MIMO ad hoc cognitive radio networks. *IEEE Trans. Inf. Theory.* 57(5), 3117–3131 (2011)
4. Zhang, Y.J.A., So, A.M.C.: Optimal spectrum sharing in MIMO cognitive radio networks via semidefinite programming. *IEEE J. Sel. Areas Commun.* 29(2), 362–373 (2011)
5. Haykin, S.: Cognitive radio: Brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.* 23(2), 201–220 (2005)

6. Si, P.B., Ji, H., Yu, F.R., Leung, V.C.M.: Optimal cooperative internetwork spectrum sharing for cognitive radio systems with spectrum pooling. *IEEE Trans. Veh. Tech.* 59(4), 1760–1768 (2010)
7. Zhang, L., Liang, Y., Xin, Y.: Joint beamforming and power allocation for multiple access channels in cognitive radio networks. *IEEE J. Sel. Areas Commun.* 26(1), 38–51 (2008)
8. Cumanan, K., Krishna, R., Musavian, L., Lambotharan, S.: Joint beamforming and user maximization techniques for cognitive radio networks based on branch and bound method. *IEEE Trans. Wireless Commun.* 9(10), 3082–3092 (2010)
9. Zhang, L., Liang, Y.C., Xin, Y., Poor, H.V.: Robust cognitive beamforming with partial channel state information. *IEEE Trans. Wireless Commun.* 8(8), 4143–4153 (2009)
10. Zheng, G., Wong, K.-K., Ottersten, B.: Robust cognitive beamforming with bounded channel uncertainties. *IEEE Trans. Signal Process.* 57(12), 4871–4881 (2009)
11. Wang, J.H., Scutari, G., Palomar, D.P.: Robust MIMO cognitive radio via game theory. *IEEE Trans. Signal Process.* 59(3), 1183–1201 (2011)
12. Anandkumar, A.J.G., Anandkumar, A., Lambotharan, S., Chambers, J.A.: Robust rate-maximization game under bounded channel uncertainty. *IEEE Trans. Veh. Tech.* 60(9), 4471–4486 (2011)
13. Parsaeefard, S., Sharafat, A.R., van der Schaar, M.: Robust equilibria in additively coupled games in communications networks. In: IEEE Global Telecommunications Conference (GLOBECOM), pp. 1–6 (2011)
14. Zhao, F., Zhang, J.Y., Chen, H.B.: Joint Beamforming and power allocation for multiple primary users and secondary users in cognitive MIMO systems via game theory. *KSII Trans. Internet Inf.* 7(6), 1379–1397 (2013)
15. Zhao, F., Li, B., Chen, H.B., Lv, X.Z.: Joint beamforming and power allocation for cognitive MIMO systems under imperfect CSI based on game theory. *Wireless Pers. Commun.* 73(3), 679–694 (2013)
16. Osborne, M.J., Rubinstein, A.: A course in game theory. MIT Press, Cambridge (1999)
17. Wang, J.H., Payaró, M.: On the robustness of transmit beamforming. *IEEE Trans. Signal Process.* 58(11), 5933–5938 (2010)
18. Parsaeefard, S., Sharafat, A.R.: Robust distributed power control in cognitive radio networks. *IEEE Trans. Mobile Comput.* 12(4), 609–620 (2012)
19. Fudenberg, D., Tirole, J.: Game theory. MIT Press, Cambridge (1991)
20. Louni, A., Khalaj, B.H.: Distributed beam-forming and power control in multi-relay underlay cognitive radio networks: a game-theoretical approach. In: 6th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), Osaka, pp. 71–75 (2011)
21. Wang, F., Wang, W.: Robust beamforming and power control for multiuser cognitive radio network. In: IEEE Global Telecommunications Conference (GLOBECOM), Miami, pp. 1–5 (2010)

Channel Allocation in Sociability-Assisted Cognitive Radio Networks Using Semi-definite Programming

Zhen Li¹, Tao Jing¹, Yan Huo¹, Lili Pan², and Wei Zhou¹

¹ School of Electronics and Information Engineering, Beijing Jiaotong University, China

² School of Science, Beijing Jiaotong University, China

Abstract. Channel allocation is an important part of cognitive radio(CR), and has received intensive studies in recent years. Previous works of channel allocation haven't taken the social relationship between primary users(PUs) and secondary users(SUs) into consideration. As a result, these allocation schemes ignore the willingness of CR users and may not adapt a personalized environment. Moreover, the traditional channel allocation schemes do not have the capability to protect the network performance from being hurt by some ill-behaved nodes. To tackle this challenge, we first introduce the social relationship into channel allocation and make some definitions about the social attributes. Then, we propose a Sociability-Assisted Channel Allocation Scheme(SACAS) which takes both the social relationship and the channel condition into consideration. Then, we use semi-definite programming(SDP) to obtain the optimal solution of SACAS. The simulation results show the superiority of SACAS over traditional algorithms.

Keywords: Sociability-assisted channel allocation, semi-definite programming, cognitive radio.

1 Introduction

With the rapid growth of wireless devices and applications, the frequency channels have become scarce and expensive resources. Nowadays, the wireless networks are regulated by a fixed channel assignment policy, i.e., the channels are assigned to license holders on a long term basis by the government. This policy causes a concentrated use on certain portions of the channels, while a large number of the channels remain unutilized. Therefore, cognitive radio has been put forward as a promising technology to solve this problem in an opportunistic way [2, 3, 12, 15, 17, 28]. Typically, cognitive radio networks have two parts of users: primary users(PUs) and secondary users(SUs). PUs have right to use their licensed channels, while SUs can change their transmitter parameters to opportunistically operate on licensed channels provided by PUs, as long as they don't cause harmful interference. The main technical parts of cognitive radio include: spectrum sensing, spectrum management, spectrum mobility and spectrum sharing [1].

The aim of spectrum management is capturing the best available spectrum to achieve the maximum network throughput. Channel allocation is a very important way of spectrum management. Various methodologies such as graph theory [23], economics-based auction [33], game theory [31] and etc, have been applied in channel allocation. However, these methods rarely consider the social relationship between PUs and SUs. Therefore, they can't adapt a personalized environment. For example, in a wireless local area

network, the devices which held by people have the willingness and the spectrum management here is somewhat a social behavior. In this case, even if some SUs have sensed the availability of the channels owned by some PUs, those PUs may not permit the SUs to use their channels because they are not acquaintances or the SUs have bad reputation. On the other hand, unfamiliar SUs and dishonest SUs are more likely to do harm to the network performance, while the sociability-assisted cognitive radio networks can protect the network from getting damaged by those malicious SUs.

Social network, exploring the social relationship between network nodes and the social attributes of large networks, is becoming a research hotspot in the recent years [6, 7, 9, 10, 20, 21, 26] and has been applied in wireless Ad hoc network [14], peer-to-peer network [18] and intrusion detection system [25]. In this paper, we first establish a sociability-assisted CRN and quantify several social attributes between PUs and SUs. Then we use a social-based filtration algorithm to remove some undesirable SUs. At last, we make an allocation both considered the social relationship and the channel condition. The main contributions of this paper are summarized as follows:

- We introduce the social relationship to channel resource allocation in cognitive radio, and quantify three social attributes: familiarity, integrity and priority. The analysis of these parameters effects the result of the allocation.
- We turn the allocation scheme into a semi-definite programming(SDP) problem, and use the interior point algorithm to obtain the optimal solution in polynomial time.

The rest of the paper is organized as follows. Section 2 presents the related work while Section 3 describes the network model and the definition of the social attributes. The sociability-assisted channel allocation scheme(SACAS) is detailed in Section 4. Section 5 evaluates the performance of the proposed scheme and Section 6 concludes the paper.

2 Related Work

In this section, we first review the most related work of channel allocation. Then, we present existing literatures leading the social relationship in cognitive radio.

Graph theory [4, 24, 32] has been applied in channel allocation and this method abstracts the topological structure of CRNs into a undirected graph. The goal is to maximize the number of channels that can be occupied by SUs. Some economic tools, such as auction [5, 11, 29, 34], has also been used, by which PUs can gain benefits through leasing idle channels while maximizing the utility function of SUs. Generally, these two methods are applied in the centralized networks. Game theory [22, 27, 31] has been introduced in the distributed cases. CR users aimed at maximizing their own utility function, employ as players to change these strategies to achieve equilibrium. And, as described in Section 1, none of them take the social relationship into account.

On the other hand, to the best of our knowledge, there only exist a few literatures leading the social relationship in other parts of cognitive radio. Li *et al.* [16] introduces a recommendation system into CR and analyzes the channel preference propagation in

the corresponding CR users. Güven *et al.* [8] proposes some social relations and uses them to make a social-aware cooperative sensing scheme. Liu *et al.* [19] considers a social metric named incentive factor to appraise the level that the PUs are willing to permit the SUs to share the channels. As claimed earlier, there are no schemes that using the social relationship in channel allocation, which is the focus of this paper.

Notation: Upper-case bold letters denote matrices. $\text{rank}(\cdot)$, $\text{Tr}(\cdot)$, and $|\cdot|$ denote the rank of a matrix, trace and determinant, respectively. $\text{Diag}(a)$ denotes a diagonal matrix with diagonal elements given in a . \mathbb{F} means the feasible region while r_i means the interior point set of \mathbb{F} . \mathbb{R} presents the set of real numbers and \mathbb{S}_+ means the set of positive semi-definite matrices. $\text{vec}(\mathbf{A})$ means the isomorphic mapping of matrix A . $\mathbf{X} \succeq 0$ means matrix \mathbf{X} is a positive semi-definite matrix.

3 Network Model and Parameter Definition

3.1 Network Model

In this paper, we consider an infrastructure-based CRN including PUs and SUs, where SUs are allowed to use the channels provided by PUs if the channels are idle. Here, we assume SUs can sense the channels accurately. Multiple terminals (PUs and SUs) use the Common Control Channel(CCC) to communicate with a base station which has the function of channel allocation. Without loss of generality, we assume that there are M PUs and N SUs in the type of the CRNs. The set of PUs and SUs are denoted by $\mathcal{M} = \{1, 2, \dots, M\}$ and $\mathcal{N} = \{1, 2, \dots, N\}$, respectively. M orthogonal channels are allocated to M primary users, biuniquely. Here, we also assume each SU only have one antenna and occupy one channel in a time slot.

3.2 Parameter Definition

As mentioned above, SUs and PUs own the social relationship and here we use three social attributes: familiarity, integrity and priority, to comprehensively measure the social relationship between SUs and PUs. The meaning of the three parameters is as follows:

Definition 1(familiarity). Familiarity, denoted by a_{ijt} , is a parameter described the degree of familiarity of PU_i and SU_j in slot t . We assume that our network model is slotted which is a common assumption in CRNs. And,

$$a_{ijt} = \frac{\min\{\sum_{n=1}^t \alpha_{ijn}, \max\}}{\max}$$

In this formulation, α_{ijn} is an integer decision variable that indicate if PU_i has allocated its channel to SU_j ($\alpha_{ijn}=1$) or not ($\alpha_{ijn}=0$) in slot n . It is obviously that the PUs are willing to share its spectrum with the SUs who have high a_{ijt} because of their successful cooperation in the past.

Definition 2(integrity). Integrity, denoted by b_{ijt} , is a parameter described the degree of credibility of PU_i and SU_j in slot t. And,

$$b_{ijt} = \frac{\min\{w_c \sum_{n=1}^t \gamma_{ijn}, \max\}}{\max}$$

In this formulation, γ_{ijn} is an integer decision variable that indicate if SU_j does harm to PU_i ($\gamma_{ijn}=1$) (e.g. SU_j has not withdrawn when PU_i comes back) or not ($\gamma_{ijn}=0$) in slot n. In order to protect the PUs, we make $w_c > 1$ to increase the intensity of punishment.

Definition 3(priority). Priority, denoted by c_j , is a parameter described the degree of priority. In a sociability-assisted CRN, the SUs usually have different priority. For instance, in a small company, the managers and employees compose a set of SUs. If they want to compete to use channels provided by PUs, managers will have high priority while employees will have low priority. And,

$$c_j = \begin{cases} 1 & \text{if } SU_j \text{ has high priority} \\ 0 & \text{if } SU_j \text{ has low priority} \end{cases}$$

This three social attributes measure the social relationship of PUs and SUs in sociability-assisted CRN. Furthermore, we will analysis and process these attributes to affect the channel allocation in the next section.

4 Sociability-Assisted Channel Allocation Scheme

In this section, we study the social-assisted channel allocation scheme(SACAS). The allocation scheme is supposed to conform to the social attributes, i.e., only the eligible SUs which achieve the threshold explained in the next subsection can participate in the allocation. In addition, not only the social relationship but also the channel condition should be taken into account, which means the channels SUs needed ought to match the channels PUs offered. Based on the above consideration, we will describe our scheme in details in the following subsections.

4.1 Social-Based Filtration

In this subsection, we pay our attentions to filtrate the eligible SUs for the allocation. Before the filtration starts, all the PUs use the CCC to send the provided channels to the BS, while all the SUs send their required channels. Here we assume the BS has the perfect knowledge of the social attributes of all SUs and PUs, then the filtration begins. Firstly, we let $a_{ijt} = 1$ and $b_{ijt} = 0$ for the SUs with $c_j = 1$ to make sure the high priority SUs can get the channels they required. Secondly, we set a threshold η to check the SUs integrity values. If the values exceed η , we will refuse the SUs to take part in the allocation. In this way, we can protect the network performance from the collision caused by some irresponsible SUs. At last, we make a summation for the familiarity values for SU_j to all the PUs, denoted by $a_j = \frac{\sum_{i=1}^M a_{ijt}}{M}$. And we also set a

Algorithm 1. Social-based Filtration Algorithm

```

for  $j = 1 : N$  do
  if  $c_j$  then
     $a_{ijt} = 1$  and  $b_{ijt} = 0$ 
  end if
end for
for  $i = 1 : M$  do
  for  $j = 1 : N$  do
    if  $b_{ijt} > \eta$  then
       $\mathcal{N} \leftarrow \mathcal{N} \setminus SU_j$ 
    end if
  end for
end for
for  $i = 1 : M$  do
  for  $j = 1 : N$  do
    Calculate  $a_j = \frac{\sum_{i=1}^M a_{ijt}}{M}$ 
    if  $a_j < \theta$  then
       $\mathcal{N} \leftarrow \mathcal{N} \setminus SU_j$ 
    end if
  end for
end for

```

threshold θ to prove only some SUs achieved θ can attend the allocation. After a series of these processing, only the SUs with good social attributes can continue to participate the scheme and the algorithm is as follows:

We will describe the allocation scheme in the next subsection.

4.2 Allocation Scheme

In this subsection, we will first make a mathematical description about our allocation scheme. Then, the mathematical problem will be transformed into a semi-definite programming problem. At last, we will use the interior point algorithm to solve it.

Mathematical Description. Before beginning the mathematical description, we would like state two principles about the allocation. Firstly, as mentioned before, the allocation between the PUs and the SUs follows a one-to-one model, i.e., one PU offers one channel and one SU accepts one channel. In other words, the allocation has to avoid the collision between the PUs and the SUs. There are two cases about the collision: i) a certain channel from PU_i may allocated to more than one SU. ii) a certain SU may get more than one channel from different PUs. Besides, we should both consider the channel condition and the social relationship. The channel condition means whether the provided channels match the required channels or not. On the other hand, the social attributes should also effect the allocation. Though we have already get rid off some unsatisfactory SUs, the SUs which achieved the minimum requirements but had different social attributes should be treated differently. For example, the passing mark is 60 in

an exam, but there are obvious differences between two students who got 80 marks and 100 marks.

Let \mathbf{P} be the outcome matrix, and the element p_{ij} in \mathbf{P} means the allocation result,

$$p_{ij} = \begin{cases} 1 & \text{if } SU_j \text{ gets the channel provided by } PU_i \\ 0 & \text{otherwise} \end{cases}$$

Let \mathbf{Q} be the allocation matrix, the element q_{ij} in \mathbf{Q} , denoted by $q_{ij} = \sigma_{ij} + a_{ijt} - b_{ijt}$, means the utility value of the successful allocation between PU_i and SU_j . And σ_{ij} is given as

$$\sigma_{ij} = \begin{cases} 1 & \text{if the provided and the needed channel matches} \\ 0 & \text{otherwise} \end{cases}$$

We can clearly see that the allocation matrix conforms to the second principle we mentioned before. Then we can turn the utility function of the allocation into maximizing the value of $\text{Tr}(\mathbf{P} \bullet \mathbf{Q})$ to make sure the eligible SUs can obtain their required channels.

With the purpose of avoiding the collision, i.e., the first principle, we have to add some constraint conditions for the maximization problem. That is,

$$\mathbf{e}_1^T \bullet \mathbf{P}_j \leq 1, j = \{1, 2, \dots, N\} \quad (1)$$

$$\mathbf{e}_2^T \bullet \mathbf{P}_i^T \leq 1, i = \{1, 2, \dots, M\} \quad (2)$$

In the above expressions, \mathbf{e}_1^T and \mathbf{e}_2^T are M- and N- dimension unit column vectors, respectively. \mathbf{P}_j and \mathbf{P}_i^T represents the j-column vector and i-row vector of the outcome matrix \mathbf{P} , respectively. So, Eq.(1) represents the channel a certain SU allocated is no more than one. And, Eq.(2) represents the channel a certain PU provided can only be occupied by one SU.

We rewrite the maximization problem into the standard form which is as follows:

$$\begin{aligned} & \max \text{Tr}(\mathbf{P} \bullet \mathbf{Q}) \\ \text{s.t. } & \mathbf{e}_1^T \bullet \mathbf{P}_j \leq 1, j = \{1, 2, \dots, N\} \\ & \mathbf{e}_2^T \bullet \mathbf{P}_i^T \leq 1, i = \{1, 2, \dots, M\} \\ & p_{ij} \in \{0, 1\} \end{aligned} \quad (3)$$

It can be easily found that this problem is NP-hard and we will use semi-definite programming to establish a polynomial time algorithm to get the optimal solution about this problem.

Problem Conversion and Interior Point Algorithm. We will solve this problem in two steps: i) transforming Eq.(3) into a semi-definite programming problem. ii) using a polynomial time algorithm named the interior point algorithm to solve the SDP problem.

STEP1:

Let matrix $\mathbf{V} = \text{Diag}(q_{11}, q_{21}, \dots, q_{m1}, q_{12}, \dots, q_{mn})$ and let $\text{vec}(\mathbf{P}) = (p_{11}, p_{21}, \dots, p_{m1}, p_{12}, \dots, p_{mn})^T$. We can transform the objective function into

$$\max \text{vec}(\mathbf{P})^T \mathbf{V} \text{vec}(\mathbf{P}) \quad (4)$$

We also make some transformations about the constraint conditions. That is

$$\mathbf{u}_i^T \bullet \text{vec}(\mathbf{P}) \leq 1, i = \{1, 2, \dots, N\} \quad (5)$$

$$\mathbf{v}_j^T \bullet \text{vec}(\mathbf{P}) \leq 1, j = \{1, 2, \dots, M\} \quad (6)$$

where for $i = 1$,

$$\mathbf{u}_1 = [\underbrace{1, 0, \dots, 0}_j, \underbrace{1, 0, \dots, 0}_j, \dots, \underbrace{1, 0, \dots, 0}_j]$$

the number 1 rotate from $i = 1$ to $i = N$. For $j = 1$,

$$\mathbf{v}_1 = [\underbrace{1, 1, \dots, 1}_i, \underbrace{0, 0, \dots, 0}_i, \dots, \underbrace{0, 0, \dots, 0}_i]$$

and the number 1 rotate from $j = 1$ to $j = M$.

After the transformation of the above equations, the maximization problem can be written as:

$$\begin{aligned} & \max \text{vec}(\mathbf{P})^T \mathbf{V} \text{vec}(\mathbf{P}) \\ \text{s.t. } & \mathbf{u}_i^T \bullet \text{vec}(\mathbf{P}) \leq 1, i = \{1, 2, \dots, N\} \\ & \mathbf{v}_j^T \bullet \text{vec}(\mathbf{P}) \leq 1, j = \{1, 2, \dots, M\} \\ & p_i \in \{0, 1\} \end{aligned} \quad (7)$$

where p_i is the element of $\text{vec}(\mathbf{P})$. We can easily find that \mathbf{V} is a symmetric matrix because it's a diagonal matrix which satisfies the restrict of SDP. However, this problem is still not a SDP problem because of two reasons. i) the objective function is a quadratic form. ii) $p_i \in \{0, 1\}$ is not a standard form of SDP. Therefore, we will make a relaxation to solve these problems.

Let $\mathbf{r} = 2 \cdot \text{vec}(\mathbf{P}) - \mathbf{e}$, $\mathbf{r}^T = (\mathbf{r}_1^T, 1)$, $\mathbf{e} = \{1, 1, \dots, 1\}^T$. Now we relax $\mathbf{u}^T \bullet \text{vec}(\mathbf{P}) \leq 1$ to $(\mathbf{u}^T \bullet \text{vec}(\mathbf{P}))^2 \leq 1$, and we also do the same relaxation to \mathbf{v}^T . Hereinafter, we omit the derivation of \mathbf{v}^T and the vector notation for brevity. Then we can write the problem as follows:

$$\begin{aligned} & \max \mathbf{r}^T \mathbf{H} \mathbf{r} + d \\ \text{s.t. } & \mathbf{r}^T \mathbf{G}_i \mathbf{r} \leq 1 - n_i^2 \\ & r_i \in \{-1, 1\} \end{aligned} \quad (8)$$

where r_i is the element of r . $\mathbf{H} = 0.25 \begin{pmatrix} \mathbf{V} & \mathbf{Ve} \\ \mathbf{e}^T \mathbf{V} & 0 \end{pmatrix}$, $\mathbf{G}_i = 0.25 \begin{pmatrix} u_i u_i^T & u_i u_i^T \mathbf{e} \\ \mathbf{e}^T u_i u_i^T & 0 \end{pmatrix}$, $d = 0.25 \mathbf{e}^T \mathbf{V} \mathbf{e}$, $n_i = 0.25 \mathbf{e}^T u_i u_i^T \mathbf{e}$. If we let $\mathbf{R} = rr^T$, Eq.(8) is equivalent to

$$\begin{aligned} & \max \operatorname{Tr}(\mathbf{H} \bullet \mathbf{R}) + d \\ \text{s.t. } & \operatorname{Tr}(\mathbf{G}_i \bullet \mathbf{R}) \leq 1 - n_i, i = \{1, 2, \dots, M\} \\ & \mathbf{R}_{jj} = 1, j = \{1, 2, \dots, M + N + 1\} \\ & \mathbf{R} \succeq 0 \\ & \operatorname{rank}(\mathbf{R}) = 1. \end{aligned} \quad (9)$$

Here, we make a rank one relaxation to remove the constraint of $\operatorname{rank}(\mathbf{R}) = 1$, then we can find Eq.(9) is a SDP problem, since all the matrices, that is, $\mathbf{R}, \mathbf{G}, \mathbf{H}$, both in the objective function and the constraints are symmetric matrices. [30] proves there exists a globally optimal solution of Eq.(9) which equals the globally optimal solution of Eq.(3), the primal problem. Until now, STEP 1 finish.

STEP2: Though we know there exists a globally optimal solution of Eq.(9), how to get it is still a question. In order to seek out the optimal solution, we first structure a penalty function $B(\cdot)$ and the penalty function satisfies two point: i) $B(x) \geq 0, \forall x \in ri(\mathbb{F})$. ii) when x approaches the boundary of \mathbb{F} , $B(x) \rightarrow +\infty$. We choose the following penalty function:

$$\mu \log |\mathbf{H} \bullet \mathbf{R}| \quad (10)$$

and the problem turns into:

$$\begin{aligned} & \max \operatorname{Tr}(\mathbf{H} \bullet \mathbf{R}) + d - \mu \log |\mathbf{H} \bullet \mathbf{R}| \\ \text{s.t. } & \operatorname{Tr}(\mathbf{G}_i \bullet \mathbf{R}) \leq 1 - n_i, i = \{1, 2, \dots, M\} \end{aligned} \quad (11)$$

We omit some constraints for brevity. The purpose of the penalty function is to force the feasible solution remains in the interior of the feasible solution set. Then we use the lagrange multiplier method to derive the KKT conditions of Eq.(11) as follows:

$$\begin{aligned} & \operatorname{Tr}(\mathbf{G}_i \bullet \mathbf{R}) = 1 - n_i, i = \{1, 2, \dots, M\}, \mathbf{R} \succ 0 \\ & \sum_{i=1}^m t_i + \mathbf{S} = \mathbf{H}, \mathbf{S} \succ 0 \\ & \mathbf{R}\mathbf{S} = 0 \end{aligned} \quad (12)$$

where $\mathbf{R} \in \mathbb{S}_+^{m \times n+1}$ and $(t, \mathbf{S}) \in \mathbb{R}^m \times \mathbb{S}_+^{m \times n+1}$ are the variable matrices of the primal problem and the dual problem, respectively. The significance of the KKT conditions is that only the feasible solution which satisfies it can be the globally optimal solution. Next we choose a initial point (R^0, t^0, S^0) from a set of points that satisfy the KKT conditions. Then we use the interior point algorithm to find the optimal solution. For more details of the interior point algorithm, readers can read [13].

5 Simulation

In this section, simulations are performed to access the performance of SACAS using CVX.

We first conduct a simulation to prove our scheme can get the optimal solution. We compare our scheme with the greedy algorithm which often gets a near-optimal solution. The CRN is formed in which all PUs and SUs are randomly distributed. The number of PUs and SUs varies from 5 to 25 at a step size of 5, we choose $\eta=0.4$ and $\theta=0.5$. The simulation results are presented in Fig. 1.

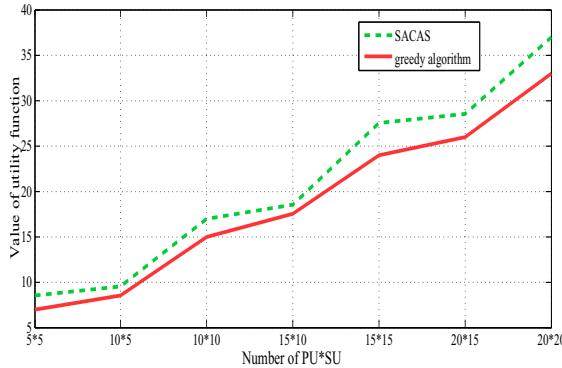


Fig. 1. Value of utility function vs. the number of PUs*SUs.

We can see from Fig. 1 that our scheme performs better than the greedy algorithm. Moreover, we also compare the solution of our scheme with the optimal solution in Table 1.

Table 1. The differential between SACAS and the optimal solution

SU*PU	10 * 10	15 * 10	15 * 15	20 * 15	20 * 20
differential	$8.7e^{-9}$	$1.5e^{-8}$	$6.1e^{-9}$	$1.3e^{-8}$	$1.3e^{-8}$

From Table 1, we can clearly see that there is almost no difference between the solution of our scheme with the optimal solution. That is the reason we express the solution of SACAS as the optimal solution.

Next, we add some dishonest SUs which have low value of integrity. These SUs make false reports about their required channels to get benefits: i) the right to use the channels; 2) enhancing the value of familiarity. However, if the dishonest SUs participate in the allocation, it will do harm to the utility. Without loss of generality, we set the number of PUs and SUs to 5 and 10, respectively. Then we increase the number of the dishonest SUs one by one. The simulation results are presented in Fig. 2 as follows:

We can see from Fig. 2 that our scheme can protect the performance of allocation from the dishonest nodes.

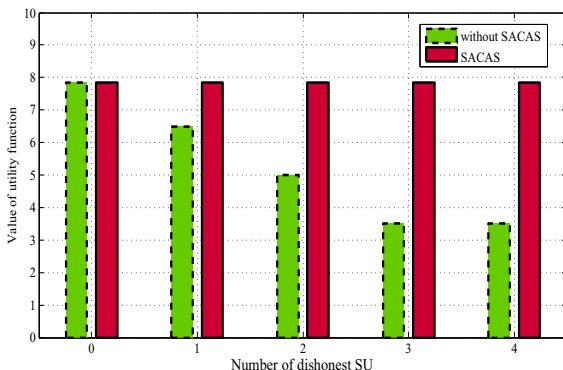


Fig. 2. Value of utility function vs. the number of dishonest SUs.

6 Conclusion

This paper brings the idea of the social relationship to channel allocation in CRNs. The proposed channel allocation scheme named SACAS takes not only whether the channels provided by the PUs match the channel needed by the SUs or not, but also whether the social relations between the PUs and the SUs are good enough or not into consideration. We present a detailed analysis using semi-definite programming on SACAS and employ simulation study to prove our analysis. Our future research is depicted as follows:

- We will drop the assumption of one PU can only offer one channel while one SU can only use one, and build a network model in which the PU can provide a set of channels while the SU can also use a set of channels, similarly.
- Due to the CCC in CRNs may exist temporarily, or may never exist, we will employ a distributed SACAS instead of the centralized one.

Acknowledgment. The authors would like to thank the support from the National Natural Science Foundation of China (Grant No.61172074, 61272505 and 61371069) and the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No.20130009110015).

References

1. Akyildiz, I.F., Lee, W.Y., Vuran, M.C., Mohanty, S.: Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Computer Networks Journal Elsevier 50, 2127–2159 (2006)
2. Cai, Z., Duan, Y., Bourgeois, A.G.: Delay efficient opportunistic routing in asynchronous multi-channel cognitive radio networks. Journal of Combinatorial Optimization, 1–21 (2013)
3. Cai, Z., Ji, S., He, J., Wei, L., Bourgeois, A.G.: Distributed and asynchronous data collection in cognitive radio networks with fairness consideration. TPDS (2014)

4. Cao, L., Zheng, H.: Distributed spectrum allocation via local bargaining. In: SECON, pp. 475–486 (2005)
5. Dong, M., Sun, G., Wang, X., Zhang, Q.: Combinatorial auction with time-frequency flexibility in cognitive radio networks. In: 2012 Proceedings IEEE INFOCOM, pp. 2282–2290 (2012)
6. Falk, H.: Applications, architectures, and protocol design issues for mobile social networks: A survey. Proceedings of the IEEE 99(12), 2125–2129 (2011)
7. Girvan, M., Newman, M.E.: Community structure in social and biological networks. Proceedings of the National Academy of Sciences 99(12), 7821–7826 (2002)
8. Guven, C., Bayhan, S., Alagoz, F.: Effect of social relations on cooperative sensing in cognitive radio networks. In: 2013 First International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 247–251. IEEE (2013)
9. Hui, P., Crowcroft, J., Yoneki, E.: Bubble rap: Social-based forwarding in delay-tolerant networks. IEEE Transactions on Mobile Computing 10(11), 1576–1589 (2011)
10. Hui, P., Yoneki, E., Chan, S.Y., Crowcroft, J.: Distributed community detection in delay tolerant networks. In: Proceedings of 2nd ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture, p. 7. ACM (2007)
11. Jing, T., Zhao, C., Xing, X., Huo, Y., Li, W., Cheng, X.: A multi-unit truthful double auction framework for secondary market. In: 2013 IEEE International Conference on Communications (ICC), pp. 2817–2822 (June 2013)
12. Jing, T., Zhu, S., Li, H., Cheng, X., Huo, Y.: Cooperative relay selection in cognitive radio networks. In: IEEE INFOCOM Mini-Conference (2013)
13. Karmarkar, N.: A new polynomial-time algorithm for linear programming. In: Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing, pp. 302–311. ACM (1984)
14. Katsaros, D., Dimokas, N., Tassiulas, L.: Social network analysis concepts in the design of wireless ad hoc network protocols. IEEE Network 24(6), 23–29 (2010)
15. Li, H., Cheng, X., Li, K., Xing, X., Jing, T.: Utility-based cooperative spectrum sensing scheduling in cognitive radio networks. In: IEEE INFOCOM Mini-Conference (2013)
16. Li, H., Song, J., Chen, C.F., Lai, L., Qiu, R.: Behavior propagation in cognitive radio networks: A social network approach. IEEE Transactions on Wireless Communications (2014)
17. Li, W., Cheng, X., Jing, T., Xing, X.: Cooperative multi-hop relaying via network formation games in cognitive radio networks. In: IEEE INFOCOM (2013)
18. Lin, K.J., Wang, C.P., Chou, C.F., Golubchik, L.: Socionet: A social-based multimedia access system for unstructured p2p networks. IEEE Transactions on Parallel and Distributed Systems 21(7), 1027–1041 (2010)
19. Liu, L., Chen, H., Deng, X., Qin, Y.: Socially inspired spectrum sharing in cognitive radio networks. In: 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS), pp. 850–853. IEEE (2010)
20. Mei, A., Stefa, J.: Swim: A simple model to generate small mobile worlds. In: IEEE INFOCOM 2009, pp. 2106–2113. IEEE (2009)
21. Newman, M.E., Girvan, M.: Finding and evaluating community structure in networks. Physical Review E 69(2), 026113 (2004)
22. Niyato, D., Hossain, E., Han, Z.: Dynamics of multiple-seller and multiple-buyer spectrum trading in cognitive radio networks: A game-theoretic modeling approach. IEEE Transactions on Mobile Computing 8(8), 1009–1022 (2009)
23. Wang, J., Huang, Y., Jiang, H.: Improved algorithm of spectrum allocation based on graph coloring model in cognitive radio. In: WRI International Conference on Communications and Mobile Computing, CMC 2009, vol. 3, pp. 353–357 (January 2009)
24. Wang, W., Liu, X.: List-coloring based channel allocation for open-spectrum wireless networks. In: IEEE Vehicular Technology Conference, vol. 62, p. 690. Citeseer (2005)

25. Wang, W., Man, H., Liu, Y.: A framework for intrusion detection systems by social network analysis methods in ad hoc networks. *Security and Communication Networks* 2(6), 669–685 (2009)
26. Wu, J., Wang, Y.: Social feature-based multi-path routing in delay tolerant networks. In: 2012 Proceedings IEEE INFOCOM, pp. 1368–1376. IEEE (2012)
27. Wu, Y., Wang, B., Liu, K.R., Clancy, T.C.: Repeated open spectrum sharing game with cheat-proof strategies. *IEEE Transactions on Wireless Communications* 8(4), 1922–1933 (2009)
28. Xing, X., Jing, T., Huo, Y., Li, H., Cheng, X.: Channel quality prediction based on bayesian inference in cognitive radio networks. In: IEEE INFOCOM (2013)
29. Xu, H., Jin, J., Li, B.: A secondary market for spectrum. In: 2010 Proceedings IEEE INFOCOM, pp. 1–5 (2010)
30. Ye, Y.: Linear conic programming. Manuscript. Stanford University, Stanford (2004)
31. Zhang, T., Yu, X.: Spectrum sharing in cognitive radio using game theory—a survey. In: 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 1–5 (2010)
32. Zheng, H., Peng, C.: Collaboration and fairness in opportunistic spectrum access. In: 2005 IEEE International Conference on Communications, ICC 2005, vol. 5, pp. 3132–3136. IEEE (2005)
33. Zhou, W., Jing, T., Cheng, W., Chen, T., Huo, Y.: Combinatorial auction based channel allocation in cognitive radio networks. In: 2013 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM), pp. 135–140 (July 2013)
34. Zhou, X., Zheng, H.: Trust: A general framework for truthful double spectrum auctions. In: IEEE INFOCOM 2009, pp. 999–1007 (April 2009)

Game-Theoretic Joint Power Allocation and Feedback Rate Control for Cognitive MIMO Systems with Limited Feedback

Feng Zhao¹, Chen Wang¹, and Rongfang Bie²

¹ Key Laboratory of Cognitive Radio and Information Processing (Guilin University of Electronic Technology), Ministry of Education, Guilin, China
zhaofeng@guet.edu.cn, 1137807313@qq.com

² College of Information Science and Technology, Beijing Normal University, Beijing, China
rfbie@bnu.edu.cn

Abstract. In this paper, we consider a case with imperfect channel state information (CSI) in practical cognitive MIMO systems. We first analyze interference to the primary users (PUs) and then propose a joint power allocation and feedback rate control algorithm based on game theory. The utility function of each secondary user (SU) is defined as the corresponding throughput by CSI feedback minus the price as a linear function of feedback rate. Besides, the existence of the Nash equilibrium (NE) is proven. We derive the relationship between power allocation and feedback rate, and an iterative algorithm is proposed to reach the NE. Also, with the purpose of reduce interference and increase system capacity, water-filling (WF) power allocation and zero-forcing (ZF) beamforming are proposed. Simulation results shows that the proposed algorithm is better than equally distributed feedback rate scheme, obviously.

Keywords: Cognitive radio, Multi-input multi-output (MIMO), Power allocation, Limited feedback, Game theory.

1 Introduction

Due to the rapidly growing demand for high data-rate communications and the number of mobile users, almost all of the spectrum resources suitable for wireless communications have been assigned to telecommunication service providers. However, these assigned spectrum resources were not utilized efficiently [1]. The cognitive radio (CR) technique can enable higher spectrum utilization efficiency by allowing unlicensed users to intelligently access licensed frequency bands [2]. Besides, the MIMO technique, which will be a key technique for next-generation mobile communication systems, brings space diversity and spatial multiplexing gain, and thus enables higher channel capacity [3]. These two techniques can be combined to achieve higher spectrum utilization efficiency. This combination is referred to as cognitive MIMO radio [4].

Recent information-theoretic research indicates that a feedback channel can be further employed to furnish CSI to the transmitter side, which may affect closed-loop

capacity gains [5]. The joint beamforming and power allocation technology can be utilized to improve system capacity and reduce the co-channel interference (CCI) between users. Down-link CSI is required at stations for beamforming and power allocation. However, only user can detect down-link CSI, and Base station (BS) obtains down link CSI only by user's feedback [6]. Perfect feedback of CSI is scarcely possible due to complexity or practicality constraints and the infinite feedback of CSI is hard to realize in practice. In the recent years, some work considers limited feedback CSI in MIMO systems [7-10], study system capacity under the condition of limited feedback and improve system capacity through cooperative. Then, feedback rate control will be discussed. In [11], an efficient channel feedback scheme for downlink multiuser MIMO (MU-MIMO) systems was proposed. The objective of a new feedback design is to adaptively control the feedback rate of each user, depend on the individual channel status, while the overall sum feedback rate is kept the same. The authors find the optimal feedback rate sharing strategy using zero-forcing transmission scheme at the transmitter and random vector quantification at each user in [12]. In [13], the authors proposed an alternative approach to investigate the CSI feedback-rate control problem in the analytical setting of a game theoretic framework. Based on [13], the authors in [14] propose a non-cooperative feedback control game for secondary transmitter in cognitive radio network.

As an important branch of mathematical theories, game theory was proposed by David Goodman for the first time to be used in wireless systems for power control [15]. The cost function was applied for Pareto equilibrium in [16]. Besides, in [13, 14], [17-19], game theory was used in feedback rate control. We propose a non-cooperative joint power allocation and feedback control game for cognitive MIMO systems design under sum feedback-rate constraint. In the game, the utility function of a SU is determined by the downlink data-rate minus a liner price function of the CSI feedback rate. We assume that SUs are rational and selfish, and they will choose the feedback-rate by maximizing their own utility function. We prove the existence of the Nash equilibrium. Moreover, we derive the relationship between power allocation and feedback rate and propose an iterative algorithm to reach the NE. Simulation results show that the proposed algorithm is better than of equally distributed feedback rate scheme.

Notation: The following notations are used in this paper. The capital boldface is used to denote matrices, and the lowercase in boldface denotes vectors. $(\bullet)^H$, $\|\bullet\|$ and $(\bullet)^{-1}$ denote the conjugate transpose operation, spectral norm operation and inverse, $diag\{\dots\}$ stands for a diagonal matrix with the given elements on the diagonal. $C^{x \times y}$ denotes the space of $x \times y$ matrices with complex entries. The quantity $\min(x, y)$ and $\max(x, y)$ denote, respectively, the minimum and the maximum between two real numbers, x and y , and $(x)^+ = \max(x, 0)$.

2 System Model

We consider a cognitive MIMO system as shown in Fig. 1, which comprises one secondary base station (SBS), N_s SUs (SU_1, \dots, SU_{N_s}), and N_p Pus

(PU1, ..., PUN_p). The SBS is equipped with N_t antennas, while both SU and PU are each equipped with a single antenna. The primary base station, with powerful computational capability and priority to access the frequency band, may not interfere with the cognitive radio networks by preprocessing techniques. We assume that the PUs and SUs can perfectly estimate their CSI respectively, and the SBS can obtain quantified CSI of SUs and PUs by limited feedback from SUs and PUs. The SBS can transmit data to SUs while effectively control the interferences to the PUs and reduce inter-user-interference (IUI) by using the quantified CSI through the power control and beamforming. The signal transmitted from the SBS is represented by

$$\mathbf{X} = \mathbf{F}\mathbf{S} \quad (1)$$

where $\mathbf{S} = [s_1, s_2, \dots, s_{N_s}]^H$ is the transmit signal vector, s_k is the signal sending to the k -th SU, $\mathbf{F} = [\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_{N_s}]$ is the beamforming matrix, $\mathbf{F} \in \mathbb{C}^{N_t \times N_s}$, with \mathbf{f}_k is the beamforming vector for the k -th SU, and $\mathbf{P} = \text{diag}\{\sqrt{p_1}, \dots, \sqrt{p_{N_s}}\}$ is the matrix of power allocated for transmitting signals. We assume that the channel fading coefficients are independent, identically distributed and ergodic.

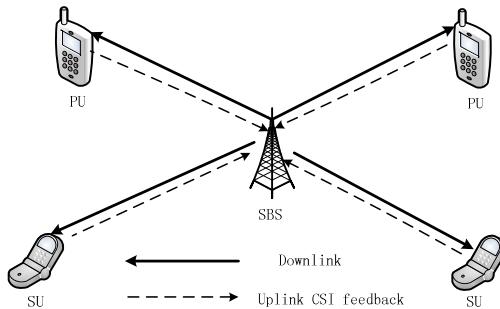


Fig. 1. Cognitive MIMO system

The signal received at the k -th SU is written as

$$\begin{aligned} y_k &= \mathbf{h}_k \mathbf{X} + n_k \\ &= \sqrt{p_k} \mathbf{h}_k \mathbf{f}_k s_k + \mathbf{h}_k \sum_{i=1, i \neq k}^K \sqrt{p_i} \mathbf{f}_i s_i + n_k \end{aligned} \quad (2)$$

where $\mathbf{h}_k \in \mathbb{C}^{1 \times N_t}$ is the channel coefficient from the SBS to the k -th SU, which is assumed to be rayleigh distributed, independent and identically distributed random variables with zero mean and unit variance, n_k is an additive white Gaussian noise with zero mean and variance σ_k^2 .

The corresponding throughput of the k -th SU is written as

$$C_k = \log_2 \left(1 + \frac{p_k \|h_k f_k\|^2}{\sum_{i=1, i \neq k}^{N_s} p_i \|h_k f_i\|^2 + \sigma_k^2} \right) \quad (3)$$

Due to the secondary transmission, there is interference received at each PU. The interference at the p -th PU is written as

$$I_p = \sum_{i=1}^{N_s} \|h_{pp} f_i\|^2 p_i \quad (4)$$

where $\mathbf{h}_p \in \mathbb{C}^{1 \times N_t}$ is the channel coefficient from the SBS to the p -th PU, and in order to ensure the quality of service (QoS) of PUs, I_p must be less than a threshold I_{th} .

In addition, we use quantified model of CSI in the literature [16], and the quantified CSI is written as

$$\overline{\mathbf{h}_k} = \sqrt{1 - 2^{-r_k}} \mathbf{h}_k + \sqrt{2^{-r_k}} \Delta \quad (5)$$

where r_k is the k -th user's CSI feedback rate, Δ is independent and identically distributed random variable with zero mean and unit variance.

In the end, for simplicity and without loss of generality, we use zero-forcing (ZF) beamforming in the paper. Beamforming matrix is written as [19]

$$\mathbf{F} = K \overline{\mathbf{H}}^H \left(\overline{\mathbf{H}} \overline{\mathbf{H}}^H \right)^{-1} \quad (6)$$

where $\overline{\mathbf{H}} = \left[\overline{h_1}, \dots, \overline{h_{N_s}}, \overline{h_{p1}}, \dots, \overline{h_{pN_p}} \right]^T \in \mathbb{C}^{(N_s + N_p) \times N_t}$ is global CSI at the SBS,

and K is a normalization constant, i.e. $K = \left\| \overline{\mathbf{H}}^H \left(\overline{\mathbf{H}} \overline{\mathbf{H}}^H \right)^{-1} \right\|^{-1}$.

3 Interference Control

3.1 Optimal Transmit Power

Considering ZF beamforming, the maximum interference is derived by combining (4) and (5), and it is written as

$$I_p = \max \left(\|h_p\|^2 \cdot 2^{-r_p} \cdot P_t \right), \quad \forall p = 1, 2, \dots, N_p \quad (7)$$

where r_p is feedback rate from the p -th PU to the SBS, and P_t is the SBS transmission power, i.e. $P_t = \sum_{k=1}^{N_s} p_k$. With the purpose of ensure the quality of service (QoS) of PUs, I_p must be less than a threshold I_{th} . Then, the SBS optimal transmit power P_t^{opt} is written as

$$P_t^{opt} = \min(P_t^*, P_{t,\max}) \quad (8)$$

where $P_t^* = \frac{I_{th}}{\max\left(\|h_p\|^2 \cdot 2^{-r_p}\right)}$, $\forall p = 1, 2, \dots, N_p$ and $P_{t,\max}$ is the maximum SBS transmit power. If $r_p \rightarrow \infty$, $P_t^* \rightarrow \infty$, hence $P_t^{opt} = P_{t,\max}$. In fact, it is almost impossible to $r_p \rightarrow \infty$ because of the limited feedback and the controlled transmit power.

3.2 Power Allocation

According to (5), the global CSI that SBS obtained is $\overline{\mathbf{H}} = [\overline{\mathbf{H}_s}, \overline{\mathbf{H}_p}]$, where $\overline{\mathbf{H}_s} = [\overline{h_1}, \dots, \overline{h_{N_s}}] \in \mathbb{C}^{N_p \times N_t}$, $\overline{\mathbf{H}_p} = [\overline{h_{p1}}, \dots, \overline{h_{pN_p}}] \in \mathbb{C}^{N_p \times N_t}$ when each SU's and each PU's feedback rate are determined. We consider a multi-user cognitive single input multiple output (SIMO) cognitive system, which can be equivalent to single user cognitive MIMO system. We considering water-filling (WF) algorithm, the SBS allocates p_k for k -th SU, and p_k is written as [20]

$$p_k = \left(\frac{1}{\varphi} - \frac{1}{\lambda_k} \right)^+ \quad (9)$$

where φ is nonnegative Lagrange multiplier and λ_k is k -th SU's channel gain.

4 Non-cooperative Game

4.1 Representation of Game Theory

Game theory is usually used for analyze competitive optimization problem. In cognitive MIMO systems, SUs share the spectrum bands of PUs in a competitive way, which may interfere with each other. Each SU is rational and selfish, with a desire to select a strategy maximizing its own benefit, without consideration of interference to other users. Hence, a cost function needs to be introduced with the purpose of reaching Nash equilibrium for the utility function. Based on the proposed system model, a non-cooperative game is represented by

$$G = \{\Omega, \{r_k\}_{k \in \Omega}, \{u_k\}_{k \in \Omega}\} \quad (10)$$

Game players includes entire SUs, Ω is the set of SUs, and game strategies are k -th SU transmission power r_k . The utility for each player is the profit (i.e., revenue minus cost, denoted by u_k for the k -th SU) in sharing the spectrum with the PUs and the other SUs. Consequently, the utility function of k -th SU is written as

$$u_k = C_k(r_k) - \alpha r_k \quad (11)$$

where $C_k(r_k)$ is the channel capacity of the k -th SU when using feedback rate r_k , and α is pricing factor which is a positive scalar.

Since the SBS uses the ZF beamforming, k -th SU can estimate the interference I_k , due to channel feedback error, beamforming vectors and transmission power of other SU as

$$I_k = \sum_{i=1, i \neq k}^{N_s} \|h_k f_i\|^2 p_i = \sum_{i=1, i \neq k}^{N_s} \|h_k\|^2 p_i \sin^2(\theta_{i,k}) \quad (12)$$

where $\theta_{i,k}$ is angle error using the feedback rate r_k . We are considering worst-case, i.e. $\theta_{k,\max} = \max(\theta_{i,k})$, lower bound of channel capacity is re-written as follows

$$C_k(r_k) = \log_2 \left(1 + \frac{p_k \|h_k\|^2 \cos^2(\theta_{k,opt} + \theta_{k,\max})}{\sum_{i=1, i \neq k}^{N_s} \|h_k\|^2 p_i \sin^2(\theta_{k,\max}) + \sigma_k^2} \right) \quad (13)$$

where $\cos(\theta_{k,opt}) = \frac{\|\bar{h}_k f_k\|}{\|\bar{h}_k\|}$, $\sin^2(\theta_{k,\max}) = 2^{-r_k}$. $\lim_{r_k \rightarrow \infty} C(r_k) = c$, and c is a constant.

A non-cooperative game problem can be represented by

$$\begin{aligned} \max u_k &= C_k(r_k) - \alpha r_k \\ \text{s.t. } &r_k^{\min} \leq r_k \leq r_k^{\max}, \forall k = 1, 2, \dots, N_s \\ &\sum_{k=1}^{N_s} r_k \leq R_{total} \end{aligned} \quad (14)$$

where r_k is strategy space of k -th SU, for guaranteeing QoS and equity of each SU, r_k^{\min} and r_k^{\max} are respectively minimum feedback rate and maximum feedback rate of k -th SU respectively, and R_{total} is feedback channel capacity. Hence, under the condition of satisfying the above two constraints, each SU can select optimal feedback rate by compete with other SUs to maximize own utility function.

4.2 Existence of Nash Equilibrium

Nash equilibrium (NE) namely that none of players can increase benefit by changing its own parameters, which is a stable state that a non-cooperative game can reach. If NE exists, it must satisfy the following conditions:

- a) The set of players is limited.
- b) The set of strategies is a closed bounded convex set.
- c) The utility function is a continuous quasi-concave on action space. A quasi-concave function is a curve without a convex down phenomenon relative to horizontal axis, i.e., for any two points x, y in domain, the inequality $f(ax+(1-a)y) \geq \min[f(x), f(y)]$ holds.

Next, whether the proposed utility function satisfies these three conditions are verified

- a) The players are N_s SUs and the player set is limited.
- b) The strategy set is feedback rate r_k . As the first constraint of formula (14) r_k is bounded and the strategy set is a closed and bounded convex set.
- c) The proposed utility function is a simple function of strategy set variables, and it is continuous and derivative. Solving for first-order derivative yields

$$u'_k = C'(r_k) - a \quad (15)$$

As $\lim_{r_k \rightarrow \infty} C(r_k) = c$, we can easily obtain $\lim_{r_k \rightarrow \infty} C'(r_k) = 0$. From (15), given the pricing factor a , then we can have

$$\lim_{r_k \rightarrow 0} u'_k > 0 \text{ & } \lim_{r_k \rightarrow \infty} u'_k < 0 \quad (16)$$

Hence, u'_k is a concave function. Finally, we conclude that NE exists in the case of determinate power allocation.

4.3 Joint Power Allocation and Feedback-Rate Control Algorithm

The k -th SU's channel capacity is an increasing function of either p_k or r_k . According to the equation (16), r_k^{temp} can be determined as

$$\frac{du_k}{dr_k} \Big|_{r_k=r_k^{\text{temp}}} = C'_k(r_k^{\text{temp}}) - \alpha = 0 \quad (17)$$

r_k^{temp} is a function of p_k . Therefore, the k -th SU achieves its maximal utility at r_k^* , where r_k^* is written as [18]

$$r_k^* = \max \left[r_k^{\min}, \min \left(r_k^{\text{temp}}, r_k^{\max} \right) \right], \forall k = 1, 2, \dots, N_s \quad (18)$$

Hence, r_k^* is the correlation function of p_k . The algorithm helps us solve equation (10). The algorithm process could be regarded as a feedback rate game. The iteration process is shown in Table 1.

Table 1. Iteration process of the proposed algorithm

The SBS
1. Initialize transmit power $\mathbf{P} = \text{diag} \left\{ \frac{P_t^{opt}}{N_s}, \dots, \frac{P_t^{opt}}{N_s} \right\}$ and $\alpha = 0$ to all SUs
Each user
2. Compute $r_k^* = \max \left[r_k^{\min}, \min(r_k^{\text{temp}}, r_k^{\max}) \right]$ and $\bar{h}_k = \sqrt{1 - 2^{-r_k}} h_k + \sqrt{2^{-r_k}} \Delta$, feedback r_k^* and \bar{h}_k to SBS.
The SBS
3. Compute $p_k^n = \left(\frac{1}{\varphi} - \frac{1}{\lambda_k} \right)^+$, $k = 1, \dots, N_s$, $R^n = \sum_{k=1}^{N_s} r_k$.
If $R^n > R_{total}$, $\alpha = \alpha + \Delta\alpha$.
Broadcast \mathbf{P} and α to all SUs, go to get 2
Until $ p_k^n - p_k^{n-1} \leq \varepsilon, k = 1, \dots, N_s$ break

5 Simulation Results

In this section, extensive simulations are conducted to examine the performance of the proposed algorithm. Matlab is used to verify the proposed algorithm. There are two PUs, one SBS and four SUs. The SBS is equipped with six antennas, each PU and SU with only one antenna. The background noise power at each user is set to $\sigma^2 = 0.01W$, and the initial interference threshold $I_{th} = 0.3W$, the maximum transmission power of SBS $p_{\max} = 10W$, the iterative threshold $\varepsilon = 10^{-3}$, minimum feedback rate $r_k^{\min} = 0.2 * R_{total}$, maximum feedback rate $r_k^{\max} = 0.8 * R_{total}$.

Fig.2 shows the performance of the proposed scheme with different feedback rates from PUs. When the PU's feedback rate is large, the optimal transmit power of SBS increases according to (7) and (8). When the sum feedback rate constraint is large, system capacity increases according to (13).

Fig.3 shows the system capacity performance under different algorithms. We can see that, when the feedback rate increases, the quantified model of CSI becomes more accurate, which leads to the increase of the system capacity. The performance in our proposed algorithm is superior to those in other algorithms, such as equally distributed feedback-size and equally power allocation, water-filling power allocation.

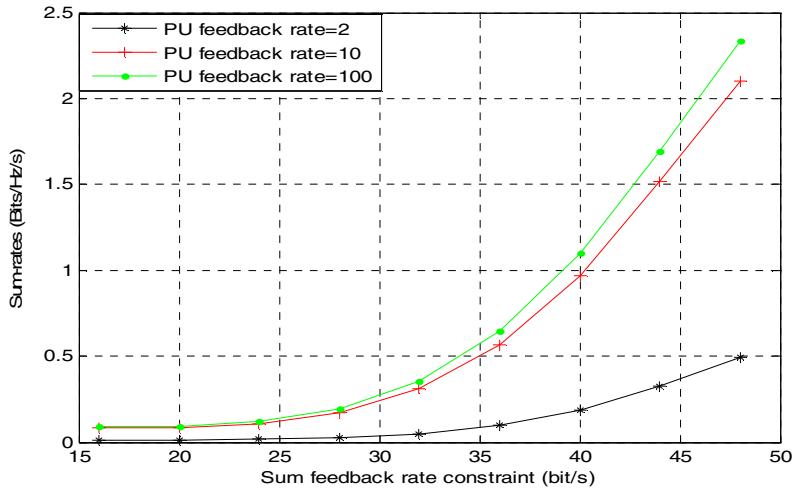


Fig. 2. Sum-rate in sum feedback-rate constraint with different feedback rate from PUs

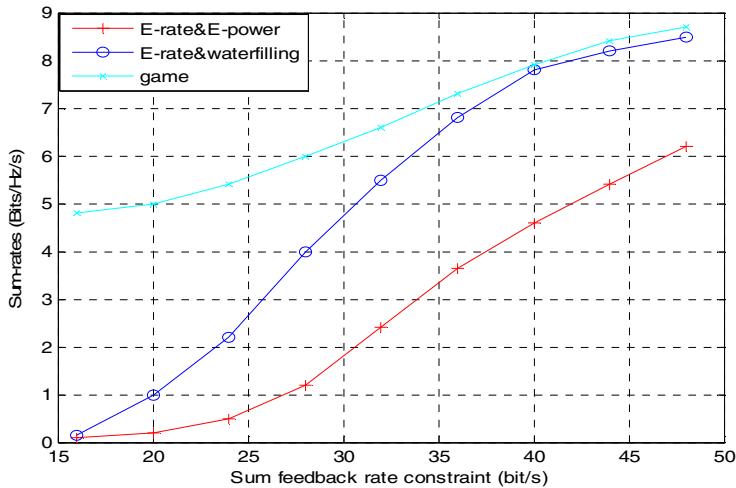


Fig. 3. Sum-rate in sum feedback-rate constraint under the different algorithms

6 Conclusion

In this paper, we investigate the joint power allocation and feedback rate control problem based on game theory for a cognitive MIMO system, which consists of multiple PUs and multiple SUs sharing the same spectrum. Joint power allocation and feedback rate control problem is formulated as a non-cooperative game in which each SU chooses a strategy from its strategy space, such that its utility function is

maximized. Besides, the existence of the Nash equilibrium (NE) is proven. We derive the relationship between power allocation and feedback rate, and an iterative algorithm is proposed to reach the NE. Simulation results show that the sum-rate of the proposed game is better than that of the equally distributed feedback rate scheme.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (61172055) and the Foundation of Department of Education of Guangxi Province (201202ZD046).

References

1. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies. Notice of Proposed Rule Making and Order FCC 03-322, Federal Communications Commission (2003)
2. Mitola, J., Maguire, G.Q.: Cognitive radio: making software radios more personal. *IEEE Personal Commun.* 6(4), 13–18 (1999)
3. Gesbert, D., Shafi, M., Shiu, D., Smith, P.J., Naguib, A.: From theory to practice: an overview of MIMO space-time coded wireless systems. *IEEE J. Sel. Areas Commun.* 21(3), 281–302 (2003)
4. Scutari, G., Palomar, D.P., Barbarossa, S.: Cognitive MIMO radio. *IEEE Signal Process Mag.* 25(6), 46–59 (2008)
5. Love, D.J., Heath, R.W., Lau, V.K.N., Gesbert, D., Rao, B.D., Andrews, M.: An overview of limited feedback in wireless communication systems. *IEEE J. Sel. Areas Commun.* 26(8), 1341–1365 (2008)
6. Love, D.J., Heath, R.W., Santipach, W., Honing, M.L.: What is the value of feedback for MIMO channels. *IEEE Commun. Mag.* 42(10), 54–59 (2004)
7. Zhang, D., Wei, G., Zhu, J., Tian, Z.: On the bounds of feedback rates for pilot-assisted MIMO systems. *IEEE Trans. Veh. Tech.* 56(4), 1727–1736 (2006)
8. Dabbagh, A.D., Love, D.J.: Feedback rate-capacity loss tradeoff for limited feedback MIMO systems. *IEEE Trans. Inf. Theory* 52(5), 2190–2202 (2008)
9. Huang, K., Zhang, R.: Cooperative feedback for multiantenna cognitive radio networks. *IEEE Trans. Signal Process.* 59(2), 747–758 (2011)
10. Huang, K., Zhang, R.: Cooperative precoding with limited feedback for MIMO interference channels. *IEEE Trans. Wireless Commun.* 11(3), 1012–1021 (2012)
11. Sohn, I., Park, C.S., Lee, K.L.: Downlink multiuser MIMO systems with adaptive feedback rate. *IEEE Trans. Veh. Tech.* 61(3), 1445–1451 (2012)
12. Lee, J.H., Choi, W.: Optimal feedback rate sharing strategy in zero-forcing MIMO broadcast channels. *IEEE Trans. Wireless Commun.* 12(6), 3000–3011 (2013)
13. Song, L., Han, Z., Zhang, Z., Jiao, B.: Non-cooperative feedback-rate control game for channel state information in wireless networks. *IEEE J. Sel. Areas Commun.* 30(1), 188–197 (2012)
14. Myung, J., Chen, Y., Liu, K.J.R., Kang, J.: Non-cooperative feedback control game for secondary transmitter in cognitive radio network. *IEEE Signal Process. Lett.* 20(6), 571–574 (2013)
15. Goodman, D.: Network assisted power control for wireless data. *Mobile Netw. Appl.* 6(5), 409–415 (2001)

16. Saraydar, C.U., Mandayam, N.B., Goodman, D.: Efficient power control via pricing in wireless data networks. *IEEE Trans. Commun.* 50(2), 291–303 (2002)
17. Maskery, M., Krishnamurthy, V., Zhao, Q.: Decentralized dynamic spectrum access for cognitive radios: cooperative design of a noncooperative game. *IEEE Trans. Commun.* 57(2), 459–469 (2009)
18. Attar, A., Nakhai, M.R., Aghvami, A.H.: Cognitive radio game for secondary spectrum access problem. *IEEE Trans. Wireless Commun.* 8(4), 2121–2131 (2009)
19. Scutari, G., Palomar, D.P., Facchinei, F., Pang, J.S.: Convex optimization, game theory, and variational inequality Theory. *IEEE Signal Processing Mag.* 27(3), 35–49 (2010)
20. Scutari, G., Palomar, D.P., Barbarossa, S.: The MIMO iterative waterfilling algorithm. *IEEE Trans. Signal Process.* 57(5), 1917–1935 (2009)

A Multi-model Based Range Query Processing Algorithm for the WSN

Guilin Li¹, Xing Gao^{1,*}, Longjiang Guo², Juncong Lin¹, and Ying Gao¹

¹ School of Software, Xiamen University, Simingnan Street 22, 361005 Xiamen, China

² School of Computer Science and Technology, Heilongjiang University,
Xuefu Road 74, 150080 Harbin, China

{glli,jclin}@xmu.edu.cn

guolongjiang@gmail.com

gaoxing@xmu.edu.cn

Abstract. One important research topic for the wireless sensor network is about the range query, i.e., retrieving the areas in the sensor network where the temperature is between 30 °C and 35°C. The traditional approaches are not feasible for such query since they use a single probability model to describe the data distribution of the sensor nodes, which is not accurate. In this paper, we propose a multi-model based range query processing algorithm, which utilizes multiple probability models to improve the accuracy and saves the energy consumption of the single model based algorithms. We conduct experiments on real dataset. The experimental results show that the multi-model based algorithm can save more energy than that consumed by the single model based algorithm.

Keywords: Range Query, Histogram, Multi-Model Driven, Query Processing, Wireless Sensor Network.

1 Introduction

The Wireless Sensor Network (WSN) has been a focused research theme in recent years. A WSN consists of a large number of sensors and collects huge amount of data with the information of locations, time, weather, temperature and so on. And they have wide applications in the areas of traffic monitoring, battlefield surveillance and environmental monitoring [1] [2] [3] [4].

A WSN is composed of two kinds of nodes, the sink and the ordinary nodes. The sink is a bridge to connect the WSN with the outside world, such as collecting data from the ordinary nodes or receiving query from a user and sending the query throughout the network. The ordinary nodes are responsible for collecting data from the environment, transmitting data to the sink or processing the query received from the sink. As a WSN consists of a large number of the ordinary nodes, it produces a huge amount of data. The WSN can be seen as a new kind of data source and a lot of query processing algorithms [5] [6] [7] [8] [9] have been proposed to efficiently manage the data produced by the WSN.

* Corresponding author.

The range query is an important type of query in the WSN. For instance, a user sends a range query to the WSN distributed in a forest, asking for the places where the temperature falls into the range $[r_1, r_2]$. The sensors, satisfying this condition, return their locations or *IDs* to the sink. If the sensors return their *IDs*, the sink transforms the *IDs* to locations and returns the locations to the user.

Some existing methods have been proposed to solve the range query in the WSN, which can be classified into two classes. The first class is the data centric storage based algorithms, such as GHT [13], DIM [14], Comb-Needle [15], Double Ruling [16], etc.. The data centric storage algorithms define different types of events for the data collected by sensors. Each type of events are stored in a particular node called event storage node in the WSN. When a node detects an event, it transmits the data of the event to the event storage node. A range query, transformed to a query for an event, is sent directly to the event storage node and answered by the node. The event defined in the data centric storage algorithm is very rigid, which means the users can only ask for the the result of a range defined by the event. So these algorithms do not fit for the query asking for the result of any range.

The second class is the local storage based algorithms, such as [10] [11] [12]. For the traditional local storage based algorithms [10] [11], the data collected by a sensor is stored in its local storage. The queries are sent to each node and the nodes satisfying the query return their results to the user. The problem of the traditional algorithm is that all nodes need to return their results to the sink whether they satisfy the query or not, which consumes a lot of energy. In [12], a probability model is used to process the range query. The probability model is used to estimate the probability that each node satisfies the query. Only if the probability of a node, satisfying the query, is above a threshold, the node is considered as a result. With the help of the probability model, nodes do not return any result to the sink for a range query. There are two problems for the algorithm. The first one is the algorithm can only give an approximate answer to a query. The second one is it is hard to determine a threshold balancing the efficiency of energy consumption and the accuracy of the query result.

In this paper, we propose a multi-model based algorithm to solve the range query in the WSN, which is a local storage based algorithm. Compared with the other local storage based algorithms, our algorithm has the following advantages. First, our algorithm constructs multiple probability models. With the help of theses probability models, only the most relevant nodes among all nodes need to transmit their results to the sink, which saves more energy than the traditional local storage algorithms. Second, our algorithm can give the precise answer to the range query with minimum energy consumption. The multi-model based range query processing algorithm proposed in this paper is composed of 3 steps:

1. Probability Model Construction
2. Sampling based Model Selection
3. Model based query processing

The probability model construction algorithm first constructs multiple probability models for each node in the WSN. By clustering the historical data collected by the nodes, m subclasses are constructed and each node builds a probability model according to the data of its own in a subclass. With the help of the multiple probability models, the query processing algorithm can select the more accurate model to describe the data distribution for the current condition than that of the single model based algorithm.

Multiple probability models have been constructed for each node in the WSN. For a particular range query, there must be a method to select a suitable probability model for each node to process the query. In this paper, a sampling based algorithm is proposed to fulfill this task. Some typical nodes are selected by a preprocessing algorithm. Then the sampling based algorithm collects the data from these typical nodes to determine a suitable model for a query.

Combining the model selected by the sampling based model selection algorithm with the real data sensed by a node, the model based query processing algorithm can minimize the energy consumption of processing a range query. Experimental results show that the cost model based algorithm can provide the accurate answer with less energy than that consumed by the the single model based algorithm.

The contributions of this paper are as follows. First, a multi-model based algorithm is proposed to solve the range query in the WSN, which utilizes multiple probability models to improve the accuracy of the data distribution function and saves the energy consumption of the algorithm. Second, extensive experiments were done to verify the efficiency of the proposed algorithm.

The rest of the paper is organized as follows. Section 2 introduces the multi-model based range query processing algorithm. In Section 3, we briefly talk about the single model based range query processing algorithm. Section 4 evaluates the performance of the proposed algorithm on real dataset. Section 5 briefly discusses the related work and in section 6 we draw the conclusion.

2 The Multi-model Based Range Query Processing Algorithm

2.1 Probability Model Construction

First, multiple probability models are constructed for each node in the WSN based on the historical data collected from each node. Let N be the set of all nodes in the WSN and $|N|$ be the number of nodes in the WSN. Each node collects data, such as the temperature, humidity, from the environment at a certain rate. The data from all nodes at a given timestamp t consists of a vector $V_t = (v_t^1, v_t^2, \dots, v_t^{|N|})$, where v_t^j represents the data collected by the j^{th} node n^j at the timestamp t . The historical data set H is composed of a set of vectors V_t at different timestamps. Given the historical data set H , the vectors in H can be clustered into many subclasses. If the vectors in H are clustered into m subclasses, represented as H_1, H_2, \dots, H_m , a probability model can be constructed

Table 1. List of Notations

Notation	Explanation
N	the set of all nodes in the WSN
n^j	the j^{th} node in the WSN
V_t	the vector of data collected at timestamp t
v_t^j	the data collected from n^j at timestamp t
H	the set of V_t for all historical data
H_i	the i^{th} subclass of H
M_i^j	the i^{th} model of H_i of node n^j
M_g^j	the general model of node n^j
m	the number of subclasses
D_i^j	$\{v_t^j \forall V_t \in H_i \& v_t^j \in V_t\}$
μ_i^j	the mean of the data set D_i^j
σ	coverage ratio
R_i^j	data range of node n^j for model M_i^j
R_{lk}^j	$R_l^j \cap R_k^j$
I	the set of (l, k) for all 2-combinations from 1 to m
T	the set of all typical nodes
CN_{lk}	the candidate node set distinguishing model l from k
MCN	the merged candidate node set
CM	the candidate model set
Q	the set of node IDs for a query

for each node based on the vectors contained in a subclass. For convenience, we list the notations used throughout this paper in Table 1.

The data collected by a node is a random variable, which can be described by a Probability Distribution Function (PDF). The PDF of a random variable is usually hard to calculate, but it can be estimated by a histogram. A histogram is a representation of tabulated frequencies, erected over discrete intervals (bins), with an area equal to the frequency of the observations in the interval. The total area of the histogram is equal to the number of data.

The vectors belonging to the i^{th} subclass H_i can be used to construct a histogram for each node in the WSN. For H_i , all data belonging to the node n^j forms a data set represented as $D_i^j = \{v_t^j | \forall V_t \in H_i \& v_t^j \in V_t\}$. Let $v_{t1}^j = \max\{D_i^j\}$ and $v_{t2}^j = \min\{D_i^j\}$, which means v_{t1}^j and v_{t2}^j are the maximum and minimum value of node n^j in D_i^j . The range $([v_{t2}^j], [v_{t1}^j])$ can be equally divided into $([v_{t1}^j] - [v_{t2}^j] + 1)$ bins, whose length is 1. f_x^j represents the number of data falling into the interval $[x, x + 1]$. In the same way, a probability model can be constructed for each node based on the vectors in each subclass. If the historical data set H is divided into m subclasses, m probability models are constructed for each node. The i^{th} probability model of a node n^j is represented by M_i^j . There is one special probability model for each node, called general model, which is constructed based on all the historical data collected by a node instead of a subset of data. The construction method of the general model is the same as that of the other models. The general model of a node n^j is represented as M_g^j .

There are altogether $m + 1$ probability models for each node, which can be classified into two classes $M^j = \{M_1^j, M_2^j, \dots, M_m^j\}$ and M_g^j .

Given a range $[a, b]$, the probability of the data falling in $[a, b]$ calculated by M_i^j is represented as $pr_i^j\{[a, b]\}$, which can be estimated by formula (1) based on the histogram. The ratio of the area of the histogram of the range $([a], [b])$ to the total area of the histogram of the range $([v_{t1}^j], [v_{t2}^j])$ is used to estimate $pr_i^j\{[a, b]\}$ in formula (1).

$$pr_i^j\{[a, b]\} = \frac{\sum_{x=\lfloor a \rfloor}^{\lceil b \rceil - 1} f_x^j}{\sum_{y=\lfloor v_{t1}^j \rfloor}^{\lceil v_{t2}^j \rceil - 1} f_y^j} \quad (1)$$

2.2 Sampling Based Model Selection

Multiple probability models have been constructed for each node in the WSN. For a particular range query, there must be a method to select a probability model for each node to process the query. In this paper, a sampling based method is proposed to fulfill this task.

Firstly, some typical nodes are selected from the WSN. Before sending a range query to the WSN, the sink samples data from the typical nodes. Based on the data sampled from the typical nodes, a suitable probability model $M_i^j \in M^j$ is selected to make the query processing algorithm be carried out efficiently. Before giving the typical node selection algorithm, we present some definitions.

Let μ_i^j represent the mean of D_i^j of the node n^j . μ_i^j can be calculated by formula (2), where $|H_i|$ represents the number of vectors in the subclass H_i .

$$\mu_i^j = \frac{\sum_{v_t^j \in D_i^j} v_t^j}{|H_i|} \quad (2)$$

Definition 1 (Data Range). *The Data Range of a node n^j , whose data belongs to D_i^j , is defined as $R_i^j = ([\mu_i^j] - x, [\mu_i^j] + y]$ and $pr_i^j\{R_i^j\} \geq \sigma$, where $\sigma(0 < \sigma < 1)$ is called the coverage threshold and the x and y are integers.*

The range R_i^j is a sub-range of the total range of the model M_i^j . The ratio of the area of R_i^j of the histogram and the total area of the histogram is not less than the coverage threshold σ .

As there are m subclasses, the node n^j has m data ranges, represented by $R_1^j, R_2^j, \dots, R_m^j$. The intersection between the l^{th} and the k^{th} data range of the node n^j is represented as $R_{lk}^j = R_l^j \cap R_k^j$. There are altogether $C(m, 2)$ intersections between any two data ranges of a node, where $C(m, 2)$ represents the number of the 2-combinations from integer 1 to m .

Definition 2 (Candidate Node). *If an intersection R_{lk}^j of the node n^j satisfies the condition $\text{length}(R_{lk}^j) = \min\{\text{length}(R_{lk}^x) | x = 1, 2, \dots, |N|\}$, the node n^j is called a candidate node. The pair (l, k) is called distinguishable by the candidate node n^j . $\text{length}()$ is a function, representing the length of the intersection.*

The typical node selection algorithm needs to prepare some parameters with the help of a preprocessing algorithm. The preprocessing algorithm first calculates the m data ranges $R_i^j (i = 1, \dots, m)$ for each node. Then the preprocessing algorithm calculates the $C(m, 2)$ intersections R_{lk}^j for each node. As there can be multiple nodes satisfying the definition of Candidate Node for a intersection R_{lk}^j , the preprocessing algorithm calculates a candidate node set CN_{lk} for each intersection, which is composed of all the candidate nodes of the intersection. Finally, the preprocessing algorithm merges the candidate nodes in the candidate node sets of all nodes into a Merged Candidate Node set MCN . Each element in MCN has two attributes, which are a counter and a list. If multiple intersections have the same candidate node in their candidate node sets, these candidate nodes are merged into a unique one, called merged candidate node. The counter of the merged candidate node is the number of CN_{lk} containing the merged candidate node. The list of the merged candidate node is all the pairs (l, k) of CN_{lk} containing the merged candidate node. Let I be a set of the pairs (l, k) , which contains the $C(m, 2)$ 2-combinations of the m subclasses.

Based on the definitions and the MCN calculated by the preprocessing algorithm, we propose a greedy based algorithm to select the typical nodes from the WSN. The greedy algorithm sorts all the merged candidate nodes in the MCN according to their counters in descending order. Then it selects the candidate node with the largest counter as the typical node and removes the selected node from the MCN . Then the entries in the list of the selected node is removed from I and the list of the other merged candidate nodes left in the MCN . When an entry is removed from the list of a merged candidate node left, the counter of the node is subtracted by 1. The greedy based algorithm repeats this process until the set I is empty, which means any two models can be distinguished by a candidate node selected. All the candidate nodes selected form the typical node set T . The j^{th} typical node n^j in T has an attribute represented as $counter^j$, which is the number of intersections n^j can distinguish.

2.3 Model Based Query Processing

The model based query processing algorithm for a range query works as follows. A node n^j in the WSN stores the m models M^j and a general model M_g^j in its local storage. After receiving a range query from a user, the sink samples data from the typical nodes in T selected by the typical node selection algorithm introduced in section 2.2. According to the data sampled, a probability model is selected. The sink sends the range query together with the index of the model selected to all nodes in the WSN. A node processes the query with the help of the probability model selected. In this section, we will introduce the algorithm selecting a suitable probability model based on the sampled data and the model based query processing algorithm.

To save energy, the model selection algorithm does not sample data from all typical nodes at the same time. We sort the nodes in T according to their counters in descending order. The model selection algorithm samples data from one node in the typical node set at a time from the beginning. Only when the sampled

Algorithm 1. The Model Based Query Processing Algorithm for the Sink

Require: query range $[r_1, r_2]$, index of the selected model $index$

Ensure: the result node set Q

- 1: $index =$ value returned by the Model Selection Algorithm
- 2: **for** $\forall n^j \in N$ **do**
- 3: pr_{index}^j = the probability of the node satisfying the received range query calculated by the $index$ model
- 4: pr_g^j = the probability of the node satisfying the received range query calculated by the general model
- 5: **if** $\max\{pr_{index}^j, pr_g^j\} > \rho$ **then**
- 6: put n^j into the result set Q
- 7: **end if**
- 8: **end for**
- 9: broadcast the query and the $index$ throughout the sensor network
- 10: collect answers from the nodes in the network
- 11: **if** receive a positive answer from a node n^j **then**
- 12: put ID of node n^j into the result set Q
- 13: **else if** receive a negative answer from a node n^j **then**
- 14: remove the ID of node n^j from the result set Q
- 15: **end if**
- 16: **return** Q

data can not determine a model, the data of the next typical node is sampled. Initially, the Candidate Model set, represented as CM , is set to $\{1, 2, \dots, m\}$. For a data v_t^j , sampled from a typical node n^j , the model selection algorithm checks whether $v_t^j \in R_i^j$ for all m data ranges of n^j . If the $v_t^j \notin R_i^j$, the model selection algorithm removes the number i from CM . If there is only one number left in CM , the corresponding model is selected as the suitable model. Otherwise, there will be no number or multiple numbers in CM . In this case, the model selection algorithm uses a distance based method to select the suitable model. The data sampled from the typical nodes forms a vector. As each subclass is composed of a lot of vectors, the center of each subclass also forms a vector. The vector formed by the data of the typical nodes is part of the center vectors of the subclasses. The data corresponding to the typical nodes is drawn from each center vector of the subclasses, which forms a partial center vector for each subclass. The model selection algorithm calculates the Euclid distance d between the typical node vector and the partial center vector of each subclass and selects the subclass with the minimum distance as the suitable model.

After the sink selects a suitable probability model for a range query, it sends the index of the model together with the range query to all the nodes in the WSN. When a node n^j receives the query, it calculates two probabilities. Firstly, it gets the index of the probability model and calculates the probability that the data of the node satisfies the range query according to the selected probability model. Secondly, it calculates the probability according to the general probability model. We represent the first probability as pr_{index}^j and the second probability as pr_g^j . The larger one of the two probability is chosen as the final

Algorithm 2. The Model Based Query Processing Algorithm for an Ordinary Node

Require: $[r_1, r_2]$, $index$, v_t^j

Ensure: $NULL$

- 1: extract the $index$ and query range $[r_1, r_2]$ from the packet received
 - 2: pr_{index}^j = the probability of the node satisfying the received range query calculated by the $index$ model
 - 3: $pr_{general}^j$ = the probability of the node satisfying the received range query calculated by the general model
 - 4: **if** $(max\{pr_{index}^j, pr_{general}^j\} > \rho) \& (v_t^j \notin [r_1, r_2])$ **then**
 - 5: send a negative answer containing the ID of the current node to the sink
 - 6: **else if** $(max\{pr_{index}^j, pr_{general}^j\} \leq \rho) \& (v_t^j \in [r_1, r_2])$ **then**
 - 7: send a positive answer containing the ID of the current node to the sink
 - 8: **end if**
-

probability represented as pr_{final}^j . If pr_{final}^j is larger than a threshold ρ , which is called the probability threshold, but the data really collected by the node does not satisfy the range query, the node returns a negative answer to the sink. If $pr_{final}^j \leq \rho$, while the data really collected by the node satisfies the range query, the node returns a positive answer to the sink. The node does not return any answer to the sink in other cases.

When $pr_{final}^j > \rho$, it means that the data sampled by the node has a large probability to satisfy the query. The event, that the real data collected by the node does not satisfy the query, is a small probability event. Only if the small probability event happens, the node needs to send the answer to the sink, which minimizes the number of messages transmitted between the node and the sink. The same reason for the other two cases. The model based range query processing algorithm is a distributed algorithm. The algorithm executed by the sink is given by Algorithm 1. The algorithm executed by an ordinary node is given by Algorithm 2.

3 The Single Model Based Range Query Processing Algorithm

In the single model based algorithm, a node n^j in the WSN only stores its general model M_g^j in its local storage. After receiving a query from a user, the sink directly broadcasts the query throughout the WSN. A node calculates the probability pr_g^j that its data satisfies the query with M_g^j . If $pr_g^j > \rho$ but the data really collected by the node does not satisfy the range query, the node returns a negative answer to the sink. If $pr_g^j \leq \rho$, while the data really collected by the node satisfies the range query, the node returns a positive answer to the sink. The node does not return any answer to the sink in other cases.

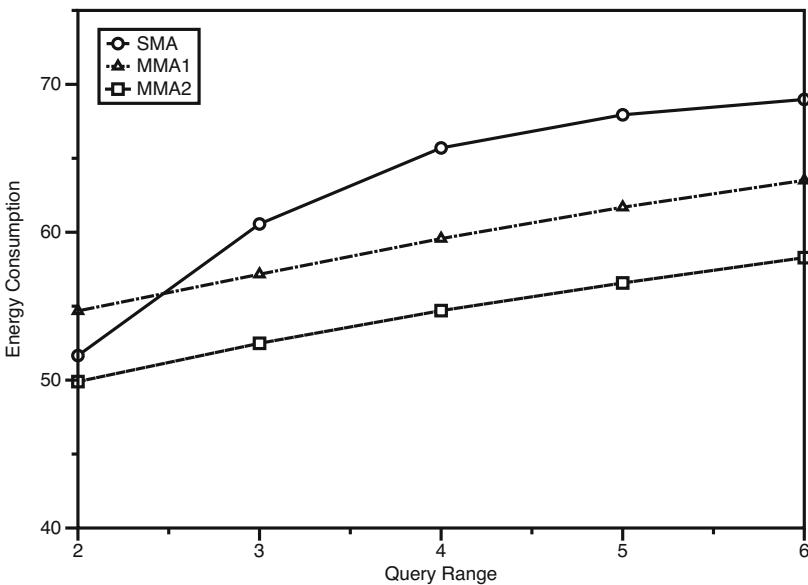


Fig. 1. Energy Consumption Comparison among SMA and MMA

4 Performance Evaluation

In this section we compare the performance of the Multi-Model based range query processing Algorithm, represented as MMA, with that of the Single Model based Algorithm, represented as SMA. The performance of the two algorithms is measured by the energy consumption, which is the number of messages transmitted. We adopt the data set collected from 34 sensors deployed in the Intel Berkeley Research lab [23] in our experiments. There are 54 sensors in the data set. As a lot of data of some sensors is lost in the data set and our algorithm needs plenty of historical data to construct the probability models, we only select 34 sensors from them. We randomly assign a integer number to each node as its number of hops to the sink, which is used to calculate the energy consumption of each query processing algorithms.

The parameter for the SMA is $\rho = 0.5$. The parameters for the MMA1 are $\rho = 0.6$, $\sigma = 0.8$ and $m = 6$. The parameters for the MMA2 are $\rho = 0.6$, $\sigma = 0.4$ and $m = 6$. The results are shown in Figure 1. The x -axis is the query range sent by a user and y -axis is the number of messages transmitted by the query processing algorithm, which is the average of the number of the messages to process the ten queries for each range.

The experimental results show that, when the query range is 2, the MMA1 consumes more energy than SMA. While the MMA2 consumes less energy than SMA when query range is 2. For other kinds of query range, the energy cost of the MMA is less than that of the corresponding SMA. Compared with the

SMA, the MMA1 can save about 5.8% energy. The MMA2 can save about 13.6% energy. The results show that the MMA is much better than the SMA.

5 Related Work

The DIM [14] divides the whole network into a lot of zones and embeds a k-d tree like index in the network. There is only one node in each zone, which acts as the index node of the zone. With the k-d tree like index, events with comparable attribute values are stored nearby and the DIM can fulfill the range query easily. In the Comb-Needle algorithm [15], when a sensor detects an event, it distributes the data of the events to the nodes in the vertical direction within h hops around it. If a query is sent to the sensor network along multiple lines in the horizontal direction and the distance between any two neighboring lines is smaller than h hops, the query will be transmitted to the event storage node and get the results. The double ruling algorithm [16] distributes the data of the events around the network in a circle. The query also traverses the network in a circle. The double ruling algorithm guarantees that the circle of the query can intersect with all circles of the queried events. [19] constructs a single dimensional address space of sensor nodes through a zigzag traversing such that geographically near nodes are located near in the linear address space. The multi-dimensional query are transformed into a single dimensional data space using Hilbert space-filling curves. [20] builds a distributed k-d tree based index structure over sensor network and proposes a dynamic programming based methodology to control the granularity of the index tree in an optimized approach. [17] proposes a bloom filter based algorithm to reduce the number of messages transmitted during the procedure of query processing. [18] proposes the bloom filter based approximate algorithms, which can save the energy even further. [21] [22] consider the security problem of the range query. [21] presents a novel spatiotemporal crosscheck approach to ensure secure range queries in event-driven two-tier sensor networks. [22] employs the order-preserving symmetric encryption and a novel data structure called Authenticity & Integrity tree to preserve authenticity and integrity of query results.

6 Conclusions

In this paper, a multi-model based query processing algorithm is proposed to solve the range query problem in WSN. The algorithm utilizes multiple probability models to improve the accuracy of the data distribution function and saves its energy consumption. Experimental results show the energy efficiency of the proposed methods.

Acknowledgments. This work was supported by a grant from the National Natural Science Foundation of China (No.61100032, No. 61202142), the National Key Technology R&D Program Foundation of China (No. 2013BAH44F00),

Joint Funds of the Ministry of Education of China and China Mobile (No. MCM20122081) and the Fundamental Research Funds for the Central Universities (No.2010121070, No.2010121072, No. 2013121030)

References

1. Lo, C., Peng, W.: Carweb: A traffic data collection platform. In: MDM (2008)
2. Li, M., Liu, Y.H.: Underground col mine monitoring with wireless sensor networks. *ACM Transactions on Sensor Networks* 5(2) (2009)
3. Keung, G.Y., Li, B., Zhang, Q.: The intrusion detectionin mobile sensor network. In: Proceedings of MobiCom (2010)
4. Tang, L., Yu, X., Kim, S., Han, J., Hung, C., Peng, W.: Tru-alarm: Trustworthiness analysis of sensor networks in cyber-physical systems. In: ICDM (2010)
5. Ai, C.Y., Guo, L.J., Cai, Z.P., Li, Y.S.: Processing area queries in wireless sensor networks. In: MSN (2009)
6. Liu, Y., Li, J.Z., Gao, H.: Enabling ϵ -Approximation Querying in Sensor Networks. In: Proceedings of VLDB (2009)
7. Yu, B., Li, J.Z., Li, Y.S.: Distributed data aggregation scheduling in wireless sensor networks. In: Proceedings of INFOCOM (2009)
8. Cheng, S.Y., Li, J.Z.: Bernoulli sampling based (ϵ, δ) - approximate aggregation algorithm in large scale sensor networks. In: Proceedings of INFOCOM (2010)
9. Cai, Z.P., Ji, S.L., Li, J.B.: Data caching-based query processing in multi-sink wireless sensor networks. *International Journal of Sensor Networks* 11(2) (2012)
10. Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: A scalable and robust communication paradigm for sensor networks. In: Proceedings of ACM MobiCom (2000)
11. Madden, S., Franklin, M.J., Hellerstein, J.M., Hong, W.: The design of an acquisitional query processor for sensor networks. In: SIGMOD (2003)
12. Deshpande, A., Guestrin, C., Madden, S.R.: Model- driven data acquisition in sensor networks. In: VLDB (2004)
13. Shenker, S., Ratnasamy, S., Karp, B.: Govindan, and D. Estrin. Data-centric storage in sensornets. In: Proceedings of ACM MobiCom (2006)
14. Li, X., Kim, Y.J., Govindan, R., Hong, W.: Multi- dimensional range queries in sensor networks. In: Proceedings of ACM SenSys (2003)
15. Liu, X., Huang, Q.F., Zhang, Y.: Combs, needles, haystacks: balancing push and pull for discovery in large- scale sensor networks. In: Proceedings of ACM SenSys (2004)
16. Sarkar, R., Zhu, X., Gao, J.: Double rulings for information brokerage in sensor networks. In: Proceedings of ACM MobiCom (2006)
17. Chen, H.H., Li, M., Jin, H., Liu, Y.H., Ni, L.M.: MDS: Efficient multi-dimensional query processing in data-centirc wsns. In: Proceedings of RTSS (2008)
18. Li, G.L., Guo, L.J., Gao, X., Liao, M.H.: Bloom filter based processing algorithms for the multi-dimensional event query in wireless sensor networks. *Journal of Network and Computer Applications* (2014)
19. Lee, J.-Y., Lim, Y.H., Chung, Y.D., Kim, M.H.: Data storage in sensor networks for multi-imensional range queries. In: Yang, L.T., Zhou, X.-s., Zhao, W., Wu, Z., Zhu, Y., Lin, M. (eds.) ICESS 2005. LNCS, vol. 3820, pp. 420–429. Springer, Heidelberg (2005)

20. Xie, L., Chen, L.J., Chen, D.X., Xie, L.: A decentralized storage scheme for multi-dimensional range queries over sensor networks. In: ICPADS (2009)
21. Shi, J., Zhang, R., Zhang, Y.C.: Secure range queries in tiered sensor networks. In: INFOCOM (2009)
22. Bu, J.J., Yin, M.J., He, D.J., Xia, F., Chen, C.: Sef: A secure, efficient and flexible range query scheme in two- tiered sensor networks. International Journal of Distributed Sensor Networks (2011)
23. Madden, S.: Intel lab data, <http://db.csail.mit.edu/labdata/labdata.html>

Secure Authentication Scheme Using Dual Channels in Rogue Access Point Environments

Arwa Alrawais^{1,2}, Abdulrahman Alhothaily^{1,3}, and Xiuzhen Cheng¹

¹ Computer Science, The George Washington University, Washington DC, USA

² College of Computer Engineering and Sciences,
Salman Bin AbdulAziz University, KSA

³ General Department of Payment Systems, Saudi Arabian Monetary Agency,
Riyadh, KSA

{alrawais,hothaily,cheng}@gwu.edu

Abstract. The ubiquitous deployment of Rogue Access Points (RAPs) presents security issues in Wireless LAN (WLAN) environments. Therefore, authentication plays a crucial role in protecting mobile users in WLAN communications. Some implementations of the existing wireless authentication schemes rely on weak authentication methods such as a username and password. Other vulnerable implementations of wireless authentication schemes do not resist rogue access point attacks such as man-in-the-middle attacks and phishing attacks. In addition, the risk of these attacks is high since they could cause sensitive information disclosure for mobile users. In this paper, we introduce a new authentication scheme using mutual authentication that leverages two different communication channels to thwart various attacks. Our scheme uses a novel approach based on dual channels that add an extra security level to the authentication process. The proposed scheme utilizes the idea of “Call before visiting” which could prevent many different security attacks. This paper argues that the proposed design mitigates or removes several popular security attacks that are claimed to be effective in the existing wireless authentication schemes. Furthermore, the proposed method does not require any major modification in the wireless network architecture or any computational device to be used and deployed.

Keywords: Authentication; Wireless Security; Rogue Access Points.

1 Introduction

Nowadays, IEEE 802.11 Wireless Local Area Networks (WLANs) have been broadly deployed in public environments such as commercial and military domains to connect high speed Internet through Access Points (APs). However, this rapid development raised a series of security issues among WLAN providers and mobile users due to the fact that there is no wired line in a WLAN to restrict access to legitimate members only. One of the WLAN security concerns is Rogue Access Point (RAP) i.e., an unauthorized wireless access point that has

been installed without a local network administrator's permission. According to [1], RAPs have reached about 20% of enterprise networks.

Because of the ubiquitous deployments of RAPs, various security attacks have presented in public WLAN environments such as phishing and Man-In-The-Middle (MITM) attacks. RAP attacks are used to learn the user's behavior on the Internet and gain their information. To combat these masquerading attacks in WLAN communication environments, we need to provide a secure authentication scheme between a legitimate access point and mobile user. The overwhelming majority of the authentication schemes are based on a password-user authentication, which is handled by basic credentials such as username and password [2].

However, password-user authentication raises major security concern since a password can be compromised easily by several attacks and reused by a hostile party. Additionally, the influence of human factors in creating a password is a significant concern, because most users would select easy-to-remember passwords, and they reuse the same password across different electronic service accounts. Thus, when an adversary succeeds in obtaining a user's password, he will exploit it to gain access to more electronic service accounts. Consequently, password based authentication is not adequate to provide a secure authentication scheme. We need a better authentication method to increase the security level and users' faith in wireless networks. In the research community, researchers have investigated several authentication schemes sacrificing the simplicity of the basic credential through involving more complex mechanisms in the authentication scheme.

There are various proposed schemes to provide authentication based on biometrics, tokens, or the use of extra software or hardware. However, the most practical and secure ones are those based on two distinct communication channels. In this paper, we design a scheme that leverages two different communication channels to thwart many attacks. In our proposed scheme, we utilize the fact that three quarters of the people around the world have mobile phones [3]. Consequently, we use SMS as a second channel. We believe SMS is suitable and secure enough to transmit authentication messages between entities. Additionally, as one of our authentication mechanisms, One-Time-Password (OTP) is used to counter different attacks, since OTP is refreshed for each login session and restricted to a very short time. Secure Socket Layer server's certificate is combined with a generated random number is used to combat MITM. Finally and significantly, our scheme provides mutual authentication in which the parties need to authenticate each other. The details of the proposed scheme will be explained in Section 3.

The rest of this paper is organized as follows. In Section 2, we briefly discuss the related work. The proposed mutual authentication scheme in WLAN networks is elaborated in Section 3. In Section 4, we analyze the security of our scheme. Our conclusion is presented in Section 5.

2 Related Work

The security threats that RAPs can cause in WLAN communication environments attracted the attention of the research community in recent years. There has been an extensive study on detecting RAP in WLAN communication environments [4–12]. Using traffic characteristics to detect RAP has been proposed in many works. In [12], a temporal traffic at a central location is used to detect RAP. Shetty *et al.* [5] proposed an automated solution to detect RAP by analyzing network traffic at the gateway router. The authors implemented their approach in two phases: in the first phase, the difference between wired and wireless patterns is identified, and in the second phase, an unauthorized host is detected by analyzing the traffic characteristics that were demonstrated in the previous phase. Another study in detecting RAP is a timing-based scheme that utilizes the Round Trip Time (RTP) between a user and Domain Name System (DNS) server [10]. Specifically, this technique enables the user to resolve whether an AP is legitimate or not by calculating the RTP between the user and the DNS server. Han *et al.* [10] extended the previous work by designing an outlier filtering algorithm to reduce the time of detection and false detection with result that reflects high accuracy [6]. Their solution is a learning based approach that requires prior knowledge about the target wireless network [7]. Thus, the practicality of their solution is limited by the pre-calculated knowledge. Online algorithms are proposed in [11] to detect RAP. The authors developed a sequential hypothesis test based on a real time passive measurement at a gateway router. Jana *et al.* showed that RAP could be detected through clock skews of AP in WLAN [8]. Their work is based on the fact that the fingerprint clock skews for each AP device is different.

In [13] and [14], Ma *et al.* proposed a scheme that collects data from wired and wireless surveillance fingerprinting to detect RAPs. A recent study focused on client side RAP detection [9]. Their method works as a scanner machine on the client side, and warns the user once RAP is exposed. Furthermore, the authors in [15] considered detecting RAPs in vehicular networks for Drive-thru Internet. They utilized the Global Positioning System (GPS) locations for each AP to differentiate between RAPs and legitimate ones. We observed that some of the prior attempts to resolve these issues have some security limitations, and may require a complicated implementation, cost computation, or extra equipment. It is worth mentioning that unlike the previous studies that seek to detect RAPs, our scheme protects the mobile users from RAP threats.

A further research area related to this paper is the existing studies that use different techniques in designing authentication schemes to protect mobile users from RAP attacks. Recently, Bumjoo *et al.* [16] utilized 3G networks to exchange SSL session keys, and used them for further communication through WLANs. The purpose of exchanging SSL keys through 3G is to protect users from RAP attacks. Another effort was proposed in [17] to mitigate the risk of

the MITM attacks that are carried out by RAP. The server's certificate is sent to the user's mobile phone through dual interface networks (3G and Wi-Fi). Then, the two certificates are compared to detect if there is any interception by MITM attacks. In [18], various studies of using mobile phones as authentication tokens for Internet service providers were evaluated and discussed.

The added complexity and some of the security limitations of previous works motivate us to improve the authentication security schemes. Our scheme, "Call before visiting", is inspired by the human behavior of calling before visiting someone. Specifically, it provides mutual authentication where a mobile user needs to verify the authentication server before visiting or using its services. The authentication server then validates the mobile users to authorize them to use its services. Our scheme employs different authentication techniques to resist various attacks, such as MITM attacks, phishing attacks, and other security attacks. Our scheme not only overcomes the security limitations of the aforementioned schemes but also provides more security features.

3 Proposed Scheme

In this section, we propose a mutual authentication scheme in wireless communications using dual channels: WLAN (Wireless Local Area Network) and SMS (Short Message Service). The scheme is immune to several types of known WLAN attacks nowadays, such as phishing and MITM attacks. Additionally, our scheme does not require any major modification in the wireless network architecture to be used and deployed. The following requirements need to be fulfilled:

- Users must have their cell phones in order to communicate with the authentication server using SMS. Only authorized mobile users will receive SMS to communicate with the authentication server.
- Our scheme requires the authentication server to possess a unique public number by subscribing to a mobile service to interact with the mobile user's mobile phone through SMS.
- The communication between the mobile user and the authentication server is going through two channels: WLAN and SMS. Our scheme utilizes the SMS as a second channel to exchange authentication messages.
- Our scheme requires mobile users to install a plugin in their web browser.
- Our scheme requires the authentication server to generate OTP for each session.
- Our scheme requires the authentication server to use SSL certificate in web communication.

The notations and their semantic meanings used to describe the proposed scheme are listed in Table 1.

Table 1. Notation used in the proposed scheme

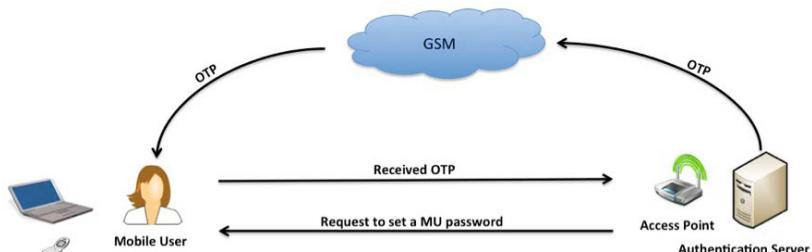
Notation	Description
MU	Mobile user
AS	Authentication server
AP	Access point
N	Generated random digits of numeric characters
M	Authentication request message
ID	Identification for an individual
$H()$	One way hash function
C	Secure Socket Layer (SSL) certificate
R	Result of the function $hash(C \parallel N)$
\parallel	String concatenation operation
$PLUGIN$	Software component
SN	Server's public number
APP	Access point login page
OTP	One time password
SMS	Short message service

Our scheme consists of three phases: registration phase, server authentication phase, and user authentication phase. We present the details of each phase respectively.

3.1 Registration Phase

In this phase, the mobile user MU must register at the WLAN authentication server by providing a form of personal identification. The information could consist of a user's ID , mobile phone number, security questions and other related information. This information is used to identify each individual. The registration phase is explained in Figure 1.

The authentication server should send a one time password OTP to the registered MU mobile phone through SMS . Then, the MU enters the received OTP

**Fig. 1.** Registration phase

in the access point login page *APP* and sets a new password that satisfies the *APP* security policy. This process is a crucial step in the registration phase to verify the registered user's mobile phone number. The registration phase can be done through the *APP*.

3.2 Server Authentication Phase

When *MU* needs to access a WLAN network, the mobile user must pass through the server authentication phase. The main purpose of this phase is to verify the authentication server legitimacy. The server authentication phase steps are outlined in Figure 2.

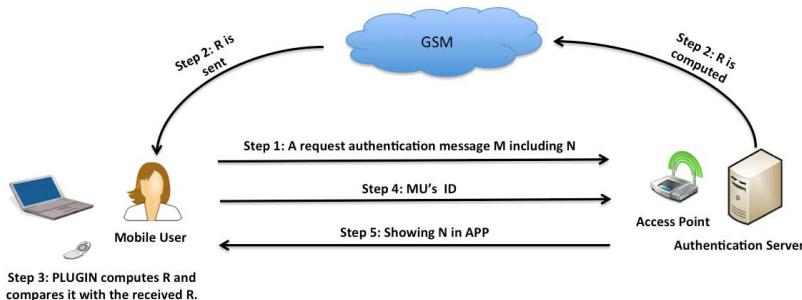


Fig. 2. Server authentication phase

- Step.1.** The *MU* should visit the access point login page *APP*, and use the *PLUGIN* to generate a random number N . This generated number N is used to add an additional security layer to the authentication process, since N is used in calculating R and helps *MU* to verify the *AS*. Then, the *MU* sends an authentication request message M over a short message service *SMS* to the *AS* using the server's public number SN .
- Step.2.** The *AS* receives the message M containing N . Then, the *AS* retrieves its own Secure Socket Layer (SSL) certificate C . The *AS* uses the received N and the retrieved C to compute $R = (\text{hash}(C \parallel N))$, and sends R back to the *MU* over *SMS*.
- Step.3.** The *MU* enters the received R in the *PLUGIN* to verify the *APP* legitimacy. The *PLUGIN* retrieves C , and computes $R = (\text{hash}(C \parallel N))$. Then, the *PLUGIN* checks the result of R to determine whether the computed R matches the received R or not. If the match occurs, the session will continue. The *MU* believes that R is from the *AS*, and the *APP* is authenticated. If there is no match, the *PLUGIN* will alert the *MU* and terminate the session.

Step.4. The *MU* enters the registered *ID* in the *APP* to identify itself to the *AS*.

Step.5. The *APP* demonstrates *N* that has been sent by the *MU*. Showing *N* makes the *MU* more confident that they are not connected to a RAP, or at a fraudulent login webpage. If the demonstrated *N* is equal to the sent *N*, the *MU* verifies the *APP*.

3.3 User Authentication Phase

Now that the *MU* has completed the server authentication phase successfully, the *AS* needs to authenticate the *MU* to accomplish the mutual authentication procedures. The user authentication phase steps are outlined in Figure 3.

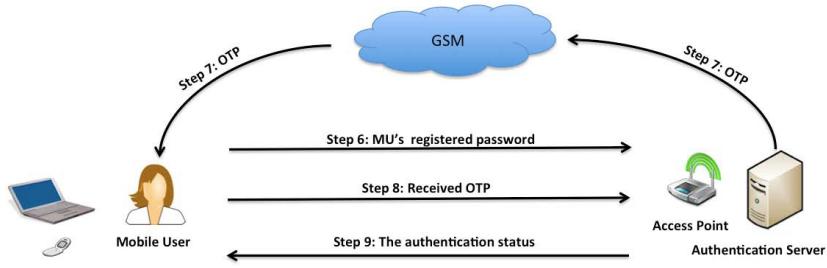


Fig. 3. User authentication phase.

Step.6. The *MU* enters the registered password in the *APP* to verify itself to the *AS*.

Step.7. For additional security, the *AS* needs to authenticate the *MU* using *OTP*. Thus, the *AS* sends the *OTP* over *SMS* to the *MU*.

Step.8. The *MU* enters the received *OTP* to the *APP* for validation process.

Step.9. The *APP* shows the authentication status. If the received *OTP* matches the sent *OTP*, the *MU* is authenticated and can gain access to the WLAN communication. Otherwise, the *MU* is not authenticated, and cannot gain access to the WLAN communication.

4 Security Analysis

Our mutual authentication scheme seeks to defend against RAP related attacks and various security threats. In this section, we examine different security aspects of our solution to verify that our scheme is secure from different WLAN communication attacks.

Mutual Authentication: In the proposed scheme, our mutual authentication aims to guarantee that the mobile user MU and the authentication server AS are both legitimate to establish a connection.

1. *User authenticates server:* In step 1 to 5 of the mutual authentication scheme, the MU challenges the AS in several steps to validate its identity. In step 1 and 2, the MU sends N and receives R from the AS by SMS . Then, in step 3 the MU enters N in the $PLUGIN$ to verify the AS . The computed R is compared with the received R from the AS . If they are equal, the MU can be sure that the AS is authorized. Furthermore, in step 4 and 5, the MU enters the registered ID in the access point login page APP to identify the legitimacy of the APP , where the APP should illustrate N . If the sent N matches the showing N , the MU believes that the webpage is meant to be the real APP .
2. *Server authenticates user:* In step 6 to 9 of the mutual authentication scheme, the MU has to identify itself by providing the registered password. Furthermore, the AS uses OTP as an additional authentication factor to counter against various security attacks including phishing attacks. The AS sends OTP to the MU mobile phone through SMS . Then, the MU is required to enter the received OTP to the APP to prove its identity. The AS checks whether the entered OTP is equal to the sent OTP . If they are equal, the AS authenticates and authorizes the MU to access the WLAN communication and use its services.

Resistance to Phishing Attacks: Phishing attacks refer to the process of attempting to obtain user sensitive information such as a username and password by masquerading as a dependable entity. It is usually performed during user authentication procedures. Our scheme prevents phishing attacks in step 5, 7 and 8. In step 5, the MU should verify N in the APP , since the illustration of N resists to phishing attacks. If the generated N matches the showed N in the APP , the MU verifies the APP credibility. Additionally, the usage of OTP over SMS in step 7 and 8 is utilized as an additional layer of authentication. The OTP counters against phishing attacks, due to its unpredictability and dynamic nature.

Resistance to Man-In-the-Middle-Attacks: MITM attacks can occur in the authentication procedure during the communication between a user and the authentication server. In step 2 and 3, we believe that our scheme defends against MITM attacks. The usage of the SSL server's certificate C in computing R determines whether a MITM attack occurs or not. R is sent to the

MU using an *SMS* channel. The received R is compared with the computed R in the *PLUGIN* to detect any kind of interception by an attacker. Furthermore, if an attacker attempts to modify C , it will be discovered easily at the *MU* terminal. For this reason, it is possible to detect and protect against MITM attacks in our scheme.

Resistance to Keylogging Attacks: Keylogging, also known as a keyboard capturing attack, refers to the action of capturing all the keystrokes that a user types on the keyboard. Our scheme can resist keylogging attacks, since the *OTP* is refreshed every time the *MU* needs to access a WLAN network. When the *MU* receives the *OTP* over *SMS*, the *OTP* is used only once for each session. Keylogging attacks can be prevented, since the *AS* sends the *OTP* to the *MU* through *SMS*. Therefore, even if the keylogging attacks succeed in recording the *MU* registered password, the attacker would not be able to use it in the future since we use the *OTP*. Thus, keylogging attacks cannot obtain access.

Resistance to Password Cracking Attacks: Password cracking is the process of reconstructing a password from a transmitted data to gain unauthorized access. This attack is considered to be a concern in password based authentication schemes. The proposed scheme defends against password cracking attacks through the *OTP* that is sent to the *MU* using *SMS*. Consequently, password cracking attacks are impossible to execute in our scheme.

5 Conclusion

In this paper, we proposed a novel authentication scheme in rogue access point RAP environments. The scheme takes advantage of two communication channels, and it does not require any extra computational cost or modification in the wireless network architecture. We investigated and analyzed various attacks that are employed in the real world against our authentication scheme. The proposed scheme can protect against various attacks such as MITM attacks, and phishing attacks. Additionally, our proposed solution is a mutual authentication scheme in which each entity needs to authenticate the other. We believe that our scheme delivers the means to secure authentication in rogue access point RAP environments.

Acknowledgment. Alrawais acknowledges the scholarship fund from the Ministry of Higher Education, Saudi Arabia and the College of Computer Engineering and Sciences, Salman bin Abdulaziz University, Saudi Arabia. Alhothaily acknowledges the scholarship fund from the Saudi Arabian Monetary Agency.

References

1. Beyah, R., Venkataraman, A.: Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security and Privacy* 9(5), 56–61 (2011)

2. Czeskis, A., Balfanz, D.: Protected login. In: Blyth, J., Dietrich, S., Camp, L.J. (eds.) FC 2012 Workshops. LNCS, vol. 7398, pp. 44–52. Springer, Heidelberg (2012)
3. Information, W.B., Technologies, C.: infoDev (Program): Information and Communications for Development 2012: Maximizing Mobile. World Bank Publications (2012)
4. Ma, L., Teymorian, A.Y., Cheng, X.: Passive listening and intrusion management in commodity wi-fi networks. In: Global Telecommunications Conference GLOBECOM 2007, pp. 327–331. IEEE (2007)
5. Shetty, S., Song, M., Ma, L.: Rogue access point detection by analyzing network traffic characteristics. In: Military Communications Conference MILCOM, pp. 1–7. IEEE (2007)
6. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A timing-based scheme for rogue ap detection. IEEE Transactions on Parallel and Distributed Systems 22(11), 1912–1925 (2011)
7. Yang, C., Song, Y., Gu, G.: Active user-side evil twin access point detection using statistical techniques. IEEE Transactions on Information Forensics and Security 7(5), 1638–1651 (2012)
8. Jana, S., Kasera, S.K.: On fast and accurate detection of unauthorized wireless access points using clock skews. IEEE Transactions on Mobile Computing 9(3), 449–462 (2010)
9. Nikbakhsh, S., Manaf, A.B.A., Zamani, M., Janbeglou, M.: A novel approach for rogue access point detection on the client-side. In: 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 684–687. IEEE (2012)
10. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A measurement based rogue ap detection scheme. In: INFOCOM, pp. 1593–1601. IEEE (2009)
11. Wei, W., Suh, K., Wang, B., Gu, Y., Kurose, J., Towsley, D.: Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, pp. 365–378. ACM (2007)
12. Beyah, R., Kangude, S., Yu, G., Strickland, B., Copeland, J.: Rogue access point detection using temporal traffic characteristics. In: Global Telecommunications Conference GLOBECOM 2004, vol. 4, pp. 2271–2275. IEEE (2004)
13. Ma, L., Teymorian, A.Y., Cheng, X., Song, M.: Rap: Protecting commodity wi-fi networks from rogue access points. In: The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops, p. 21. ACM (2007)
14. Ma, L., Teymorian, A.Y., Cheng, X.: A hybrid rogue access point protection framework for commodity wi-fi networks. In: The 27th Conference on Computer Communications INFOCOM. IEEE (2008)
15. Han, H., Xu, F.: C. Tan, C., Zhang, Y., L, Q.: Vr-defender: Self defense against vehicular rogue aps for drive-thru internet. IEEE Transactions on Vehicular Technology, 21 (2014)
16. Park, B., Kim, N.: Secure and efficient communication method in rogue access point environments. International Journal of Smart Home 7(4) (2013)
17. Lee, J., Tu, C., Jung, S.: Man-in-the-middle attacks detection scheme on smart-phone using 3g network. In: The Fourth International Conference on Evolving Internet, pp. 65–70 (2012)
18. Jrstad, I., Jonvik, T.: et al.: Strong authentication with mobile phone as security token. In: 6th International Conference on Mobile Adhoc and Sensor Systems MASS 2009, pp. 777–782. IEEE (2009)

Approximate Self-Adaptive Data Collection in Wireless Sensor Networks^{*}

Bin Wang¹, Xiaochun Yang¹, Wanyu Zang², and Meng Yu²

¹ Northeastern University, Liaoning 110819, China

² Virginia Commonwealth University, Virginia 23284, USA

{binwang, yangxc}@mail.neu.edu.cn,
{wzang, myu}@vcu.edu

Abstract. To extend the lifetime of wireless sensor networks, reducing and balancing energy consumptions are main concerns in data collection due to the power constraints of the sensor nodes. Unfortunately, existing data collection schemes mainly focus on energy saving while overlook balancing the energy consumption of the sensor nodes. In addition, most of them assume that each sensor has a global knowledge about the network topology. However, in many real applications, such a global knowledge is not desired due to the dynamic features of the wireless sensor network. In this paper, we propose an Approximate Self-Adaptive data collection technique (ASA), to approximately collect data in a distributed wireless sensor network. ASA investigates the spatial correlations between sensors to provide an energy-efficient and balanced route to the sink, while each sensor does not know any global knowledge on the network. Based on our synthetic experiences, we demonstrate that ASA can provide significant communication (and hence energy) savings and equal energy consumption of the sensor nodes.

1 Introduction

One of the most important applications in Wireless Sensor Networks (WSNs) is Data Collection, where the sensor nodes collect the sensing data and then forward them to the sink [1, 2]. Sensor nodes have limited supply of power, thus such operation may cause energy-hungry and further shorten the *lifetime* of sensor network since wireless transmission costs more energy compared with other operations, i.e., computing [3]. There are different definitions on the network lifetime, here we use the lifetime definition of [4], in which it is defined as the duration from initial start of the network to the moment when a certain percent of sensors is disconnected from the sink.

To extend the network lifetime, reducing while balancing the power consumption among all sensor nodes are great challenges in designing data collection schemes. Unfortunately, existing research on data collection mainly focuses on low energy consumption and overlooks the importance of balancing the power consumption of the sensor

* The work is partially supported by the National Basic Research Program of China (973 Program) (No. 2012CB316201), the National Natural Science Foundation of China (Nos. 61322208, 61272178, 61129002), the Doctoral Fund of Ministry of Education of China (No. 20110042110028), and the National Science Foundation (No. CCF-1441253).

nodes. Besides, most of the existing data collection approaches assume that each sensor in the network has the global knowledge on the network topology, which is not feasible due to the dynamic features of WSNs.

Furthermore, an effective data collection method needs to consider the following technical challenges as well: (i) How to find an efficient routing (forwarding) path to the sink for a sensor without the global knowledge on the network topology? (ii) Sensing data often has spatial correlations, that is, sensors in a certain region read the same or quiet similar data in each time step. How to utilize this unique feature in the routing path search? (iii) How to resilient to the failure caused by the sensor nodes and data transmission?

To address above mentioned challenges, we propose an *Approximate Self-Adaptive* (ASA) method, which can approximately gather the sensing data and prolong the network lifetime without any global knowledge of the network. That is, given a fixed sink and an arbitrary distributed sensor network, by using query “SELECT * FREQ f WITHIN $\pm\epsilon$,” ASA makes the $\rho(\%)$ sensors connected to the sink as long as possible. ASA first divides the WSNs into multiple disjointed clusters based on the spatial correlations between the sensors. It then searches a “minimal” routing path to the sink by transmitting the clusters readings instead of the sensor readings. To balance the energy consumption of the sensor nodes, the sensing data will be forwarded to the sink through different nodes periodically. The main contributions of this paper are as follows:

- We propose a novel ASA approach to cluster sensors into different groups according to their sensing values without global knowledge of network topology. If a set of sensors detect similar values with $\pm\epsilon$, then ASA classifies them into one cluster, which we call a *Value Cluster* (VC). Different from the existing clustering approaches, ASA uses at most 4 messages to construct small clusters when initializing the network. Then, for each time step, it expands and maintains its clusters gradually through its routing nodes. This clustering strategy is more practical for sensor applications, since ASA needs a few message communications for each time step and get optimal clusters in convergent fashion.
- We design an effective map-based forwarding technique, which guides sensors self-adaptively finding a “minimal” routing path to the sink. Furthermore, ASA only forwards updates to the sink and changes routing path periodically to balance the energy consumption of the sensor nodes.
- We describe different failures occurred in the data collection, and analyze why ASA is resilient to the failures.
- Last but not the least, we evaluate ASA and demonstrate its advantages on energy-balanced and energy-efficient data collection through extensive experiments on synthetic data sets.

2 Data Collection Framework

Sensor Network. A sensor network consists of a set of fixed-location sensors, each of which has a unique ID. We use an $m \times n$ grid to describe sensor locations. For each cell in the grid, it contains at most one sensor. Without loss of generality, we assume

that the sink has unlimited energy, which locates in one edge of the grid and knows all sensors' ID and locations, and is responsible for performing computation. Two sensors are said to be neighbors if they are within the transmission range of each other.

For the data collection task, the sink initially broadcasts the locations of all sensors and a query “SELECT * FREQ f WITHIN $\pm\epsilon$ ” to the network. Different from the existing work, we assume that only the sink knows all sensor locations [5] and each sensor maintains a location map about the sensor location but does not know the topology of the network. Notice that, the sensor location changes only when the network changes, i.e adds new sensors to keep the network live, so location information is only broadcasted once when initializing the network.

Problem Definition. Given a sensor network that continuously sensing values at each time step, and a sink that requires an ϵ -loss approximation of the sensing data at all times, design a data collection protocol that makes $\rho\%$ sensors connected to the sink as long as possible.

In our proposed approach, there are two interlaced steps to accomplish approximate data collection at each time step: clustering sensors and forwarding the cluster values.

3 Value-Based Cluster Model and Initialization

As illustrated in Section 1, spatial constraints determine if the sensing data in a certain region are the same or quiet similar. We can divide the whole sensing region into several disjoint regions/clusters based on the sensing data value.

Fig. 1(a) shows the snapshot of network communication among 10 sensors and their sensing values at time step t . For clear presentation, no grid lines are drew in the figure. Note that, grid only describes locations of sensors, but not the communication topology. For example, two sensors within communication distance does not mean that they are located in adjacent cells, and vice versa, since there may exist an obstacle preventing them from communicating with each other. Each node in the figure represents a sensor. Edges between nodes represent neighbors, i.e. one hop communication distance. For example, sensors s_1 and s_2 are neighbors. The inner layer sensors s_4 , s_5 , and s_9 are neighbors to the sink. Fig. 1(b) shows an optimal clustering result when $\epsilon = 0.3$. We use shade colors to describe clusters.

Once a wireless sensor network is constructed, the sink broadcasts a start message to all sensors to construct disjoint VCs (DVCs for short). We define DVCs as follows:

Definition 1. *Value cluster (VC): A set of sensors $S = \{s_1, \dots, s_m\}$ belong to a value cluster C at time step t , if and only if C is connected, and for any two sensors $s_i, s_j \in S$, $|v_t(s_i) - v_t(s_j)| \leq \epsilon$, where $v_t(s)$ denotes sensing value of s at time step t .*

Definition 2. *Disjoint cluster model: A cluster model is denoted as $C_v = C_1, \dots, C_k$, where k is number of VCs and for any two C_i and C_j , they are disjoint.*

Some sensors are chosen to actively invite their neighbors to join in its cluster. We call such chosen sensors *seeds*. In order to let all sensors to be involved in the clustering procedure simultaneously, seeds are desired to distribute evenly in the network. That

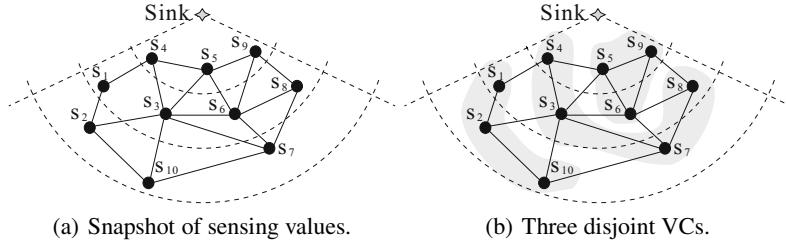


Fig. 1. Disjoint value clusters when $\epsilon = 0.3$. Sensors and their values at time t are $\langle s_1, 25.0 \rangle, \langle s_2, 24.9 \rangle, \langle s_3, 24.8 \rangle, \langle s_4, 24.7 \rangle, \langle s_5, 25.1 \rangle, \langle s_6, 25.0 \rangle, \langle s_7, 24.5 \rangle, \langle s_8, 24.7 \rangle, \langle s_9, 25.1 \rangle, \langle s_{10}, 25.2 \rangle$.

Algorithm 1. Construct DVCs for seed sensors

Input: A set of seeds S , time step t ;

- 1 Each seed s in S broadcasts its value $v_t(s)$ to invite its neighbors to join in its region;
- 2 Seed s gets messages from its neighbors s'_1, \dots, s'_h ;
- 3 **if** there is at least one response message **then**
- 4 s constructs its VC contains s'_1, \dots, s'_k ;
- 5 s.t. $V_I(s) = [v_l, v_u]$;
- 6 $v_l = \min_{i=1}^k \{v(s), v(s'_i)\}$;
- 7 $v_u = \max_{i=1}^k \{v(s), v(s'_i)\}$;
- 8 s notifies $V_I(s)$ and its member IDs to s'_1, \dots, s'_k ;
- 9 **else if** it is an invite message from other seeds **then**
- 10 s changes it to a non-seed sensor;
- 11 s responses the invitation according to Algorithm 2;
- 12 **else if** no neighbors send messages **then**
- 13 s changes it to a non-seed sensor;
- 14 s chooses a seed s'' to join in, such that s has closest value distance to s'' ;

is, for any sensor s in the network, either s is a seed, or s is a neighbor to a seed. For example, in Fig. 1(a), sensors s_2 , s_4 , and s_6 are good choices as seeds, since any other sensor in the network is neighbor of one of them. On the other hand, sensors s_7 , s_8 , and s_9 are not good candidate of seed. Therefore, the choice of seeds is critical to the performance of the disjoint VC model.

We propose a self-clustering approach. The detailed techniques are covered in Algorithms 1 and 2. Algorithm 1 illustrates that a seed constructs a set of disjoint VCs and Algorithm 2 describes that a non-seed behaviors using at most four messages. In Fig. 1(a), after using Algorithms 1 and 2, ASA builds up four disjoint VCs, which are $C_1 = \{s_1, s_2, s_{10}\}$, $C_2 = \{s_3, s_4\}$, $C_3 = \{s_7, s_8\}$, and $C_4 = \{s_5, s_6, s_9\}$. If s_2 , s_4 , and s_6 are chosen as seeds, ASA only needs two messages to build up these VCs, whereas if s_1 , s_2 , and s_{10} are chosen as seeds, then ASA needs four messages to achieve the four VCs.

Algorithm 2. Construct DVCs for non-seed sensors

Input: A set of non-seeds S' , time step of the start message from the sink;

- 1 Each $s' \in S'$ monitors messages from its neighbors;
- 2 **if** there is no messages from its neighbors **then**
- 3 s' changes it to a seed;
- 4 s' uses Algorithm 1 to construct its VC;
- 5 **else if** s' receives $v_t(s)$ from s at time step t **then**
- 6 **if** $|v_t(s') - v_t(s)|$ is minimize and less than ϵ **then**
- 7 s' sends $v_t(s')$ to s ;
- 8 **if** s' receives message $V_I(s)$ from s **then**
- 9 s' stores $V_I(s)$;
- 10 s' broadcasts $v(s')$ to its other neighbor seeds;
- 11 go to 2;

4 Self-Adaptive Routing

Once we finish constructing the DVCs, a crucial problem that we need to address is how to find a “minimal” route to catenate all DVCs.

Definition 3. *Valid data route:* Given a set of DVCs $\mathcal{C}_1, \dots, \mathcal{C}_k$ and sink s , a route $s_1 \rightarrow \dots \rightarrow s_m \rightarrow s$ is valid, if and only if for each VC \mathcal{C}_i , there exists at least one routing sensor $s_j \in \mathcal{C}_i$ ($1 \leq j \leq m$).

Based on above definition, the problem of *minimal valid data route analysis* can be represented as: Given a set of disjoint value clusters $\mathcal{C}_1, \dots, \mathcal{C}_k$, find a valid route $s_1 \rightarrow \dots \rightarrow s_m \rightarrow s$ to forward values of all clusters to the sink s . The valid route is minimal if (i) s_1 is disconnected to s after removing s_j ($1 \leq j \leq m$) from the route, and (ii) only updates are transmitted to the sink.

4.1 Routing Map

We propose a new data structure, called *routing map* to guide sensors to concatenate the constructed DVCs. Fig. 2(a) shows a sketch of a routing map. The routing map is an $m \times n$ matrix corresponding the network grid, each cell in the matrix is labelled using 0 or 1. If a VC has been routed, then all cells covered by the VC are marked, i.e. labelled 1. All un-routed cells are unmarked, i.e. labelled 0. Using a routing map, a sensor can know which regions need to be routed.

In the initialization phase, the sink broadcasts sensors’ locations, i.e. the grid to the network. For each time step t , sink randomly selects a sensor s to start routing. s first marks 1 on sensors in its VC, then it finds a shortest path to reach to areas that (i) have not been marked and (ii) have long distances to the sink if there are more than one shortest paths. The requirement (i) guarantees that the route acrosses non-routed VCs, and the requirement (ii) lets ASA heuristically route sensors with more hops to the sink in priority, which helps balance energy consumption of the sensors.

Besides appending $v_t(s)$ in the forwarding message, in order to navigate sensors to find a valid route, the last routing sensor adds its routing map to the forward message. When a routing sensor s' receives the forward message, it determines routing according to the attached routing map.

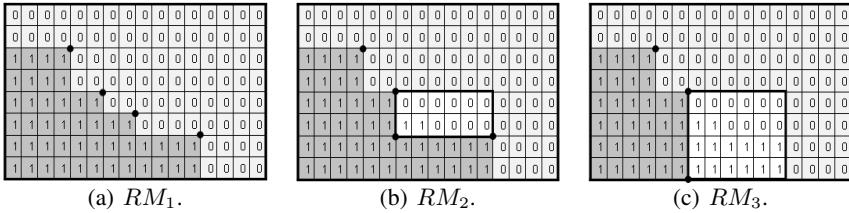


Fig. 2. Different routing maps

Although routing map can guide sensors to find non-routed VCs, it is infeasible when a sensor network involves large number of sensors. One possible solution is using greedy algorithm to compact the routing map matrix. Due to the page limit, we will not discuss the detailed technique here.

4.2 Balance of Energy Consumption

In order to balance the energy consumption of sensors, ASA builds up different routes periodically. During one period of time T , the route is expected to be the same so that only updates need forward. We first describe how to forward messages when a new route is built up. Then, we discuss forwarding updates to the sink along the constructed route. Rules R_1 and R_2 describe how to forward messages along the route at the time a new route is built up.

- R_1 . For each routing sensor, it appends one sensing value and the member sensors ID of its VC to the forwarding message.
- R_2 . If there are more than one sensor in a VC has been routed, then only the last routing sensor needs append message.

For different period of routing time, sensors find a different route to balance the energy consumption in the network. Each sensor in the network keeps its routing history and is aware of its remaining energy. Also, ASA utilizes Gossip protocol [6] to intelligently find the new valid route. For instance, at the first step of a new time period T , a new routing sensor s_a is chosen and sensor is selected s_b as its downstream routing node. s_b checks its routing history and remaining energy. In case that s_b serves a routing sensor in recently time period or has no enough energy to forward messages, it will not forward messages further. After s_a sends message to s_b , it can listen messages sent from s_b although those messages are not sent to s_a according to Gossip protocol. If s_a cannot hear message from s_b , then s_a knows that s_b does not forward its message. So, s_a chooses another sensor s'_b . In this way, a sensor can self-determine its role of

routing according to its own status. There is one exception that s_a failed to monitor the broadcast message from s_b , then s_a chooses another routing sensor and meanwhile s_b continues to forward messages. Therefore, at least two routes will arrive the sink.

5 Failure-Resilient Data Collection

According to our observations over real experiments, there are two major failures in data collection: (i) node failure: a sensor is power off, and (ii) forwarding failure: a message gets lost when it is forwarded along a certain routing path.

Node Failure. Our approach is robust to node failure. In our DVC model, a sensor forwards its message only after it detects an update reading. When a sensor s is power off, it acts as no update detected. In this case, if the neighbors of s do not report any updates, then it assumes that readings in the region of s do not change. If neighbors of s report updates, s is either inside or on the boundary of the changed region. For the first case, a new VC covering s is constructed, since s is the only sensor that has a different value (i.e. keep old value) from those of its neighbors. For the second case, a sensor on the boundary of the VC will not affect the sensing value much. When s is chosen to forward message, the previous sensor s_a cannot listen any message from s using Gossip protocol, then s_a will choose another sensor to forward its message as discussed in Section 4.1

Forwarding Failure. Forwarding failure is a critical problem to our approach, since we use single path to forward values of all update VCs to the sink. If one sensor along the routing path fails, all previous collected messages will be lost. In order to address this issue, we use gossip protocol to make our approach robust. Consider a routing path $s_1 \rightarrow s_2 \rightarrow s_3$ and assume that s_2 failed forwarding message to s_3 . There are three possible reasons that cause such a failure: (i) s_3 failed to receive the message; (ii) the radio signal between s_2 and s_3 is breached; or (iii) s_2 failed to broadcast its message. For the first two cases, if s_2 cannot listen a message from s_3 after s_2 forwarding message, s_2 will choose another sensor and resend message. For the third case, s_1 cannot listen messages sent from s_2 , then s_1 will resent its message to another sensor.

The side-effect of this strategy is that s_3 correctly forwards message to the next sensor, but s_2 may not detect the message. Thus, s_2 makes wrong judgement that forwarding failure happens in between $s_2 \rightarrow s_3$. The immediate result is that two routing paths are constructed, one is from s_3 to its next sensor s'_3 and the other is from s_2 to another sensor s'_2 . Thus, energy is wasted. As we discussed, for a period of time T , sensors use the same route to forward messages. After the two routes are built up, s_2 chooses a path $s_2 \rightarrow s'_2$ to forward message, whereas, s_3 assumes that the value of previous sensors (e.g. s_2) does not change, since it does not get update message from s_2 . After sink receives messages from these two routes, sink records all updates and chooses one route to forward updates in the remaining of T .

6 Experimental Results

We simulated the data collection scenario of a light monitoring application in our experiments. In order to simulate a network with large number of sensors, we developed a simulator to construct a network based on our lab data set. We built up a 30×40 grid, where each cell in the grid contains one sensor node. We set 10K communication edges but varied the degrees of different sensors to imitate dynamic network topology. We randomly chose several cells to take the values of our lab data set as their readings and partition the grid from 40 to 60 value regions. Our simulator can vary number of node failures and forwarding failures. The sensing values already contained sensing failure, since they are generated based on real data set.

We let each sensor read values every 5 seconds and let routing time period be 1000 seconds. We let each sensor to communicate at most 20K packets before it exhausted, where a sensor reading is 2 bytes, and each packet contains 49 bytes based on our application development experiences on the Crossbow MICA2 motes [7]. The initial battery capacity of each sensor is set to the simulated cost of 20K forwarding packets (around 33K receiving packets or 50K sensing operations), i.e., the energy consumption is calculated as $E = x + 0.6y + 0.4z$, where x is the number of forwarding packets, y is the number of receiving packets, and z is the number of sensor readings. When $E > 20K$, we say a sensor “died”. We omit the energy cost of computing in each sensor. Basically, we divide our experiments into two parts: 1) energy consumption comparison of ASA and other approaches on data collection and 2) energy consumption of ASA during its self maintenance.

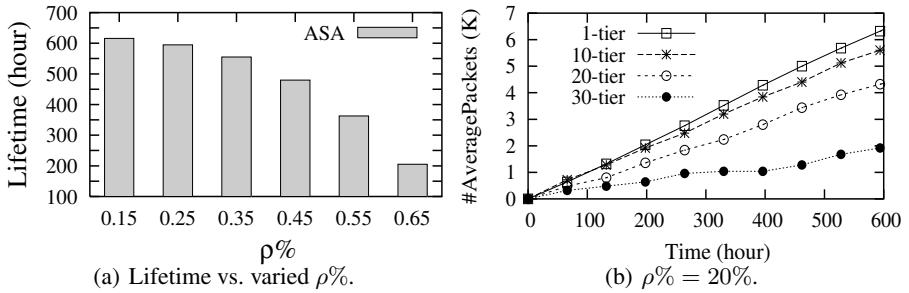
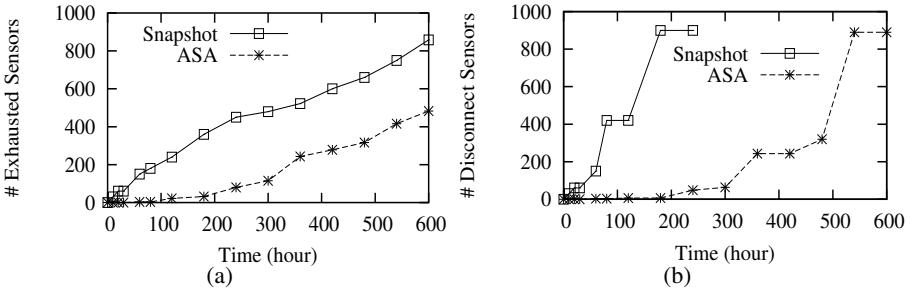
To evaluate the effectiveness of ASA, we did extensive experiments measuring the followings:

Network Life Time. As defined in Section 1, the lifetime is defined to be related with $\rho\%$ connected sensors in the network. We considered the readings of the network to be unreliable anymore, whenever the ratio of the disconnected sensors exceeds a threshold $\rho\% \times n$, where n is the number of sensors in the network. Fig. 3(a) shows that we varied ρ values to test the lifetime of the network using the synthetic data set. When ρ increases, the lifetime of the network drops.

Energy Balance. Fig. 3(b) is energy-balanced test under $\rho\% = 20\%$. We used TAG model [8] to classify sensors in “tiers” and evaluate energy consumptions of different tiers. We chose nodes that have different distances to the sink to do the test and considered three kinds of energy consumptions: forwarding message, receiving message, and sensor readings as described in the first part of this section. The figure shows that ASA can effectively decrease the energy consumption ratio of inner “tier” sensors to outer layer sensors.

Energy Consumption Comparison between Snapshot [10] and ASA. We implemented snapshot and compare its performance with ASA. Fig. 4 shows comparison results between Snapshot and ASA.

We show the increase on the number of exhausted nodes in Fig. 4(a). As we expected, we found that the first node failure using ASA at the 60 hours, which is later than Snapshot. This is because ASA is an energy-balanced approach. There are 30 nodes in the first layer of the network, after these nodes failed, the outer layer nodes were disconnected to the sink. Therefore, in Fig. 4(b), we can observe the network produced

**Fig. 3.** Energy consumption**Fig. 4.** Lifetime comparison, $\rho\% = 20\%$

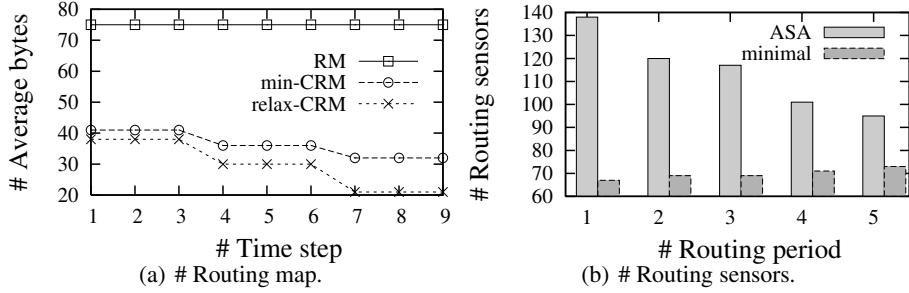
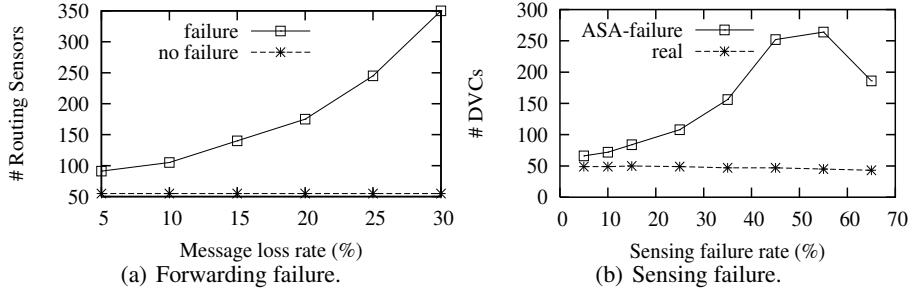
reliable readings within 600 hours when $\rho\%$ is set to 20% for both two approaches. The network lifetime using ASA is much longer than that using Snapshot.

We also found that only small number of outer layer sensors encounter an energy problem before inner tier nodes became exhausted. Therefore, the number of disconnected nodes in Fig. 4(b) increases much sharper than the number of exhausted nodes in Fig. 4(a).

Effect of Routing Map. We evaluate the sizes of different types of routing map and their impact to the number of routing sensors (see Fig. 5).

Fig. 5(a) shows the comparison of different sizes among routing map types. We compared three types of routing maps, which are (i) routing map without compression (denoted RM), (ii) compact map with minimal size (denoted min-CRM), and (iii) relax compact routing map (denoted relax-CRM). As discussed in Section 4, routing map is useful for building up or maintaining a data routing during the start of the routing period of time and updates. Fig. 5(a) depicts the used routing map size when build up a new routing. Since RM describes all sensors in the network, its size kept stable. Min-CRM and relax-CRM required less bytes to transmit routing navigation messages. Fig. 5(b) shows the number of routing sensors needed when adopted min-CRM technique at different period of times.

Impact of Failures. We tested forwarding failure and sensing failure using our synthetic data set. We used message loss rate to quantify forwarding failures. Fig. 6(a) shows the

**Fig. 5.** Self-adjusted routing map size**Fig. 6.** Impact of failures

impact of quality of routing sensors when varying message loss. We let the probability of message loss vary from 5% to 30%. We found that ASA needed much more routing sensors when increases message loss rate. It is not surprising since more forwarding failures sensors to find longer paths to forward updates to the sink.

Fig. 6(b) shows the impact of energy consumption when varying sensing failure rate, i.e. ratio of number of incorrect sensing nodes to all sensor nodes in the network. We set a fix number of VCs in advance and test the effect of sensing failure rate. When sensing failure rate is small, the number of DVCs is close to the real number of VCs, 50. However, with more sensing failures happen, sensors may use wrong sensing values to construct small DVCs, which cause the increases of the number of DVCs. This number climbed to a peak and then drop sharply, as we observed in our lab experience, most sensors under energy may produce the same sensing values.

7 Related Work

A number of research work have been published on energy efficient data collection over sensor networks in database domain. We can classify them into centralized [11–17] and decentralized control approaches [8, 10, 18–23].

Centralized Control. Most of the existing prediction model-based approaches adopt centralized control strategy. A prediction model [14–16] is generated at the sink (or

PC base station) based on the collected historic data and the sink further disseminates the model to the network. Both sensor and sink maintain a prediction model of how data evolves and keep the model in sync. BBQ[11] is a model-driven data acquisition framework that adopts a trained statistical model. BBQ can limit the number of sensor readings required to answer a posed query with high confidence. [11] uses a global model to capture dependencies based on a relatively stable network topology. Both *Ken* framework[13] and Kalman Filter[12] fit the data into a model. Sensing data will be forwarded to the sink only when they are beyond an approximation threshold. A disjoint-clique model is also proposed in [13] to partition sensor attributes to multiple localized clusters. CONCH [2] is value-based data collection approach. The base station globally determines and disseminates a minimal CONCH plan into the whole network so that both temporal and spatial suppression can be combined for saving as much communication energy cost as possible.

Different from the above centralized control approaches, our work, ASA, lets an individual sensor self-adaptively makes local decisions for data suppression without global controller, which enables ASA to deal with the changes of sensing data, network topology, sensor deployment and failures. Considering these dynamic cases, data distribution update may frequently arise and it is hard to find a perfect model adapted.

Decentralized Control. TAG[8, 20] can be put into the category of decentralized control approaches. Upon receiving a broadcast message from the sink, each individual sensor self-determines their parent nodes and build up a routing tree rooted at the sink. The most related work to ours is Snapshot[10], which also deals with both data and network dynamics. The primary difference between Snapshot and ASA is the definition of clusters and forwarding path chosen. In Snapshot, the sensor nodes of a cluster are within one hop count and only the chosen representative node can produce approximate data[24]. ASA, however, can partition the network into several multi-hop disjoint VCs. Any sensors in a value-based cluster can in charge of forwarding task. [18, 21] uses selective sampling technique to increase the network lifetime. A quiet similar cluster definition to DVC is proposed in [19]. Different from [19], ASA self-adaptively finds a “minimal” routing path to concatenate all clusters to the sink. Using this way, ASA saves more communication cost. Furthermore, ASA only forwards updates to the sink. In addition, self-adaptive routing protocols for sensor network are well-developed in network domain[9]. The above network-centric approaches take sensor readings into consideration, whereas, ASA towards data-centric sensor networks, combines clustering using the routing path for expansion and maintenance of DVCs to increase the network lifetime.

8 Conclusion

In this work, we present ASA approach, which is an energy-efficient and balanced data collection method based on adaptive map forwarding strategy. Moreover, ASA investigates the spatial correlations between sensor readings to provide an energy efficient route without knowing the global network topology of WSNs. The experimental results demonstrate that ASA provides significant energy savings and equal energy consumption among all sensor nodes.

References

1. Tan, H., Körpeoğlu, İ.: Power efficient data gathering and aggregation in wireless sensor networks. *SIGMOD Record* 32(4), 66–71 (2003)
2. Silberstein, A., Braynard, R., Yang, J.: Constraint chaining: On energy-efficient continuous monitoring in sensor networks. In: *SIGMOD* (2006)
3. Sharaf, M.A., Beaver, J., Labrinidis, A., Chrysanthis, P.K.: Balancing energy efficiency and quality of aggregation data in sensor networks. *VLDB.J* 13, 384–403 (2004)
4. Xu, Y., Heidemann, J., Estrin, D.: Geography informed energy conservation for ad hoc routing. In: *MobiCom*, pp. 70–84 (2001)
5. Moore, D., Leonard, J., Rus, D., Teller, S.: Robust distributed network localization with noisy range measurements. In: *SenSys* (2004)
6. Kempe, D., Kleinberg, J., Demers, A.: Spatial gossip and resource location protocols. In: *STOC* (2002)
7. Crossbow Inc. Mpr-mote processor radio board user's manual
8. Madden, S., Franklin, M.J., Hellerstein, J.M., Hong, W.: Tag: a tiny aggregation service for ad-hoc sensor networks. In: *OSDI* (2002)
9. Buragohain, C., Agrawal, D., Suri, S.: Power aware routing for sensor databases. In: *INFOCOM* (2005)
10. Kotidis, Y.: Snapshot queries: Towards data-centric sensor networks. In: *ICDE* (2005)
11. Deshpande, A., Guestrin, C., Madden, S., Hellerstein, J., Hong, W.: Model-driven data acquisition in sensor network. In: *VLDB* (2004)
12. Jain, A., Chang, E., Wang, Y.: Adaptive stream resource management using kalman filters. In: *SIGMOD* (2004)
13. Chu, D., Deshpande, A., et al.: Approximate data collection in sensor networks using probabilistic models. In: *ICDE* (2006)
14. Silberstein, A., Gelfand, A., Munagala, K., Puggioni, G., Yang, J.: Making sense of suppressions and failures in sensor data: A bayesian approach. In: *VLDB*, pp. 842–853 (2007)
15. Yang, X., Lim, H., Özsu, M.T., Tan, K.-L.: In-network execution of monitoring queries in sensor networks. In: *SIGMOD Conference*, pp. 521–532 (2007)
16. Ahmad, Y., Nath, S.: Colr-tree: Communication-efficient spatio-temporal indexing for a sensor data web portal. In: *ICDE*, pp. 784–793 (2008)
17. Li, J., Deshpande, A., Khuller, S.: On computing compression trees for data collection in wireless sensor networks. In: *INFOCOM*, pp. 2115–2123 (2010)
18. Gedik, B., Liu, L.: Energy-aware data collection in sensor networks: a localized selective sampling approach. In: *IEEE TPDS* (2006)
19. Meka, A., Singh, A.K.: Distributed spatial clustering in sensor networks. In: Ioannidis, Y., et al. (eds.) *EDBT 2006. LNCS*, vol. 3896, pp. 980–1000. Springer, Heidelberg (2006)
20. Bhattacharya, A., Meka, A., Singh, A.K.: Mist: Distributed indexing and querying in sensor networks using statistical models. In: *VLDB*, pp. 854–865 (2007)
21. Lin, S., Arai, B., Gunopulos, D., Das, G.: Region sampling: Continuous adaptive sampling on sensor networks. In: *ICDE*, pp. 794–803 (2008)
22. Li, Z., Liu, Y., Li, M., Wang, J., Cao, Z.: Exploiting ubiquitous data collection for mobile users in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 24(2), 312–326 (2013)
23. Wang, C., Ma, H.: Data collection in wireless sensor networks by utilizing multiple mobile nodes. *Ad Hoc & Sensor Wireless Networks* 18(1), 65–85 (2013)
24. Wang, C., Ma, H., He, Y., Xiong, S.: Adaptive approximate data collection for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 23(6), 1004–1016 (2012)

R-Focus: A Rotating Platform for Human Detection and Verification Using Electronic and Visual Sensors

Fan Yang¹, Yiran Xuan², Sihaoy Ding¹, Adam C. Champion¹,
and Yuanfang Zheng¹

¹ The Ohio State University, Columbus, OH 43210, USA

² Dublin Jerome High School, Dublin, OH 43016, USA

Abstract. Prolific sensing devices like mobile phones and video cameras can sense electronic and visual information, respectively, which can help detect and verify a person. Accurate detection and verification of a person's identity from this sensed data is important for enabling applications such as surveillance and e-health. This is challenging due to sensed data heterogeneity, measurement noise, and the prohibitive cost of specialized equipment. This paper proposes R-Focus, a rotating platform with electronic and visual sensors that can detect and verify a person of interest in an area. R-Focus performs electronic and visual data collection and rotates based on the collected data. R-Focus uses the electronic identity information for a person to gather visual identity information for the person, who is verified and tracked. We implement R-Focus on commercial off-the-shelf hardware and software. Our experimental evaluation shows R-Focus's promise for detecting and verifying a person of interest.

Keywords: Wireless, rotation, verification.

1 Introduction

1.1 Motivation

Today, various sensing devices are prolific in society. In particular, static video cameras and mobile smartphones are widespread sensing devices that can sense identifying information about a person. Video cameras sense a person's appearance and activities within videos. We refer to a person's unique visual (V) information (such as facial appearance) as this person's visual identity (VID). Mobile devices emit electronic (E) signals containing various textual device identity information such as devices' IMSIs, WiFi and Bluetooth MAC addresses, and NFC identifiers. As such, we refer to these pieces of electronic information as the person's electronic identity (EID).

Accurate detection and verification of a person's identity within a (large) volume of sensory data is essential for enabling various applications in a *cost-effective* manner. Example applications include surveillance for public safety [1],

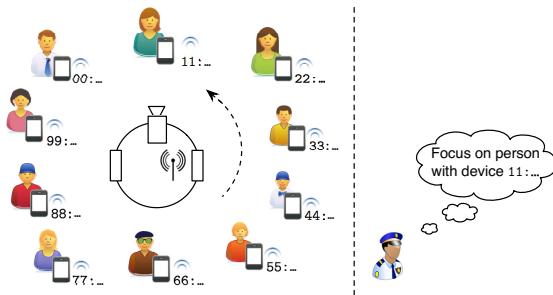
e-health [2], and object tracking [3]. This task entails associating non-trivial heterogeneous identity information about a person, the EID and VID. Challenges arise from information heterogeneity and erroneous measurements. In this context, EIDs are textual pieces of information whereas VIDs are images (i.e., matrices of pixel values). EIDs identify mobile devices carried by persons, not persons themselves. Both electronic and visual measurements can suffer errors. Electronic signals' RSSIs vary considerably due to small-scale wireless fading. Visual occlusions and varying illumination can hamper person identification. Moreover, it is challenging to solve this problem using inexpensive commercial off-the-shelf (COTS) equipment. Though some directional antennas can precisely determine a signal direction, they tend to be very expensive and specialized. Accomplishing this task with COTS directional antennas is non-trivial. Furthermore, real-time image transmission and processing is hard, especially on resource-constrained embedded systems. The image processing workload needs to be reduced in order to realize timely cost-effective visual processing on such systems. Electronic signals may afford an opportunity to increase the efficiency of image processing.

1.2 Our Contributions

This paper presents R-Focus, which is an automatic Rotating platform carrying electronic and visual sensors. R-Focus locates a person of interest in its camera's field of view carrying a mobile device with a specific EID. To do so, R-Focus leverages *spatial information* shared among the person's EID and VID. R-Focus collects people's electronic information (e.g., WiFi MAC addresses of people's mobile devices) and visual information (e.g., faces). R-Focus uses this information to rotate until it faces an EID corresponding to a person of interest. For example, R-Focus can use the EID of a person's mobile device to guide its rotation to face the person of interest. Next, R-Focus performs visual detection and verification on the person. For instance, R-Focus can detect faces in its camera's field of view and perform facial verification using a database of faces stored on the platform. True to its name, R-Focus maintains focus on the person of interest even if he/she moves. R-Focus is well-suited for security purposes; it can verify the presence and/or identity of persons carrying devices that emit electronic signals.

The following usage scenario illustrates R-Focus in action. Consider a conference where each attendee needs to be verified as shown in Fig. 1. R-Focus's electronic sensor can obtain attendees' identity information such as their mobile phones' WiFi MAC addresses. As the antenna is directional, R-Focus can ascertain the specific direction of each electronic signal via its RSSI. With an attendee's EID, R-Focus rotates to face the direction where this EID was emitted. The onboard camera focuses in that direction to capture the attendee's VID (the person's face). R-Focus detects the attendee's face in the image and performs face verification; the attendee's face is compared with a database of registered conference attendees' faces. If there is a match, R-Focus verifies the attendee's presence at the conference.

In summary, this paper makes the following contributions:

**Fig. 1.** R-Focus usage scenario

- We propose a Rotating platform called R-Focus that uses electronic and visual information in tandem and finds a person carrying a specific mobile device. We integrate E and V operations in this system to find and verify the person of interest.
- We use the platform’s rotation ability and the antenna’s directionality to estimate the person’s direction. Two different approaches, *Progressive Maximum Method* and *Model Based Method*, are proposed and compared.
- The person’s identity is verified via face verification. We design mechanisms to find and verify the target person.
- We implement our design and algorithms on R-Focus’s hardware platform. We build a client-server infrastructure using COTS hardware and software (i.e., a mobile robot and a laptop). We perform real-world experimental evaluation of our platform’s design and performance.

The rest of this paper is structured as follows. We review related work in §2. §3 describes R-Focus’s design. §4 describes R-Focus’s implementation and experimental evaluation. §5 gives final remarks.

2 Related Work

Some work has examined how to use wireless receivers’ directionality and rotation ability to determine the signal source direction. Nemmaluri et al. [4] sweep a room using a steerable directional antenna in order to localize an RFID tag. They propose coarse, localize, and fast scan strategies to address different scanning scenarios. In robotics, a dual-directional antenna is used for navigation and target tracking [5] so the robot obtains the direction of arrival (DoA) of the signal of interest. This kind of work is usually associated with active RFID technology. However, such work needs specially designed directional antennas that are not readily available. In other work, “simulated” directional antennas are used to determine the signal source. This work leverages a rotating wireless receiver and a signal-blocking obstacle to emulate the function of a directional antenna [6]. [6, 7] use this “emulated directional antenna” to localize access points and users. Teng et al. [8] propose another way whereby wireless receivers move in particular patterns to detect the signal source’s DoA. But the reliability of such “emulated”

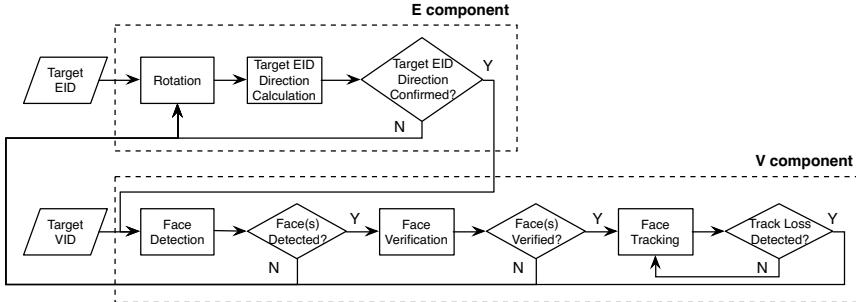


Fig. 2. R-Focus workflow

directional antennas is limited. Specialized devices such as a modified Intel 5300 network interface card [7] are needed for localization.

Meanwhile, great improvements have taken place in the area of object detection, especially regarding the human body. There is considerable existing work [9], among which Histograms of Oriented Gradients (HOG) feature-based algorithms [10] are widely used. One state-of-the-art algorithm for human detection is the Deformable Part Model (DPM) [11], which models objects as a combination of several deformable parts. In addition, there is much existing work on face detection [12, 13] using skin color, neighboring pixel patterns, and other cues. The Viola-Jones face detection method [12] is widely used. Some approaches explicitly address side view face recognition [14].

There is some work on sensor fusion between electronic and visual data. Electronic data can help improve visual processing's efficiency and accuracy. An electronic filtering process can significantly reduce the workload for human retrieval in video sequences [15]. Electronic and visual data fusion is also used in improving the accuracy of localization. [16] presents an accurate human localization approach by first performing visual and electronic localization, then solving a bipartite matching problem. [17] borrows visual information to rectify distance estimation based on RSSI in order to improve localization accuracy.

3 R-Focus Design

3.1 System Workflow

Fig. 2 illustrates the workflow of R-Focus. The system consists of two parts: the *rotating electronic direction sensor* and the *visual verification module*. The rotating electronic direction sensor is a sensor with a directional antenna that measures an EID's direction. The visual verification module performs automatic face detection and verification to verify the target person's identity.

Suppose we aim to locate a person in a room and we have the person's EID and VID. First, the rotating electronic direction sensor rotates to face the EID's direction. After the target person's direction is obtained electronically, face detection and verification are performed on the image captured in this direction.

Ideally, the correct face appears and is verified with the input VID. If any failure occurs, the above procedure is repeated.

R-Focus implements four basic functions:

- *Collecting electronic and visual data*: A special WiFi MAC address collector is integrated on R-Focus that monitors MAC addresses from surrounding users' mobile devices and measures the signals' RSSIs. A camera is also connected to the platform to collect visual data. Specifically, people's faces are used their VIDs and a face detection procedure is implemented.
- *Sensing-guided rotation*: As a rotating platform, R-Focus's rotation is guided by sensing data. Thus, based on previous sensing data, the platform can automatically adjust its rotating and direction for further data collection.
- *EID-guided VID finding*: R-Focus calculates an EID's specific direction, then the corresponding VID is found in this direction.
- *Target person verification*: After the target person is found, R-Focus will verify the person with face verification.

3.2 Rotating Electronic Direction Sensor

We use a rotating directional antenna to estimate the direction of an EID. Our rationale is as follows: when the directional antenna faces a different direction, the RSSI measurement of the (fixed position) signal source differs due to the directional antenna's radiation characteristics. Ideally, the receiver will get the strongest RSSI when its main lobe faces the EID. In this sense, the received *RSSI pattern* indicates the direction of the EID.

Definition 1. *The RSSI pattern defines the variation of an antenna's RSSIs as a function of the signal source direction away from the antenna.*

The RSSI pattern is similar to an antenna's *radiation pattern*. Both patterns express variation of received signal power as a function of incident angle. Actually, an antenna's radiation pattern is the antenna's power gain in every direction. Power gain is a relative value and only depends on antenna properties such as shape, size, structure, and material. The RSSI pattern is more practical; it is the actual absolute received signal strength in a specific wireless environment. It depends on the radiation pattern, the relative position of the signal source with respect to the antenna, and the wireless transmission channel, all of which are subject to multipath effects. The RSSI pattern covers every angle in spherical coordinates. This paper only focuses on the RSSI pattern for the antenna's horizontal plane, which we call the *horizontal RSSI pattern*.

Due to limitations of the rotator's mechanical structure and the direction sensor's accuracy, it is impractical to accurately collect RSSI at each horizontal angle. Thus, we uniformly divide 360° into several segments. The RSSIs collected in each segment are averaged to represent the RSSI value at the segment's central angle in the horizontal RSSI pattern. This can mitigate RSSI errors arising from each measurement. We call the size of each segment (in degrees) the *resolution* of the horizontal RSSI pattern. Let *res* denote the resolution, $N = \lceil 360^\circ / \text{res} \rceil$

denote the number of segments, and $RSSI(n)$ denote the average RSSI value measured in the angular interval $[(n - 0.5)res, (n + 0.5)res]$.

Now we develop two strategies to determine the EID's direction: the *progressive maximum method* and the *angular correlation method*.

Progressive Maximum Method (PMM). Intuitively, we find the direction with the maximum RSSI. Let $RSSI(x)$ denote the RSSI measured in direction x . We need to solve the following problem to find the EID's direction:

$$\arg \max_{x \in [0, 2\pi]} RSSI(x). \quad (1)$$

However, multipath effects originating from the signal transmission environment can distort RSSI, making RSSI inaccurate. This means the source's direction is not necessarily the one with the maximum RSSI. Thus, it is reasonable to average the RSSIs measured in neighboring angular intervals to smooth the noise. A smoothing operation within $2s + 1$ intervals is

$$RSSI_{smooth}(n) = \frac{1}{2s+1} \sum_{i=n-s}^{n+s} RSSI(i \bmod N). \quad (2)$$

The proposed *progressive maximum method* works as follows. First, we scan the RSSI values in all directions with low resolution and perform smoothing. From this result, we can judge in which angular range the signal source lies (e.g., a semicircle). Then we reduce the sensing range, improve the resolution, and perform another scan. In each iteration, we reduce the scan range to half the previous angular range whose central angle is determined by Equation (1). The overall procedure is shown in Procedure 1. *RotateToAngle()* rotates the platform so the directional antenna faces *current_angle*; the angle is the orientation sensor's output. *MeasureRSSI()* measures the EID's RSSI several times and averages the results. *FindMaxRSSIIndex(rssi_map)* finds the index in *rssi_map* with the maximum RSSI value.

Procedure 1. Progressive Maximum Method

```

1: res  $\leftarrow 40^\circ$ 
2: start_angle  $\leftarrow 0^\circ$ 
3: while res  $\geq 10^\circ$  do
4:   N  $\leftarrow \lceil 360^\circ / res \rceil$ 
5:   rssi_map  $\leftarrow \{\}$ 
6:   for i = 0 to N - 1 do
7:     current_angle  $\leftarrow i \cdot res$ 
8:     RotateToAngle(current_angle)
9:     rssi  $\leftarrow MeasureRSSI()$ 
10:    rssi_map  $\leftarrow rssi\_map \cup \{(i, rssi)\}$ 
11:    index_maxrssi  $\leftarrow FindMaxRSSIIndex(rssi\_map)$ 
12:    start_angle  $\leftarrow ((index\_maxrssi - \lfloor N/4 \rfloor) \cdot res) \bmod 360^\circ$ 
13:    res  $\leftarrow res/2$ 

```

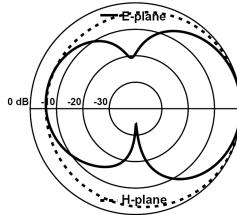


Fig. 3. Directional antenna radiation pattern

Model Based Method (MBM). From the directional antenna radiation pattern shown in Fig. 3, which is a small lightweight COTS log-periodic directional antenna, we see that the directions of the main lobe and signal attenuation can indicate the direction of the signal source. For example, the back lobe faces opposite the signal source direction and the direction with the weakest RSSI is perpendicular to the signal source direction. Using this observation, we leverage all these pieces of information to detect the target’s direction.

Towards this end, we calculate the similarity between the horizontal RSSI pattern to a standard pattern to determine the signal source direction. The standard pattern can be the nominal antenna radiation pattern. But this approach entails calibrating the standard pattern every time R-Focus rotates. Thus, we use the antenna’s radiation pattern and perform angular correlation between it and rotations of the horizontal RSSI pattern. The rotation with the maximum correlation with the radiation pattern indicates the signal source’s direction. We achieve this by solving the following problem:

$$\arg \max_{i=0,1,\dots,N-1} \sum_{n=0}^{N-1} \text{RSSI}((n-i) \bmod N) \cdot G(n \cdot res, 0), \quad (3)$$

where $G(\theta, \varphi)$ is the power gain of the antenna in direction (θ, φ) . To solve this problem, we rotate the horizontal RSSI pattern to some angle and perform angular correlation with the antenna’s radiation pattern. The angle with the maximum correlation is the direction of the signal source.

Multipath effects and noise may distort the received signal strength pattern from an antenna’s radiation pattern measured in an open environment. But this method still works well in our working scenarios proposed in §1 where all the EIDs surround R-Focus and have line-of-sight paths as shown in our experimental evaluation (§4.2).

3.3 Visual Verification Module

R-Focus’s electronic sensor resolution is limited and multiple persons may be in the area determined by this sensor. Thus, we propose using a visual sensor (i.e., a camera) to locate and verify the target person.

After we determine the direction of the target person’s EID, face detection is performed to gather the person’s VID. We perform face detection instead of

human body detection as cameras cannot see each person’s entire body when people sit around a table facing the center thereof, a typical working scenario.

In order to reduce the false positive rate of face detection, we intersect the results of two different face detection algorithms. We leverage Viola-Jones [12] and LBP cascade classifier [18] face detection. We determine intersection by computing the percentage of overlapping areas of the bounding boxes.

After faces are detected, their identities need to be verified. We can assume that the target person’s face images are in a database. We partition our database into two parts: positive samples comprising the target person’s training face images; and negative samples consisting of many randomly gathered face images that do not belong to the target identity. These two parts are labeled as two classes and Fisher Linear Discriminant Analysis (FLDA) [19] is leveraged for model training. During the test process, the vectorized test images are projected onto the LDA subspace computed in the training process; the projected vectors are used as feature vectors for verification. Euclidean distances between feature vectors for test and training face images are calculated. The identity of the testing face is verified if and only if the distance between the feature vectors is closer to the positive samples than the negative samples.

After identity verification, our system tracks the target person. To achieve this, the visual sensor is calibrated to obtain its focal length. Combined with the physical size of the camera’s charge-coupled device (CCD) and the image resolution, the angle between the center column of the image and the column of the detected face can be obtained from Equation (4):

$$\theta = \arctan(\text{CCD_width}/(\text{number_of_columns} \cdot \text{focal_length})). \quad (4)$$

The platform rotates to center the face in the image’s central area. This process is performed at every timestamp such that our system always focuses on the face in the image’s central area and tracks the person as he/she moves.

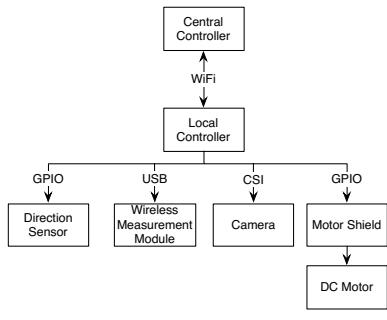
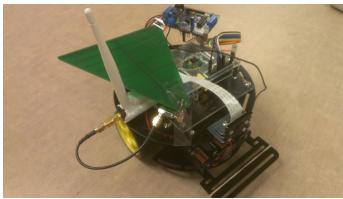
4 Implementation and Evaluation

4.1 Implementation

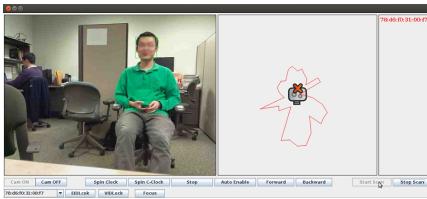
We implement a prototype of R-Focus. This section describes the prototype’s architecture and implementation details.

Fig. 4 shows the R-Focus prototype’s architecture. The architecture has three main components: (1) user interface and central controller; (2) local controller; and (3) enabling functional units. Each component is described below.

User interface and central controller. This component processes user instructions and issues commands to the local controller for electronic sensing, camera capture, and motor control; *Local controller.* This module is implemented on a Raspberry Pi. It receives commands from the central controller and directly controls all functional units; *Functional units.* There are four functional units on R-Focus connected to the local controller that perform specific functions: (1) The *direction sensor* senses R-Focus’s orientation; (2) The *wireless measurement module* is a WiFi NIC operating in monitor mode; (3) The *camera*

**Fig. 4.** Function block**Fig. 5.** R-Focus prototype**Table 1.** Functional modules

WiFi NIC	Tenda W311Ma
Directional antenna	WA5VJB log-periodic-array antenna
Camera	Raspberry Pi camera board (5 MP)
Direction sensor	Freescale MAG3110 3-axis magnetometer
Rotator	SainSmart L293D motor driver shield; 2WD Arduino-compatible mobile platform

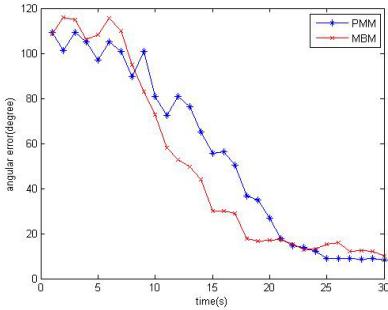
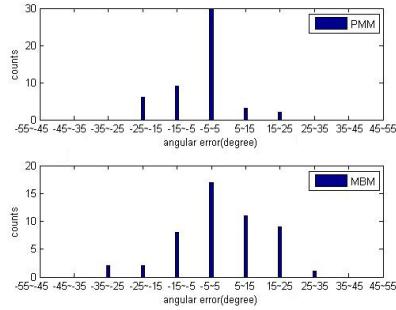
**Fig. 6.** R-Focus control panel

captures images of the surrounding area; (4) The *DC motor controller* provides the platform's rotation ability.

Hardware. We implement the central controller on a Lenovo Y570 laptop with an Intel Core i5 2.30 GHz CPU and 4 GB of memory. We implement the local controller on a Raspberry Pi Model B with a 700 MHz ARM CPU and 512 MB of memory. Table 1 shows functional modules.

The R-Focus platform is shown in Fig. 5. The WiFi NIC, camera, and directional sensor are connected to the Raspberry Pi via USB, camera serial interface (CSI), and GPIO, respectively. We leverage a 2-wheel mobile robotic platform to perform rotation. The Raspberry Pi controls the motors via the L293D motor driver shield. This implementation lets us easily enable other forms of motion besides rotation as platform enhancements.

Software. The central controller program interacts with the local controller, processes data and queries, and displays results. Textual data (e.g., instructions, direction sensor data, and WiFi RSSIs) are conveyed via TCP connection. Images captured by the Raspberry Pi's camera are transferred to the laptop via mjpg-streamer [20]. A graphical user interface (GUI) is designed as shown in Fig. 6. Users can control platform motion and find a specific target via the GUI, which shows real-time camera imagery, face detection results, each EID's RSSI directional pattern, and the directions of EIDs and VIDs. The local controller performs data collection following the central controller's instructions from each function unit and controls platform's motion.

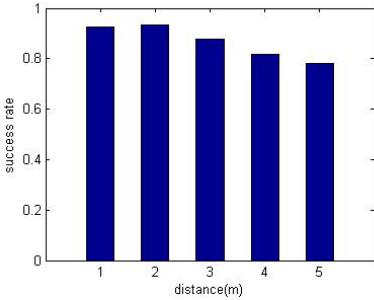
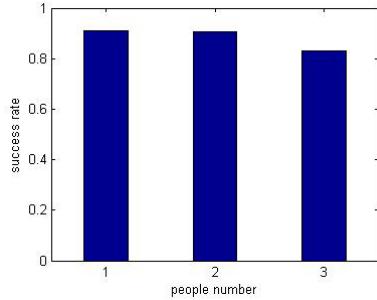
**Fig. 7.** Angular error vs. time**Fig. 8.** Final angular error distribution

4.2 Experimental Evaluation

We conduct experimental evaluation in a $10\text{ m} \times 10\text{ m}$ laboratory. A table lies at the center of the room; different numbers of people carrying mobile phones sit around the table at various distances from its center. R-Focus rotates on the table until it finds the person carrying the mobile phone with the target EID; then it verifies the person's VID. It takes $\sim 15\text{ s}$ for the platform to rotate 360° .

First, we evaluate the performance of the rotating electronic direction sensor in terms of time efficiency and angular accuracy. A typical RSSI pattern we measured with R-Focus is illustrated in Fig. 6. It is generally consistent with the antenna's radiation pattern shown in Fig. 3.

- *Time efficiency:* Initially, R-Focus faces a random direction. Multiple 360° rotations are needed (capturing RSSI measurements at different angles) for estimating the target EID's direction. Over time, the angular difference between the estimated and true directions decreases, finally yielding a stable estimate. Fig. 7 shows this process. 50 experiments are performed with 1 person carrying a mobile phone 2–4 m away from R-Focus. Progressive Maximum Method's (PMM's) and Model Based Method's (MBM's) angular errors converge. As PMM rotates gradually in order to achieve high resolution, its convergence time is greater than MBM's. PMM's accuracy is high as the RSSI pattern is not "ideal" due to multipath effects and noise. In average, PMM takes 25 seconds to achieve a stable measurement, and the average angular error is about 10° , while BMM takes 17 seconds to converge with a larger angular error.
- *Direction error:* Fig. 8 shows the average absolute angular error distribution of PMM and MBM after 50 experiments. For PMM, 60% of the error lies within 5° (the resolution in our experiments is 10°) and another 24% lies within 15° . For MBM, 34% of the error in the results lies within 5° , another 38% lies within 15° , and the error lies within 25° with high probability. We see that PMM achieves higher accuracy in estimating the final EID direction. This is reasonable since in our application scenario, EIDs are near R-Focus and the signal strength from the direct path dominates. In contrast, the

**Fig. 9.** Success rate vs. distance**Fig. 10.** Success rate vs. number of people

RSSI pattern is biased from the standard radiation pattern model due to complex transmission environments. R-Focus is tolerant to direction error as the camera's field of view is 60° in our implementation.

From Fig. 3, we see the directionality of our antenna is limited. Alternatively, we could use a more advanced directional antenna with higher resolution, but this is costly and the antenna size needs to be much larger in order to work with WiFi frequencies. With our small commercial off-the-shelf antenna, we can achieve desirable performance at lower cost.

Next, we evaluate R-Focus's overall success rate. The device senses the target EID's direction, rotates facing this direction, performs face detection, and verifies the target person's VID. We consider verification of this VID as a success. If any step fails, R-Focus repeats this entire process.

- We evaluate the overall success rate with respect to the distance between the device and the target person. The overall success rate decreases as distance increases as shown in Fig. 9. The overall success rate is 95% at 1 m distance, declining to $\sim 80\%$ at 5 m distance. This is due to two reasons: (1) As distance increases, RSSI drops dramatically and is more susceptible to noise, decreasing directional sensing accuracy; (2) As distance increases, the quality of a person's face decreases, making correct verification harder.
- If multiple persons appear in the final image, the method in §3.3 may verify the wrong person. We measure the overall success rate with respect to the number of persons; the results are shown in Fig. 10. With 1 or 2 people, the success rate is over 95%; with 3 people, the success rate is 85%. Each face can be verified as the target person with a certain probability; more persons near the target person increase the wireless environment's complexity. Thus, with more persons, it is harder to find and verify the target person.

After verifying the target person, R-Focus can track this person if the person's face can be detected continuously. Due to hardware limitations, our prototype rotates with angular speed $20^\circ/\text{s}$. Thus if the target person moves at a slower speed, continuous tracking can be performed successfully.

We achieve the above performance with a \$30 directional antenna and a \$25 Raspberry Pi camera. With $\sim \$100$ higher-dBi directional antennas [21] and

higher resolution cameras, we expect to achieve better performance. Conducting more extensive experiments with this equipment is part of our future work.

5 Final Remarks

R-Focus innovates with the combination of electronic and visual sensing that works in tandem to detect and verify persons of interest. Future challenges involve reducing the functionality of R-Focus in practical settings. For example, electronic signals suffer from multipath effects, noise, and occlusions from the environment and objects. A possible solution is to leverage multiple R-Focus platforms to counteract such disturbances; this solution would present new challenges. The final product will be a compact platform that will be convenient for integration into other systems.

References

1. Räty, T.D.: A Survey on Contemporary Remote Surveillance Systems for Public Safety. *IEEE TSMC-C* 40(5), 493–515 (2010)
2. Prabhakar, K., Rehg, J.M.: Categorizing Turn-Taking Interactions. In: Fitzgibbon, A., Lazebnik, S., Perona, P., Sato, Y., Schmid, C. (eds.) *ECCV 2012*, Part V. LNCS, vol. 7576, pp. 383–396. Springer, Heidelberg (2012)
3. Yilmaz, A., Javed, O., Shah, M.: Object Tracking: A Survey. *ACM CSUR* 38(4), 13 (2006)
4. Nemmaluri, A., Corner, M.D., Shenoy, P.: Sherlock: Automatically Locating Objects for Humans. In: *MobiSys* (2008)
5. Kim, M., Chong, N.Y.: RFID-enabled Target Tracking and Following with a Mobile Robot Using Direction Finding Antennas. In: *CASE* (2007)
6. Zhang, Z., Zhou, X., Zhang, W., Zhang, Y., Wang, G., Zhao, B.Y., Zheng, H.: I am the antenna: Accurate Outdoor AP Location Using Smartphones. In: *MobiCom* (2011)
7. Sen, S., Choudhury, R.R., Nelakuditi, S.: SpinLoc: Spin Once to Know Your Location. In: *HotMobile* (2012)
8. Teng, J., Zhang, B., Li, X., Bai, X., Xuan, D.: E-Shadow: Lubricating Social Interaction using Mobile Phones. In: *ICDCS* (2011)
9. Teixeira, T., Dublon, G., Savvides, A.: A Survey of Human-Sensing: Methods for Detecting Presence, Count, Location, Track, and Identity. *ACM CSUR* 5 (2010)
10. Dalal, N., Triggs, B.: Histograms of Oriented Gradients for Human Detection. In: *CVPR* (2005)
11. Felzenszwalb, P.F., Girshick, R.B., McAllester, D., Ramanan, D.: Object Detection with Discriminatively Trained Part-Based Models. *IEEE TPAMI* 32(9), 1627–1645 (2010)
12. Viola, P., Jones, M.: Rapid Object Detection using a Boosted Cascade of Simple Features. In: *CVPR* (2001)
13. Zhang, C., Zhang, Z.: A Survey of Recent Advances in Face Detection. Technical report, Tech. Rep., Microsoft Research (2010)
14. Wei, G., Li, D., Sethi, I.K.: Detection of Side-View Faces in Color Images. In: *Applications of Computer Vision* (2000)

15. Teng, J., Zhu, J., Xuan, D., Zheng, Y.F.: E-V: Efficient Visual Surveillance with Electronic Footprints. In: INFOCOM (2012)
16. Zhang, B., Teng, J., Zhu, J., Xuan, D., Zheng, Y.F.: EV-Loc: Integrating Electronic and Visual Signals for Accurate Localization. In: MobiHoc (2012)
17. Li, X., Teng, J., Zhai, Q., Zhu, J., Xuan, D., Zheng, Y.F., Zhao, W.: EV-Human: Human Localization via Visual Estimation of Body Electronic Interference. In: INFOCOM-MiniConf. (2013)
18. Ojala, T., Pietikainen, M., Maenpaa, T.: Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns. IEEE TPAMI 24(7), 971–987 (2002)
19. Belhumeur, P.N., Hespanha, J.P., Kriegman, D.: Eigenfaces vs. Fisherfaces: Recognition Using Class-Specific Linear Projection. IEEE TPAMI 19(7), 711–720 (1997)
20. Stoeveken, T.: mjpg-streamer, <http://mjpg-streamer.sourceforge.net/>
21. Wikipedia: Yagi-Uda antenna,
https://en.wikipedia.org/wiki/Yagi-Uda_antenna

QS-PS: A New Approach for Emergency Packet Delivery in WBAN

Ming Li^{1,2}, Jing Liu^{1,2}, Qiang Shen¹, and Bin Yuan¹

¹ Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China
² The State Key Laboratory of Integrated Service Networks, Xidian University, Shaanxi, China
{xiaoshiwu,jingliu1j,shen19900811,billryan}@sjtu.edu.cn

Abstract. Energy efficiency, reliability and latency for packet delivery are three key issues in WBAN. Energy efficiency and reliability can be guaranteed in a tree-based WBAN. However, there exists an inertial problem: when an emergency packet occurs in one node, that node has to wait for its assigned slot to transmit such a life-critical packet, resulting in unbearable delay. Here, we propose a new scheme named Quasi-Sleep-Preemption-Supported (QS-PS) to tackle with that problem. First, those nodes whose dedicated slots have elapsed will enter a new Quasi-Sleep mode. When an emergency event occurs, emergency node will first broadcast a special designed Awakening Message at the beginning of next slot to wake up the whole network. Then, the slot preemption strategy allows the emergency node to preempt the right to use the slot. This process will continue until the emergency packet arrives at the root, thus reducing delay. Compared to two basic threshold methods, Full-Active-Preemption-Supported (FA-PS, delay guaranteed) and Strict-Sleep-Preemption-Unsupported (SS-PU, energy efficiency guaranteed), the newly proposed QS-PS scheme can achieve the similar latency as FA-PS while reducing energy consumption of the whole network by 57%, and holds tremendous latency improvement over SS-PU just at a small energy cost.

1 Introduction

Due to the burgeoning of aging population in developing countries and longer life expectancy of human beings, the rising cost of health care has posed a great challenge to the development of society. Under such a severe situation, many technology-based innovations have been proposed to improve current health-care practice and Wireless Body Area Network (WBAN) emerges as a promising one.

WBAN is a special kind of network, which is designed for human body, for the purpose of continuous monitoring of vital life signals. It usually consists of several sensor nodes and a central coordinator. Sensor nodes are strategically placed on the body or implanted in the body to acquire specific biological signals such as electrocardiogram (ECG), pulse rate, oxygen saturation, blood glucose, etc. The coordinator receives data from sensor nodes, aggregates and then transmits it to the remote health-care center for diagnostic and therapeutic purposes [1]. WBAN samples real-time medical data and delivers to medical center in time, thus fulfilling the goal of remote long-term continuous monitoring and relieves medical staffs from burdensome work. So, it will be widely used in health-care system, sporting activities, military, to name a few [2].

Since the sensor node is miniaturized to be attached to human body, the battery capacity is naturally limited. How to prolong the lifetime of sensor node without degrading the monitoring quality has always been a conundrum for WBAN. Achieving high energy efficiency requires a holistic thinking including MAC protocol, routing strategy, etc [3].

The existing MAC protocols used in WBAN can be classified into three categories: Low Listening Protocol, Scheduled-Contention, and TDMA based Protocol [4]. B-MAC [5] falls in the category of Low Listening Protocol that sender should broadcast a long preamble before each message in order to be detected by the right receiver. By doing so, it can reduce idle-listening and overhearing. However, the long preamble will incur unnecessary overheads. S-MAC [6] is a classic scheduled-contention based schemes that synchronize its transmission schedule and listening periods to maximize throughput, while reducing energy by turning off radio during sleeping periods. However, performance varies in different traffic rate. Besides, periodically exchange of schedule will result in extra energy consumption. TDMA is collision-avoid protocol, since each slot is assigned to one node for exclusive use. Besides, nodes can go into sleep in others' slots, thus naturally solving the problems of overhearing and idle listening. It also holds some disadvantages: the synchronization over the whole network incurs some cost and slot resource will be wasted if the node has no packet to send in its dedicated slot. Even so, it seems that TDMA is probably more better for WBAN, since the traffic in WBAN is quite smooth due to the periodically sampling of sensor node.

Besides, tree-based WBAN is a good method to counter with the variation in body-channel caused by body movement. Furthermore, The routing strategy is quite simple that every node should just deliver the packet to its parent, thus providing good end-to-end latency performance. However it may suffer a problem: when an emergency event occurs, an emergency packet will generate in the relevant sensor node. This life-concerning information must be delivered to central coordinator immediately. But, due to the fixed tree structure and the predefined slot allocation scheme, it has to wait for the next assigned slot, resulting in unbearable delay!

Here, we introduce a holistic scheme called Quasi-Sleep-Preemption-Supported (QS-PS) to solve that inertial problem. In QS-PS, when the dedicated slot elapses, node will enter a new Quasi-Sleep mode by decreasing the clock rate of circuit while preserving some detecting ability, contrasted to the conventional sleep mode which completely turns off the radio. When an emergency packet occurs in one node, a special designed m-sequence based Awakening Message will be broadcasted by that node to wake up those nodes in Quasi Sleep mode. After being waken up, all the other nodes learn the existence of an emergency packet. Next, the slot preemption strategy allows emergency node to preempt the use of the current slot without interference, this process will continue until the emergency packet reaches the root, thus fulfilling the fast delivery of emergency packet.

The rest of this paper is organized as follows: Section 2 discusses related works. The details of the proposed QS-PS are presented in Section 3. Numerical results are displayed in Section 4 with further discussion. Finally, we conclude this paper and announce further work in Section 5.

2 Related Works

Periodical sleep and wake-up strategy is a good method to save energy, but how to wake up a node which is in sleep state is a problem. The authors in [7] introduced E-MiLi to minimize the idle-listening in WiFi. E-MiLi puts the stations into a subconscious state. When AP has packets for one targeted station, it will first send a special preamble which containing the address information to wake up the targeted station. At the station side, each station will run SRID algorithm to decode that preamble and decides to wake up or not based on the check result of addressed information. Due to the limitation of device, such a sophisticated design is unapplied to WBAN. Even so, E-Mili provides an instructive thought.

The optimal topology design problem of WBAN is investigated in [8]. The author introduced an integer linear programming model which optimizes the number and location of relays and the data routing strategy, aiming to minimize the energy cost and increase the lifetime of the network. However it requires the placement of external nodes acting only as relays. In [9], a cross-layer communication protocol called CICADA focusing on the slot allocation is proposed based on a tree topology. In CICADA, superframe is divided into two subparts, control subcycle and data subcycle. CICADA allows the slot allocation to be updated based on the demand of nodes, adjusting to different traffic rate. However, the control overheads are a constraining factor for CICADA.

Delay performance of emergency packet is another important issue in WBAN [10]. HBC-MAC [11] devotes to providing low delay service to emergency packet by inserting several free slots in superframe as special window for emergency packet. The proper number of free slots can be calculated based on historical data or emergency happening rate which is assumed to be known as a prior, it still results in unnecessary slot waste due to the burst and rather rare rate of emergency packet. While in our newly proposed QS-PS, no such special windows is needed, and QS-PS enables the emergency node to preempt the current slot to transmit that emergency packet without interference, thus reducing delay.

3 Quasi-sleep-Preemption-Supported Scheme

In order to deliver the emergency packet fast when occurred in a tree-based WBAN, two requirements should be satisfied: First, the parent node of that emergency node should be waken up and ready to receive emergency packet. Second, emergency node should be able to use the current slot which may not belong to it, without the interference from other nodes. In our QS-PS, we introduce a new low power saving mode called Quasi-Sleep mode and design a special Awakening Message to meet the first requirement. Besides, a slot preemption strategy which enables emergency node to preempt the right to use the current slot is invented. The whole scheme fulfils the goal of delivering the emergency packet rapidly.

3.1 Quasi-sleep Mode

In the conventional active-sleep pattern depicted in Fig. 1(a), node will enter the sleep mode when the assigned slot passes and wakes up in the next assigned slot. Since the

radio is completely turned off during sleep period, node cannot be waken up by external message. Consider the case when the emergency node want to transmit the emergency packet to its parent node at once, but its parent node may still in sleep state with radio off. How to wake up the sleepy parent node? To tackle with that problem, we introduce a new power saving mode named Quasi-Sleep mode to replace the conventional sleep mode, depicted in Fig. 1(b). Node will be put into Quasi-Sleep mode when the dedicated slot elapses and wakes up in the next assigned slot in the same manner. However, contrasted to conventional mode, node in Quasi-Sleep mode can be waken up by some special designed Awakening Message during sleep period!

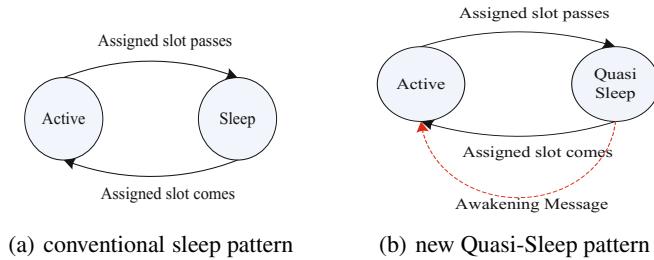


Fig. 1. Comparison of two active-sleep pattern

Such a Quasi-Sleep mode can be realized in hardware. Fig. 2 illustrates the architecture of a modern digital receiver used in a wireless node [7]. The receiving signal is first amplified, and then carried to the baseband by a mixer. Next, the analog-to-digital (ADC) samples the baseband signal and delivers the results to CPU for decoding. The sampling frequency of ADC and the working frequency of CPU are directly provided by the Phase-Locked-Loop which can obtain different frequency from the crystal oscillator. Previous study shows that a circuit's power consumption follows: $P \propto V_{dd}^2 f$, where V_{dd} is the supply voltage and f the clock rate [12]. So we can put node in Quasi-Sleep mode by decreasing its clock rate to save energy while preserving some detecting ability.

The energy consumption of Quasi-Sleep mode is higher than the conventional sleep mode but less than the active mode. The idea behind the introduction of Quasi-Sleep

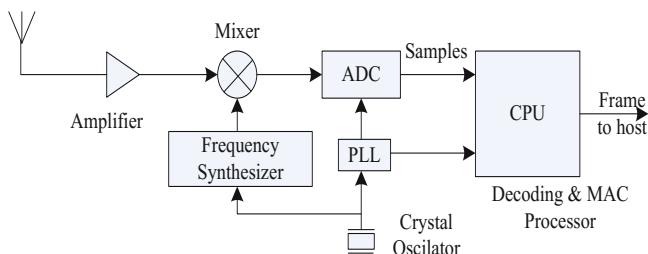


Fig. 2. Architecture of a receiver used in WBAN

mode is that we use a bit higher energy cost in exchange for limited awareness of the outside environment during sleep period.

For instance, CC2510 is a low power device popularly used in WBAN sensor node as the radio part. CC2510 supports eight different clock rates. The full clock rate is 26MHz, and it can be decreased at the ratio of 1/2, 1/4, 1/8, 1/16, 1/32, 1/64 and 1/128. We use a current probe and voltage probe to measure the power consumption of CC2510 under different clock rates. The tested results are tabulated in Table 1:

Table 1. Power consumption of CC2510 under different clock rates, Full rate=26MHz

Decreased ratio	Power (mW)
1	82.17
1/2	74.58
1/4	69.96
1/8	68.64
1/16	67.98
1/32	67.32
1/64	66.69
1/128	66.33

The energy consumption decreases monotonically as the clock rate decreases. Note that the power reduction becomes quite small as ratio decreases further. This is because those part of consumptions are caused by peripheral devices which are irrelevant to clock ratio. Quasi-Sleep method is different from currently existing wake-up methods, like WUR or WoR. WUR(Wake-Up Receiver), like the one proposed in [13], is a special design wake-up receiver. During the sleep period, the main receiver will be turned off and the WUR is on, for detecting wake-up message. One limitation of WUR is that it requires an external receiver to be attached and due to the fact that WUR is usually special design to save energy, it is only laboratory available not commercially available yet. Quasi-Sleep method does not require such an external receiver and we show that it can be fulfilled in purchasable circuits. While, WoR(Wake on Radio) is an explicit function that can be deployed in CC1100 and CC2500 chips. The main idea of WoR is that during the sleep period, receiver will periodically wake up to check whether there is packet for it or not. Using periodical mechanism can save energy but a sender may not wake up the targeted receiver in time. Quasi-Sleep mode avoids such a drawback since it is consistently monitoring the wake-up signal, thus the sleepy parent node can be wakened up more quickly.

3.2 M-sequence Based Awakening Message

Note that when node is in Quasi-Sleep mode, its ADC sampling rate and CPU working rate are low, the detecting ability is quite feeble in Quasi-Sleep mode. Due to these limitations, the Awakening Message should be tailored for the Quasi-Sleep mode to detect and has good noise immunity. It seems that m-sequence is a qualified candidate. M-sequence is one kind of pseudo-random sequence widely used as a spread spectrum

technique in wireless communication. The most significant property is its sharp auto-correlation value, when performing autocorrelation of the sequence, it will produce a peak value while remaining nearly zero in other cases. Due to the same reason, it has been used for customer distinguishing in cellular system, for instance cdma2000.

Integrate the m-sequence in Awakening Message. In the Quasi-Sleep mode, ADC sends the sampling results to CPU, and CPU does the autocorrelation of those sampling points. When a peak value above some threshold emerges at some moment, it is quite reasonable to assume that an Awakening Message is received. Since Awakening Message implies the occurrence of an emergency event, after detecting a peak value, node in Quasi Sleep mode will quickly switch back to active mode.

Besides, some changes should be made about the original m-sequence. A m-sequence usually has the length of $2^N - 1$. Assume that the clock rate is decreased by a ratio of 1/D, so the sampling rate of ADC is only 1/D of that when operating in full clock rate. So, we should replicate every single bit of the m-sequence by D to make sure enough sampling points are acquired to correctly detect the Awakening Message. Such a design of Awakening Message does not require receiver to decode every single bit, it exploits the peak autocorrelated value property of m-sequence to make it easy for Quasi-Sleep mode to detect.

It's worth mentioning that the energy consumption of Quasi-Sleep mode listed in Table 1 can be reduced further. Since the Awakening Message is only used to wake up the Quasi-Sleep mode, it can just carry the payload part, different from a standard packet which usually consists of header, payload and FCS. Without unnecessary header and FCS parts, the ADC and CPU have less decoding work to do, thus reducing energy cost of Quasi-Sleep mode. However, implementing such a design needs some hardware programming, here we use the statistics in Table 1, which was obtained when decoding a standard packet. We will extend this part of work in our further research.

3.3 Slot Preemption Strategy

Before elaborating the slot preemption strategy, we should first explain our time slot allocation scheme in a tree-based WBAN.

(i) Time Allocation Scheme

Use the three levels binary tree as an example, depicted in Fig. 3. Root node 0 denotes the coordinator.

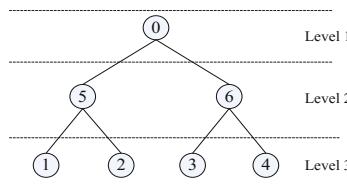


Fig. 3. A three level binary tree

Time axis is segmented as superframes and each superframe consists of a beacon and several slots, depicted in Fig. 4. Beacon is used to broadcast control information. There is a short period t_0 at the beginning of each slot for node to perform listening and the rest of the slot is proper to transmit one packet.

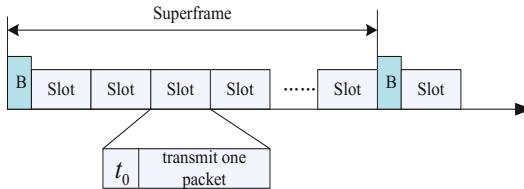


Fig. 4. Superframe structure

Slot allocation order is based on each node's location in the tree: First assign Level 3, then towards the upper ones layer by layer. Then, we identify how many slots should be assigned for each node in different levels. Each node in the bottom level is assigned one slot, while every node in Level 2 is assigned three time slots, two slots to transmit the packets received from its children and one for its own packet. In our slot allocation scheme, for each node in the middle level, the number of slots assigned to it is the sum of its children's slots plus one. So the length of the superframe for a three binary tree should be 10 slots, and the assignment order is illustrated in Table 2.

Table 2. Slot allocation in a three level tree

Time axis (-slot)	1	2	3	4	5	6	7	8	9	10
Allocation node	1	2	3	4	5	5	5	6	6	6

In practical application, since different sensor node may have different data rate, assigning every sensor node with only one slot to transmit its own packet is not appropriate. In such case, central coordinator will assign proper slots to each sensor node accommodated to its sampling rate but the aforementioned assigning rules are unchanged.

(ii) Slot Preemption Process

After the initial process, a binary tree is built, and the slot assignment order is determined and every node knows its dedicated slot(s) from the beacon. So node can be put into Quasi Sleep mode when the dedicated slot has passed. When an emergency packet generated in one node, in order to transmit the emergency packet immediately, emergency node should preempt the right to use the current slot without the interference from other nodes.

Our slot preemption protocol solves that problem based on the aforementioned slot allocation scheme by the following procedures:

1. The emergency node broadcast an Awakening Message at the beginning of the next slot.

2. Those nodes in Quasi-Sleep mode will be wakened up and informed that an emergency event occurs. Since the owner of the current slot will perform a very short listening duration t_0 at the beginning of the slot before transmitting its own packet, it will also know the existence of an emergency event and restrain transmission, avoiding causing interference.
3. Now the whole network is wakened up and in receive state, emergency node transmits the emergency packet to its parent. This process will continue until arriving at the root.
4. Root will broadcast disarming message when accepts the emergency packet. After receiving that message, the whole network will resume the normal slot allocation scheme.

When there are more than one emergency packets in the network, they will be dealt with according to First-In-First-Serve. Even the whole network is wakened up after the broadcasting of Awakening Message, the delivery of emergency packet still goes through the tree, instead of directly to the coordinator. This is because the direct link between the emergency node and the coordinator may be volatile due to body movement and tree-routing is more reliable since emergency node transmits emergency packet to its parent node with which it has better communication link.

Furthermore, in QS-PS, since the routing strategy for the emergency packet still follows the tree structure, those nodes in the bottom level will not be relays for any emergency packet, thus can be put into conventional sleep mode by completely turning off its radio to save energy further.

4 Simulation and Discussion

Consider a real scenario depicted in Fig. 5. There are totally 15 nodes. Node 0 denotes the coordinator. These nodes can be built as a four-level tree based on link quality, abstracted by Fig. 5(b).

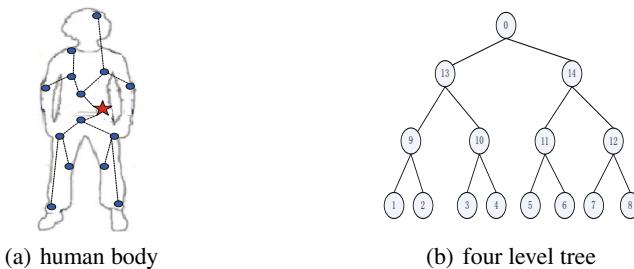


Fig. 5. A real scenario

According to the slot allocation scheme described in Section 3, the length of one superframe should be 34 slots. For Quasi Sleep mode, the clock rate is decreased at a ratio of 1/8 for authentically practical use. Assume that packet arrival follows Poisson distribution. Since the arrival rate of emergency packet is quite small, we make sure

Table 3. Simulation Parameters

Simulation duration	10,000 slots
Slot duration	200 μ s
Average arrival interval of normal packet	40 slots
Power consumption in Tx/Rx	82.17(mW)
Power consumption in Quasi Sleep mode	68.64(mW)

that at least 10 emergency packets will generate in each node during the simulation time. The simulation parameters are tabulated in Tab. 3.

We also implement two other threshold schemes as comparisons, Full-Active-Preemption-Supported(FA-PS) and Strict-Sleep-Preemption-Unsupported(SS-PU). In FA-PS, since all node will be constantly in active mode, there is no need to wake up sleepy parent node, and the emergency node just carries out the slot preemption process. So, FA-PS is a delay guaranteed scheme. While in SS-PU, since nodes will be put into conventional sleep mode strictly following the slot allocation scheme, all the nodes will be constantly in active mode and slot preemption is supported. And Strict-Sleep-Preemption-Unsupported(SS-PU): nodes will be put into conventional sleep mode strictly following the slot allocation scheme to save energy. SS-PU is similar to CI-CADA in [9], which is also energy efficient. However, since a node cannot be waked up in conventional sleep node, the slot preemption for emergency packet is unsupported in SS-PU.

4.1 Delay Performance

The average arrival interval of normal packet is set to 40 (slots/packet), nearly 8ms. Such setting matches sampling rate requirement of body signal in practical use. The result is depicted in Fig. 6. It can be found that the delay performance of normal packets are quite similar among the three schemes. A trend can also be found that lower layer nodes will experience quite longer delay than the upper layer. The reason for that trend is that nodes in lower layer will traverse more hops before reaching the root. Even so, the average delay of each node is below the average arrival interval (40 slots/packet), which means routing strategy in a tree structure can provide good end-to-end delay service, this is due to the fact that the tree structure provides contention-free access and collision-avoid transmission.

However, the delay performance of emergency packet varies a lot among three schemes, as depicted in Fig. 7. For the preemption supported schemes, both FA-PS and the newly proposed QS-PS can transmit emergency packet immediately, while SS-PU experiences a quite longer delay. This is because in SS-PU, the emergency node cannot wake up its sleepy parent node when needed, it has to wait for its assigned slot to transmit that emergency packet. In a word, SS-PU fails to transmit emergency packet in time. In FA-PS, since all nodes are constantly in active node, the emergency node can preempt the current slot to transmit that emergency packet. While in QS-PS, the emergency can use the Awakening Message to wake up the parent node in Quasi Sleep mode, then use the preemption process to transmit emergency packet at once.

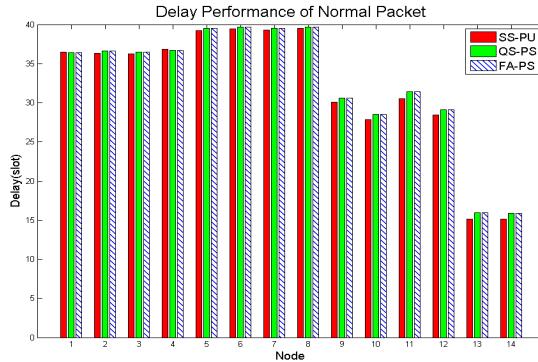


Fig. 6. Delay performance of normal packet

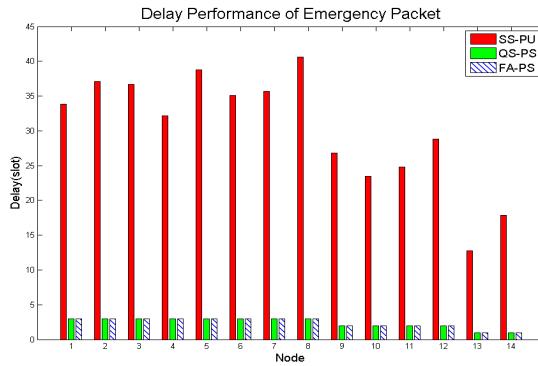


Fig. 7. Delay performance of emergency packet

4.2 Energy Consumption

Fig. 8 depicts the energy consumption of the three schemes. For FA-PS scheme, since every node must be active in full time, the energy consumption is very high. While in SS-PU, the energy consumption is the least. This is because that in SS-PS, node will follow a strict active-sleep rule. Besides, the upper level node will consume more energy than lower level node, due to fact that the upper level node has to relay the packets received from its children.

In the proposed QS-PS, for those nodes in bottom level (node 1-8), they consume nearly the same energy as those in SS-PU, that is because in QS-PS, nodes in bottom level follow the same strict active-sleep pattern. For nodes in other levels, the energy consumption is between SS-PU and FA-PS. In QS-PS, the energy consumption for the whole network is 57% less than FA-PS.

Combine the delay and energy consumption performance together, we find that: although SS-PU consumes the least energy but its unbearable long delay for emergency packet make it unsuitable for real application. FA-PS can provide good delay service for

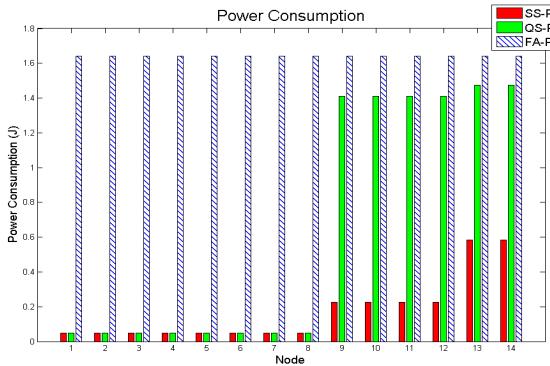


Fig. 8. Energy consumption

both normal packet and emergency packet but comes at a high energy cost. In QS-PS, we achieve a more balance between delay performance and energy consumption. It can obtain the same delay service for both normal packet and emergency packet as FA-PS, while achieves a 57 % energy reduction for the whole network.

5 Conclusion and Future Work

In this paper, we propose a new scheme called QS-PS to solve the inertial problem of slow response to the delivery of emergency packet delivery in a tree-based WBAN. QS-PS puts those nodes whose assigned slots have elapsed in Quasi-Sleep mode and Quasi-Sleep mode can be awakened by a special designed Awakening Message. Emergency node can broadcast the Awakening Message to awaken the whole network, then our slot preemption strategy allows that node to preempt the use of the current slot. Numerical results shows that QS-PS can achieve a better balance between delay and energy consumption. Besides, the proposed approach has the potential application for large networks as well [14] [15].

QS-PS can be improved in the future. We consider the case where only one WBAN exists, in the future work, coexistence of several WBAN should be included. How to awaken the desire WBAN without falsely triggering other undesired WBAN is another issue worth further studying.

Acknowledgement. This work is supported by China International Science and Technology Cooperation Program (No.S2010GR0445), National Science and Technology Major Project (No.2010ZX03002-007-01) and National Natural Science Foundation of China (NSFC, No.61102052).

References

1. Yan, H., Huo, H., Xu, Y., Gidlund, M.: Wireless sensor network based e-health system-implementation and experimental results. *IEEE Transactions on Consumer Electronics* 56(4), 2288–2295 (2010)

2. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., Kwak, K.S.: A comprehensive survey of wireless body area networks. *Journal of Medical Systems* 36(3), 1065–1094 (2012)
3. Smith, D.B., Lamahewa, T., Hanlen, L.W., Miniutti, D.: Simple prediction-based power control for the on-body area communications channel. In: Proc. IEEE ICC 2011, pp. 1–5 (2011)
4. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., Leung, V.C.: Body area networks: A survey. *Journal of Mobile Networks and Applications* 16(2), 171–193 (2011)
5. Polastre, J., Hill, J., Culler, D.: Versatile low power media access for wireless sensor networks. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 95–107 (2004)
6. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient mac protocol for wireless sensor networks. In: Proc. IEEE INFOCOM 2002, pp. 1567–1576 (2002)
7. Zhang, X., Shin, K.G.: E-mili: energy-minimizing idle listening in wireless networks. *IEEE Transactions on Mobile Computing* 11(9), 1441–1454 (2012)
8. Elias, J., Mehaoua, A.: Energy-aware topology design for wireless body area networks. In: Proc. IEEE ICC 2012, pp. 3409–3410 (2012)
9. Latre, B., Braem, B., Moerman, I., Blondia, C., Reusens, E., Joseph, W., Demeester, P.: A low-delay protocol for multihop wireless body area networks. In: Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous 2007, pp. 1–8 (2007)
10. Shen, Q., Zhuang, W.: Energy efficient scheduling for delay constrained communication in wireless body area networks. In: Proc. IEEE GLOBECOM 2012, pp. 262–267 (2012)
11. Otgonchimeg, B., Kwon, Y.: Emergency handling for mac protocol in human body communication. *EURASIP Journal on Wireless Communications and Networking* 2011(1), 786903 (2011)
12. Dieter, W.R., Datta, S., Kai, W.K.: Power reduction by varying sampling rate. In: Proceedings of the 2005 International Symposium on Low Power Electronics and Design, pp. 227–232 (2005)
13. Cho, H., Bae, J., Yoo, H.-J.: A 37.5 body channel communication wake-up receiver with injection-locking ring oscillator for wireless body area network. *IEEE Transactions on Circuits and Systems* 60(5), 1200–1208 (2013)
14. Wang, X., Huang, W., Wang, S., Zhang, J., Hu, C.: Delay and capacity tradeoff analysis for motioncast. *IEEE/ACM Transactions on Networking* 19(5), 1354–1367 (2011)
15. Huang, W., Wang, X.: Capacity scaling of general cognitive networks. *IEEE/ACM Transactions on Networking* 20(5), 1501–1513 (2012)

Resource Allocation for Uplink-Downlink Cellular Network with Small Cells and Relays Enhanced

Yisha Lou¹, Meng Zhang¹, Hui Yu¹, Hanwen Luo¹, and Haiquan Wang²

¹ Department of Electronic Engineering,
Shanghai Jiao Tong University, Shanghai, P.R. China

² Hangzhou Dianzi University, Hangzhou, P.R. China
`{louys,mengzhang,yuhui,hwluo}@sjtu.edu.cn, tx_wang@hdu.edu.cn`

Abstract. With the rising demand of wireless network capacity and coverage, heterogeneous network consisting of Macro Base Stations (MBSs), Small-cell Base Stations (SBSs) and relay nodes (RNs) can be a promising technique which might be widely deployed in the future system framework. However, user throughput in heterogeneous network can be largely degraded by co-channel interference, which is brought by the reuse of frequency. In this paper, we study a general multi-cell heterogeneous network model, and propose a power-based classification criterion and a range-expansion-based association criterion to classify RNs and users, respectively. Based on these criterions, Cooperative MultiPoint (CoMP) transmission is utilized for some specific users. Afterwards, based on fairness metric, we formulate the resource allocation problem into a convex optimization problem. By adopting dual decomposition method, a closed-form solution is obtained. Finally, system level simulation is operated and the obtained results verify the advantageous performance of the proposed optimal resource allocation strategy.

Keywords: resource allocation, small cell, heterogeneous network.

1 Introduction

Orthogonal Frequency Division Multiple Access (OFMDA) has emerged as an efficient radio access for high speed wireless communication networks such as Long Term Evolution-Advanced (LTE-A) system. In OFDMA system, a wide-band frequency spectrum is shared by distinct users, and the whole frequency domain is partitioned into orthogonal narrow subcarriers. However, as the system frequency reuse factor is one in the future system framework, the decrease of user throughput is expected by the presence of intra-cell and inter-cell interference. On the other hand, as the rapidly rising demand of data rate and coverage, heterogeneous network which consists of Macro Base Stations (MBSs), Small-cell Base Stations (SBSs) and Relay Nodes (RNs), might be widely deployed.

Resource allocation strategies for OFDMA networks have been broadly investigated in the literature as an efficient way to schedule the wide-band frequency spectrum and mitigate the negative influence brought by interference.

In [1], [2], [3], the researchers discuss optimal resource allocation strategies for users in single-cell OFDMA system with decode-and-forward (DF) type relaying for different system configurations. However, with presence of multi-cells the co-channel interference caused by adjacent cells and RNs must be taken into consideration. For multi-cell scene without the assistance of RNs, the optimal resource allocation strategy for downlink cellular OFDMA system has been proposed in [4], [5] by jointly designing the schemes for power control and subcarrier assignment. Further, a specific relay-assistant network where the RNs are fixed in a circle near the MBS is considered in [6]. In [7], the authors make a further step by proposing a corresponding resource allocation strategy for the scenario where the RNs are uniformly distributed to serve the users in both cooperative and noncooperative model.

In this paper, we study a more general multi-cell heterogeneous network model where SBSs and RNs are uniformly distributed in each macro cell. The RNs we deployed work in DF mode by using in-band backhauls to communicate with the base stations. Moreover, both cooperative and noncooperative model can be implemented in the network according to our proposed criterion. Furthermore, we assume all the SBSs function in the uplink mode, and simultaneously MBSs transmit data in downlink mode in the same time slot. We propose a power-based classification criterion and a range-expansion-based association criterion to classify RNs and users, respectively. Besides, we utilize fairness metric as proposed in [8], to ensure fairness among the users while achieving a good performance of overall system throughput. Afterwards, the resource allocation problem can be formulated into the form of convex optimization problem, and an asymptotically optimal solution is derived by using dual decomposition.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model and the categories of links in the heterogeneous network. The resource allocation problem is formulated in Section 3 into a convex optimization problem, and the criteria we proposed to classify RNs and users are described as well. In Section 4, a dual decomposition method is used to solve the optimization problem and the optimal radio resource scheduling strategy is elaborated. Simulation results are given in Section 5 to illustrate the performance of the proposed resource allocation strategy. Finally, we conclude this paper in Section 6.

2 System Model

We consider a heterogeneous Time-Division Duplexing (TDD) cellular network, where each cell is deployed with one high-power MBS, N_f uniformly distributed SBSs and N_r uniformly distributed low-power RNs. The total number of cells in the network is N_c , and N_u . User Equipments (UEs) are also uniformly distributed in the network. All the UEs fall into two categories, MUE and SUE, which are served by MBS and SBS, respectively.

In the system, we consider a transmission time slot during which downlink communication between MBS and MUE, uplink communication between SBS and SUE are triggered simultaneously. We denote the direct link between a

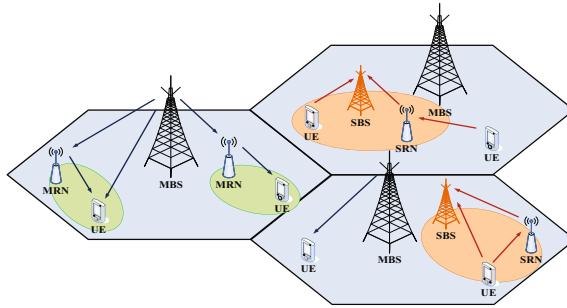


Fig. 1. Heterogeneous network with MBSs, SBSs and RNs

MBS and a MUE as MBS-MUE and the direct link between a SBS and a SUE as SUE-SBS. In the network, RNs help with downlink communications between a MBS and a MUE as well as uplink communications between a SBS and a SUE by using a DF mode relaying scheme. In a transmission time slot, a specific relay node can be indicated as a Macro-cell Relay Node (MRN) or Small-cell Relay Node (SRN) according to its association status. RN-MUE and SUE-RN represent the link between a RN and a MUE, and the link between a RN and a SUE, respectively. Moreover, RN-MUE and SUE-RN are one-hop transmission links meaning the UEs in these links are solely served by the RNs, without BS coordination. In the relay system, the UEs at the edge of a RN cell might receive a relatively high SINR from a nearby BS. Therefore, significant gain is expected to be achieved by using Cooperative MultiPoint (CoMP) transmission for these UEs. Furthermore, we denote CM-MUE and SUE-CF as the link between a RN and a MUE with coordination of a MBS, and the link between a RN and a SUE with coordination of a SBS, respectively. Moreover, it is assumed that each UE can only access to one kind of links. For the purpose of simplifying the description, UEs are divided into six user clusters as follows, where \mathcal{K} denotes the cluster of UEs and $\{m_0, m_1, m_2, f_0, f_1, f_2\}$ indicate the different kinds of links:

$$\mathcal{K}_{m_0} : MBS - MUE, \mathcal{K}_{m_1} : RN - MUE, \mathcal{K}_{m_2} : CM - MUE, \quad (1)$$

$$\mathcal{K}_{f_0} : SUE - SBS, \quad \mathcal{K}_{f_1} : SUE - RN, \quad \mathcal{K}_{f_2} : SUE - CF. \quad (2)$$

We divide the total frequency resources into N_{RB} resources blocks (RBs). The UEs will be assigned with an integer number of RBs. More specifically, $N_{\mathcal{K}_{m_0}, k, i, 0}$ denotes the number of RBs assigned to the link between the MBS in the i -th cell and the k -th UE who belongs to the user cluster \mathcal{K}_{m_0} , while $N_{\mathcal{K}_{m_1} \text{ or } m_2, k, i, j}$ denotes the number of RBs assigned to the link between the j -th RN in the i -th cell and the k -th UE belonging to the user cluster $\mathcal{K}_{m_1} \text{ or } m_2$. We denote the number of RBs assigned to the link between k -th UE who belongs to the user cluster \mathcal{K}_{f_0} and the f -th SBS in the i -th cell as $N_{\mathcal{K}_{f_0}, k, i, f, 0}$, while the number of RBs assigned to the link among the k -th UE who belongs to the user cluster $\mathcal{K}_{f_1} \text{ or } f_2$, the j -th RN and the f -th SBS in the i -th cell as $N_{\mathcal{K}_{f_1} \text{ or } f_2, k, i, f, j}$. In addition, the backhaul link is defined as the link between the RN and the

donor MBS or SBS. The capacity of these backhaul links is always higher than the other communication links by the fact that RNs are usually equipped with multiple antennas and placed in a proper location for providing a steady link to BSs. We denote the number of RBs used in the backhaul link by adding a superscript b at N as N^b . Fig.1 shows the considered system configuration.

We assume that the wireless channel is frequency flat across RBs. Besides, the channel gain between the k -th UE and the MBS in the i -th cell is denoted as $h_{k,i}$. $h_{k,i,j}$ denotes the channel gain between the k -th UE and the j -th RN in the i -th cell. Additionally, $h_{k,i,f}$ denotes the channel gain between the k -th SUE and the f -th SBS in the i -th cell. For the channel between the k_1 -th MUE in the i_1 -th cell and the k_2 -th SUE in the i_2 -th cell, we denote the channel gain as $h_{(k_1,i_1),(k_2,i_2)}$. We take a specific user who is classified to \mathcal{K}_{m_0} for instance. The received SINR of the can be evaluated as (7), where P_{MBS} , P_{RN} and P_{UE} denote the power of MBS, RN and UE, respectively. k , i and j are the indexes of the user, cell and RN, respectively. N_0 is the variance of the additive white Gaussian noise. The SINR expression of other kinds of UEs can be derived similarly.

$$\text{SINR}_{\mathcal{K}_{m_0}, k', i', 0} = \frac{P_{MBS} |h_{k', i', 0}|^2}{\sum_{i \neq i'} P_{MBS} |h_{k', i, 0}|^2 + \sum_{i=1}^{N_c} \sum_{j=1}^{N_r} P_{RN} |h_{k', i, j}|^2 + \sum_{k \in \mathcal{K}_{f_y}} \sum_{y=0,1,2} P_{UE} |h_{(k', i'), (k, i)}|^2 + N_0}. \quad (3)$$

By obtaining received SINR values, the data rate for each link can be calculated using Shannon formula as

$$R_{\mathcal{K}_{m_y}, k, i, j} = \log(1 + \text{SINR}_{\mathcal{K}_{m_y}, k, i, j}), \quad (4)$$

$$R_{\mathcal{K}_{f_y}, k, i, f, j} = \log(1 + \text{SINR}_{\mathcal{K}_{f_y}, k, i, f, j}). \quad (5)$$

where $y \in \{0, 1, 2\}$ is the type index of communication links, $k \in \{0, 1, \dots, N_u\}$, $i \in \{1, 2, \dots, N_c\}$, $f \in \{1, 2, \dots, N_f\}$ and $j \in \{0, 1, \dots, N_r\}$. $R_{\mathcal{K}_{m_y}, 0, i, j}$ denotes the data rate of the link between the MBS and the j -th RN in the i -th cell, $R_{\mathcal{K}_{m_y}, 0, i, f, j}$ denotes the data rate of the link between the f -th SBS and the j -th RN in the i -th cell.

3 Problem Formulation

By applying relay nodes in the heterogeneous network, CoMP transmission can be implemented to enhance the received signal quality of certain users. For instance, the users at the edge of a RN cell may receive a relative low SINR from the RN while receiving a relative high SINR from nearby MBS or SBS. In this case, CoMP can be implemented for these users to improve communication quality with the coordination between MBS and MRN for downlink communication, or between SBS and SRN for uplink communication. On the other hand, for the users who locate in the shadow of base station, CoMP transmission with RNs can significantly ameliorate the received SINR so that significant performance gain can be achieved.

For all the deployed RNs, we propose a classification criterion to sort them into two categories as MRN and SRN. Moreover, in order to avoid low utilization of SBSs, the range-expansion-based classification scheme is applied to compensate the transmit power disparity between MBSs and SBSs. By applying the classification criterion in formula (6) and (7) for each RN, we get the set of RNs that are associated with MBS and the set of RNs that are associated with SBS, respectively. Additionally, $\{(i^*, j)\}_{MRN}$ and $\{(i^*, f^*, j)\}_{SRN}$ denote the j -th MRN in the i^* -th cell and the j -th SRN in the i^* -th cell who serves the f^* -th SBS, respectively. δ_f denotes the compensating coefficient of range-expansion-based scheme.

$$\begin{aligned} \{(i^*, j)\}_{MRN} = & \left\{ (i^*, j) \mid P_c |h_{0,i^*,j}|^2 > \delta_f P_f |h_{0,i,f,j}|^2 \forall i, f \right. \\ & \left. \text{and } P_c |h_{0,i^*,j}|^2 > P_c |h_{0,i,j}|^2 \forall i, f, i \neq i^* \right\} \end{aligned} \quad (6)$$

$$\begin{aligned} \{(i^*, f^*, j)\}_{SRN} = & \left\{ (i^*, j) \mid \delta_f P_f |h_{0,i^*,f^*,j}|^2 > P_c |h_{0,i,j}|^2 \forall i \right. \\ & \left. \text{and } P_f |h_{0,i^*,f^*,j}|^2 > P_f |h_{0,i,f,j}|^2 \forall (i, f), (i, f) \neq (i^*, f^*) \right\} \end{aligned} \quad (7)$$

As seen in formula (6) and (7), for each RN, the proposed classification criterion evaluates the range-expansion-based received power of all the links between the specific RN and the base stations in the network, and then associates the specific RN with the link achieving the largest received power. By applying this classification criterion, the optimal choice of whether a RN should associate with a MBS or a SBS is made at the RN side. Since all the MBSs, SBSs and RNs are position fixed, the change of channel conditions between BSs and RNs are relatively slow. Thus, this classification operation could be done once in several time slots to reduce complexity.

For each UE that is granted into the network, we propose an association criterion to decide the optimal link, and sort it to one of the six user clusters: $\{\mathcal{K}_{m_0}, \mathcal{K}_{m_1}, \mathcal{K}_{m_2}, \mathcal{K}_{f_0}, \mathcal{K}_{f_1}, \mathcal{K}_{f_2}\}$. Similarly, range-expansion-based association scheme is utilized to compensate the transmit power disparity between BSs and RNs. The proposed association criterion for each UE is expressed as

$$(i^*, f^*, j^*)_k = \max_{\substack{i \in \{1, \dots, N_c\}, f \in \{0, \dots, N_f\} \\ j \in \{0, \dots, N_r\}}} \left\{ P_c |h_{k,i,f,j}|^2, \right. \\ \left. \delta_r P_r |h_{k,i,f,j}|^2, \delta_f P_f |h_{k,i,f,j}|^2 \right\}, \quad (8)$$

$$k \in \begin{cases} \mathcal{K}_{m_0}, & \text{if } f^* = 0 \text{ and } j^* = 0 \\ \mathcal{K}_{m_1 \text{ or } m_2}, & \text{if } f^* = 0 \text{ and } j^* \neq 0 \\ \mathcal{K}_{f_0}, & \text{if } f^* \neq 0 \text{ and } j^* = 0 \\ \mathcal{K}_{f_1 \text{ or } f_2}, & \text{if } f^* \neq 0 \text{ and } j^* \neq 0, \end{cases} \quad (9)$$

Further, for $k \in \mathcal{K}_{m_1}$ or m_2

$$k \in \begin{cases} \mathcal{K}_{m_2}, & P_c|h_{k,i^*,0}|^2 > \delta_r \sigma_1 \text{ and } P_r|h_{k,i^*,j^*}|^2 > \sigma_2 \\ \mathcal{K}_{m_1}, & \text{otherwise,} \end{cases} \quad (10)$$

for $k \in \mathcal{K}_{f_1}$ or f_2

$$k \in \begin{cases} \mathcal{K}_{m_2}, & P_f|h_{k,i^*,f^*,0}|^2 > \sigma_3 \text{ and } P_r|h_{k,i^*,f^*,j^*}|^2 > \sigma_4 \\ \mathcal{K}_{m_1}, & \text{otherwise.} \end{cases} \quad (11)$$

where $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ is the threshold to judge whether the k th user should implement CoMP, and δ_r, σ_f are the compensating coefficients.

In order to describe the result, boolean variables $x_{\mathcal{K}_{m_y},k,i,j}$ and $x_{\mathcal{K}_{f_y},k,i,f,j}$ are defined as decision variables which indicate the connection status with 1 or 0. Specifically, $x_{\mathcal{K}_{m_1},k,i,j} = 1$ denotes that the k -th UE is sorted to cluster \mathcal{K}_{m_1} and decided to be associated with the j -th RN in the i -th cell. It is assumed that each UE in the network can only be associated with one type of links. Thus, the $x_{\mathcal{K}_{m_y},k,i,j}$ and $x_{\mathcal{K}_{f_y},k,i,f,j}$ should satisfy the following constraints.

$$\sum_{i=1}^{N_c} \sum_{j=0}^{N_r} x_{\mathcal{K}_{m_y},k,i,j} \leq 1, \quad \sum_{i=1}^{N_c} \sum_{f=0}^{N_f} \sum_{j=0}^{N_r} x_{\mathcal{K}_{f_y},k,i,f,j} \leq 1. \quad \forall k. \quad (12)$$

We aim at optimizing the overall throughput while considering fairness among the UEs. Thus, fairness metric is used to achieve a good trade-off between fairness and spectrum efficiency. The optimization problem is then formulated as

$$[P1] \quad \max \sum_k \log R_k, \quad (13)$$

subject to:

Constraint on each MBS

$$C_{MBS} \triangleq \sum_{k=1}^{N_u} x_{\mathcal{K}_{m_0},k,i,0} N_{\mathcal{K}_{m_0},k,i,0} + \sum_{j=1}^{N_r} \sum_{k=1}^{N_u} x_{\mathcal{K}_{m_1},k,i,j} N_{\mathcal{K}_{m_1},k,i,j}^b \\ + \sum_{j=1}^{N_r} \sum_{k=1}^{N_u} x_{\mathcal{K}_{m_2},k,i,j} (N_{\mathcal{K}_{m_2},k,i,j} + N_{\mathcal{K}_{m_2},k,i,j}^b) \leq N_{RB}, \text{ for } i = 1, \dots, N_c, \quad (14)$$

Constraint on each SBS

$$C_{SBS} \triangleq \sum_{k=1}^{N_u} x_{\mathcal{K}_{f_0},k,i,f} N_{\mathcal{K}_{f_0},k,i,f} + \sum_{j=1}^{N_r} \sum_{k=1}^{N_u} x_{\mathcal{K}_{f_1},k,i,f,j} N_{\mathcal{K}_{f_1},k,i,f,j}^b \\ + \sum_{j=1}^{N_r} \sum_{k=1}^{N_u} x_{\mathcal{K}_{f_2},k,i,f,j} (N_{\mathcal{K}_{f_2},k,i,f,j} + N_{\mathcal{K}_{f_2},k,i,f,j}^b) \leq N_{RB}, \\ \text{for } i = 1, \dots, N_c, f = 1, \dots, N_f, \quad (15)$$

Constraint on each RN

$$\begin{aligned}
 C_{RN} &\triangleq \sum_{y \in \{1,2\}} \left(\sum_{k=1}^{N_u} x_{\mathcal{K}_{my}, k, i, j} (N_{\mathcal{K}_{my}, k, i, j} + N_{\mathcal{K}_{my}, k, i, j}^b) \right. \\
 &\quad \left. + \sum_{k=1}^{N_u} \sum_{f=1}^{N_f} x_{\mathcal{K}_{fy}, k, i, f, j} (N_{\mathcal{K}_{fy}, k, i, f, j} + N_{\mathcal{K}_{fy}, k, i, f, j}^b) \right) \leq N_{RB}, \\
 & \text{for } i = 1, \dots, N_c, j = 1, \dots, N_r,
 \end{aligned} \tag{16}$$

Constraint on each UE

$$\begin{aligned}
 C_{UE} &\triangleq \sum_{y \in \{1,2\}} \left(\sum_{i=1}^{N_c} \sum_{j=0}^{N_r} x_{\mathcal{K}_{my}, k, i, j} N_{\mathcal{K}_{my}, k, i, j} \right. \\
 &\quad \left. + \sum_{i=1}^{N_c} \sum_{f=1}^{N_f} \sum_{j=0}^{N_r} x_{\mathcal{K}_{fy}, k, i, f, j} N_{\mathcal{K}_{fy}, k, i, f, j} \right) \leq N_{RB}, \quad \text{for } k = 1, \dots, N_u,
 \end{aligned} \tag{17}$$

Other constraints

$$N_{\mathcal{K}_{my}, k, i, j}, N_{\mathcal{K}_{my}, k, i, j}^b \geq 0, \quad N_{\mathcal{K}_{fy}, k, i, f, j}, N_{\mathcal{K}_{fy}, k, i, f, j}^b \geq 0, \quad \forall y, k, i, f, j \tag{18}$$

Where

$$\begin{aligned}
 R_k &= \sum_{y \in \{1,2\}} \left(\sum_{i=1}^{N_c} \sum_{j=0}^{N_r} x_{\mathcal{K}_{my}, k, i, j} R_{\mathcal{K}_{my}, k, i, j} N_{\mathcal{K}_{my}, k, i, j} \right. \\
 &\quad \left. + \sum_{i=1}^{N_c} \sum_{f=1}^{N_f} \sum_{j=0}^{N_r} x_{\mathcal{K}_{fy}, k, i, f, j} R_{\mathcal{K}_{fy}, k, i, f, j} N_{\mathcal{K}_{fy}, k, i, f, j} \right).
 \end{aligned} \tag{19}$$

By solving the optimization problem $P1$, we are able to find the optimal resource allocation strategy $N = (\{N_{\mathcal{K}_{my}, k, i, j}\}, \{N_{\mathcal{K}_{fy}, k, i, f, j}\})$ for the network to achieve a good performance of overall throughput as well as fairness. Equation (14) is the constraint of resource number on each MBS. The first term in (14) computes the number of resources used in MBS-MUE links at the MBS side. The second term computes the number of resources used in RN-MUE links at the MBS side which, in other words, is the resource consumption of the backhaul links between MBSs and RNs. The third term computes the number of resources used in CM-MUE links which consists of backhaul links and direct links. Equation (15) is the constraint of resource number on each SBS in each cell, and equation (16) is the constraint of resource number on each RN in each cell. The terms in (15) and (16) are formulated in a similar way as in (14).

In the following section, the optimization problem $P1$ is solved by jointly utilizing dual decomposition method and Karush-Kuhn-Tucker (KKT) conditions, and the process to get the optimal resource allocation strategy is illustrated.

4 Optimal Radio Resource Allocation Scheme

As we use fairness metric to guarantee the fairness of resource allocation among all the users, the optimization problem presents nonlinear so that the closed-form of the optimal solution cannot be derived by simply using KKT conditions [9]. In this section, we jointly use dual decomposition method and KKT conditions to solve the convex optimization problem, and the solution is asymptotically optimal. In the following subsections, it is shown that by applying the dual decomposition method, the solution of optimization problem $P1$ can be obtain by simply implementing iteration algorithm.

4.1 Optimizing the Dual Function

We define \mathcal{N} as the set of all possible combinations of $N_{\mathcal{K}_{my},k,i,j}$ and $N_{\mathcal{K}_{fy},k,i,f,j}$ for all UEs in the network. $\beta = (\{\lambda_i\}, \{\mu_{i,f}\}, \{\nu_{i,j}\}, \{\varphi_k\})$ is defined as the vector of Lagrange multipliers. By obtaining all the constraints for resource allocation imposed in the network in section 2, the Lagrange dual function of problem $P1$ can be written as

$$g(\beta) \triangleq \max_{(N_{\mathcal{K}_{my},k,i,j}, N_{\mathcal{K}_{fy},k,i,f,j}) \in \mathcal{N}} L(N_{\mathcal{K}_{my},k,i,j}, N_{\mathcal{K}_{fy},k,i,f,j}, \beta), \quad (20)$$

where the Lagrangian is

$$\begin{aligned} L(N_{\mathcal{K}_{my},k,i,j}, N_{\mathcal{K}_{fy},k,i,f,j}, \beta) &= \sum_{k=1}^{N_u} \log R_k \\ &+ \sum_{i=1}^{N_c} \lambda_i (N_{RB} - C_{MBS,i}) + \sum_{i=1}^{N_c} \sum_{f=1}^{N_f} \mu_{i,f} (N_{RB} - C_{SBS,i,f}) \\ &+ \sum_{i=1}^{N_c} \sum_{j=1}^{N_r} \nu_{i,j} (N_{RB} - C_{RN,i,j}) + \sum_{k=1}^{N_u} \varphi_k (N_{RB} - C_{UE,k}), \end{aligned} \quad (21)$$

with $\beta = (\{\lambda_i\}, \{\mu_{i,f}\}, \{\nu_{i,j}\}, \{\varphi_k\}) \geq 0$ denoting the vector of the dual variables which are associated with the individual resource constraints. Then, the dual optimization problem is given by

$$\min_{\beta} g(\beta), \quad s.t. \beta \geq 0. \quad (22)$$

Let $N^*(\beta)$ denotes the optimal resource allocation strategy in (20) while the Lagrange multipliers are given as β . Gradient or subgradient-based methods can be used to solve a dual problem as it's always convex by definition. Then, the subgradient of β can be denoted by

$$\Delta\beta = (\{\Delta\lambda_i\}, \{\Delta\mu_{i,f}\}, \{\Delta\nu_{i,j}\}, \{\Delta\varphi_k\}), \quad (23)$$

where

$$\Delta\lambda_i = N_{RB} - C_{MBS,i}(N^*(\beta)), \quad \forall i \quad (24)$$

$$\Delta\mu_{i,f} = N_{RB} - C_{SBS,i,f}(N^*(\beta)), \quad \forall i, f \quad (25)$$

$$\Delta\nu_{i,j} = N_{RB} - C_{RN,i,j}(N^*(\beta)), \quad \forall i, j \quad (26)$$

$$\Delta\varphi_k = N_{RB} - C_{RN,k}(N^*(\beta)). \quad \forall k \quad (27)$$

By getting the subgradient of β , the dual variables can be updated as $\beta^{(l+1)} = \beta^{(l)} + \epsilon^{(l)}\Delta\beta$, where the update of the step size $\epsilon^{(l)}$ follows the diminishing step size policy. The subgradient method used above is guaranteed to converge to the optimal dual variable β^* which leads to an asymptotically optimal solution of the optimization problem $P1$.

4.2 Optimizing Primal Variables at a Given Dual Point

At a given dual point β^* , we can get the optimal resource allocation strategy $N^*(\beta^*)$ by solving the following optimization problem:

$$\begin{aligned} [P2] \quad g(\beta^*) &= \max L(N_{\mathcal{K}_{m_y},k,i,j}, N_{\mathcal{K}_{f_y},k,i,f,j}, \beta^*) \\ &= \max \sum_{k^*=1}^{N_u} L'(N_{\mathcal{K}_{m_y},k^*,i,j}, N_{\mathcal{K}_{f_y},k^*,i,f,j}, \beta^*) + \sum_{i=1}^{N_c} \lambda_i N_{RB} \\ &\quad + \sum_{i=1}^{N_c} \sum_{f=1}^{N_f} \mu_{i,f} N_{RB} + \sum_{i=1}^{N_c} \sum_{j=1}^{N_r} \nu_{i,j} N_{RB}, \\ \text{s.t.} \quad N_{\mathcal{K}_{m_y},k,i,j} &\geq 0, \quad N_{\mathcal{K}_{f_y},k,i,f,j} \geq 0, \end{aligned} \quad (28)$$

where

$$\begin{aligned} L'(N_{\mathcal{K}_{m_y},k^*,i,j}, N_{\mathcal{K}_{f_y},k^*,i,f,j}, \beta^*) &= \log R_{k^*} - \sum_{i=1}^{N_c} \lambda_i C_{MBS,i,k=k^*} \\ &\quad - \sum_{i=1}^{N_c} \sum_{f=1}^{N_f} \mu_{i,f} C_{SBS,i,f,k=k^*} - \sum_{i=1}^{N_c} \sum_{j=1}^{N_r} \nu_{i,j} C_{RN,i,j,k=k^*} - \varphi C_{UE,k^*}. \end{aligned} \quad (29)$$

For each specific UE $k^* \in \{\mathcal{K}_{m_y}, \mathcal{K}_{f_y}\}$, only one specific link can be connected to it in a time slot. That is to say, there is only one specific combination of subscript which denotes as $(\mathcal{K}_{m_y}, k^*, i^*, j^*)$ or $(\mathcal{K}_{f_y}, k^*, i^*, f^*, j^*)$ that makes the decision variable x nonzero. Thus, for a specific UE k^* , there is only one item in the expression of $\log R_{k^*}$. By observing this, we can find that for a specific UE k^* , $L'(N_{\mathcal{K}_{m_y},k^*,i,j}, N_{\mathcal{K}_{f_y},k^*,i,f,j}, \beta^*)$ is a concave function of $(N_{\mathcal{K}_{m_y},k^*,i,j}, N_{\mathcal{K}_{f_y},k^*,i,f,j})$. Then the KKT conditions can be applied to obtain the optimal primal variables $(N_{\mathcal{K}_{m_y},k,i,j}, N_{\mathcal{K}_{f_y},k,i,f,j})$ at a given dual point β^* .

The KKT conditions of problem $P2$ are given as follows:

$$\nabla_{N_{\mathcal{K}_{m_y},k,i,j}} L(N_{\mathcal{K}_{m_y},k,i,j}, N_{\mathcal{K}_{f_y},k,i,f,j}, \beta^*, \xi_{\mathcal{K}_{m_y},k,i,j}, \xi_{\mathcal{K}_{f_y},k,i,f,j}) = 0, \quad (30)$$

$$\nabla_{N_{\mathcal{K}_{f_y},k,i,f,j}} L(N_{\mathcal{K}_{m_y},k,i,j}, N_{\mathcal{K}_{f_y},k,i,f,j}, \beta^*, \xi_{\mathcal{K}_{m_y},k,i,j}, \xi_{\mathcal{K}_{f_y},k,i,f,j}) = 0, \quad (31)$$

$$\xi_{\mathcal{K}_{m_y},k,i,j} N_{\mathcal{K}_{m_y},k,i,j} = 0, \quad \xi_{\mathcal{K}_{f_y},k,i,f,j} N_{\mathcal{K}_{f_y},k,i,f,j} = 0, \quad (32)$$

$$\xi_{\mathcal{K}_{m_y},k,i,j} \geq 0, \quad \xi_{\mathcal{K}_{f_y},k,i,f,j} \geq 0. \quad (33)$$

By applying KKT conditions, we can obtain the optimal resource allocation strategy:

$$N_{\mathcal{K}_{m_y},k,i,j} = \begin{cases} \frac{1}{\lambda_i + \varphi_k}, & y = 0 \\ \frac{1}{a\kappa_{m_1,k,i,j}\lambda_i + (1+a\kappa_{m_1,k,i,j})\nu_{i,j} + \varphi_k}, & y = 1 \\ \frac{1}{(1+a\kappa_{m_2,k,i,j})(\lambda_i + \nu_{i,j}) + \varphi_k}, & y = 2 \end{cases} \quad (34)$$

$$N_{\mathcal{K}_{f_y},k,i,f,j} = \begin{cases} \frac{1}{\mu_{i,f} + \varphi_k}, & y = 0 \\ \frac{1}{a\kappa_{f_1,k,i,f,j}\mu_{i,f} + (1+a\kappa_{f_1,k,i,f,j})\nu_{i,j} + \varphi_k}, & y = 1 \\ \frac{1}{(1+a\kappa_{f_2,k,i,f,j})(\mu_{i,f} + \nu_{i,j}) + \varphi_k}, & y = 2 \end{cases} \quad (35)$$

By substituting $N_{\mathcal{K}_{m_y},k,i,j}$ obtained by (34) into equation (24), substituting $N_{\mathcal{K}_{f_y},k,i,f,j}$ obtained by (35) into equation (25) and substituting $(N_{\mathcal{K}_{m_y},k,i,j}, N_{\mathcal{K}_{f_y},k,i,f,j})$ into equation (26) and (27), we have the expression of $\Delta\lambda_i$, $\Delta\mu_{i,f}$, $\Delta\nu_{i,j}$ and $\Delta\varphi_k$ expressed by the given dual point β^* . Finally, by operating the dual decomposition method based iteration algorithm and rounding down the expression of N , we can get the asymptotically optimal solution of problem $P1$.

5 Simulation Results

In this section, simulation results are provided to verify the effectiveness of the proposed algorithms. We simulate the proposed resource allocation strategy in a 7-cell cellular network with three-ring hexagonal cell structure. The radius of each cell is 500m, inside which 4 SBSs and 2 RNs are uniformly employed. The transmit powers of MBS, SBS, RN and UE are 46 dBm, 30 dBm, 30 dBm and 23 dBm, respectively. UEs are uniformly distributed in the network, and each cell serves 10 to 15 UEs. The entire frequency band is composed of 50 RBs, while the frequency reuse factor is set to one. Flat Rayleigh fading channel weighted by path loss is used as the channel model and the path-loss exponent α is fixed to 2.5. Besides, compensating coefficients δ_r and δ_f are set to 30, as illustrated in equation (8). Totally, 5000 time slots are simulated.

In Fig. 2, we compare the system performance under different CoMP configurations by presenting the cumulative distribution function (CDF) of the received SINR for all UEs with different cooperative strategies. Specially, in order to simplify the analysis, $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ is set to a same value denoted as σ . It is demonstrated that a better CDF performance can be achieved with CoMP transmission between RNs and BSs. With the decrease of σ , the received SINR of

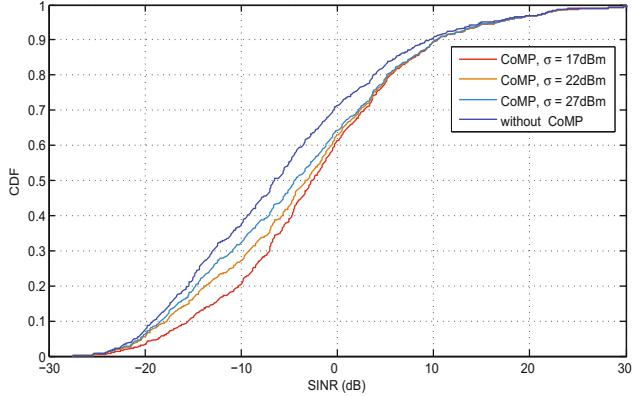


Fig. 2. SINR Empirical CDF comparison for systems with different CoMP threshold

UEs is improved gradually. This result is consistent with the understanding that the condition to utilize CoMP transmission is looser under lower σ value so that BSs can serve more UEs through cooperative model. This observation indicates the performance gain of implementing CoMP transmission in the system.

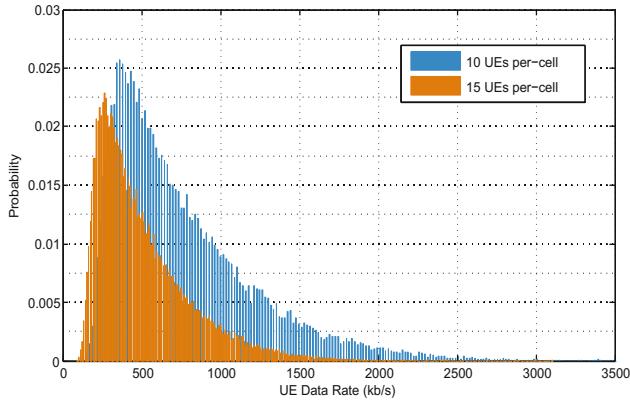


Fig. 3. UE data rate distribution comparison for systems with different UE number

In Fig. 3, the throughput performance for system with 10 UEs per cell and 15 UEs per cell is provided. It is illustrated that 80% UEs achieve a data rate in the range of 300 - 1350 kb/s in the 10 UEs per-cell case, and 200 - 900 kb/s in the 15 UEs per-cell case. Firstly, since only a small portion of UEs (5%) achieve a high data rate (≥ 1500 kb/s), the fairness of the proposed resource allocation strategy can be intuitively observed. In other words, the UEs with good channel quality are selectively ignored. Secondly, it is displayed that the majority of UEs' data rates is lower in the 15 UEs per-cell case than that in the 10 UEs per-cell case,

which is mainly caused by the additional interference and resource competition due to a greater number of UEs.

6 Conclusion

In this paper, we considered a general uplink-downlink multi-cell heterogeneous network model where small-cell base stations and relay nodes are uniformly distributed in each macro cell. By using dual decomposition method, we contributed a closed-form solution to the fairness optimization problem. System level simulation demonstrates the relatively balanced rate of UEs and the advantageous performance of our resource allocation strategy.

Acknowledgement. This paper is partially sponsored by National Key Project of China (No.2012ZX 03001013-003) and the open research fund of Zhejiang Provincial Key Lab of Data Storage and Transmission Technology, Hangzhou Dianzi University (No.201306)

References

1. Cui, Y., Lau, V., Wang, R.: Distributive subband allocation, power and rate control for relay-assisted OFDMA cellular system with imperfect system state knowledge. *IEEE Trans. Wireless Commun.* 8, 5096–5102 (2009)
2. Weng, L., Murch, R.: Cooperation strategies and resource allocations in multiuser OFDMA systems. *IEEE Trans. Veh. Technol.* 58, 2331–2342 (2009)
3. Fooladivanda, D., Rosenberg, C.: Joint resource allocation and user association for heterogeneous wireless cellular networks. *IEEE Trans. Wireless. Commun* 12(1) (January 2013)
4. Ksairi, N., Bianchi, P., Ciblat, P., Hachem, W.: Resource allocation for downlink cellular OFDMA systems part I: optimal allocation. *IEEE Trans. Signal. Processing*. 58(2), 720–734 (2010)
5. Ksairi, N., Bianchi, P., Ciblat, P., Hachem, W.: Resource allocation for downlink cellular OFDMA systems part II: practical algorithms and optimal reuse factor. *IEEE Trans. Signal. Processing*. 58(2), 735–749 (2010)
6. Ng, D., Schober, R.: Resource allocation and scheduling in multi-cell OFDMA systems with decode-and-forward relaying. *IEEE Trans. Wireless. Commun.* 10(7), 2246–2258 (2011)
7. Li, Q., Hu, R., Qian, Y., Wu, G.: Intracell cooperation and resource allocation in a heterogeneous network with relays. *IEEE Trans. Veh. Technol.* 62(4), 1770–1784 (2013)
8. Kelly, F., Maulloo, A., Tan, D.: Rate control for communication networks: shadow prices, proportional fairness and stability. *J. Oper. Res. Soc.* 49(3), 237–252 (1998)
9. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge Univ. Press, Cambridge (2004)

A Priority-Based Access Control Model for Device-to-Device Communications Underlaying Cellular Network Using Network Calculus

Jun Huang¹, Zi Xiong¹, Jibi Li¹, Qianbin Chen¹,
Qiang Duan², and Yanxiao Zhao³

¹ School of Communication and Information Engineering,
Chongqing University of Posts and Telecommunications, 400065 Chongqing, China
{xiaoniuadmin,xiong0000000}@gmail.com,
{lijb,chenqb}@cqupt.edu.cn

² Information Science and Technology Department,
The Pennsylvania State University, Abington, Pennsylvania 19001
qduan@psu.edu

³ Electrical and Computer Engineering Department,
South Dakota School of Mines and Technology, Rapid City, SD 57701
yanxiao.zhao@sdsmt.edu

Abstract. Device-to-Device (D2D) communication has been proposed as a beneficial complement for cellular networks. Access control for D2D communications underlaying cellular network, however, has not received attention yet. In this paper, we investigate the access control for cellular and D2D communications in a single cell setting. We propose a priority-based model to characterize access control of both cellular and D2D users. The proposed model prioritizes the cellular communications, cellular mode D2D communications, and reuse mode D2D communications with different priority levels. We then apply Network Calculus theory to analyze the worst-case performance for access control, including service rate, delay, and backlog for processing service requests of cellular and D2D communications. Both of the theoretical analysis and the numerical results verify that the proposed model is valid and applicable to characterize the access control for D2D underlaying cellular network.

Keywords: Device-to-Device (D2D), multi-priority, network calculus, performance analysis.

1 Introduction

The ever-growing mobile multimedia services impose a great challenge on higher data rate of wireless communication, which calls for a new communication scheme underlay current cellular systems. *Device-to-Device* (D2D) communication is an emerging technology that has been introduced as a beneficial complement of cellular infrastructure. D2D communication paradigm facilitates mobile devices to directly communicate with each other without help of infrastructure and reuse

radio resource of cellular networks; thus mitigating the system overhead, increasing the spectrum utilization, and improving the cellular coverage [1]. Recent advancements from both academia and industries show that D2D technology has been attracting considerable interest. For example, the *Third Generation Partnership Project* (3GPP), *Long Term Evolution* (LTE) as well as the *LTE-Advanced* (LTE-A) project consider to employ D2D as the potential solution for supporting growing communication demands. Therefore, D2D plays a vital role in improving the performance of cellular system, and it is expected to be an indispensable ingredient of the next generation wireless communication systems [2].

When D2D users share the spectrum resources with cellular users, a major technical concern lies in the mutual interference between them. While there have been various radio resource management schemes proposed to address intra- and inter-cell interferences [3], [4], [5], [6], access control as an initial step toward resources coordination for mitigating interference, however, has not received enough attention yet in existing works. In prior works there lacks a direct insight about the achievable performance for system access perceived by the cellular and D2D users when they request connection setup. On the other hand, modeling access control for D2D underlaying cellular network is facing a special challenge: the diversity of D2D communication modes requires a general modeling approach that is applicable to various D2D flows. Therefore, modeling the access control is a significant issue for D2D underlaying cellular network, which is the main research focus of our work.

In general, D2D underlaying cellular network can be classified into three communication modes: cellular, dedicated and reuse [1]. Plus cellular communications, there are four communication varieties in a cell when D2D co-existing with cellular users, that is, cellular communications, cellular mode D2D communications, dedicated mode D2D communications, and reuse mode D2D communications. Among these communications, in fact, each of them should be granted different priorities. For example, the cellular communications have to be guaranteed first without harmful interference, and thus it stays at the top priority over D2D communications. Within D2D communications, cellular mode D2D communication is essentially interference-free, while the reuse mode D2D communications may cause interference to existing cellular communications. Therefore cellular mode D2D requests have the higher priority than the reuse mode D2D communications. It is worth to mention that D2D communications using dedicated mode are not considered since such requests employ reserved channels and do not need to compete with other communications.

In this paper, we investigate the access control for cellular and D2D communications in a single cell setting. We propose a priority-based model to characterize the spectrum access of both cellular and D2D users. The proposed model consists of three priority queues, which are designed for the cellular communications, cellular mode D2D communications, and reuse mode D2D communications, respectively. We then apply *Network Calculus* theory to analyze the worst-case system performance in terms of service rate, delay, and backlog for two types of

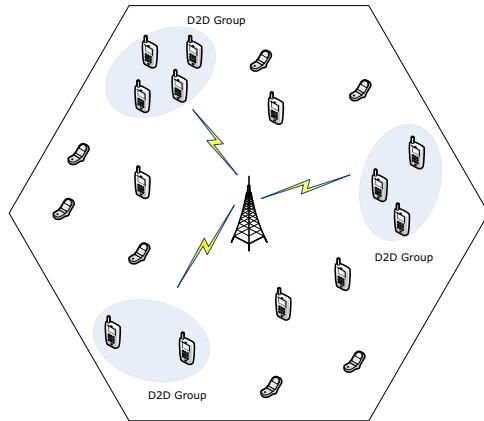


Fig. 1. D2D communications as an underlay in a cell

flows. Numerical results further confirm the validity of our theoretical analysis. The major contributions of this paper are briefly summarized as follows:

- We propose a priority-based model to characterize the access control of cellular and D2D communications in a single cell. The proposed model provides insights into analyzing access control performance, which facilitate mitigating interferences and enhancing QoS for D2D communications.
- We apply network calculus to analyze the worst-case performance of the proposed model. The performance bounds, including service rate, delay, and backlog of both cellular and D2D flows are obtained. To the best of our knowledge, this is the first work that applies network calculus in analyzing access control of D2D communications underlaying cellular network.
- We perform thorough theoretical analysis and extensive numerical simulations. Results verify that the proposed model is valid and applicable to characterize the access control for D2D underlaying cellular network.

The rest of this paper is organized as follows. Section 2 presents the system framework, then models the access control for D2D underlaying cellular networks. Section 3 analyzes the performance of both cellular and D2D communications using network calculus and obtains the performance bounds. The numeric experiments are presented in Section 4 to validate the analyzing results. Section 5 concludes the paper.

2 Modeling Access Control for D2D Underlaying Cellular Network

2.1 System Overview

We consider a networking scenario as shown in Fig. 1, in which D2D communications form an underlay that coexists with cellular communications in a single

cell. For such a scenario, we assume that all communications follow a centralized control pattern; that is, the Base Station (BS) serves as the mediator that establishes connections for both cellular and D2D users. Upon receiving a connection request from a cellular user, the BS sets up a direct uplink from the user to the BS. When a D2D user submits a connection request, the BS assists the D2D user to discover the peers, pair the candidate peers, and eventually establish a D2D communication connection.

Since the BS is able to readily obtain location information of user equipments (UEs), the peer discovery and pairing procedures can be accomplished through a certain signaling approach, which is not detailed here due to the space limitation. For link establishment procedure, the BS classifies each request and endows it a priority according to the D2D communication mode. The rules for request classification and prioritization are given in the following of our proposed model.

2.2 Access Control Model

In order to characterize the behavior of connection requests to access the central controller at a BS, we propose a priority-based access control model as shown in Fig. 2. The model consists of three queues where the top, middle, and bottom queue are designed for flows with the highest priority (f_H), the medium priority (f_M), and the lowest priority (f_L), respectively. As D2D communications can be generally classified into cellular, dedicated, and reuse modes according to their locations in a cell, we enable the regular cellular connection requests to have the highest priority, D2D requests with cellular mode to have the medium priority, and D2D requests with reuse mode to have the lowest priority in the model. This is because for the regular cellular communication, the high priority should be strictly guaranteed; for D2D requests with reuse mode, they may cause interference to the cellular users, and thus it should have the lowest priority; while for D2D requests with cellular mode, they will not cause interference to the cellular users, therefore it should have higher priority than D2D requests with reuse mode but lower priority than regular cellular requests. Note that D2D requests using dedicated mode are excluded in our model since such a kind of requests can be served immediately after they arrive.

Working in this way, the model characterizes the access control of both cellular and D2D communications. In the following, we analyze the performance for three types of flows according to the model. We will obtain the insights of access control performance, which may facilitate mitigating interferences and enhancing QoS for D2D communications.

3 Performance Analysis for Access Control

In this section, we first present the definitions and notations on network calculus, and then we analyze the performance for access control of flows based on proposed model.

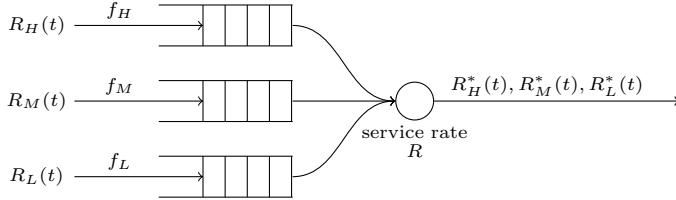


Fig. 2. Priority-based access control model

3.1 Definitions and Notations

The theory of network calculus was first developed by Chang [7] and Cruz [8], [9] and then extended by others (e.g. [10], [11], [12], [13]). The theory formulates the access control model on the following definitions basis.

Definition 1. (*Wide-sense Increasing Sequences*). If $F = \{f(t) | f(t) = 0, \forall t < 0; f(0) \geq 0; f(s) \leq f(t), \forall s \leq t, s, t \in [0, +\infty]\}$, we say that F is wide-sense increasing sequences.

Definition 2. (*Min-Plus Convolution*). Let f and g be two functions or sequences of F . The min-plus convolution of f and g is the function $(f \otimes g)(t) = \inf_{0 \leq u \leq t} [f(u) + g(t-u)]$, if $t < 0$, $f \otimes g = 0$.

Definition 3. (*Arrival Curve*). Given a wide-sense increasing function α defined for $t \geq 0$, we say that a flow R is constrained by α if and only if for all $s \leq t$ such that $R(t) - R(s) \leq \alpha(t-s)$. We say that R has α as an arrival curve, or also that R is α -smooth.

Since the arrival curve is often regulated by the leaky buckets, we will use affine arrival curves $\gamma_{r,b}$, defined by: $\gamma_{r,b}(t) = rt + b$ for $t > 0$ and 0 otherwise. Parameters b and r are called the burst tolerance and rate.

Definition 4. (*Service Curve*). Consider a system S and a flow through S with input and output function R and R^* . We say that S offers to the flow a service curve β if and only if β is wide sense increasing, $\beta(0) = 0$ and $R^* \geq R \otimes \beta$.

Assume a flow constrained by arrival curve α , traverses a system that offers a service curve of β , then

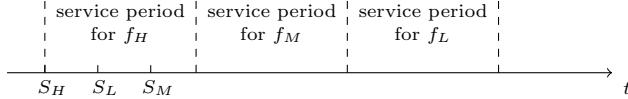
Definition 5. (*Delay Bound*). The delay bound $P(t)$ is expressed as

$$P(t) \leq h(\alpha, \beta) \quad (1)$$

$$h(\alpha, \beta) = \sup_{t \geq 0} \{\inf \{d \geq 0 : \alpha(t) \leq \beta(t+d)\}\} \quad (2)$$

Definition 6. (*Backlog Bound*). The delay bound $Q(t)$ is expressed as

$$Q(t) = R(t) - R^*(t) \leq \sup_{s \geq 0} \{\alpha(s) - \beta(s)\} \quad (3)$$

**Fig. 3.** A flows' arriving example

3.2 Performance Analysis

Consider the BS that serves three request flows f_L , f_M and f_H where f_L , f_M and f_H denotes flow with low priority, medium priority, and high priority, respectively, and they are arrived in a short interval. Suppose $R_L(t)$, $R_M(t)$, $R_H(t)$ and $R_L^*(t)$, $R_M^*(t)$, $R_H^*(t)$ are the inputs and outputs accumulation functions for the three flows as illustrated in Fig. 2, $\alpha(t)$, $\beta(t)$ is the arrival curve and service curve respectively, the backlogged period of flow f_i starts at S_i such that $R(S_i) = R^*(S_i)$.

Without loss of generality, we assume that all of the flows arrive in a short period and the arrival order of flows are f_H , f_L , and f_M as indicated in Fig. 3. Note that the analysis for the cases of arbitrary flows' arriving interval and order can also be conducted in a similar way based on the assumptions.

Let us first consider the low priority flow f_L . S_L falls in the period of f_H , i.e. the case of above example. Assume $\alpha_M = \gamma_{r_M, b_M}$ and $\alpha_H = \gamma_{r_H, b_H}$ be the arrival curves, namely, the f_M and f_H are constrained by the leaky buckets, to any time t and S_L , the system output during the interval $(S_L, t]$ is $R(t - S_L)$. Thus

$$\begin{aligned} R_L^*(t) - R_L^*(S_L) &= R(t - S_L) - \\ [R_M^*(t) - R_M^*(S_L)] - [R_H^*(t) - R_H^*(S_L)]. \end{aligned} \quad (4)$$

At time S_L , the backlog of f_L is empty, hence $R_L^*(S_L) = R_L(S_L)$, therefore

$$\begin{aligned} R_L^*(t) &= R_L(S_L) + R(t - S_L) - \\ [R_M^*(t) - R_M^*(S_L)] - [R_H^*(t) - R_H^*(S_L)]. \end{aligned} \quad (5)$$

This suggests that

$$R_M^*(t) - R_M^*(S_L) \leq R_M(t) - R_M(S_L) \leq \alpha_M(t - S_L), \quad (6)$$

$$R_H^*(t) - R_H^*(S_L) \leq R_H(t) - R_H(S_L) \leq \alpha_H(t - S_L), \quad (7)$$

and

$$R_M^*(t) - R_M^*(S_L) \geq 0, R_M^*(t) - R_M^*(S_L) \geq 0. \quad (8)$$

Integrating equations (5), (6), (7), (8), we can obtain

$$\begin{aligned} R_L^*(t) &\geq R_L(S_L) + [R(t - S_L) - \alpha_M(t - S_L) \\ - \alpha_H(t - S_L)]^+ = R_L(L) + S(t - S_L), \end{aligned} \quad (9)$$

where $S(u) = [Ru - \alpha_M(u) - \alpha_H(u)]^+$.

If $S(u)$ is wide-sense increasing, the service curve of f_L equals to the function $S(u)$, i.e. $\beta_{R_L, T_L}(t) = R_L(t - T_L)^+$, where $(x)^+ = \max(x, 0)$. This is the rate-latency service curve with service rate $R_L = R - r_M - r_H$ and latency $T_L = \frac{b_M + b_H}{R - r_M - r_H}$.

Let us proceed to examine the flow that has medium priority. Since the flows arrive in the short period, f_M will wait for the transmission of f_H until the queue is empty. To an arbitrary time t , the output of system during period $(S_M, t]$ is $R(t - S_M)$. Thus

$$\begin{aligned} R_M^*(t) - R_M^*(S_M) &\geq R(t - S_M) - \\ &[R_H^*(t) - R_H^*(S_M)]. \end{aligned} \quad (10)$$

Likewise, we can rewrite above formula as

$$\begin{aligned} R_M^*(t) &\geq R_M(S_M) + [R(t - S_M) - \alpha_H(t - S_M)]^+ \\ &= R_M(S_M) + S(t - S_M) \end{aligned} \quad (11)$$

where $S(u) = [Ru - \alpha_H(u)]^+$. If $S(u)$ is wide-increasing, the service curve f_M equals to the function $S(u)$, the rate is $R_M = R - r_H$ and the latency is $T_M = \frac{b_H}{R - r_H}$.

Now we consider the high priority flow. Suppose f_H arrives at the system first. The flow of f_H would be accepted immediately as long as it arrives, until the queue for f_H becomes empty, then

$$R_H^*(t) - R_H^*(S_H) = R(t - S_H). \quad (12)$$

Therefore we can obtain

$$\begin{aligned} R_H^*(t) &= R_H(S_H) + R(t - S_H) \\ &= R_H(S_H) + S(t - S_H). \end{aligned} \quad (13)$$

That is, the service curve of f_H is $\beta_{R_H, T_H}(t) = S(u) = R(t - 0)^+$, in which the service rate is $R_H = R$, and the latency is $T_H = 0$.

With above analysis in hand, we can write the delay and backlog bounds for three flows according to Eq. (1), (2), and (3).

For high priority flow, we have

$$P_H \leq \frac{b_H}{R}, \quad (14)$$

$$Q_H \leq b_H. \quad (15)$$

For medium priority flow, we have

$$P_M \leq \frac{b_H + b_M}{R - r_H}, \quad (16)$$

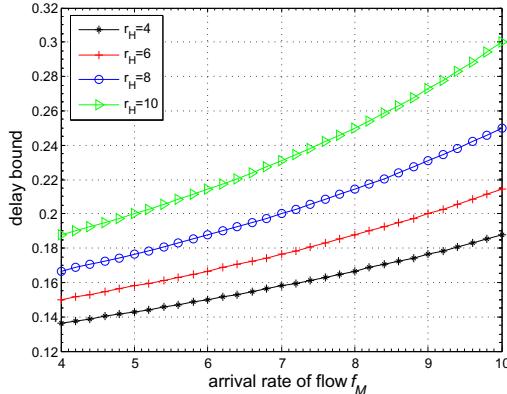
$$Q_M \leq b_M + r_M \cdot \frac{b_H}{R - r_H}. \quad (17)$$

For low priority flow, we have

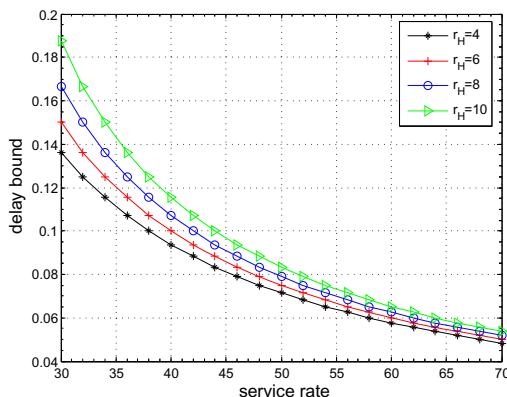
$$P_L \leq \frac{b_L + b_M + b_H}{R - r_M - r_H}, \quad (18)$$

$$Q_L \leq b_L + r_L \cdot \frac{b_M + b_H}{R - r_M - r_H}. \quad (19)$$

Eq. (14) – (19) indicate that the delay and backlog bounds of low priority flow are affected by the arrival curves of higher priority flows, and those of high priority flow are impacted by its own arrival curve. These observations conform to the design of our model.



(a) $R = 30, r_M \in [4, 10], r_L = 4, r_H = 4, 6, 8, 10$



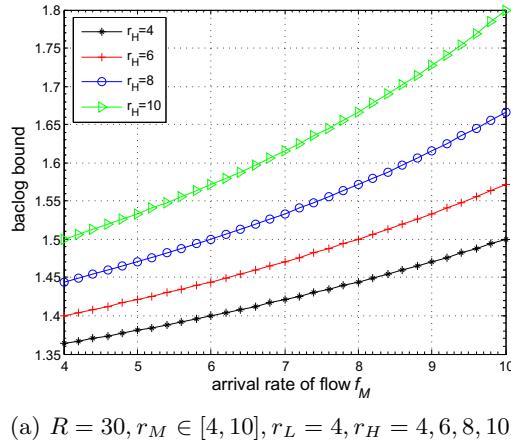
(b) $R \in [30, 70], r_M = r_L = 4, r_H = 4, 6, 8, 10$

Fig. 4. Delay bounds of low priority flow with different parameters settings

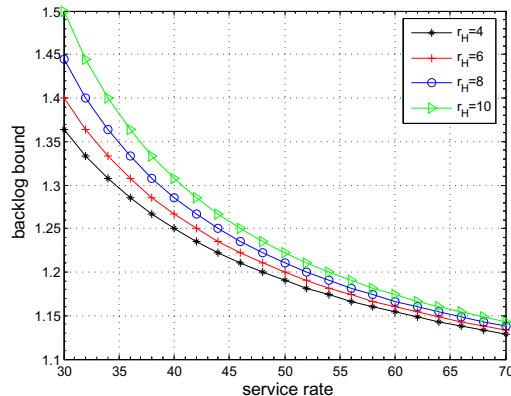
4 Numeric Results

In this section, we verify the proposed model and the performance analysis by numerical experiments. We set the burst parameter of leaky bucket and the maximum packet all to be 1. Note that the value used herein is for illustrative validation, the same conclusion can be obtained if other values are set. Using these settings, we also examine the factors that affect the delay and backlog bounds.

Fig. 4 plots the delay bounds of reuse mode D2D request flow (f_L) with different parameter setting of cellular (f_H) and cellular mode D2D request flows (f_M). As can be observed from Fig. 4(a) that, the delay bound of reuse mode D2D flow turns to be loose with higher arrival rate of higher priority flow when the service rate of BS and arrival rate of f_L are fixed. This implies that the delay bound of low priority flows is affected by the arrival rate of higher priority flows,



(a) $R = 30, r_M \in [4, 10], r_L = 4, r_H = 4, 6, 8, 10$



(b) $R \in [30, 70], r_L = r_M = 4, r_H = 4, 6, 8, 10$

Fig. 5. Delay bounds of low priority flow with different parameters settings

which conforms our analysis in previous section: the larger arrival rate of higher priority flow is, the longer time low priority flow waits. Fig. 4(b) shows the delay bounds of f_L with different service rate and arrival rate of highest priority flow. As expected, the delay bound tends to be tighter with the higher service rate of BS. It is natural to infer from the model that the waiting time in the queue is short when the service rate of BS is high. This again confirms the validity for our proposed model and analysis.

Fig. 5 illustrates the backlog bounds with the same conditions. We observe that the backlog bound increases when the arrival rate of high priority flows becomes higher, but decreases when the service rate turns to be higher. These fully match the similar insights obtained from Fig. 4.

In summary, we claim that the proposed model and derived analysis are reasonable and valid, thus are applicable to characterize the access control for D2D communications underlaying cellular network.

5 Conclusion

In this paper, we have addressed the access control for cellular and D2D communications in a single cell setting. We have proposed a priority-based model to characterize the access of both cellular and D2D users. The proposed model consists of three priority queues, which are designed for the cellular communications, D2D communications using cellular mode, and D2D communications using reuse mode, respectively. We have applied network calculus theory to analyze the worst-case system performance in terms of service rate, delay, and backlog for different types of flows. Through extensive numeric results, it has been shown that the service rate of BS and the arrival rate of cellular request flow will have impacts on the worst-case performances of D2D request flows. The proposed model is reasonable, and thus it is applicable to characterize the access control for D2D underlaying cellular network.

As for future works, we plan to investigate how our solutions adapts to the mobile devices and how can our model be integrated with current and future cellular networks.

Acknowledgement. This work is supported by NSFC (Grant No. 61309031), Program for Innovation Team Building at Institutions of Higher Education in Chongqing (Grant No. KJTD201310), Natural Science Foundation of Chongqing, (Grant No. cstc2013jcyjA40026), Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant No. KJ130523, J2012-13), and CQUPT Research Fund for Young Scholars (Grant No. A2012-79).

References

1. Fodor, G., Dahlman, E., Mildh, G., Parkvall, S., Reider, N., Miklos, G., Turanyi, Z.: Design aspects of network assisted device-to-device communications. *IEEE Communications Magazine* 50, 170–177 (2012)

2. Doppler, K., Rinne, M., Wijting, C., Ribeiro, C., Hugl, K.: Device-to-device communication as an underlay to lte-advanced networks. *IEEE Communications Magazine* 47, 42–49 (2009)
3. Fodor, G., Della Penda, D., Belleschi, M., Johansson, M., Abrardo, A.: A comparative study of power control approaches for device-to-device communications. In: 2013 IEEE International Conference on Communications (ICC), pp. 6008–6013 (June 2013)
4. Phunchongharn, P., Hossain, E., Kim, D.: Resource allocation for device-to-device communications underlaying lte-advanced networks. *IEEE Wireless Communications* 20, 91–100 (2013)
5. Xu, C., Song, L., Han, Z., Zhao, Q., Wang, X., Cheng, X., Jiao, B.: Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach. *IEEE Journal on Selected Areas in Communications* 31, 348–358 (2013)
6. Pei, Y., Liang, Y.-C.: Resource allocation for device-to-device communications overlaying two-way cellular networks. *IEEE Transactions on Wireless Communications* 12, 3611–3621 (2013)
7. Chang, C.-S.: Stability, queue length, and delay of deterministic and stochastic queueing networks. *IEEE Transactions on Automatic Control* 39(5), 913–931 (1994)
8. Cruz, R.: A calculus for network delay. i. network elements in isolation. *IEEE Transactions on Information Theory* 37(1), 114–131 (1991)
9. Cruz, R.: A calculus for network delay, part ii: Network analysis. *IEEE Transactions on Information Theory* 37(1), 132–144 (1991)
10. Agrawal, R., Cruz, R.L., Okino, C., Rajan, R.: Performance bonds for flow control protocols. *IEEE/ACM Trans. Netw.* 7(3), 310–323 (1999)
11. Jiang, Y., Liu, Y.: Stochastic network calculus. Springer, London (2008)
12. Le Boudec, J.-Y., Thiran, P.: Network Calculus. LNCS, vol. 2050. Springer, Heidelberg (2001)
13. Le Boudec, J.-Y.: Application of network calculus to guaranteed service networks. *IEEE Transactions on Information Theory* 44(3), 1087–1096 (1998)

A Privacy Threat in 4th Generation Mobile Telephony and Its Countermeasure

Changhee Hahn¹, Hyunsoo Kwon¹, Daeyoung Kim¹, Kyungtae Kang²,
and Junbeom Hur¹

¹ School of Computer Science and Engineering, Chung-Ang University,
Seoul, Republic of Korea

{Mckinsey, khs910504, rlaeod, jbhur}@cau.ac.kr

² Department of Computer Science and Engineering, Hanyang University,
Ansan, Republic of Korea
ktkang@hanyang.ac.kr

Abstract. Mobile telephony device is widely used these days. Protecting subscribers privacy is crucial and can be achieved by evading linkability of subscribers by malicious third parties. In this paper, we analyze the privacy-related security properties of 4th generation mobile telephony, especially LTE. We suggest an attack model which makes it possible to trace a victim's mobile device so that the attacker can know the presence of the victim's device in a specific area. Tracking subscribers' location by unauthorized third parties may violate the privacy of subscribers. To solve this problem, we propose a modified authentication protocol in LTE to preserve location privacy of the device. Considering security level and efficiency, we build our scheme to have low computational overhead and strong secrecy. Also we prove that the proposed scheme satisfies unlinkability property using the automatic verification tool ProVerif.

Keywords: LTE, location privacy, authentication, security.

1 Introduction

Tracing location of a mobile subscriber is only available to legitimate network operators, which is for the purpose of providing communication service to their subscribers [1]. Activities such as collecting the information of a subscriber's location is allowed only when subscribers agree with it. If it is possible for a third party group to track subscribers' location, various kinds of malicious behaviors can occur. For example, someone may collect a subscriber's location information illegally to monitor their movements. Then, he uses the information for commercial purpose. Besides, the exposure of a subscriber's personal location can be used for a crime-purpose, which leaves their privacy vulnerable. Therefore, protecting such private information from being exposed to an illegal third party is crucial for keeping one's privacy intact [2].

Across countries all around the world, LTE(Long Term Evolution), the 4th generation mobile communication protocol has been widely adopted. In South Korea, for example, the ratio of increasing number of subscribers for LTE is

rapidly growing. Total subscribers reached 7 millions only a year after launching LTE service in domestic market [3]. In LTE protocol, before a mobile management entity(MME) provides communication service to a mobile equipment(ME), it is necessary to verify that the ME is a valid subscriber of the MME. For this, the Evolved Packet System Authentication and Key Agreement(EPS-AKA) protocol is used to authenticate the ME. When the authentication succeeds, the ME then gets approved from the MME for the service access which it provides.

For the procedure of authentication, first the MME sends an authentication request message to the ME. After receiving the message, the ME sends a response message to the MME to identify himself. In this situation, a third party can eavesdrop the message which the MME sends by performing man-in-the-middle attack, then he sends the same message to the ME [4,5]. When received, the ME sends an authentication response message to the attacker. By checking some information included in the message, the attacker can decide whether the ME is in his observation area. For this reason, a subscriber's location information is revealed. A similar problem of a subscriber's location information exposure exploiting the weakness of authentication procedures was introduced in other communication protocols including third generation mobile protocol [16].

To solve such a subscriber's location information exposure problem, we suggest a modified EPS-AKA protocol. In the proposed scheme, authentication response messages are encrypted using symmetric key encryption algorithm. Therefore, secrecy and indistinguishability of messages can be achieved. This leads to protection of a subscriber's privacy. According to our unlinkability experiments [22], our proposed scheme guarantees the secrecy of a subscriber's location information. In addition to that, we design the protocol to lower computation and storage costs by minimizing additional overhead of key generation procedures without security degradation.

2 Related Work

In this section, we first look at the overall architecture of Authentication and Key Agreement(AKA) protocol introduced in 3G networks, and then describe a security threat.

2.1 The Structure of 3G-AKA Protocol

Since a similar problem exists in 3G protocol, we first introduce the structure of 3G-AKA protocol, and look at the attack scenario of how an adversary fulfills his goal. In 3G networks, a mobile station(MS) and a network operator mutually authenticate each other through 3G-AKA protocol. They generate shared session keys respectively which are used for further communication between the two parties. International Mobile Subscriber Identities(IMSI) are shared between the network and the MS. IMSI is used for identifying a subscriber, and is a special parameter for generating a key K_{IMSI} . K_{IMSI} is a main element with regard to the authentication procedure. It is only available to the network and the MS. Two parties share the same sequence number(SQN) to protect themselves against replay attack. The detailed 3G-AKA protocol is shown in Figure 1.

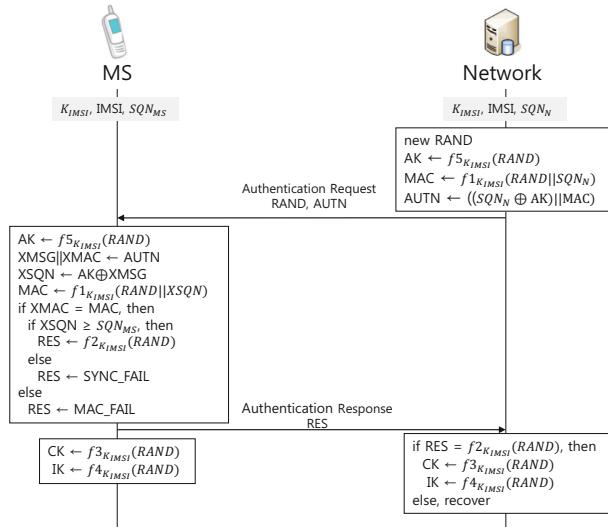


Fig. 1. 3G AKA Authentication Procedure

Network → MS: Authentication Request

1. The network generates a random number RAND.
2. The network generates an anonymity key(AK) using $f5$, a pseudo-random function that takes RAND as an input.
3. Another pseudo-random function $f1$ takes $RAND||SQN_N$ to generate Message Authentication Code(MAC).
4. $SQN_N \oplus AK$ and MAC are concatenated to make an Authentication Token(AUTN). Then, AUTN is sent with RAND to the MS.

When the MS takes the authentication request message, it generates an authentication response message as follows.

MS → Network: Authentication Response

1. Given RAND, the MS generates AK using $f5$.
2. From AUTN, the MS extracts $SQN_N \oplus AK$ (say XMSG) and MAC(say XMAC).
3. By calculating $AK \oplus XMSG$, the MS gets SQN_N (say XSQN).
4. MAC is generated by $f1$ on input XSQN and RAND.
5. If $MAC \neq XMAC$, the MS sends a MAC_FAIL message.
6. If $MAC = XMAC$ and $XSQN < SQN$, the MS sends a SYNC_FAIL message.
7. If $MAC = XMAC$ and $XSQN \geq SQN$, the RES is generated by another pseudo-random function $f2$ on input RAND. Then, the RES is sent to the network.

After sending RES, the MS generates a Ciphering Key(CK) and a Integrity Key(IK) using pseudo-random functions $f3$ and $f4$ respectively on input RAND. In the meantime, the network compares RES with the output of $f2$. If both are the same, then it generates CK and IK in the same way the MS does.

2.2 A Linkability Attack Scenario in 3G-AKA

3G-AKA protocol is vulnerable to a Man-in-the-Middle attack. The attack procedure is as follows.

1. An attacker eavesdrops the authentication request message $RAND||AUTN$ sent from the network to the mobile station(MS).
2. After the victim MS sends the authentication response message RES to the network, the attacker broadcasts the captured message $RAND||AUTN$ to all MSs who are in the observation area.
3. Since the message from the attacker is exactly the same as the previous one sent from the network, the victim MS sends RES' to the attacker. In this case, RES' contains SYNC_FAIL. On the other hand, all the other MSs also send RES's to the attacker. This time, every RES' contains MAC_FAIL.
4. The attacker now knows the existence of the victim MS since only the victim MS sent SYNC_FAIL while all the others sent MAC_FAILS.

This type of attack is called *message-device linkability attack*. This can be performed not only to 3G-AKA protocol, but also to EPS-AKA protocol. [16] shows a countermeasure for this problem in 3G networks, but it has several disadvantages. With regard to computational overhead, it exploits public key encryption to encrypts the message rather than symmetric encryption algorithm. Also, its response message size is much longer compared to the original one, which requires more communication and storage cost. There's another solution for solving such *message-device linkability attack* in EPS-AKA protocol [6]. This is also, however, inefficient because of a public-key encryption scheme. Lai et al. [25] introduced a group authentication protocol for LTE networks. In case of location privacy issues, their scheme encrypts MAC failure messages by exploiting Arpinis et al.'s scheme [16]. However, since it does not encrypt the synchronization messages, the linkability problem cannot be solved along with the efficiency issue. Although Ta and Baras [26] also proposed a scheme to solve the location privacy issues, their scheme cannot solve the problem in EPS-AKA protocol since it only handles the issue during paging procedures.

3 EPS-AKA Message-Device Linkability Attack and Its Countermeasure

3.1 The Structure of 4th Generation Mobile Network

Authentication Participants. There are four entities involved in LTE authentication procedure between a mobile operator and a subscriber. On subscriber-side, there are Universal Subscriber Identification Module(USIM) and mobile

equipment(ME). USIM has a subscriber's information and identification number. Also, most of parameters and keys used in authentication procedure are generated in USIM [7]. ME, the other participant on subscriber-side, acts like a intermediate relay point. It relays messages between USIM and a mobile operator.

On mobile operator-side, there are Mobile Management Entity(MME) and Home Subscriber Server(HSS). MME is a core component for LTE. It manages data transmission, signals configuration, and security service between MEs. Meanwhile, HSS manages all subscribers' information, such as location, authentication and service. It generates authentication parameters which are needed to identify a ME, and sends them to MME [8,9].

Authentication Parameters. A set of pseudo-random functions f_1, f_2, f_3, f_4 , and f_5 are used in EPS-AKA procedure to generate a set of authentication parameters and keys [12]. Authentication Management Field(AMF) is inserted into AUTN. It specifies a certain algorithms to use for generating authentication parameters [10]. By using a high-level master key K , Access Security Management Entity(ASME) generates K_{ASME} . K_{ASME} is a local master key in LTE and used for secure communication between a mobile user and network [19]. Only a ME and a MME who manages certain area where the ME is in have the access authority to K_{ASME} [20]. Key Derivation Function(KDF) is a key generation function, which is used for generating K_{ASME} [11]. AUTN consists of SQN, AK, MAC, and AMF. Finally RAND, RES, K_{ASME} , and AUTN make up an Authentication Vector(AV). HSS sends it to MME.

3.2 EPS-AKA

As shown in Figure 2, compared to the 3G-AKA protocol, EPS-AKA has its own specific keys and authentication vector generation procedure.

1. HSS → MME: AV
 - HSS generates RAND and SQN.
 - MAC is generated using f_1 on input RAND, SQN, and AMF.
 - RES is generated using f_2 on input RAND.
 - A set of keys CK, IK, AK are generated using f_3, f_4 , and f_5 on input RAND respectively.
 - KDF takes CK, IK, SN_{id} , and $SQN \oplus AK$ to make K_{ASME} .
 - AUTN consists of the output of KDF on input $SQN \oplus AK$, MAC, AMF.
 - HSS makes AV which contains RAND, RES, K_{ASME} , and AUTN, which is sent to MME.
2. MME → ME: (RAND, AUTN)
 - MEE sends RAND and AUTN out of AV to ME. It has other components of AV for future communication and authentication purpose.
3. ME → USIM: (RAND, AUTN)
 - ME relays RAND and AUTN to USIM.
4. USIM → ME: (RES, CK, IK)

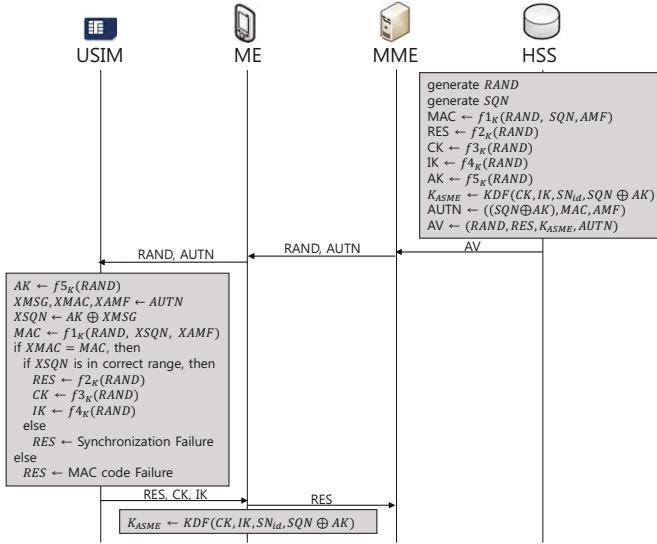


Fig. 2. Key Generation and Delivery in EPS-AKA Protocol

- AK is generated in just like the way in HSS.
 - From AUTN, USIM extracts $SQN \oplus AK$ (say XMSG), MAC (say XMAC), and AMF (say XAMF).
 - By calculating $AK \oplus XMSG$, USIM gets SQN (say XSQN).
 - If $XMAC \neq MAC$, RES is MAC Code Failure.
 - If $XMAC = MAC$ and XSQN not in correct range, RES is Synchronization Failure.
 - If $XMAC = MAC$ and XSQN in correct range, RES, CK, and IK are generated on input RAND using f_2 , f_3 , and f_4 respectively.
 - USIM finally sends RES, CK, and IK to ME.
5. ME → MME: RES
- ME sends RES to MME. It keeps keys CK and IK to generate K_{ASME} for future communication with MME.

When received RES, MME checks RES with the other that was given from HSS. If they are the same, the authentication procedure is successful.

3.3 Proposed Scheme

EPS-AKA Message-Device Linkability Attack. In EPS-AKA protocol, ME and MME do not exchange any key alone to prevent an adversary from performing active attacks [14]. In light of a third party, he can not deduce any location information of a specific ME. However, by simply sending the captured message, an adversary can detect the location of the ME within his observation area.

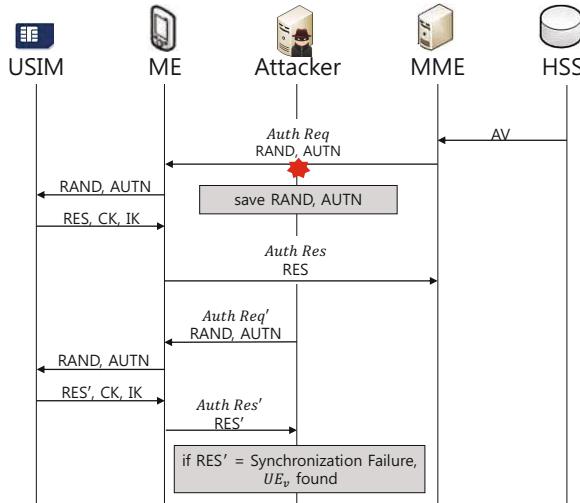


Fig. 3. Message-Device Linkability Attack using Authentication Message

As shown in Figure 3, an attacker can eavesdrop a message sent from MME on the air using femtocell techniques [15,16]. After capturing *Auth Req*, he re-sends it to all MEs in his observation area including the victim ME, say *ME_v*. In case of *ME_v*, since *Auth Req'* is the same as the one sent from MME, *ME_v* sends *Auth Res'* to the attacker. In this case, *RES'* contains Synchronization Failure. On the contrary, from the perspective of all other MEs, the MAC in the AUTN is not the same as XMAC. This leads each ME except for *ME_v* to send *Auth Res'*. This time, each *RES'* contains MAC Code Failure [17,18]. Because the messages sent from *ME_v* and the other MEs are clearly different, the attacker now can know whether *ME_v* is located in his observation area or not. This is severe violation of one's privacy.

Solution. To avoid such a leak of a subscriber's location information, the two types of authentication failure messages must be indistinguishable under an adversary's view. By encrypting two types of failure messages, MAC Code failure and Synchronization failure, it is not possible to track the origin of messages. Our proposed scheme is shown in Figure 4. The main difference between the original EPS-AKA and our scheme is the key generation procedure in USIM. Unlike the original one, we generate CK, IK, and K_{ASME} before validation tests of MAC and SQN. If either of the validation tests fails, the authentication failure message is sent. However, to avoid them from being distinguishable, the message is encrypted randomly by adding rn . More detailed message encryption procedure is as follows.

- When the authentication fails, two random numbers, rn and $rand$ are generated.

- A new pseudo-random function f_0 is used with K_{ASME} on input $rand$ to make a secret key(SK).
- Then, the failure message is encrypted by SK on input rn , and sent with $rand$ to MME.

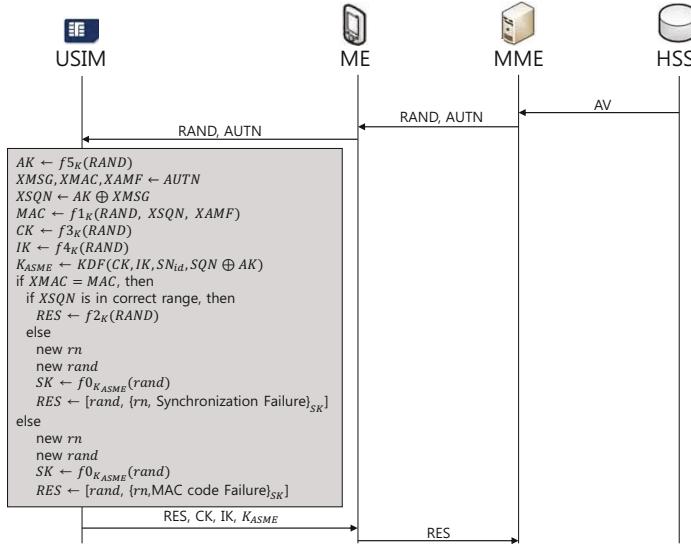


Fig. 4. The Modified EPS-AKA Protocol

It is notable that rn is newly generated whenever authentication fails. By randomizing any encrypted messages using rn , they are indistinguishable in the presence of an eavesdropper. After receiving the encrypted message, MME uses K_{ASME} (sent from HSS) on input $rand$ to generate SK. If both SKs are the same, MME can decrypt it. While MME can check which type of failure it is, it is infeasible for an adversary to decrypt the message because any of K_{ASME} or SK is not known to the adversary. That is to say our scheme is secure in the presence of an eavesdropper. One may think that sending a simple *fail* message whenever authentication fails could solve the privacy issue in EPS-AKA. This approach is not suitable for our scheme since the MME and HSS process further EPS-AKA protocol on the basis of the type of the failure message. Therefore, indicating the type of failure and hiding its type are essential to protect users' privacy.

4 Security and Efficiency Analysis

4.1 Security

To show that our proposed scheme preserves a subscriber's location information, we prove that authentication failure messages observationally equal in the

presence of an adversary. If observational equivalence of messages is satisfied, it is not possible for an attacker to achieve a subscriber's location information.

We use ProVerif [21] tool to verify the privacy property of the proposed scheme in terms of strong unlinkability [22]. Unlinkability of two messages means that, from an attacker's perspective, both messages no more and no less related after his observation compared to his background knowledge [23]. By the definition of strong unlinkability property [24], we model the verification scenario as follows. First an ME initiates a connection to a network several times. Meanwhile, the other ME initiates a connection once. In this situation, strong unlinkability guarantees that any adversaries cannot distinguish both connections made up by two MEs. The result of verification using ProVerif is shown in table 1.

Table 1. Unlinkability Analysis using ProVerif

	EPS-AKA	Modified EPS-AKA
Unlinkability	No	Yes

Unlike the original one, the proposed scheme achieves strong unlinkability property. That is, an adversary cannot track the origin of the encrypted authentication failure message. This shows that a subscriber's location information is preserved. Due to the space constraints, we omit the detailed experiment using ProVerif. More rigorous security analysis can be found in the full paper.

4.2 Efficiency

Communication Overhead. We first show that how efficient the modified EPS-AKA compared to the fixed 3G-AKA in terms of communication. The result is shown in table 2.

Table 2. Communication Overhead

	3G-AKA	EPS-AKA	Fixed 3G-AKA	Modified EPS-AKA
Length of a Message	L_{fail}	L_{fail}	$L_{fail} + L_{IMSI} + L_{RAND} + L_{rn} + L_{fail}$ $L_{rand} + L_{synch} +$ $L_{SQN} + L_{rn}$	

We first denote the length of x as L_x . For example, L_{IMSI} points to the length of IMSI. In case of 3G-AKA, one of two types of fail messages is sent without encryption. On the other hand, the fixed 3G-AKA takes six parameters to encrypt, and send it. The encrypted message can be expanded since it uses a public key encryption scheme. This can cause an increase of communication overhead. Meanwhile, in EPS-AKA, an ME sends either a failure message without encryption. The modified EPS-AKA maximize efficiency by diminishing the number of parameters and adopting a symmetric encryption scheme. We, therefore, minimize communication overhead.

Computation Overhead. In this section, we analyze computation overhead of each scheme. The result is shown in table 3.

Table 3. Computation Overhead

	3G-AKA	EPS-AKA	Fixed 3G-AKA	Modified EPS-AKA
Encryption per AKA	$5H$	$6H$	$6H + Enc_{pub} + Enc_{sym}$	$7H + Enc_{sym}$
Decryption per AKA	$5H$	$6H$	$6H + Dec_{pub} + Dec_{sym}$	$7H + Dec_{sym}$

We denote each of encryption, decryption, and pseudo-random function as follows:

- Symmetric key encryption(Enc_{sym}) / decryption(Dec_{sym}).
- Public key encryption(Enc_{pub}) / decryption(Dec_{pub}).
- Pseudo-random function(H).

The modified EPS-AKA, however, do not use a public key encryption scheme due to its heavy computation process. Additionally, our scheme reduces the number of key generation by reordering the key generation procedure in USIM. We, therefore, minimize computation overhead in constructing the authentication procedure secure.

Storage Overhead. In this section, we analyze storage overhead. The result is shown in table 4, which shows the secret keys and parameters that each entity should store in each scheme.

Table 4. Storage Overhead on Mobile Device and Network

	3G-AKA	EPS-AKA
Mobile Device	AK,MAC,RES,CK,IK	AK,MAC,RES,CI,IK, K_{ASME}
Network	AK,MAC,RES,CK,IK	AK,MAC,RES,CK,IK, K_{ASME}
	Fixed 3G-AKA	Modified EPS-AKA
Mobile Device	UK,pbN,AK,MAC,RES,CK,IK,	SK,AK,MAC,RES,CK,IK, K_{ASME}
Network	UK,pvN,AK,MAC,RES,CK,IK	SK,AK,MAC,RES,CK,IK, K_{ASME}

In the fixed 3G-AKA, UK and pbN are both used in symmetric and public key encryption respectively. The network also needs to store UK and pvN to decrypt messages. Unlike this, the modified EPS-AKA stores SK only for encryption. This makes our scheme to minimize additional memory space. Considering both sides of a mobile device and a network operator, we designed it to be applicable with a minimal cost.

5 Conclusion

A mobile network operator collects and manages a subscriber's location information to provide seamless communication service. If a subscriber's location information is revealed to a malicious third party, then he will be under serious privacy attack. To prevent it, only a legitimate network should be able to trace the location of a subscriber.

We showed that the current EPS-AKA protocol is vulnerable to such an attack by just eavesdropping messages on the air between a subscriber and a network. By capturing and replaying messages, he can know the existence of a certain ME in his observation area. To keep one's privacy intact, we proposed a modified EPS-AKA protocol which encrypts any messages. Every time a message is encrypted, a new random number is added so that an adversary cannot distinguish any encrypted messages. Our proposed scheme achieves strong unlinkability property by encrypting authentication failure messages randomly.

Acknowledgment. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2012R1A1A1001835 and 2013R1A2A2A01005559).

References

1. Kim, M., Kang, C., Kim, Y., Kim, W.: WiBroWiMAX LTE Mobile Broadband. Kwangmoonkag, Seoul (2011)
2. Varshney, U.: Location Management for Mobile Commerce Applications in Wireless Internet Environment. *ACM Transactions on Internet Technology* 3, 4–6 (2003)
3. Park, J., Kim, H., Joo, Y., Pyeun, S., Lim, J.: Lte New World. Miraebook, Seoul (2012)
4. Køien, G.M., Oleshchuk, V.A.: Location privacy for cellular systems; analysis and solution. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 40–58. Springer, Heidelberg (2006)
5. Meyer, U., Wetzel, S.: A man-in-the-middle attack on UMTS. In: 3rd ACM Workshop on Wireless Security, WiSe 2004, pp. 90–91. ACM DL, Philadelphia (2004)
6. Xiehua, L., Yongjun, W.: Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network. In: 7th International Conference on Wireless Communications Networking and Mobile Computing, pp. 1–3. IEEE, Wuhan (2011)
7. 3GPP: Universal Mobile Telecommunications System(UMTS); USIM and IC card requirements. Technical report, 3GPP (2008)
8. Dahlman, E., Parkvall, S., Skold, J., Beming, P.: 3G Evolution: HSPA and LTE for Mobile Broadband. Academic Press, Waltham (2010)
9. The LTE Network Architecture — Strategic White Paper, <http://www.alcatel-lucent.com>
10. 3GPP: Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application. Technical report, 3GPP (2012)
11. Gueron, S., Johnson, S., Walker, J.: SHA-512/256. In: 8th Conference on Information Technology New Generations, pp. 2–6. IEEE Computer Society Press, Las Vegas (2011)

12. 3GPP: Technical Specification Group Services and System Aspects; 3G Security; Cryptographic algorithm requirements. Technical report, 3GPP (2009)
13. 3GPP: Network Access Security in Next-Generation 3GPP Systems: A Tutorial. Technical report. IEEE Communications Magazine (2009)
14. Bortolozzo, M., Centenaro, M., Focardi, R., Steel, G.: Attacking and fixing PKCS#11 security tokens. In: 17th ACM Conference on Computer and Communications Security, pp. 1–3. ACM Press, Chicago (2010)
15. Golde, N., Redon, K., Borgaonkar, R.: Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In: 19th Annual Network and Distributed System Security Symposium, pp. 2–4. NDSS, San Diego (2012)
16. Arpinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., Borgaonkar, R.: New Privacy Issues in Mobile Telephony: Fix and Verification. In: 19th ACM Conference on Computer and Communications Security, pp. 4–10. ACM Press, Raleigh (2012)
17. Forsberg, D., Horn, G., Moeller, W., Niemi, V.: LTE Security. John Wiley and Sons, New Jersey (2012)
18. 3GPP: Universal Mobile Telecommunications System(UMTS); 3G Security; Security architecture. Technical report, 3GPP (2010)
19. Agilent Technologies: LTE and the Evolution to 4G Wireless: Design and Measurement Challenges. WILEY, Hoboken (2013)
20. Zugenmaier, A., Aono, H.: Security Technology for SAE/LTE. NTT DOCOMO Technical Journal 11(3), 28–30 (2009)
21. Cheval, V., Blanchet, B.: Proving More Observational Equivalences with ProVerif. In: 2nd Conference on Principles of Security and Trust, pp. 9–17. ETAPS, Rome (2013)
22. Arpinis, M., Chothia, T., Ritter, E., Ryan, M.: Analysing Unlinkability and Anonymity Using the Applied Pi Calculus. In: 23rd Computer Security Foundations Symposium, pp. 8–9. IEEE Press, Edinburgh (2010)
23. Pfitzmann, A., Kohntopp, M.: Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: International Workshop on Design Issues in Anonymity and Unobservability, pp. 8–9. ACM DL, Berkeley (2001)
24. Ryan, M., Smyth, B.: Applied pi calculus. In: Formal Models and Techniques for Analyzing Security Protocols. IOS Press, Amsterdam (2011)
25. Lai, C., Li, H., Lu, R., Shen, X.: SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. The International Journal of Computer and Telecommunications Networking 57, 2–9 (2013)
26. Ta, T., Baras, J.S.: Enhancing Privacy in LTE Paging System using Physical Layer Identification. In: Di Pietro, R., Herranz, J., Damiani, E., State, R. (eds.) DPM 2012 and SETOP 2012. LNCS, vol. 7731, pp. 15–28. Springer, Heidelberg (2013)

Enabling Smartphone Based HD Video Chats by Cooperative Transmissions in CRNs

Tao Jing¹, Xuewei Cui¹, Wei Cheng², Shixiang Zhu¹, and Yan Huo¹

¹ School of Electronics and Information Engineering, Beijing Jiaotong University, China

² Department of Computer Science, Virginia Commonwealth University, USA

Abstract. Smartphones have been equipped with the cameras that can shoot HD videos, and the video chat apps such as Skype are becoming popular. We can, therefore, intuitively predict the trend that users are expecting to enjoy HD video chats via utilizing their smartphones. Most of the current Internet services, however, cannot support the live HD video transmissions because of their low uplink rate. In order to overcome this limit, we propose to offload the uplink transmissions to cooperative users via Cognitive Radio Networks. Specifically, we first divide the video stream into several substreams according to the H.264/SVC standard and the cooperative users' uplink rates. Then, the cooperative users are selected by employing our proposed optimal multiple stopping method. Finally, the substreams are assigned to the selected cooperative users by a 0-1 Knapsack based allocation algorithm. The simulation results demonstrate that our proposed scheme can successfully support 720P HD video chats.

Keywords: HD video chat, cooperative relay selection, optimal multiple stopping theory.

1 Introduction

High-Definition cameras are currently available on popular smartphones. These cameras have been physically ready to support HD video shootings (such as 720P and 1080P). According to [8], 720P and 1080P video require the transmission speeds of 6Mbps and 12Mbps, respectively. However, most of the popular Internet services are mainly optimized for downlink transmission. The uplink transmission rate supported by most popular Internet access networks is only 2Mbps, and the typical upload speed on 3G/4G approximately ranges from 0.45Mbps to 1.93Mbps [1]. As a result, a single user's Internet upload speed is generally not enough to support live HD video transmission. Therefore, an open problem is how could users enjoy the HD video chats without upgrading their Internet services, which maybe too expensive and/or not necessary for other applications.

In order to enable the smartphone based HD video chat, we propose to utilize cooperative users to help with the uplink transmission in cognitive radio networks (CRNs). The challenge of this task is how to efficiently select appropriate CR relays for cooperative uplink transmission as the *realtime* requirement of video chat is very strong. In other works, the sender does not have enough time to look at all the candidate relays to select the best subset for the transmission. The sender has to do quick decisions

on relay selection while guaranteeing the HD video transmission with a reasonable low cost. Therefore, our objective is to design an efficient relay selection method, which can support HD video chat with the lowest cost, and a load assignment method, which can optimally distribute the video data among the selected relays. Specifically, the major work and the contributions can be summarized as the followings:

- we propose a scheme to support smartphone based HD video chat without upgrading the user's internet service by utilizing the cooperative CR users' uplink resource. Simulations verify that our proposed scheme can successfully support 720P HD video chat.
- Intuitively, the selected relays can use more time to forward packets if the relay selection time can be reduced. According to the requirement of HD video transmission rate and the cooperative CR users' uplink rate, given a number of time slots, we analyze the relationship between the relay selection time and the relay forwarding time so that the requirement can be satisfied.
- To the best of our knowledge, this is the first work to formulate an optimal multiple stopping model to solve the problem of relay selection for supporting HD video chat via cooperative transmission. We derive the multiple optimal stopping rules by jointly considering the instantaneous reward (of selected relays) and the expected sum reward (of the unobserved candidate relays). The proposed selection method can select the relays. Whose instantaneous reward is at least the same as the expected sum reward.
- Extensive simulations have been conducted to investigate the impact of the parameters on the performance of the proposed scheme.

The rest of this paper is organized as follows. The most related work is summarized in Sec. 2. The overview of H.264/SVC, the network model, and the adopted relaying framework are illustrated in Sec. 3. Sec. 4 introduces our optimal stopping policy based cooperative relay selection scheme and the packets assignment algorithm. The results of performance evaluation are reported in Sec. 5. The paper is concluded in Sec. 6.

2 Related Work

In recent years, researchers have shown a great interest in HD video technology. [10] studies Video-conferencing system for home. [13] studies and compares mechanisms and performance of the existing video conference systems. [14] introduces a HD video broadcasting scheme by using scalable video coding so that the devices under various network environments can obtain the video with different resolutions. All of these work are studied under ideal network situations. However, for smartphone users, their uplink rate is generally not enough for HD transmission.

Several current video coding standards such as H.264/AVC, Dirac, AVS China and VC-1 are introduced in [15]. [17] provides the comparison of the coding efficiency for these video coding standards. [16] gives an detailed overview of the scalable video coding extension of the H.264/AVC standard. In our work, we consider H.264/SVC as the coding standard utilized by HD video chat app.

An overview of existing cooperative relaying selection schemes is provided in [5–7, 11]. They require channel-related information from all the candidate relay nodes,

which is inefficient when the number of candidate relays is large or the time for relay selection is limited. For example, channel state information and SNR are required by the relay selection approaches proposed in [12] and [3] respectively. Moreover, [2] needs to compute the SNR thresholds for all candidate relays.

3 Preliminaries

3.1 System Model

We consider a simple time-slotted cooperative transmission model depicted in Fig.1 which consists of a pair of primary users and a number of secondary users. To implement a HD video chat, a PU transmitter, denoted by P_t , transmits its HD video stream to a primary receiver, denoted by P_r , with the assistance of multiple cooperative users. The n secondary users, represented by S_i , $i=1, 2, \dots, n$, which have the ability to help transmit packets for the primary system are called *candidate relays*. When P_t needs to transmit packets to P_r , m free secondary users, which have favorable channel condition, can be selected as relay nodes by the PU transmitter. The m secondary users finally selected by the PU transmitter are called *cooperative relays*. In this paper, we adopt AF to illustrate our designs [18].

It is assumed that the multiple cooperative relay selection is performed at each time slot. The duration of a time slot is $T = \frac{D_{HD}}{R_{HD}}$, where D_{HD} represents the amount of the packets to be transmit for HD video, R_{HD} represents the required transmission rate for HD video. As illustrated in Fig. 2, each time slot T is partitioned into three components T_S , T_{sr} , T_{rd} . Let τ be the time needed for observing a candidate relay. We assume that τ is identical for different SUs and for different time slots. Denoted by $S = \{s_1, s_2, \dots, s_n\}$ an observation order/sequence, which is a permutation of the SU candidate relays index set $\{1, 2, \dots, n\}$. At the beginning of a time slot, P_t starts to observe the SU candidate relay nodes sequentially according to the observation sequence. If the reward of the k^{th} observation satisfies a specific criterion, P_t stops at the k^{th} SU candidate relay node, and then continues to observe candidate relay nodes for the following stops. The whole observation ends after P_t stops m times. T_S represents the time of selecting relays in each time slot. After the cooperative relay selection process,

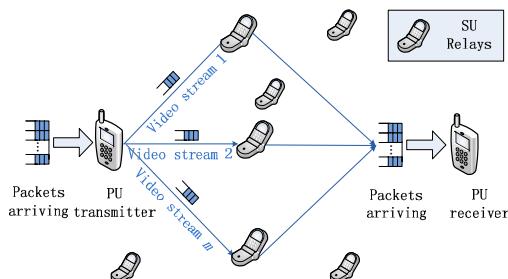


Fig. 1. Cooperative Transmission Model

P_t transmits packets to relay node i in T_i . The total time for transmission between PU transmitter and the relay nodes is denoted by T_{sr} , which is the sum of T_1, T_2, \dots, T_m . Then the m cooperative relays forward the video stream packets to P_r simultaneously in T_{rd} .

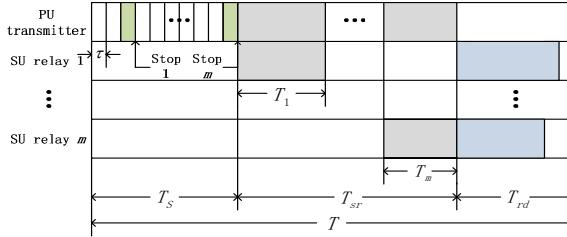


Fig. 2. The Time Slot Structure

From Fig.2 we can see that $T = T_s + T_{sr} + T_{rd}$. $T_{sr} = \frac{D_{HD}}{R_{sr}}$, where R_{sr} represents the transmit rate between the PU transmitter and the cooperative relay node. Then we can get $T_s + T_{rd} = T - T_{sr} = \frac{D_{HD}}{R_{HD}} - \frac{D_{HD}}{R_{sr}} = T^*$. Then we calculate the estimated value of T_{rd} . During T_{rd} , the cooperative relays forward the video packets to the PU receiver simultaneously. When there are m relays forwarding packets, the estimated value of T_{rd} is given by $T_{rd}^* = \frac{D_{HD}}{mR_{rd}^*}$, where R_{rd}^* denotes the expected rate of a relay node in a flat Rayleigh fading channel. Since the condition that observation time T_s is larger than zero should be satisfied, we estimate the value of m as $m^* = \min\{m | T^* - T_{rd}^* > 0\}$. Then we can get the estimated observation time $T_s^* = T^* - T_{rd}^*$ and the size of observation sequence $n = \frac{T_s^*}{\tau}$.

4 Optimal Multiple Stopping Policy

4.1 Problem Formulation

In this paper, we formulate the cooperative transmission problem as multiple stopping problem in CRNs. In order to select m relays for cooperative transmission, the PU transmitter observes multiple SU candidate relays one by one in an observation sequence. After contacting with a candidate relay, the PU decides whether to make a stop to select the current relay as a cooperative relay. The observation comes to the end if the PU finishes selecting m relays.

When PU makes a decision, it considers the reward in the sum case. In other words, we assume the PU has selected l relays before observing i^{th} relay, if PU selects the current relay, we can get a sum reward denoted by $y_i + V_i^{m-l-1}$, where y_i represents the instantaneous reward of the i^{th} relay and V_i^{m-l-1} represents an expected reward of the $m-l-1$ relays to be selected from the remaining candidate relays; if PU does not select the current relay, we can get an expected sum reward of $m-l$ relays to be selected from the remaining candidate relays V_i^m . If the sum reward with selecting the current

relay is larger than the one without selecting the current relay, the PU makes a stop, and vice versa. The PU transmitter finally stops the observation till m cooperative relays are all selected. Note that no recall is allowed since the channel quality is changing rapidly in cognitive radio networks due to the complicated conditions such as the mobility of the users. Therefore, the multiple relay selection problem can be further formulated as a sequential decision problem which can be solved by the optimal multiple stopping theory.

In order to further investigate the channel quality in our cooperative relay selection problem, we assume that the underlying channel is a flat Rayleigh fading channel, in which the instantaneous interference-plus-noise ratio (SNR) is received by the destination with an exponential distribution having a probability density function (PDF) $f(\gamma) = \frac{1}{\bar{\gamma}}e^{-\frac{\gamma}{\bar{\gamma}}}$, where $\bar{\gamma}$ denotes the average SNR in the channel model. Then we can model the Rayleigh fading channel as a finite state Markov chain (FSMC) as proposed in [15]. In the FSMC we partition the SNR into U intervals and then divide SNR into a finite-state space. Thus the SNR thresholds are denoted by $\mathcal{T} = \{\gamma_1 = 0, \gamma_2, \dots, \gamma_U, \gamma_{U+1} = \infty\}$. If an instantaneous SNR Γ is in $[\gamma_u, \gamma_{u+1})$, the channel of the SU candidate relay is said to be in state u . When the PU pair observes the channel of the candidate relay, the probability of the SU being in state s_u for the channel can be given by

$$q_u = \int_{\gamma_u}^{\gamma_{u+1}} f(\gamma) d\gamma = e^{-\frac{\gamma_u}{\bar{\gamma}}} - e^{-\frac{\gamma_{u+1}}{\bar{\gamma}}}, u = 1, \dots, U \quad (1)$$

In our cooperative transmission problem, the achievable transmission rate is viewed as a metric for the channel quality in wireless communications. Let r_k denote the achievable transmission rate between the PU pair and the SU candidate relay node k . According to the Shannon's theorem, r_k is calculated as follows:

$$r_k = W \log(1 + \gamma_k) \quad (2)$$

where W denotes the bandwidth of the spectrum. Thus, the corresponding date rate, denoted as $R = \{r_1, r_2, \dots, r_U\}$, can also model the transmission rate as a discrete random variable, which has a same distribution as the channel state

$$\Pr\{R = r_u\} = q_u, u = 1, 2, \dots, U \quad (3)$$

The PU pair acquires the achievable transmission rate of the channel between itself and the SU candidate relay by executing the observation in relay selection. The process of observation is similar to the RTS/CTS access mechanism designed for the 802.11 technique [4]. At each observation step, the PU transmitter sends a RTS (Request-To-Send) frame to the candidate relay. Upon receiving of a RTS frame, the candidate relay returns a CTS (Clear-To-Send) frame, which includes the information for calculating the achievable rate. We define $X_k = R_k$ as the valid transmission rate of the k^{th} observation step. Then the distribution of X_k can be calculated as follows:

$$p_u = \Pr\{X_k = x_u = r_u\} = q_u, \text{ for } 1 \leq u \leq U, 1 \leq k \leq n \quad (4)$$

Then we derive the instantaneous reward function denoted by Y_k based on the the valid transmission rate and the number of observation steps. First, we denote c_k as a

scaling factor if the PU pair stops at the k^{th} observed candidate relay node, which is given by

$$c_k = 1 - \frac{k\tau}{T} \quad (5)$$

From (5), we can see that the larger the value of k , the smaller the value of c_k . In other words, the greater the number of SU candidate relay nodes the PU transmitter observes, the lower the efficiency of the cooperative relay selection process.

We denote d_l as another scaling factor if the PU Pair has selected l SU relay nodes.

$$d_l = 1 - \frac{m-l}{m^\sigma} \quad (6)$$

Where m denotes the stopping times for the whole observation and l denotes the times we have stopped. From (6), we can see that the larger the value of σ , the larger the value of d_l . Namely, the more relays the PU transmitter has selected, the less stops remained, so the efficiency of the cooperative relay selection process becomes higher to some extent.

Therefore, the payoff after the k^{th} observation attempt with having stopped l times is given by

$$Y_k = c_k d_l X_k \quad (7)$$

4.2 Optimal Multiple Stopping Rule

In this subsection, we solve the multiple stopping problem in the sum case by deriving the optimality equations.

For the finite payoff reward sequence Y_1, \dots, Y_n that are independent and identically distributed as depicted in 4.1, the optimality equations can be stated as follows for the m -stopping problem.

We denote F_i as the probability distribution function of the instantaneous reward Y_i after the i^{th} observation. We derive the sum reward sequence by backwards induction for $i = n-m, \dots, 0$ as follows:

$$V_{n-m+1}^m := -\infty \quad (8)$$

$$V_i^0 := 0 \quad (9)$$

$$V_i^m := E[(Y_{i+1} + V_{i+1}^{m-1}) \vee V_{i+1}^m | F_i] \quad (10)$$

where V_i^m represents the expected sum reward of continue observing for m stopping times after i^{th} observation, \vee denotes the maximum.

From (10), we know that V_{i+1}^{m-1} and V_{i+1}^m can be calculated by backwards induction. We compute V_i^m as follows:

$$\begin{aligned} V_i^m &= E[(Y_{i+1} + V_{i+1}^{m-1}) \vee V_{i+1}^m | F_i] \\ &= E[(c_{i+1} d_l X_{i+1} + V_{i+1}^{m-1}) \vee V_{i+1}^m | F_i] \\ &= \sum_{\alpha} (c_{i+1} d_l x_{\alpha} + V_{i+1}^{m-1}) p_{\alpha} + \sum_{\beta} V_{i+1}^m p_{\beta} \end{aligned} \quad (11)$$

where $\alpha \in \{k \mid c_{i+1}d_lx_k + V_{i+1}^{m-1} > V_{i+1}^m, k = 0, 1, 2, \dots, U\}$, $\beta \in \{k \mid c_{i+1}d_lx_k + V_{i+1}^{m-1} \leq V_{i+1}^m, k = 0, 1, 2, \dots, U\}$, subject to

$$\begin{cases} 0 \leq \alpha \leq U \\ 0 \leq \beta \leq U \\ \alpha + \beta = U \end{cases} \quad (12)$$

Then we can get the sum reward function:

$$z_i^l(x_1, x_2, \dots, x_i) = y_i(x_1, x_2, \dots, x_i) + V_i^{m-l} \quad (13)$$

Where $y_i(x_1, x_2, \dots, x_i)$ denotes the instantaneous reward after the i^{th} observation. It is optimal to stop if $z_i^l(x_1, x_2, \dots, x_i)$ is larger than V_i^{m-l+1} and otherwise.

Then we define the corresponding threshold stopping times $T_l^m(k)$ for $1 \leq m \leq n$, $0 \leq k \leq n - m$ by

$$\begin{aligned} T_1^m(k) := \min \{ &k < i \leq n - m + 1 \\ &| z_i^l(x_1, x_2, \dots, x_i) > V_i^m \} \end{aligned} \quad (14)$$

Algorithm 4.2. The Optimal Multiple Stopping Rule

```

1: Construct the observation sequence  $S = \{s_1, s_2, \dots, s_n\}$ ;
2: Decide the value of  $m$ ;
3: Let  $S_a$  and  $l$  denote the set and the number of cooperative relay nodes that have
   been selected,  $S_a \leftarrow \emptyset$ ,  $l \leftarrow 0$ ;
4: for  $i \leftarrow 1$  to  $n - m$  do
5:   if  $m - l = n - i + 1$  then
6:     Select  $S_a \cup \{s_i, s_{i+1}, \dots, s_n\}$  as the output;
7:     Break;
8:   else
9:     Compute the instantaneous reward  $y_i$  given by (7) after obtaining the achiev-
       able transmission rate  $r_i$  by observing the  $i^{th}$  relay;
10:    Compute the sum reward  $z_i^l$  given by (13).
11:    Compute the expected sum reward  $V_i^{m-l+1}$  given by (11);
12:    if  $z_i^l < V_i^{m-l+1}$  then
13:      Continue;
14:    else
15:      Stop at the current step and select the  $i^{th}$  SU node as one of the cooperative
         relays,  $S_a \leftarrow S_a \cup s_i$ ,  $l \leftarrow l + 1$ ;
16:      if  $l < m$  then
17:        Continue;
18:      else
19:        Break;
20:      end if
21:    end if
22:  end if
23: end for

```

$$\begin{aligned} T_l^m(k) &:= \min\{T_{l-1}^m(k) < i \leq n - m + l \\ |z_i^l(x_1, x_2, \dots, x_i) > V_i^{m-l+1}\}, 2 \leq m \leq n. \end{aligned} \quad (15)$$

We propose the optimal multiple stopping rule in Algorithm 4.2.

4.3 Video Frames Allocation Algorithm

Since different cooperative relay nodes have disparate transmission rates, we hope to maximize the transmission amount of each relay under a certain rate limit for saving energy. In this subsection, we intend to find an optimal video frames allocation algorithm by formulating it as 0-1 Knapsack problem [9]. The PU video source encoder divides the video stream into a base sub-stream and M enhancement stream. Let $D = \{D_1, D_2, \dots, D_M\}$ denote the set of divided packets, where D_k ($k = 1, 2, \dots, M$) represents the amount of a specific video packet. Then we allocate the packets to the selected cooperative relays one by one in descending order of their transmission rates. For the i^{th} cooperative relay s_i , we denote set $D^i = \{D_1^i, D_2^i, \dots, D_{M_i}^i\}$ as the set of amount of packets that has not been allocated.

Then we formulate the video frames allocated problem. We have got m cooperative relays with the rate $\{r_1, r_2, \dots, r_m\}$ for forwarding packets to the PU receiver. Let A_i , $i = 1, 2, \dots, m$, denote the available transmission amount of relay s_i , which is defined as the amount of packets that can be forwarded by s_i . In T_{rd} , the amount of packets relay s_i can forward is $r_i \cdot T_{rd}$. Therefore, we obtain $A_i = r_i \cdot T_{rd}$. Then we define an available transmission amount of vector A as $A = \{A_1, A_2, \dots, A_m\}$.

In our allocation model, we take the $D^i = \{D_1^i, D_2^i, \dots, D_{M_i}^i\}$ as both the weigh and value for items of base layer and enhancement layers. Set $A = \{A_1, A_2, \dots, A_m\}$ is regarded as the given limits. In 0-1 Knapsack problem, the weigh and limit should be integers, so we construct other integer sets $D^{i*} = \{D_1^{i*}, D_2^{i*}, \dots, D_{M_i}^{i*}\}$ and $A^* = \{A_1^*, A_2^*, \dots, A_m^*\}$. Where $D_k^{i*} = \lfloor D_k^i \rfloor + 1$ and $A_i^* = \lceil A_i \rceil$. Here, $\lfloor \cdot \rfloor$ represents the integral function. Note that after the allocation for a relay, the set D^{i*} changes regularly.

The objective of our allocation is to determine the subset $Q_i \subseteq \{1, 2, \dots, M_i\}$ that

$$\max \sum_{t \in Q_i} D_t^{i*}, \text{ subject to } \sum_{t \in Q_i} D_t^{i*} \leq A_i^*. \quad (16)$$

For $1 \leq k \leq M_i$, $0 \leq r \leq A_i^*$, we set

$$G(0, r) = 0, \quad G(k, 0) = 0 \quad (17)$$

$$\text{if } D_k^{i*} > r, \quad G(k, r) = G(k - 1, r) \quad (18)$$

$$\text{if } D_k^{i*} \leq r, \quad G(k, r) = \max\{D_k^{i*} + G(k - 1, r - D_k^{i*}); G(k - 1, r)\} \quad (19)$$

From (18) and (19), we can see that there are only two choices to compute $G(k, r)$:
(i)Leave D_k^{i*} : the largest amount relay i can forward from $\{D_1^{i*}, D_2^{i*}, \dots, D_{M_i}^{i*}\}$ with

limit r is $G(k-1, r)$; (ii)Take D_k^{i*} (only possible if $D_k^{i*} \leq r$): then we gain D_k^{i*} of transmission amount and the largest amount the relay can transmit from $\{D_1^{i*}, D_2^{i*}, \dots, D_{M_i}^{i*}\}$ with rate limit $r - D_k^{i*}$ is $G(k-1, r - D_k^{i*})$. Totally, we get $D_k^{i*} + G(k-1)$.

To allocate packets for relay i , we first do the bottom-up computation using iteration by (18) and (19), then we can get the set Q_i . The video frames allocation algorithm which is based on Knapsack problem is depicted in Algorithm 4.3.

Algorithm 4.3. Video Stream Allocation

```

1: Construct the not-increasing sequence of the rate limit  $A = \{A_1, A_2, \dots, A_m\}$ 
   and evolve it to a not-increasing integer sequence  $A^* = \{A_1^*, A_2^*, \dots, A_m^*\}$ .
2: Construct the set of weigh and value  $D^i = \{D_1^i, D_2^i, \dots, D_{M_i}^i\}$  and its integer set
    $D^{i*} = \{D_1^{i*}, D_2^{i*}, \dots, D_{M_i}^{i*}\}$ .
3: for  $i \leftarrow 1$  to  $m$  do
4:   if  $D^{i*} \neq \emptyset$  then
5:     for  $r \leftarrow 0$  to  $A_i^*$  do
6:        $G(0, r) \leftarrow 0$  ;
7:     end for
8:     for  $k \leftarrow 1$  to  $M_i$  do
9:        $G(k, 0) \leftarrow 0$  ;
10:    end for
11:   Compute the bottom-up computation table;
12:   Derive set  $Q_i$ ;
13:   else
14:     break;
15:   end if
16: end for

```

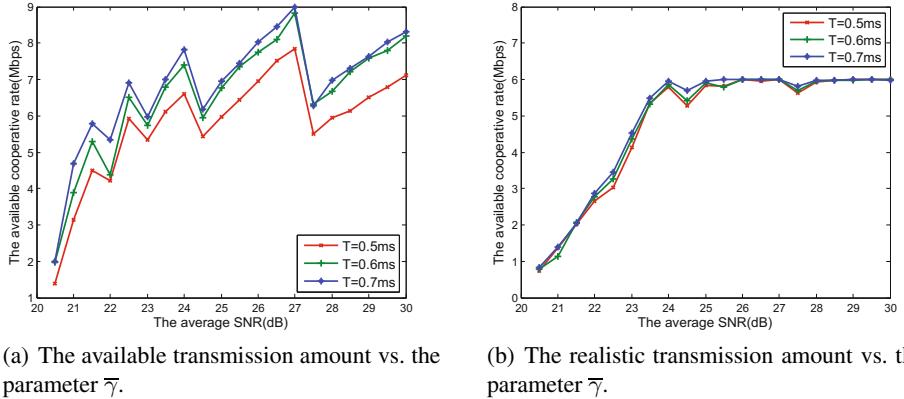
5 Performance Evaluation

In this section we evaluate the performance of our cooperative HD video transmission scheme by conducting extensive simulation study. The video stream is divided into five parts: one base layer substream and four pieces of enhancement layer substream. It is assumed that the transmission rate r_k of the k^{th} SU candidate relay node does not change within one slot. We divide the finite-state space of SNR received by the receiver into $U = 30$ intervals. The bandwidth W is set to be 1 MHz. The rate of PU source is set to be the average rate of channel. The controlling factor σ is set to be 50. We set the transmission rate for 720P HD video to be 6Mbps. The numerical results reported in this section are run at an averaged over 100 times.

To provide a deep insight into the feasibility of our cooperative HD video transmission scheme, we study the impact of the average SNR $\bar{\gamma}$ and the observation duration τ on the transmission performance.

5.1 The Impact of the Parameter $\bar{\gamma}$

In this subsection, we investigate the impact of the parameter $\bar{\gamma}$ on available cooperative transmission rate and realistic cooperative transmission rate under the situation where



(a) The available transmission amount vs. the parameter $\bar{\gamma}$.

(b) The realistic transmission amount vs. the parameter $\bar{\gamma}$.

Fig. 3. The impact of The parameter $\bar{\gamma}$

the average SNR $\bar{\gamma}$ changes regularly. We set the observation duration τ to be $3\mu s$. The transmission time T is set to be 0.5ms, 0.6ms and 0.7ms.

From Fig. 3(a), we can see that the available cooperative transmission rate increases with rising average SNR. Actually, the higher average SNR results in the larger number of candidate relays when the number of cooperative relays remains unchanged. With the number of candidate relays increases, the PU transmitter has higher probability to choice relays with better performance. Therefore, the available cooperative transmission rate increases. Similar results can be obtained in Fig. 3(b). With the increasing of $\bar{\gamma}$, the realistic cooperative transmission rate increases and then keep stable state that can satisfy the transmission rate for 720P HD video.

5.2 The Impact of Observation Duration τ

In this subsection, we investigate the impact of observation duration τ on the length of observation steps and available cooperative transmission rate. We set the average SNR $\bar{\gamma}$ to be 28 dB, 29 dB and 30 dB.

From Fig. 4(a), we can see that the length of observation steps decreases slowly with the observation duration τ increases regularly. In other words, the larger the τ , the smaller the number of observation steps. This is because the value of τ represents the cost of observing one SU candidate relay, the PU needs to stop observing as soon as possible to avoid generating a large cost. On the contrary, when the value of τ is small, the cost for observation is low, the PU tends to observe more candidate relays to find better cooperative relays. We also can see that different $\bar{\gamma}$ impacts the length of observation. The larger the $\bar{\gamma}$ is, the larger the number of candidate relays is, so we tend to observe more relays before transmission, which leads to a larger length of observation steps.

We can see from Fig. 4(b) that the available cooperative transmission rate declines slowly with the increasing of the time duration for each observation τ . The relationship can be obtained in Section 4.2, when τ increases, the expected sum reward decreases,

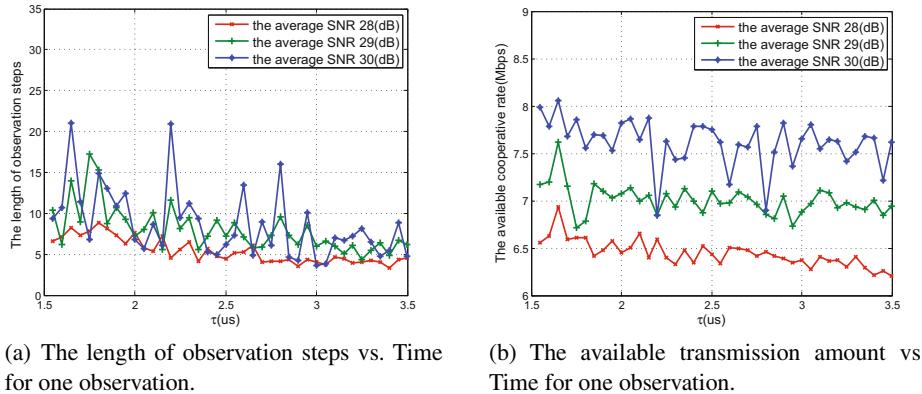


Fig. 4. The impact of observation duration τ

so the performance of selected relays decreases, which leads to a lower available cooperative transmission rate. On the other hand, the cost increases with the τ increases, so the PU is eager to find cooperative relays, which also leads to performance degradation of selected relays. Therefore, the available cooperative transmission rate declines. Similarly, different $\bar{\gamma}$ impacts the available transmission rate, which is explained in 5.1 for Fig. 3(a).

6 Conclusion

In this paper, we propose an optimal multiple stopping scheme to solve the problem of multiple cooperative relay selection for supporting smartphone based HD video chat in CRNs. In the proposed scheme, the video source selects the candidate CR relays by following a proposed optimal multiple stopping rule to guarantee the success of HD video chat. The proposed scheme has been verified to be able to support 720P video chat via simulations. In the future, we will implement the proposed scheme on android smartphones.

Acknowledgment. The paper is partially supported by the National Natural Science Foundation of China (Grant No. 61272503, 61272505 and 61172074) and the National Science Foundation of US (CNS-1265311).

References

1. 3g/4g performance map: Data speeds for at & t sprint, t-mobile, and verizon, http://www.techhive.com/article/254888/3g_4g_performance_map_data_speeds_for_atandt_sprint_t_mobile_and_verizon.html
2. Amarasuriya, G., Ardakani, M.: Adaptive multiple relay selection scheme for cooperative wireless networks. In: Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE (2010)

3. Amarasuriya, G., Ardkani, M., Tellambura, C.: Adaptive multiple relay selection scheme for cooperative wireless networks. In: Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE (2010)
4. Bianchi, G.: Performance analysis of the ieee 802.11 distributed coordination function. IEEE Journal on Selected Areas in Communications 18(3), 535–547 (2000)
5. Cai, Z., Ji, S., He, J., Bourgeois, A.: Optimal distributed data collection for asynchronous cognitive radio networks. In: 2012 IEEE 32nd International Conference on Distributed Computing Systems (ICDCS), pp. 245–254 (June 2012)
6. Cai, Z., Ji, S., He, J.S., Wei, L., Bourgeois, A.G.: Distributed and asynchronous data collection in cognitive radio networks with fairness consideration. IEEE Transactions on Parallel and Distributed Systems 99, 1 (2013)
7. Elmenreich, W., Marchenko, N., Adam, H., Hofbauer, C., Brandner, G., Bettstetter, C., Hueemer, M.: Building blocks of cooperative relaying in wireless systems. Elektrotechnik und Informationstechnik 125, 353–359 (2008), doi:10.1007/s00502-008-0571-7
8. Gonzalez, B.: All about internet speed requirements for hulu, netflix, and vudu movie viewing,
<http://hometheater.about.com/od/internethometheater2/a/Internet-Speed-for-Netflix-Vudu.htm>
9. Hristakeva, M., Shrestha, D.: Different approaches to solve the 0/1 knapsack problem (2004)
10. Jansen, J., Cesar, P., Bulterman, D.C., Stevens, T., Kegel, I., Issing, J.: Enabling composition-based video-conferencing for the home. IEEE Transactions on Multimedia 13(5), 869–881 (2011)
11. Jing, T., Zhu, S., Li, H., Cheng, X., Huo, Y.: Cooperative relay selection in cognitive radio networks. In: IEEE INFOCOM Mini-Conference (2013)
12. Jing, Y., Jafarkhani, H.: Single and multiple relay selection schemes and their achievable diversity orders. IEEE Transactions on Wireless Communications 8(3), 1414–1423 (2009)
13. Lu, Y., Zhao, Y., Kuipers, F., Van Mieghem, P.: Measurement study of multi-party video conferencing. In: Crovella, M., Feeney, L.M., Rubenstein, D., Raghavan, S.V. (eds.) NETWORKING 2010. LNCS, vol. 6091, pp. 96–108. Springer, Heidelberg (2010)
14. Mirta, S., Schierl, T., Wiegand, T., Inigo, P., LeGuern, C., Moreau, C., Guarnieri, L., Tronc, J.: Hd video broadcasting using scalable video coding combined with dvb-s2 variable coding and modulation. In: Advanced Satellite Multimedia Systems Conference (Asma) and the 11th Signal Processing for Space Communications Workshop (Spsc), pp. 114–121 (2010)
15. Rao, K., et al.: Current video coding standards: H. 264/avc, dirac, avs china and vc-1. In: 42nd Southeastern Symposium on System Theory (SSST), pp. 1–8. IEEE (2010)
16. Schwarz, H., Marpe, D., Wiegand, T.: Overview of the scalable video coding extension of the h.264/avc standard. IEEE Transactions on Circuits and Systems for Video Technology 17(9), 1103–1120 (2007)
17. Schwarz, H., Sullivan, G., Tan, T., Wiegand, T.: Comparison of the coding efficiency of video coding standards – including high efficiency video coding, hevc (2012)
18. Su, W., Sadek, A.K., Liu, K.R.: Cooperative communication protocols in wireless networks: Performance analysis and optimum power allocation (2007)

A Transparent Correlation-Based Scheme for Energy Efficient Context Sensing and Fusion under Android Systems

Nicholas Capurso¹, Liran Ma¹, Tianyi Song², and Xiuzhen Cheng²

¹ Department of Computer Science, Texas Christian University,
Fort Worth, TX, USA

² Department of Computer Science, The George Washington University,
Washington, DC, USA

Abstract. A primary concern with modern smartphones is battery consumption. With so many different hardware components in modern smartphones, there are situations where certain components may be powered down or reduced in functionality without disrupting the user experience. We propose a transparent correlation-based scheme for energy efficient context sensing and fusion under Android systems. We experiment with the idea of disabling hardware functionality based on context. Our scheme focuses on inferring a user's location and subsequently disabling the GPS, which is considered to be one of the most energy-expensive components included in a smartphone. For example, when a user has connected to a Wi-Fi network with a known location, we disable GPS navigation and deliver the known location in its place. Based on our experiments, we conclude that this approach can significantly improve a device's battery life.

Keywords: Energy Efficiency, Android Systems, Context Sensing, GPS, Location, Wi-Fi.

1 Introduction

Modern smartphones are sophisticated enough that a GPS, a Wi-Fi and cellular radio, and a bank of sensors can all be packed onto the same device. As a result, one apparent issue that concerns all users is battery consumption. With so many different components, it is difficult for the average user to make the best decisions when it comes to saving power.

At many times, however, there are always certain components that can be safely powered down or reduced in functionality without disturbing the user's experience. For example, many users tend to leave Wi-Fi turned on, even when they are not using their phones. Thus, a simple solution would be to disable Wi-Fi while the phone is idle and the connection is not being utilized. It follows that similar logic can be applied to other smartphone components as well and overall, the battery life of a device would improve.

Typically, one of the most battery-intensive components on modern smartphones is the GPS. Today, applications that require location data pervade our

society. Social networking applications often attach location data to status updates, weather applications use location data to fetch an accurate forecast, and, of course, there are mapping and navigational applications. Any application that requires prolonged use of the GPS results in the battery draining rather quickly. Many users rely on the functionality of navigational applications, but pay the price of a lower battery life throughout the day. In addition, there are times where the GPS may be unavailable or unreliable, such as in a building or underground. Thus, a smartphone's GPS is one of the most practical components to develop an energy-efficient solution for.

Ideally, one would like to minimize power consumption without sacrificing the accuracy or functionality of the GPS. An efficient way of providing location services to a user while using the GPS sparingly is by inferring a user's location based on context. For example, consider a user connected to their Wi-Fi network while at home. Because of the range of a typical user's Wi-Fi network, it can be assumed that the user's location will not change while they remain connected to their network. As a result, if the location of the user's home is known, the GPS does not need to be employed while the device remains connected to the user's home network. This specific case may also apply to a user's workplace or learning institution.

We propose such a scheme that attempts to infer a user's location based on context and reduce the use of a smartphone's GPS. Our solution is designed to disable GPS functionality while connected to a known Wi-Fi network with a location that has been pre-defined. It is also designed to be as transparent as possible such that already existing applications need not be modified and leaves the user unaware of whether their location is being inferred or obtained by the GPS.

This solution may be expanded to work with virtually any Wi-Fi networks, as locations can be looked up using online services. Further improvements may be made by incorporating logic and relationships to disable other smartphone components. For example, if Wi-Fi is not being utilized and the accelerometer is used to determine that a smartphone is idle, Wi-Fi can be safely turned off. In combination with our solution for disabling the GPS, we expect this approach would have significant battery savings. This approach mirrors those taken in [1], [2], and [3] to adjust or disable the GPS based on sensor readings, such as the accelerometer. We also perform a similar test using the accelerometer in order to verify its effectiveness.

Our main contributions are as follows: i) Propose a scheme to infer a user's location based on context and reduce the use of a smartphone's GPS; ii) Develop a solution that disables GPS functionality once a user's location can be inferred from Wi-Fi connection information; iii) Implement our proposed solution into the Android operating system transparently such that existing application code does not need to be rewritten; iv) Confirm that our proposed solution results in significant battery savings.

The rest of the paper is organized as follows. Section 2 lists related work. Section 3 discusses our development environment, information on the Android

location framework, and relevant information about Wi-Fi. Section 4 gives the goals of our work and introduces our solution design. Section 5 discusses our testing environment and the results of our experiments. Finally, Section 6 concludes the paper.

2 Related Work

Reducing power consumption on mobile devices is an important and ongoing topic with many proposed approaches. Ideally, a solution should save energy while minimizing the harm done to the user experience. Proposed approaches include using middleware, trade-offs, minimizing GPS usage, or determining/inferred locations without the use of a GPS.

The development of middleware to reduce GPS power consumption is proposed by Zhuang, *et al.* in [4] and Nath in [5]. Zhuang, *et al.* proposes a middleware that uses context to determine whether it is more appropriate to invoke either a smartphone's GPS or a Wi-Fi/cellular location provider. Their solution also follows the idea of using low-power sensors to reduce unnecessary invocations of location services. In addition, they also dynamically adapt location sensing parameters according to a device's battery level and attempt to clump location requests together so as to increase the time interval between subsequent uses of the GPS. Nath proposes ACE, a middleware that defines context attributes (such as being at home, or jogging, etc) and relationships between them in order to derive their values efficiently. Energy efficiency is gained through attempting to use the least power-consuming components to derive an attribute. However, an issue that comes with middleware solutions, such as those proposed by Nath and Zhuang, *et al.*, is that existing applications must be modified to interface with the middleware.

Trading location accuracies for reduced power consumption is proposed by Lin, *et al.* in [6]. Their research recognizes that accuracy requirements may be relaxed based on context. Their work involves using various location sensors to determine locations based on energy cost and required accuracy.

Controlling a GPS to acquire or update a location when a device enters or leaves a region (crosses a boundary) is explored by Farrell, *et al.* in [7]. A similar concept is proposed by Paek, *et al.* in [2]. Their work focuses on controlling the GPS to only be turned on when accurate location readings may be obtained. This logic is based on the user's location, movement, and a user's history of visited locations and velocities obtained by a smartphone's sensors.

Attempting to minimize a device's power consumption based on a user's mobility is explored by You, *et al.* in [3] and by Kjærgaard, *et al.* in [1]. You, *et al.*'s research aims to adjust the rate at which the GPS is invoked to get a location fix (i.e., the sampling rate) based on a user's movements. Their research intends to reduce energy consumption of using location services and improve the location accuracy of mobile users. Kjærgaard, *et al.* proposes EnTracked, which also focuses on minimizing power consumption based on a user's mobility. EnTracked determines when to turn the GPS on or off and keeps track of whether the user is stationary or in motion.

The use of Wi-Fi to infer locations is researched by Youssef and Agrawala in [8]. Their work involves using Wi-Fi signal strength to track a user’s location. Finally, VTrack, a system developed by Thiagarajan, *et al.* in [9] uses Wi-Fi, instead of the GPS, to estimate a vehicle’s trajectory and travel time in the interest of reducing the amount of time that one spends in traffic.

Our work in this paper combines approaches to minimize GPS usage with inferring locations via Wi-Fi. As opposed to the middleware approach, where applications must be written to interface with the middleware, our solution is implemented transparently such that existing applications need not adapt to our modifications. We attempt to minimize GPS usage by disabling it when a user’s location can be inferred from Wi-Fi connection information.

3 Background

First, we discuss our development environment and the capabilities of our prototype device. Then, we explain and illustrate the data flow in the Android location framework. Finally, we describe the features of Wi-Fi that are relevant to our work.

3.1 Development Tools

The Android Open Source Project (AOSP) provides for an environment where we can study the GPS operation and integrate our solution into the operating system itself. We develop our solution for a custom Android firmware called Cyanogenmod (CM) [10]. CM adds on various features that are not present in stock Android and thus, also provides us with greater flexibility when developing our solution. Our solution is written in Java and is developed with the Eclipse IDE and the Android SDK [11].

Our prototype device is the Samsung Galaxy S4. The device currently runs Cyanogenmod 10.2 with Android version 4.3.1 (Jelly Bean). The technical specifications of the device are as follows: a 1.9 GHz quad-core processor, 2 GB of RAM, and 16 GB of storage [12]. The Android location framework [13] allows a user’s location to be derived from either the GPS or a network provider, such as Wi-Fi or the cellular network. However, our research focuses on the GPS as it typically consumes more power than the latter. The S4 also boasts a variety of hardware sensors, such as an accelerometer, which we may use in addition to Wi-Fi to make energy-saving decisions based on context. Finally, our prototype device lacks a SIM card, making cellular functions unavailable. As a result, power consumption is expected to be greater for a normal user’s device that has cellular functions enabled.

3.2 Android Location Framework and Operation

To obtain information about the device’s location, an Android application does the following. To declare its interest in receiving location information, an application registers a “listener” object with the operating system. When the device’s

location has been pinpointed by the GPS (i.e., a “fix” has been obtained), the Android operating system delivers this information to all registered listeners for applications to use.

Fig. 1 depicts a simplified view of the Android location framework. At the lowest layers, the Location Engine aids the GPS in obtaining a location fix. Upon obtaining a fix, the relevant information is passed up to the GpsLocationProvider (GLP) where it is all wrapped together into a single Location Object and passed to the LocationManagerService (LMS). The LMS is responsible for the delivery of Location Objects to interested listeners. The information contained in a Location Object includes a timestamp, a latitude, longitude, and an accuracy (a confidence radius, given in meters).

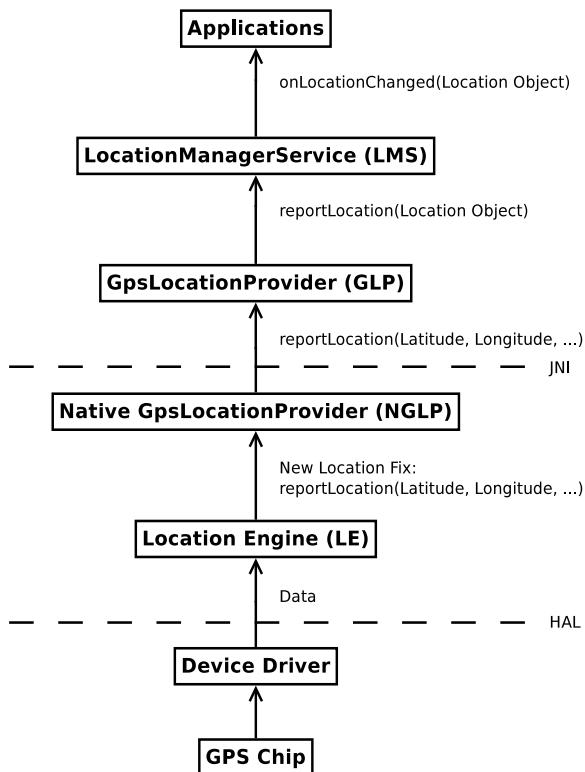


Fig. 1. Android Location Framework

The process of attempting to obtain a fix on a device’s location is known as navigating (tracking) and contributes to the bulk of the power consumed when employing the GPS. This process runs continuously as long as there remains at least one registered listener for location information.

In the Settings application for Android smartphones, an option called “Location Services” (a.k.a. “Location Access”) may be interacted with to manually

enable or disable GPS navigating. Enabling or disabling Location Services causes the corresponding action to occur in the location framework - for example, disabling Location Services causes the LMS to disable the GLP which, in turn, stops the Location Engine from navigating. Whether or not the physical GPS chip is powered down is dependent upon implementation, however the energy cost to power the chip is negligible compared to the power consumed to determine a location.

3.3 Android Wi-Fi Operation

The actual operation of the Wi-Fi subsystem is not pertinent to our research. However, it is important for us to receive connection information such as the state of the connection, a network's SSID, and an access point (AP)'s MAC address. After a connection has been made to a Wi-Fi network, the Android operating system fires a broadcast containing connection information throughout the system. Thus, it suffices for our solution to listen for these specific broadcasts and make decisions based on the connection information.

One should also take into account that the average user may leave Wi-Fi on at all times, though it may or may not be connected to an AP. It follows that the total power cost combines the cost of using Wi-Fi with that of the GPS.

4 Design

The main goal of our solution is to reduce a device's energy consumption by analyzing the device's context and turning off unnecessary components, such as GPS, Wi-Fi, or sensors. Our solution must also be implemented in a seamless manner such that applications need not be modified to accommodate any changes.

To meet our power consumption goal, we first experiment with the idea of disabling a device's GPS when the device has connected to a Wi-Fi network with a location that has been previously user-defined or may be looked up using online services such as WiGLE [14], or another wardriving database. If this location is known ahead of time, the GPS may be turned off while the device remains connected to the network. The known location can just be pushed regularly to interested applications while the GPS remains unused.

Because control over the physical GPS chip is left to the device driver, directly powering off the GPS is not straightforward and an approach that works on one device may not work on another device with GPS hardware from a different manufacturer. Thus, an alternative approach to tackling the power consumption problem is to turn off GPS navigation, as discussed in Section 3.

A few considerations surround this approach. First, applications must not be notified that the GPS is unavailable as per the standard protocol when the user manually disables the Location Services option. Many applications are programmed to adapt to the user enabling and disabling Location Services, but in our case, we wish to disable GPS functionality and push a predetermined

location in its stead. Second, a suitable location within the location framework must be chosen to implement our solution. To achieve a seamless integration with existing applications, we cannot require that application code be adapted to our changes to the location framework.

GPS navigation may be disabled as high as the GpsLocationProvider (GLP) level, shown in Fig. 1. By disabling the GLP, it calls downward to the Location Engine to stop navigating. It is favorable to make our modifications to higher levels in the location framework so as to maximize compatibility. The typical way to disable the GLP is to interact with an Android class called SettingsProvider, which manages changes to a user's settings, such as enabling or disabling Location Services. However, going through the SettingsProvider class to disable a given location provider causes applications to be notified that the provider is unavailable. Thus, to circumvent this, we create a class that directly interacts with the GLP to enable or disable it when needed. Because it is not the responsibility for a location provider to notify applications that it is disabled, applications still believe it is enabled even when we disable it. Our modification to the location framework is shown in Fig. 2.

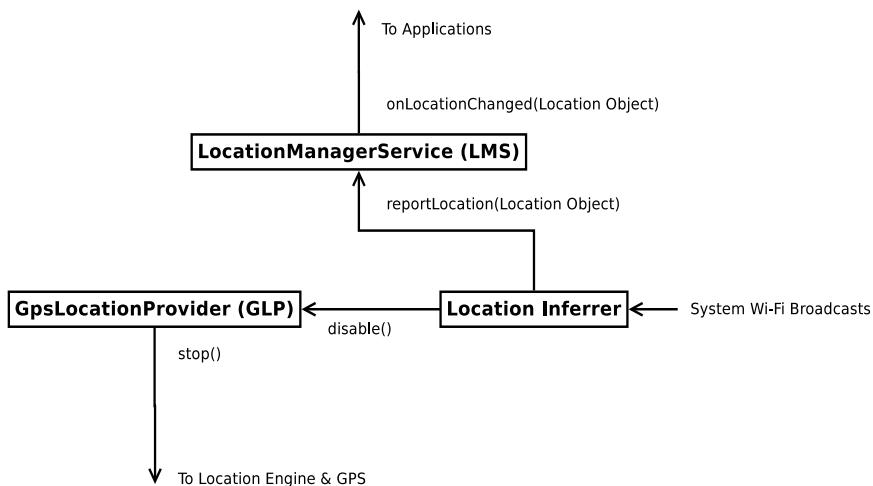


Fig. 2. Proposed Location Framework Modifications

This class, which we refer to as the Location Inferrer (Inferrer, for short), is instantiated by the LocationManagerService (LMS) after the GLP has been instantiated. It receives Wi-Fi-related broadcasts and, if connected to a Wi-Fi network with a known location, will disable the GLP which, in turn, stops GPS navigating. While remaining connected to such a network, the Location Inferrer regularly sends the known location to the LMS which will deliver the location information to interested applications. Once disconnected from the network, the GLP will be enabled again and will enable GPS navigation, thus taking over

from the Inferrer. By choosing to implement our solution this way and at this level, minimal changes are made to the location framework itself and our solution achieves transparency. The LMS still is responsible for delivering Location Objects to listeners and the Location Engine/driver are still responsible for obtaining a location fix when necessary. The operation of the Location Inferrer is shown in Fig. 3.

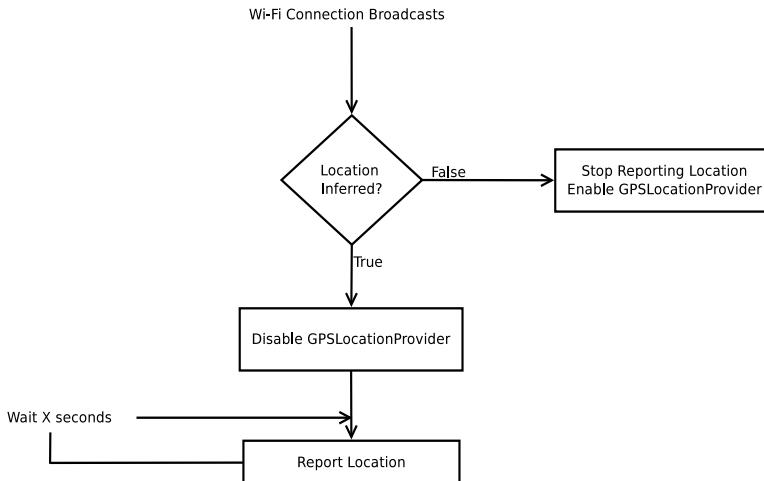


Fig. 3. Location Inferrer Flow Diagram

We expect this approach may result in power consumption to be close to that of Wi-Fi while the Location Inferrer is in use. It also should be noted that the interval on which the Location Inferrer will report a location can be adjusted to meet application requirements.

Aside from the GPS, we hypothesize other components may also be powered off or unused based on context. As mentioned in Section 2, a user's movement can be used as a trigger to disable certain components, such as the GPS. If a user is not moving and is not utilizing their Wi-Fi connection, then Wi-Fi may be shut off to further energy savings. Thus, to measure the battery impact of this idea, we add an additional test to our evaluation in which we use the accelerometer to turn off Wi-Fi while the device is idle.

5 Evaluation

First, we give the settings and conditions under which we measure power consumption of our implemented Location Inferrer. Then, we discuss the results and remarks of our tests.

5.1 Settings

We evaluate our solution by measuring the change in our prototype device's battery level over time in different situations. This approach is taken as opposed to looking at battery usage statistics as those statistics typically do not list hardware components, such as the GPS, by themselves. These tests are done indoors with the phone stationary so that movement is not a factor in determining the device's location from the GPS. The location where testing is done is predefined such that it is known to the Location Inferrer. Our first set of tests are performed with the device set in airplane mode, with screen brightness at the lowest level, and using an application that continually needs location data, but does little with it. Tests are performed in this fashion so as to keep other battery draining factors as minimal as possible. Two tests are performed using the Maps application from Google to evaluate performance under a realistic setting. Finally, we conduct one additional test with the minimal application in which the accelerometer is used to disable Wi-Fi while the phone is idle, but still allows the Location Inferrer to work.

Measuring the change in the device's battery level is done as follows. First, the phone is charged fully (when the battery indicator reads "Charged" rather than "Charging, 100%"). Second, our testing application is set up to receive battery-related broadcasts. Such broadcasts are fired every time the battery level changes (for example, from 100% to 99%). Thus, the application keeps track of the amount of time it takes for the battery level to decrease by 1%. Each test was measured in the amount of time it took for the battery level to decrease from 100% to 99%.

A total of 10 types of tests were conducted, 8 of which used the minimal application, 2 of which used the Maps application. First, a baseline test was conducted in which the device was purely in airplane mode, with Wi-Fi and Location Services disabled. Then, a test was conducted with Wi-Fi enabled and idle, but without the Location Inferrer implemented. A test was also conducted where GPS and Wi-Fi were both on, but the Inferrer was not implemented and Wi-Fi was not connected - just left idle. The GPS acted normally to find a location fix. This test was intended to simulate a user who leaves Wi-Fi on constantly. Following those, were three tests with the standard GPS to see if GPS's energy consumption was different under different situations. The first of the three was to let the GPS act as normal and find a location fix naturally. The second was taken in a basement to test the energy consumption of the GPS in a situation where it would be unable to obtain a location fix. The third test was performed after the GPS had already obtained a fix and was constantly updating its location.

Two test types were conducted with the Location Inferrer. The first involved letting the Inferrer operate normally after the smartphone had connected to a Wi-Fi network with a predefined location. The second test incorporated the use of the accelerometer to disable Wi-Fi while the smartphone was idle. In this case, the Location Inferrer was still allowed to run while Wi-Fi was turned off.

The final 2 of the 10 total test types were performed with the Maps application to measure the differences in using a commercial application - one test with the Location Inferrer and one test with the standard GPS.

5.2 Results

Table 1 displays the results of each of the 10 tests performed. The results are the averages of multiple tests of the same type. As can be expected with minimal functionality, the baseline test took 13.58 minutes to decrease the battery level by 1%. Adding on Wi-Fi functionality, although idle, decreased the time by about two minutes, or 12.8%.

Table 1. Test Results - Battery Life from 100% to 99%

Test	Time (seconds)	Time (minutes)
Baseline	814.83	13.58
Wi-Fi Idle	710.44	11.84
GPS & Wi-Fi Idle	541.96	9.03
GPS - Normal	546.89	9.11
GPS - No fix Obtained	572.97	9.55
GPS - Obtained Fix	558.18	9.30
Location Inferrer - with Wi-Fi	687.22	11.45
Location Inferrer - with Accelerometer	781.64	13.03
Maps - Location Inferrer	544.83	9.08
Maps - GPS	396.67	6.61

Implementing the Location Inferrer yielded an average time of 11.45 minutes, which is only about 4.7% less than the Wi-Fi Only test and 15.7% less than the baseline. It is expected to be slightly less as the Inferrer has to report a location at a regular interval and also has to manage Wi-Fi-related broadcasts. All three of the GPS tests yielded a time between 9 and 10 minutes which, at best, is 30% worse than the baseline. However, it does show that the GPS consumes about the same amount of energy regardless of the progress it has made in obtaining a location fix. Having Wi-Fi idle while using the GPS seemed not to make too much of difference compared to the other GPS tests, however it had the most effect on the battery life of all the initial tests.

The main feature to note is that the Location Inferrer, on average, performs two minutes better than the standard GPS operation. Compared to the GPS - Normal test, using the Inferrer is a 25.7% increase in battery life and is a 19.9% increase compared to the GPS - No Fix Obtained test. This two minute relationship is also held when performing the tests with the Maps application. In this case, there is a 37.4% increase in battery life by using the Inferrer. As expected with the Maps tests, the battery drains faster than with the minimal application - the Maps - GPS test is shown to consume about twice as much energy as the baseline. Finally, using the accelerometer to disable Wi-Fi while the smartphone is idle and still allow the Location Inferrer to run yielded an average time that was only 4.1% less than the baseline.

5.3 Remarks

As expected, using our Location Inferrer causes energy consumption to be closer to that of Wi-Fi, rather than the GPS. Many users leave Wi-Fi and Location Services on at all times and users of Wi-Fi often have their devices set to automatically connect to a familiar network once it is in range. It follows that a user with the implemented Location Inferrer gets the most energy savings while at home, the office, or on a college campus. The use of Wi-Fi is pervasive enough in today's society that it is often available in many locations. Moreover, while indoors or in underground locations, the accuracy of the GPS drops significantly and a location fix may not even be possible. However, because locations may be user-defined or looked up online, our solution is still able to deliver accurate location data when the GPS is not reliable.

Android 4.4 (KitKat) introduces a battery saving mode for the GPS. Although our prototype device is not running KitKat, this battery saving mode uses fewer reference points to find a location fix. As a result, the location fix is less accurate. In this respect, the Inferrer may still be able to deliver more accurate location data while still only using Wi-Fi.

6 Conclusion

In this paper, we devise a solution to disable GPS functionality based on context in order to conserve battery life. Specifically, once a location can be inferred from Wi-Fi connection information, our solution disables GPS navigation. Once GPS navigation has been disabled, our solution reports the inferred location in its stead. Our solution is implemented transparently into the Android location framework such that application code needs not be adapted to our modifications. Our results show that battery usage with our solution implemented is significantly improved from that of the natural GPS operation. In addition, the battery usage is similar to that of using Wi-Fi rather than using Wi-Fi plus the GPS. Finally, our results show that implementing a solution to disable Wi-Fi while the smartphone is idle causes battery usage to be close to our baseline. We plan to expand upon this solution by introducing additional modules to disable other smartphone components, such as Wi-Fi or sensors, based on device context.

Acknowledgement. This work was supported in part by the National Science Foundation of the US (CNS-1352726 and CNS-1265311).

References

- [1] Kjærgaard, M.B., Langdal, J., Godsk, T., Toftkjær, T.: Entracked: Energy-efficient robust position tracking for mobile devices. In: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services. MobiSys 2009, pp. 221–234. ACM, New York (2009)

- [2] Paek, K.G.: Energy-efficient rate-adaptive gps-based positioning for smartphones. In: MobiSys 2010 Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, pp. 299–314. ACM (2010)
- [3] You, C.W., Huang, P., Chu, H.H., Chen, Y.C., Chiang, J.R., Lau, S.Y.: Impact of sensor-enhanced mobility prediction on the design of energy-efficient localization. *Ad Hoc Netw.* 6(8), 1221–1237 (2008)
- [4] Zhuang, K.S.: Improving energy efficiency of location sensing on smartphones. In: MobiSys 2010 Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, pp. 315–330. ACM (2010)
- [5] Nath: Ace: Exploiting correlation for energy-efficient and continuous context sensing. In: MobiSys 2012 Proceedings of the 10th International Conference on Mobile Systems, Applications and Services, pp. 29–42. ACM (2012)
- [6] Lin, K., Kansal, A., Lymberopoulos, D., Zhao, F.: Energy-accuracy trade-off for continuous mobile device location. In: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, MobiSys 2010, pp. 285–298. ACM, New York (2010)
- [7] Farrell, C.R.: Energy-efficient monitoring of mobile objects with uncertainty-aware tolerances. In: IDEAS 2007 Proceedings of the 11th International Database Engineering and Applications Symposium, pp. 129–140. IEEE (2007)
- [8] Youssef, A.: The horus wlan location determination system. In: MobiSys 2005 Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, pp. 205–218. ACM (2005)
- [9] Thiagarajan, A., Ravindranath, L., LaCurts, K., Madden, S., Balakrishnan, H., Toledo, S., Eriksson, J.: Vtrack: Accurate, energy-aware road traffic delay estimation using mobile phones. In: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys 2009, pp. 85–98. ACM, New York (2009)
- [10] Inc, C.: Cyanogenmod Official Website, <http://www.cyanogenmod.org/>
- [11] Android: Android SDK, [http://developer.android.com/sdk/index.html/](http://developer.android.com/sdk/index.html)
- [12] Samsung: The Galaxy S4 smartphone specifications, <http://www.samsung.com/global/microsite/galaxys4/index.html/>
- [13] Android: Android Location Strategies, <http://developer.android.com/guide/topics/location/strategies.html/>
- [14] WiGLE: WiGLE Official Website, <https://wigle.net/>

Exploiting and Defending Trust Models in Cooperative Spectrum Sensing

David Jackson¹, Wanyu Zang¹, Qijun Gu², and Wei Cheng¹

¹ Department of Computer Science, Virginia Commonwealth University, USA

² Department of Computer Science, Texas State University, USA

Abstract. Cognitive radios are currently presented as the solution to the ever-increasing spectrum shortage problem. However, their increased capabilities over traditional radios introduce a new dimension of security threats. Cooperative Spectrum Sensing (CSS) has been proposed as a means to protect cognitive radio networks from the well known security threats: Primary User Emulation (PUE) and Spectrum Sensing Data Falsification (SSDF). We demonstrate a new threat to trust-based CSS protocols, called the *Rogue Signal Framing* (RSF) intrusion. Rogue signals can be exploited to create the illusion of malicious sensors which leads to the framing of innocent sensors and consequently, their removal from the shared spectrum sensing. Ultimately, with fewer sensors working together, the spectrum sensing is less robust for making correct spectrum access decisions. To counter RSF, we introduce a new defense based on cluster analysis from analyzing the network's Received Signal Strength (RSS) diversity, which demonstrates up to 95% damage reduction to sensor reputations.

Keywords: Cognitive Radio Network, Cooperative Spectrum Sensing, Rogue Signal, Trust, Reputation.

1 Introduction

The growing demand for wireless services shows an inevitable overcrowding of the spectrum bands, in large part due to the rapid increase of wireless mobile services in recent years. Conventionally, the Federal Communications Commission (FCC) had statically assigned spectrum bands to licensed users for exclusive use on a long term basis, precluding anyone else from access [1]. Yet, analysis of the spectrum bands clearly indicate that current FCC policies have created severely under-utilized channels, causing a bottleneck for new wireless services [1]. Dynamic Spectrum Access (DSA) is the proposed solution to alleviate the overcrowding of bands by allowing licensed Primary Users (PUs) to share unused spectrum with unlicensed Secondary Users (SUs) in an opportunistic fashion [1, 2].

Cognitive Radios (CR) utilize the DSA technology that enables autonomous optimization of radio configurations and the scanning of spectrum bands to locate the best available channels on a non-interference basis [3]. The cognitive

radio network (CRN), i.e. the secondary network, is given permission to coexist in licensed channels under two preconditions mandated by the FCC: (1) giving spectrum priority to licensed users and (2) minimizing interference to licensed users. To meet these requirements, the cognitive radios must have the ability to reliably detect, in real time, the presence or absence of a primary signal from a given spectrum band. Otherwise, these cognitive radios can unknowingly transmit signals simultaneously with the primary transmitter, causing unacceptable levels of interference to nearby PUs.

Cooperative Spectrum Sensing has been proposed as an effective approach for boosting the detection of primary signals in CR networks [2, 4]. In centralized CSS, the SUs submit their sensor reports to the Fusion Center (FC), which is a server for aggregating and cross-examining the network's sensor reports for a more robust analysis of the spectrum availability. Here, the FC collects the network's sensor reports and outputs a global decision to notify SUs if they can access a licensed spectrum band. CSS is vulnerable to attacks like the Spectrum Sensing Data Falsification (SSDF) where a SU maliciously rewrites the spectrum sensing result to mislead the FC [5].

In an NSF 2009 workshop, the FCC had raised the question, “What authentication mechanisms are needed to support cooperative cognitive networks? Are reputation-based schemes useful supplements to conventional Public Key Infrastructure (PKI) authentication protocols?” [6] Reputation-based schemes in CSS are a popular technique for performing robust and accurate spectrum sensing, because it does not require any interaction with the primary network. However, the question remains on how effective they are at satisfying the FCC requirements. The extended programmability and the operational flexibility of cognitive radios have dramatically increased the attack surface, in that it becomes possible to create a wide range of unauthorized waveforms with low-cost consumer devices [6].

Unfortunately, we find that the sensor reputations are exploitable by rogue signals in trust-based CSS protocols. In secondary networks, it is very hard to conclude the root cause of bad sensor reports; such as malfunctioning sensors, the hidden node problem, SSDF attacks, and rogue signals. The trust-based protocols treat all inaccurate sensors the same way, in a loss of reputation. We consider these trust models as overly sensitive Intrusion Detection Systems (IDS) for penalizing sensors without taking into account the root cause of the abnormal sensor reports. As a result, attackers can cause inaccurate sensor reports by transmitting narrow rogue signals in order to destroy the reputation of the targeted sensors. Accordingly, we present a new threat to a variety of trust-based CSS protocols, named the Rogue Signal Framing (RSF) intrusion. To launch this attack, we exploit directional antennas to spoof rogue signals on clusters of sensors. The outcome is the emulation of an SSDF attack through sporadic and misleading rogue signals, causing division of sensor reports in the network. This contrast leads to innocent sensors being treated as malicious, and consequently removed from the shared spectrum sensing.

To counteract this new threat, we propose a new defense scheme, named the RSF Clustering Defense (RCD) module, that looks for dense clusters of sensors from the proximity and similarity of sensor reports in order to look for isolated radiation patterns caused by the RSF intrusion. Thus, the RCD module can distinguish sensors under the RSF intrusion and mitigate the trust damage. In effect, our defense prevents trust models from becoming an overly sensitive IDS by minimizing the false alarms caused by rogue signals, but still *relies* on a trust model to stop SSDF attacks. The following are a list of contributions:

- Introduced the Rogue Signal Framing Intrusion, an attack on the trust model of CSS protocols
- Developed a solution, the RSF Clustering Defense (RCD), that protects sensor reputations from manipulation in trust models
- Ran simulations that demonstrated the impact of the RSF intrusion and the RCD solution

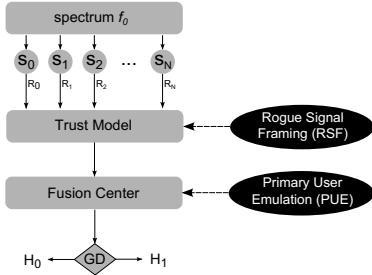
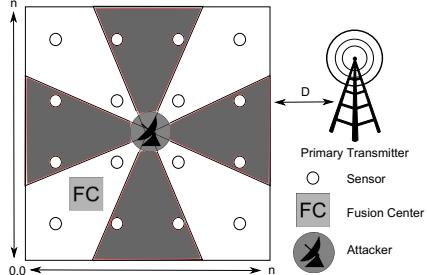
The rest of the paper is outlined as follows. Section 2 reviews common CRN attacks and trust-based CSS protocols. Then, we present the system model in Section 3, and show the details and analysis of the RSF intrusion in Section 4. We propose the RCD defense and evaluate it in Section 5 and conclude the paper in Section 6.

2 Related Works

Our work is mostly related to the following attacks and defenses in CRNs.

Attacks: Although CRNs are vulnerable to a variety of attacks [3], two attacks received much attention. One is the primary user emulation (PUE) attack [3, 7], where an attacker masquerades as the primary transmitter from the vantage point of its neighbors. The other attack is the spectrum sensing data falsification (SSDF) [2, 5], in which compromised users falsify the local spectrum sensor reports to obscure the existence or create an illusion of a primary signal at the FC. Both attacks deceive the FC on the perception of the primary signal that leads to wrong decisions of spectrum accessing. In contrast, the RSF intrusion disrupts the trust between the FC and sensors, which makes the spectrum sensing less stable.

Trust-based CSS Protocols: To defeat the PUE and the SSDF attacks, several trust-based schemes were developed. Chen *et al.* [5] presented a sequential probability ratio test (SPRT) and weighing the result by reputation to mitigate the impact of SSDF attacks. Their model incorporates sampling votes on the detection or absence of the primary signal, and weighing each vote according to the sensor’s reputation. Kaligineedi *et al.* [10] presented a pre-filtering average combination scheme. The scheme’s filters are responsible for (1) filtering extreme outlier sensor reports and (2) ignoring sensors that have a history of deviating from the majority. Arshad *et al.* [8] presented a beta reputation system model for hard-decision CSS protocols. Similar to [5], the sensors are rewarded for agreeing with the global decision, and otherwise penalized.

**Fig. 1.** System Model**Fig. 2.** Illustration of Attack Model

Contributions: What makes our solution unique is that our defense protects the integrity of trust models, i.e. sensor reputations, from rogue signal manipulation. Previous literature used trust models to stop malicious SUs from deceiving the CSS, but did not consider the trust models themselves to be the target of attacks. Trust models were considered reliable solutions against SSDF attacks and malfunctioning sensors, but to our knowledge, none of the papers discussed how to manipulate and disrupt trust models. We realized the vulnerability of trust models due to their coarse threshold of penalizing inaccurate sensor reports, i.e. a sensor is deemed untrustworthy if it does not behave in a predetermined way. However, if an attacker knows how the sensors should behave, then they can exploit rogue signals to disrupt typical sensor behavior and thus destroy their reputations.

3 Attack Model

In this section, we define the RSS model and the method of attack for the RSF which employs *directional antennas*. The attacker manipulates sensor reputations by transmitting rogue signals to targeted sensors, thus causing conflicting sensor reports in the network. To ensure that reports do conflict, directional antennas are used to avoid targeting the entire network.

Fig. 1 illustrates the system model of trust-based CSS protocols and the different targets of PUE and RSF intrusions. In it, f_0 represents some wireless spectrum frequency, S_i a set of sensors, and R_i the corresponding sensor reports. The system model is a stack of dependent layers, starting with the spectrum channel, the network of sensors, the trust model, and finally the FC. The accuracy of the CSS depends on if the FC receives reliable input from the above layers. For example, the spectrum channel must be clear enough for communication, the majority of sensors must not be malicious or malfunctioning, and the trust model must filter the malicious sensors to protect the FC from bad input.

Without loss of generality, we use a system as shown in Fig. 2 to discuss the proposed security issues. Within the network area, the spectrum sensors are randomly distributed and the attacking antennas are positioned in the middle. The FC collects the sensor reports and cross-examines the local observations to

make a global decision on channel vacancy. Spectrum sensing occurs in scheduled time intervals when all communications from the secondary network stops, called *quiet periods*, in order to listen for the primary signal [2].

3.1 Propagation Model

Energy Detection: We decided to use energy detection because it is the most common type of spectrum sensing [4]. Secondly, the three trust-based CSS protocols that we borrow for our simulations, from papers [5, 8, 10], all have energy detection as their spectrum sensing.

The received signal strength (RSS) in decibels per milliwatt (dBm) for any given sensor s_i can be modeled as below according to [9]:

$$R_i = \begin{cases} \mathcal{N}(\mu_\omega, \sigma_\omega), & H_0 \\ 10 \log_{10}(P_{ray}(d_{ij})) + L_s[x_i, y_i], & H_1 \end{cases} \quad (1)$$

The model gives two possible RSS values. When the antenna is not transmitting (i.e. case H_0), the RSS is actually from the noise, for which μ_ω is the noise power mean and σ_ω is the noise variance. On the other hand, when the antenna is emitting signals (i.e. case H_1), the RSS is determined by the attenuation of signal propagation from the attacker to the sensor and shadow fading. In the H_1 case, we use the Rayleigh fading model in milliwatts (mW), expressed as: [11]

$$P_{ray}(d_{ij}) = \frac{P_t G_t G_r \lambda^2}{(4\pi d_{ij})^2} \sqrt{r_1^2 + r_2^2} \quad (2)$$

where d_{ij} is the distance between s_i and the j^{th} attacking antenna, λ denotes the wavelength (meters), P_t is the emission power, G_t and G_r are the antenna gains of the transmitter and receiver, and $r_1, r_2 \sim \mathcal{N}(0, 1)$.

The RSS value R_i is measured in decibels per milliwatt (dBm). However, the Rayleigh fading model (from eq. 2) is in milliwatts (mW), so we apply the unit conversion $dBm = 10 \log_{10}(mW)$ in eq. 2 under hypothesis H_1 . In addition, $L_s[x_i, y_i] \sim \mathcal{N}(0, \sigma_L)$ is the correlated shadow fading gain [12] between s_i 's position $[x_i, y_i]$ and the j^{th} antenna's position $[x_j, y_j]$, and σ_L is the shadow fading variance.

4 Rogue Signal Framing Intrusion

In the CSS paradigm, the physical layer (i.e. the sensor) provides local signal detection. The FC collects the sensor reports and validates the signal authenticity through cross-examination of the network's sensor reports. However, verifying the source of RF waves at the physical layer is incredibly challenging, especially for energy detectors that can only observe the RSS. Since the energy detectors only measure raw RF energy, there is no cryptographic means to identify the source [3].

According to the first CRN standard, the IEEE 802.22, the secondary network must be self-reliant in minimizing interference to the primary network which requires accurate spectrum analysis [7]. In the case of SSDF attacks, trust models have been effective at removing malicious sensors from the shared spectrum sensing [5, 8, 10]. Trust models remain effective so long as the non-malicious sensors generally show normal behavior. In other words, sensors are labeled untrustworthy when they have a consistent history of abnormal sensor reports, regardless if the sensor is malicious or simply overshadowed by terrain.

Rogue signals can raise a sensor's RSS well above what is expected, especially in the absence of the primary signal. So a prolonged rogue signal on a group of sensors can cause a sharp contrast from the others, thus appearing malicious and no different than SSDF. Consequently, the security protocol brands these sensors as untrustworthy and removes them from the shared spectrum analysis for as long as the stigma remains. As such, the RSF intrusion over many quiet periods constitutes as an exploitation of the trust model. In the context of CSS, we define the term *Rogue Signal Framing* intrusion as follows,

Definition: *Rogue Signal Framing* intrusion breaks the trust between the Fusion Center (FC) and a group of sensors via rogue signals to create the illusion of malicious sensors

To launch this attack, we exploit directional antennas to isolate a radiation pattern to a group of sensors in close proximity, and thereby causing them to report abnormally high RSS relative to the rest of the unaffected network. This scenario emulates a false alarm SSDF to innocent sensors that causes them to appear malicious, and consequently removed from the shared spectrum sensing.

4.1 Simulation Setup

To test our proposed framing intrusion, we simulated three different trust-based CSS protocols with the Matlab software. The first protocol F_A , by Chen *et al.* [5], utilizes the sequential probability ratio test (SPRT) and weights the probability by the sensor's reputation to mitigate the impact of SSDF attacks. The second protocol F_B , by Kaligineedi *et al.* [10], utilizes a pre-filtering average combination scheme. These filters are responsible for (1) filtering extreme outlier sensor reports and (2) ignoring sensors with high trust penalties. The third protocol F_C , by Arshad *et al.* [8], utilizes a beta reputation system model for hard-decision CSS protocols. Like F_A , the sensors are rewarded for agreeing with the global decision, and otherwise penalized.

We make the following assumptions on the simulation's environment according to an IEEE 802.22 WRAN environment that encompasses UHF/VHF TV bands and the use of Customer Premise Equipment (CPE) for SUs. Cognitive radios that are CPE infer that their positions are fixed with respect to the SU's residency, so we make the assumption that we know the positions of all the sensors based on the SU's address and that they cannot move. In our simulation, 400 sensors are located inside a 2000×2000 grid. Like Fig. 2, there are four rogue

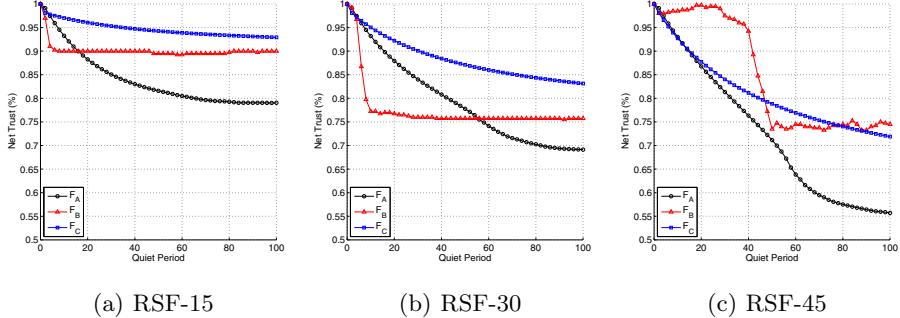


Fig. 3. Displays the network's total trust (from Eq. 3) over 100 quiet periods for protocols F_A , F_B , and F_C . The beamwidth of each rogue antenna is 15° , 30° , and 45° for scenarios RSF-15, RSF-30, and RSF-45, respectively.

directional antennas facing the cardinal directions and positioned on the map's center. Protocols F_A , F_B , and F_C are tested on RSF intrusion scenarios, labeled as RSF-15, RSF-30, and RSF-45 which corresponds to its antenna beamwidths of 15° , 30° , and 45° , respectively. In our simulation, sensors are affected by a rogue signal attack when they are within the rogue signal's radiation pattern.

The main goal of the RSF attack is to compromise the trust between the FC and network sensors. To quantify the trust damage, we use the following equation to measure the network's trust score $T_\Sigma[q]$ on quiet period q with:

$$T_\Sigma[q] = \frac{1}{T_\Sigma[0]} \sum_{s_i \in S} t_i[q] \quad (3)$$

where $T_\Sigma[0]$ is the initial trust score and $t_i[q]$ is the trust score of sensor $s_i \in S$. For each trust-based CSS protocol, the trust score is represented differently. In order to compare the trust damage between each protocol, we normalized the trust score t_i such that $t_i[q] \in [0, 1]$ in the equation.

4.2 Attack Evaluation

Fig. 3 shows the network's total trust $T_\Sigma[q]$ over 100 quiet periods for each scenario. Depending on the protocol and different evaluation environment, the RSF intrusion removed nearly 15% to 45% of the network's total trust which correlates to the percentage of sensors removed from the shared spectrum sensing. As expected, $T_\Sigma[q]$ decreases and plateaus over time. It plateaus when the attacked sensors eventually have no more trust to lose.

In Fig. 3, the change in the network's total trust $\Delta T_\Sigma[q]$ per quiet period is different for protocols F_A , F_B , and F_C , because a sensor's trust score is adjusted differently for each protocol. Hence, these protocols behave differently against rogue signals, but the overall trend is a net loss of total trust $T_\Sigma[q]$ as q increases.

From Fig. 3, we observe that both protocols F_A and F_C start to plateau, because the t_i of attacked sensors eventually converge on 0, causing the $\Delta T_{\Sigma}[q]$ to become stagnant over time. However, protocol F_B differs in that it does not have local decisions to compare to FC's global decisions. Instead, it uses a dynamic threshold for deciding malicious sensor reports which scales with the RSS variance. As the attack coverage increases from RSF-15 to RSF-45, so does the RSS variance and the F_B 's behavior towards the RSF intrusion.

5 Rogue Signal Framing Clustering Defense

This section introduces the RSF Clustering Defense (RCD) module that operates in three steps: 1) analyze the RSS diversity for any clustering behavior, 2) compute the clustering strength in order to conclude the presence of a rogue signal, and if so 3) ignore trust penalties on sensors in the attacked clusters. The defense relies on the fact that directional antennas leave isolated radiation patterns that form dense communities of sensors. Malicious sensors can perform SSDF attacks from the software layer without the need of rogue signals, and thus operates outside the physical limitations of signal properties. In contrast, the RSF attack coverage is bound by the rogue signal's radiation pattern.

5.1 Network Classification and Clustering

Our solution, which involves graph partitioning and community detection, is based on the principle of assortative mixing, but tailored in the context of cognitive radio networks. The RCD has three requirements for operation. First, it needs the local spectrum decision $c_i \in \{H_0, H_1\}$ for all sensors $s_i \in S$. Second, it needs two sets of sensors where $S_{H_0} = \{s_i | c_i = H_0\}$ and $S_{H_1} = \{s_i | c_i = H_1\}$. Lastly, it needs an adjacency matrix A of size $|S| \times |S|$ such that

$$A_{ij} = \begin{cases} 1 & \text{if } d_{ij} \leq d_{\theta} \\ 0 & \text{if } d_{ij} > d_{\theta} \end{cases} \quad (4)$$

where d_{ij} is the distance between sensors s_i and s_j , and d_{θ} is the distance threshold.

The RCD module locates k disconnected clusters of sensors C_k such that $s_j \in C_k$, $A_{ij} = 1$ and $c_i = c_j$ for sensors $s_i, s_j \in C_k$. The RCD module's goal is to locate isolated communities C_k that are surrounded by sensors in S_{H_0} . To start, we measure the cluster density of sensors with the same class by counting all connected pairs (s_i, s_j) such that $s_i \in C_k$, $s_j \in S_{H_1}$ and $A_{ij} = 1$. This is computed on all sensors in C_k with:

$$\{d_i^{H_1}\}_k = \left\{ \sum_{s_j \in C_k} (A_{ij} \delta(c_i, c_j)) - 1 \mid s_i \in C_k \right\} \quad (5)$$

$$\delta(c_i, c_j) = \begin{cases} 0 & \text{if } c_i \neq c_j \\ 1 & \text{if } c_i = c_j \end{cases}$$

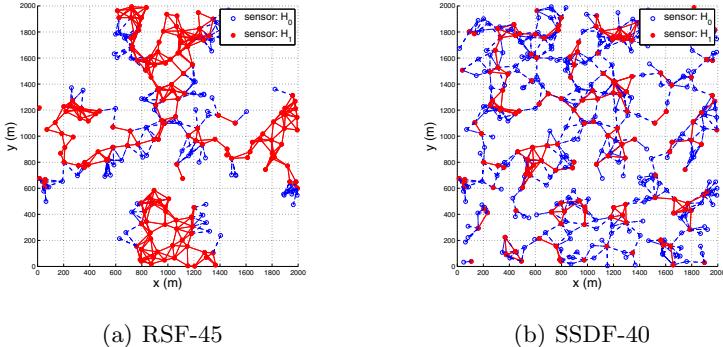


Fig. 4. The sensor network is partitioned into a red and blue graph before being analyzed by the RCD module. The red graph contains edges between sensors reporting H_1 . The blue graph contains edges between sensors having opposing local spectrum decisions.

where $\delta(c_i, c_j)$ is a simple Kronecker's delta function that indicates a difference in a node's class c , i.e. the local spectrum decision. Next, we measure the isolation of sensor $s_i \in C_k$ from $s_j \in S_{H_0}$ by counting all connected pairs (s_i, s_j) such that $A_{ij} = 1$. This is computed on all sensors in C_k by:

$$\{d_i^A\}_k = \left\{ \sum_{s_j \in S_{H_0}} A_{ij} \delta'(c_i, c_j) \mid s_i \in C_k \right\} \quad (6)$$

$$\delta'(c_i, c_j) = \begin{cases} 0, & \text{if } c_i = c_j \\ 1, & \text{if } c_i \neq c_j \end{cases}$$

Finally, to measure the isolated clustering strength Z_k we use the function:

$$Z_k = Z(\{d_i^{H_1}\}_k, \{d_i^{\Delta}\}_k) = \frac{\sum_i d_i^{H_1}}{\sum_i (d_i^{H_1} + d_i^{\Delta})} \quad (7)$$

In the off chance that a number of malicious sensors from SSDF are positioned near each other, we want to have a level of tolerance, so we use a clustering threshold Z_θ and a required minimum number of sensors per cluster C_{min} . The restraint C_{min} prevents a group of sensors from being falsely protected based on a high clustering score Z_k that was found from an insignificant sized cluster. However, adjusting the parameters cannot always guarantee that a cluster of deviating sensors is caused by a rogue signal, as opposed to malicious sensors. Instead, our solution heavily mitigates the damage done by rogue signals, and makes it more difficult for the attacker.

Fig. 4 shows two scenarios; (1) the RSF-45 where each rogue antenna has a beamwidth of 45° and (2) the SSDF-40 where 40% of the sensors, randomly selected, perform SSDF. The red nodes are sensors reporting H_1 and the blue

nodes are sensors reporting H_0 . The red edges are formed when $c_i = c_j$ and $d_{ij} < d_\theta$ for sensors s_i and s_j . The blue edges are formed by the same rules except that $c_i \neq c_j$.

The red and blue graph both give valuable information in which to deduce through the network analysis. The goal of the red graph is to identify a strong concentration of sensors perceiving a radio signal within a small area. In contrast, the blue graph demonstrates disagreements in spectrum decisions (i.e. H_0 and H_1) between neighboring sensors. As can be seen in the RSF scenario in Fig. 4, the red graphs (created by the rogue signals) is surrounded by the blue graph and lacks any significant overlap between the two graphs. The presence of a red graph, without the intersections of blue edges, outlines a radio's antenna coverage, and becomes a clear indication of a rogue signal. However, the SSDF scenario in Fig. 4 shows that an overlapping of red and blue graphs reveal a strong likelihood of malicious or malfunctioning sensors, instead of a rogue signal's presence, since there is no apparent pattern of spectrum decisions.

5.2 Defense Evaluation

In this section, we evaluate the RCD module's performance on its ability to mitigate trust loss from RSF intrusions. Additionally, we compare the RCD module's outcome on RSF and SSDF attacks.

In our simulations, we have two groups of scenarios, the RSF and SSDF. The simulation environment is the same as the one used by the RSF intrusion in Section 4. The beamwidth of each rogue antenna is 15° , 30° , and 45° for scenarios RSF-15, RSF-30, and RSF-45, respectively. The SSDF scenarios simulate malicious sensors by randomly selecting a percentage of the sensors and raising their RSS by 20 dBm from the noise floor. We randomly selected 20%, 30%, and 40% of sensors from the scenarios SSDF-20, SSDF-30, and SSDF-40, respectively.

Fig. 5 shows the amount of mitigated trust damage (%) with the RCD module under the same scenarios. The mitigated trust damage is denoted as $T_M[q]$ and calculated by:

$$T_M[q] = \frac{T_\Sigma^R[q] - T_\Sigma[q]}{T_\Sigma[0] - T_\Sigma[q]} \quad (8)$$

where $T_\Sigma^R[q]$ is the network's total trust on quiet period q when using the RCD module, $T_\Sigma[q]$ is the network's total trust without the RCD module (from Fig. 3), and $T_\Sigma[0]$ is the initial state of trust scores. We use a minimum cluster size $C_{min} = 5$, a clustering threshold $Z_\theta = 0.3$, and a distance threshold $d_\theta = 150$ m.

As shown in Fig. 5, each protocol benefited from our proposed defense against the RSF intrusion. However, the RCD module offered less protection to protocol F_A due its sequential random sampling of sensors, instead of cross-examining all sensor reports for a more robust analysis. The spikes from F_B in Fig. 5 are due to its protocol design of having a dynamic threshold for deciding malicious sensors. During the spikes, F_B 's dynamic threshold is stabilizing as it replaces the old RSS statistics with new data.

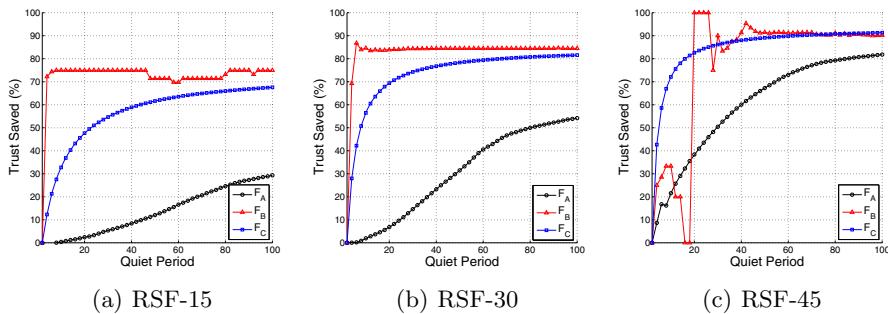


Fig. 5. Displays the network's total mitigated trust damage (defined in Eq. 8) from the RCD module

Fig. 6 shows the rate of false alarms, i.e. the number sensors reporting H_1 when the FC reports H_0 , before and after applying the RCD module. In all three RSF scenarios, the RCD module managed to limit the false alarms to a maximum of 3%. That means the RSF-15 scenario reduced nearly 40% of all false alarms from misleading the trust model and penalizing innocent sensors.

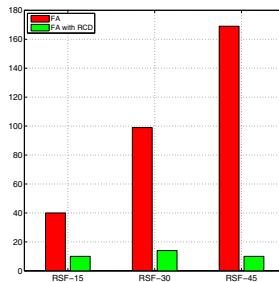


Fig. 6. The number of false alarms before and after applying the RCD module

6 Conclusion

In this paper, we demonstrated the RSF intrusion, a new threat to trust-based CSS protocols. The attackers can transmit rogue signals onto groups of sensors to emulate SSDF and ruin their reputation with the intent of having them removed from the shared spectrum sensing. Our work cautions the use of trust-based CSS protocols and warrants a line of defense against rogue signals. The RSF simulations were conducted in a realistic environment based on the 802.22 WRAN and illustrates the impact of the RSF intrusions on sensor reputation scores. To mitigate the trust damage, we introduced a new defense based on community detection and cluster analysis. The simulation experiments showed

that our defense solution, the RCD module, could effectively keep the sensor reputations intact while distinguishing rogue signals from malicious sensors.

Acknowledgment. This work was supported by the National Science Foundation under Grant No. 0915318, 1048339, 0916469, and 1441253.

References

- [1] Akyildiz, I.F., Lee, W.-Y., Vuran, M.C., Mohanty, S., Akyildiz, I., Lee, W., Vuran, M., Mohanty, S.: Next Generation/Dynamic Spectrum Access/cognitive radio wireless networks: A Survey. *Computer Networks* 50(13), 2127–2159 (2006)
- [2] Chen, R., Park, J.M., Hou, Y., Reed, J.: Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. *IEEE Communications Magazine* 46(4), 50–55 (2008)
- [3] Clancy, T., Goergen, N.: Security in Cognitive Radio Networks: Threats and Mitigation. In: *Cognitive Radio Oriented Wireless Networks and Communications*, 2008. CrownCom (2008)
- [4] Wang, B., Liu, K.: Advances in Cognitive Radio Networks: A Survey. *IEEE Journal of Selected Topics in Signal Processing* 5(1), 5–23 (2011)
- [5] Chen, R., Park, J.M., Bian, K.: Robust Distributed Spectrum Sensing in Cognitive Radio Networks. In: *INFOCOM 2008 The 27th Conference on Computer Communications*, pp. 1876–1884 (2008)
- [6] Steenkiste, P., Sicker, D., Minden, G., Raychaudhuri, D.: Future Directions in Cognitive Radio Network Research. In: *NSF Workshop* (2009)
- [7] Chen, R., Park, J.M.: Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. In: *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, SDR 2006* (2006)
- [8] Arshad, K., Moessner, K.: Robust Collaborative Spectrum Sensing based on Beta Reputation System. In: *Future Network and Mobile Summit 2011 Conference Proceedings* (2011)
- [9] Anand, S., Jin, Z., Subbalakshmi, K.P.: Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks. In: *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008* (2008)
- [10] Kaligineedi, P., Khabbazian, M., Bhargava, V.K.: Secure Cooperative Sensing Techniques for Cognitive Radio Systems. In: *IEEE International Conference Communications, ICC 2008* (2008)
- [11] Kuntz, A., Schmidt-Eisenlohr, F., Graute, O., Zitterbart, M.: Introducing Probabilistic Radio Propagation Models in OMNeT++ Mobility Framework and Cross Validation Check with NS-2. In: *OMNeT++ 2008: Proceedings of the 1st International Workshop on OMNeT++* (2008)
- [12] Forkel, I., Schinnenburg, M., Ang, M.: Generation of Two-Dimensional Correlated Shadowing for Mobile Radio Network Simulation. In: *Proceedings of The 7th International Symposium on Wireless Personal Multimedia Communications, WPMC* (2004)

Towards Reliable and Real-Time Routing with Active Slot Augmentation in Low-Duty-Cycle WSNs

Quan Chen and Hong Gao

Department of Computer Science and Technology,
Harbin Institute of Technology, Harbin 150001
{chenquan,honggao}@hit.edu.cn

Abstract. In this paper, we propose a routing protocol framework (RRAD) to solve the problem of real-time and reliable routing in a low-duty-cycle WSNs with unreliable communication links. The proposed RRAD protocol is able to achieve the probabilistic QoS guarantee in the timeliness and reliability domains by giving the concept of Real-Time Relay Probability, which reflects the probability of successful delivering data through a link within a given deadline. Moreover, the potential forwarder discovering mechanism is designed to compensate for local decision inaccuracies when packets routing toward the destination, and by this mechanism at least 10% deadline miss ratio is reduced. Through comprehensive experiments, we demonstrate the energy efficiency and routing latency of the RRAD protocol.

Keywords: low-duty-cycle network, real-time routing, unreliable link.

1 Introduction

Wireless Sensor Networks (WSNs) have been applied in many mission-critical applications, such as target tracking , assisted living, and closed-loop sensing and control [1, 2]. Many of these applications are expected to be in operation as long as several months or years. Normally, since the sensor nodes have very limited energy supply, a widely employed approach is to let the nodes work in a low-duty-cycle fashion, in which the nodes can alternately work in the active and dormant state according to a wakeup schedule. And it is impossible to continuously maintain a ready-to-use End-to-End (E2E) communication connectivity. In other words, when a node has packets ready to be sent, all of its neighboring nodes may be in the dormant state and it has to wait for one of its neighbors to wake up to forward the packets. Therefore, the existing nodes always-awake real-time routing schemes are impractical in the low-duty-cycle network.

Besides the energy constraints, many applications require reliable and real-time sensory data delivering. Generally, there is a delay constraints assigned with the packets when routing from their sources to the destinations. For example, in a surveillance system, the positions of intruders need to be reported within

several seconds so as to initiate the timely pursuit actions[3]. Nonetheless, due to the lossy and unreliable link, the delay between a link or along a path are dynamic and probabilistic[4]. However, nodes need to identify paths that ensure certain delay bounds in a localized way in the real-time routing.

To overcome the challenges above, we propose a reliable and real-time routing framework (RRAD) with Active Slot Augmentation in a low-duty-cycle WSNs. Unlike previous real-time routing protocols in low-duty-cycle wireless networks, which mainly works in a centralized way or in an source to sink routing scheme(which requires building a broadcasting tree from the sink to the source node) [3, 5–7]. Our protocol not only works in a distributed manner that every node decides its forwarder node(in the following, we use the relay node and forwarding node interchangeably)in a localized way, but also can achieve the probabilistic QoS guarantee in the timeliness and reliability domains. Moreover, the proposed Potential Forwarder Discovering Mechanism was designed to compensates for local decision inaccuracies when packets routing toward the destination according to the two-hop neighboring information. Through comprehensive experiments, the energy efficiency and routing latency of our RRAD protocol and proposed mechanism was demonstrated.

The rest of this work is organized as follows. Section 2 introduces the related work. In Section 3, we propose our RRAD protocol framework design in detail. Simulation results are discussed in Sections 4. Section 5 concludes the paper.

2 Related Work

Real-time routing has been extensively investigated in WSNs. Based on geographic forwarding, [8, 9] was designed to probabilistic guarantee the specified deadline by choosing the relay node according to the forwarding speed at each hop. [10–14]explored the approximation algorithms in reducing the latency. To handle the lossy link in sensor networks, [15] analysed and measured the impact of the unreliable link on the packet loss rate and E2E communication delay. However, they were all designed for nodes always-aware wireless networks.

As to low-duty-cycle sensor networks, [3] provides the real-time guarantee of communication in low-duty-cycle network by increasing duty-cycle at individual nodes, but it works in a source-to-sink and centralized manner. Dousse et al. analysed the delay bound for sending data from source to the sink without co-ordinated working schedules[5]. Nevertheless, these approaches in low-duty-cycle networks all assume perfect communication links. Considering the unreliable communication links, [6] proposes a Dynamic Switch-based Forwarding (DSF) mechanism to optimizes the expected E2E delay, and energy consumption by choosing the different forwarding sequence. However, it can't be apply to the arbitrary E2E communication scenario.

There is relatively few researches on the real-time and reliable routing in the low-duty-cycle WSNs. Based on expected sleep latency, [7] proposes a delay-driven routing algorithm to reduce the delivery delay for the source-to-sink communication. [16] apples a priority-based schedule which only aims at delivering

the high-priority packets quickly. Therefore, to address the problem of real-time routing in the arbitrary E2E communication with unreliable wireless links, we propose the RRAD routing protocol.

In this paper, we consider the following scenario: In a low-duty-cycle wireless networks, when nodes initialize a message(packet) need to be sent, each message is assigned with a specified deadline d and a reliable probability Δp , which means the probability of the message reaching the destination within the given deadline d must be beyond or equal to Δp .

3 Main Design

We assume a multi-hop low-duty-cycle network with N nodes deployed in the target field. Like [7], we assume the time is locally synchronized, and the link quality and geographical location can be attained by [17, 18]. Without loss of generality, the working cycle T of each node is equally divided into a sequence of time slots with same length. Let τ denotes the length of one time slot, which is normally very limited. In traditional wireless sensor networks, the delay in message routing is mainly caused by delivery latency. However, nodes wake up asynchronously in the low-duty-cycle network, and they may have to wait a long period of time for the neighbors to wake up to forward the packet. The waiting time at the sender is called sleep latency. We define t_i as the wakeup time of node i , and $SL(i, j)$ as the sleep latency between node i and j .

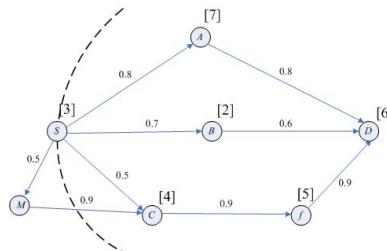


Fig. 1. An Example of Duty-Cycle Network

To elaborate, Fig.1 gives a sample network where the periodically wakeup time of is depicted in brackets and the working period is set $T = 10$. Assuming the source node S gets a packet to be sent at slot 3, it has to buffer the packet for a period of time until one of the neighbors wakes up. If node S chooses B as its relay node, it would have to wait for a whole working cycle, and the sleep latency between node S and B is $SL(S, B) = 2 + 10 - 3 = 9$. But if it chooses node A as its relay node, the sleep latency between S and A is only $SL(S, A) = 7 - 3 = 4$.

3.1 The RRAD Architecture Overview

In this following, we propose our reliable and real-time routing protocol with Active Slot Augmentation (RRAD) design in detail. The architecture of the RRAD

routing protocol is shown in Fig.2. It consists of four core modules: Neighbor Management, Active Slot Augmentation Mechanism, Forwarding Decision, and Potential Forwarder Discovering Mechanism.

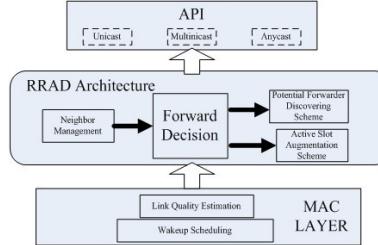


Fig. 2. The Architecture of RRAD

The Neighbor Management module maintains all the one-hop neighbors' information, including the wakeup time of each neighbors and the link quality between each neighbor with the sender. These information can be attained by neighbor beacon message broadcasting in a low frequency. The Forwarding Decision modules computes the optimal relay node to satisfy the requirement of deadline and reliability constraints, is the main part of a routing protocol. The Active Slot Augmentation mechanism is aroused when there exist a failure in the procedure of transmission. However, if the Forwarding Decision modules can't find such a neighboring node satisfying the requirement, then the Potential Forwarder Discovering mechanism is waked up to help find a potential forwarder with two hop neighbors' information. The Potential Forwarder Discovering mechanism and Forwarding Decision modules are our main design.

3.2 Active Slot Augmentation Mechanism

We consider an Active Slot Augmentation Mechanism[3] in our routing protocol. In the lossy environment, a large number of transmissions may fail due to the channel confliction, environment noise or decoding error etc. In this case, the sender has to wait for a whole working cycle for the receiver to wake up again. Apparently, this would introduce large latency in the packet delivering, which is very suffering for real-time routing, especially when the working cycle is set large. In order to reduce the latency, another extra active time slot is added on the original working schedules when there is a failure in transmission.

For example, as shown in Fig.1, we assume node S chooses node C as its forwarding node to help deliver the packet to the destination. When node C wakes up at time slot 4, S is waked up and tries to forward the packet to C . Due to the unreliable link, there occurs a failure in the first transmission and succeeds in the second round. In the traditional case, the delivering delay between node S and C is $DL(S, C) = 4 - 3 + 10 = 11$. But by adding another active time slot when C fails to receive the packet, we can reduce the delivering delay to $DL(S, C) = 1+1 = 2$, only 2 time slots is needed to accomplish the transmission.

3.3 Forwarding Decision

In our protocol, the Forwarding Decision module is designed to satisfy the real-time and reliability requirement according to the concept of Real-Time Relay Probability, which is the main part of the routing protocol. Here, considering the scalability of wireless sensor network, the proposed method is only based on one-hop neighbors' information.

Firstly, each node maintains a neighbor table which can be attained from the Neighbor Management module. Let $NB(i)$ represents the set of i 's one-hop neighbors which i can communicate directly with. According to the distance to the destination, the neighboring nodes in $NB(i)$ are partitioned into two classes: the nodes more close to the destination and the nodes not. Like [8], only the nodes in the first class can be chose as the relay node to speeding up the data delivering. According to this, we have the definition of forwarding candidate set, where the sender chose the forwarding node from.

Definition 1. Forwarding Candidate Set of node i . A set of nodes that: 1)belong to $NB(i)$; 2)are closer to the destination D than the current node. Formally,

$$FCS_i(D) = \{node j | j \in NB(i) \&& dist(i, D) > dist(j, D)\} \quad (1)$$

where $dist(i, D)$ is the distance from node i to the destination D . In order to guarantee the deadline constraints locally, the whole deadline was divided into each hop. We define the Relay Time to represent the maximum time of a packet can be used at each hop.

Definition 2. Relay Time. Relay Time for link l_{ij} is estimated by the advanced distance and the remaining time after the packet reach node i (i.e. $deadline_i$). The advanced distance is calculated by $dist(i, D)$ subtracting $dist(j, D)$. Formally,

$$r_delay_i^j(D) = \frac{dist(i, D) - dist(j, D)}{dist(i, D)} \cdot deadline_i \quad (2)$$

It should be noted that, the remaining time should be update immediately when the packet get to node i . According to formula(4), the link with further advanced distance(the packet is more close to the destination), will have the more Relay Time. The deadline constraints could be guaranteed if we choose the link of which the latency is not larger than the Relay Time at each hop.

Due to the highly unreliable link, the number of transmissions and the link delay would be uncertain and dynamic. In other words, whether the delay of a packet through a link is not exceeding the Relay Time is probabilistic. In order to handle these uncertainties in real-time routing, we have the following definition.

Definition 3. Real-Time Relay Probability. The Real-Time Relay Probability for link l_{ij} is the probability that node i successfully forward the packet to node j within the Relay Time $r_delay_i^j(D)$. Formally,

$$RP_{ij} = 1 - (1 - q_{ij})^{r_{ij}} \quad (3)$$

$$r_{ij} = \begin{cases} (r_delay_i^j(D) - SL(i, j)) / \tau, & \text{if } r_delay_i^j(D) > SL(i, j) \\ r_delay_i^j(D) / SL(i, j), & \text{other} \end{cases} \quad (4)$$

where q_{ij} is the link quality and r_{ij} represents the maximal number of retransmissions given the Relay Time. With the Real-Time Relay Probability, the node with high link quality and further advanced distance would be found. Moreover, Real-Time Relay Probability can improve the routing in two aspects: 1) if the remaining deadline is not enough, then the link with small latency and poor link will be used, 2) if the deadline is enough, we can exploit slow and good link quality to reduce the number of transmissions for energy saving.

For instance, in Fig.1 the immediate neighbor set node of S is $NB(S) = \{A, B, C, M\}$, but only A, B and C are more close to the destination, so the Forwarding Candidate Set $FCS_i(D) = \{A, B, C\}$. If we calculate the Relay Time $r_delay_S^A(D) = 3, r_delay_S^B(D) = 6$, the Real-Time Relay Probability for link l_{SA} and l_{SC} is $RP_{SA} = 0.8$ and $RP_{SC} = 1 - (1 - 0.5)^3 = 0.875$ respectively. Though the link quality for node A is higher, but due to the high sleep latency, only node C is satisfied, which means more transmissions and energy cost. But if the given deadline is long enough, A will be chose to save the energy.

However, only the local reliability was guaranteed with the Real-Time Relay Probability, how to devise local decision mechanisms to identify forwarding paths to meet packets' end-to-end reliability requirement remains a challenge. To address this problem, we give the concept of E2E reliability.

Definition 4. E2E Reliability. In real-time routing, we use E2E Reliability to denote the probability of successful delivering the packet from current node to destination under the given deadline. According to the Real-Time Relay Probability RP_{ij} , node i can locally estimate the E2E Reliability for a neighbor j as follows:

$$e2e_rp(i, j) = (1 - RP_{ij})(1 - RP_{ij})^{r_hop} \quad (5)$$

$$r_hop = \frac{dist(j, D)}{dist(i, D) - dist(j, D)} \quad (6)$$

Note that this local estimation equation is based on the assumptions that the advanced distance will be similar for each following hop.

Definition 5. Forwarding Feasible Set. We use the Forwarding Feasible Set of node i to represent the set of neighbors whose E2E Reliability is larger or equal than Δp .

$$FFS(i) = \{node j \mid j \in FCS(i) \text{ and } e2e_rp(i, j) \geq \Delta p\} \quad (7)$$

Without specification, we will choose the neighbor with the largest E2E Reliability as the optimal forwarder. When $FFS(i)$ is null, it indicates that there may be no node can satisfy the real-time and reliability requirement in the current hop. In this case, the Potential Forwarder Discovering Mechanism is aroused to solve this problem.

3.4 Potential Optimal Forwarder Discovering Scheme

Since each node makes its forwarding decisions locally, some nodes may not satisfy the E2E Reliability requirement and would be neglected in the current hop. However, they can fetch up in the next hop with a link of higher Real-Time Relay Probability. We call this node the potential forwarder. In this section, our goal was to find this kind of node with two hop neighbors' information to reduce the inaccuracy by local decision .

To increase the possibility of finding a potential forwarder, the whole neighboring set of nodes is considered. The main procedure works as follows. Firstly, the sender i sorts the nodes in the Neighboring set with the wakeup time in an ascending order. Let the node with the earliest wakeup time is j , then a 'REQUEST' packet will be sent to j . The 'REQUEST' packet contains a request for Potential Forwarder Discovering and the maximum E2E Reliability in $FCS(i)(rp_max)$. The using of rp_max is to make sure that we can always return a node if none of j 's neighbor can satisfy the reliability requirement Δp . After receiving the 'REQUEST' packet, node j updates the remaining time and computes the E2E Reliability for each neighbor according to the above method. If a relay node can be found to satisfy the E2E Reliability requirement again, j returns a 'FOUND' packet to the sender. But If such a relay node can't be found, then it'll fall into the following two situations: one of its neighbor's E2E Reliability is larger than rp_max or otherwise. In the first situation, node j will be chose as the relay node with a probability p in case of no relay node can be found to satisfy the E2E Reliability requirement in the following procedure. In the second situation, node j just return a 'NOT FOUND' message, then we have to ask the second earliest node and do the above procedure again. This procedure goes on until we find a new relay node.

The 'REQUEST' and the 'FOUND' message can be implemented in the RTS and CTS packet. If it fails, only the RTS and CTS packet are wasted, which are negligible compared to data transmission.

As the example shown in Fig.1, the Forwarding Candidate Set of node S is $FCS(S) = \{A, B, C\}$. If for each candidate node, the E2E Reliability is calculated as 0.6, 0.4 and 0.75 respectively, which are all less than the reliability requirement 0.85. According to the sorting of wakeup time, the sender S first sends a 'REQUEST' message at the time when node C wakes up. If C calculates the E2E Reliability for next forwarder F is 0.9, then C would reply the 'FOUND' message in the CTS packet.

4 Evaluation

In this section, we present the performance evaluation results with extensive simulations. Three baseline solutions below was considered to verify the effectiveness of our design.

1) Geographic-based routing algorithm(GPRS)[17]: Each node chooses the node which is nearest from the destination as its relay node. As the distance is referred, it seems like to find the route with the minimum number of hops.

2) Minimum Latency First(MLF): In this method, the node with the minimum sleep latency will be chose as the relay node. In order not to loss the destination, we only choose the relay node from the Forwarding Candidate Set.

3) Forwarding Speed(SPEED)[8]: Each node calculates its neighbor's forwarding speed(the advanced distance divides by the neighbors expected latency). The fastest node will be chose as the relay node.

Without specification, in the simulation 200 nodes are randomly deployed in a 200m*200m field. The radio parameters strictly follow Chipcon CC2420 hardware specification[19]. The node transmission range is set as 40m. The duty cycle is changed from 1% to 5% and one active time slot is 50 ms. In our simulation, the source and the destination node are randomly chose in the opposite side of the sensor area. In the experiments, all the results are repeated 100 times.

In the simulation, we measure the average E2E delay and deadline miss ratio to demonstrate the efficiency of our method in the timeliness domains. The deadline miss ratio is the ratio of the packet missing the deadline, which is the most important metric in the soft real-time systems[8]. We also compare the energy efficiency of the above methods, which are evaluated by the number of transmissions.

4.1 Performance of Active Slot Augmentation

First, we demonstrates the efficiency of the Active Slot Augmentation Mechanism(ASA). Figure 3(a) shows the delay performance of all the four methods in two modes: with the active slot Augmentation Mechanism(With-ASA) and without that mechanism(Normal). The working cycle is set $T=30$ in this experiment. we can see that the method with-ASA performs much better, and the average E2E delay of the Normal method is at least 2 times larger than the methods with-ASA. We can also notice that our method RRAD produces the lowest average E2E delay among the four methods. Figure 3(b) investigates the impact of link quality on the network performance. The number of transmissions increases when the average link quality declines, which would result the delay performance of the normal methods be poorer. Without specification, all the methods will exploits the Active Slot Augmentation Mechanism in the following experiments for fairness.

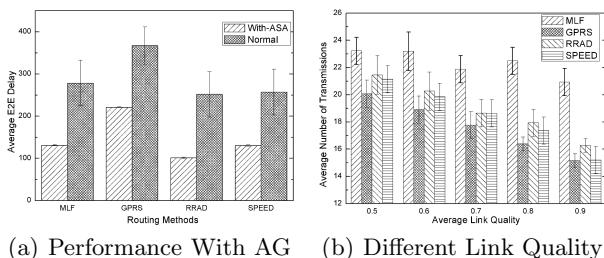


Fig. 3. Performance Of Active Slot Augmentation

4.2 Performance with Different Deadline Constraints

Figure 4 compares the performance of our method and other baseline methods under different deadline constraints. Our method without the Potential forwarder Discovering Mechanism(RRAD-N) is also evaluated to demonstrate the efficiency of the proposed mechanism. Comparing the delay performance, our method generates the lowest average E2E delay and deadline miss ratio, which demonstrates the efficacy of our method in real-time routing. Compared to the RRAD-N, Our method reduces the deadline miss ratio by almost 10%. This demonstrates the Potential forwarder Discovering mechanism is very effective in helping discovering the potential relay node to satisfy the real-time requirement. We can also find that the E2E hops and the number of E2E transmissions in MLF method is the biggest, which means it consumes the maximum energy cost. In addition, we can find the RRAD-N method performs almost the same as the SPEED method in E2E delay and the deadline miss ratio, but better in the number of E2E transmissions, this is because our method explores better on the links with both less latency and good link quality.

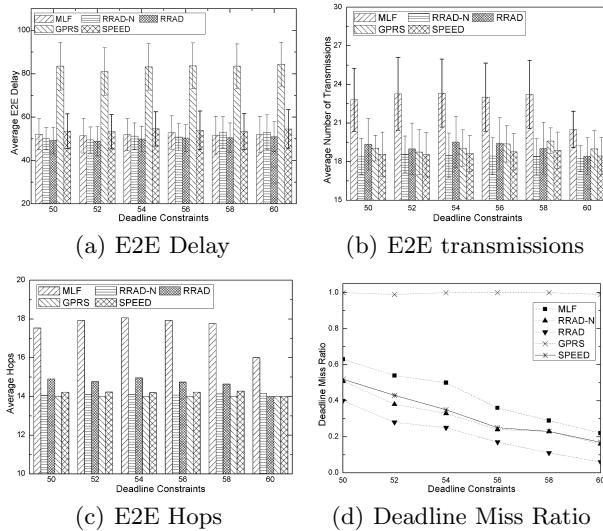


Fig. 4. Different Deadline Constraints

5 Conclusion

Real-time routing in wireless sensor networks(WSNs) is very essential and indispensable for many applications and network operations. In this paper,we propose a novel Real-Time Routing Protocol(RRAD) framework to solve the problem of real-time and reliable routing in a low-duty-cycle WSNs. Three mechanisms are implemented in a localized way to provide the QoS guarantee. Through comprehensive experiments, we demonstrate the energy efficiency and routing latency of our RRAD protocol.

Acknowledgement. The authors' work is supported in part by the Key Program of the National Natural Science Foundation of China 61190115 and 61033015.

References

1. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. *Computer Networks* 52, 2292–2330 (2008)
2. WirelessHART, http://www.hartcomm2.org/hart_protocol/wireless_hart
3. Gu, Y., He, T., Lin, M., et al.: Spatiotemporal delay control for low-duty-cycle sensor networks. In: 30th IEEE RTSS 2009, pp. 127–137. IEEE (2009)
4. Liu, X., Zhang, H., Xiang, Q., et al.: Taming uncertainties in real-time routing for wireless networked sensing and control. *IEEE Transactions on Smart Grid* (2013)
5. Dousse, O., Mannersalo, P., Thiran, P.: Latency of Wireless Sensor Networks with Uncoordinated Power Saving Mechanisms. In: Proc. ACM MobiHoc (2004)
6. Gu, Y., He, T.: Dynamic switching-based data forwarding for low-duty-cycle wireless sensor networks. *IEEE Transactions on Mobile Computing* (2011)
7. Fan, Z.: Delay-Driven Routing for Low-Duty-Cycle Sensor Networks. *International Journal of Distributed Sensor Networks* (2013)
8. He, T., Stankovic, J., Lu, C., et al.: SPEED: a stateless protocol for real-time communication in sensor networks. In: Proceedings of International Conference on Distributed Computing Systems (2003)
9. Felembane, E., Lee, C., Ekicie, E.: MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Transactions on Mobile Computing* 5(6), 738–754 (2006)
10. Cheng, S., Li, J., Cai, Z.: O(ϵ)-Approximation to Physical World by Sensor Networks. In: IEEE INFOCOM, pp. 3084–3092 (2013)
11. Cai, Z., Lin, G., Xue, G.: Improved Approximation Algorithms for the Capacitated Multicast Routing Problem. In: Wang, L. (ed.) COCOON 2005. LNCS, vol. 3595, pp. 136–145. Springer, Heidelberg (2005)
12. Cai, Z., Chen, Z., Lin, G.: A 3.4713-Approximation Algorithm for the Capacitated Multicast Tree Routing Problem. *Theoretical Computer Science* (2009)
13. Ai, C., Guo, L., Cai, Z., Li, Y.: Processing Area Queries in Wireless Sensor Networks. In: MSN (2009)
14. Li, J., Cheng, S., Gao, H., Cai, Z.: Approximate Physical World Reconstruction Algorithms in Sensor Networks. *IEEE Transactions on TPDS*
15. Wang, J., Dong, W., Cao, Z., Liu, Y.: On the Delay Performance Analysis in A Large-Scale Wireless Sensor Network. In: Proc. of IEEE RTSS 2012, San Juan, Puerto Rico, December 4–7 (2012)
16. Sun, G., Xu, B.: Dynamic Routing Algorithm for Priority Guarantee in Low Duty-Cycled Wireless Sensor Networks. In: Pandurangan, G., Anil Kumar, V.S., Ming, G., Liu, Y., Li, Y. (eds.) WASA 2010. LNCS, vol. 6221, pp. 146–156. Springer, Heidelberg (2010)
17. Karp, B., Kung, H.: Greedy Perimeter Stateless Routing for Wireless Networks. In: Proc. IEEE/ACM Conf. Mobile Computing and Networking (2000)
18. Couto, D., Aguayo, D., Bicket, J., Morris, R.: A High ThroughputPath Metric for Multi-Hop Wireless Routing. In: MobiCom 2003 (2003)
19. CC2420 Datasheet, <http://www.ti.com>

IDUC: An Improved Distributed Unequal Clustering Protocol for Wireless Sensor Networks^{*}

Chuanqing Chen¹, Xin Gu¹, Jiguo Yu^{1,2,*,} and Dongxiao Yu²

¹ School of Computer Science, Qufu Normal University,
Rizhao, Shandong, 276826, China

Chen_053189@126.com, {guxinsd,jiguoyu}@sina.com, yu@mail.qfnu.edu.cn

² Department of Computer Science, The University of Hong Kong
Pokfulam, Hong Kong, China
dxyu@cs.hku.hk

Abstract. Due to the imbalanced energy consumption among nodes in wireless sensor networks, some nodes die prematurely, which decreases the network lifetime. To solve this problem, existing clustering protocols usually construct unequal clusters by exploiting uneven competition radius. Taking their imperfection on designing the uneven competition radius and inter-cluster communication into consideration, this paper proposes an improved distributed unequal clustering protocol (IDUC) for wireless sensor networks, where nodes are energy heterogeneous and scattered unevenly. The cores of IDUC are the formation of unequal cluster topology and the construction of inter-cluster communication routing tree. Compared with previous protocols, IDUC is suitable for various network scenarios, and it can balance the energy consumption more efficiently, and extend the lifetime of networks significantly.

1 Introduction

A wireless sensor network (WSN) consists of plentiful low-power sensor nodes capable of sensing, processing and communicating. These sensor nodes observe the environment phenomenon at different points in the field, collaborate with each other and send the monitored data to the Base Station (BS). As sensor networks have limited and non-rechargeable energy resources, energy efficiency is a very important issue in designing the network topology, which affects the lifetime of WSNs greatly. Thus, how to minimize energy consumption and maximize network lifetime are the central concerns when designing protocols for WSNs.

In recent years, clustering has been proved to be an important way to decrease the energy consumption and extend lifetime of WSNs. In clustering scheme, sensor nodes are grouped into clusters, in each cluster, a node is selected as the

* The work is supported by NNSF of China for contract(61373027, 11101243) and NSF of Shandong Province for contract(ZR2012FM023).

** Corresponding author.

leader named as the cluster head (CH) and the other nodes are called cluster members (CMs). Each CM measures physical variables related to its environment and then sends them to their CHs. When the data from all CMs is arrived, CHs aggregate data and send it to the BS. Since CHs are responsible for receiving and aggregating data from their CMs, and then transmitting the aggregated data to the specified destination, the energy consumption of which is much higher than that of CMs. To solve this problem, most clustering algorithms divide the operation into rounds and periodically rotate the roles of CHs in the network to balance the unequal energy consumption among nodes. However, there exists another problem, that is, energy consumption among CHs is also imbalanced due to the distance to the BS. In single-hop networks, CHs farther away from the BS need to transmit data to a long distance. Thus, the energy consumption of these CHs is larger than that of CHs closer to the BS. In multi-hop networks, CHs closer to the BS undertake the task of forwarding data, which means that the energy consumption of CHs closer to the BS is larger. The imbalanced energy consumption of nodes leads to a certain number of nodes dying prematurely, causing network partitions. To solve this problem, researchers design unequal clustering algorithms to balance the energy consumption among CHs.

In this paper, aiming at energy heterogeneous networks where nodes are deployed unevenly, a more practical network case, we propose an improved distributed unequal clustering protocol (IDUC), in which a new competition radius and a new inter-cluster communication routing tree are designed to balance the energy consumption among CHs and extend the network lifetime.

The rest of the paper is organized as follows. Section 2 introduces the related works in this field. Section 3 gives the network model and related problem description. Section 4 presents the improved distributed unequal clustering protocol in details. Section 5 analyzes several properties of our algorithm. In Section 6, concludes the paper. In Appendix, exhibit and analyze simulation results.

2 Related Works

Since the energy consumption of CHs is much larger than that of CMs, in order to balance the energy among nodes, most clustering protocols adopt a rotation mechanism of CHs. The rotation methods used by the existing clustering algorithms can be divided into time-driven rotation and energy-driven rotation. In time-driven clustering algorithms [1-5], the role of the CH is rotated in the entire network periodically according to a predetermined time threshold. As each rotation is carried out in the entire network, the large overhead of re-cluster causes a lot of unnecessary energy waste. In energy-driven clustering algorithms [6-11], the role of CH is rotated when the residual energy of CH is less than a threshold. Re-cluster process only happens in local area, thus the large cost of global topology reconstruction can be avoided.

However, aside from the imbalance energy consumption among CHs and CMs, there also exists another imbalance consumption phenomenon among CHs that can impact the network lifetime significantly. To solve this problem, many unequal clustering algorithms have been proposed. The unequal clustering

algorithms proposed in [12-14] all divide the network field into cirques. In [12], clusters in the same cirque have the same size, whereas clusters in different cirques have different sizes. Some high-energy nodes are deployed to take on the CH role to control network operation, which ensures that the energy dissipation of nodes is balanced. In [13], a cirque-based static clustering algorithm for multi-hop WSNs is proposed. Clusters closer to the BS have smaller sizes. Utilizing virtual points in a corona-based WSN, static clusters with dynamic structures are formed in ERP-SCDS [14].

The communication way of CHs in the distributed clustering protocol EECS [15] is single-hop, and the protocol adopts a weighted faction to control the numbers of CMs to construct unequal clusters. That is, the cluster size is smaller if it is farther away from the BS, vice versa.

EEUC [16] is also a distributed unequal clustering algorithm with inter-cluster multi-hop communication, which elects CHs based on the residual energy of nodes. Each node becomes a tentative CH with a probability T . However, the competition radius used by EEUC is not ideal for heterogeneous WSNs, and since the quality of the generated CHs is affected by T , there also exists “isolate points” in EEUC in some cases. LUCA [17] is similar to EEUC but presents more accurate theoretical analysis of optimal cluster size based on the distance between the CH and the BS.

In [18], we proposed EADUC to overcome the defects of EEUC. When designing the competition radius, besides the distance between nodes and the BS, the residual energy of nodes is also taken into account. That is, CHs closer to the BS and possessing lower residual energy have smaller cluster sizes to preserve some energy for the inter-cluster data forwarding, thus the cluster size is more reasonable and more suitable for heterogeneous WSNs. Simultaneously, EADUC overcomes the “isolate points” problem.

These protocols described above, such as EEUC, only considers the distance between nodes and the BS, which is not suitable for heterogeneous networks, thus EADUC also takes residual energy of nodes into account besides the distance factor. However, they all overlook the distribution of nodes in WSNs, it is not always effective to apply these algorithms into networks where nodes are scattered unevenly.

Aiming at this problem, what we need to do is to design a protocol, which is suitable for various network scenarios, an improved distributed unequal clustering protocol (IDUC) is proposed in this paper. IDUC is effective in both heterogeneous and homogeneous network scenarios, simultaneously, it is suitable for WSNs where nodes are scattered evenly or unevenly. Our main contribution in the paper is as follows: 1) a new cluster head competition radius is proposed, it considered the distance among nodes and the BS, the residual energy of nodes and the number of neighbor nodes within the nodes’ communication range.

- 2) To meet the gap between the number of nodes within the communication ranges and the finally cluster ranges, when designing the inter-cluster routing tree, CHs will choose CH nodes that possessing higher energy and fewer CMs as their next hops.

3 Network Model and Problem Description

A. Network Model

To simplify the network model, we adopt a few reasonable assumptions as follows.

1. There are N sensor nodes that are distributed in an $M \times M$ square field.
2. The BS and all nodes are stationary after deployment.
3. All nodes can be heterogeneous.
4. All nodes are location-unaware.
5. All nodes can use power control to adjust the transmit power.
6. The BS is out of the sensor field. It has enough energy, and its location is known by each node.
7. Each node has a unique identity id .

To transmit an l -bit data to a distance d , the radio expends energy is

$$E_{Tx}(l, d) = \begin{cases} l \times E_{elec} + l \times \varepsilon_{fs} \times d^2, & d < d_0 \\ l \times E_{elec} + l \times \varepsilon_{mp} \times d^4, & d \geq d_0 \end{cases} \quad (1)$$

Where d is the transmission distance, E_{elec} , ε_{fs} and ε_{mp} are parameters of the transmission/reception circuit. According to the distance between the transmitter and receiver, free space ε_{fs} or multi-path fading ε_{mp} channel models is used. While receiving an $l - bit$ data, the radio expends energy is

$$E_{Rx}(l) = l * E_{elec}. \quad (2)$$

B. Problem Description

As described above, some clustering protocols construct unequal clustering topology by uneven cluster head competition radius. However, these protocols, such as EEUC, only considers the distance between nodes and the BS, which is not suitable for heterogeneous networks, thus EADUC also takes residual energy of nodes into account besides the distance factor. Nonetheless, if we applied these algorithms into networks where nodes are scattered unevenly, such case is very likely to appear as shown in Figure 1, if the distance between s_i and BS is near to the distance between s_j and BS, meanwhile, the residual energy of s_i and s_j is also approximate, it is notable that the number of CMs within the cluster range of s_i is much larger than s_j , which can also lead to the imbalanced consumption of s_i and s_j .

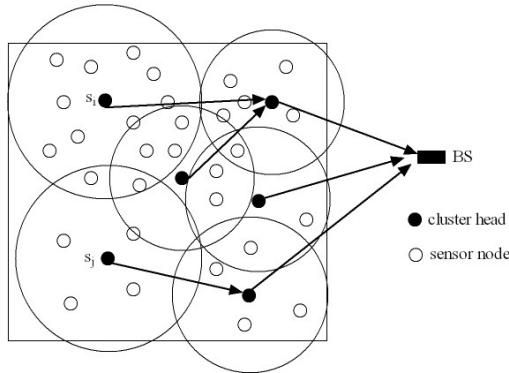


Fig.1. Imbalance energy consumption between s_i and s_j

Meanwhile, in most practical applications, the deployment of nodes in networks is not always uniform. If nodes are unevenly scattered, the nodes density is different in different area of the network. In such scenario, case appearing in Figure 1 easily happen when we applied exist clustering protocol. Thus, we need to control the number of CMs of each cluster, that is, if nodes have more communication neighbor nodes, their cluster competition radius should be smaller, vice versa. In fact, it is easy to obtain a method to solve this problem, as shown in Figure 1 that is to reduce the competition radius of s_i , and to increase the competition radius of s_j , correspondingly. With the adjustment of competition ranges, the numbers of CMs covered by s_i and s_j are all adjusted to be more reasonable. Thus, it is necessary to design a new CH competition radius for such networks, besides the distance from the nodes to BS and the residual energy of nodes, we also take the number of neighbor nodes within the nodes' communication range into account.

However, we have to admit that the number of neighbor nodes within the node initial communication range is very likely to be not equal with the number of CMs within its finally cluster range. Thus, to further balance the consumption among CHs, when we construct the inter-cluster multi-hop routing tree, each CH needs to count the number of its CMs, and then it chooses the neighbor CH with fewer CMs and higher residual energy as its next hop.

4 IDUC Details

The whole operation is divided into rounds, where each round contents a cluster set-up phase and a data transmission phase. In the cluster set-up phase, a clustering topology is formed, and in the data transmission phase, a new routing tree is constructed to forward data. To save energy, the data transmission phase should be longer than the cluster set-up phase. The description of node states and several control messages are shown in Table 1, respectively.

Table 1. Description of control messages

Message	Description
<i>Node_Msg</i>	Tuple(selfid, selfenergy)
<i>Head_Msg</i>	Tuple(selfid)
<i>Join_Msg</i>	Tuple(selfid, headid)
<i>Schedule_Msg</i>	Tuple(schedule, order)
<i>Route_Msg</i>	Tuple(selfid, selfenergy)

A. Cluster Set-up Phase

In the network deployment phase, the BS broadcasts a signal, each node can compute its approximate distance to the BS based on the received signal strength, this step is necessary when designing an unequal distributed clustering algorithm. The following is the cluster set-up phase. The first sub-phase of this phase is information collection phase, whose duration is set as T_1 . At the beginning of this phase, each node broadcasts a *Node_Msg* message within its communication range r , the message contains the node id and its residual energy. Meanwhile, the node will receive *Node_Msgs* from its neighbor nodes, and each node calculates the average residual energy E_{ia} of its neighbor nodes by using the following formula.

$$E_{ia} = \frac{1}{n} * \sum_{j=1}^n E_{jr}. \quad (3)$$

Where n denotes the number of neighbor nodes of s_i , E_{jr} denotes the residual energy of the j th neighbor of s_i . For any node s_i , it calculates its waiting time t_i for broadcasting the *Head_Msg* message according to the following formula.

$$t_i = \begin{cases} \frac{E_{ia}}{E_{ir}} T_2 V_r, & E_{ir} \geq E_{ia} \\ T_2 V_r, & E_{ir} < E_{ia} \end{cases} \quad (4)$$

Where V_r is a real value randomly distributed in $[0.9, 1]$, which is introduced to reduce the probability that two nodes send *Head_Msgs* at the same time. After T_1 expires, it starts the next sub-phase, cluster head competition phase, whose duration is set as T_2 . In this phase, for any node s_i , if it receives no *Head_Msg* when time t_i expires, it broadcasts the *Head_Msg* within competition range R_c to advertise that it will be a CH. Otherwise, it gives up the competition. In order to generate unequal clusters, these nodes need to calculate their own competition radius R_c . In [15], based on the distance between nodes and BS, the formula of R_c is as follows.

$$R_C = [1 - \alpha \frac{d_{max} - d(s_i, BS)}{d_{max} - d_{min}}] R_{max}. \quad (5)$$

Where d_{max} and d_{min} are the maximum and minimum distance from nodes to the BS, $d(s_i, BS)$ is the distance from node s_i to the BS, α is a weighted factor

whose value is in $[0, 1]$, and R_{max} is the maximum value of competition radius. By analyzing the formula (5), we can obtain that a larger $d(s_i, BS)$ can generate a larger R_C , which can guarantee that CHs farther away from the BS will control larger cluster areas, whereas CHs closer to the BS can control smaller cluster areas.

In heterogeneous networks, nodes have heterogeneous initial energy. In the case that each node has the same energy consumption, nodes with low initial energy will die prematurely, reducing the network lifetime. In order to take full advantage of high-energy nodes, these high-energy nodes should take more tasks. Therefore, considering both the distance from nodes to the BS and the residual energy of nodes, we gave an improved formula of R_C in EADUC [18] as follows.

$$R_C = [1 - \alpha \frac{d_{max} - d(s_i, BS)}{d_{max} - d_{min}} - \beta(1 - \frac{E_{ir}}{E_{max}})]R_{max}. \quad (6)$$

Where α and β is the weighted factors in $[0, 1]$, E_{ir} is the residual energy of node s_i . From the above formula we can see that the competition radius of the node is determined by $d(s_i, BS)$ and E_{ir} . Formula (6) means that CHs with higher residual energy and farther away from the BS will control larger cluster area.

However, the cluster competition radius R_c designed above are all not suitable for networks where nodes are scattered unevenly, especially when the distance between these nodes and BS is similar, and the residual energy of these nodes is also approximate. Thus, we need to design a new competition radius to avoid imbalanced energy consumption in such case.

Meanwhile, another remarkable problem generated in EADUC is that there is not a restriction on the relation of α and β , thus in such case where both $\frac{d_{max} - d(s_i, BS)}{d_{max} - d_{min}}$ and $1 - \frac{E_{ir}}{E_{max}}$ are large, and their weighted factor and are also large, then the R_c we obtain is likely to be a negative value, which is not meaningful in practical applications, therefore, it is necessary to give a limit on the relation of α and β . Aiming at above disadvantages of existing R_c , we propose a new cluster head competition radius R_c , which is set as follows.

$$R_C = [1 - \alpha \frac{d_{max} - d(s_i, BS)}{d_{max} - d_{min}} - \beta(1 - \frac{E_{ir}}{E_{max}}) - \gamma(\frac{n_i}{N - n_i})]R_{max}. \quad (7)$$

Where N denotes the number of nodes in the network, n_i is the number of neighbor nodes within the communication range of s_i . α , β and γ is the weighted factors in $[0, 1]$, and we set $\alpha + \beta + \gamma \leq 1$. Formula (7) means that CHs closer to the BS, with lower residual energy and more communication neighbor nodes will have smaller cluster size. In conclusion, firstly, CHs closer to the BS can save energy for data forwarding. Secondly, CHs with lower residual energy dominating smaller clusters can avoid their premature death and prolong the network lifetime. Thirdly, CHs with more communication neighbor nodes control smaller clusters, which makes the competition radius more suitable for nonuniform networks. Obviously, R_c in formula (7) makes IDUC suitable for various network scenarios:

- (1) If the network is energy homogeneous, we can set $\beta = 0$ and $\alpha + \gamma \leq 1$.
- (2) If the distribution of nodes in the network is uniform, we can set $\gamma = 0$ and $\alpha + \beta \leq 1$.

(3) If nodes in the network is energy homogeneous and the distribution is nonuniform, we can set $\alpha + \beta + \gamma \leq 1$.

According to practical network applications, we can adjust α , β and γ , and to be the optimal value to extend the network lifetime.

When T_2 expires, the next sub-phase is the cluster formation phase, whose duration is T_3 . In this phase, each plain node chooses the nearest CH and sends the *Join_Msg*, which contains the id and its residual energy. According to the received *Join_Msgs*, each CH creates a node schedule list including the *Schedule_Msg* for its CMs. At this point, the entire cluster set-up phase is completed. The following pseudo-codes give the details of the whole cluster set-up phase.

```

begin (cluster set-up algorithm)
    state  $\leftarrow$  Plain
    Broadcast the Node_Msg
    while ( $T_1$  has not expired)
        Receive Node_Msgs
        Update neighborhood table NT[ ]
    end while
     $t_i \leftarrow$  broadcast waiting time for competing a CH
    while ( $T_2$  has not expired)
        if CurrentTime  $< t_i$ 
            if receive a Head_Msg from a neighbor NT[i]
                state  $\leftarrow$  Plain
                NT[i].state  $\leftarrow$  CH
            else
                Continue
            end if
        else if state = Plain
            state  $\leftarrow$  CH
             $R_c \leftarrow$  competing radius
            Broadcast the Head_Msg
        end if
    end while
    while ( $T_3$  has not expired)
        if state = Plain&& has not sent Join_Msg
            Send Join_Msg to the nearest CH
        else
            Receive Join_Msg from its neighbor nodes
        end if
    end while
    if state = CH
        Broadcast the Schedule_Msg
    end if
end
```

B. Data Transmission Phase

In the data transmission phase, each CM collects local data from the environment periodically and then sends the data to the CH within its time slot according to the TDMA scheduling list to avoid the collisions among the members in the same cluster. When data from all the member nodes has arrived, the CH aggregates the data and sends it to the BS. Thus, this section is divided into two sub-phases, *intra-cluster communication* and *inter-cluster communication*. CMs sense and collect local data from the environment, and send the collected data to CHs. This process is called intra-cluster communication. For simplification, CMs communicate with CHs directly, just like LEACH.

In inter-cluster communication phase, we will construct a routing tree on the elected CH set, each CH will forward these data they have collected and aggregated from their CMs to the BS by other CHs. This multi-hop communication from CHs to the BS will further reduce and balance the energy consumption.

Several nodes need to be selected as child nodes of the BS from all CHs, and communicate with the BS directly. Therefore, each CH determines whether to be selected as the child node of the BS depending on its distance to the BS according to a threshold Euclidean distance $DIST$. If the distance from CH s_i to the BS is less than $DIST$, s_i communicates with the BS directly, and sets the BS as its next hop. Otherwise, it communicates with the BS through a multi-hop routing tree.

The concrete process is as follows. We set the duration as T_4 . At the beginning, each CH broadcasts a *Route_Msg* message within the radio radius R_r with the values of the id, the residual energy and the distance to the BS. To ensure the connectivity of all CHs, we set the radio radius $R_r = 3R_c$. If the distance from CH s_i to the BS is less than $DIST$, it chooses the BS as its next hop. Otherwise, it chooses its next hop according to these received *Route_Msgs*. CH s_i chooses the neighbor CH with higher residual energy, fewer CMs and no farther away from the BS as its next hop. We give the formula of “Cost” when CH s_i chooses CH s_j as its next hop as follows

$$Cost(s_i, s_j) = \omega \frac{E_{jr}}{E_{max}} + (1 - \omega)(1 - \frac{n_j}{N}) \quad (8)$$

Where E_{jr} denotes the residual energy of CH s_j , n_j denotes the number of CMs of s_j . ω is a random value in $[0,1]$, and it is used to determine which factor is more important in choosing the next routing node. We can obtain from (8) that, nodes with higher residual energy and fewer CMs have larger cost value.

```

begin (cluster-based routing algorithm)
  Broadcast the Router_Msg
  if (disttoBS < DIST)
    nexthop  $\leftarrow$  BS
  else
    while(T has not expired)
      Receive Router_Msgs
    
```

```

        Compute the cost
        Update CH neighborhood table  $CHNT[]$ 
end while
end if
if  $s_j$  has the max value of cost in  $CHNT[]$ 
    &&  $s_j$  has a smaller  $disttoBS$  in  $CHNT[]$ 
    Update MR[]
end if
end

```

5 Protocol Analysis

Theorem 1. *There is at most one CH within each cluster competition radius R_c .*

Proof. As we state previously, formula (4) ensures that different nodes have different waiting time. Assume that node s_i has a shorter waiting timer than others and broadcasts the *Head_Msg* within radius R_c . Thus, all nodes within this range will give up the competition and become plain nodes. Therefore, there is no more than one CH within the radius R_c of any CH.

Theorem 2. *The cluster head set generated by the IDUC algorithm is a dominating set.*

Proof. According to theorem 1, there is no more than one CH within a cluster, so the cluster head set must be an independent set. After the execution of the IDUC algorithm, each node in the network either is the CH, or the member node of one cluster, any plain node adding to the cluster head set will destroy its independence. Hence, the cluster head set is the maximum independent set. Since the maximum independent set is also a dominating set, the cluster head set generated by the IDUC algorithm is a dominating set.

Theorem 3. *The cluster head set generated by IDUC can cover all the network nodes.*

Proof. (a) When $E_{ir} \geq E_{ia}$, we have $t_i = \frac{E_{ia}}{E_{ir}} T_2 V_r$ according to formula(4). Thus, we can obtain $t_i \leq T_2$ since $V_r \leq 1$. (b) When $E_{ir} \leq E_{ia}$, we have $t_i = T_2 V_r$ according to formula(4). Thus $t_i \leq T_2$, since $V_r \leq 1$.

Therefore, we conclude that the waiting time of any node is smaller than T_2 . That is, any expected CH will broadcast a *Head_Msg* and become a CH before T_2 expired, which can avoid the generation of “isolate points”.

Theorem 4. *The overhead complexity of control message in the network is $O(N)$ and the time complexity of IDUC is $O(1)$.*

Proof. At the beginning of each round, each node broadcasts a *Node_Msg*. Thus, there are N *Node_Msgs* in the whole network. In each round, each CM broadcasts a *Join_Msg*, while each CH broadcasts a *Head_Msg*, a *Schedule_Msg* and a *Route_Msg*. Suppose the number of generated CHs is k , then the total number of *Join_Msgs* is $N - k$, and the numbers of *Head_Msgs*, *Schedule_Msgs* and *Route_Msgs* messages are all k . Thus, the total number of control messages in the entire network is $N + (N - k) + k + k + k = 2N + 2k$. Therefore, the overhead complexity of control messages in the network is $O(N)$.

6 Conclusion

In this paper, an improved distributed unequal clustering protocol is proposed, we design a new cluster competition radius considering the distance between nodes and the BS, the residual energy of nodes and the numbers of neighbor nodes within the node communication range. Furthermore, to bridge the gap between the numbers of nodes within the initial communication radius and the finally cluster radius, we design a new inter-cluster communication routing tree. Theoretical analysis and simulation show that, the protocol is suitable for various network scenarios, In these scenarios, the nodes energy can be efficiently balanced and the network lifetime can be extended significantly.

References

- Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proc. of HICSS, pp. 1–10 (February 2000)
- Younis, O., Fahmy, S.: Heed: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. IEEE Trans. on Mobile Computing 3(4), 660–669 (2004)
- Liu, M., Cao, J., Chen, G.: EADEEG: An energy-aware data gathering protocol for wireless sensor networks. Journal of Software 18(5), 1092–1109 (2007)
- Kumar, D., Trilok, C., Patel, R.B.: EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks. Computer Commun. 32, 662–667 (2009)
- Zhou, X., Wu, M., Xu, J.: BPEC: An energy-aware distributed clustering algorithm in WSNs. J. of Compu. Research and Development 46(5), 723–730 (2009)
- Wu, Y., Chen, Z., Jing, Q.: LENO: Least rotation near optimal cluster head rotation strategy in wireless sensor networks. In: Proc. of AINA (2007)
- Wang, L., Wei, R., Tian, Z.: Cluster based node scheduling method for wireless sensor networks. Science China Information Sciences 55(4), 755–764 (2012)
- Gamwarige, S., Kulasekere, E.: An algorithm for energy driven cluster head rotation in a distributed wireless sensor network. In: Proc. of ICIA, pp. 354–359 (2005)
- Huang, H., Shen, J.: An energy-driven adaptive cluster head rotation alforithm for wireless sensor networks. J. of Electr. Inform. Tech. 31(5), 1040–1044 (2009)
- Yu, J., Qi, Y., Wang, G.: An energy-driven unequal clustering protocol for heterogeneous wireless sensor networks. J. Control Theory Appl. 9(1), 133–139 (2011)
- Yu, J., Qi, Y., Wang, G., Gu, X.: A cluster-based routing protocol for wireless sensor networks with non-uniform node distribution. Inter'l J. of Electr. and Commun. 66, 54–61 (2012)

12. Qian, Y., Zhou, J., Qian, L., Chen, K.: Prolonging the lifetime of wireless sensor network via multihop clustering. In: Koucheryavy, Y., Harju, J., Iversen, V.B. (eds.) NEW2AN 2006. LNCS, vol. 4003, pp. 118–129. Springer, Heidelberg (2006)
13. Xiang, M.: Energy efficient clustering algorithm for maximizing lifetime of wireless sensor networks. *Inter'l J. of Electr. and Commun.* 64(4), 289–298 (2010)
14. Ferng, H.W., Tendean, R., Kurniawan, A.: Energy-efficient routing protocol for wireless sensor networks with static clustering and dynamic structure. *Wireless Pres. Commun.* 65(2), 347–367
15. Ye, M., Li, C.F., Chen, G.H., Wu, J.: EECS: An energy efficient clustering scheme in wireless sensor networks. In: Proc. of the IPCCC 2005, pp. 535–540 (2005)
16. Li, C.F., Ye, M., Chen, G.H., Wu, J.: EEUC: An energy-efficient unequal clustering mechanism for wireless sensor networks. In: Proc. of the IEEE MASS 2005, pp. 1–8 (2005)
17. Lee, S., Choe, H., Park, B., Song, Y., Kim, C.K.: LUCA: An Energy-efficient unequal clustering algorithm using location information for wireless sensor networks. *Wireless Pers. Commun.* 56, 715–731 (2011)
18. Yu, J., Qi, Y., Guo, Q., Gu, X.: EADUC: An energy-aware distributed unequal clustering protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks* (2011), doi:10.1155/2011/202145
19. Gamwarige, S., Kulasekere, E.: An algorithm for energy driven cluster head rotation in a distributed wireless sensor network. In: Proc. of the ICIA 2005, pp. 354–359 (2005)

OFDP: A Distributed Algorithm for Finding Disjoint Paths with Minimum Total Energy Cost in Wireless Sensor Networks^{*}

Kejia Zhang^{1,2}, Hong Gao², Guisheng Yin¹, and Qilong Han¹

¹ College of Computer Science and Technology,
Harbin Engineering University, Harbin, China

² School of Computer Science and Technology,
Harbin Institute of Technology, Harbin, China

Abstract. This paper investigates the MINimum-energy-cost- k -Disjoint-Paths (MIN- k -DP) problem : in a sensor network, given two nodes s and t , a positive integer k , finding k (node) disjoint paths connecting s and t with minimum total energy cost. An efficient distributed algorithm named Optimally-Finding-Disjoint-Paths (OFDP) is proposed for this problem. OFDP guarantees *correctness* and *optimality*, i.e., 1) it will find k disjoint paths if there exist k disjoint paths in the network or the maximum number of disjoint paths otherwise; 2) the disjoint paths it outputs do have minimum total energy cost. To the best of our knowledge, OFDP is the first distributed algorithm that can solve the MIN- k -DP problem with correctness and optimality guarantee. Compared with the existing centralized algorithms which also guarantee correctness and optimality, OFDP is shown to be much more efficient by simulation results.

1 Introduction

Let s and t denote a routing request in a wireless sensor network (WSN), i.e., two sensor nodes who want to communicate with each other. The main objective of routing is to optimally find paths connecting s and t , i.e., $s \sim t$ paths. A set of $s \sim t$ paths are (node) disjoint if any two of them do not have any common nodes except s and t .

Compared with transmitting data through a single path, transmitting data through multiple disjoint paths can increase throughput, robustness, and load balance of routing in WSNs. In addition to being disjoint, the users always want the paths used for routing to have minimum total energy cost. For example, to improve load balance, k disjoint paths are alternately used for relaying messages between s and t . The energy cost to transmit every k messages is the sum of the energy cost of these paths. Besides improving load balance, the users always

* This work is supported by National Natural Science Foundation of China (Grant No. 61300207), Fundamental Research Funds for the Central Universities (Grant No. HEUCF100610).

want to use minimum energy to relay messages, i.e., these paths have minimum total energy cost.

This paper investigates the MINimum-energy-cost- k -Disjoint-Paths (MIN- k -DP) problem: in a WSN, given two nodes s and t , a positive integer k , finding k disjoint $s \sim t$ paths with minimum total energy cost. We expect that the MIN- k -DP problem can be solved with *correctness* and *optimality* guarantee. By “correctness”, we mean that an algorithm will output k disjoint paths if there exist k disjoint paths in the network or the maximum number of disjoint paths otherwise. By “optimality”, we mean that the disjoint paths output by an algorithm do have minimum total energy cost.

In recent years, the problem of finding multiple disjoint $s \sim t$ paths has become more and more widely researched [8,13,1,6,7,14,15,12,16,2,11,10,17,5,9,3,4].

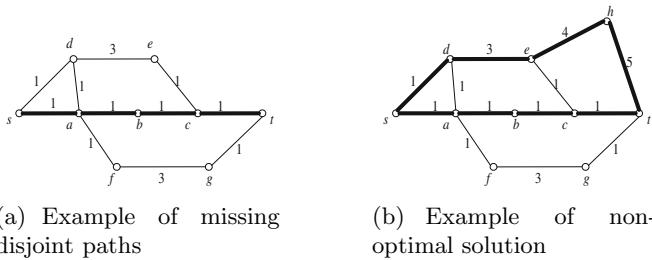


Fig. 1. Two sensor networks (the numbers on the edges denote the energy cost of the corresponding links)

For general k , some distributed algorithms are proposed in [8,13,1,15,6,7,14,12] for finding k disjoint $s \sim t$ paths in a network. However, they do not consider the energy cost of the routing paths. These algorithms have the same basic idea. They find paths one by one. Once a path is found, it is fixed and all its internal nodes are removed from the network so that they cannot participate in another path. To solve the MIN- k -DP problem, these algorithms (we let these algorithms find the $s \sim t$ path with minimum energy cost in each iteration) can guarantee neither correctness nor optimality. For example, the users want to find two disjoint $s \sim t$ paths in the given network as shown in Figure 1(a). Using these algorithms, we will find the first path $P = (s, a, b, c, t)$ as shown by bold lines in Figure 1(a). Then we cannot find another $s \sim t$ path disjoint from P , so we have to report nonexistence of two disjoint paths. In fact, there do exist two disjoint paths (s, d, e, c, t) and (s, a, f, g, t) in the network. As another example, the users want to find two disjoint $s \sim t$ paths with minimum total energy cost in the given network as shown in Figure 1(b). Using these algorithms, we will find the first path $P_1 = (s, a, b, c, t)$ and the second path $P_2 = (s, d, e, h, t)$ as shown by bold lines in Figure 1(b). The total energy cost of P_1 and P_2 is $4 + 13 = 17$. However, the optimal answer should be $P'_1 = (s, d, e, c, t)$ and $P'_2 = (s, a, f, g, t)$ with total energy cost $6 + 6 = 12$.

In [16,2,11,10,17,5,9], some centralized algorithms are given for finding k disjoint $s \sim t$ paths in graphs. All these algorithm guarantee correctness. In particular, the algorithms in [16,2,17,9] will find k disjoint $s \sim t$ paths with the minimum total length (energy cost), i.e., they guarantee both correctness and optimality. If we use these centralized algorithms to solve the MIN- k -DP problem in a WSN, we have to collect every node's neighbor list to build the topology of the whole network. The communication cost of such operation is very high for a large-scale network. On the other hand, to guarantee correctness, we have to update the network's topology with each topology change such as link failing, link recovering, node dying and new node joining in. Since these topology changes happen frequently in WSNs, we need to pay a lot of communication to make the topology we built up-to-date.

To solve the MIN- k -DP problem, all the existing distributed algorithms [8,13,1,15,6,7,14,12] (some of them are very communication-efficient) can guarantee neither correctness nor optimality. Although some centralized algorithms [2,17,9] can solve the problem with correctness and optimality guarantee, they need to build the topology of the whole network and update it with every topology change, so their communication cost is overwhelming for a large-scale WSN. Therefore, we have two challenges to solve the MIN- k -DP problem in WSNs: 1) to guarantee correctness and optimality, 2) to maintain communication-efficiency.

In this paper, we propose an efficient distributed algorithm named Optimally-Finding-Disjoint-Paths (OFDP) for the MIN- k -DP problem with correctness and optimality guarantee. OFDP finds disjoint paths in a totally distributed manner, i.e., each node participates by exchanging short messages with its neighbors and the exchange of messages does not rely on any pre-defined structures. OFDP is very communication-efficient and can adapt to topology changes with no extra cost. Simulation results confirm the communication-efficiency of OFDP. As far as we know, OFDP is the first totally distributed algorithm which can solve the MIN- k -DP problem with correctness and optimality guarantee.

2 Preliminaries

The given sensor network can be expressed as a weighted undirected graph $G = (V, E)$, where V is the set of sensor nodes and E is the set of wireless links (edges). Function $l : E \rightarrow \mathbb{R}^+$ defines the edges' lengths, i.e., the energy cost of the corresponding links. A path P in G is a subgraph which can be expressed as a sequence of distinct nodes $P = (v_1, \dots, v_m)$, where $v_i \in V$ and $(v_i, v_{i+1}) \in E$. The length of path P is the sum of its edges' lengths, i.e., $l(P) = \sum_{e \in P} l(e)$. Now the MIN- k -DP problem becomes finding k disjoint $s \sim t$ paths with minimum total length.

Although we model the given network as an undirected graph, we still emphasize the direction of a path by nodes' order in its expression or the words "from" and "to". Thus, the direction of path $P = (v_1, \dots, v_{i-1}, v_i, v_{i+1}, \dots, v_m)$ is from v_1 to v_m . v_i 's previous hop in P is v_{i-1} and its next hop in P is v_{i+1} . The direction of each $s \sim t$ path is from s to t .

Suppose that we have found n disjoint $s \sim t$ paths P_1, \dots, P_n in G . The nodes (edges) in the found paths are called *occupied nodes (edges)*, the other nodes are called *free nodes (edges)*. Let v be an occupied node. We respectively use $\text{prev}(v)$ and $\text{next}(v)$ to denote v 's previous hop and next hop in the found path v belongs to. A *forward segment* is a segment (for at least one hop) of some found path along the direction from s to t . A *backward segment* is a segment of some found path along the direction from t to s . In the network as shown in Figure 2, after finding the first $s \sim t$ path $P_1 = (s, a, b, c, t)$ as shown by bold lines in Figure 2(a), b is an occupied node. $\text{prev}(b) = a$ and $\text{next}(b) = c$. (a, b, c) is a forward segment and (c, b, a) is a backward segment.

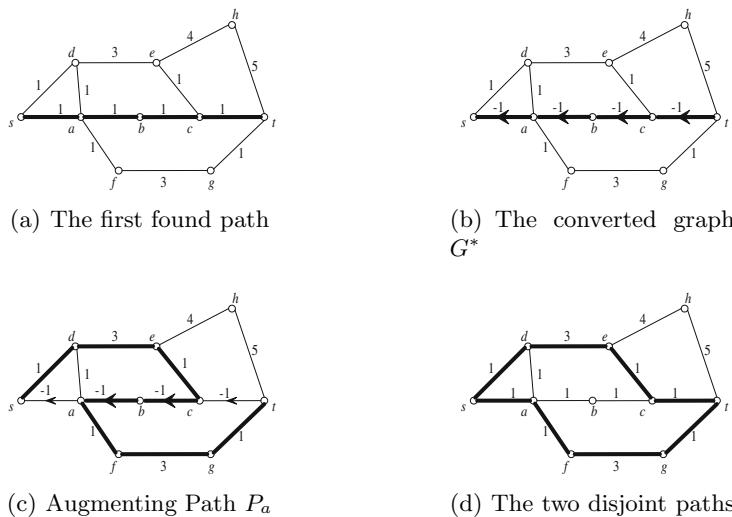


Fig. 2. An example of finding disjoint $s \sim t$ paths with minimum total length ($k = 2$)

After finding some disjoint $s \sim t$ paths, we can convert the original graph G to another graph G^* by replacing each occupied edge with a directed edge along the direction from t to s . The length of each directed edge is set to the opposite number of the original length. In the example of Figure 2(a), after finding P_1 , we convert G to G^* as shown in Figure 2(b). P_1 becomes a “river” flowing from t to s . Actually, G^* is another way to interpret G . In the following, we do not distinguish the path in G and its corresponding path in G^* . However, a path has different lengths in these two graphs. For a path P , we use $l(P)$ to denote the length of P in G and use $l^*(P)$ to denote the length of P in G^* .

A path in G^* follows the *Crossing Restriction* if it does not go through any occupied nodes except by going through a backward segment. The paths following the Crossing Restriction are called *CR-paths*. For example, after finding P_1 , in the converted graph as shown in Figure 2(b), the path $Q_1 = (s, d, a, f)$ is not a CR-path because it goes through occupied node a by directly crossing P_1 . The

path $Q_2 = (s, d, e, c, t)$ is not a CR-path either because it goes through occupied node c by going through forward segment (c, t) . The path $P = (s, d, e, c, b, a, f)$ is a CR-path because it goes through occupied nodes c, b, a by going through backward segment (c, b, a) .

An CR-path from s to t is an *augmenting path*. We can get $n + 1$ disjoint $s \sim t$ paths by adding an augmenting path P_a to the found paths P_1, \dots, P_n , where “add” means adding the edges that only belong to P_a and removing the overlapping edges of P_a and P_1, \dots, P_n . In the example of Figure 2(a), after finding the first path $P_1 = (s, a, b, c, t)$, we can find an augmenting path $P_a = (s, d, e, c, b, a, f, g, t)$ as shown by bold lines in Figure 2(c). By adding P_a to P_1 , we can get two disjoint $s \sim t$ paths $P'_1 = (s, d, e, c, t)$ and $P'_2 = (s, a, f, g, t)$ as shown by bold lines in Figure 2(d).

Lemma 1. *After finding n disjoint $s \sim t$ paths, there exist more than n disjoint $s \sim t$ paths iff there exists an augmenting path [10].*

According to how we get one more disjoint $s \sim t$ path by adding an augmenting path to the paths found before, we have the following lemma.

Lemma 2. *Suppose that after finding n disjoint $s \sim t$ paths P_1, \dots, P_n , there is an augmenting path P_a . Let P'_1, \dots, P'_{n+1} be the $n + 1$ disjoint $s \sim t$ paths generated by adding P_a to P_1, \dots, P_n . Then $l^*(P_a) + \sum_{i=1}^n l(P_i) = \sum_{i=1}^{n+1} l(P'_i)$.*

Hereinafter, we use the term “the shortest augmenting path / CR-path” to denote the shortest augmenting path / CR-path w.r.t. l^* . According to Lemma 1 and Lemma 2, we can solve the MIN- k -DP problem with correctness and optimality guarantee by repeatedly searching for the shortest augmenting path P_a and adding P_a to the paths found before.

3 Distributed Algorithm

In the given network G with two specified nodes s and t , a positive integer k , the algorithm OFDP will output $\min\{k, k^*\}$ disjoint $s \sim t$ paths with minimum total length. Here, we assume that there exist up to k^* disjoint $s \sim t$ paths in the given network. OFDP runs in a totally distributed manner, i.e., each node

Algorithm 1. Optimally-Finding-Disjoint-Paths (OFDP)

Input: two nodes s and t ; a positive integer k

Output: $\min\{k, k^*\}$ disjoint $s \sim t$ paths with minimum total length

- ```

1 repeat
2 Each node executes Procedure Finding-Shortest-Augmenting-Path;
3 if cannot find an augmenting path then
4 Stop and output all the found paths;
5 Each node executes Procedure Tracing-Shortest-Augmenting-Path;
6 until Finding k disjoint $s \sim t$ paths;
```
-

participating by exchanging short messages with its neighbors and the exchange of information does not rely on any pre-defined structures.

OFDP finds disjoint paths by iteratively searching for the shortest augmenting path  $P_a$  and adding  $P_a$  to the paths found before. There are two phases in each iteration. In Phase 1, each node executes Procedure Finding-Shortest-Augmenting-Path to find the shortest augmenting path  $P_a$ . In Phase 2, each node executes Procedure Tracing-Shortest-Augmenting-Path to add  $P_a$  to the paths found before and generate more disjoint paths. OFDP is given by Algorithm 1.

### 3.1 Finding Shortest Augmenting Path

In Phase 1 of each iteration, each node executes Procedure Finding-Shortest-Augmenting-Path to find the shortest CR-path from  $s$  to itself. In the end, we will find the shortest augmenting path.

---

#### Procedure. Finding-Shortest-Augmenting-Path

---

```

1 s broadcasts a FIND-SAP message $\{0\}$;
2 while $v \neq s$ receives a FIND-SAP message $\{dist(u)\}$ from u do
3 case v is a free node:
4 $dist(v) \leftarrow dist(u) + l(u, v)$;
5 if $dist(v) < \text{FN_}dist(v)$ then
6 $\text{FN_phcr}(v) \leftarrow u$;
7 $\text{FN_}dist(v) \leftarrow dist(v)$;
8 Broadcast a FIND-SAP message $\{dist(v)\}$;
9 case v is an occupied node and u is not $prev(v)$ or $next(v)$:
10 $dist(v) \leftarrow dist(u) + l(u, v)$;
11 if $dist(v) < \text{FHB_}dist(v)$ then
12 $\text{FHB_phcr}(v) \leftarrow u$;
13 $\text{FHB_}dist(v) \leftarrow dist(v)$;
14 if v is not t then
15 Send a FIND-SAP message $\{dist(v)\}$ to $prev(v)$;
16 case v is an occupied node and u is $next(v)$:
17 $dist(v) \leftarrow dist(u) - l(u, v)$;
18 if $dist(v) < \text{OHB_}dist(v)$ then
19 $\text{OHB_phcr}(v) \leftarrow u$;
20 $\text{OHB_}dist(v) \leftarrow dist(v)$;
21 Broadcast a FIND-SAP message $\{dist(v)\}$;

```

---

To make sure the path we found follows the Crossing Restriction, we divide the nodes in a CR-path into three categories: Free Node (FN), First Hop of a Backward segment (FHB) and Other Hops of a Backward segment (OHB). In the example of Figure 2, for CR-path  $P_a = (s, d, e, c, b, a, f, g, t)$ , the nodes  $\{d, e, f, g\}$  are FNs, node  $c$  is a FHB, and the nodes  $\{b, a\}$  are OHBs.

Each free node  $v$  maintains variables  $\text{FN\_phcr}(v)$  and  $\text{FN\_}dist(v)$ .  $\text{FN\_}dist(v)$  records the length of the shortest CR-path from  $s$  to  $v$ , and  $\text{FN\_phcr}(v)$

records  $v$ 's previous hop in the CR-path. Each occupied node  $v$  maintains variables  $\text{FHB\_phcr}(v)$ ,  $\text{FHB\_dist}(v)$ ,  $\text{OHB\_phcr}(v)$  and  $\text{OHB\_dist}(v)$ .  $\text{FHB\_dist}(v)$  records the length of the shortest CR-path from  $s$  to  $v$  with  $v$  as a FHB, and  $\text{FHB\_phcr}(v)$  records  $v$ 's previous hop in the CR-path.  $\text{OHB\_dist}(v)$  records the length of the shortest CR-path from  $s$  to  $v$  with  $v$  as an OHB, and  $\text{OHB\_phcr}(v)$  records  $v$ 's previous hop in the CR-path.

The nodes find the shortest CR-paths from  $s$  to themselves by exchanging FIND-SAP messages. Each FIND-SAP message (let the sender be  $u$ ) has a 2-byte data field to record  $dist(u)$ , which is the length of the shortest CR-path from  $s$  to  $u$  found by now.

$s$  broadcasts FIND-SAP message  $\{0\}$  to start the process (Line 1 in Procedure Finding-Shortest-Augmenting-Path). If a node  $v \neq s$  receives a FIND-SAP message  $\{dist(u)\}$  from  $u$ , it means that  $v$  finds a new path from  $s$  to  $v$  with  $u$  as its previous hop in the path. Let the new path be  $Q$ .  $u$  sends out this FIND-SAP message because it has found a CR-path from  $s$  to  $u$  with  $l^*$ -length  $dist(u)$ , so the segment from  $s$  to  $u$  in  $Q$  follows the Crossing Restriction. Next, we discuss in the following four cases while node  $v \neq s$  receives a FIND-SAP message  $\{dist(u)\}$  from  $u$ .

Case 1:  $v$  is a free node. As a FN in a CR-path,  $v$ 's previous hop in the path could be any neighbor of  $v$ , so the segment  $(u, v)$  of  $Q$  also follows the Crossing Restriction and  $Q$  a CR-path. The length of  $Q$  w.r.t.  $l^*$  is  $l^*(Q) = dist(u) + l(u, v)$ , and we use variable  $dist(v)$  to record it (Line 4 in Procedure Finding-Shortest-Augmenting-Path). If  $dist(v) < \text{FN\_dist}(v)$ , i.e.,  $Q$  is shorter than the shortest CR-path from  $s$  to  $v$  found by now, then  $Q$  should be the new shortest CR-path from  $s$  to  $v$ . In this situation, we set  $\text{FN\_phcr}(v)$  to  $u$  (Line 6 in Procedure Finding-Shortest-Augmenting-Path). The length of the shortest CR-path from  $s$  to  $v$  should be updated as  $\text{FN\_dist}(v) = dist(v)$  (Line 7 in Procedure Finding-Shortest-Augmenting-Path). Since  $v$  is a FN in  $Q$ , to further extend  $Q$  as a CR-path, the next hop of  $v$  could be any neighbor of  $v$ , so we let  $v$  broadcast a FIND-SAP message  $\{dist(v)\}$  (Line 8 in Procedure Finding-Shortest-Augmenting-Path).

Case 2:  $v$  is an occupied node and  $u$  is  $prev(v)$ . Since  $u = prev(v)$ , the segment  $(u, v)$  of  $Q$  is a forward segment of some found path. Thus,  $Q$  is not a CR-path and we let  $v$  discard the message in this case.

Case 3:  $v$  is an occupied node and  $u$  is not  $prev(v)$  or  $next(v)$ . As an occupied node in a CR-path,  $v$ 's previous hop in the path could be any neighbor besides  $prev(v)$ , so the segment  $(u, v)$  of  $Q$  follows the Crossing Restriction and  $Q$  is a CR-path. Since  $u$  is not  $prev(v)$  or  $next(v)$ ,  $v$  is a FHB in  $Q$ . The length of  $Q$  w.r.t.  $l^*$  is  $dist(v) = dist(u) + l(u, v)$  (Line 10 in Procedure Finding-Shortest-Augmenting-Path). If  $dist(v) < \text{FHB\_dist}(v)$ , i.e.,  $Q$  is shorter than the current shortest CR-path from  $s$  to  $v$  with  $v$  as a FHB, then  $Q$  should be the new shortest CR-path path from  $s$  to  $v$  with  $v$  as a FHB. In this situation, we update  $\text{FHB\_dist}(v) = dist(v)$  and  $\text{FHB\_phcr}(v) = u$  (Line 12-13 in Procedure Finding-Shortest-Augmenting-Path). Since  $v$  is a FHB in  $Q$ , to further extend  $Q$  as a CR-path, the next hop of  $v$

must be  $prev(v)$ , so we let  $v$  send a FIND-SAP message  $\{dist(v)\}$  to  $prev(v)$  (Line 15 in Procedure Finding-Shortest-Augmenting-Path).

Case 4:  $v$  is an occupied node and  $u$  is  $next(v)$ .  $Q$  is a CR-path. Since  $u$  is  $next(v)$ ,  $v$  is an OHB in  $Q$ . The length of edge  $(u, v)$  changes to  $-l(u, v)$  while converting  $G$  to  $G^*$ , so the length of  $Q$  w.r.t.  $l^*$  is  $dist(v) = dist(u) - l(u, v)$  (Line 17 in Procedure Finding-Shortest-Augmenting-Path). If  $dist(v) < \text{OHB\_}dist(v)$ , i.e.,  $Q$  is shorter than the current shortest CR-path from  $s$  to  $v$  with  $v$  as an OHB, we update  $\text{OHB\_}dist(v) = dist(v)$  and  $\text{OHB\_}phcr(v) = u$  (Line 19-20 in Procedure Finding-Shortest-Augmenting-Path). Since  $v$  is an OHB, to further extend  $Q$  as a CR-path, the next hop of  $v$  could be any neighbor of  $v$  except  $next(v)$ , so we let  $v$  broadcast a FIND-SAP message  $\{dist(v)\}$  (Line 21 in Procedure Finding-Shortest-Augmenting-Path). Although this message will be redundantly received by  $next(v)$ ,  $next(v)$  will discard this message according to Case 2.

We assume that for each node  $v$ ,  $\text{FN\_}dist(v)$ ,  $\text{FHB\_}dist(v)$  and  $\text{OHB\_}dist(v)$  are all positive infinity at the beginning of each iteration. This can be implemented by involving a variable  $round(v)$  to denote the current iteration number in each FIND-SAP message.

### 3.2 Tracing Shortest Augmenting Path

At first, let us describe the last hop of a backward segment in a CR-path. In the example of Figure 2, after finding the shortest augmenting path  $P_a$  as shown in Figure 2(c), we say  $a$  is the last hop of the backward segment  $(c, b, a)$ . By adding  $P_a$  to the paths found before (as shown in Figure 2(d)),  $a$  should be an occupied node,  $prev(a)$  does not change and  $next(a)$  changes to its next hop in  $P_a$ , i.e.,  $f$ . In a CR-path, the last hop of a backward segment is certainly an OHB.

---

#### Procedure. Tracing-Shortest-Augmenting-Path

---

```

1 t sends a TRACE-SAP message to $\text{FHB_}phcr(t)$;
2 while $v \neq s$ receives TRACE-SAP message from u do
3 case v is a free node
4 Mark itself as an occupied node;
5 $prev(v) \leftarrow \text{FN_}phcr(v)$;
6 $next(v) \leftarrow u$;
7 Send a TRACE-SAP message to $\text{FN_}phcr(v)$;
8 case v is an occupied node and $u \neq prev(v)$
9 Still mark itself as an occupied node;
10 $next(v) \leftarrow u$;
11 Send a TRACE-SAP message to $\text{OHB_}phcr(v)$;
12 case v is an occupied node and $u = prev(v)$ and $\text{FHB_}dist(v) > \text{OHB_}dist(v)$
13 Mark itself as a free node;
14 Send a TRACE-SAP message to $\text{OHB_}phcr(v)$;
15 case v is an occupied node and $u = prev(v)$ and $\text{FHB_}dist(v) \leq \text{OHB_}dist(v)$
16 Still mark itself as an occupied node;
17 $prev(v) \leftarrow \text{FHB_}phcr(v)$;
18 Send a TRACE-SAP message to $\text{FHB_}phcr(v)$;

```

---

After finding the shortest augmenting path  $P_a$ , nodes execute Procedure Tracing-Shortest-Augmenting-Path to add  $P_a$  to the paths found before. While  $t$  receives a FIND-SAP message for the first time in a new iteration,  $t$  waits long enough for the end of Phase 1. Meanwhile, the shortest augmenting path  $P_a$  (if there is any) is found. Next, starting from  $t$ , in sequence, each node  $v$  in  $P_a$  sends a TRACE-SAP message to its previous hop in  $P_a$ . Each TRACE-SAP message has empty data field.

$t$  sends a TRACE-SAP message to  $\text{FHB\_phcr}(t)$  to start the process (Line 1 in Procedure Tracing-Shortest-Augmenting-Path). If  $v \neq s$  receives a TRACE-SAP message from  $u$ , it means that  $v$  is a node in  $P_a$  and its next hop in  $P_a$  is  $u$ . We discuss in the following four cases while  $v \neq s$  receives a TRACE-SAP message from  $u$ .

Case 5:  $v$  is a free node. Then  $v$  is a FN in  $P_a$ . Its next hop in  $P_a$  is  $u$ . Its previous hop in  $P_a$  should be  $\text{FN\_phcr}(v)$ . To add  $P_a$  to the paths found before,  $v$  becomes an occupied node.  $\text{prev}(v)$  should be  $\text{FN\_phcr}(v)$  and  $\text{next}(v)$  should be  $u$ . In this case, we let  $v$  executes Line 3-7 in Procedure Tracing-Shortest-Augmenting-Path.

Case 6:  $v$  is an occupied node and  $u$  is not  $\text{prev}(v)$ . Since  $v$ 's next hop in  $P_a$  is not  $\text{prev}(v)$ ,  $v$  is the last hop of a backward segment. Thus,  $v$  is an OHB in  $P_a$ .  $v$ 's previous hop in  $P_a$  should be  $\text{OHB\_phcr}(v)$ . By adding  $P_a$  to the paths found before,  $v$  is still an occupied node.  $\text{prev}(v)$  does not change and  $\text{next}(v)$  changes to  $u$ . In this case, we let  $v$  execute 8-11 in Procedure Tracing-Shortest-Augmenting-Path.

Case 7:  $v$  is an occupied node and  $u$  is  $\text{prev}(v)$  and  $\text{FHB\_dist}(v) > \text{OHB\_dist}(v)$ .  $v$ 's next hop in  $P_a$  is  $\text{prev}(v)$ , so  $v$  is not the last hop of a backward segment and  $v$  may be a FHB or OHB in  $P_a$ . Since  $\text{FHB\_dist}(v) > \text{OHB\_dist}(v)$ ,  $v$  is an OHB in  $P_a$  and  $v$ 's previous hop in  $P_a$  should be  $\text{OHB\_phcr}(v)$ . By adding  $P_a$  to the paths found before,  $v$  becomes a free node. In this case, we let  $v$  execute 12-14 in Procedure Tracing-Shortest-Augmenting-Path.

Case 8:  $v$  is an occupied node and  $u$  is  $\text{prev}(v)$  and  $\text{FHB\_dist}(v) \leq \text{OHB\_dist}(v)$ .  $v$ 's next hop in  $P_a$  is  $\text{prev}(v)$ , so  $v$  may be a FHB or OHB in  $P_a$ . Since  $\text{FHB\_dist}(v) \leq \text{OHB\_dist}(v)$ ,  $v$  is a FHB in  $P_a$  and its previous hop in  $P_a$  should be  $\text{FHB\_phcr}(v)$ . By adding  $P_a$  to the paths found before,  $v$  still marks itself as an occupied node.  $\text{prev}(v)$  changes to  $\text{FHB\_phcr}(v)$  and  $\text{next}(v)$  does not change. In this case, we let  $v$  execute 15-18 in Procedure Tracing-Shortest-Augmenting-Path.

### 3.3 Proof of Correctness and Optimality

**Theorem 1.** *If there are  $n$  disjoint  $s \sim t$  paths in the given network, OFDP will find  $n$  disjoint  $s \sim t$  paths with minimum total length in the  $n$ th iteration.*

*Proof.* There are two phases in each iteration. In Phase 1, nodes execute Procedure Finding-Shortest-Augmenting-Path and exchange FIND-SAP messages. By the description of 3.1, if Phase 1 ends, OFDP will find the shortest augmenting

path  $P_a$  (if there is any). In Phase 2, nodes execute Procedure Tracing-Shortest-Augmenting-Path and exchange TRACE-SAP messages. By the description of 3.2, each node in  $P_a$  will send one TRACE-SAP message in sequence, so Phase 2 will definitely end and  $P_a$  is correctly added to the paths found before. By Lemma 1 and 2, if Phase 1 ends in the first  $n$  iterations, OFDP will find  $n$  disjoint  $s \sim t$  paths with minimum total length in the  $n$ th iteration. Next, we prove that Phase 1 will end in each iteration by induction on  $n$ .

For  $n = 1$ : OFDP has found no paths yet,  $G^* = G$ . Finding the shortest augmenting paths is equivalent to finding the shortest  $s \sim t$  path.  $G^*$  does not contain negative edges, so Phase 1 will end.

Suppose that this theorem is true for  $n = m$ , which means that OFDP has found  $m$  disjoint  $s \sim t$  paths  $P_1, \dots, P_m$  with minimum total length. Next, we prove that in the  $(m + 1)$ th iteration, Phase 1 will end, i.e., the length of the shortest CR-path from  $s$  to any node will not be updated unlimited times, i.e.,  $G^*$  does not contain negative cycles. Suppose that  $G^*$  contains a negative cycle  $C$ , whose length is  $l^*(C) < 0$ . By adding  $C$  to  $P_1, \dots, P_m$ , we can get another set of disjoint  $s \sim t$  paths  $P'_1, \dots, P'_m$ . From the proof of Lemma 2, we know that  $l^*(C) + \sum_{i=1}^m l(P_i) = \sum_{i=1}^m l(P'_i)$ . Therefore, the total length of  $P'_1, \dots, P'_m$  is less than the total length of  $P_1, \dots, P_m$ , which contradicts the fact that  $P_1, \dots, P_m$  are  $n$  disjoint  $s \sim t$  paths with minimum total length.

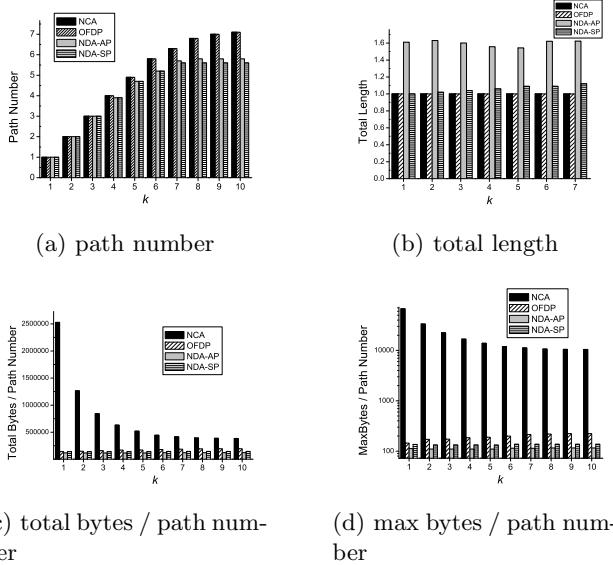
## 4 Simulation Results

We use a simulator written in C++ to evaluate the proposed algorithm. The simulator is a high level simulator which neglects the MAC layer. The transmitting radius of each sensor node is set to 50m. To simulate the given network, 2500 sensor nodes are randomly deployed in a 1500m  $\times$  1500m area. Each node has 8.7 neighbors on average. The length (energy cost) of each link is set to a random integer between 1 and 10. To get each result, we performed 10 simulations with different  $(s, t)$  pairs, and took their average value. The  $(s, t)$  pairs are generated randomly.

We compare the proposed distributed algorithm OFDP with other three algorithms: the centralized algorithm in [16] (denoted by NCA), the Natural Distributed Algorithm with Any Path (NDA-AP) and the Natural Distributed Algorithm with Shortest Path (NDA-SP). NDA-AP finds paths iteratively. In each iteration, NDA-AP finds a  $s \sim t$  path  $P$  (any  $s \sim t$  path) and removes the nodes in  $P$  from the network. NDA-AP is the basic idea of the algorithms in [8,13,1,6,7,14]. NDA-SP also finds paths iteratively. In each iteration, NDA-SP finds the shortest  $s \sim t$  path  $P$  and removes the nodes in  $P$  from the network. NDA-SP is an improved version of NDA-AP. Note that both NDA-AP and NDA-SP can guarantee neither correctness nor optimality.

We evaluate the performances of the algorithms at four aspects: 1) path number 2) total length 3) communication-efficiency 4) load balance. “Path number” is the number of the disjoint paths found by an algorithm. “Total length” is the total length of the found paths. We use “*total bytes*” divided by “path number”

to measure communication-efficiency, where “total bytes” is the total number of the bytes sent and received by all the nodes in the network. Load balance is measured by “*max bytes*” divided by “path number”, where “*max bytes*” is the maximum number of bytes sent and received by any node in the network. The comparison results are given by Figure 3.



**Fig. 3.** Simulation Results

Compared with NDA-AP and NDA-SP, OFDP finds significantly more and shorter disjoint paths. In the aspect of communication efficiency and load balance, OFDP is a little worse than NDA-AP and NDA-SP, but the gaps are negligible. OFDP and NCA find the same number of disjoint paths with the same total length. However, in the aspect of communication efficiency and load balance, OFDP is much better than NCA.

## 5 Conclusion

This paper proposes an efficient distributed algorithm OFDP to find  $k$  disjoint paths connecting two given nodes  $s$  and  $t$  with minimum total length in a WSN. Unlike the existing distributed algorithms for this problem, OFDP guarantees correctness and optimality. Compared with the existing centralized algorithms which also guarantee correctness and optimality, OFDP is much more efficient. Compared with the state-of-the-art distributed algorithms for the same problem, OFDP almost has the same efficiency, with the important advantage that OFDP guarantees a correct and optimal answer, whereas the compared algorithms do not. In conclusion, OFDP is correct and efficient to find disjoint paths between two nodes with minimum total length in a WSN.

## References

1. Baek, J.-W., Nam, Y.J., Seo, D.-W.: An energy-efficient k-disjoint-path routing algorithm for reliable wireless sensor networks. In: Obermaisser, R., Nah, Y., Puschner, P., Rammig, F.J. (eds.) SEUS 2007. LNCS, vol. 4761, pp. 399–408. Springer, Heidelberg (2007)
2. Bhandari, R.: Optimal physical diversity algorithms and survivable networks. In: Proceedings of the 2nd IEEE Symposium on Computers and Communications, ISCC (1997)
3. Cai, Z., Chen, Z., Lin, G.: Approximation algorithm for the capacitated multicast tree routing problem. *Theoretical Computer Science* 410, 5415–5424 (2009)
4. Cai, Z., Goebel, R., Lin, G.: Size-constrained tree partitioning: a story on approximating the multicast k-tree routing problem. *Theoretical Computer Science* 412, 240–245 (2011)
5. Chen, Y., Guo, X., Zeng, Q.: Amr: a multipath routing algorithm based on maximum flow in ad hoc networks. *Acta Electronica Sinica* 32, 1297–1301 (2004)
6. Deb, B., Bhatnagar, S., Nath, B.: Reinform: Reliable information forwarding using multiple paths in sensor networks. In: Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (2003)
7. Fang, X., Shi, S., Li, J.: A disjoint multi-path routing algorithm in wireless sensor network. *Jounal of Computer Research and Development* 46, 2053–2061 (2009)
8. Ganesan, D., Govindan, R., Shenker, S., Estrin, D.: Highly-resilient, energy-efficient multipath routing in wireless sensor networks. In: Proceedings of the 2nd ACM International Symposium on Mobile Ad hoc Networking & Computing, MobiHoc (2001)
9. Hashiguchi, T., Tajima, K., Takita, Y., Naito, T.: Node-disjoint paths search in wdm networks with asymmetric nodes. In: International Conference on Optical Network Design and Modeling, ONDM (2011)
10. Iwama, K., Iwamoto, C., Ohsawa, T.: A faster parallel algorithm for k-connectivity. *Information Processing Letters* 61, 265–269 (1997)
11. Khuller, S., Schieber, B.: Efficient parallel algorithms for testing connectivity and finding disjoint s-t paths in graphs. In: 30th Annual Symposium on Foundations of Computer Science (1989)
12. Kumar, A., Varma, S.: Geographic node-disjoint path routing for wireless sensor networks. *IEEE Sensors Journal* (2010)
13. Li, S., Wu, Z.: Node-disjoint parallel multi-path routing in wireless sensor networks. In: Proceedings of the Second International Conference on Embedded Software and Systems, ICESS (2005)
14. Omar, S., Zoulikha, M., Cousin, B.: Energy efficiency in ad hoc wireless networks with node-disjoint path routing. In: International Workshop on Systems, Signal Processing and their Applications, WOSSPA (2011)
15. Sidhu, D., Nair, R., Abdallah, S.: Finding disjoint paths in networks. In: Proceedings of the Conference on Communications Architecture & Protocols, SIGCOMM (1991)
16. Srinivas, A., Modiano, E.: Minimum energy disjoint path routing in wireless ad-hoc networks. In: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, MobiCom (2003)
17. Suurballe, J.W.: Disjoint paths in a network. *Networks* 4, 125–145 (1974)

# Information Theory Based Opportunistic Sensing in Radar Sensor Networks

Ishrat Maherin and Qilian Liang

Department of Electrical Engineering, University of Texas at Arlington,  
Arlington, TX 76019-0016 USA

**Abstract.** In this paper, we propose to use information theory to automatically select the best sensors in a Ultra Wide Band (UWB) Radar Sensor Networks (RSN) to detect target in foliage environment. Information theoretic algorithms such as entropy and mutual information are proven methods that can be applied to data collected by various sensors for target detection. However, the complexity of the environment brings uncertainty in fusion center and the big data collected by sensors can have huge processing load. In this paper, we propose to use another information theoretical criterion known as Chernoff information that can provide the best error exponent of detection in Bayesian approach. We also used Chernoff Stein Lemma for fusing the data to optimize the performance. The performance of the algorithm was evaluated, based on real world data. Results show that our opportunistic sensing (OS) algorithm does efficient utilization of sensing assets and provide same performance while it is compared with the existing method without OS.

**Keywords:** Target detection, opportunistic sensing, UWB, Radar Sensor Networks, Chernoff information, sense-through-foliage and entropy.

## 1 Introduction

Time varying and rich scattering complex environment of forest makes target detection through foliage an ongoing challenge. In Radar Sensor Network (RSN), multiple distributed radar sensors survey a large area and observe targets from different angles. Major limitations of such conventional approaches include inadequate performance for target recognition and huge processing load for big data. Opportunistic Sensing (OS) refers to a paradigm for signal and information processing in which a network of sensing systems can automatically discover and select sensor platforms based on an operational scenario. From the experimental data collected by Air Force, it has been found that echoes with target are more random than the region without target [1]. This finding leads us to use Maximum entropy Method (MEM) and mutual information as the target detection tool [2]. However, there can still be redundancy in the big data collected by various radars. Since its possible that less sensors can achieve better performance, and less sensors can save the bandwidth, energy, memory and storage resource of sensor networks, its very desirable that principal sensors can be

selected. Also the error probability associated with the detection is crucial in understanding the performance of the detection. Chernoff information gives the best error exponent in hypothesis testing, thus can be used as sensor selection scheme in fusion center. This OS reduces the processing load significantly and effectively utilize the sensing assets. In order to optimize the performance, data fusion is done based on Chernoff Stein Lemma.

The potential of Chernoff information is widely explored recently. Chernoff information was used in optimization of sensor network in distributed detection [3]. Error exponents in target class detection was investigated in [4]. It was used in UWB [5] and was also used in analysis of energy detectors of cognitive radio [6]. Some theoretical works on radar sensor network-based target detection were reported in [7] [8] and [9]. In [10], detecting and eliminating redundancy in a sensor network with a view to improving energy efficiency, while preserving the networks coverage was studied using Voronoi diagrams. In [11], Liang and Wang applied a singular-value decomposition (SVD)- QR algorithm to redundancy reduction for acoustic sensor networks. In [12] [13], Liang applied rate distortion function for opportunistic sensing in RSN scenario. In [14], Aughenbaugh applied information theory for metric selection for information fusion.

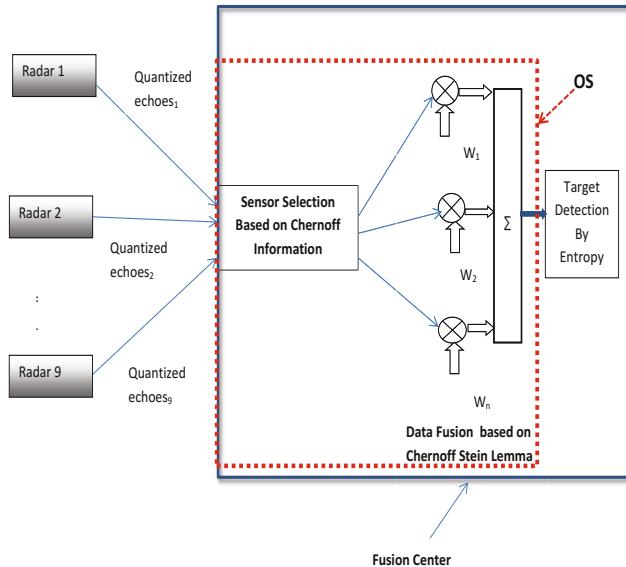
The rest of the paper is organized as follows. In Section 2, we describe the system model. In Section 3, we explain design and analysis of Chernoff information based sensing and Chernoff Stein Lemma based data fusion. In Section 4, we present the simulation results. We conclude this paper and propose some future research in Section 5.

## 2 System Model

RSN and rake structure that we employ in our work has nine different radars, each collected 35 reading as shown in Fig.1. These radars are mono-static and independent. Since two radars will not experience deep fading at the same time, RSN provides better signal quality when they are spaced sufficiently far apart. Also the collections of the reading from different position of the radar were not taken at the same time. This guarantees the time as well as spatial diversity in the proposed RSN. Information collected by individual radars are quantized and sent to fusion center to combine by using the weighted average. But before the weighted average is applied best sensors will be selected based on their Chernoff information. Also the weight will be applied based on Chernoff Stein Lemma. Detailed analysis of these theorems are discussed in the Section 3. Finally an information theoretic algorithm, Maximum entropy Method(MEM) is used to detect target [1].

## 3 Design and Performance Analysis Based on Chernoff Information and Chernoff Stein Lemma

Chernoff information gives best error exponent for hypothesis testing in Bayesian approach. The higher the Chernoff information the lower the probability of error



**Fig. 1.** Detailed block diagram for information theory based opportunistic sensing in Radar Sensor Network

in detection. In this paper, we propose to use Chernoff information as sensor selection scheme. This will significantly reduce the processing delay and improves the performance as well.

*Definition 1:* Let  $\mathbf{x}$  be a sequence of  $n$  symbols from an alphabet  $X = \{a_1, a_2, \dots, a_{|X|}\}$ . The type  $P_{\mathbf{x}}(a)$  (empirical probability distribution) of sequence is the relative proportion of occurrences of each symbol of  $X$  and can be written as [15],

$$P_{\mathbf{x}}(a) = N(a|\mathbf{x})/n, \quad \forall a \in X \quad (1)$$

where  $N(a|\mathbf{x})$  denotes the number of occurrences of the symbols  $a$  in the sequence.

*Definition 2:* Entropy is a measure of uncertainty of a random variable [15]. Let  $\mathbf{x}$  be a sequence with alphabet  $X$  and empirical distribution  $P_{\mathbf{x}}(a)$  as defined by (1), then the entropy of  $\mathbf{x}$  is defined as,

$$H(\mathbf{x}) = - \sum_{a \in X} P_{\mathbf{x}}(a) \log_2 P_{\mathbf{x}}(a) \quad (2)$$

*Definition 3:* The KL divergence or relative entropy is defined for probability mass functions of  $P_{\mathbf{x}}$  and  $Q_{\mathbf{x}}$  as,

$$D_{KL}(P_{\mathbf{x}}||Q_{\mathbf{x}}) = \sum_{a \in X} P_{\mathbf{x}}(a) \log\left(\frac{P_{\mathbf{x}}(a)}{Q_{\mathbf{x}}(a)}\right) \quad (3)$$

where  $|X|$  in (2) and (3) depends on the quantization level.

If we assume the 9 radar sensors are independent and the observations of the sensors are i.i.d then; let  $X_1, X_2 \dots X_n$  be i.i.d  $Q(x)$ ; let  $A_n \subseteq \chi_n$  is acceptance region for hypothesis  $H_1$ ; we can consider the two hypothesis as follows,

$$\begin{aligned} H_1 : & Q = P_1 \quad \text{Target present} \\ H_2 : & Q = P_2 \quad \text{Target absent} \end{aligned} \quad (4)$$

Consider the general decision function when  $g(X_1, X_2, \dots, X_n) = 1$  mean  $H_1$  is accepted and  $g(X_1, X_2, \dots, X_n) = 2$  means  $H_2$  is accepted. We can define the two probabilities of error, one is the missed detection  $\alpha_n$  and other is the false alarm  $\beta_n$ ,

$$\alpha_n = Pr(g(X_1, X_2, \dots, X_n) = 2 | H_1 \text{ true}) = P_1^n(A_n^c) \quad (5)$$

and

$$\beta_n = Pr(g(X_1, X_2, \dots, X_n) = 1 | H_2 \text{ true}) = P_2^n(A_n) \quad (6)$$

Now if we assume that  $Q = P_1$  with prior probability  $\pi_1$  and  $Q = P_2$  with prior probability  $\pi_2$ , the overall probability of error is,

$$P_e^{(n)} = \pi_1 \alpha_n + \pi_2 \beta_n \quad (7)$$

In order to get the minimum probability of error, in general we wish to minimize both error as expressed by (7). The probability of error in detection  $P_e$  asymptotically it holds that [15],

$$\lim_{n \rightarrow \infty} \frac{\log P_e}{n} = -CI^* \quad (8)$$

In other words for large n we obtain

$$P_e \approx \exp(-nCI^*) \quad (9)$$

here  $CI^*$  is the Chernoff information. The Chernoff information between two pmf p and q is defined as [15],

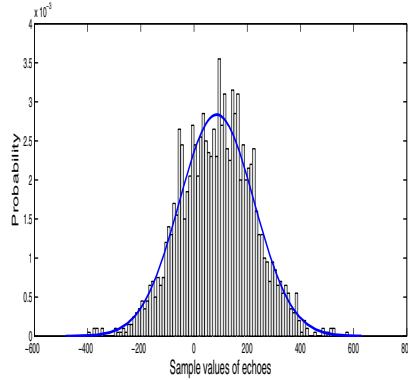
$$CI^* = C(p, q) = -\min_{0 \leq \lambda \leq 1} \log \sum_{k=1}^M p_k^\lambda q_k^{1-\lambda} \quad (10)$$

where M is related to quantization level.  $\lambda$  value should be chosen by the following,

$$D(p||\lambda) = D(q||\lambda) \quad (11)$$

Here D is defined by (3).

**Chernoff Stein Lemma.** As an alternative to Bayesian approach, we can minimize one of the error subject to the constraint of the other error, which is known as Chernoff-Stein Lemma. In that case  $\alpha_n < \epsilon$ , and  $\beta_n$  for two distribution  $P_1$  and  $P_2$  can be expressed as,



**Fig. 2.** Clutter distribution in the far-field for the last 2000 samples collected by 9 different radars with bin size =10

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n^\epsilon = -D(P_1 || P_2) \quad (12)$$

here  $\alpha_n$  and  $\beta_n$  is defined in (5) and (6), D is KL distance. From this we can say that the false alarm probability is inversely proportional to KL distance. In order to get a better result in the fusion center, we can do the data fusion and apply weighted average in the fusion center of the RSN based on Chernoff Stein lemma as follows:

Let  $Q_r$  be the pmf of quantized received echoes for the  $r^{th}$  radar and B be the pmf of the quantized received echoes of the clutter then the K-L divergence based weighting,  $w_r$  for each radar of the RSN can be given by the following,

$$w_r = \frac{D_r}{\sum_{r=1}^9 D_r} \quad (13)$$

and

$$D_r = D_{KL}(Q_r || B) \quad (14)$$

where  $D_{KL}$  is the divergence calculated from (3). The returned echoes are quantized and pmf are calculated before applying this.

One of the popular indoor UWB channel model is S-V model. But the foliage environment differs from indoor and we plotted the histogram of the clutter in the far field which follows the Gaussian Distribution as shown in Fig. 2. Also in a previous paper, it has been shown that the target region is uniform [1].

**Theorem 1:** If target has a distribution which follows  $U(a, b)$  and the clutter Q follows  $N(\mu, \sigma)$ , then the probability of error in target detection  $Err_d$  can be expressed as,

$$Err_d \approx \exp(-n(C)) \quad (15)$$

where C can be denoted as,

$$\begin{aligned} C = & -\lambda(b-a)\ln(b-a) - (1-\lambda)(b-a)\ln(\sqrt{2\pi}\sigma) \\ & -(1-\lambda) \left[ \left( \frac{b^3 - a^3}{6\sigma^2} \right) - \mu \left( \frac{b^2 - a^2}{2\sigma^2} \right) + \frac{\mu^2}{2\sigma^2}(b-a) \right] \end{aligned} \quad (16)$$

### Proof

Chernoff information between a uniform density  $p(x)$  and Gaussian distribution  $q(x)$  can be written as,

$$\begin{aligned} CI = & C(p(x), q(x)) \\ = & -\min_{0 \leq \lambda < 1} \ln \int_a^b \left[ \frac{1}{b-a} \right]^\lambda \left[ \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \right]^{1-\lambda} dx \end{aligned} \quad (17)$$

Now denoting the natural log term as  $C(\lambda)$ , this can be further simplified as,

$$\begin{aligned} C(\lambda) = & -\lambda \int_a^b \ln(b-a)dx - (1-\lambda) \int_a^b \ln(\sqrt{2\pi}\sigma)dx - (1-\lambda) \int_a^b \frac{(x-\mu)^2}{2\sigma^2} dx \\ = & -\lambda(b-a)\ln(b-a) - (1-\lambda)(b-a)\ln(\sqrt{2\pi}\sigma) \\ & -(1-\lambda) \left[ \left( \frac{b^3 - a^3}{6\sigma^2} \right) - \mu \left( \frac{b^2 - a^2}{2\sigma^2} \right) + \frac{\mu^2}{2\sigma^2}(b-a) \right] \end{aligned} \quad (18)$$

As the theoretical close form approximation of Chernoff information between a uniform and gaussian density can be expressed as (18), theorem 1 can be proved from (18) and (9).

**Theorem 2:** If target has a distribution which follows  $\mathbf{U}(a, b)$  and the clutter Q follows  $\mathbf{N}(\mu, \sigma)$  and missed detection is fixed, the false alarm rate can be expressed as  $Err_f$  can be expressed as,

$$Err_f \approx \exp(-n(D(P||Q))) \quad (19)$$

where D can be denoted as,

$$D(P||Q) = -\ln(b-a) + \ln\sqrt{2\pi}\sigma + \frac{\mu}{6\sigma^2}(b^2 + ab + a^2) - \frac{\mu}{4\sigma^2}(b+a) + \frac{\mu^2}{2\sigma^2} \quad (20)$$

**Proof:** Proof is attached in Appendix A.



**Fig. 3.** Trihedral reflector as Target

## 4 Simulation Results

Our work is based on the sense-through-foliage data from Air Force Research Lab [16]. The target is a trihedral reflector with a slant length of 1.5 was located 300 feet away as shown in Fig. 3. Each sample is spaced at 50 picoseconds interval, and 16,000 samples were collected for total time duration of 0.8 microseconds at a rate of approximately 20 Hz [16]. The target should then be located around sample 13900. Initially, the Barth pulse source was operated at lower amplitude and 35 pulses of signals were obtained. This collection is referred to as “poor” data. The integration of these 100 pulses with higher amplitude is referred to as “good” data, and some works have been done on target detection based on such data sets, such as DCT-based approach [17] and differential-based approach [18]. The window size was used as 50.

In Fig. 4, we assess the proposed method of target detection in terms of the probability of error for nine different radars, in 16 levels of quantization. To compare the performance in terms of probability of error in detection, we used three different methods, Chernoff Information, Chernoff Stein Lemma and the theoretical approximation of Chernoff Stein Lemma. Clearly the probability of error in detection decreases as number of radars increases. Between these methods Chernoff Information performs much better than Chernoff Stein Lemma. Chernoff information can achieve less than 0.1 of probability of error in detection with only 2 radars whereas Chernoff Stein Lemma needs at least 7 radars for achieving similar performance.

Fig. 5 shows the Chernoff information in various radar position. The purpose of this study is to apply OS so that we can utilize the sensing assets efficiently. We want to select the radars which will provide the highest Chernoff information as they will provide the lowest error in detection while hypothesis testing is done using Bayesian approach.

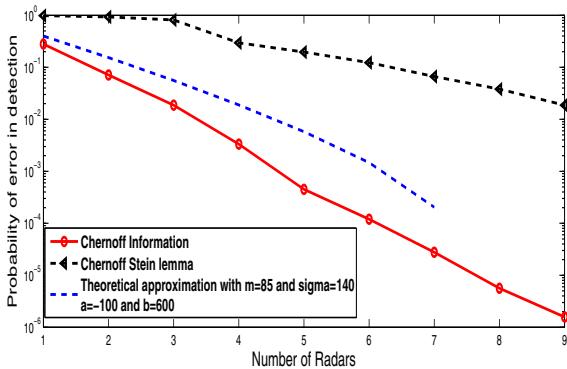


Fig. 4. Probability of error versus number of sensors, with 16 level of quantization

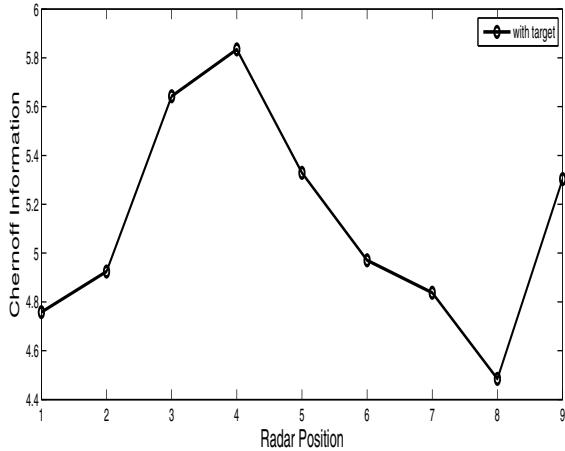
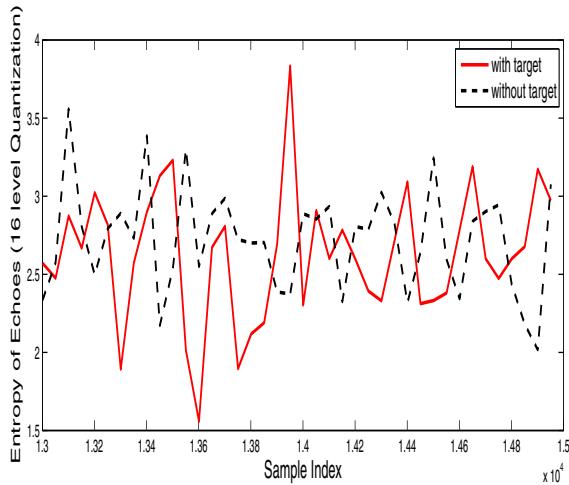


Fig. 5. Chernoff Information versus radar in nine different positions

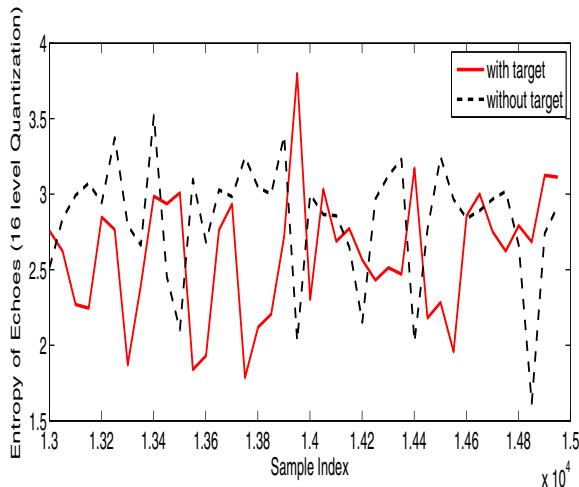
Fig. 6 shows the performance of an entropy based target detection using Chernoff information as sensor selection scheme. Here only five sensors are chosen with the highest Chernoff information. Clearly the position of the radar with highest Chernoff is selected as position 3,4,5,6,9. The target is detected around sample 13900.

Fig. 7 shows the performance of an entropy based target detection while only three radars are chosen based on their Chernoff information. The target is detected around sample 13900.

Fig. 8 shows the performance of an entropy based target detection while only one radar is chosen based on their Chernoff information. The target is detected around sample 13900. Fig. 9 shows the performance of the target detection algorithm without OS. If we compare the performance between Figs. 8 and 9, clearly

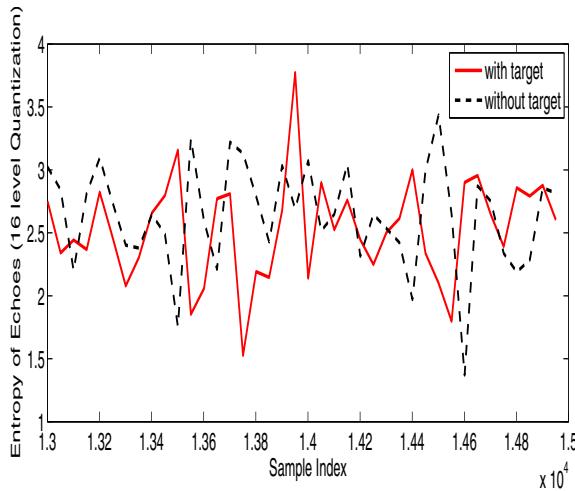


**Fig. 6.** Entropy based Target detection with five sensors(position 3,4,5,6,9) selected by Chernoff Information with 16 level quantization. Target is detected.

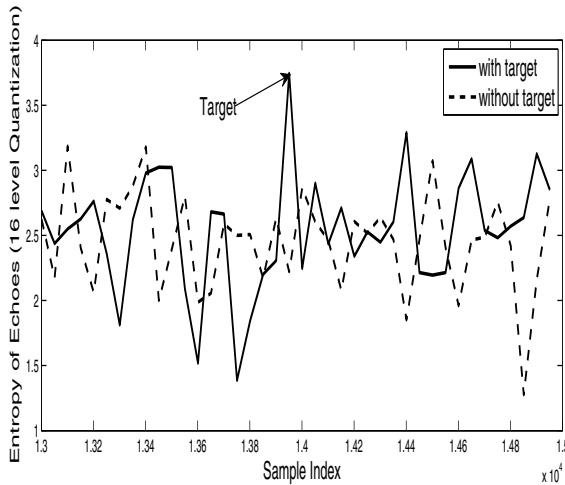


**Fig. 7.** Entropy based Target detection with three sensors(position 3,4,5) selected by Chernoff Information with 16 level quantization. Target is detected.

the performance with OS is equally good as the performance without OS. This proves the effectiveness of our algorithm in detection while significantly reducing the huge processing load of the big data, collected by 9 different radars in 35 different position with 16000 sample. The reduction in processing load is 9:1.



**Fig. 8.** Entropy based Target detection with one sensor (position 4) selected by Chernoff Information with 16 level quantization. Target is detected.



**Fig. 9.** Entropy based Target detection without OS

## 5 Conclusion

We propose theory and algorithm for a new scheme of Opportunistic sensing(OS) that not only ensures effective utilization of sensing assets but also provides optimal performance. We propose to use Chernoff information as sensor selection scheme and we also propose to use Chernoff Stein Lemma based information fusion in the fusion center. We derived the close form approximation for the Chernoff information and KL distance between uniform and Gaussian densities.

This is a novel approach since it has not been investigated so far. Simulation results show that our approach can work successfully with real world data. Using this novel approach we could significantly reduce the number of radars from 9 to 1 while maintaining good performance. In future, we shall acquire more data and apply this algorithm to multi-target detection.

## A Closed Form Approximation of False Alarm Rate between Uniform Target and Gaussian Clutter

KL distance for the continuous case can be written as

$$D(p(x)||q(x)) = \int_0^\infty p(x) \ln \frac{p(x)}{q(x)} dx \quad (21)$$

For our case  $p(x)$  follows  $U(a, b)$  and  $q(x)$  follows  $N(\mu, \sigma)$  then KL distance can be expressed as,

$$D(p(x)||q(x)) = \int_a^b \frac{1}{b-a} \ln \left( \frac{\frac{1}{b-a}}{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}} \right) dx \quad (22)$$

After simplification this can be written as,

$$D(p(x)||q(x)) = \frac{1}{b-a} \int_a^b -\ln(b-a) dx + \frac{1}{b-a} \int_a^b \ln \sqrt{2\pi}\sigma dx + \frac{1}{b-a} \int_a^b \frac{(x-\mu)^2}{2\sigma^2} dx$$

This can be further simplified as,

$$D(p(x)||q(x)) = -\ln(b-a) + \ln \sqrt{2\pi}\sigma + \frac{\mu}{6\sigma^2} (b^2 + ab + a^2 - \frac{\mu}{4\sigma^2} (b+a) + \frac{\mu^2}{2\sigma^2}) \quad (23)$$

Now replacing this (23) in (12), we can find the Theorem 1.

**Acknowledgement.** The authors would like to thank Dr. Sherwood W. Samm in Air Force Research Laboratory for providing the sense-through-foliage data. This work was supported in part by U.S. Office of Naval Research under Grants N00014-13-1-0043, N00014-11-1-0865 and U.S. National Science Foundation under Grants CNS-1247848, CNS-1116749, CNS-0964713.

## References

1. Maherin, I., Liang, Q.: An Entropy Based Approach for Sense- through Foliage Target Detection using UWB Radar. In: Cheng, Y., Eun, D.Y., Qin, Z., Song, M., Xing, K. (eds.) WASA 2011. LNCS, vol. 6843, pp. 180–189. Springer, Heidelberg (2011)

2. Maherin, I., Liang, Q.: A mutual information based approach for target detection through foliage using UWB radar. In: IEEE Int. Conf. Commun. (ICC), June 10-15, pp. 6406–6410 (2012)
3. Fabeck, G., Mathar, R.: Chernoff information-based optimization of sensor networks for distributed detection. In: IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), December 14-17, pp. 606–611 (2009)
4. Misra, S., Tong, L., Ephremides, A.: Error Exponents for Target-Class Detection in a Sensor Network. In: IEEE Conf. Military Commun. (MILCOM), October 23-25, pp. 1–7 (2006)
5. Sadler, B.M., Swami, A.: On the performance of episodic UWB and direct-sequence communication systems. IEEE Transactions on Wireless Communications 3(6), 2246–2255 (2004)
6. Lee, Y., Sung, Y.: Generalized Chernoff Information for Mismatched Bayesian Detection and Its Application to Energy Detection. IEEE Signal Processing Letters 19(11), 753–756 (2012)
7. Liang, Q.: Radar Sensor Wireless Channel Modeling in Foliage Environment: UWB Versus Narrowband. IEEE Sensors J. 11(6), 1448–1457 (2011)
8. Liang, Q.: Automatic Target Recognition Using Waveform Diversity in Radar Sensor Networks. Pattern Recognition Letters (Elsevier) 29(2), 377–381 (2008)
9. Liang, Q., Cheng, X.: KUPS: Knowledge-based Ubiquitous and Persistent Sensor networks for Threat Assessment. IEEE Transactions on Aerospace and Electronic Systems 44(3) (July 2008)
10. Carbunar, B., Grama, A., Vitek, J., Carbunar, O.: “Coverage Preserving Redundancy Elimination in Sensor Networks. In: IEEE SECON 2004 (October 2004)
11. Liang, Q., Wang, L.: Redundancy Reduction in Wireless Sensor Networks Using SVD-QR. In: IEEE Military Communication Conference, Atlantic City, NJ (October 2005)
12. Liang, Q., Cheng, X., Chen, D.: Opportunistic Sensing in Wireless Sensor networks: Theory and Application. In: IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1–5 (December 2011)
13. Liang, Q., Cheng, X., Huang, S., Chen, D.: Opportunistic Sensing in Wireless Sensor networks: Theory and Application. Accepted by IEEE Trans. on Computers
14. Aughenbaugh, J.M., La Cour, B.R.: Metric selection for information theoretic sensor management. In: 11th Int. Conf. Information Fusion, June 30-July 3, pp. 1–8 (2008)
15. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley-Interscience Press, New York (1991)
16. Dill, C.: Foliage Penetration (phase II) Field Test Narrow band vesus Wideband Foliage Penetration. Final report of contract number F41624-03-D-700/04 (July to February 2006)
17. Liang, J., Liang, Q.: Sense-through-foliage target detection using uwb radar sensor networks. Pattern Recognition Letters 31, 1412–1421 (2010)
18. Liang, Q., Samn, S.W., Cheng, X.: UWB radar sensor networks for sensethrough-foliage target detection. In: IEEE International Conference on Communications, pp. 2228–2232 (2008)

# Isolate Safe Area Detection for Rescue in Wireless Sensor Networks

Chunyu Ai and Frank Haizhon Li

Math & Computer Science Division, University of South Carolina Upstate,  
Spartanburg, SC, USA  
[{aic,fli}@uscupstate.edu](mailto:{aic,fli}@uscupstate.edu)

**Abstract.** Isolate safe area detection is significant for various applications of wireless sensor networks since it can provide precious information for the rescue crew to save trapped persons. We propose a centralized method to detect isolate safe areas via discovering holes in event areas. In order to shorten the detection delay, a distributed method is also studied. Detecting isolate safe areas in a building is addressed specially since the regular detecting method is not applicable. Our simulation results show that the distributed method can detect all isolate safe areas in acceptable short delay.

**Keywords:** Wireless sensor networks, Isolate safe area, Area detection, Rescue.

## 1 Introduction

As communication technology, embedded computing technology and sensing technology are becoming more and more advanced, sensors that have the capabilities of sensing, computation, and communication are emerging all over the world. Sensor networks consisting of different kinds of sensors are capable of gathering a large amount of information such as temperature, humidity, and light intensity, at any time, any place, and under any circumstances [1]. Therefore, sensor networks are widely deployed to monitor surrounding environment and detect various events in military fields, national security, traffic control, health, environmental monitoring, industry, and disaster prevention and recovery. In recent years, researchers have proposed various data collection, query processing, event detection and monitoring systems since monitoring systems of sensor networks are significant for various fields [2–7]. However, most proposed systems in the literature focus only on how to detect various events and delivery alarms. Our focus centers on providing real-time and accurate information for rescue when a dangerous event happens.

An Intelligent Monitoring System (IMS) can be widely used for various monitored environments and monitoring missions such as coal mine monitoring [8, 9], underground structure monitoring [10], and fire detection and rescue [11, 12]. For instance, an IMS can be used for monitoring fires in a building as shown in Fig. 1a. The system can detect a fire according to abnormal temperature and smoke

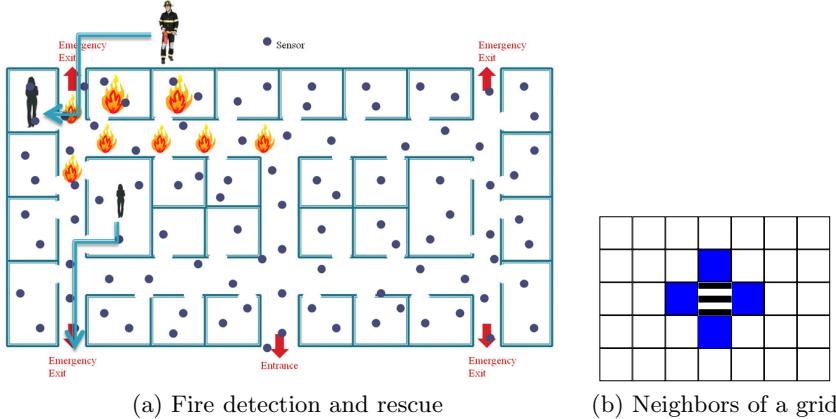


Fig. 1.

intensity reports sensed by sensors. Then, a fire alarm is triggered automatically to inform people in the building to evacuate and notify firefighters to come to the scene. Since sensors can sense environmental changes and activities of human beings, an IMS can collect and integrate useful information from sensor networks in a real-time manner and generate a real-time fire map which can reflect the real circumstances in the building. The people in the building can use a smart phone, tablet, or computer to ask for a safe escape route. Through accessing IMS, the fire department can find the locations of trapped persons and the most efficient route to implement rescue. An IMS can be used for various fields to prevent and reduce loss of life and property when dangerous events happen. For example, safety is always a big concern in the coal industry. Gas leak and collapse accidents have caused so many worker injuries and fatalities. An IMS can help rescue crew locate trapped workers and accomplish rescue missions efficiently.

After analyzing the common features of events, we conclude that finding the locations of trapped persons are the key of rescue. An isolate safe area is a safe area which is contained by a dangerous area. Detecting isolate safe areas are significant for rescue missions since there is a big probability that people are trapped in these areas when a dangerous event happens. Also, these isolate safe areas are just temporarily safe because dangerous areas usually spread quickly such as fire. Therefore, detecting isolate safe areas and informing rescue crew of the locations in a short time are significant.

In this paper, we address isolate safe area detection issue. To the best of our knowledge, this is the first work studying isolate safe area detection problem. The rest of the paper is organized as follows. Our proposed centralized and distributed detection methods are introduced in Section 2. Section 3 shows our simulation results, and Section 4 concludes this paper.

## 2 Isolate Safe Area Detection

### 2.1 Preliminaries

In many applications, users expect information about areas of their interests instead of sensed values of individual sensor nodes. Users can write a query to describe desired area results by specifying area size and conditions of sensing attributes. Only an area which has every sensor node in it satisfied all attribute conditions can be returned as results.

Our previous work [13] proposed an energy-efficient in-network area query processing scheme which can answer area queries with low energy consumption. In order to process area queries efficiently, the monitored area is partitioned into grids, and each grid is assigned a unique gray code number as its Grid ID (GID) as shown in Fig. 2a. A GID is formatted as  $(X, Y)$  where  $X$  represents a gray code number in horizontal direction, and  $Y$  represent a gray code number in vertical direction. The GID of the grid at the top-right corner is  $(100, 000)$ . The grid at the bottom-right corner is  $(100, 10x)$ , where  $x$  means either 0 or 1 indicating the union of  $(100, 101)$  and  $(100, 100)$ . Gray code based area description can significantly reduce the size of query results compared to other description methods since one gray code can represent multiple grids, thus saving energy consumption during transmission of results or partial results. To perform in-network query processing, a reporting tree is constructed by the base station. In Fig. 2a, a reporting tree example is shown. An area query is processed in bottom-up manner along the reporting tree. An internal node receives the reports from its children and merges the reports to generate partial results, then sends to its parent.

This scheme can detect dangerous areas when an event happens. Intuitively, we can use this scheme to detect dangerous areas, then detect isolate safe areas by judging whether there are holes in a dangerous area.

### 2.2 Centralized Isolate Safe Area Detection

In order to discover isolate safe areas, a  $m \times n$  matrix  $A$  ( $m$  rows and  $n$  columns) is created to help the processing. Each element of the matrix  $A$  represents a grid of the monitored area. The base station of wireless sensor networks can send an event query to find all grids which have the event happened in it. As shown in Fig. 2b, the shaded grids are affected by the event. According to the event query results, the matrix element of a safe grid is set to 0, and the matrix element of a dangerous grid (affected by the event) is set to  $-1$ . Neighbors of a grid are defined as the adjacent grids located at above, below, left, and right of the current one. As shown in Fig. 1b, the shaded grids are neighboring grids of the stripped grid. Only neighboring grids with the same status (either safe or dangerous) can be merged to generate a bigger area. An isolate safe areas is continuous area which is surrounded by a dangerous area. Fig. 2b shows two isolate safe area examples. We assume safe grids located at boundary of the whole monitored area cannot be a grid of an isolate safe area. This assumption is applicable to a lot of applications.

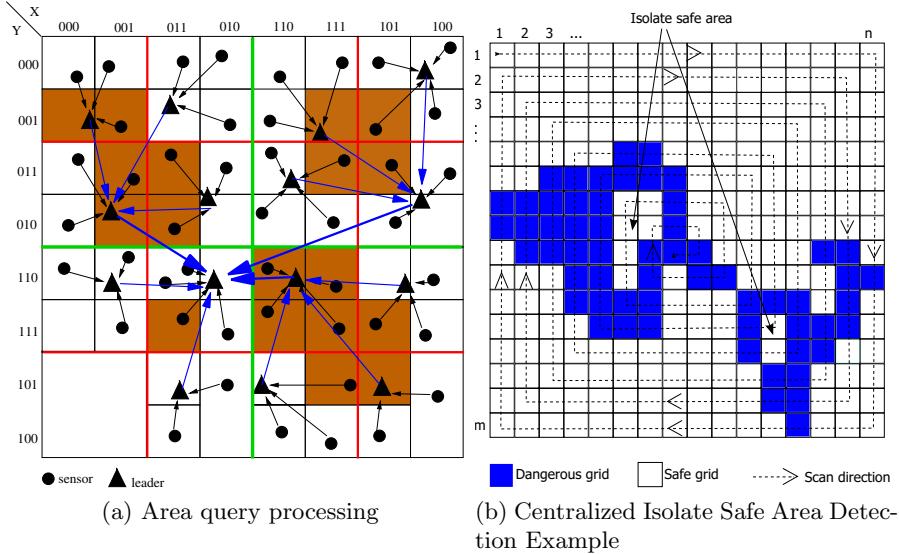


Fig. 2.

Algorithm 1 is proposed to detect isolate safe areas. The basic idea is to mark each safe grid with an either safe or safe\_isolate area\_id. The area\_id of a grid is stored in the corresponding element in Matrix  $A$ . Since safe grids on the boundary must be a part of a safe area, we start to process all grids on the boundary, then move to the inner grids next to boundary grids until the center is reached. The order of processing grids is shown in Fig. 2b. Initially, two empty lists,  $List_{safe}$  and  $List_{isolate\_safe}$ , are created to store area\_ids (starting at 1) of safe areas and isolate safe areas, respectively. First, we mark each safe grid on the boundary with an area\_ids, and add the area\_id to  $List_{safe}$  if it is new. If the current processing safe grid has a processed safe neighboring grid, the neighbor's area\_id is used to mark the current grid; otherwise, use a new area\_id to mark it. For inner safe grids, if the current processing grid is a dangerous grid, we don't change its value; otherwise, we use one of its processed safe neighboring grid's area\_id to mark it. If it has no processed safe neighboring grid, we use its processed isolate safe neighboring grid's area\_id to mark it. If all its processed grids are dangerous, we mark it with a new area\_id, and add this new area\_id to  $List_{isolate\_safe}$ .

Possibly, neighboring safe grids are marked with different area\_ids even though they belong to the same safe or isolate safe area; so after we marked a safe grid, if the current processing grid's area\_id is different from area\_ids of its neighboring safe grids, we unite the sublists which these area\_ids belong to as one. If this union is between a sublist in  $List_{safe}$  and a sublist in  $List_{isolate\_safe}$ , remove the sublist from  $List_{isolate\_safe}$  and add it to  $List_{safe}$  first, then union them. Thus, after marking every safe grid, each sublist in  $List_{isolate\_safe}$  can be used to identify one isolate safe area.

**Algorithm 1.** Centralized Isolate Safe Area Discovery

---

**Input:** Matrix  $A$   
**Output:** Isolate safe areas

```

1: $id_{area} = 0$
2: set $List_{safe}$ to empty
3: set $List_{isolate_safe}$ to empty
4: set $pre_id = 1$
5: add $\{1\}$ into $List_{safe}$
6: for every element in Matrix A , scan it from boundary to center as the order shown in Fig. 2b
do
7: if the current scanning element $A[i, j]$ is not -1 where i is the row number and j is the column
number then
8: if $A[i, j]$ is on the boundary, that is, (i is 1 or m) and (j is 1 or n) then
9: if pre_id is not -1 then
10: $A[i, j] = pre_id$
11: else
12: $id_{area} ++$
13: $A[i, j] = id_{area}$
14: $pre_id = A[i, j]$
15: add $\{id_{area}\}$ into $List_{safe}$
16: end if
17: else
18: if pre_id is in $List_{safe}$ then
19: $A[i, j] = pre_id$
20: else
21: if there exists a processed neighbor is marked with a safe area_id id then
22: $A[i, j] = id$
23: else if pre_id is not -1 then
24: $A[i, j] = pre_id$
25: else if $A[i, j]$ has a processed neighbor is marked with an isolate safe area_id id then
26: $A[i, j] = id$
27: else
28: $id_{area} ++$
29: $A[i, j] = id_{area}$
30: add $\{id_{area}\}$ into $List_{isolate_safe}$
31: end if
32: end if
33: $pre_id = A[i, j]$
34: if $A[i, j]$ is in $List_{safe}$ then
35: for each value id of any processed neighbor of $A[i, j]$ is in $List_{isolate_safe}$ do
36: remove the sublist which id belongs to from $List_{isolate_safe}$ and add it to $List_{safe}$
37: end for
38: end if
39: end if
40: end if
41: merge area_ids of $A[i, j]$ and its processed non-dangerous neighbor grids in either $List_{safe}$ or
 $List_{isolate_safe}$
42: end for
43: return $List_{isolate_safe}$, each sublist in it represents an isolate area

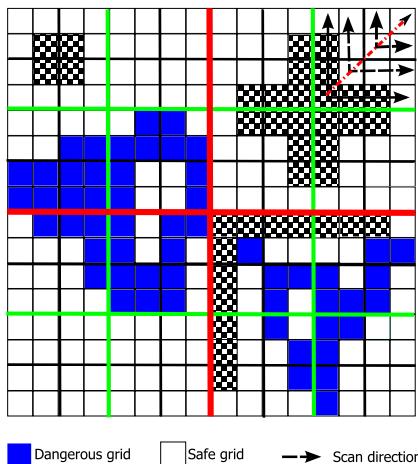
```

---

Centralized isolate safe area detecting is easy to be implemented on the base station, and its time complexity is  $O(m \times n)$ ; however, the base station has to wait for the sensor nodes to finish processing the event query, then run Algorithm 1 to discover isolate safe areas. Therefore, the time delay of centralized method might not be acceptable for a serve time sensitive rescue mission. One way to shorten the time delay is to design an in-network detecting method, that is, discovering isolate safe areas during processing the event query.

### 2.3 Distributed Isolate Safe Area Detection

In order to shorten the response delay of isolate safe area detection, we design a distributed method to discover isolate safe areas during the in-network processing of event queries. The motivation of distributed design is to discover isolate safe areas as early as possible and send the locations of these areas to the rescue crew. We use the query scheme in our previous work introduced briefly in Section 2.1. As shown in Fig. 2a, when a sensor node senses a value satisfied the predefined condition of an event, it sends the report to its parent in the reporting tree. An internal node in the reporting tree receives the reports from its children, then merges the reports to generate a partial result for the subarea it covers (the subarea includes all grids represented by sensor nodes in the subtree rooted at the current internal node); then, it sends the subarea merging result to its parent. The whole query is processed from the bottom to the top of the reporting tree.



**Fig. 3.** Distributed Isolate Safe Area Detection

In order to discover isolate safe areas as early as possible, we also process along the reporting tree from the bottom to the top. For each internal node, its responsibility is to discover isolate safe areas within the subarea it covers. Here, an isolate safe area within a subarea means that any grid of this isolate area cannot be located at the boundary of the subarea. The grids at the boundary have a chance to be merged with grids in its adjacent subareas, thus whether it is an isolate safe area or not and its range cannot be determined at the current stage; so these will be saved for the current node's ancestor to judge. When an internal node discovers an isolate safe area within its subarea, it will send the report of the isolate safe area to the base station directly instead of sending along the reporting tree, thus guaranteeing the isolate safe areas can be reported immediately.

The method of detecting an isolate safe area in a subarea is described in Algorithm 2. Algorithm 2 is run on each internal node of the reporting tree. Each internal node also uses a matrix  $A$  to record status of each grid within its subarea. The element  $A[i, j]$  is  $-1$  if the grid is dangerous; otherwise,  $A[i, j]$  is  $0$ . The current internal node updates matrix  $A$  according to the reports sent by its children.

As shown in Fig. 3, the smallest subarea covered by the direct parent of leaf nodes has only 4 grids. It is not necessary to run detecting algorithm since there is no isolate safe area to be found. The rationale is that an isolate safe area must be surrounded by dangerous grids in all above, below, left, and right directions. The next level internal nodes have 16 grids in its covered area including 4 subareas covered by its 4 children respectively. Fig. 3 shows an example at the top-left corner. Only 4 grids shaded with checkerboard can be part of an isolate area detected in this phase, thus we just need to start scanning from these 4 grids. For the next level internal nodes, they have 64 grids in their covered area. An example is shown at the top-right corner in Fig. 3. If there is an isolate area, one of its grid must be in the grids shaded with checkerboard. So, if we start scanning from these shaded grids, it is guaranteed that all isolate safe areas can be discovered. The isolate areas (which don't include these shaded grids) don't span two subareas, thus they must be found and reported already in its child node. For each internal node, we define these grids with shaded checkerboard as potential isolate grids. The potential isolate grids of an area are these grids which are adjacent to vertical and horizontal center lines but except these grids also located at the boundary. In Fig. 3, for the whole area, the grids shaded with checkerboard in the bottom-right corner are potential grids in bottom-right subarea.

According to analysis results, for each internal node, we can start scanning from potential isolate grids to discover all isolate safe areas. In each processing area, we divide the area into four subareas, that is, four subareas in which its four children covered. In each subarea, we start scanning grids adjacent to the vertical and horizontal center lines, then scan grids adjacent to the grids scanned in the previous round, and so on until scanning all grids in the subarea. An example of the scanning order is shown in Fig. 3 at top-right corner.

In order to reduce the running time, whenever the current scanning round has no grid added to any candidate isolate areas, isolate safe areas are discovered and the process is terminated. Also, if all candidate isolate areas are excluded since they are directly or indirectly merged with boundary grids, the process will be done, and no isolate safe area are found. After scanning all four subareas and discovering all candidate isolate areas, merge these candidates if possible. Then, use the gray code based method in [13] to generate an isolate safe area information report and send to the base station. The reason we use the gray code based description is that the report size is smaller than other description methods, thus saving transmission energy consumption and also achieving a shorter transmission delay. For each internal node, the time complexity of detecting algorithm is  $O(m \times n)$  where  $m \times n$  is the number of grids the current internal node covers.

**Algorithm 2.** Distributed Isolate Safe Area Discovery

---

**Input:** Matrix  $A$   
**Output:** Isolate safe areas

```

1: $id_{area} = 0$
2: create an array $List_{isolate_safe}$ with four lists in it and initialize all lists to empty
3: $i = 0$
4: for each subarea do
5: $next_round = true$
6: for each round scanning do
7: if continue is not true then
8: break
9: else
10: if the current processing element $A[i,j]$ is a potential isolate grid and $A[i,j]=0$ (safe) then
11: if $A[i,j]$ has no processed safe neighboring grids in its subarea then
12: $id_{area} ++$
13: $A[i,j] = id_{area}$
14: add $\{id_{area}\}$ to $List_{isolate_safe}[i]$
15: else
16: use its processed safe neighboring gird's value to set $A[i,j]$
17: end if
18: else if $List_{isolate_safe}[i]$ is empty then
19: break
20: else if $A[i,j] = 0$ and $A[i,j]$ is a boundary grid then
21: if any of its processed neighboring grid value $id \geq 1$ then
22: remove the sublist contains id from $List_{isolate_safe}[i]$
23: end if
24: else if $A[i,j] = 0$ then
25: if the processed neighboring grid value $id \geq 1$ and id is in a sublist of
 $List_{isolate_safe}[i]$ then
26: $A[i,j] = id$
27: $next_round = true$
28: merge area_ids of $A[i,j]$ and its processed non-dangerous neighbor grids in
 $List_{isolate_safe}[i]$
29: end if
30: end if
31: end if
32: end for
33: $i ++$
34: end for
35: if there are non-empty list in $List_{isolate_safe}$ then
36: merge discovered isolate areas if possible
37: use the method in [13] to generate a GID lists description for each isolate area and send to
the base station
38: end if
```

---

## 2.4 Isolate Safe Area Detection in a Building

The method introduced above cannot be directly used to detect isolate safe areas in a building since walls and dangerous areas together can generate an isolate safe area too. For instance, the room at top-left corner in Fig. 1a is an isolate safe area because its only exit is next to a fire area. In order to detect isolate safe areas in a building, we modify the proposed algorithm as follows:

1. The safe grids located at the boundary of the whole monitored area cannot be used to mark its adjacent safe area not isolate.
2. Only the safe grid located at an exit can claim that the safe area it belongs to is not isolate.
3. An safe area in a room is not isolate only if it is adjacent to a non-isolate safe area which includes at lease one of the room's exits. For grids in each

room, we will assign a unique room number and a list of the room exit grids. A grid with a room number can only merge with other grids with the same room number or the the grids in the exit list.

The method we proposed is applicable in two dimensional monitored areas. However, for buildings with multiple floors, our method cannot be applied directly. We can use the proposed method for each floor separately. For the stairs and elevators which connect exits of multiple floors, we process them individually before we start detecting isolate safe areas on each floor.

### 3 Simulation Results

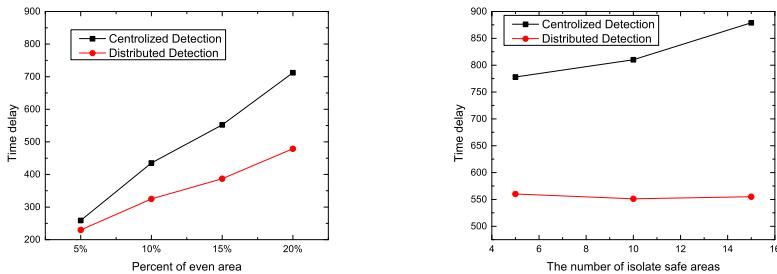
In this section, we evaluate the performance of our proposed centralized and distributed isolate safe area detection methods. When an severe event happens, the time delay is the biggest concern, thus we focus on evaluating the time delay of these two proposed methods.

We simulate the event query and isolate safe area detection of a coal mine. The monitored area size is  $64 \times 64$  grids. The payload size limit of a packet is 29 bytes which are the standard payload sizes provided by the TinyOS [14]. The transmission range of sensor nodes is 30m, and the sensing range is 15m. DSDV [15] is used as the routing protocol. We randomly generate 10 event and isolate safe area distribution scenarios to test the performance for each parameter value, and the results is the average of these 10 tests.

First, we evaluate the time delay with a different percent of the event area. The event area includes both dangerous grids and grids in isolate safe areas. The time delay with different percent of the event area is shown in Fig. 4a. The response delay is the average detection time of all isolate safe areas. As seen in the figure, the distributed detection method has an obvious shorter average delay than the centralized method. The reason is that some isolate safe areas can be detected at the lower levels of the reporting tree and results are sent to the base station directly. Also, the time delay increases with the increasing of the percent of event area because more event grids means more message transmissions.

Fig. 4b shows the time delay with different numbers of isolate safe areas. The percent of the event area is 20%. As shown in the figure, the delay of the centralized method increases with the number of isolate safe areas because more isolate safe areas inside event areas makes the size of the description of event areas bigger thus causing more transmissions. The distributed method is affected by this too but not as obvious. The reason is that when the number of isolate safe areas is bigger, more of them can be detected at the lower levels of the reporting tree.

Overall, the distributed detection method performs significantly better than the centralized method in terms of detection delay. However, the distributed method causes some internal nodes of the reporting tree to spend more energy for detection compared to the centralized method. Consuming more energy is worth while to gain shorter delay, thus more people and properties can be saved.



(a) Time delay with different percent of the event area      (b) Time delay with the number of isolate safe areas

**Fig. 4.** Simulation results

## 4 Conclusion

In order to detect isolate safe areas to save trapped persons, we proposed a centralized detection method and a distributed detection method respectively. The centralized version is easy to be implemented; however, its response delay is longer than the distributed method. This is verified by our simulation results. Also, detecting isolate safe areas in a building is a special case. We also addressed this issue in our work.

**Acknowledgement.** This work is partially supported by a RISE grant from the Office of the Vice President for Research at the University of South Carolina.

## References

1. Arampatzis, T., Lygeros, J., Manesis, S.: A survey of applications of wireless sensors and wireless sensor networks. In: Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control 2005, pp. 719–724 (June 2005)
2. Cai, Z., Ji, S., Li, J.: Data caching-based query processing in multi-sink wireless sensor networks. IJSNet 11(2), 109–125 (2012)
3. Cheng, S., Li, J., Cai, Z.:  $O(\epsilon)$ -approximation to physical world by sensor networks. In: 2013 Proceedings IEEE INFOCOM, pp. 3084–3092 (April 2013)
4. Wu, T., Cheng, Q.: Distributed dynamic event region detection in wireless sensor networks. In: 2011 IEEE Conference on Prognostics and Health Management (PHM), pp. 1–8 (June 2011)
5. Li, J., Cheng, S., Gao, H., Cai, Z.: Approximate physical world reconstruction algorithms in sensor networks. IEEE Transactions on Parallel and Distributed Systems 99(PrePrints), 1 (2014)
6. Y.-H. C. Ja Won Ko, A grid-based distributed event detection scheme for wireless sensor networks. Sensors (11) (2011)
7. Li, Y., Ai, C., Cai, Z., Beyah, R.: Sensor scheduling for p-percent coverage in wireless sensor networks. Cluster Computing 14(1), 27–40 (2011)

8. Wang, X., Zhao, X., Liang, Z., Tan, M.: Deploying a wireless sensor network on the coal mines. In: 2007 IEEE International Conference on Networking, Sensing and Control, pp. 324–328 (April 2007)
9. Yang, W., Huang, Y.: Wireless sensor network based coal mine wireless and integrated security monitoring information system. In: Proceedings of the Sixth International Conference on Networking, ICN 2007, pp. 22–28. IEEE Computer Society, Washington, DC (2007)
10. Li, Z., Liu, Y.: Underground structure monitoring with wireless sensor networks. In: 6th International Symposium on Information Processing in Sensor Networks, IPSN 2007, pp. 69–78 (April 2007)
11. Khadivi, A., Hasler, M.: Fire detection and localization using wireless sensor networks. In: Kominos, N. (ed.) SENSAPEAL 2009. LNICST, vol. 29, pp. 16–26. Springer, Heidelberg (2010)
12. Sha, K., Shi, W., Watkins, O.: Using wireless sensor networks for fire rescue applications: Requirements and challenges. In: 2006 IEEE International Conference on Electro/information Technology, pp. 239–244 (May 2006)
13. Ai, C., Guo, L., Cai, Z., Li, Y.: Processing area queries in wireless sensor networks. In: 5th International Conference on Mobile Ad-hoc and Sensor Networks, MSN 2009, pp. 1–8 (December 2009)
14. Tinyos faq (online), <http://www.tinyos.net/faq.html> (accessed December 20, 2013)
15. Perkins, C.E., Bhagwat, P.: Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. SIGCOMM Comput. Commun. Rev. 24(4), 234–244 (1994)

# Multi-Hierarchies: Accurately Computing Realtime Statistical Measures on Data Streams

Penghe Qi and Shengfei Shi

Harbin Institute of Technology, Harbin, China  
qph807@163.com, shengfei@hit.edu.cn

**Abstract.** Computing statistical measures is a fundamental problem for mining data streams. Sometimes user wants to query the realtime correlation of data streams. In this paper, we introduce a system for computing realtime statistical measures of data streams. The system updates the realtime summaries which are used to compute affine relationships. We process every elements in every data stream only once, and get a similar accuracy rating compared with the static methods. To the best of our knowledge, we present a new method of computing affine relationship. Our system employs the multi-Hierarchies approach in the Sliding Window Model. First, we change AFCLST Clustering algorithm. Second, the Bottom-Up Updating algorithm updates the summaries which every hierarchy has stored after the Cumulative Calculation algorithms. Third, the Query Response algorithm uses summaries to compute the statistical measure. Finally, we establish the accuracy rating of our approach by performing several experiments on real datasets.

## 1 Introduction

In the recent years the data we have to process is becoming more and more. However, the users want to get the realtime information of the data, such as correlation coefficient. Information solutions should be realtime and satisfy the scalable data management. Primary sources of data streams are sensor networks, financial applications and social net working applications. The typical need on such data is querying some realtime correlation between two data streams, or finding out whose statistical measure (covariance, etc) has great change in the data lately, which is a realtime query requesting.

### 1.1 Background

Recently, the realtime processing for data streams is mostly based on the DFT. In [3], the correlation coefficient is computed based on DFT in the Sliding Window Model. [4] uses base window to compute the correlation coefficient. These approaches [3],[4],[9], which process the realtime correlation coefficient, are not universal for computing every statistical measure(mean, median, correlation coefficient, dot product, etc.).

[20] computes the k-medians and covariance over data stream windows, but is not suitable for other statistical measures. In [2] and [14], the monitoring method of streams can help us to design the realtime system. The methods in [9]-[11] can not find out whose statistical measures have great change lately. However, the realtime information is very valuable for user. In the paper, we satisfy the realtime query request.

In the Sliding Window Model,[16] divides the window into some hierarchies, which is suitable for realtime request. Because the affine relationship has many advantages [1], but there is not a method to compute the realtime affine relationship. In this paper, we propose a method to update the summaries which are key to compute the realtime affine relationship, then we can compute the realtime statistical measures with the updated summaries. In the following section, we describe the new computing method of affine relationship, which is importable for updating the summaries in the system.

## 1.2 Theoretical Basis for Computing the Affine Relationship

Affine relationships have the feature of solving most of the statistical measures in the statical case [1]. If we want to use the affine relationships to compute the realtime statistical measures for data streams in the dynamic case, we should change the computing method of the affine relationships. In the Table 1, we explain these symbols which are used in the following.

**Table 1.** Symbols

| Symbol           | Description                              |
|------------------|------------------------------------------|
| $S$              | Data matrix                              |
| $x$ or $x_i$     | Column vector                            |
| $x_{i,j}$        | element j of a vector $x_i$              |
| $(x_i, x_j)$     | Stream pair                              |
| $w(x_i)$         | cluster identifier of the vector $x_i$   |
| $r$              | Cluster matrix                           |
| $r_l$            | Column vector $l$ of $r$                 |
| $(x_i, r_l)$     | Pivot pair                               |
| $R^n$            | Set of n-dimensional real column vectors |
| $R^{m \times n}$ | Set of m-by-n real matrices              |

Before presenting the modified computing method of the affine relationships, we first analyze the disadvantage of the primary computing method of the affine relationships[1].

Consider the stream pair matrix  $B = [x_i \ x_j]$  and the pivot pair matrix  $A = [x_i \ r_{w(x_j)} \ 1_t]$ , where  $x_i$ ,  $x_j$ ,  $r_{w(x_j)}$  are column vectors of size  $t$ ; thus,

$A \in R^{r \times 3}$ ,  $B \in R^{r \times 2}$ . The new data  $b_{t+1} = [x_{i,t+1} \ x_{j,t+1}]$  will flow into the  $B$ , where  $b_{t+1} \in R^{1 \times 2}$ . The new data  $a_{t+1} = [x_{i,t+1} \ r_{w(x_j),t+1} \ 1]$  will flow into the  $A$ , where  $a_{t+1} \in R^{1 \times 3}$ . In [1], the affine relationship  $AF$  is computed by  $AF = \text{pinv}(A) * B$ , where the  $AF \in R^{3 \times 2}$ . The  $\text{pinv}(A)$  computes the pseudo-inverse of the matrix  $A$ . However, when the new data  $a_{t+1}$  arrives,  $\text{pinv}(A)$  can not be computed expediently. So, we should propose a new computing method of  $AF$  so that we can update the realtime  $AF$  dynamically.

In the paper, the new method for computing the affine relationship is defined as  $AF = (A^T A)^{-1} A^T B$ , where  $(A^T A)^{-1} A^T$  is the left pseudo-inverse of the matrix  $A$ . We describe the difference between the left pseudo-inverse matrix and the pseudo-inverse matrix in the following.

**Definition 1:** Suppose  $A$  is the m-by-n real matrix. If the matrix  $L$  has these features:  
(1)  $L * A = I_n$ , (2)  $A * L \neq I_m$ , where  $L \in R^{n \times m}$ . Then, the matrix  $L$  is the left inverse matrix of the  $A$ .

**Definition 2:** Suppose  $A$  is the m-by-n real matrix. If the matrix  $R$  has these features:  
(1)  $A * R = I_m$  (2)  $R * A \neq I_n$ , where  $R \in R^{n \times m}$ . Then, the matrix  $R$  is the right inverse matrix of the  $A$ .

If  $m > n$ , the matrix  $A$  may have many left inverse matrices. Similarly, if  $m < n$ ,  $A$  may have many right inverse matrices. However, if  $m > n$  and the matrix  $A$  is column full rank, the matrix  $(A^T A)^{-1}$  is existing. So, the n-by-m matrix  $(A^T A)^{-1} A^T$  satisfy the definition of the left inverse matrix. Most of all, this matrix  $(A^T A)^{-1} A^T$  is one and only, and is called as the left pseudo-inverse matrix.

In the paper, the pivot pair matrix  $A = [x_i \ r_{w(x_j)} \ 1]$  is always column full rank. So, we can calculate the  $AF$  with the left pseudo-inverse matrix instead of the pseudo-inverse matrix. Under this kind of change, we can dynamically update the summaries which we have stored for computing the statistical measures of data streams.

We begin by presenting the Modified AFCLST Clustering algorithm in Section 2. In Section 3, we propose the Cumulative Calculation algorithms and the multi-Hierarchies Bottom-Up Updating algorithm for computing the realtime statistics measures. In Section 4, we introduce the Query Response algorithm for responding to the user's request. Last, several experiments are presented in Section 5, followed by a conclusion in Section 6.

## 2 Modified Affine Clustering

In [1], an affine clustering processing reduces the computing cost of the statics data streams. Similarly, we do the same operation before computing the realtime statistical measures. However, we make some changes in the clustering.

At first, we randomly select k data streams as the cluster's centers(Line 1-2). This main processing is similar to the K-means algorithm(Line 4-14). However, at the end of each iteration of the clustering, we compute the mean value of the data streams belong to the same cluster (Line 17-22) where the algorithm differs from [1], then update the clusters' center(Line 23).

---

**Algorithm 1.** The Modified AFCLST Clustering algorithm

---

**Input:** Data matrix  $S \in R^{l \times n}$ , maximum iteration  $\gamma_{\max}$ , number fo clusters  $k$ , minimum cluster changes  $\delta_{\min}$

**Output:** Cluster centers  $r_l$  and cluster assignment function  $w(v)$

```

1: for $l=1$ to k
2: $r_l = randcol(S)$
3: $nChg = -1$
4: for $iter=1$ to γ_{\max}
5: $\min Proj = \infty, clustID = 0$
6: $currNchg = -1$
7: for $j=1$ to n
8: for $l=1$ to k
9: $proj_e = \|x_j - r_l\|$
10: if $proj_e < \min Proj$
11: $clustID = l$
12: if $w(j) \neq clustID$
13: $currNchg = currNchg + 1$
14: $w(j) = clustID$
15: if $|nChg - currNchg| < \delta_{\min}$
16: break
17: for $l=1$ to k
18: $num = 0, Sum = 0$
19: for $j=1$ to n
20: if $w(j) == l$
21: $num = num + 1$
22: $Sum = Sum + x_j$
23: $r_l = Sum / num$
24: return $r_l, w(v)$

```

---

**Algorithm 2.** The Cumulative Calculation algorithm

---

**Input:** The new data  $S_{t+1} \in R^{l \times n}$ , cluster centers  $r_l$ , cluster assignment function  $w(v)$

**Output:** The cumulative summaries  $AB_{base}$  and  $AA_{base}$ , cluster centers  $r_l$

```

1: for $j=1$ to k
2: $num = 0, r_{j,t+1} = 1$
3: for $i=1$ to n
4: if $w(i) == j$
5: $r_{j,t+1} = r_{j,t+1} + x_{i,t+1}, num++$
6: $r_{j,t+1} = r_{j,t+1} / num$
7: for $i=1$ to $n-1$
8: for $j=i+1$ to n
9: if $(t+1)\%T == 1$
10: $AB_{base}(i, j) = 0$
11: $a_{t+1} = [x_{i,t+1} \quad r_{w(x_j),t+1} \quad 1]$
12: $b_{t+1} = [x_{i,t+1} \quad x_{j,t+1}]$
13: $AB_{base}(i, j) = AB_{base}(i, j) + a_{t+1}^T b_{t+1}$
14: for $i=1$ to n
15: for $j=1$ to k
16: if $(t+1)\%T == 1$
17: $AA_{base}(i, j) = 0$
18: $a_{t+1} = [x_{i,t+1} \quad r_{w(x_j),t+1} \quad 1]$
19: $AA_{base}(i, j) = AA_{base}(i, j) + a_{t+1}^T a_{t+1}$
20: if $(t+1)\%T == 0$
21: Bottom-Up Updating algorithm
 (AA_{base}, AB_{base})

```

---

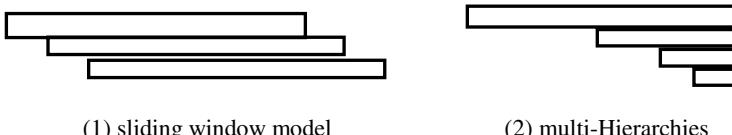
**Complexity Analysis:** The time complexity of the Modified AFCLST Clustering algorithm is similar to the *K-means* algorithm. It is not hard to analyze that the time complexity of the algorithm is  $O(n \times k \times \gamma_{\max})$ .

The clustering algorithm terminates when the cluster membership changes are less than  $\delta_{\min}$  or  $\gamma_{\max}$  iterations are completed. The cluster centers  $r_1, r_2, \dots, r_k$  and the cluster assignment function  $w(v): v \mapsto l$  which returns the cluster identifier  $l$  for a given data stream  $v$ . More details can be found in [1]. After the clustering, we can compute the summaries so that we can query the real-time statistical measures. What's more, the summaries we have stored can be updated when the new data flows into the system.

### 3 Computing Summaries in Sliding Window Model

The Sliding Windows Model continues M elements in the window. When the new data flows into the window, the oldest elements outflow from the window. The Fig. 1(1) gives more details.

If the size of the window is very large, sometimes the user wants to query the statistical measures over a certain time period of the window. The Sliding Window Model can be divided into the multi-Hierarchies from the bottom up. If the query time is equal to a certain hierarchy, the statistical measures can be computed by using the summaries directly. However, when the query time contains several hierarchies which have no the overlapping time, the result can not be computed directly. First, we combine the summaries of these hierarchies. Then, the statistical measures are got by computing the combined summaries. The Fig.1(2) can tell us more detail such as the time span of every hierarchy and the relationship between the neighboring hierarchies.



**Fig. 1.** Sliding Window Model and multi-Hierarchies

Supposing that the Sliding Window Model has *segs\_num* hierarchies and the size of the smallest hierarchy is  $T$ . We shore the summaries  $AA$ , where  $AA = A^T A$  is 3-by-3 matrix, and the summaries  $AB$ , where  $AB = A^T B$  is 3-by-2 matrix. For example,

$AA(i, j, l)$  is the summaries the pivot pair  $(x_i, r_j)$  has stored in the  $l_{th}$  hierarchy, and,  $AB(i, j, l)$  is the summaries the stream pair  $(x_i, x_j)$  has stored in the  $l_{th}$  hierarchy.

### 3.1 Cumulative Calculation Algorithm

In consideration of the efficient and the reality, the system does not update the summaries when a new data  $S_{t+1}$  flows into the system. The system does not update the summaries until the size of the new data is equal to the smallest hierarchy. In order to deal with the new data only once, the Cumulative Calculation algorithm firstly processes the new data when it flows into the system. When the size of the new data is equal to the smallest hierarchy, the system will update the summaries by the Bottom-Up Updating algorithm. The system never read the new data from the disk again in the following process.

The Cumulative Calculation algorithm updates the current clusters' center(Line 1-6). Then, it computes the current summaries respectively(Line 7-13, Line 14-19). When the current time satisfies the condition(Line 20), the system calls the Bottom-Up Updating algorithm(Line 21).

**Complexity Analysis:** The Cumulative Calculation algorithm monitors the current moment. All the time, it calculates the summaries of the new data. The space complexity of  $AB_{base}$  is  $O(n^2)$ , and the space complexity of  $AA_{base}$  is  $O(k \times n)$ . In a actual situation, the number of clusters k is constant. So, the space complexity is  $O(n^2)$ .

### 3.2 Bottom-Up Updating Algorithm

When the System calls the Bottom-Up Updating algorithm, the summaries in every hierarchy will be update from the bottom up. First, we compute the top-most hierarchy we should update at the current moment(Line 1-6). Then, the algorithm updates the summaries of the stream pairs in the system(Line 7-18), and updates the summaries of the pivot pairs(Line 21), which is similar to the process(Line 9-18). [12],[13],[18],[19] give more details about the management for the summaries of affine relationships.

**Complexity Analysis:** In the system, the space complexity of  $AB$  is  $O(segs\_num \times n^2)$ , and the space complexity of  $AA$  is  $O(segs\_num \times k \times n)$ . In a actual situation, the number of clusters  $k$  and the number of the hierarchies  $segs\_num$  are constant. So, the space complexity is  $O(n^2)$ , which is similar to [1]. Above all, the level of RMSE is similar to the statics situation in [1], which is demonstrated in the Section 5.

**Algorithm 3.** The Bottom-Up Updating algorithm

**Input:** The cumulative summaries  $AB_{base}$  and  $AA_{base}$

**Output:** The cumulative summaries  $AB$  and  $AA$  in every hierarchy

```

1: grade = 0
2: for j=1 to segs_num
3: if ((t%M)/T)%power(2,i)==0
4: grade = i+1
5: if grade == 0
6: grade = 1
7: for i=1 to n-1
8: for j=i+1 to n
9: ABtemp[grade-1] = 03,2
10: for l=1 to grade
11: if l==1
12: if l < grade
13: ABtemp[l] = ABbase(i, j) + AB(i, j, l)
14: AB(i, j, l) = ABbase(i, j)
15: else
16: if l < grade
17: ABtemp[l] = ABtemp[l-1] + AB(i, j, l)
18: AB(i, j, l) = ABtemp[l-1]
19: for i=1 to n
20: for j=1 to k
21: deal with AA in the same way
22: return AB, AA

```

**Algorithm 4.** The Query Response algorithm

**Input:** query request  $(x_i, x_j)$ , time period  $[t_1, t_2]$

**Output:** The statistical measures  $result$

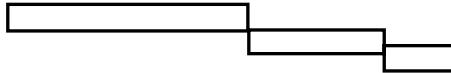
```

1: grade = (t2 - t1) / T
2: number[segs_num] = 0
3: i = 0, j = 0
4: while grade != 0
5: i ++
6: if (grade & 1) == 1
7: number[j ++] = i
8: grade >> 1
9: i = 0, AA_temp = 03,3, AB_temp = 03,2
10: while number[i] != 0
11: AA_temp = AAx_i, r_{i(x_j)}, number[i] + AA_temp
12: AB_temp = ABx_i, x_j, number[i] + AB_temp
13: i ++
14: measure = function_1(AA_temp)
15: AF = inv(AA_temp) * AB_temp
16: result = function_2(AF, measure)
17: return result

```

## 4 Querying Statistical Measures in Sliding Window Model

In the system, the summaries contain some statistical information in different time period. When the user hands in the query request which is equal to a certain hierarchy, the system can return the statistical measures after computing easily. However, when the time period contains several hierarchies which have no the overlapping time, the statistical measures are computed after combining the summaries of these hierarchies, which is more visual in the Fig. 2.



**Fig. 2.** Time period. All of time intervals have no the same time period

Supposing that the time period overlaps these hierarchies from  $i_{th}$  to  $j_{th}$ , Where  $i < j$ , the summaries of these hierarchies have these features:

$$(1) AA(,, i \sim j) = \sum_{l=i}^j AA(,, l), (2) AB(,, i \sim j) = \sum_{l=i}^j AB(,, l).$$

These features of the summaries is important to compute the realtime statistical measures when the query time contains several hierarchies. The new computing method of the affine relationship is so fatal that we can satisfy this query request. The Query Response algorithm finds out these hierarchies which the time period contains(Line 1-8). Then, it combines the summaries which are included in the time period (Line 10-13). The statistical measures of the pivot pair  $(x_i, r_{w(x_j)})$  and the stream pair  $(x_i, x_j)$  are computed by the *function\_1* (Line 14)and *function\_2*(Line 16) respectively[1][8]. Such as, in the *function\_1*, the covariance matrix of the pivot pair can be easily computed with the several elements of the summaries AA [5], [6]. The affine relationship between the pivot pair and the stream pair is computed in Line 15.

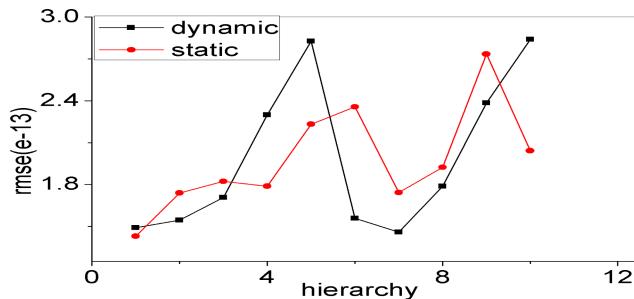
**Complexity Analysis:** The summaries in the system are stored like the hash map. The time cost of the responding to the query request depends on querying in the hash map. After a simple computing in the memory, the system returns the statistical measure of the query request. It is obvious that the computing cost in the Query Response algorithm is similar to O(1).

## 5 Experiment Evaluation

In this section we perform several experiments to prove the accuracy rating and the feasibility of the solution. In section 5.1, we analyze the accuracy rating for computing the realtime statistical measures of the data streams. We find that the accuracy rating is equal to that in the statical statistical measures in [1]. In section 5.2, we query some stream pairs, and prove the universality of the solution for computing and querying different statistical of the stream pairs.

### 5.1 Analyzing the Accuracy Rating

In this section, the number of the hierarchies (segs\_num) is 5, the size of the smallest hierarchy (T) is 10, and the size of the sliding windows model (M) is 160. We have 100 data streams, and every stream has 320 elements. We set the number of the clusters (k ) is 4. The Modified AFCLST clustering algorithm processes the first 10 elements in every stream. The system calls the Bottom-Up Updating algorithm every ten elements. The Fig. 3 is the accuracy rating.



**Fig. 3.** Accuracy rating, The red line is the RMSE[1] of the realtime statistical measures in the dynamic situation, and the black line is the RMSE of the statistical measures in the statical situation

The accuracy rating in the dynamic situation is very similar to that of the statical situation, where the undulation in Fig.3 is not the key we analyze. Observe that the percentage is kept in the same level after changing the computing method of the affine relationship, and the RMSE does not increase observably. Moreover, the system never execute the clustering again after clustering the data streams in the beginning.

## 5.2 Universality of the Solution

The affine relationship can be used in computing most of the statistical measures, such as mean, dot product, covariance, correlation coefficient, Jaccard coefficient, etc. So, we change the computing method of the affine relationship in order to satisfying user's more query request with a small computational cost. Most of the statistical measures of the pivot pairs can be computed so quickly by the function\_1 that we can compute the query request by combining the summaries we have stored. Table 2 shows the solution's universality of computing for the most of the statistical measures.

**Table 2.** RMSE of some statistical measures

| measure<br>RMSE<br>number  | 1        | 10        | 100      | 500      | 1000     |
|----------------------------|----------|-----------|----------|----------|----------|
| Mean                       | 1.36e-13 | 2.19e-13  | 1.25e-13 | 2.92e-13 | 2.17e-13 |
| Dou product                | 2.66e-13 | 3.45e-13  | 3.03e-13 | 4.55e-13 | 3.24e-13 |
| Covariance                 | 1.49e-13 | 1.71e-13  | 1.54e-13 | 2.29e-13 | 1.56e-13 |
| Correlation<br>coefficient | 1.46e-13 | 2.383e-13 | 1.78e-13 | 2.12e-13 | 1.99e-13 |

Table 2 depicts that the affine relationship can be used to compute many statistical measures dynamically. When the numbers of the stream pairs which are queried increase from 1 to 1000, the RMSE does not undulate observably. What is more, the summaries the system has stored can be used to compute the affine relationship quickly.

## 6 Conclusion

In this paper, for the first time, we define the new computing method of the affine relationships for computing the realtime statistical measures dynamically, and improve the affine clustering algorithm for finding the good affine relationships between the stream pair and the pivot pair. Then, we calculate the new base summaries of the new data for updating the summaries of every hierarchy. We update the summaries the system has stored to compute the realtime affine relationships from bottom up. We propose a query processing for responding to the user. Lastly, we performed several experiments highlighting the effectiveness of the new computing method of the affine relationships.

## References

1. Sathe, S., Aberer, K.: AFFINITY: Efficiently Querying Statistical Measures on Time-Series Data. In: ICDE 2006 (2013)
2. Zhu, Y., Shasha, D.: Statstream:Statistical monitoring of thousands of data streams in real time. In: VLDB, pp. 358–369 (2002)
3. Li, C.-S., Yu, P.S., Castelli, V.: HierarchyScan:A hierarchical similarity search algorithm for databases of long sequences. In: ICDE, pp. 546–553 (1996)
4. Cole, R., Shasha, D., Zhao, X.: Fast window correlations over uncooperative time series. In: SIGKDD, pp. 743–749 (2005)
5. Maronna, R., Martin, R., Yohai, V.: Robust statistics. Wiley Series in Probability and Statistics (2006)
6. Golub, G., Van Loan, C.: Matrix computations. The Johns Hopkins University Press (1996)
7. Sathe, S., Aberer, K.: AFFINITY:Efficiently querying statistical measures on time-series data. EPFL. Tech. Rep. (2012), <http://infoscience.epfl.ch/record/180121>
8. Bishop, C.: Pattern recognition and machine learning. Springer (2006)
9. Gehrke, J., Korn, F., Srivastava, D.: Oncomputing correlated aggregates over continual data streams. In: SIGMOD, pp. 13–24 (2001)
10. Ke, Y., Cheng, J., Ng, W.: Correlation search in graph databases. In: SIGKDD, pp. 390–399 (2007)
11. Agrawal, R., Lin, K., Sawhney, H., Shim, K.: Fast similarity search in the presence of noise,scaling and translation in time-series databases. In: VLDB (1995)
12. Reeves, G., Liu, J., Nath, S., Zhao, F.: Managing massive time series streams with multi-scale compressed trickles. In: VLDB, pp. 97–108 (2009)
13. Bulut, A., Singh, A.: SWAT: Hierarchical stream Summarization in Large Networks. In: Proc. of the 19th International Conference on Data Engineering, pp. 303–314 (2003)

14. Bulut, A., Ambuj, K., Singh, A.: A Unified Framework for Monitoring Data Stream in Real Time. In: Proc. of the 21st International Conference on Data Engineering, pp. 44–55 (2005)
15. Richard, A.J., Dean, W.W.: Applied Multivariate Statical Analysis, 6th edn. Prentice Hall, New York (2007)
16. Rodrigues, P.P., Gama, J., Pedroso, J.P.: ODAC: Hierarchical clustering of time series data streams. In: SIAM (2006)
17. Domingos, P., Hulten, C.: Mining high-speed data streams. In: Proc. of the KDD (2000), <http://citeseer.ist.psu.edu/domigos00mining.html>
18. Greenwald, M., Khanna, S.: Space-efficient online computation of quantile summaries. In: SIGMOD, pp. 58–66 (2001)
19. Qiao, L., Agrawal, D., El Abbadi, A.: Rhist: adaptive summarization over continuous data streams. In: Proceeding of the Eleventh International Conference on Information and Knowledge Management, pp. 469–476 (2002)
20. Babcock, B., Datar, M., Motwani, R., Callaghan, L.: Maintaining covariance and k-medians over data stream windows. In: Proc. of the 22nd ACM SIGACT-SIGMOD-SIGART Symp., Principles of Database Systems, pp. 234–243 (2003)
21. Jagadish, H., Mendelzon, A.: Similarity-based queries for time series data. In: SIGMOD, pp. 13–25 (1997)

# Iceberg Cube Query on Heterogeneous Information Networks

Dan Yin and Hong Gao

School of Computer Science and Technology,  
Harbin Institute of Technology Harbin, 150001, China  
[yindan630@gmail.com](mailto:yindan630@gmail.com), [honggao@hit.edu.cn](mailto:honggao@hit.edu.cn)

**Abstract.** With the rapid development of social networks and cyber-physical systems, heterogeneous information networks have become increasingly popular. In many cases, such networks contain multiple types of objects and links. In traditional data warehouses and OLAP technique, iceberg cube are those whose aggregated functions are larger than a specific threshold. However traditional iceberg cube analysis techniques cannot be directly applied to graphs for finding interesting cubes due to the lack of structures in graphs. This paper addresses the interesting problem of iceberg cube query on heterogeneous information networks. Based on the intuition, we proposed a cube model based on attribute consistency and link consistency. And the iceberg cubes computation is realized by pruning on the two parts. And random walk is used to aggregate the nodes in heterogeneous information networks for approximate iceberg cubes. Experiments on real world heterogeneous information networks demonstrate the algorithm effective and efficiency.

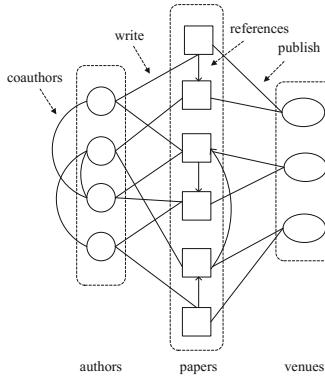
**Keywords:** Iceberg cube, heterogeneous information network, random walk.

## 1 Introduction

With the rapid development of social networks, cyber-physical systems and on-line shopping sites, heterogeneous information networks have become increasingly popular and content-rich over time. Such networks contain multiple types of objects and links. So heterogeneous information networks are anywhere. Next we give a real world example.

Figure 1 gives us an example of heterogeneous information network bibliographic information network. The nodes are partitioned according the their types and the edges are constructed based on the relationships between different nodes. Finally, the graphs contains three types of entities: papers( $P$ ), authors( $A$ ) and venues( $V$ ), and four type edges among these nodes. The edges represent cooperation relationships between  $A$ , the writing relationships between  $A$  and  $P$ , the citation relationships between  $P$  and the publishing relationship between  $P$  and  $V$ . The attributes of nodes are:  $P$ (title, fields, key words);  $A$ (names, companies, fields and locations);  $V$ (name, year).

Multiple types of objects and links in this network. For papers that are associated with text attributes, using link information can further help the clustering quality when the observations of the text data is very limited.



**Fig. 1.** Bibliographic information network

In traditional data warehouses and OLAP technique, iceberg cube are those whose aggregated functions are larger than a specific threshold.

The lattice of a heterogeneous information networks is huge by exponent size. Most of these cuboids are redundancy and useless. So the iceberg cube query is useful and effective for users to discover the most interesting cuboids in such complicated graphs. However traditional multi-dimensional data analysis techniques such as iceberg cube cannot be directly applied to graphs for finding interesting or anomalous vertices due to the lack of dimensionality in graphs.

The research work on iceberg query in large graphs is a new topic. Until now, there has little work on this field. The only existed study of iceberg analysis in graphs is by Li[4], which focused on the iceberg vertices for which the aggregation of an attribute in their vicinities as above a given threshold. So it cannot help handle the iceberg cube query for which the aggregation of a cuboid, which involves attributes and structures of the nodes in the cuboid. Especially in heterogeneous information networks, the problem seems more challenging and interesting.

In this paper, we explore a cube model based on attribute consistency and link consistency for heterogeneous information networks. And further the iceberg cube query is realized by pruning on the two parts respectively. Random walk is used to aggregation the nodes in heterogeneous information networks for approximate computation. By defining the meta-path between different types of node, the probability of reaching another vertex with respect to the meta-path reflects how close the two vertexes are. We will also show in our experiments that the iceberg cube query can help users to discover interesting results from DBLP networks.

The primary contributions of this paper are shown as follow:

1. We propose a novel concept, the first definition of iceberg cube on graphs, also the first on heterogeneous information networks;
2. We design a model for the problem of iceberg cube on heterogeneous information networks, which focuses on the attribute consistency and link consistency with user-depended threshold;
3. We design an excellent algorithm to compute the iceberg cubes, where the efficient pruning strategy improves the performances greatly;
4. Experiments real-world large graphs demonstrate the proposed algorithms in this paper are effective and scalable, and the iceberg cubes on heterogeneous information networks are valuable.

## 2 Related Work

The research work on iceberg query in large graphs is a new topic. Until now, there has little work on this field. The iceberg query in large graphs is first proposed by Li[4] in 2013. which focused on the iceberg vertices for which the aggregation of an attribute in their vicinities as above a given threshold.

Chen et al. [1] first proposes the idea of OLAP on graphs. In [1,2], the input data is a set of graphs, and each graph has a set of attributes. All the nodes in the set of graphs are the same types. The algorithm aggregates multiple graphs into a summary static graph based on the attributes of each graph.

Graph Cube[10] studies the OLAP techniques on a single graph, where nodes are uniform in types and have a group of attributes. But it ignores the structures of graphs in cubes. Tian et al.[8,9] aggregates the graph to a summarized version based on user's input of node attributes and edge relationships. In each group, all the nodes are homogeneous in terms of both attributes and relationships. It preforms rolling-up and drilling-down by decreasing and increasing the number groups in the summary graphs. While in our paper, cube query and OLAP operations are performed along the dimensions of nodes' types and attributes.

Most research work on heterogeneous information networks are done by Sun [7,3,6,5], which are based on the idea of *meta-path*. [3] constructs the multi-type networks into star schema which includes more information. But they ignore the multi attributes of nodes and cannot model for graphs with more types of nodes. Search techniques based on meta-path in heterogeneous information networks has been proposed by Sun. [6] searches the top-k similar entities using meta-path in heterogeneous information networks, where entities can be correlated by different meta-path representing different kinds of relations. For example, author-paper-author represents closely corporation. Such intuition could be used for predicting links in graph[5]. Such existing techniques cannot handle the problem of OLAP on heterogeneous information networks.

### 3 Preliminaries

**Definition 1.** *Heterogeneous information network.* A heterogeneous information network is triple tuple  $G = (V, E, A_v, A_e)$ , where  $V$  is the node set,  $E$  is the edge set,  $A_v$  is the attributes of nodes and  $A_e$  is the attributes of edges of  $G$ . Node set  $\mathcal{V} = \{\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_m\}$ , where  $V$  is the set of nodes of type  $i$ . Each type node  $\mathcal{V}_i$  have  $l_i$  attributes  $A(\mathcal{V}_i)$ . For arbitrary  $v \in \mathcal{V}_i$ ,  $A_j(v)$  is the  $j$ th attribute of  $v$ , where  $1 \leq j \leq l_i$ .  $A_v = \bigcup A(\mathcal{V}_i)$  is the set of node attributes of all the types.  $A_e = (A_{e1}, A_{e2}, \dots, A_{em})$  is the attribute set of edges of  $G$ . For arbitrary  $e \in E$ , there exists  $A(e) \in A_e$ .

**Definition 2.** *Partition.* A partition of the node set of a heterogeneous information network  $G = (V, E, A_v, A_e)$  is a family of disjoint subsets  $U_i$  whose union is  $V$ , i.e.,  $\mathcal{P}(V) = \{U_1, U_2, \dots, U_p\}$ , where  $p = |\mathcal{P}(V)|$ , and iff it satisfies:

1. For arbitrary  $U_i \in \mathcal{P}(V)$ ,  $U_i \subseteq V$  and  $U_i \neq \emptyset$ ;
2.  $V(G) = \bigcup_{i=1}^p U_i$ ;
3. For arbitrary  $U_i, U_j \in \mathcal{P}(V)$ , and  $i \neq j$ ,  $U_i \cap U_j = \emptyset$ .

#### 3.1 Meta Path-Based Cuboid

**Definition 3.** *Meta-path.* A meta-path  $P$  is a path defined on the heterogeneous information network  $G = (V, E, A_v, A_e)$ , and is denoted in the form of  $A_1 \xrightarrow{R_1} A_2 \xrightarrow{R_2} \dots \xrightarrow{R_l} A_{l+1}$ , which defines a composite relation  $R = R_1 \circ R_2 \dots \circ R_l$  between types  $A_l$  and  $A_{l+1}$ , where  $\circ$  denotes the composition operator on relations.

In this paper, we mainly take the symmetric meta-path in the form of  $P = P_l P_l^{-1}$  into consideration. In DBLP networks, two authors can be connected via 2-length "author-paper-author" path, 3-length "author-paper-venue-paper-author" path and so on.

**Definition 4.** *Meta-path-based similarity measure.* Given a symmetric meta-path  $P$ , similarity measure between two objects  $x$  and  $y$  of the same type is:

$$s(x, y) = \frac{2 \times |\{p_{x \rightsquigarrow y} : p_{x \rightsquigarrow y} \in P\}|}{|\{p_{x \rightsquigarrow x} : p_{x \rightsquigarrow x} \in P\}| + |\{p_{y \rightsquigarrow y} : p_{y \rightsquigarrow y} \in P\}|}$$

where  $p_{x \rightsquigarrow y}$  is a path instance between  $x$  and  $y$ ,  $p_{x \rightsquigarrow x}$  is that between  $x$  and  $x$ , and  $p_{y \rightsquigarrow y}$  is that between  $y$  and  $y$ .

**Definition 5.** *Cuboid.* Given a heterogeneous information network  $G = (V, E, A_v, A_e)$ , which has  $m$  types of nodes and the node set  $V = \{\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_m\}$ . Given query node types  $T \subseteq \{1, 2, \dots, m\}$ , for arbitrary  $i \in T$ , the query attributes of type  $i$  are  $R_i \subseteq 1, 2, \dots, l_i$ , and the referenced symmetric meta-path is  $\theta_i$ . So the cuboid based on  $(T, R_i, \theta_i)$  of  $G = (V, E, A_v, A_e)$  is an aggregated graph  $C = (V_c, E_c)$ , which satisfies:

1.  $V_c = \{U_1, U_2, \dots, U_k\}$  is a partition of  $\bigcup_{i \in T} V_i$ ;
2. The nodes in  $U_i$  have the same type. For arbitrary  $u, v \in U_i$ , assume that  $u$  and  $v$  are the  $n$ th type nodes, we have that  $A_j(u) = A_j(v)$ ,  $j \in R_n$ . The weight of  $U_i$  is  $w(U_i) = \Gamma_U(v)$ , where  $\Gamma_V(\cdot)$  is the aggregate function in  $V$ ;
3.  $(U_i, U_j) \in E_c$  iff  $u \in U_i$  and  $v \in U_j$ ,  $(u, v) \in E$ . The weight of  $(U_i, U_j)$  is  $w(U_i, U_j) = \Gamma_E((u, v))$ , where  $\Gamma_E(\cdot)$  is the aggregate function in  $E$ , and  $(u, v) \in E$ .
4. The meta-path similarity measure of nodes in  $U_i$  is larger than  $\delta$ .

Some explanations for definition 5:

1. In graph OLAP, these measures can also be average degree, centrality, degree, diameter, containment and so on, besides the traditional measures like MAX, MIN, SUM, COUNT, AVG etc. Note that the measures for vertex and edge can be different. In these examples, COUNT, SUM, AVG are the measures for both vertex and edge dimensions.
2. When the threshold  $\delta$  is equal to 1, the nodes in the same group have exactly same links according to the meta-path given. The larger  $\delta$  is, the more similarly the nodes perform in the light of user-selected meta-path.

Above all, we give the aggregated functions of cuboid in heterogeneous information networks in definition 6.

**Definition 6. Cuboid Aggregated Function.** Given a heterogeneous information network  $G = (V, E, A_v, A_e)$ , cuboid  $C = (V_c, E_c, w)$ , where  $V_c = \{U_1, U_2, \dots, U_k\}$ , the aggregated function of  $AGG(C) = \max \Gamma(U_i)$ , where  $U_i \in V_c$ .

### 3.2 Iceberg Cube Query

In traditional data warehouse and OLAP technique, iceberg cuboids whose measures are larger than a specific threshold.

**Definition 7. Iceberg Cube.** For a cube  $c$ , if its cuboid aggregated function is above a certain threshold,  $c$  is called an iceberg cube; otherwise it is called a non-iceberg vertex.

The problem description of iceberg cube query is:

**Input:** 1. a heterogeneous information network  $G = (V, E, A_v, A_e)$ ; 2. iceberg threshold  $\xi$ ; 3. cuboid threshold  $\delta$ ; 4. meta-path;

**Output:** Iceberg cubes w.r.t  $\xi$ .

## 4 Iceberg Cube Computation Model

In this section, we propose a novel model for iceberg cube computation in heterogeneous information networks. Firstly we give a baseline model for computing the cuboids in heterogeneous information networks from attribute consistency and link consistency. Next we designed a iceberg cuboid computation algorithm based on pruning strategy.

#### 4.1 Model Attribute Consistency

Nodes in the same cuboid should have consistent attributes according to user selected. The algorithm of modeling attribute consistency in heterogeneous information networks is easy to realize by scanning the graph once time. The time complexity is  $O(|V| + |E|)$ .

#### 4.2 Model Link Consistency Based on Meta-Path

The nodes in the same group should have similar structure based on the given meta-path. In fact, it's also a semantic attribute of nodes in another form. For example, authors' similarities about meta-path "author-paper-author" represent the research interests of them. So We make the nodes in the same group have similar structures in line with user-selected. From the view of links, the more similar the two nodes are in terms of structures, the more likely they are connected by a link. In order to quantitatively measure the consistency of nodes with the network structures, we use the meta-path based similarity measure defined in 4.

The pseudo-code of the naive algorithm for computing cuboids in heterogeneous information networks is described in algorithm 1. The time complexity is  $O(|V| + |E|)$ .

---

**Algorithm 1.** Exact algorithm for link consistency in heterogeneous information networks

---

**Input:** A heterogeneous information network  $G = (V, E, A_v, A_e)$ , cuboid  $C = (V_c, E_c)$ , 1-length meta-path  $\theta_i = V_i \rightarrow V_j \rightarrow V_i$ .

**Output:** Iceberg cuboid w.r.t query.

```

1: Initialize cuboid threshold of δ with 1;
2: Initialize hash table mapping from nodes to groups
3: for $U_k \in U_1, U_2, \dots, U_p$ do
4: for $v \in U_k$ do
5: for $u \in V_j$ do
6: if $(v, u) \in E$ then
7: Construct a new group for v if not existed;
8: Insert v ;
9: Construct cuboid $C = (V_c, E_c)$;
10: Compute Γ_{V_c} and Γ_{E_c} ;
11: return C
```

---

#### 4.3 Iceberg Cube Computation Based on Pruning

In this part, we introduce the details of computing iceberg cubes based on the procedure of the former two parts. The effective pruning strategies are carried out in attribute consistency and link consistency respectively. Therefore, the searching space can be reduced significantly.

In this simple situation, the threshold  $\delta$  in cuboid is set to 1, and the threshold  $\xi$  in iceberg query is decided by users. The naive algorithm for computing iceberg cubes in heterogeneous information networks time complexity is  $O(|V| + |E|)$ . Due to the space limited, we omit the algorithm pseudo-code.

Next we will study the more complex case. Besides for the pruning in the procedure of attribute consistency, the approximated random walk pruning is executed in link consistency. The main idea is presented in algorithm 2.

---

**Algorithm 2.** Approximate algorithm for iceberg cubes in heterogeneous information networks

---

**Input:** A heterogeneous information network  $G = (V, E, A_v, A_e)$ , threshold of iceberg  $\xi$ , threshold of cuboids  $\delta$ , set of meta-paths.

**Output:**Iceberg Cube.

```

1: Initialize hash table mapping from nodes to groups
2: Initialize random walks number RW ;
3: for $U_k \in U_1, U_2, \dots, U_p$ do
4: for $v \in U_k$ do
5: for $u \in V_j$ do
6: if $(v, u) \in E$ then
7: Construct a new group for v if not existed;
8: Insert v ;
9: delete the groups whose sizes are smaller than ξ ;
10: for $U_k \in U_1, U_2, \dots, U_p$ do
11: repeat
12: for $v \in U_k$ do
13: random walk starting from v ;
14: if random walk ends with $u \in U_k$ then
15: check the paths between v and u ;
16: until Number of random walks reaches RW ;
17: Compute similarity of nodes in U_k ;
18: Cluster the nodes in U_k guaranteeing threshold of cuboid δ ;
19: Construct cuboid $C = (V_c, E_c)$;
20: Compute Γ_{V_c} and Γ_{E_c} ;
21: return C
```

---

## 5 Experiment Evaluation

For the experiments, we use the real world data set extracted from DBLP to show the effectiveness and efficiency of the proposed algorithms. All the experiments are implemented on a Microsoft Windows 7 machine with an Intel(R) Core i5-2400 CPU 3.1GHz and 4GB main memory. Programs are compiled by Microsoft Visual Studio 2010.

## 5.1 Data Sets

We use the DBLP data set downloaded in Nov. 2009 as the main test dataset. The data set includes four types of nodes, papers, authors, venues and terms. And four types of edges exist between these nodes, the writing relation between author and paper, the publishing relation between paper and venue and the relation between paper and term representing the papers have the terms as key contents. We use a subset by extracting a subset from the full dataset by Sun et al. [6], which contains 8340 authors, 5000 papers, 4729 terms and 37 venues. There are 13351 edges between authors and papers, 5000 edges between papers and venues, and 32540 edges between papers and terms. In this paper, we select the COUNT aggregated function as the  $\Gamma(\cdot)$  function.

## 5.2 Performances Study

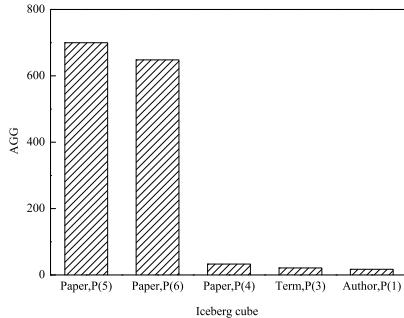
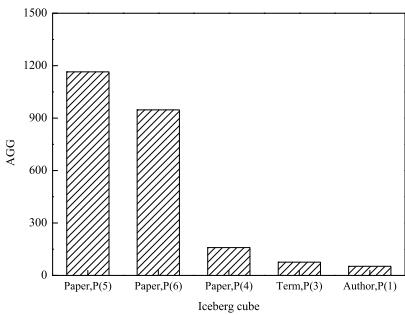
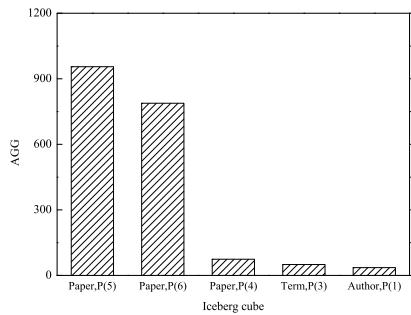
First, we evaluate the exact iceberg cube algorithm in simple case, where the cuboid threshold  $\delta=1$ , to show that our algorithm is able to find interesting cubes. We conduct a case study on DBLP: (1) given an iceberg threshold  $\xi$ ; (2) given a set of meta-paths. we find the iceberg cubes and remove the rest. The query example is shown as follow:

### Query

- (a) Iceberg cube threshold  $\xi = 15$ ;
- (b) Set of meta-paths for DBLP networks:
  - (1)  $P_1 = A - P - A$ ; (2)  $P_2 = V - P - V$ ; (3)  $P_3 = T - P - T$ ; (4)  $P_4 = P - A - P$ ;
  - (5)  $P_5 = P - V - P$ ;
  - (6)  $P_6 = P - T - P$ .

In the results of effectiveness experiments below, the x-axis represents the iceberg cube which has two parts: nodes types and its referenced meta-path. y-axis shows the AGG values corresponding to the x-axis. Figure 2 shows the iceberg cubes in DBLP networks. As shown in the figure, there are five cuboids above the threshold  $\xi$ . And three of them are paper nodes. Because the papers are the central core of the networks. The paper cuboid based on meta-path "P-V-P" has the highest AGG 700. And the paper cuboid based on meta-path "P-T-P" follows with AGG 648. But the meta-path "P-A-P" has little AGG on papers. It can be seen that papers are more similar on their venues and terms than authors. Every venue publishes hundreds of papers every year, and plenty of papers on similar topics are published. However, an author can write finite papers in all his life compared with the total papers published in all venues and in all fields.

Next we evaluate the performance of the approximate algorithm. We set the round of random walk to 20. We investigate the approximate algorithm with different cuboid thresholds  $\delta = 0.9$  and  $\delta = 0.8$ . In this part, we use query 1 previous, and the iceberg threshold  $\xi$  is set to 15 and 100 respectively. Figure 3 and figure 4 give the iceberg cubes by approximate algorithm with cuboid thresholds  $\delta = 0.8$  and  $\delta = 0.9$ . Compared with exact algorithm, the approximate

**Fig. 2.** Results of iceberg cube in DBLP**Fig. 3.** Approximate iceberg cube with  $\delta = 0.8$  in DBLP**Fig. 4.** Approximate iceberg cube with  $\delta = 0.9$  in DBLP

algorithm could get iceberg cubes with larger  $AGG$ . This is because the link consistency based on meta-path is relaxed by  $\delta$ . Meanwhile, the smaller  $\delta$  is, the more the link consistency relaxed. So approximate algorithm with smaller  $\delta$  could get higher  $AGG$  iceberg cubes.

## 6 Conclusions

This paper introduces a novel concept, iceberg cube query in heterogeneous information networks. A cube model based on attribute consistency and link consistency. And the iceberg cubes computation is realized by pruning on the two parts. And random walk is used to aggregation the nodes in heterogeneous information networks for approximate computation. Experiments on real world heterogeneous information networks demonstrate the algorithm effective and efficiency. Iceberg cube query can help users to discover interesting results from DBLP networks.

**Acknowledgement.** This work is supported in part by the National Grand Fundamental Research 973 Program of China under grant 2012CB316200, the Program of the National Natural Science Foundation of China under grant 61190115, 61173022, 61033015, 61173023.

## References

1. Chen, C., Yan, X., Zhu, F., Han, J., Yu, P.S.: Graph olap: Towards online analytical processing on graphs. In: Proc. of Int. Conf. on Data Mining, ICDM 2008, pp. 103–112. IEEE, NJ (2008)
2. Chen, C., Yan, X., Zhu, F., Han, J., Yu, P.S.: Graph olap: a multi-dimensional framework for graph data analysis. Knowledge and Information Systems 21(1), 41–63 (2009)
3. Ji, M., Han, J., Danilevsky, M.: Ranking-based classification of heterogeneous information networks. In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1298–1306. ACM (2011)
4. Li, N., Guan, Z., Ren, L., Wu, J., Han, J., Yan, X.: giceberg: Towards iceberg analysis in large graphs. In: Proceedings of the 2013 IEEE International Conference on Data Engineering, pp. 1021–1032. IEEE (2013)
5. Sun, Y., Barber, R., Gupta, M.: Co-author relationship prediction in heterogeneous bibliographic networks. In: International Conference on Advances in Social Networks Analysis and Mining, pp. 121–128. IEEE, NJ (2011)
6. Sun, Y., Han, J., Yan, X., Yu, P.S., Wu, T.: Pathsim: Meta path-based top-k similarity search in heterogeneous information networks. In: Proc. VLDB Endow., vol. 4(11), pp. 992–1003. ACM, New York (2011)
7. Sun, Y., Norick, B., Han, J., Yan, X., Yu, P.S., Yu, X.: Integrating meta-path selection with user-guided object clustering in heterogeneous information networks. In: Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2012, pp. 1348–1356. ACM, New York (2012)
8. Tian, Y., Hankins, R.A., Patel, J.M.: Efficient aggregation for graph summarization. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, SIGMOD 2008, pp. 567–580. ACM, New York (2008)
9. Zhang, N., Tian, Y., Patel: Discovery-driven graph summarization. In: Proceeding of IEEE International Conference on Data Engineering, pp. 880–891. IEEE, Piscataway (2010)
10. Zhao, P., Li, X., Xin, D., Han, J.: Graph cube: on warehousing and olap multi-dimensional networks. In: Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, SIGMOD 2011, pp. 853–864. ACM, New York (2011)

# An Energy Optimization Algorithm of Date Centers Base on Price Volatility

Liang Hao, Gang Cui, Wende Ke, and Bindi You

School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China  
{haoliangoorr, cuigang, wendeke, huaidanxiaotian}@163.com

**Abstract.** Optimizing the energy consumption of date centers has become a focus of attention in mobile cloud computing. However, the existing researches on energy management are rarely associated with the effect of price volatility. In this paper we propos an algorithm of energy optimization base on price volatility. The tariff interval is set base on the world time zones and energy optimization is iterative calculations using dynamic price method, a dependencies hierarchical strategy of tasks base on this policy is proposed and designed. By increasing the parallelism and execution dependencies of tasks, the amount of data movement and idle probability of data center nodes is reduced. The experimental results show that the algorithm can significantly minimize energy consumption while improving the efficiency of system.

**Keywords:** Tariff interval, mobile cloud computing, energy optimization, price volatility.

## 1 Introduction

As the new technology the mobile internet and cloud computing combining, mobile cloud computing industry is increasingly becoming a new hotspot. By using the characteristics of cloud computing that concentrates virtualization on the physical resources, dynamic management of virtual resources, and demand assignment achieve mobile internet services efficient and stable service. However, with the global climate warming, as well as the low-carbon economy and green energy is proposed, energy consumption of mobile cloud computing has become a critical issue[1].

Energy problem is getting worse, how to solve the problems of energy consumption optimization of mobile cloud computing is particularly crucial at the lowest cost down. In this paper, the use of resources in multiple data center for mobile cloud computing, the current situation of energy consumption, regional energy and other aspects are studied deeply in the literature [2]. The low cost constraint is proposed in resource scheduling algorithms in the literature [3]. The energy consumption of mobile cloud computing is minimized through the design of task hierarchical strategy, and the scheduling studies of cloud computing based on world time zone is proposed.

## 2 Related Work

Nowadays the research on the impacts of energy cost optimization techniques in cloud pricing model are rarely considered in the existing energy consumption

algorithms. The literature [4-6] considers that reduce data center energy costs is in line with the commercial interests. By using time series analysis techniques, and combines with different pricing strategies to predict cloud market demand, considering the difference in a multi-user market demand in the literature [7]. The dynamic resource allocation problem is modeled into a multidimensional knapsack problem in the literature. The best return algorithm is given for different pricing model. Anton in the literature [8] proposes a cloud system framework, and designs three kinds of virtual machine migration algorithm base on this framework.

However, the algorithm did not consider the cost and time constraints, lack of a detailed reasoning process in virtual machines, and did not consider the cost of porting between different geographical cloud modules. Cardosa in the literature [9-10] performs tasks that own a similar start and end time together from the perspective of map reduce module. But the energy consumption requires migration tasks is not considered. These energy optimization algorithms are considered from the perspective of the virtual machine, but a lot of energy is consumed by the virtual machine itself in Adding and transplantation.

Base on the above deficiencies, a distributed scheduling algorithm on the energy consumption of mobile cloud computing is studied in this paper, ECMC is proposed, and the algorithm combines cost of scheduling as constraints, not only in reducing the consumption while meeting the cost constraints.

### 3 Problem Model

All resources are existed as the form of services in the cloud computing model. So some definitions are given use the resource model as following.

Definition 1,  $S(t, v, h)$  is a collection of random tasks, and  $t$  is a set of tasks. When  $i$  is not equal  $j$ ,  $t_i$  is not equal  $t_j$ ,  $v(i, j)$  are the relationship for the task execution,  $w$  is the workload demands of task.

Definition 2, cloud computing model is  $(P, E, W_1, W_2)$ , whereas  $P$  is a set of  $p$  cloud data center servers,  $E$  is a corresponding matrix that the random task to a processor node,  $E_{ij}$  indicates that task  $t_i$  execution on the processor  $P_j$ .  $W_1$  is idle power of computing node,  $W_2$  is the peak power of node.

Definition 3, the network bandwidth matrix of each cloud data center is  

$$D = \begin{bmatrix} d_{11} & d_{12} & \dots & d_{1p} \\ \vdots & \vdots & \ddots & \vdots \\ d_{p1} & d_{p2} & \dots & d_{pp} \end{bmatrix}$$
, where  $d_{ij}$  is the transmission bandwidth between the net-

work nodes in the cloud data center.

Definition 4,  $S_1, S_2, \dots, S_X$  is the tasks level derived in the task hierarchical algorithm, each layer is stratified base on relevance. The workload of  $S_1$  is greater than  $S_2$ . When the cost constraints are not satisfied, the first task layer is scheduled to perform. The hierarchical algorithm will be given in 3.2.

Definition 5, the price of electricity is defined as  $R$ . Due to electricity prices around the world region vary, so the value of  $R$  is different. But because of the impact of different factors such as time, execution efficient, so the energy is different. In this paper, six world time zones electricity are assumed in the energy consumption study. They are Asia-Pacific time zone, the European time zone, North and South America time zone, Oceania and the New Zealand time zone, Africa time zone. There are 20 data centers in each time zone is assumed, 128 data centers in total. The real work-load, network conditions and the price cost is different due to differences of time zone. So the time zone prices are as defined  $R = \{R_1, R_2, \dots, R_6\}$  in the study.

The network transmission distance is  $Z$ . The cost of the task in cloud is defined as  $M$ , the cost of task are  $M_1, M_2, \dots, M_n$  respectively. The transmission power is defined as  $W_3$ . The energy consumption is defined as  $E$ . And  $f$  is the frequency of computing nodes;  $u$  is the utilization of computing nodes. Energy optimization with cost constraints can significantly minimize energy consumption while saving the cost of services and improving the efficiency of system significantly. The model is formally described as follows:

$$\sum_{i=0}^n \sum_{k=1}^k Y_{ik} R_{ik} = M \quad (1)$$

$$Y_{ik} \in \{0,1\} \quad (2)$$

$$\text{s.t. } \sum_{k=1}^n Y_{ik} = 1, \forall i \in V \quad (3)$$

$$F_i \leq F_j - \sum_{k=1}^n t_{ik} Y_{ik} \quad (4)$$

$$\text{Min } E \quad (5)$$

$Y_{ik}$  is a Boolean variable in the above formula, which means that you can only choose one service task to perform,  $F_i$  means that The minimum completion time of each task. (1) represents that the agreed total cost of a given cloud service is given. (2) represents that  $Y_{ik}$  is a Boolean variable. (3) represents that each task only can select a service node to perform. (4) indicates that the tasks meet the partial order. (5) means energy consumption will be minimized.

## 4 Design and Analysis of Algorithms

### 4.1 Analysis of Energy Consumption

According to the comparison of idle nodes and peak power nodes in the literature [7], it can be calculated, the power of idle computing nodes account for about 60% of peak power in cloud computing, so idle node consumes a lot of energy. And the

compute nodes running at full load in a data center can not reaches peak power  $W_1$  due to CPU utilization., so that the idle nodes consumption in cloud occupy most of the total energy consumption. How to optimize the energy consumption of the idle nodes in cloud data centers has become the primary problem. The number of total data center computing nodes is assumed  $p$ . The percentage of idle nodes is assumed  $B$ , so the computing nodes that are being performed can be expressed as  $(1-B)$ , total energy consumption  $E$  can be expressed as:

$$\Delta E = W_1 p f(1-B)t_1 + W_2 p B t_2 + W_3 \frac{Z_{ij}}{D_{ij}} \quad (6)$$

It can be seen from the Equation (6), the calculation time, the peak and idle power, and total number of nodes is constants. The size of energy consumption is mainly relevant with the percentage  $B$  of idle nodes.  $B$ -substitution is carried out in the Equation (6) as follows:

$$\Delta E = W_1 p f + W_3 \frac{Z_{ij}}{D_{ij}} + (W_2 p t_2 - W_1 p f t_1)B \quad (7)$$

It can be seen from the Equation (7), the energy consumption of computing nodes can be reduced by reducing the percentage of idle nodes. So a hierarchical task strategy base on dependencies and energy consumption are proposed. This strategy calculates the task dependency through data collection in cloud data center firstly, and according to demand for energy work the tasks are stratified by hierarchical algorithm. The first floor tasks are scheduled into idle server to perform priority, so that the percentage of idle computing node is reduced.

## 4.2 Dependencies Hierarchical Strategy

The correlation degree of the task is calculated according to the needs of  $h$  data and the amount of computing nodes workload in the task hierarchical strategy. The calculated results would be divided into  $m$  layers according to the exponential distribution of correlation degrees. Task increments are formally expressed as:

$$S_X = S_{X-1} + \Delta h \quad (8)$$

$$X = \frac{\sum_{i=1}^p \int_0^t f_i(t) u_i(t)}{\log_2 \sum_{i=1}^p \int_0^t f_i(t) u_i(t)} \quad (9)$$

$$\Delta h = \frac{\int_{t_{p-1}}^{t_p} f_n(t) u_n(t) - \int_{t_1}^{t_2} f_1(t) u_1(t)}{X} \quad (10)$$

In the above formula,  $m$  is the task number of layers. The greatest work demand of task layer  $S_1$  is the first layer, the other sort order is  $S_1, S_2, \dots, S_X$ . The percentage of

idle nodes is as the target in scheduling algorithm. Firstly, the first floor tasks are scheduled to idle data centers with small price to running. When scheduling needs come again, the next layer tasks are scheduled in order to idle or sub-idle data center for running. The movement amount of data compute nodes is reduced; the overhead of task execution is saved by increasing the parallel characteristics of task execution in hierarchical algorithm.

### 4.3 Algorithm Description

Resource scheduling optimization algorithm of energy consumption for mobile cloud computing with cost constraints (ECMC) gave the initial cost of tasks, energy consumption. When the initial cost is less than the minimum cost constraints, the algorithm is ends. Otherwise, the tasks are stratified according to workload needs as hierarchical algorithm. These dates are collected hierarchically and calculated by cloud data centers. At the same time the cost of time region is compared with each other, and every floor tasks are scheduled priority to idle data center with low cost.

The first task layer  $S_1$  is scheduled to idle servers with low cost for running. The total consumption cost would be compared with the initial cost after the end of scheduling. It is end until the cost is less than or equal to the minimum cost constraints. Otherwise, the next task layer would be scheduled until the minimum cost requirement is met. Algorithm is as follows:

```

L1: for all incoming tasks, generate R and R'
L2: if R' ≤ R , jump L13
L3: else if R' ≥ R
L4: create S1,S2,…SX using task hierarchical strategy
L5: for all date centers P1,P2,…Pp , calculate W and K
L6:for(i=1;i<p ;i++) , j=i+1
L7:if WPi < WPj , W= WPi , K= KPi
L8:else while WPi = WPj caculate KPi and KPj
L9:if KPi < KPj , P= WPi
L10:scheduling Si to date center Pi , calculate R'
L11:if R' ≤ R , jump 13
L12:else continue loop
L13: return E

```

### 4.4 Analysis of Algorithms

Because the energy is equal to power multiplied by time, so when smaller electricity prices areas are select by tasks, the consumption cost is calculated as follows:

$$R = \left( W_3 \frac{Z}{D_{ij}} + W_2 t \right) K_j \quad (11)$$

Equation (11) is the total cost when tasks are dispatched to a new node. After a long distance and lower-cost cloud server area is selected, the resulting price difference and the energy consumption difference are calculated as follows respectively:

$$\Delta E = \left( W_3 \frac{Z}{D_{ij}} + W_2 t \right) - W_1 t \quad (12)$$

$$\Delta R = W_1 t K_i - \left( W_3 \frac{Z}{D_{ij}} + W_2 t \right) K_j \quad (13)$$

Equation (12) is the energy difference generated by the new node after the scheduling. Equation (13) is the difference of the resulting cost. The difference between the cost and the lowest cost constraint at this time would be compared after calculating.

#### 4.5 Analysis of Algorithm Complexity

The complexity of ECMC algorithm is determined on the predetermined gap between the lowest cost constraints and the initial cost. The current cost is getting close to the lowest cost after each iteration calculation of the algorithm, so the algorithm is convergent. The complexity of algorithm depends on the price comparison between cloud servers. More cloud servers, the comparison and the search are more complicated. When the initial cost is close to the lowest cost, task iteratively, so the maximum complexity of the algorithm is  $PN$ ,  $P$  is selectable cloud servers regional nodes,  $N$  is the total number of tasks.

### 5 Simulation Experiment

#### 5.1 Experimental Environment Settings

To test the performance and operating efficiency of ECMC algorithm under different environments, the experimental environment is 30 systems with LINUX2.6.18 kernel, CPU is Inter Core (TM) 2 Duo 1.86GHz, RAM is 2G,, Hard disk is 500GB, 100M network bandwidth to simulate the cloud computing environment in this paper, JAVA programming language is used to program in the algorithm.

In order to compare the performance of the ECMC algorithm, a comparison of three kinds of the energy optimization algorithm of random tasks is made in the experiments. They are the MIN-MIN algorithm studied in the literature [9], the Cluster algorithm in the literature [10], and our algorithm. The basic idea of the MIN-MIN algorithm is: The algorithm calculates the order of scheduling task priority from an average of implementation, and the task is assigned priority to computing nodes with the minimum average power to perform. Cluster Strategy: The tasks strategy is

mentioned in the literature [10]. In the establishment phase, all the random tasks are assigned to K data sets, and then K data sets are placed into the appropriate data centers. In the operational phase, the newly created task is placed into the appropriate data center.

In this paper, the three algorithms are compared and analyzed from six aspects of the average energy consumption, the average cost, the average power, the average response time, the data movement amount and load balance. The 4 parameters of the task scale, the number of data center node, the time zone of node, and cost constraints are select in the experiments. The nodes scale of the experimental task are {16,32, ..., 128} nodes, tasks scale are simulated {20,40, ..., 120}, etc., and electricity price of six regional nodes and real-time load are simulated. The average value under different scale is select as the experimental results, and the average cost, average execution power of the system, the average total energy consumption and other aspects are select to compare comprehensively between the three algorithms.

## 5.2 Experimental Results

**The Effects Resulting in Changes of Random Task Scale.** Figure 1 is a comparison of average energy consumption of the task execution under different system scale in three algorithms. It can be seen from the experimental results, the average power consumption of ECMC algorithm under different task scale have increased about 6.34% than MIN-MIN algorithm, reduced 11.52% compared to the Cluster strategy. The energy consumption of the three strategies tends to equal, when the scale of the task becomes larger gradually. This is mainly due to cost constraints of ECMC algorithm, the cloud computing service node in low price range and relatively distant is selects priority in the process of optimizing the energy consumption. Although ECMC algorithm saves the cost compared to MIN-MIN algorithm, increasing energy transmission slightly.

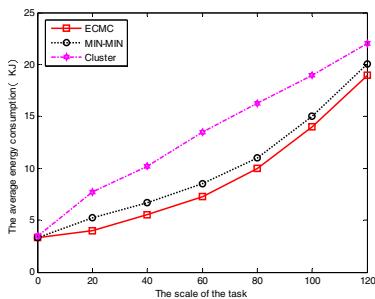


Fig. 1. Energy consumption comparison

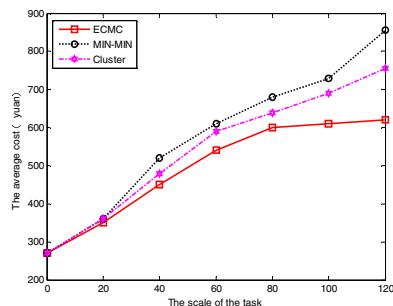


Fig. 2. Cost comparison

Figure 2 is the comparison of the average cost of system in different task scales in three algorithms. As can be seen from the figure, with the increasing of the amount of the task, the average cost of the three algorithms is gradually increasing. The average cost of ECMC algorithm and Cluster strategy is lower than the MIN-MIN algorithm. The average cost of ECMC algorithm is slightly lower than the average cost of Cluster strategy. When the amount of the task increases to a certain extent, ECMC algorithm remained unchanged. It is mainly due to cost constraints. Due to the correlation of data, the portion of the transmission energy is reduced in Cluster strategy.

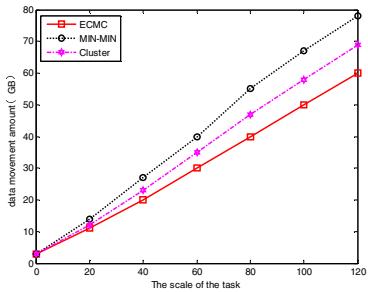


Fig. 3. Data movement comparison

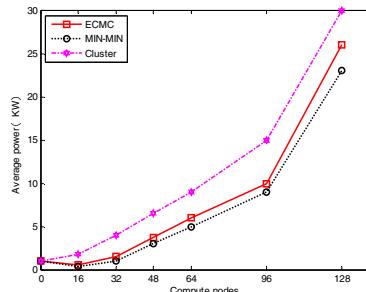
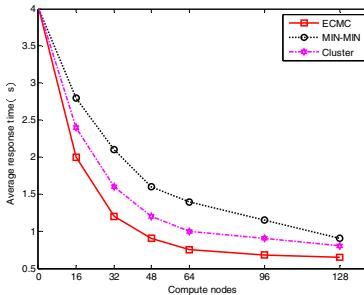
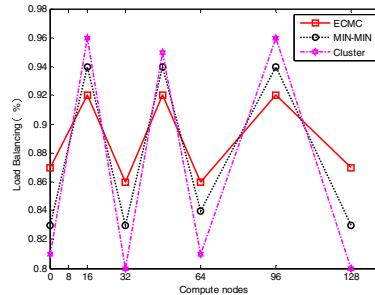


Fig. 4. System power comparison

Figure 3 is the comparison of the average movement amount of data under different task scales in three algorithms. As can be seen from the figure, the three algorithms are presented with linear growth trend with the growing of task scales. Since the task dependency is stratified in ECMC algorithm, the movement amount of data is the least. Since the dependencies of K tasks in Cluster Strategy, data movement is less than MIN-MIN algorithm.

**The Effects Resulting in Changes of Data Center Scales.** The comparison of system average power of the three algorithms in different computing node scales is shown in Figure 4. As can be seen from the figure, with the increase of computing nodes, the average power of the three algorithms decreases firstly and then increases. The average power of MIN-MIN algorithm is the lowest, and ECMC algorithm is better than Cluster strategy. This is due to when the node scales is less, the idle nodes are less and the response time is larger than Cluster strategy.

The comparison of the average response time and the system load balancing of the three algorithms in different computing node scales is shown in Figures 5 and Figures 6. As can be seen from the figure, with the increase of data center computing nodes, the response time of three algorithms show a downward trend and flat gradually. The response time of ECMC algorithm is shortest, and Cluster strategy is better than MIN-MIN algorithm. In Figure 6, the load balancing of ECMC is the best, MIN-MIN algorithm is the second, and Cluster strategy is the worst, which is mainly because the initial task allocation of Cluster strategy concentrate in a few of computing nodes.

**Fig. 5.** Response time comparison**Fig. 6.** Load balancing comparison

### 5.3 Experimental Summary

When the task scales change in the range of 0-120, the electricity price change in six regional nodes and the cost constrains in the closed interval [0,1000], ECMC algorithm is about 6.34% higher than MIN-MIN algorithm in the average energy consumption in different task scales, but ECMC algorithm is about 11.52% lower than Cluster strategy. With computing tasks gradually increase, the cost of ECMC algorithm saves about 12% compares to MIN-MIN algorithm and Cluster strategy. The movement amount of data of MIN-MIN algorithm and Cluster strategy floats in [35-45], but every 10 assignments is added to ECMC, the gap better than the other algorithms increase about 3%. When the data center nodes change in the range of 0-128, the average power of ECMC algorithm under different tasks increases about 5.97% than MIN-MIN algorithm, but reduce 18.56% than Cluster strategy. On the system response time and load balancing algorithm, ECMC algorithm is better than MIN-MIN algorithm and Cluster Strategy.

The experimental results show that, when ECMC algorithm is used, the advantages of mobile cloud computing is reflects on the cost, system response time and load balancing, under the premise of small increase of system power and energy consumption, which provides a better option for mobile cloud service providers.

## 6 Conclusions

The disadvantages of instantaneous energy consumption and transmission energy consumption increases too fast will be avoided in ECMC. ECMC algorithm increases the small amount of scheduling overhead, but reflects the great advantages of computing performance at the same time. And ECMC algorithm not only solves the problems of energy is wasted seriously, but also makes it possible to save costs. The advantages of mobile cloud computing are reflects on the cost, system response time and load balancing, under the premise of small increase of system power and energy consumption, which provides a better selection for mobile cloud service providers.

## References

1. Silva, M., Morais, H., Vale, Z.: An integrated approach for distributed energy resource short-term scheduling in smart grids considering realistic power system simulation. *Energy Conversion and Management* 64(3), 273–288 (2012)
2. Weiss, A.: Computing in the cloud. *ACM Networker*, pp. 8–25 (2007)
3. Young, C.L., Albert, Y.Z.: Energy efficient utilization of resources in cloud computing systems. *J. Supercomput.* 60(4), 268–280 (2012)
4. Jayant, B., Robert, W.A., Kerry, H., et al.: Green Cloud Computing: Balancing Energy in Processing, Storage and Transport 99(1), 149–167 (2011)
5. Rajni, L., Inderveer, C.: Bacterial foraging based hyper-heuristic for resource scheduling in. *Future Generation Computer Systems* 29(1), 751–762 (2013)
6. Lien, D., Bert, V.: Efficient resource management for virtual desktop cloud computing. *J. Supercomput.* 62(1), 741–767 (2012)
7. Jie, S., Tiantian, L.: Energy-Efficiency Model and Measuring Approach for Cloud Computing. *Journal of Software* 23(2), 200–213 (2012)
8. Dzmitry, K., Pascal, B., Samee, U.K.: Green Cloud: a packet-level simulator of energy-aware cloud computing data centers. *J. Supercomput.* 62(1), 1263–1283 (2012)
9. Anton, B., Jemal, A., Rajkumar, B.: Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing. *Future Generation Computer Systems* 28(1), 755–768 (2012)
10. Michael, C., Aameek, S.: Exploiting Spatio-Temporal Tradeoffs for Energy-Aware MapReduce in the Cloud. *IEEE Transactions on Computers* 61(12), 1731–1751 (2012)
11. Chervenak, A., Schuler, R.: A data placement service for petascale applications. *Super Computing* 62(1), 63–68 (2007)
12. Tang, M., Lee, X.T.B.S.: Dynamic replication algorithms for the multi-tier data grid. *Future Generation Computer Systems* 37(2), 775–790 (2005)
13. Yuan, D., Yang, Y.: A data placement strategy in scientific cloud workflows. *Future Generation Computer Systems* 26(8), 1200–1214 (2010)
14. Armbrust, M., Fox, A., Griffith, R., et al.: A view of cloud computing. *Communications of the ACM* 53(4), 50–58 (2010)
15. Verma, A., Ahuja, P.: Mapper: power and migration cost aware application placement in virtualized systems. *Lecture Notes in Computer Science* 53(46), 243–264 (2008)

# Keyword Search on Graphs Based on Content and Structure

Zhiqiang Zhang, Deping Xia, and Xiaoqin Xie

College of Computer Science and Technology, Harbin Engineering University, Harbin, China  
[zqzhang@hrbeu.edu.cn](mailto:zqzhang@hrbeu.edu.cn)

**Abstract.** In this paper, one new keyword search algorithm on graphs based on the content and structure (KSGCS) was proposed, which considers not only the structure of the distance between the nodes, but also the similarity between node and query in searching phase. We present new method for computing the similarity between node and query, and design the new methods for node searching algorithm and result generation algorithm.

## 1 Introduction

Keyword search over a graph finds a substructure of the graph containing all or some of the input keywords. Most of previous methods in this area find connected minimal trees that cover all the query keywords. Recently, it has been shown that finding subgraphs rather than trees can be more useful and informative for the users. However, the current tree or graph based on the existing methods may produce answers in which some content nodes are not very close to each other. They only considered the relevance between node and query and all the keyword nodes are regarded as the same. The answers are determined by the shortest distance between keyword nodes. So the real relevance between keyword node and query might be not high.

The main contributions of this paper are as follows: (1) we adopt two new factors PageRank and keyword position into the language model to calculate the similarity between graph nodes and query. (2) While choosing the candidate nodes for adding to result, KSGCS algorithm chooses the nodes with the shortest sum of distance to the result set, rather than the nodes with the shortest distance to a node.

## 2 Related Work

The BANKS system adopts the backward search method to find the minimum spanning tree [1]. But the algorithm need execute *Dijkstra* algorithm many times. Hristidis et al. propose an IR-Style keyword search sorting strategy over relational databases [2]. Inspired by the backward search algorithm in BANKS, Kacholia et al. propose the bidirectional extension algorithm. It replaces the single backward search with bidirectional search, so it can significantly improve the query performance of the system. BLINKS algorithm [4] uses the bi-level index and graph partition technology

to implement keywords search. In [5], Bolin Ding et al. put forward the group Steiner tree algorithm, which obtain the minimum cost of Steiner tree through dynamic programming with best-first strategy. Though the search results getting from the above algorithms cover all the keywords, but the distance between leave nodes may be far.

Guoliang Li et al. propose the EASE algorithm which defines the result as  $r$ -radius Steiner graph [6]. Since the algorithm for finding the maximal  $r$ -radius graph index regardless the keywords, if some of the highly ranked  $r$ -radius Steiner graphs are included in other lowly ranked graphs, this approach might miss them. Community [7] defines the result as multi-center subgraph. Lu Qin et al. also put forward the corresponding index technology to handle big graphs. But this approach has three drawbacks. First, some keyword nodes may close to each other, while others may be far away. Second, the performance is worse. Last, some center nodes and some middle nodes in results may be irrelevant to query. Kargar et al. defined  $r$ -clique to constraint the result [8]. This approach overcomes the drawbacks of community, and it ensures that the distance between any two nodes in results is no longer than  $r$ . In [9], Kargar et al. further propose an algorithm to generate duplication free and minimal results. But it needs explore each keyword node as a center for finding a result, so the performance is not good. In order to deal with big graphs, paper [10] proposes a distributed indexing technology, which deletes the nodes that wouldn't appear in top- $k$  results according to the topology information of graph before heuristic search. In [11], it is the first time to apply language model into keyword search on graphs.

In a word, the drawbacks of the existing algorithms are as follows: (1) all the keywords in query are regarded as the same. (2) In searching phase, the existing algorithms only consider the structure of results, but the similarity between query and keyword nodes may be not high. (3) Overlapping nodes may exist in results, and some related results may not be returned.

### 3 Preliminary Knowledge

Keyword search on graphs is defined that giving a set of data graph and keywords, finding the set of graph, the nodes in which can cover all keywords and also satisfy some structure constraints. The constraint condition for results in this paper is the same as [9]: (1) the subgraphs cover all keywords. (2) the distance between any two keyword nodes in result is not longer than  $r$ . (3) each node in result must cover at least one keyword which was not covered by other nodes. (4) the nodes in two subgraphs can't be same completely.

**Definition 1. Keyword node** The nodes contain one or more keywords.  $V_t$  is the node that contain keywords  $t$ .  $V_Q = \bigcup_{t \in Q} V_t$  means the node set that contain all keywords in query  $Q$ .

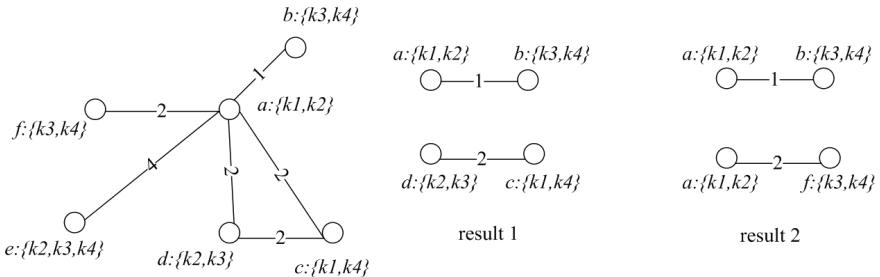
**Definition 2.  $r$ -cliques** Given a graph  $G$  and a query  $Q=\{k_1, k_2, \dots, k_l\}$ , the  $r$ -cliques related to query  $Q$  are the keyword nodes sets in  $G$ , which cover all query keywords and the shortest distance between any two nodes is no longer than  $r$ , where the shortest distance is the sum of weights on the shortest path between two nodes.

**Definition 3. Latent Steiner node** The nodes that appears in the shortest path between any keyword nodes is called Latent Steiner node. Notice that the shortest path defined in definition 3 is refers to the path with the least sum of edges weights.

**Definition 4. Latent Steiner Graph** The graph which construct by the keywords nodes and edges of Latent Steiner node, represented as *LSG*.

**Definition 5. Query Result** Given data graph  $G$  and query keywords  $Q=\{k_1, k_2, \dots, k_l\}$ , the query result defines as *answer*=(*LSG*,  $(n_1, n_2, \dots, n_k)$ ), where  $n_i$  ( $1 \leq i \leq k$ ) is the keyword node, *LSG* is Latent Steiner Graph.

In this paper, we define the query result as Latent Steiner Graph, because it can display how the keyword nodes are connected, and the Latent Steiner nodes in the graph are also highly correlated with keyword nodes. So, it can contain the nodes that don't contain any keywords, but they are highly related to query.



**Fig. 1.** Data graph and result of  $Q=\{k1, k2, k3, k4\}$

From Fig.1 we can see that the two results all satisfy the conditions that cover all keywords and dense structure. However, the result 1 is better than result 2, because there are no overlapped nodes in result 1, and it can contain more different keyword nodes. So, we introduce the concept of node repetition rate in section 5.3.

## 4 Keyword Search on Graph Based on the Content and Structure Methods

The system flowchart is shown in Fig. 2 which mainly includes four steps. First, compute the weight of graph, including the PageRank of nodes and the edge weights. Second, update the keyword nodes weight according to query. Third, search the data graph and find the top- $k$  results according to the sorting method. Last, generate the top- $k$  subgraphs as results.

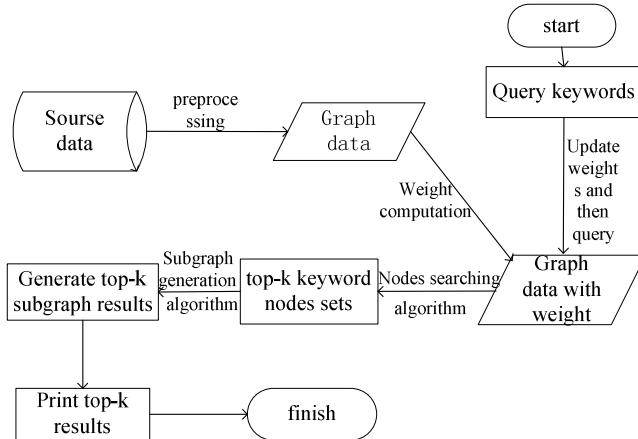
### 4.1 Sorting Method

For sorting the result of keyword search on graphs, we considered two aspects. First, in structure, the less the edge weights is, the stronger semantic relationship between

the nodes will be. Second, in content, the more keywords that nodes contain, and the stronger relevant would be with the query.

#### 4.1.1 Graph Weighting

The graph weighting include two aspects, node weighting and edge weighting. We compute the node weight based on the language model, while the existing algorithms adopt the *tf-idf* method. But the *tf-idf* method does not guarantee that nodes with more query keywords is assigned higher relevance score [12].



**Fig. 2.** The system flowchart

For computing the node weight, the nodes of graph are regard as the documents of the information retrieval, and the terms in nodes are regard as the terms in documents. The probability of node  $n$  for query  $Q$  is computed by formula (1):

$$P(n | Q) = P(n) \prod_i ((1 - \lambda)P(k_i | n) + \lambda P(k_i | G)) \quad (1)$$

Where  $0 < \lambda < 1$  is a smoothing parameter,  $P(n)$  is the PageRank of node  $n$ .  $P(k_i | n)$  and  $P(k_i | G)$  are the probability of keyword  $k_i$  present in node  $n$  and graph  $G$  respectively. The computation of  $P(k_i | n)$  and  $P(k_i | G)$  is shown as formula (2).

$$P(k_i | X) = \frac{tf(k_i, text(X))}{L_{text(X)}} \quad (2)$$

Where  $text(X)$  is the terms included by  $X$ ,  $X$  is node  $n$  or whole graph  $G$ ,  $L_{text(X)}$  is the term number in  $X$ . Moreover, users usually put the main keywords in forward position to express their intention. So, we introduce the position as another factor into the language model to measure the node weight. As shown in formula (3).

$$P(n|Q) = P(n) \prod_i pos_{k_i} [(1-\lambda)P(k_i|n) + \lambda P(k_i|G)] \quad (3)$$

Where  $pos_k = 1/\log_2(i+1)$  is the position weight of the keyword  $k_i$ . We apply logarithm function to formula (3) according to the monotone increasing nature of the logarithmic function and get the formula (4).

$$P(n|Q) = \ln P(n) + \sum_i \ln [pos_{k_i} ((1-\lambda)P(k_i|n) + \lambda P(k_i|G))] \quad (4)$$

Chengxiang Zhai et al. has proven that the smoothing effect is the best when  $\lambda$  is 0.1 by experience [13]. So, we also set  $\lambda$  to 0.1 in this paper.

Further we normalize the above formula and get formula (5). Where  $score(n, Q)$  is the node weight with respect to query  $Q$ .

$$score(n, Q) = 1 / \ln(-P(n|Q) + 2.718) \quad (5)$$

The constant 2.718 in formula (5) is to guarantee that the value range of node weight is [0,1]. This method is the same with [11], but we put the PageRank of nodes and the position of keywords into language model when computing the relevance between node and query, while they apply the language model directly to sort the results.

We adopt the same method with the [3,8,9] to compute edges weight. The edges weights are determined by the degree of nodes and the distance of edges that connect node  $u$  and  $v$  is defined below:

$$dist(u, v) = (\log_2(1 + u_{\deg}) + \log_2(1 + v_{\deg})) / 2 \quad (6)$$

Where  $u_{\deg}$  and  $v_{\deg}$  is the degree of node  $u$  and  $v$  respectively.

#### 4.1.2 Score Function

The results are generated by keyword nodes. So, we only consider the keyword node for sorting. In this paper, the relevance of node and query is the node weight, and the distance between two nodes is the shortest distance between nodes. In order to make the sorting mechanism more perfect, we add the nodes number in results, the proportion of keyword number and query number into the sorting mechanism. Formula (7) is the score function in this paper.

$$score = \frac{1}{size(answer)} * \frac{count(key_{answer})}{count(key_{query})} * ((1 - \beta)score(Q, N) + \beta score(Q, E)) \quad (7)$$

Where, (1)  $size(answer)$  is the number of keywords in result;  $count(key_{answer})$  and  $count(key_{query})$  is the number of keyword in result and query respectively; the parameter  $\beta$  is to measure the importance of edge weight. When edge weight is more important than node weight, we set  $\beta > 0.5$ , otherwise, set  $\beta < 0.5$ .

(2)  $score(Q, N)$  is the score of subgraphs with respect to query, we use the sum of all node score to compute it.

$$\text{score}(Q, N) = \sum_{n \in \text{answer}} \text{score}(n, Q) \quad (8)$$

Where,  $\text{score}(n, Q)$  is the weight of node  $n$ .

(3)  $\text{score}(Q, E)$  is the edge weight with respect to subgraphs, and computed by the shortest distance between keyword nodes. Since the node score is higher, the relevance is stronger, while the distance of nodes is larger, the relevance is weaker. So we should normalize the edge weight before compute the edge weight of subgraphs. After normalizing, when the edge weight is larger, the relevance of two nodes in structure is bigger. In this paper, we adopt the sum of shortest distance between nodes as the edge weight with respect to subgraphs. The computation formula is shown below.

$$\text{score}(Q, E) = \sum_{n_i, n_j \in \text{answer}} 1 / \ln(\text{dist}(n_i, n_j)) \quad (9)$$

Where,  $\text{dist}(n_i, n_j)$  is the shortest distance between node  $n_i$  and  $n_j$ .

## 4.2 Searching Method

We divide the search process into two parts in this paper. First, we search the data graph and find the node sets which cover all keywords. Then connect those nodes to construct the result subgraphs. Since we needn't consider the nodes that don't contain keywords when searching, it reduces the search space greatly and improves the search efficiency. In addition, generating the top- $k$  subgraphs from the keyword nodes is also faster than explore the whole graph. When searching, we firstly add the nodes with shortest distance into the result set, since those nodes are high relevant to query.

### 4.2.1 Search Node Algorithm

On the basis of the relevance of node and query, and the structure relevance of nodes, we also discuss how to make overlapping nodes in results as less as possible. Since so many subgraphs are found from the whole graph, however, the users usually pay more attention to the top- $k$  results.

The basic idea of the node searching algorithm is represented as followed. First, we find the set of keyword nodes and choose each node in set as the first node in results respectively. Then, the keywords that the first node contains are deleted from query then got a new query. Next, the next keyword node from the set is found and added into the result set, the process does not stop until the nodes can cover all keyword in query. Now we introduce the detail process to finding the next keyword. First, get the node sets containing same keyword, and find the nodes with the minimal sum of distance to nodes in results respectively, choose the node with the highest relevance and add it into result. Then update the query by deleting the keyword that the node contains. Then find the next node and add it into results until the query is null. The pseudo code of this procedure is described in Table 1.

**Table 1.** Keyword search algorithm

---

```

Algorithm 1: Keyword search algorithm
Input: data graph G , query Q , r , k
Output: top- k result
1 C = the set of nodes containing keywords
2 Initialize the k minimum heap $H \leftarrow \text{NULL}$
3 for all nodes in C do
4 compute each node weight in C use formula (5)
5 end for
6 for each node n_i in C do
7 $\text{answer} \leftarrow \{n_i\}$
8 $\text{Score}_{node} \leftarrow \text{score}(n_i)$
9 $Q \leftarrow Q - \text{keywords}(n_i)$
10 $(\text{answer}, \text{score}_{node}) \leftarrow \text{findAnswer}(G, Q, r, k, \text{answer},$
 $\text{Score}_{node})$
11 compute the score of each results use formula (7)
12 if(answer not in H)then
13 insert the result answer and the score score_{node} into
 H , the heap H is sorted according to the score
14 end if
15 end for
16 for $i \leftarrow 1$ to k do
17 output the results from heap
18 end for

```

---

In algorithm 1, the first line is to get the node sets that contain keywords, Initialization the  $k$  minimum heap in order to storage the results and the heap is initialized to null in line 2. Compute the nodes weight with respect to query in line 3-5. Choose every node in  $C$  as initial node respectively, and find the keyword nodes by call the `findAnswer` algorithm which is depicted in Table 2. Then compute the score of the subgraph result in line 6-11. At last output the  $k$  result from heap in line 16-18.

In algorithm 2, first get the node sets that contain one keyword in query respectively in line 1-2. Then in line 9-19 we find the nodes with the shortest distance between node and result from each set and the distance shouldn't more than  $r$ . If we find many nodes, we choose the nodes with the biggest intersection between query  $Q$  and the keywords in the node. From line 20 to line 24, we choose the node with the highest weight from above process as the next extent candidate. So, we not only consider the distance between nodes, but also consider the relevance between nodes and query. After we choose the extent candidate, we update the result and keywords in query, add the node into result and add the node weight into the sum of node weight of result. Then delete the keyword that the node contains from query. Last return the result.

**Table 2.** findAnswer algorithm

---

```

Algorithm 2: findAnswer algorithm
input: graph G , query Q , r , k , $answer$, $score$
output: r clique and the sum of node weight
1 for each key_i in Q do
2 D_i is the set of nodes which contain keywords key_i
3 while (Q is not null) do
4 for each keywords key_i in Q do
5 $leastDist[i] \leftarrow \infty$
6 $nearest[i] \leftarrow NULL$
7 end for
8 for each keyword key_i in Q do
9 for each node n_i^j in D_i do
10 for each node n_k in $answer$
11 if $dist(n_i^j, n_k) \leq r$ do
12 $dist \leftarrow \sum_{k \in answer} dist(n_i^j, n_k)$
13 end for
14 if $dist < leastDist[i]$ do
15 $leastDist[i] \leftarrow dist$
16 $nearest[i] \leftarrow n_i^j$
17 else if $dist = leastDist[i]$ do
18 $nearest[i] \leftarrow max(keywords(nearest[i]) \cap Q, keywords(n_i^j) \cap Q)$
19 end for
20 $nearest \leftarrow nearest[1]$
21 for $i \leftarrow 2$ to $size(Q)$
22 if $Score(nearest) < Score(nearest[i])$ then
23 $nearest \leftarrow nearest[i]$
24 end for
25 $answer \leftarrow answer \cup nearest$
26 $Score \leftarrow Score + Score(nearest)$
27 $Q \leftarrow Q - keywords(nearest)$
28 Delete D_i which not contain keyword in Q from D
29 end while
30 return ($answer$, $score$)

```

---

#### 4.2.2 Results Generation Algorithm

The results generation algorithm includes two parts. First, we find the shortest distance between any two nodes, and then the nodes and edges in the shortest path can make up the Latent Steiner Graph. The algorithm is shown in Table 3.

In above algorithm, compute the shortest distance between any nodes in every result and output the edges in the shortest path. In order to get the right result form that the previously defined, the keyword node in results are output before next process.

**Table 3.** Subgraph answer generation algorithm

---

```

Algorithm 3: Subgraph answer generation
input : graph G , keyword node $answers$
output : keyword nodes and the edge of Latent Steiner graph
 which containing keyword nodes
1 for $i=1$ to $\text{size}(answers)$ do
2 for any two nodes in $answer$ do
3 find the shortest path between the two nodes though
 the adjacency list of graph G
4 output the edges in the shortest path
5 output the keyword nodes in $answer$

```

---

## 5 Experimental Results

### 5.1 Data Sets

We use the DBLP and IMDb data sets to verify the feasibility and validity of the algorithm. The DBLP data can be modeled to undirected graph according to the citation relationships. There are 11350 nodes and 79002 edges in DBLP graph. IMDb data set describes the relationship between user and the evaluation to the film. We connect the user node and movie node by the ratings about movies from user. In IMDb graph, there are 1000 user nodes, 3952 movie nodes and 15517 undirected edges.

### 5.2 Search Efficiency

The queries used in our experiments are randomly generated from the different sets of keywords with the constraint that in each query all keywords have the same frequency

**Table 4.** Keywords in DBLP data set

| Keyword frequency | keywords                                                               |
|-------------------|------------------------------------------------------------------------|
| 0.0003            | scalable, protocols,<br>distance, discovery                            |
| 0.0006            | space, graph, routing,<br>scheme                                       |
| 0.0009            | environment, database,<br>support, development,<br>optimization, fuzzy |
| 0.0012            | dynamic, application,<br>modeling, logic                               |
| 0.0015            | web, parallel, control,<br>algorithms                                  |

**Table 5.** Keywords in IMDb data set

| keyword frequency | keywords                               |
|-------------------|----------------------------------------|
| 0.0003            | summer, bride, game,<br>dream          |
| 0.0006            | Friday, heaven, street,<br>party       |
| 0.0009            | death, star, all, girl,<br>lost, blood |
| 0.0012            | city, American, blue,<br>world         |
| 0.0015            | king, house, night, sto-<br>ry         |

(in order to better observe the relationship between run time and keyword frequency). Note that the set of input keywords is the same as the ones in [8] and [9]. The keywords used in experiments as shown in table 4 and 5.

In order to analyze the relationship between keywords and run time, we choose different number of keywords for query and find top-10 results.

We search the DBLP and IMDb data sets with Dup-Free algorithm [9] and the KSGCS algorithm respectively, the query time is shown in table 6. The  $r$  is set to 6 and 11 respectively, and keyword frequency is set to 0.0009.

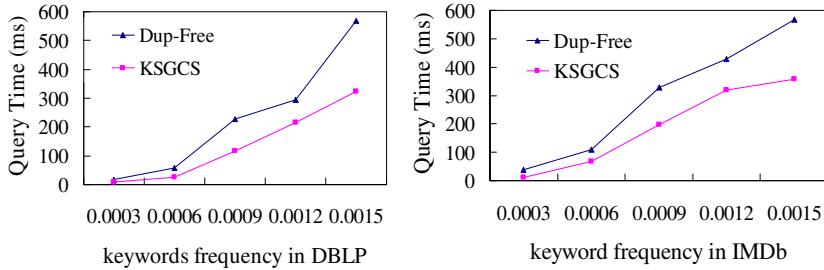
**Table 6.** Query time on DBLP and IMDb data set

| keywords<br>number | query time of<br>Dup-Free (ms)<br>in DBLP | query time of<br>KSGCS (ms)<br>in DBLP | query time of<br>Dup-Free<br>(ms) in IMDb | query time of<br>KSGCS (ms) |
|--------------------|-------------------------------------------|----------------------------------------|-------------------------------------------|-----------------------------|
| 2                  | 77.656                                    | 22.016                                 | 50.919                                    | 20.951                      |
| 3                  | 143.344                                   | 95.078                                 | 177.279                                   | 120.849                     |
| 4                  | 310.781                                   | 252.61                                 | 346.336                                   | 320.964                     |
| 5                  | 458.437                                   | 502.578                                | 478.683                                   | 539.751                     |

We can see from Table 6 that along with the increase of the number of keyword, the run time of KSGCS and Dup-Free are both increasing. Because the number of keyword nodes to be explored is increasing with the increase of number of keyword. In this way, the searching time from every keyword node will increase. So, the run time will increase. The run time of KSGCS algorithm is faster than Dup-Free algorithm when the number of keyword is fewer. With the increase of number of keywords, the difference between KSGCS and Dup-Free is becoming little. But the run time of KSGCS algorithm is slower than Dup-Free when the number of keywords is 5. That is because the time complexity of Dup-Free for finding top- $k$  is  $O(k*m^2*|D_{max}|^2)$ , while the time complexity of KSGCS is  $O(m^4*|D_{max}|^2)$ . The difference of running time from these two algorithms depends on the value of  $k$  and  $m^2$ . The run time of KSGCS will be longer than Dup-Free if the value of  $m^2$  is larger than  $k$ .

According to [14], the average number of query keywords is 2.91. So, we choose 3 keywords from Table 4 and Table 5 respectively and this is consistent with the statistics that the number of keywords used by users [15]. Fig. 3 describes the relationship between keyword frequency and query time in DBLP and IMDb data set respectively.

We can see from Fig. 3 that the query time of KSGCS and Dup-Free algorithm will increase with the increase of keyword frequency. The  $r$  is set to 6 and 11, the number of keywords is set to 3 respectively. This is because when the keyword frequency increases, the number of keyword nodes also increase. So the time of searching nodes is increasing. The run time of KSGCS algorithm is faster than Dup-Free, because we choose 3 keywords for searching to find top- $k$  results. This leads the advantage of run time on KSGCS algorithm more obvious.

**Fig. 3.** Query time on DBLP and IMDb data set

### 5.3 Search Quality

We adopt different methods to evaluate the quality of results in this paper. First we use the well-known Discounted Cumulative Gain (DCG) measure. Further, we propose the Average Repetition Rate (ARR) measure to evaluate the node repetition. In order to observe the relevance between results and query, we choose 10 queries with practical significance and analysis the results.

#### (I) DCG measure

DCG[16] measure adopts multistage evaluation method to evaluate the quality of search results. The formula is described as below.

$$DCG(p) = \sum_{i=1}^p (2^{rel_i} - 1) / \log_2(1+i) \quad (10)$$

Where,  $p$  is the number of results,  $rel_i$  is the score of the  $i^{\text{th}}$  subgraph in results.

In order to gain the score of every result, five users are asked to score the nodes in results according to the relevance with respect to the query. The score range is from 0 to 4. The score of the results is the average score of nodes in results, and the last score of result is the average score of the five users. The detailed role is as follows:

0: Irrelevant to the query; 1: relevant to the query, but the PageRank is low; 2: relevant to the query, and the PageRank is high; 3: strong relevant to the query, but the PageRank is low; 4: strong relevant to the query, and the PageRank is high.

The value of DCG is larger, the better of the results with the searching algorithm. For different query, we compute the corresponding DCG value of their results, and then compute the average DCG. The 10 queries are randomly generated from each data set. We compute the DCG of the results respectively, DCG(Dup-Free)=40.33514, DCG(KSGCS)=42.22944.

We can see that the DCG of KSGCS algorithm is higher than Dup-Free algorithm. This is because KSGCS not only chooses the shortest distance between nodes, and also considers the importance of nodes when searching the results. The algorithm adds the nodes with high weight into results first, in this way, the weight of nodes in results are all high. So, the weights of nodes which returned for users are all high, and these nodes are also important. When sorting, the nodes with high weight will be

ranked in top positions. However, the Dup-Free algorithm doesn't consider the importance of nodes and only consider the distance of nodes.

### (II) ARR measure

We propose the ARR(Average Repetition Rate) measures to evaluate the repetition of nodes in results. ARR is presented by the average probability that the repetition nodes with any two results. If the ARR is high, it indicates that the repetition frequency of the nodes in results is larger, so the quality of the results is worse. Otherwise, the quality is better. The computation is shown as formula (11).

$$ARR = \frac{\sum nodes(answer_i) \cap nodes(answer_j) / count(answer_i)}{C_N^2} \quad (11)$$

Where,  $nodes(answer_i)$  is the keyword nodes that result  $answer_i$  contains in result list,  $N$  is the number of results in result list. We only find the top- $k$  results in this paper, so the value of  $N$  is  $k$ ,  $count(answer_i)$  is the number of keyword nodes contained by  $answer_i$ .

Since the structure of the graph is different, the nodes repetition may vary different. So, we should search each data set with KSGCS algorithm and Dup-Free algorithm respectively and then compute the ARR of results. The following results described the difference of results quality between the two algorithms.

DBLP: ARR(Dup-Free)=0.43651, ARR(KSGCS)=0.38043

IMDb: ARR(Dup-Free)=0.53735, ARR(KSGCS)=0.39062

We can see the nodes repetition rate of KSGCS algorithm is lower than Dup-Free algorithm obviously. This is because we get an optimal solution from each keyword node. We can get different results from different nodes according to the searching process of KSGCS. It makes the keyword nodes appear in results at least once. While the Dup-Free algorithm starts from keywords nodes, the results may have overlapped nodes when many results can be found from the keyword node. So the quality of results get from KSGCS algorithm is higher than that from Dup-Free algorithm.

## 6 Conclusion

We proposed the keyword search on graphs based on content and structure in this paper. We mainly discussed the problems of nodes weighting, sorting results mechanism, nodes searching and results generation. We also analysis the query efficiency and the query quality through experiment. Since the query efficiency will be a problem to be solved when the data is big. So we need to find the other index method and parallel computing model to solve it.

**Acknowledgment.** This paper is supported by the National Natural Science Foundation of China under grant No.61202090, 61272184, the Program for New Century Excellent Talents in University No. NCET-11-0829, the Natural Science Foundation of Heilongjiang Province under grant F201130, and the Fundamental Research Funds for the Central Universities under grant No. HEUCF100609, HEUCFT1202.

## References

1. Bhalotia, G., Hulgeri, A., Nakhe, C., et al.: Keyword searching and browsing in databases using BANKS Data Engineering. In: Proceedings of the 18th International Conference on Data Engineering, pp. 431–440. IEEE (2002)
2. Hristidis, V., Gravano, L., Papakonstantinou, Y.: Efficient IR-style keyword search over relational databases. In: Proceedings of the 29th International Conference on Very Large Data Bases, pp. 850–861. VLDB Endowment (2003)
3. Kacholia, V., Pandit, S., Chakrabarti, S., et al.: Bidirectional expansion for keyword search on graph databases. In: Proceedings of the 31st International Conference on Very Large Data Bases, pp. 505–516. VLDB Endowment (2005)
4. He, H., Wang, H., Yang, J., et al.: BLINKS: ranked keyword searches on graphs. In: Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data, pp. 305–316. ACM (2007)
5. Ding, B., Xu Yu, J., Wang, S., et al.: Finding top-k min-cost connected trees in databases. In: IEEE 23rd International Conference on Data Engineering, ICDE 2007, pp. 836–845. IEEE (2007)
6. Li, G., Ooi, B.C., Feng, J., et al.: EASE: an effective 3-in-1 keyword search method for unstructured, semi-structured and structured data. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, pp. 903–914. ACM (2008)
7. Qin, L., Yu, J.X., Chang, L., et al.: Querying communities in relational databases. In: IEEE 25th International Conference on Data Engineering, ICDE 2009, pp. 724–735. IEEE (2009)
8. Kargar, M., An, A.: Keyword search in graphs: Finding r-cliques. Proceedings of the VLDB Endowment 4(10), 681–692 (2011)
9. Kargar, M., An, A., Yu, X.: Duplication free and minimal keyword search in large graphs. Department of Computer Science and Engineering, York University. Technical Report CSE-2013
10. Zhong, M., Liu, M.: A distributed index for efficient parallel top-k keyword search on massive graphs. In: Proceedings of the Twelfth International Workshop on Web Information and Data Management, pp. 27–32. ACM (2012)
11. Mass, Y., Sagiv, Y.: Language models for keyword search over data graphs. In: Proceedings of the Fifth ACM International Conference on Web Search and Data Mining, pp. 363–372. ACM (2012)
12. Arora, N.R., Lee, W.: Graph based Ranked Answers for Keyword Graph Structure. New Generation Computing 31(2), 115–134 (2013)
13. Zhai, C., Lafferty, J.: A study of smoothing methods for language models applied to ad hoc information retrieval. In: Proceedings of the 24th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 334–342. ACM (2001)
14. Coffman, J., Weaver, A.C.: A framework for evaluating database keyword search strategies. In: Proceedings of the 19th ACM International Conference on Information and Knowledge Management, pp. 729–738. ACM (2010)
15. Jansen, B.J., Spink, A.: How are we searching the World Wide Web? A comparison of nine search engine transaction logs. Information Processing & Management 42(1), 248–263 (2006)
16. Järvelin, K., Kekäläinen, J.I.: evaluation methods for retrieving highly relevant documents. In: Proceedings of the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 41–48. ACM (2000)

# Max-Weight Algorithm for Mobile Data Offloading through Wi-Fi Networks

Shirong Lin, Zhijun Li, and Shouxu Jiang\*

Dept.of Computer Science and Technology,  
Harbin Institute of Technology, Heilongjiang, China  
[linger\\_lilac@163.com](mailto:linger_lilac@163.com),  
[{lizhijun\\_os,jsx}@hit.edu.cn](mailto:{lizhijun_os,jsx}@hit.edu.cn)

**Abstract.** We consider the data uplink control problem for mobile terminals in wireless networks subjected to time-varying channels, reconfiguration delays and interference constraints. We analysis the uplink capacity region of multiple mobile users in wireless networks, and we use Clarke Gan's channel model for channel process of mobile terminals. We evaluate the impaction caused by schedule changing and also the changing of network topologies, and then we proposed a Max-Weight algorithm for the system. The proposed algorithm makes schedule by considering the impaction of reconfiguration and the expectation throughput of a schedule. The schedule generated by this algorithm can achieve a larger throughput subjected to existing approaches.

**Keywords:** Mobile Cloud Computing, Reconfiguration Delay, Capacity Region, Max-Weight.

## 1 Introduction

Lots of research works [1,3,2,6] have studied the scheduling algorithms in wireless networks with interference constraints based on some particular channel models. However, to the best of our knowledge, the effects of reconfiguration delays have not been considered in the context of mobile wireless networks subject to interference constraints and time-varying channels conditions. Reconfiguration delay is a widespread phenomenon that is observed in many practical high speed communication systems. In these systems, the controllers always need to change the parameters of the systems to get optimal performance. Every time the parameter is changed, there is a corresponding reconfiguration process to make the new system adaptive. For example, in satellite networks where multiple mechanically steered antennas are providing service to ground stations, the time to switch from one station to another can be around 10ms [4]. In optical communication systems, laser tuning delay for transceivers can take significant time ( $\mu s - ms$ ) [5]. In wireless networks, delay for electronic beamforming for channel switching that occurs in phased-lock loops in oscillators can be more than

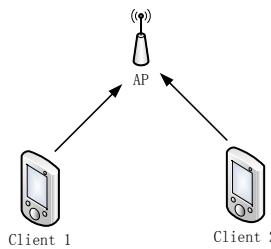
---

\* Corresponding author.

$200 \mu s$  [4,7]. Research work in [1] provides a measurement of reconfiguration delay for Atheros 5212 wireless card, the results show that it is about  $4.11/0.244$  ms for the switching process of channel and channel width. And in [8] the author quantify the overhead of switching channel width in their implementation, the results shows this delay is about 5 to 45 ms, most of the value is about 17ms. This 17ms is much longer than  $4.11/0.244$ ms in [8], there are two reasons for this, the first is that their hardware is not the same; and the second reason is that  $4.11/0.244$ ms contains only the hardware reconfiguration delay while 15ms contains the hardware switching delay and the overhead of coordination handshake.

Although the reconfiguration delay is observed in these research works, but almost all of them doesn't focus on it. Work in [1] mainly focus on the conflict graph model of different links and it leaves the problem of reconfiguration delay to the development of hardware, also, the author give an example that some wireless cards have switching delay of less than  $100 \mu s$  [13]. Work in [8] claims that the median 17ms is small enough for most applications.

Though work in [6] focuses on the capacity of wireless network with considering of reconfiguration delay, but the channel model used in their paper is too theoretical, in their research work, memoryless channel and two-state markov channel are considered, and as we know, these two channel models are too ideal in practical environments, especially in mobile cloud computing applications.



**Fig. 1.** Uplink of two-user in mobile cloud computing

We consider an uplink data transmission problem in mobile cloud computing applications, in these applications, data is generated on mobile terminals, and then transmitted to the cloud for computing through cellular networks or Wi-Fi networks. Offloading mobile data receives more and more attention. So, here comes the problem, when there is a free wireless networks and plenty of mobile terminals, and these mobile terminals want their data to be upload by the Wi-Fi network, is there a schedule which could achieve the optimal throughput? What the schedule looks like and how it works?

Supposing there is a schedule  $W(t)$  in current system for time period  $t$ , when the period is over, there should be another schedule for the period  $t+1$  system, if  $W(t+1) \neq W(t)$ , this is a reconfiguration process in which no data can be

transmitted, and the throughput decreases. If  $W(t+1) = W(t)$ , we continue the previous schedule, throughput won't be decreased by reconfiguration process but by the topologies changes (e.g., backlogs, channel states and so on). So, whether or not change the schedule, we should consider the impaction cause by both changing the schedule and the change of topologies. The topologies includes backlog on terminals, mobilities, and the channel state (SINR), the backlog and mobilities can be sensed by the controller, So, we only need to know the channel process. In this paper we used Clarke and Gan's channel model to simulate the channel process for the system and then proposed a Max-Weight based scheduling algorithm for the system.

The remainder of this paper is organized as follows. First, in Section 2, we describe the state-of-the-art research of capacity region and the state-of-the-art wireless channel model. Next, in Section 3, we present the Max-Weight based algorithm for the uplink transmission and also the MAC protocol for the system. The results of simulation are in Section 5, and conclude in Section 6.

## 2 Network Model

### 2.1 System Architecture for Data Offloading

A wireless network contains several APs, these APs always use different channels. Let  $A = \{A_1, A_2, \dots, A_k\}$  represents the set of  $k$  APs. The  $n$  clients are represented as  $M = \{m_1, m_2, \dots, m_n\}$ .

We suppose the data generates by the mobile clients is a stochastic process whose rate is  $\lambda_i (\lambda_i \in \Lambda = \{\lambda_1, \lambda_2, \dots, \lambda_n\})$  ( $\Lambda$  is the convex of  $\lambda_i$ ), and these generated data forms a queue  $Q_i (Q_i \in Q = \{Q_1, Q_2, \dots, Q_n\})$  with length of  $|Q_i|$  on mobile client  $i$ . When a mobile client  $m_i$  enter the coverage of a wireless network, it could sense and join the wireless network, and then transmit its offloading data. The velocity of mobile terminal is  $v_i (v_i \in V = \{v_1, v_2, \dots, v_n\})$ . The channel process of mobile client  $i$  is  $c_i$  ( $c_i \in C = \{c_1, c_2, \dots, c_n\}$ ). The schedule is define as  $W(t) \in \mathcal{W} = \{(w_1, w_2, \dots, w_n)\}$ ,  $w_n = 0$  means it couldn't transmit data in this period, and the reconfiguration process means  $W(t+1) \neq W(t)$ . We also use  $I_\ell \in \mathcal{I}$  to represent whether channel  $\ell$  is scheduled, i.e.,  $I_\ell = 1$  if and only if  $w_\ell \neq 0$ , actually, a schedule contains the information about which links are scheduled and also about the their corresponding channels.

Let  $T_c$  to be this time, i.e., in the offloading process, the clients will take  $T_c$  to get connected with an AP and configured, and also, when the channel changes, it will take  $T_c$  to get its data retransmitted for the terminal.

The reconfiguration delay  $T_c$  would change the structure of optimal policy derived from Max-Weight algorithm, because this reconfiguration delay will diminish the gain of diversity, and the capacity of wireless network changes to be an average way. Taking a wireless network with memory channel process as an example, memoryless channel means the channel process  $c_\ell(t), t \geq 0$  takes value independent and identically distributed (i.i.d.) values from the set of  $C$  at each time slot  $t$ . The capacity region of wireless network [6] is

$$\Lambda = \left\{ \lambda | \exists \alpha \geq 0, \sum_{I \in \mathcal{I}} a_I \leq 1, \text{ such that } \lambda_\ell \leq \overline{C}_\ell \sum_{I \in \mathcal{I}} \alpha_I I_\ell, \forall \ell \in \mathcal{L} \right\} \quad (1)$$

This means that in presence of reconfiguration delay, no policy can take advantages of the diversity in time-varying memoryless channels and achieve a greater rate than the average channel gain for each link [6].

*Example Uplink AWGN channel* The baseband discrete-time model for the uplink AWGN channel with two users (Figure 1) is

$$y[m] = x_1[m] + x_2[m] + w[m], \quad (2)$$

where  $w[m] \sim \mathcal{CN}(0, N_0)$  is i.i.d. complex Gaussian noise [9].  $P_k$  ( $k=1,2$ ) is the average power constraint of user  $k$ .

The original definition of capacity region of wireless network is [3] the closure of the set of all arrival rate matrices ( $\lambda_i$ ) that can be stably supported by the network, considering all possible strategies for choosing the control variables. For this simple two-user example, there is a very simple characterization of the capacity region  $\mathcal{C}$  of it: the set of all rates  $(R_1, R_2)$  satisfying the three constraints:

$$R_1 < w_1 \log_2 \left( 1 + \frac{P_1}{N_0} \right) \quad (3)$$

$$R_2 < w_2 \log_2 \left( 1 + \frac{P_2}{N_0} \right) \quad (4)$$

$$R_1 + R_2 < w_1 \log_2 \left( 1 + \frac{P_1}{N_0 + X_{21}} \right) + w_2 \log_2 \left( 1 + \frac{P_2}{N_0 + X_{12}} \right). \quad (5)$$

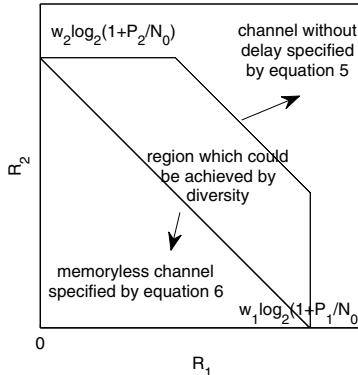
where  $w_1, w_2$  is the channel width of user 1 and 2,  $X_{ij}$  means the interference caused by  $i$  to  $j$ .

With reconfiguration delay, the capacity region for wireless networks with memoryless channel is as:

$$\frac{R_1 w_2 \log_2 \left( 1 + \frac{P_2}{N_0} \right) + R_2 w_1 \log_2 \left( 1 + \frac{P_1}{N_0} \right)}{w_1 w_2 \log_2 \left( 1 + \frac{P_1}{N_0} \right) \log_2 \left( 1 + \frac{P_2}{N_0} \right)} \leq 1. \quad (6)$$

where  $P_1 \geq 0$  and  $P_2 \geq 0$ . We represent this capacity region as  $\Lambda_0$ .

Channel memory could be used to enlarge the capacity region for wireless networks [6], it is because the channel model contains information about the channel diversity, and the algorithm designed with these information could enlarge the capacity region. This is why with reconfiguration delay, the capacity region can be enlarged to be a convex region  $\Lambda_1$ , and we could see that  $\Lambda_0 \subseteq \Lambda_1 \subset \Lambda$  [6]. From figure 2 we could see  $\Lambda_1$  is actually trapezoid region.



**Fig. 2.** The capacity region under memoryless (i.i.d) channels process and channels without delay, practical channel can achieve a capacity region between them

## 2.2 Channel Model

From a practical point of view, memoryless or markov memory channel in [6] is too theoretical for using. In mobile cloud computing applications, there are Doppler spread and multipath spread caused by the mobility of the terminals. Memoryless or markov models couldn't simulate the environment accurately for the complexities of the varying environments. We model the continuous time multipath fading channel as

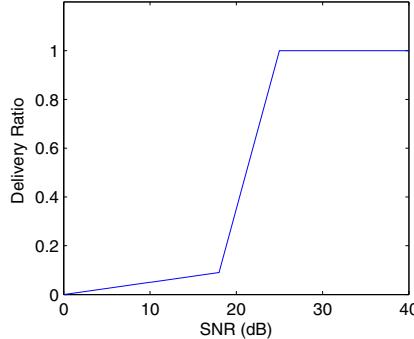
$$y(t) = \sum_i a_i(t)x(t - \tau_i(t)) + \omega(t). \quad (7)$$

where  $x(t)$  is the transmitted signal and  $y(t)$  is the received signal. The time-varying multi-path propagation is captured by the attenuation of each path  $a_i(t)$ , the time delays  $\tau_i(t)$  and the number of paths  $p(t)$ . The last term  $\omega(t)$  is zero-mean additive white Gaussian with power spectral density  $N_0/2$  (i.e.,  $E[\omega(0)\omega(t)] = (N_0/2)\delta(t)$ ), and we use it to model the background noise and represents the thermal noise of the receiver. Note that the signals loss is due to the paths on which signals travel and the distance between sender and the receiver. SNR is always a form of attention of signals.

The SNR at the receiver side can be used to capture the packet level performance of physical layer implementation, and we could learn the relationship between the delivery ratio and the SNR from [1] in 802.11 wireless networks. The relationship can be represented in a piecewise function:

$$P(SNR) = \begin{cases} \frac{1}{200}SNR & \text{if } SNR < 18dB \\ \frac{91}{700}SNR - \frac{9}{4} & \text{if } 18db \leq SNR < 25dB \\ 1 & \text{if } SNR \geq 25dB. \end{cases} \quad (8)$$

By drawing the figure 3 through this function 8, we could see the relationship between SNR and delivery ratio, this figure implies that SNR plays an important role in data transmission.



**Fig. 3.** The delivery ratio as a function of SNR [1]

In this paper, we refer [10] and use the Clarke and Gan's Model for the received SNR for transmitter power  $P$  at the packet transmission time  $t_p$

$$SNR(t_p) = Pd(t_p)^{-\beta} \frac{\rho(t_p)}{\sigma^2}, \quad (9)$$

where  $d(t_p)$  is the distance between the sender and the receiver at time  $t_p$ ,  $\beta$  is the path loss exponent,  $\rho(t_p)$  is the average channel gain for the packet at time  $t_p$ , and  $\sigma^2$  is the variance of the background noise  $\omega(t)$ .

The time-varying parameter  $\rho(t_p)$  control the short time-scale variation in the received SNR, for an environment full of multipath, we could use Rayleigh fading channel as the probability model for the system. When there line-of-sight path is large and has a known magnitude, and there are also a large number of independent paths, modeling  $\rho(t_p)$  as Rician distribution is more suitable:

$$p(\rho) = \frac{\rho}{\sigma^2} e^{-\left(\frac{\rho}{2\sigma^2} + K\right)} J_0(2K\rho), \quad (10)$$

where  $K$  is the distribution parameter representing the strength of the line of the sight component of the received signal and  $J_0(\cdot)$  is the modified Bessel function of the first kind and zero-order [11]. The power spectral density  $S(f)$  divided on  $[-1/2, +1/2]$ , is given by

$$S(f) = \frac{1.5}{\pi f_m b \sqrt{1 - \left(\frac{f-f_c}{f_m}\right)^2}}. \quad (11)$$

where  $f_c$  represents the carrier frequency of the transmitted signal.

### 3 Scheduling Algorithm for Mobile Terminals

We proposed a Max-Weight based algorithm in this paper. The main idea of this algorithm is: the topologies of the network can be sensed by the controller,

and the expected ability of the channel can be computed through the channel model, so the controller could know the impaction of schedules, and it can pick the optimal schedule.

On the schedule point, among the flexible channel allocations, there is a  $W^*(t+1)$  for time period  $t+1$ :

$$W^*(t+1) = \arg \max_{\{W \in \mathcal{W}\}} \sum_{\ell} \frac{I_{\ell} \overline{SINR}_{\ell}(t) Q_{\ell}(t)}{v_{\ell}(t)} \quad (12)$$

where  $W_{\ell}$  means the channel allocated to  $\ell$ , and  $\mathcal{W}$  is a set of feasible and interference free channel schedules. This  $W^*(t+1)$  plays important role in the schedule, it may be the optimal allocation. This equation implies that the terminals with large data amount, high SNR and slow velocity will achieve larger throughput, this is true in practical scenarios: large data amount means it is enough for a long time of transmission, high SNR means its rate is high and slow velocity means the scheduling time could be long.

As mentioned in the section 2, for system without reconfiguration delay, the scheduling algorithms could always change to the best schedule to get a optimal throughput. But with delay, the change process is time consuming and will decrease the throughput of system. Traditional strategies to diminish the impaction caused by reconfiguration delay are to let the scheduling period to be long enough. In this paper, we also make the scheduling period as a function of backup queue length on the mobile terminals:

$$t_p(t+1) = f \left( \sum_{i=1}^N I_i(t+1) Q_i(t+1) \right) \quad (13)$$

By referring [6], we set  $f(x)$  as a sub-linear function, i.e.,  $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = 0$ . And we update this schedule period dynamically with the change of queue length.

Considering the impaction of reconfiguration delay, we weight the expectation gain of new schedule and its reconfiguration loss, and then give the best schedule which make the maximal gain. We define the similarity set between current schedule  $W(t)$  and  $W^*(t+1)$  as  $S = \{\ell_i | W_i(t) = W^*(t+1)\}$ . The similarity set  $S$  means the links (or terminals) which keep their channels the same as before when the schedule changes. These links don't suffer for throughput loss during the reconfiguration process.

If we continue to use  $W(t)$  in the next period, we will get a expected throughput gain of

$$Th(W^t(t+1)) = \mathbb{E}\{t_p(t+1) \sum_{\ell \in \mathcal{L}} w_{\ell} \log(1 + SINR_{\ell}(t+1)) | SINR(t)\}. \quad (14)$$

If we change the schedule to  $W^*(t+1)$  in the next schedule period, we would get a throughput gain of:

$$\begin{aligned} Th(W^*(t+1)) &= \mathbb{E}\{t_p(t+1) \sum_{\ell \in S} w_{\ell} \log(1 + SINR_{\ell}(t+1)) \\ &+ (t_p(t+1) - t_c) \sum_{\ell \in \mathcal{L}-S} w_{\ell} \log(1 + SINR_{\ell}(t+1)) | SINR(t)\}. \end{aligned} \quad (15)$$

---

**Algorithm 1.** Max-Weight Based Up-Link Scheduling Algorithm for Mobile Terminals
 

---

**Input:**  $Q_1, \dots, Q_n$  (packet on clients),  $v_1, \dots, v_n$  (mobile terminals' velocity),  $lu_1, \dots, lu_n$  (the latest schedule time),  $W_{must}$  links must be scheduled.

**Output:** The schedule  $W^*(t+1)$  and  $t_p(t+1)$

- 1  $W_1 = \mathcal{W}, W_2 = 0, W_{must} = 0$
- 2 **for**  $i$  in  $0 \dots n$  **do**
- 3    Terminal  $i$  broadcast its  $(q, v, lo, lu)$
- 4     $q_i = q, v_i = v, lo_i = lo, lu_i = lu$
- 5    **if**  $lu_i \geq T_l$  **then**
- 6      $w_i(t+1) = \text{Choose a w from } W$
- 7      $W_1 = W_1 - w_i$
- 8      $W_{must} += w_i$
- 9  $t_p(t+1) = f\left(\sum_{i=1}^N I_i(t+1)Q_i(t+1)\right)$
- 10 **for**  $i$  in  $0 \dots k$  **do**
- 11     $W^*(t+1) = \arg \max_{\{W \in W_1\}} \sum_{\ell} \frac{I_{\ell} \overline{SNR}_{\ell}(t) Q_{\ell}(t)}{v_{\ell}(t)}$
- 12     $W_1 -= W^*(t+1)$
- 13     $W_2 += W^*(t+1)$
- 14  $W^*(t+1) = \text{Get\_Max\_thpt}(\{W(t), W_2\})$
- 15 **return**  $W^*(t+1) + W_{must}$  and  $t_p(t+1)$

---

In this equation, the first part means the expected throughput gain from the links which keep the channels the same as previous schedules, and the second part means the gain from the links which are newly added into schedule, and because their configuration process take a delay of  $t_c$ , so the total schedule time is  $t_p(t+1) - t_c$ .

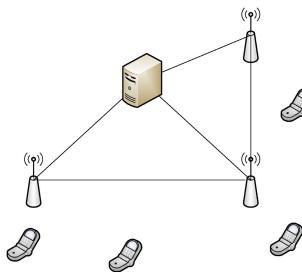
Based on  $Th(W^t(t+1))$  and  $Th(W^*(t+1))$ , our algorithm decide its behavior at  $t+1$ , if  $Th(W^t(t+1))$  is bigger than  $Th(W^*(t+1))$ , we keep the schedule  $W(t)$  while re-compute the scheduling period based on the queue length at  $t+1$ ; Otherwise, we change the schedule to  $W^*(t+1)$  and also re-compute the period.

Though the chosen  $W^*(t+1)$  significantly implies it is the optimal allocation, sometimes it is not, so we choose  $k$   $W^*(t+1)$  and form a set  $W_{setfrom}$ , and then the controller chooses the optimal  $W^*(t+1)$  from this set.

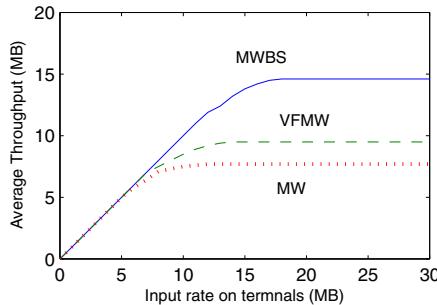
The algorithm 1 works as follows: When mobile terminals enter the coverage of wireless network, they broadcast its information (include last schedule time, backup data amount, current SNR, velocity) to APs. Then, the controller select the first  $k$  best schedules, and then from these  $k$  schedules and current on-going schedule, the controller select the best schedule.

## 4 Evaluation

Our implementation of scheduling algorithm consists of: (a) a central controller that generates the interference-free schedule to the mobile terminals. We have



**Fig. 4.** Experiment layout, 3 APs, 4 mobile terminals and a controller



**Fig. 5.** Throughput with algorithm for MWBS (proposed in this paper), VFMW and simple MW

implemented this on a Linux PC (3.0 GHz Intel(R) Core(TM) i3-3220, 4 GB DRAM). (b) We use 3 wireless APs to be the access points, and we don't set password on the APs to avoid the difference caused by different security types. (c) We did the experiment in a building near the street to make the experiment environments more realistic, in this environment, there are several line-of-sight components and lots of multi-path components, which makes Rician Channel Model works well.

We implemented our experiment as Figure.4, we implemented a mobile cloud computing environment, there are three APs, 4 mobile terminal and a controller. Data was generated on mobile terminals in an increase order, we increase the generate rate from 0 MB to 3.5 MB, and the terminals moved a random way from the first AP to the last one and we test the total throughput. We also implemented VFMW [6] and simple MW algorithm in our experiment, the results is shown in Figure.5.

From the result we could see our algorithm could achieve a larger throughput gain than the other state-of-the-art algorithms. The reason why MW algorithm achieves the smallest throughput is because the reconfiguration delay diminishes the diversity. VFMW algorithm achieves a larger throughput, because the schedule period is a sub-linear function of queue length. Our MWBS algorithm

outperforms them because the channel model used in our algorithm is better than them, and also, we take the reconfiguration process on a link level.

## 5 Conclusion

In this paper we use Clarke and Gan's channel model for mobile terminals, and based on current research about capacity region of wireless network, we propose a Max-Weighted scheduling algorithm for mobile's offloading data transmission, the proposed approach can be used in everyday life for economical and some other reasons.

## References

1. Rayanchu, S., Shrivastava, V., Banerjee, S., Chandra, R.: Fluid: improving throughputs in enterprise wireless lans through flexible channelization. In: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking, MobiCom 2011, pp. 1–12. ACM, New York (2011)
2. Neely, M.J., Modiano, E., Rohrs, C.E.: Power and server allocation in a multibeam satellite with time varying channels. In: Proceedings of IEEE INFOCOM 2002, pp. 1451–1460 (2002)
3. Georgiadis, L., Tassiulas, M.J.R.: Resource allocation and cross-layer control in wireless networks. Foundations and Trends in Networking, 1–149 (2006)
4. Blake, X.I.L.: Antennas: Fundamentals, Design, Measurement. SciTech (2009)
5. Brzezinski, A., Modiano, E.: Dynamic Reconfiguration and Routing Algorithms for IP-over-WDM networks with Stochastic Traffic. IEEE Journal of Lightwave Tech. 23(10), 3188–3205 (2005)
6. Celik, G.D., Le, L.B., Modiano, E.: Scheduling in Parallel Queues with Randomly Varying Connectivity and Switchover Delay. In: Proc. IEEE INFOCOM 2011 Mini Conference (April 2011)
7. Yun, M., Zhou, Y., Arora, A., Choi, H.A.: Channel assignment and scheduling in wireless mesh networks considering switching overhead. In: IEEE International Conference on Communications, ICC 2009, pp. 1–6 (2009)
8. Chandra, R., Mahajan, R., Moscibroda, T., Raghavendra, R., Bahl, P.: A case for adapting channel width in wireless networks. SIGCOMM Comput. Commun. Rev. 38(4), 135–146 (2008)
9. Tse, D., Viswanath, P.: Fundamentals of Wireless Communication. Cambridge University Press, New York (2005)
10. Sadeghi, B., Kanodia, V., Sabharwal, A., Knightly, E.: Opportunistic media access for multirate ad hoc networks. In: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, MobiCom 2002, pp. 24–35. ACM, New York (2002)
11. Rappaport, T.: Wireless Communications: Principles and Practice, 2nd edn. Prentice Hall PTR, Upper Saddle River (2001)
12. National Center for Biotechnology Information, <http://www.ncbi.nlm.nih.gov>
13. Intel pro/wireless network connection for mobile,  
<http://www.intel.com/network/connectivity/products>
14. Walking, <http://en.wikipedia.org/wiki/Walking>

# Capture Missing Values Based on Crowdsourcing

Chen Ye and Hongzhi Wang

Harbin Institute of Technology, Harbin, China

sunnyleaves0228@qq.com, {wangzh, honggao}@hit.edu.cn

**Abstract.** Due to the unreliable environment in mobile could, attribute values or tuples may be missing or lost. Thus we should capture missing values to make data mining and analysis more accurate. Besides ignoring or setting to default values, many imputation methods have been proposed, but they also have their limitations. This paper proposes a human-machine hybrid workflow to study the missing value filling method with crowdsourcing. First we propose a missing value selection algorithm to select the missing values which are suitable to use crowdsourcing for filling. Then we propose three missing values filling methods according to different attribute types to select answers from crowdsourcing. Experimental results show that our algorithms could improve data quality significantly with low costs.

**Keywords:** data cleaning, missing values, crowdsourcing.

## 1 Introduction

In real life, data is often dirty and there may be more missing values in mobile cloud environment. No matter how rigorous we write the queries and how efficient our database, the results could not be guarantee accurate and correct. Incomplete information has been a longstanding issue. This is led by many reasons such as human negligence, rule violations, and external factors limitation. The scale of the problem is such that it is common to find critical information missing from databases. For instance, it is estimated that pieces of information perceived as being needed for clinical decisions were missing from 13.6% to 81% of the time [16]. As incompleteness affects the data usability, it is necessary to estimate the missing values.

Instead of neglecting all the missing value, using imputation to solve incomplete data is a desirable idea. The current data cleansing methods can be divided into three categories. The easiest way to fill the missing values is to replace them with average value or the most frequent value. The second one is statistical methods. Many existing models can be applied, such as the expectation-maximization algorithm [5], regression-based imputation [7, 8] and sampling method [6]. Statistical parameters obtained from existing values are used to fill the missing values. The last category is the machine learning methods which fill missing values by training the model with existing data. Machine-learning-based methods include classification methods [9-12], clustering methods [13,14] and neural network methods [15].

Even though many methods have been proposed, this problem is not solved throughout. Most of the proposed methods are only suitable for numeric data and it is difficult to simply extend them to the categorical data, which is also an important part of missing value problem. For example, if a paper misses one author, it is difficult to get it through its existing authors or the name of the paper. However, human can deal with this problem very simple by filling the name of the author directly. As the case of the authors information collection does not require any specialized knowledge, non-professionals who know the answers can fill the information very easily. Thus we attempt to fill the missing values based on crowdsourcing in this paper.

Crowdsourcing is used to solve problems hard for machines, such as comprehending and analyzing abstract concepts which human does better. Companies or individuals can outsource tasks to the crowdsourcing platform with reward, while freelance workers login the crowdsourcing platform to complete the tasks.

Therefore, this paper presents missing values filling algorithm based on crowdsourcing, using crowdsourcing to give suggested answers and choose the best answer to fill back to the database. Experimental results show that we perform a data cleaning for a given database based on crowdsourcing which improve the data quality with low costs.

Contribution of this paper can be summarized as the following three points:

We present the method of dealing with missing values with crowdsourcing. To our knowledge, this is the first use of crowdsourcing to fill the missing values.

We propose a missing value selection algorithm to select the missing values which are suitable to apply crowdsourcing for filling.

(3) Due to the different quality workers of crowdsourcing platform provided, some workers maybe provide malicious or incorrect answers, we propose the best answer selection technique to select the correct answer to fill the attributes in various types.

The paper is organized as follows:

Section 2 describes the missing values selection algorithm which selects the missing values which are suitable to use crowdsourcing for filling. Section 3 presents three missing values filling algorithms for various data types of attributes. Section 4 studies proposed method experimentally. Section 5 draws the conclusions and discusses future research directions.

## 2 Missing Values Selection Algorithm

Although it is necessary to estimate the missing values, all missing values are not suitable to use crowdsourcing for filling. For instance, if one person is not married, the information of his spouse must be missing values which not exists. Obviously we cannot fill his spouse information through crowdsourcing. Thus when we find a record with missing values, we should analysis the type of missing values. First we classify missing values into three categories according to its semantics. Then we propose our missing values selection algorithm.

According to different semantics, missing values are divided into three types.

**Inexistence Missing Value:** There not exists a meaningful value for a specific region. We always give a special value to fill.

**Existence Missing Value:** The value exists but is unknown at the moment. We always give a default value such as default data, default property.

**Occupied Missing Value:** There is not any information about the missing values.

**Table 1.** Customers information

| name    | city        | postcode | status  | spouse |
|---------|-------------|----------|---------|--------|
| Curry   | Sillion     | NJ582    | single  |        |
| Hayes   | Los Angeles |          | married | Adams  |
| Jack    | New York    | NJ 07974 | single  |        |
| Jackson | Sillion     |          | married |        |
| Jary    | New York    | NJ 07974 | single  |        |
| Jim     |             | NJ 07974 | married | LiLi   |
| Mary    | New York    | AK 27    | married |        |

We give an example to demonstrate the meaning of the three types of missing values. For the first tuple in the Table 1, the marital status of *Curry* is single, so the missing value of *spouse* is an *inexistence missing value*. For the second tuple, the value of *postcode* is missing. As the postcode exists, the missing value of postcode is an *existence missing value*. If the marital status and spouse of someone are missing at the same time, the missing value of marital status is an *existence missing value* and the missing value of spouse is *occupied missing value*. We can infer from the above example that we mainly deal *existence missing values* with crowdsourcing.

As the type of the missing values is divided according to semantics, we should label the missing values manually. The three types of missing values are labeled as *I*(Inexistence missing value), *E*(Existence missing value), *O*(Occupied missing value). For example, in the Table 1 there are two attributes related to different types of missing values, so we only need to select the records labeled as *E* which *status = married&&spouse == null*. The result after missing values selection is shown in Table 2, and we assign a unique *task\_id* to each pending record. Then we send these tasks for crowdsourcing to obtain candidate answers.

The process of missing values selection is shown in Algorithm 1.

**Table 2.** Missing values selection result

| task_id | name    | city        | street  | postcode | status |
|---------|---------|-------------|---------|----------|--------|
| 10001   | Hayes   | Los Angeles |         | married  | Adams  |
| 10002   | Jackson | Sillion     |         | marreid  |        |
| 10003   | Jim     |             | NJ07974 | married  | LiLi   |
| 10004   | Mary    | New York    | AK27    | married  |        |

---

**Algorithm 1.** *missing\_selection( T, A, L )*

---

**Input:** tuple T, attribute A and label L**Output:** *task\_id* represents records which need to be deal with

- 1: Find the missing value from each tuple  $T_i$
  - 2: Label each missing value according to its semantics
  - 3: Select the tuples which are labeled as  $E$
  - 4: Give the pending tuples a *task\_id*
- 

### 3 Different Attribute Values Selection

As the answers which different workers provide on the crowdsourcing have different quality, we present missing values filling algorithm to determine the result based on these answers.

Answer selected method for different attribute types is not the same. Thus we intend to propose different missing values filling methods according to different attribute types. Attributes can be divided into three categories according to different comparative method named numerical attributes, comparable attributes, and categorical attributes. The difference of numerical attributes can be calculated by the absolute value of subtraction. The comparable attributes have different distance which cannot be calculated by subtraction. Two categorical attributes are the same or not which the difference cannot be calculated quantitatively.

For example, integer and real type are numerical attributes; string and character are comparable attributes; Gender and job classification are categorical attributes, two values in which can only be distinguished whether the same or not, but cannot describe quantitatively the differences.

Here we consider the filling missing value methods of three types of attribute, respectively. We assume that the reliability of each worker is known. The input is a binary set  $S$ , where in each tuple  $(w_i, v_i)$ ,  $w_i$  represents the confidence of the worker,  $v_i$  represents the worker's input. Worker confidence can be computed by the machine learning method [1]. When the worker has high quality,  $w_i$  is positive. When the worker has low quality,  $w_i$  is negative. When the worker is a random input,  $w_i = 0$  which indicates that the worker's input has no reference value.

#### 3.1 Numerical Attributes Filling Algorithm

For numeric attributes, we can make filling value as the weighted average answers from trusted workers. The pseudo code is shown in algorithm2.

As a malicious worker may give false value deliberately which is no clear correlation with the correct value, we only consider the answer trusted workers provide. We give an example to show the process. The missing value is the years that Harbin Institute of Technology has been built. We have obtained five answers in Table 3 where we can see there is a malicious worker whose answer is obviously wrong. Thus we get the result based on the answers of the trusted workers. That is  $(0.90 \times 93 + 0.83 \times 92 + 0.80 \times 93 + 0.56 \times 90) / (0.90 + 0.83 + 0.80 + 0.56) = 92.18$ .

**Algorithm 2.** *NAFA(W, V)***Input:** workers confidence  $W$ , workers answer  $V$ **Output:** the filling value  $v$ 1: find the candidate answer set( $w_i, v_i$ )

$$\sum w_i v_i$$

2: calculate  $v = \frac{\sum_{w_i > 0} w_i v_i}{|\{w_i | w_i > 0\}|}$ 3: return  $v$ **Table 3.** Workers answers of numeric attributes

| ID | confidence | answer |
|----|------------|--------|
| A  | 0.90       | 93     |
| B  | 0.83       | 92     |
| C  | -0.50      | -2     |
| D  | 0.80       | 93     |
| E  | 0.56       | 90     |

### 3.2 Comparable Attributes Filling Algorithm

For the same reason as numeric attributes, we also only choose answers provided by trusted users. For example, for  $task\_id = 10003$  in table2 we get five answers in the following Table 4. We use a similarity function and a threshold to judge the similarity of the comparable attributes. Similarity function requires one pair of records as input and outputs a similarity value. The more similar the two records are, the higher the output value is. The basic approach is to calculate the similarity of all pairs of records. If the similarity is no less than the specified threshold, the pair of records is considered to be similar.

**Table 4.** Workers answers of comparable attributes

| ID | confidence | answer        |
|----|------------|---------------|
| A  | 0.86       | San Francisco |
| B  | 0.93       | San Antonio   |
| C  | 0.54       | San Francisco |
| D  | -0.50      | New York      |
| E  | 0.80       | San Francisco |

For example, the similarity function is designed to be *Jaccard*, the specified threshold value is 0.6. The *Jaccard* can be calculated by formula (1). For example, comparing with the answers of  $TASK\_ID = 10003$ , the *Jaccard* similarity between  $r_1$  and  $r_5$  is  $J(r_1, r_5) = 0.78 \geq 0.6$ . So we consider  $(r_1, r_5)$  refer to the same entity. Similarly, it will not be considered the same as  $J(r_1, r_2) = 0.46 < 0.6$ .

$$Jaccard(A, B) = \frac{|A \cap B|}{|A \cup B|} \quad (1)$$

The process to filter out the best answer in a similar pair of records is shown in Algorithm 3.

---

**Algorithm 3.** BestAnswer( $R, A$ )

---

**Input:** similar pair of records gather  $R$

**Output:** the filling value  $A$

$T = \text{HashString}(R); // \text{ calculate the frequency of different records appearance}$

$M = \text{Similar}(T); // \text{ save the similarity of different pairs of results in } M$

for each  $t \in T$  do

$$w_t = \sum_{(w_i, v_i) \in R \wedge v_i = t} w_i \sum_{(w_j, v_j) \in R} M(t, v_j)$$

$$A = \arg \max_{t \in T} \{w_t\}$$

return  $A$

---

### 3.3 Categorical Attributes Filling Algorithm

For categorical attributes, we use weighted voting algorithm [15]. The maximum weight value is selected as the true value. That is, for the worker  $(w_i, v_i)$ , if he is a trusted worker, then we increase  $w_i$  of  $v_i$ . If he is a malicious worker, then we decrease  $w_i$  of  $v_i$ . After we get all the answers, the maximum weight value is selected as the filling value. The pseudo code is shown in Algorithm 4.

---

**Algorithm 4.** WVote( $W, V$ )

---

**Input:** workers confidence  $W$ , workers answer  $V$

**Output:** the maximum weight value  $v$

1: find the candidate answer gather( $w_i, v_i$ ) and calculate the weight value

2: find the value  $v$  which has the maximum weight value  $v$

3: return  $v$

---

We use an example to show the strategy. The question is to judge a student Jim's whereabouts after graduation, and the answers are limited to continue stay at school, go abroad and go to work. The answer is shown in Table 5. The weight of member is  $0.90 + 0.83 - 0.50 = 1.23$ , the weight of probationary member is 0.80, and the weight value of masses is 0.80, so the value with the maximum is "stay at school". Thus the filling value is stay at school.

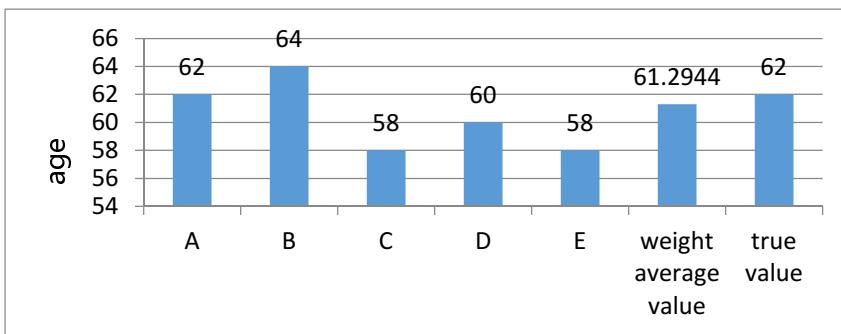
**Table 5.** Workers answers of categorical attributes

| ID | confidence | answer         |
|----|------------|----------------|
| A  | 0.90       | stay at school |
| B  | 0.83       | stay at school |
| C  | -0.50      | stay at school |
| D  | 0.80       | go abroad      |
| E  | 0.56       | go to work     |

## 4 Experimental Results

To verify the effectiveness of proposed methods, we selected five workers (A, B, C, D, E) to fill the missing values in various types. In order to determine their weights, we first give everyone twenty questions which we have known the answers. We obtain the weight (0.90, 0.83, -0.50, 0.80, 0.56) based on their answers.

For numerical attributes, we sent the following questions on the crowdsourcing platform: "Please fill the age of the famous film director Chen Kaige ". We found that the result using the weighted average method is close to the true value in Figure1.

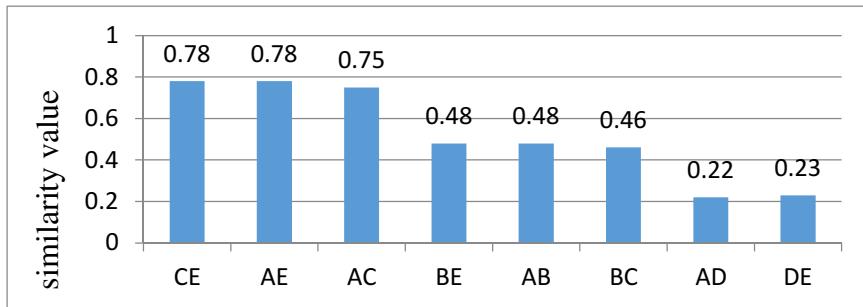
**Fig. 1.** The age of the famous film director Chen Kaige

For comparable attributes, we get five answers for  $task\_id = 10003$  in Table 4. We still select trusted workers' answers doing research. First calculate the similarity of each pair of answers in Figure 2, then calculate the weight of each answer according to similarity answers. After calculation we found that  $r_1$  has the maximum weight value which is the same as the true value.

$$r_1 : 0.78 \times 0.86 + 0.75 \times 0.86 = 1.3158$$

$$r_3 : 0.78 \times 0.54 + 0.75 \times 0.54 = 0.8262$$

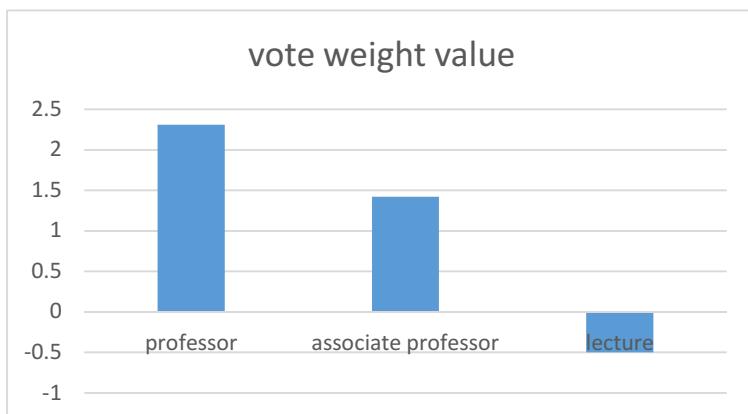
$$r_5 : 0.80 \times 0.78 + 0.80 \times 0.78 = 1.248$$

**Fig. 2.** The similarity value of each pair of answers

For categorical attributes, we sent the following questions on the crowdsourcing platform: "Give the position of the famous singer Liu Huan." Table 6 shows the answers we got. After calculating the weight of each classification, the maximum weight value answer is our suggested answers. Figure 3 shows 'professor' is the best answer we have got which is the same as the true value.

**Table 6.** Workers answers of categorical attributes

| ID | confidence | answers             |
|----|------------|---------------------|
| A  | 0.90       | professor           |
| B  | 0.83       | professor           |
| C  | -0.50      | lecturer            |
| D  | 0.86       | associate professor |
| E  | 0.56       | associate professor |
| F  | -0.34      | professor           |
| G  | 0.92       | professor           |
| H  | 0.70       | associate professor |

**Fig. 3.** The vote weight value

Through the analysis of these three types of experiments, we found that we can fill the missing values based on crowdsourcing with a high quality.

## 5 Conclusion

In this paper, we present a method to fill the missing values with crowdsourcing. Since any kind of traditional machine learning has its shortcoming, and completely human identification method is too slow and expensive. Therefore, we propose a human-machine hybrid workflow to study the missing value filling method with crowdsourcing. First we propose a missing value selection algorithm to select the missing values which are suitable to use crowdsourcing for filling. Then we propose three missing values filling methods according to different attribute types to select answers from crowdsourcing. Experimental results show that our algorithms achieve good efficiency and high accuracy.

Our study represents an initial attempt to use crowdsourcing platform to solve human problems. There are many further researches to explore.

(1) The degree of confidentiality of information that we should make more profound constraints. With the permission of owners, information can be provided to the workers, but the information belongs to privacy should be masked out.

(2) The cost of different quality workers is different. We intend to find a way to balance the cost and the accuracy.

**Acknowledgement.** This paper was partially supported by NGFR 973 grant 2012C B316200, NSFC grant 61003046, 61111130189 and NGFR 863 grant 2012AA011004.

## References

1. Amazon Mechanical Turk (2013), <http://www.mturk.com>
2. Qiang, L., Jian, P., Alexander, T.: Ihler: Variational Inference for Crowdsourcing. In: NIPS, pp. 701–709 (2012)
3. Wang, J., Kraska, T., Franklin, M.J., Feng, J.: CrowdER: Crowdsourcing Entity Resolution. In: VLDB (2012)
4. Dempster, A.P., Laird, N.M., Rubin, D.B.: Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society. Series B (Methodological), 1–38 (1977)
5. Walsh, B.: Markov chain Monte Carlo and Gibbs sampling. Lecture notes for EEB 581 (version April 26, 2004)
6. Yang, K., Li, J., Wang, C.: Missing values estimation in microarray data with partial least squares regression. In: Alexandrov, V.N., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2006. LNCS, vol. 3992, pp. 662–669. Springer, Heidelberg (2006)
7. Shan, Y., Deng, G.: Kernel PCA regression for missing data estimation in DNA microarray analysis. In: IEEE International Symposium on Circuits and Systems, ISCAS 2009, pp. 1477–1480. IEEE (2009)

8. Lakshminarayanan, K., Harp, S.A., Goldman, R., et al.: Imputation of missing data using machine learning techniques. In: Proceedings of the Second International Conference on Knowledge Discovery and Data Mining, pp. 140–145 (1996)
9. Li, X.B.: A Bayesian approach for estimating and replacing missing categorical data. *Journal of Data and Information Quality (JDIQ)* 1(1), 3 (2009)
10. Di Zio, M., Scanu, M., Coppola, L., et al.: Bayesian networks for imputation. *Journal of the Royal Statistical Society: Series A (Statistics in Society)* 167(2), 309–322 (2004)
11. Mayfield, C., Neville, J., Prabhakar, S.: ERACER: a database approach for statistical inference and data cleaning. In: Proceedings of the 2010 International Conference on Management of Data, pp. 75–86. ACM (2010)
12. Zhang, S.: Shell-neighbor method and its application in missing data imputation. *Applied Intelligence* 35(1), 123–133 (2011)
13. Zhang, C., Zhu, X., Zhang, J., Qin, Y., Zhang, S.: GbkII: An imputation method for missing values. In: Zhou, Z.-H., Li, H., Yang, Q., et al. (eds.) PAKDD 2007. LNCS (LNAI), vol. 4426, pp. 1080–1087. Springer, Heidelberg (2007)
14. Setiawan, N.A., Venkatachalam, P., Hani, A.F.M.: Missing attribute value prediction based on artificial neural network and rough set theory. In: International Conference on Bio-Medical Engineering and Informatics, BMEI 2008, vol. 1, pp. 306–310. IEEE (2008)
15. Shen, L., Joshi, A.K., An, S.V.M.: based voting algorithm with application to parse reranking. In: Proceedings of the Seventh Conference on Natural Language Learning at HLT-NAACL 2003, vol. 4, pp. 9–16. Association for Computational Linguistics (2003)
16. Fan, W., Geerts, F., Ma, S., Tang, N., Yu, W.: Data Quality Problems beyond Consistency and Deduplication. In: Tannen, V., Wong, L., Libkin, L., Fan, W., Tan, W.-C., Fourman, M., et al. (eds.) Buneman Festschrift 2013. LNCS, vol. 8000, pp. 237–249. Springer, Heidelberg (2013)

# Sectional and Conditional Functional Dependencies

Mingda Li, Hongzhi Wang, and Ye Li

Department of Computer Science and Technology, Harbin Institute of Technology, China  
`{limingda,wangzh,liye32}@hit.edu.cn`

**Abstract.** This paper proposes the concept and applications of the sectional and conditional functional dependency (SCFD), which is an important extension of the conditional functional dependency (CFD) and the functional dependency (FD). SCFDs describe relationship between parts of an attribute with other attributes, and they can be used as rules during data cleaning. Two algorithms named DBCFD and DKMP are designed for SCFD discovery. The DBCFD can find general SCFDs using the attributes in CFDs, while the DKMP can find SCFDs for the other attributes outside CFDs. The combination of DBCFD and DKMP is able to ensure the completeness of SCFDs. Meanwhile, we provide the SQL technique to clean data based on SCFDs. In experiment we evaluate the effectiveness and efficiency of the SCFDs using dataset generated by TPC-H, and the experiment results illustrate the effect of our algorithm on two kinds of real dataset.

## 1 Introduction

It is well recognized that business and scientific data are growing rapidly and the value of data becomes higher. However, the quality of such data is compromised by sources of noise that are hard to remove from the data. Therefore, people discover different kinds of rules such as the functional dependencies (FDs) in data and use them for cleaning. Recently, conditional functional dependencies(CFDs) were introduced for data cleaning. They extend FDs and have been proven more effective than FDs in finding and repairing dirtiness of data[1][2].

But both FDs and CFDs deal with the relationship among integrated attributes. In many conditions, you will find that it is meaningful to find the dependencies among parts of attributes and integrated attributes, as illustrated by the example below.

**Example 1.** The following table specifies a person in a school in terms of his basic information.(college code(CC), major code(MC), status(ST), grade(GR), school identification number(SIN), name(NA), gender(GE) [M:Men;W:Women]).

From the table, we can find the traditional FD:

$$f1:[ MC,ST,GR,NA] \rightarrow SIN$$

In contrast, the CFDs include not only the FD  $f1$ ,but also the following :

$$\beta1:([ MC,ST, GR,NA] \rightarrow SIN, (., ., ., ., .) \parallel (., .))$$

$$\beta2:([NA] \rightarrow GE, (John \parallel M)) \quad \beta3:([ST] \rightarrow GR, (Professor \parallel XX))$$

However, if we observe the table carefully, we will find some new dependencies after we divide the SIN into five parts: SIN<sub>1-4</sub>, SIN<sub>5-6</sub>, SIN<sub>7-8</sub>, SIN<sub>9-11</sub>, and SIN<sub>12</sub>. We can divide the MC into two parts: MC<sub>1-2</sub>, MC<sub>3-4</sub>. The new dependencies are as follows.

$$\begin{aligned} \varphi_1: & [\text{MC}] \rightarrow \text{SIN}_{1-4}(\_\|\_) \quad \varphi_2: [\text{ST}] \rightarrow \text{SIN}_{5-6}(\_\|\_) \quad \varphi_3: [\text{GR}] \rightarrow \text{SIN}_{7-8}(\_\|\_) \\ \varphi_4: & [\text{GE}] \rightarrow \text{SIN}_{12}(\_\|\_) \quad \varphi_5: [\text{CC}] \rightarrow \text{MC}_{1-2}(\_\|\_) \end{aligned}$$

**Table 1.** Basic information of persons in a school

|    | CC | MC   | ST        | GR | SIN          | NA    | GE |
|----|----|------|-----------|----|--------------|-------|----|
| t1 | 11 | 1103 | Bachelor  | 01 | 11030101002X | David | M  |
| t2 | 11 | 1104 | Master    | 01 | 11040201010X | John  | M  |
| t3 | 01 | 0109 | Bachelor  | 03 | 01090103002Y | Chris | W  |
| t4 | 01 | 0109 | Master    | 01 | 01090201001Y | Diana | W  |
| t5 | 03 | 0301 | Doctor    | 01 | 03010301018X | John  | M  |
| t6 | 03 | 0305 | Bachelor  | 02 | 03010102037Y | Laura | W  |
| t7 | 03 | 0305 | Master    | 01 | 03010201011Y | Jones | W  |
| t8 | 03 | 0305 | Professor | XX | 030504XX012X | Chris | M  |
| t9 | 03 | 0305 | Professor | XX | 030504XX001X | John  | M  |

You will find these new dependencies help a lot to find the faults of dirty tuples easily because you only need to compare the part of an attribute's string with others. We define this kind of dependencies as sectional and conditional functional dependencies(SCFDs). Meanwhile, when we see integrated attribute as a whole part of itself, CFDs can be seen as SCFDs. Therefore, the SCFDs we find contain CFDs.

To discover SCFDs, we need to find the attributes to be divided firstly. Then we discover an algorithm called *FACFD* based on results of *CFD* algorithms to find some attributes to be divided defined as *d-attributes*. And we develop *DSCFD* to find SCFDs to the d-attributes. Meanwhile, to other attributes cannot be determined by the help of *CFDs*, we develop *KMP* algorithm to *OKMP* for finding *d-attributes*. After that, we use *SCFDMiner* developed from CFDMiner to discover SCFDs to the *d-attributes* found by *OKMP*. In the process, you can find that we do not just divide one attribute to several attributes to use existing CFD algorithms for finding SCFDs . We keep the original integrated attributes and just see the parts of attributes as *sub-attributes*. After discovering the SCFDs, we use them to clean data with the SQL technology introduced in Section 5.

## 2 Preliminaries

A CFD is a pair  $(X \rightarrow A, t_p)$ , where  $X$  is a set of attributes in the items and  $A$  is a single attribute decided by  $X$ .  $t_p$  is a pattern tuple with attributes in  $X$  and  $A$ , and for an attribute  $C$  in  $X \cup A$ , the  $t_p[C]$  is either a constant or an undetermined variable shown as “\_”. The  $X$  is called the LHS and the  $A$  is called the RHS by us. A sign “||” is to separate the  $X$  and  $A$  attributes.

When the  $t_p[A]$  and  $t_p[B]$  are both constants, we define such CFDs as *constant CFDs*. When  $t_p[A]$  is “\_” and the value of  $t_p[B]$  depends on that of  $t_p[A]$ , we call such CFDs as *variable CFDs*. The *general CFDs* include both the constant and variable CFDs. We call a CFD as a *left-reduced CFD* when there is no  $Z$  making a

new CFD ( $Z \rightarrow A, (t_{\text{plla}})$ ). Similarly, we can know the *constant SCFDs*, the *variable SCFDs* and the *general SCFDs*. The SCFDs we find are also left-reduced.

### 3 DBCFD: Discover SCFDs Based on CFDs

To find the SCFDs, we need to ensure the attributes we need to divide. We find that when an attribute set  $\{r_1, r_2, r_3, \dots, r_n\}$  can decide another attribute  $r_0$ , we can find many new dependencies on the *sub-attributes* after dividing  $r_0$  which has been shown in Example 1. Therefore, we use the CFDs to help us decide the attributes to be divided. And to get enough CFDs to help us finding SCFDs, we need to synthesize three algorithms in [3] effectively, which is introduced in Section 3.1. Based on the CFDs discovered by us, we ensure the *d-attributes* by an algorithm *FACFD* developed by us. After ensuring the attributes, we develop an algorithm *DSCFD* which is introduced in Section 3.3 to divide the d-attributes and find SCFDs on them.

#### 3.1 Synthesis of CFD Algorithms

Since we want to get enough CFDs, we need to synthesize the CFD algorithms efficiently. We find the three algorithms all need to calculate the number of supporters for different amount of attributes. Therefore, we establish a hash table and with it we reduce repeat calculation in process of finding CFDs by three algorithms.

Meanwhile, from [3], we find the CFDMiner is faster than the other two methods by three orders of magnitude. The CTANE works better than FastCFD when the data set has small arity and large amount of items. When there are more than 17 attributes in an item, the CTANE can hardly run. And the FastCFD scales well with the large arity and large size of data. Therefore, we use the CFDMiner and CTANE for the data set with attributes smaller than 11 and more than 1 million tuples according to the conclusion and Fig.5 in[3]. We use the CFDMiner and FastCFD for discovering CFDs for the other kinds of data set.

#### 3.2 FACFD: Find the d-attributes Based on CFDs

After we get the CFDs, we need to find the d-attributes based on them. The pseudo code is shown in Algorithm 1 to help you understand following process. A d-attribute is to be divided into many sub-attributes and we can find dependencies between its sub-attribute with other sub-attributes or attributes. So for a CFD ( $X \rightarrow A, t_p$ ) we do not find d-attributes from it when the LHS i.e.  $X$  only includes one attribute.(Line 2) When LHS includes several attributes, we need to assure there are dependencies between the sub-attributes of *RHS* and the attributes in LHS.

**To Variable CFDs:** We use the control variable method to help us. We set a bool variable *label* as 0 which will help us later(Line4). We divide the data set into two parts and find a set of items  $S$  from the former half of data set.  $S$  are with only an attribute  $X_i (1 \leq i \leq |X|)$  in LHS different(Line 5-6).We choose an item  $t$  in  $S$  randomly,

and we compare it with the other items(Line 7-11). In the comparing process, we record the starting position different character appears and the ending position.

When we compare  $t$  with an item  $t_j$ . The attribute  $A$  in  $t$  contains  $a_1$  characters and the  $A$  in  $t_j$  contains  $a_2$  characters. When we compare the two strings, we find the characters are all the same from the 1<sup>st</sup> to  $h^{\text{st}}$  character in  $t$  and  $t_j$ (Line 11). And it is different for each character from the  $h^{\text{st}}$  to  $(h')^{\text{st}}$  of  $t[A]$  and  $t_j[A]$ (Line 11). After the  $(h')^{\text{st}}$ , there is no character left or only the same characters left(Line 12). Similarly, we compare the characters in  $X$ . And we find the characters from the  $h_1^{\text{st}}$  to  $(h_1')^{\text{st}}$  of  $t[X]$  and  $t'[X]$  are different(Line 13).

We compare the  $h' - h$  with  $h_1' - h_1$ (Line 14). If they are not the same, or the left characters are not all the same from  $h'$ , we quit this CFD and find another(Line 15). If they are the same number no matter which item in  $S$ , we see the  $A$  as a d-attribute(Line 18-19). In the process of comparing, we save the result  $h', h$  into an array  $dif$  which we will use in the Section 3.3(Line 17).

**To Constant CFDs:** It is hard to find SCFDs from constant CFDs due to the lack of changing which can tell us the dependency in the changing. Therefore, we find all the constant CFDs with the same RHS(Line 21-22). And for each attribute except  $X$ , we see if there are more than two constant CFDs including it in LHS and have the same amount.(Line 24-27). We put these CFDs in a CFD set and find if there is a same sub-attribute of  $X$  appearing at the same space with the method similar to original one. (Line 25-30). If there is, we can define  $X$  as a d-attribute. Meanwhile, we will see if this conclusion is right or not in Section 3.3.

### Algorithm 1. FACFD

**Input:** The data set  $D$ . The CFDs found by the synthesis of algorithms. The *arity* (a constant) attributes numbered from 1 to *arity* in each item.

**Output:** The array  $d\text{-attribute}[arity]$  showing the d-attributes ensured by us. The array  $dif[arity][arity][|S|][2]$  saving the result  $h', h$  for each d-attribute.

```

1. for each CFD β do
2. if β -LHS contains only an attribute then break;
3. else if β is a variable CFD then
4. label=0;
5. for each attribute $X_i \in \beta[X]$ do
6. find a set S with only X_i different
7. Choose an item t from S randomly;
8. $S=S-\{t\}$;
9. While $S \neq \emptyset$ do
10. Choose the j_{th} item t_j from S
11. $h=\text{FD}(t[X_i], t_j[X_i], 1); h'=\text{FS}(t[X_i], t_j[X_i], h)$
12. if $(\text{FD}(t[X_i], t_j[X_i], h')=a_1 \text{ then}$
13. $h_1=\text{FD}(t[A], t_j[A], 1); h_1'=\text{FS}(t[A], t_j[A], h_1)$
14. if $(h-h_1 \neq h'-h_1) \text{ || } (\text{FD}(t[X_i], t_j[X_i], h) \neq a_1) \text{ then}$
15. label=1; go to 1;
16. else
17. $dif[A][i][j][0]=h; dif[A][i][j][1]=h'; S=S-\{t'\}$
18. if $\text{label}=0 \text{ then}$
19. add A to $d\text{-attribute}$
```

```

20. else if β is a constant CFD then
21. if a constant CFD ϕ with same RHS as β then
22. Add ϕ into a CFD set S_1
23. if $S_1 \neq \phi$, then
24. for each attribute X_i in the LHS of β do
25. if there is CFD ϕ' in S_1 having X_i and $\phi'[X_i] = \beta[X_i]$
26. $h_1 = FS(\phi'[A], \beta[A], 1)$ $h_1' = FD(\phi'[A], \beta[A], h)$
27. $h = FD(t[X_i], t_j[X_i], 1)$ $h' = FS(t[X_i], t_j[X_i], h)$
28. if $h - h = h_1 - h_1'$ then
29. $j++$; add A to d-attribute array;
30. $dif[A][i][j][0] = h; dif[A][i][j][1] = h'$
31. Output two arrays dif and d -attribute

```

*Note:* 1.  $FD(string1, string2, i)$  is a function to find the position of the different character firstly appears in the string1.

2. The  $FS(string1, string2, i)$  is a function to find the position of the same character firstly appears from the  $i^{th}$  character in string1

---

Time complexity Analysis During the process of finding d-attributes, we can find that after getting the CFD and a set of items  $S$  with only one attribute different, we need only choose an item and compare in finite times. As to constant CFDs, comparing times are less because we see constant CFDs as items. Therefore, the major part of time is to search for  $S$  with only one attribute different. And this is an  $O(n)$  process.

### 3.3 DSCFD: Use the d-Attributes to Discover SCFDs

Utilizing the FACFD algorithm, we can get the d-attributes and the array  $dif[arity][arity][|S|][2]$ . The  $dif$  shows us that, to a d-attribute  $i$ , if a part of  $i$  depends on another attribute  $X_j$ , with  $X_j$  compared to all other items in  $S$ , we can get different ways to divide  $i$ . A way of dividing is shown by a couple of  $h$  and  $h'$  which means we divide the  $i$  attribute from the  $h^{th}$  character to the  $h'^{th}$  character to form a sub-attribute. And  $X_j$  can decide the sub-attribute. The  $h$  and  $h'$  are in  $dif[i][j][m][0]$  and  $dif[i][j][m][1]$  respectively. With  $m$  changes from 1 to  $|S|$ , we can get many  $h$  and  $h'$ .

To discover SCFDs, we need to ensure a couple to divide  $i$ . And since in Algorithm 1, we choose a random item from  $S$  and compare it with the other items in  $S$ . We know it is better to find the couple with  $\max_{1 \leq m \leq |S|} (h_m - h_m')$  to divide  $i$ .

So we develop the DSCFD to discover SCFDs based on the output in Algorithm 1. The pseudo code is shown in Algorithm 2 to help understand the process. We choose different d-attribute and see if we can divide it to parts and find the relation between parts and the other integrated attributes(Line 2-4). We find the biggest length in  $i$  influenced by  $X_j$ (Line 6-8). Then we get an SCFD which is variable. We sample randomly and test it on the sampling results. Since we samples from the front part of data set, we now test it on the back part of data(Line 10). If it works well on the items sampled by us, we can accept it. Otherwise, we quit it and choose a constant CFD replace it when the constant CFD can work well(Line 13-15). During the process, you may find the  $dif$  has some empty items which shows  $i$  is not a d-attribute or there is little connection between  $i$  and  $X_j$ . Then we can ignore it.(Line 5)

**Algorithm 2.** DSCFD

**Input:** The array  $d\text{-attribute}[arity]$ .The array  $diff[arity][arity][|S|][2]$ saving the result  $h', h$ . The  $arity$  (a constant) attributes numbered from 1 to  $arity$ .

**Output:** The array  $h0[arity][arity][2]$  which implies the SCFDs

```

1. int q=0;
2. for i = 1 to arity do
3. for j= 1 to arity do
4. for m= 1 to |S|do
5. if dif[i][j][m][1]=0 ,then go to 4
6. if (q<dif[i][j][m][1] - dif[i][j][m][0]) ,then q=dif[i][j][m][1] - dif[i][j][m][0];
7. h0[i][j][0]=dif[i][j][m][0];h0[i][j][1]=dif[i][j][m][1];
8. c=h0[i][j][0];d=h0[i][j][1];
9. get a variable SCFD $\beta(X_j \rightarrow i_{(c-d)}, (_||_))$
10. if β works well for items sampled from the back part
11. Accept it as a variable SCFD
12. else
13. Find the most popular couple of X_j and $i_{(c-d)}$
14. B turns to a constant SCFD $\beta'(X_j \rightarrow i_{(c-d)}, (fq||FQ))$
15. Test β' to decide whether accept it or not
16. Output all variable and constant SCFDs

```

Time complexity Analysis During the process , we can find the number of comparing times for finding SCFDs is  $arity^2 \times |S|$  |Since most items in  $dif$  are 0, the probability for comparing is  $p$  . So the time complexity is  $p \times arity^2 \times |S|$  with small  $p$  and  $arity$ .

## 4 DKMP: Discover SCFDs with the Help of KMP Algorithm

We have discovered SCFDs by help of CFDs in Section 3. However, there may be SCFDs among other attributes. We develop OKMP to find d-attributes. Then we develop CFDMiner to SCFDMiner for finding constant SCFDs on it. The reason for finding constant CFDs is that we cannot get so many supporters for the other attributes not in CFDs. The supporters for a variable CFD may be less. And since the rule we set in OKMP is too strict, we cannot wish all items meet the SCFDs.

### 4.1 OKMP: Find d-Attributes by the Ordered KMP Algorithm

To ensure the d-attributes, the pseudo code is shown in Algorithm 3. We find that the d-attribute always contains much more characters in it which can make itself be divided into many sub-attributes. So we count the average length of each attribute(Line 1-2). And we sort the attributes in an ascending order to form an attribute set  $\{r_1, r_2, r_3, \dots, r_n\}$ . (Line 3) Then we suppose when the d-attributes  $r_o$  we find can be divided into many parts  $r_{sub1}, r_{sub2}, \dots, r_{subn}$ , and  $r_i$  can decide  $r_{subj}$  , than  $r_i=r_{subj}$  . The reason we set such a strict rule is for SCFD need to be strict to promise the efficience.

Meanwhile, using this strict rule, when  $r_i$  decides the sub-attribute of  $r_j (j \geq i)$  and  $r_k$  decides  $r_l (k \leq i)$ , we can know  $r_k$  must decide the sub-attribute of  $r_j$ . So we set array  $del[n]$  to record the attributes an attribute need not compare with. And the array  $line[n]$  to record the attributes can decide(Line 5). We do not need to check the relation between  $r_k$  and  $r_j$ . Therefore, the order of comparing the attributes using KMP is from  $r_n$  to  $r_1$ . (Line 7-8) We modify KMP to KMPS and let it give amount to array  $a[2]$  when there is a sub-string. KMPS return 0 when there is no string in. The array is with a starting number  $a[0]$  and an ending number  $a[1]$  of characters in  $r_j$  that can be decided by  $r_i (j \geq i)$ . This means  $r_i > r_j [a[0]-a[1]]$ . To make the following process of finding SCFDs in Section 4.2, we need to store the  $a[0]$  and  $[1]$  in an array.

### Algorithm 3. OKMP

**Input:** The attribute set  $S = \{r_1, r_2, r_3, \dots, r_n\}$  with attributes numbered from 1 to  $n$ .  
The d-attributes  $d\text{-attribute}[q]$  found by FACFD .

**Output:** The array  $label[n][n][2]$  storing at most  $n$  kinds of method to divide an attribute.(There are at most  $n$  kinds of dividing for each attribute.)

1. **for**  $i = 1$  to  $n$  **do**
2.     **Calculate** average length of each attribute for  $r_i$  in  $S$
3.     Sort attributes by length in ascending order
4.     Restore  $n$  attributes in the ascending order
5.     **int**  $a[2]$ ; **int**  $del[n]$ ; **int**  $line[n]$ ;
6.     **for a set of items S**
7.         **for**  $i=n-1$  to 1 **do**
8.             **for**  $j$  from  $i+1$  to  $n$  and  $j$  not in  $del[n]$
9.                 **if** (KMPS( $S_i, S_j, a$ )=1 for each item in  $S$ )
10.                      $label[i][j][0]=a[0]$ ;  $label[i][j][1]=a[1]$ ;
11.                     **add**  $i$  **to**  $line[i]$ ; **add**  $line[j]$  **to**  $del[i]$ ;
12.     **For** each number  $y$  in  $d\text{-attribute}[q]$
13.         **let**  $label[y][*][*]=0$ ;
14.     **output**  $label[n][n][2]$

Time complexity Analysis During the process, we use the SKMP algorithm whose time complexity is the same with KMP which is  $O(m+n)$ . And since circulation needs about  $arity \times arity / 2$  times. Therefore,  $(m+n) \times arity \times arity / 2 \times |S|$  is time complexity

## 4.2 SCFDMiner: Develop CFDMiner to Find SCFDs

By OKMP, we can find d-attributes and the method of dividing them to get sub-attributes. Since the rule we set in OKMP is too strict, we cannot wish the other items except samples meet the SCFDs. So we just find constant SCFDs by SCFDMiner.

The SCFDMiner is developed from CFDMiner. It modifies it as following:.

(a) Before we find SCFDs, we divide the d-attributes according to the arrays we get from the method above and add the sub-attributes to the data set. Meanwhile, we keep the d-attributes because there are some CFDs we can find on it.

(b) In CFDMiner, it finds free and their closed set by the GCGROWTH algorithm in[5]. However, we should avoid the d-attributes and their sub-attributes appear in

the same set. Therefore, when we contain a d-attribute in a closed item set, we do not contain their sub-attributes in the same set or the free set associated with the closed set. When there is a sub-attribute in a closed item set, we ignore its d-attribute.

Meanwhile, we also need to avoid all sub-attributes of the same d-attribute appear together. Because this is the same to the d-attribute. Except adding the (a) process and modify the (b)process, we do to the data set with the same way as CFDMiner does.

## 5 Clean Data Set with SCFDs

The SCFDs we find contains the functional dependencies between the integrated attributes and sub-attributes. When we use SQL technology to clean data, we cannot do the cleaning to the items directly. Therefore, for a d-attribute  $r_1$ , we establish a table called  $r_1$  containing its sub-attributes and  $r_1$  as the major key. Each time when we clean data with SCFDs on the whole attribute, we need only use the original table.

Otherwise, when the SCFDs are based on the sub-attributes, we need to use the  $r_1$  table. When we check item  $t$ , we need to visit the  $r_1$  table and find the item whose major key is the  $r_1$  attribute of  $t$ . We provide the SQL technique for finding the violations of a single SCFD for sub-attributes .

For a SCFD  $\beta=(R : X \rightarrow A, Tp)$ , if it is a constant SCFD and A is a sub-attribute for attribute  $X_i$ , the SQL sentence is:

```
Select * from table1 left join table2 on table1. $X_i=table2. X_i$ t, Tp tp
```

```
Where t[X]=tp[X] and t[A]≠tp[A]
```

If it is a variable CFD, we use SQL like following

```
Select distinct X from table1 left join table2 on table1. $X_i=table2. X_i$ t, Tp tp
```

```
Where t[X]=tp[X] and tp[A]='_ 'Group by X having count(distinct A)>1
```

## 6 Experimental Study

We present experimental study of our algorithm for discovering SCFDS. To verify efficiency and effectiveness of proposed algorithms, we do extensive experiments. We use DBCFD for attributes in CFDs and DKMP for other attributes each time.

### 6.1 Experimental Settings

The experiments were conducted on both synthetic data sets and on both real-life data. We firstly use the synthetic data generated by TPC-H, which is a decision support benchmark and can generate data in any size to evaluate the performance and scalability of our algorithm.

We also used real data sets from the UCI machine learning repository (<http://archive.ics.uci.edu/ml/>), namely,Amazon Access Samples Data Set and KEGG Metabolic Reaction Network (Directed).The following table describes two sets:

**Table 2.** The Parameters of Real Dataset

| Dataset                                    | Arity | Size(# of tuples) |
|--------------------------------------------|-------|-------------------|
| Amazon Access Samples Data Set             | 20000 | 30000             |
| KEGG Metabolic Reaction Network (Directed) | 24    | 53414             |

All algorithms are implemented in C++. The program has been tested on Intel kurui i7 4770 (3.4GHZ) with 8 GB of memory running Ubuntu operating system.

## 6.2 Experimental Result

We first present our experimental results on generated data, and then on real data.

### 6.2.1 Scalability Experiments

**The Impact of Tuple Number.** We varied DBSIZE from 30K to 120k tuples by fixing the ARITY 10. From Fig.1, we can know that we use FastCFD for discovering CFDs firstly from 30K to 1000K. After 1000K, the line changes the shape due to the use of CTANE rather than FastCFD.

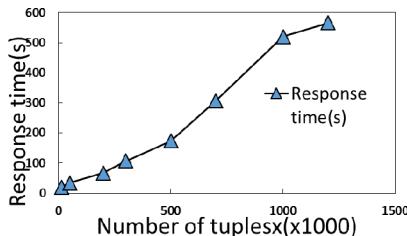


Fig. 1. The impact of tuple number for TPC-H

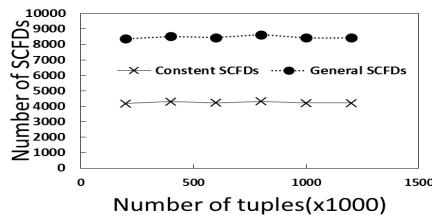


Fig. 2. The number of SCFDs for TPC-H

The Fig.2 shows the SCFDs we discovered by our algorithm. Since we think the CFDs as a kind of SCFDs on the whole attributes, the SCFDs in Fig.2 include both the integrated attributes and sub-attributes. From the figure, we can know that there are more variable SCFDs than constant SCFDs . And the amount of SCFDs is stable.

**The Impact of Attribute Number.** We varied the arity from 5 to 29 by fixing the DBSIZE as 30K items. Fig.3 shows when the number of ARITY  $\leq 15$ , the response time is low. When ARITY is over 20, the time increases faster than before.

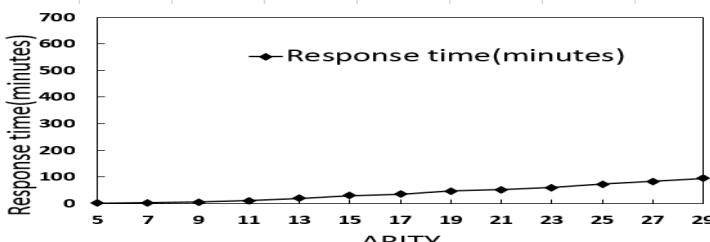
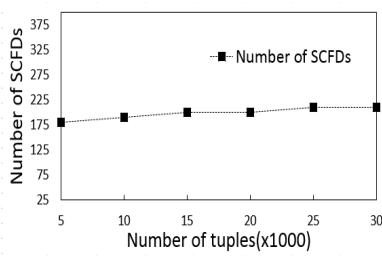


Fig. 3. The impact of attribute number for TPC-H

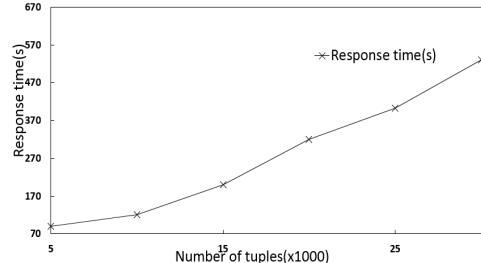
### 6.2.2 Real Data Experiments

We did the experiments on real data, including Amazon Access Samples Data Set and KEGG Metabolic Reaction Network (Directed). To the Amazon Access Samples Data Set, we choose about 13 attributes from this datasets to do experiment. It is because the original datasets have 20000 attributes for each item and many of them are not available. We use KEGG Metabolic Reaction Network (Directed) directly.

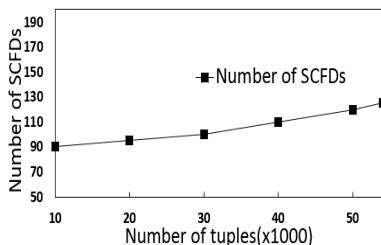
Figs. 4,5 show the number of SCFDs and the response time of the varied tuples in Amazon Access Samples Data Set. Figs. 6,7 are for the other real data set. The SCFDs there only contain those SCFDs on sub-attributes found by our methods:



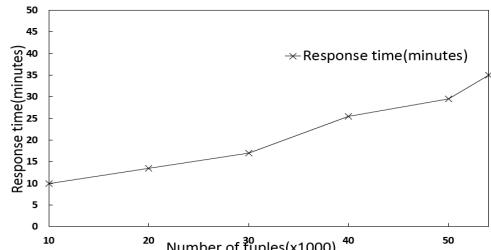
**Fig. 4.** The number of SCFDs for 1<sup>st</sup> real data set



**Fig. 5.** The impact of tuple number for 1<sup>st</sup> real data set



**Fig. 6.** The number of SCFDs for 2<sup>nd</sup> real data set



**Fig. 7.** The impact of tuple number for 2<sup>nd</sup> real data set

Figs.4, 6, show the number of SCFDs are not related to attributes. Although item has more attributes, the SCFDs can be few when there is little relation. Meanwhile, Figs.5,7 show relation between time and tuple number is similar to linear relationship.

## 7 Conclusions

In this paper, a new kind of functional dependency called SCFD is proposed by us. We provide two methods to discover SCFDs. We use the DBCFD for attributes in CFDs and DKMP for other attributes each time for finding SCFDs. Meanwhile, we

give SQL technology to help us use SCFDs clean data set. By experiments, we find our method can find SCFDs in a linear time to number of tuples. Meanwhile, we find the number of SCFDs on sub-attributes found by us is stable with change of tuples.

**Acknowledgment.** This paper was partially supported by NGFR 973 grant 2012C B316200, NSFC grant 61003046, 61111130189 and NGFR 863 grant 2012AA 011004.

## References

1. Fan, W., Geerts, F., Jia, X., et al.: Conditional functional dependencies for capturing data inconsistencies. *ACM Transactions on Database Systems (TODS)* 33(2), 6 (2008)
2. Cong, G., Fan, W., Geerts, F., et al.: Improving data quality: Consistency and accuracy. In: *Proceedings of the 33rd International Conference on Very Large Data Bases*, pp. 315–326. VLDB Endowment (2007)
3. Fan, W., Geerts, F., Li, J., et al.: Discovering conditional functional dependencies. *IEEE Transactions on Knowledge and Data Engineering* 23(5), 683–698 (2011)
4. Chu, X., Ilyas, I.F., Papotti, P.: Holistic data cleaning: Putting violations into context. In: *2013 IEEE 29th International Conference on Data Engineering (ICDE)*, pp. 458–469. IEEE (2013)
5. Li, H., Li, J., Wong, L., et al.: Relative risk and odds ratio: A data mining perspective. In: *Proceedings of the Twenty-fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 368–377. ACM (2005)
6. Knuth, D.E., Morris, J.J.H., Pratt, V.R.: Fast pattern matching in strings. *SIAM Journal on Computing* 6(2), 323–350 (1977)

# Author Index

- Abdeldjalil, Tabouche 90  
Ai, Chunyu 44, 718  
Alhothaily, Abdulrahman 356, 554  
Alrawais, Arwa 356, 554  
  
Bi, Ran 215, 246  
Bie, Rongfang 102, 356, 436, 507, 531  
  
Capurso, Nicholas 648  
Champion, Adam C. 576  
Chen, Chuanqing 682  
Chen, Dechang 436  
Chen, Di 22  
Chen, Jian-xin 401  
Chen, Qianbin 613  
Chen, Quan 215, 672  
Chen, Yingwen 78, 114, 126  
Cheng, Wei 482, 636, 660  
Cheng, Xiuzhen 356, 482, 554, 648  
Cho, Sunghyun 194  
Cui, Gang 750  
Cui, Xuewei 636  
  
Ding, Sihao 576  
Dong, Yi 401  
Duan, Qiang 613  
  
Egli, Richard 313  
  
Fan, Haosheng 389  
Fan, Xiumei 126  
Feng, Zhenqian 34  
Fives, Aaron 313  
Fu, Hai 34  
  
Gao, Hong 1, 173, 215, 246, 672, 694, 740  
Gao, Jing 225  
Gao, Xing 542  
Gao, Ying 542  
Gu, Qijun 660  
Gu, Xin 682  
Guo, Chao 183, 256  
Guo, Junqi 236  
Guo, Longjiang 44, 542  
  
Hahn, Changhee 267, 624  
Han, Qilong 347, 694  
Han, Zhenhua 494  
Hao, Liang 750  
He, Yan 54  
Howell, Russell 313  
Hu, Chengchen 22  
Huang, Baogui 150  
Huang, Jianhui 436  
Huang, Jun 613  
Humayoo, Mohammad 54  
Huo, Yan 482, 519, 636  
Hur, Junbeom 267, 624  
  
Jackson, David 660  
Jia, Lili 378  
Jiang, Huaipan 368  
Jiang, Libo 290  
Jiang, Shouxu 773  
Jing, Tao 482, 519, 636  
  
Kang, Kyungtae 267, 624  
Ke, Wende 750  
Kim, Daeyoung 267, 624  
Kim, Donghyun 368  
Kim, Jae-Hyun 194  
Kuang, Xiaohui 412  
Kwon, Hyunsoo 267, 624  
  
Larson, Maya 126  
Lee, Joonglyul 368  
Lee, Kyu-Hwan 194  
Lee, Victor C.S. 389  
Li, Bowen 412  
Li, Changle 183, 256  
Li, Dazhou 279  
Li, Deying 368  
Li, Fan 90, 290  
Li, Frank Haizhon 718  
Li, Guilin 542  
Li, Jianzhong 1, 225  
Li, Jibi 613  
Li, Ming 589  
Li, Mingda 793

- Li, Minming 389  
 Li, Pei 114  
 Li, Ruiling 90  
 Li, Sinan 279  
 Li, Wei 66  
 Li, Xin 90  
 Li, Ye 793  
 Li, Yingshu 246, 424  
 Li, Zhen 519  
 Li, Zhijun 773  
 Li, Zhuorong 102, 236  
 Liang, Qilian 706  
 Liang, Wenshuang 102, 236, 436  
 Lin, Juncong 542  
 Lin, Shirong 773  
 Liu, Bo 336  
 Liu, Hang 161  
 Liu, Huiying 183  
 Liu, Jing 589  
 Liu, Li 412  
 Liu, Yinshan 302  
 Lou, Yisha 601  
 Lu, Gan 22  
 Lu, Junjie 12  
 Lu, Xi-ruo 401  
 Luo, Hanwen 446, 601  
 Luo, Lin 161  
  
 Ma, Liran 648  
 Ma, Zan 66  
 Ma, Zhiqiang 347  
 Maherin, Ishrat 706  
 Mcintyre, Odayne 313  
  
 Pan, Haiwei 347  
 Pan, Lili 519  
 Peng, Yue 22  
  
 Qi, Penghe 729  
 Qian, Yuqiu 12  
  
 Ren, Meirui 44  
  
 Saad, Walid 302  
 Shen, Qiang 589  
 Shi, Shengfei 729  
 Song, Tianyi 648  
 Song, Yueyang 256  
 Su, Jinshu 324  
 Sun, Yunchuan 102  
  
 Tan, Haisheng 494  
 Tian, Chenfei 290  
 Tian, Ning 44  
 Tokuta, Alade O. 368  
  
 Wang, Bin 564  
 Wang, Chao 126  
 Wang, Chen 54, 531  
 Wang, Cui 150  
 Wang, Feng 313  
 Wang, Haiquan 601  
 Wang, Hao 173  
 Wang, Hongzhi 205, 783, 793  
 Wang, Jing 302  
 Wang, Shengling 436  
 Wang, Shenling 236  
 Wang, Xia 436  
 Wang, Xiaofei 22  
 Wang, Xiaojie 470  
 Wang, Xue 424  
 Wang, Yongcai 494  
 Wang, Yu 290  
 Wang, Zeye 290  
 Wei, Ziling 324  
 Wu, Chunqing 34, 336  
 Wu, Dengyuan 161  
  
 Xia, Deping 760  
 Xia, Xiaochen 458  
 Xie, Xiaobo 236  
 Xie, Xiaoqin 760  
 Xing, Kai 12  
 Xiong, Zi 613  
 Xu, Biaofei 368  
 Xu, Bingqing 54  
 Xu, Jing 66  
 Xu, Kuai 313  
 Xu, Ming 78, 114  
 Xu, Youyun 458  
 Xuan, Yiran 576  
 Xue, Ruiqi 446  
  
 Yan, Yang 302  
 Yang, Fan 576  
 Yang, Xiaochun 564  
 Ye, Chen 783  
 Yi, Dongyun 470  
 Yin, Dan 740  
 Yin, Guisheng 694  
 You, Bindu 750

- Yu, Dongxiao 150, 378, 682  
Yu, Hui 446, 601  
Yu, Jiguo 150, 378, 682  
Yu, Meng 564  
Yu, Wanrong 34  
Yuan, Bin 589
- Zang, Wanyu 564, 660  
Zhai, Yanlong 54  
Zhang, Bin 114  
Zhang, Fan 482  
Zhang, Guangzhi 236  
Zhang, Haidong 78  
Zhang, Hongyang 102  
Zhang, Jiayi 507  
Zhang, Kejia 347, 694  
Zhang, Meng 446, 601  
Zhang, Qingbo 378  
Zhang, Shuo 66  
Zhang, Xiao 389  
Zhang, Xue 470  
Zhang, Yan 205  
Zhang, Yu 256
- Zhang, Zhenming 336  
Zhang, Zhiqiang 760  
Zhao, Baokang 34, 324, 336  
Zhao, Chengli 470  
Zhao, Feng 507, 531  
Zhao, Hai 279  
Zhao, Hongbin 347  
Zhao, Yanxiao 613  
Zhao, Yingchao 389  
Zheng, Guanbo 138  
Zheng, Huanxia 279  
Zheng, Rong 138  
Zheng, Xu 1  
Zheng, Yuanfang 576  
Zhi, Huijiang 446  
Zhong, Xiaofeng 302  
Zhou, Jipeng 494  
Zhou, Liang 401  
Zhou, Tongqing 78  
Zhou, Wei 519  
Zhou, Xuan-cheng 401  
Zhu, Jinghua 424  
Zhu, Shixiang 636