OMiN - Opportunistic Microblogging Network

Neil Wells, supervised by Tristan Henderson

Abstract

OMiN is a pocket switched network running on smartphones. It allows users to send and receive microblog messages without using any global infrastructure such as the internet. Smartphones in close proximity to each other pass on messages according to a variation of the PROPHET routing protocol. Steps have been taken to verify the security of the network by protecting it against known attack vectors.

Declaration

I declare that the material submitted for assessment is my own work except where credit is explicitly given to others by citation or acknowledgement. This work was performed during the current academic year except where otherwise stated.

The main text of this project report is **NN,NNN*** words long, including project specification and plan.

In submitting this project report to the University of St Andrews, I give permission for it to be made available for use in accordance with the regulations of the University Library. I also give permission for the title and abstract to be published and for copies of the report to be made and supplied at cost to any bona fide library or research worker, and to be made available on the World Wide Web. I retain the copyright in this work.

Contents

- Abstract
- Declaration
- Contents
- Introduction
- Objectives
  - Primary Objectives
  - Secondary Objectives
  - Tertiary Objectives
- Context Survey
  - History
  - Similar Projects
    - Haggle
    - Firechat
    - SWIM
  - Security
    - IRONMAN
    - Social trust
  - Routing Algorithms
    - Epidemic
    - PROPHET
    - Bubble RAP
    - MV

- Requirements Specification
  - User Requirements
    - Non-Functional Requirements
    - Functional Requirements
  - System Requirements
    - Non-Functional Requirements
    - Functional Requirements
- Software Engineering Process
- Ethics
- Design
- Implementation
- Evaluation and Critical Appraisal
- Conclusions
- TODO
- Appendices
  - Appendix A - Testing Summary
  - Appendix B - Status Report
  - Appendix C - User Manual
  - Appendix D - Maintenance Document

Introduction

TODO

Objectives

Primary Objectives

- design and implement a protocol for discovering nodes in close proximity and passing messages and necessary metadata between them.
- Create a core library to manage message storage and routing.
- Implement a simple epidemic routing algorithm to send messages to all available nodes.
- Design a routing algorithm using user metadata to route messages while disguising message content and metadata.

Secondary Objectives

- Create a smartphone UI.
- Implement a more advanced routing algorithm.
- Design and implement a mechanism to decide whether a node is trustworthy or not.
- Evaluate the performance of the implemented routing algorithms.

Tertiary Objectives

- Compare the real world vs simulated performance of the routing algorithms.

Context Survey

The following provides brief summary of the current state-of-the-art in opportunistic network technology. Only the most relevant subjects will be addressed in order to give the reader sufficient background information to fully understand the project.

Opportunistic Networks

PSN

TODO

Similar Projects

Haggle

One of the largest opportunistic platforms is Haggle (http://www.haggleproject.org)[1], a pocket switched network designed to run on smartphones. There are implementations for a number of clients including Android (play.google.com/store/apps/details?id=org.haggle.kernel) and Windows Mobile.

By monitoring use of the platform, the authors discovered trends in inter-contact times and contact durations, showing that existing algorithms are poorly suited to real world models[2].

Firechat

Firechat (opengarden.com/firechat) is a new smartphone application used for off-the-grid messaging between nearby users. It has been used to circumvent government restrictions in Iraq (http://www.theguardian.com/technology/2014/jun/24/firechat-updates-as-40000-iraqis-download-mesh-chat-app-to-get-online-in-censored-baghdad) and during the Hong Kong protests (http://www.theguardian.com/world/2014/sep/29/firechat-messaging-app-powering-hong-kong-protests).

However, the app mostly relies on an internet connection, and its simple protocol is insecure (http://breizh-entropy.org/~nameless/random/posts/firechat_and_nearby_communication) and unable to implement the store-and-forward functionality of a proper opportunistic network.

SWIM

The Shared Wireless Infostation Model (SWIM) proposes using an opportunistic network to monitor whales[3]. Small nodes are attached to the whales, which record data such as location and interaction with other whales. Connected nodes transfer this data between each other. Whenever data is transferred to a base station (the paper proposes using seabirds), it can be collected and stored.

Because data is shared between nodes, it is no longer necessary to find a whale with a sensor in order to acquire data from that sensor. This is a perfect example of the power of opportunistic networks in an environment with very limited connectivity.

Security

TODO

IRONMAN

Social trust

Dissemination Based Routing Algorithms

There are two approaches to sending messages in an opportunistic network[7]:

In dissemination based routing, copies of the message are spread throughout the network in the hope that they will reach the destination. This is analogous to a breadth-first graph search. This tends to use lots of resources, because there are multiple copies of a message, but is usually very good at finding the best path to the destination. One common problem with dissemination based routing is determining when a message has been received and can be removed from the network.

In context based routing, limited copies of the message are passed between nodes until it reaches the destination. This is analogous to a greedy AI search technique. Very few resources are used because there are few copies of the message, but it is unlikely to find the fastest path to the destination.

I will focus on some well known dissemination based techniques here, as our network will use a dissemination based algorithm. This is because our network allows multiple destinations, and the message sender is not necessarily aware of every destination node. This makes a context based approach impossible.

Epidemic

The simplest method of message routing is called epidemic routing - messages are passed at every opportunity, aiming to reach every single user[4]. This can be likened to the spread of a virus, or a uniform cost AI search for the destination. If every node has an infinite buffer size, messages are guaranteed to reach the recipient by the shortest path. However, the routing protocol breaks down when nodes have a finite buffer size and are forced to evict messages from their buffer. For this reason,

routing protocols often use advanced heuristics to determine where the message should be send, to avoid flooding the whole network.

PROPHET

The Probabilistic Routing in Intermittently Connected Networks (PROPHET) algorithm[5] improves on epidemic routing by attempting to predict the paths that are most likely to reach the destination. It draws close parallels with the A* AI search algorithm - a utility function is used to determine how close a node is to the recipient, and the algorithm will only pass on messages to nodes that are close to the recipient. This utility function - the delivery predictability metric - is derived from recent encounters with destination nodes.

Bubble RAP

Bubble RAP[6] is an algorithm which seeks to build on the Haggle project's discovery that existing algorithms are unsuited to PSNs. Bubble RAP exploits the social structures of communities to identify nodes to forward messages to in order to reach other communities. This has been shown using the data collected from Haggle to be more effective than standard routing algorithms.

Requirements Specification

User Requirements

Non-Functional Requirements

- High: The user shall be able to create a unique identity.
- High: The user shall be able to send text messages to all others who follow the user or a hashtag in the message.
- High: The user shall be able to 'follow' any user and receive messages sent by that user.
- Low: The user shall be able to 'follow' any hashtag and receive messages containing that hashtag.
- Low: The user shall be able to send encrypted direct messages to a single user.
- Low: The user shall be able to send multimedia messages to all others who follow the user or a hashtag in the message.

Functional Requirements

None

System Requirements

Non-Functional Requirements

- High: The system shall work on smartphones or tablets capable of connecting to a wifi network.
- High: The system shall allow creation of user identities with a unique cryptographic identity.
- High: The system shall automatically connect to nearby nodes and pass on relevant information such as messages.
- Medium: The system shall provide a mechanism for securely distributing the cryptographic identity of a user.
- Medium: The system shall protect user metadata such as location and friends list from all other nodes.
- Medium: The system shall ensure that messages cannot be modified in transit or that such modifications can be detected.
- Medium: The system shall ensure that nodes cannot send a message that appears to be from another user.
- Medium: The system shall be robust and able to continue functioning when it encounters an unexpected state such as a malfunctioning or untrustworthy node.
- Medium: The system shall ensure that encrypted direct messages cannot be read by third parties.
- Low: The system shall be able to support multiple user identities on a single node.

Functional Requirements

- High: The system shall collect anonymous logging data for debugging and profiling purposes.
- Medium: The system shall ensure that a reasonable number of messages reach their intended recipients.
- Medium: The system shall restrict the size of the message buffer by evicting messages.
- Medium: The system shall use a minimal amount of the available power.

Software Engineering Process

TODO

Ethics

In order to test the real world performance of the network, we may ask people to use the application. In this case, some metadata will be collected on users, with their consent. This may include:

- An anonymous user ID.
- Anonymised 'Friends list' (or equivalent) of users.
- Times and locations of encounters between anonymous users.
- Metadata of messages passed during encounters, including message ID and origin ID, but NOT message contents.

Design

TODO

Implementation

TODO

Evaluation and Critical Appraisal

TODO

Conclusions

TODO

References

[1] Scott J, Crowcroft J, Hui P, Diot C, Others. Haggle: A networking architecture designed around mobile users. In: WONS 2006: Third Annual Conference on Wireless On-demand Network Systems and Services; 2006. p. 78-86.

[2] Chaintreau A, Hui P, Crowcroft J, Diot C, Gass R, Scott J. Impact of human mobility on opportunistic forwarding algorithms. Mobile Computing, IEEE Transactions on. 2007;6(6):606-620.

[3] Small T, Haas ZJ. The Shared Wireless Infostation Model: A New Ad Hoc Networking Paradigm (or Where There is a Whale, There is a Way). In: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing. MobiHoc '03. New York, NY, USA: ACM; 2003. p. 233-244. Available from: http://doi.acm.org/10.1145/778415.778443.

[4] Vahdat A, Becker D, Others. Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University; 2000.

[5] Lindgren A, Doria A, Schelén O. Probabilistic Routing in Intermittently Connected Networks. SIGMOBILE Mob Comput Commun Rev. 2003 Jul;7(3):19-20. Available from: http://doi.acm.org/10.1145/961268.961272.

[6] Hui P, Crowcroft J, Yoneki E. Bubble Rap: Social-based Forwarding in Delay Tolerant Networks. In: Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing. MobiHoc '08. New York, NY, USA: ACM; 2008. p. 241-250. Available from:http://doi.acm.org/10.1145/1374618.1374652.

[7] Pelusi L, Passarella A, Conti M. Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. Communications Magazine, IEEE. 2006 Nov;44(11):134-141. Available from: http://dx.doi.org/10.1109/MCOM.2006.248176.

Appendices

Appendix A - Testing Summary

TODO

Appendix B - Status Report

TODO

Appendix C - User Manual

TODO

Appendix D - Maintenance Document

TODO