SPRINGER BRIEFS IN COMPUTER SCIENCE

Yunchuan Sun
Houbing Song *Editors*

Secure and Trustworthy Transportation Cyber-Physical Systems

Springer

SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Yunchuan Sun · Houbing Song
Editors

Secure and Trustworthy Transportation Cyber-Physical Systems

Springer

Editors
Yunchuan Sun
Beijing Normal University
Beijing
China

and

China Information Technology Security Evaluation Center
Beijing
China

Houbing Song
Department of Electrical, Computer, Software, and Systems Engineering
Embry-Riddle Aeronautical University
Daytona Beach, FL
USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-981-10-3891-4 ISBN 978-981-10-3892-1 (eBook)
DOI 10.1007/978-981-10-3892-1

Library of Congress Control Number: 2017948629

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

The application of IT along with a rapid development of the Internet has dramatically changed both society and our daily lives; Critical Information Infrastructure (CII) thus plays an increasingly important role in safeguarding social stability and promoting economic development. The transportation network, including highways, airports and railroad systems, has evolved into a "social artery"—with vast amounts of goods as well as human beings moving day to day using the transportation network, making it a sensitive and significant part of the National Critical Information Infrastructure.

In modern transportation networks, the new concept of Cyber-Physical Systems (CPS) is emerging at the same time as the challenges we are facing are becoming more serious and complicated than ever before. It is now possible for vehicles (cars, trucks, airplanes, and trains) and important infrastructures (highways, airports, and railroad tracks) to connect with each other via the Internet. The applications of CPS in transportation, not only change the way people interact with transportation systems, but also change the world in which we live.

However, the greater the reliance becomes on information and communication technologies (ICT), the greater the challenges to transportation's CPS. Cybersecurity threats really place the development of the world's transportation systems at high risk. Therefore, securing the safety and reliability of transportation's CPS (automotive, aerospace, and rail) is one of the most important challenges that we face.

In order to meet the basic needs of transportation's CPS security development, that is, to overcome the increasing scientific challenges and secure sensitive information within the system, we need to further investigate optimized technologies. This is the motivation which drives the promotion of research and education in the fields of cybersecurity, privacy, CPS and transportation systems.

We believe this is the very first book researching the security and privacy of transportation's CPS. It is a long-awaited book which specifically presents current trending technologies, the practices of security and the reliability of transportation's CPS. In addition, this book bridges the gap between theory and practice.

This book presents techniques leveraging fundamental physical properties and laws; it aims to increase security, protect privacy, improve usability and support scalability within the extreme heterogeneity and mobility of transportation's CPS. It provides the readers with a deep understanding of the key technical, social and legal issues at stake as well as identifying a range of technical issues affecting cybersecurity and privacy in transportation's CPS. In the foreseeable future, this book will foster scientific research in transportation cybersecurity and encourage practical methods to overcome the difficulties and address the challenges that we face in transportation.

Dr. Sun is very hardworking and innovative in his research at CNITSEC . I very much appreciate his efforts and am thankful for his contributions. I hope there will be more academic research in this area to promote the harmonious development of the cyberspace society.

Beijing, China
January 2017

Shizhong Wu
China Information Technology
Security Evaluation Center

Preface

According to the definition of the US National Science Foundation, Cyber-Physical Systems (CPS), which are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications, are transforming the way people interact with engineered systems. Cyber-Physical Systems applied in transportation, i.e., transportation CPS (TCPS), are transforming the way people interact with transportation systems, including personal and commercial automotive, aerospace, and rail transport. However, TCPS are subject to various cybersecurity and privacy threats. To address these cybersecurity and privacy challenges in TCPS , novel, transformative, multidisciplinary approaches at the confluence of cybersecurity, privacy, and TCPS are needed.

This edited book, *Secure and Trustworthy Transportation Cyber-Physical Systems*, aims to summarize the scientific foundations and engineering principles needed to ensure the cybersecurity and privacy of TCPS, and the state-of-the-art research findings and practices in tackling the cybersecurity and privacy issues of TCPS. This book is organized into three parts: System Foundations; Principles; and Tools and Practices.

Part I is composed of three chapters. In addition to the opportunities and challenges facing the cybersecurity and privacy of TCPS (Chap. 1), this part also presents various scientific foundations of TCPS, including architecture and enabling technologies (Chap. 2), and properties, principles, and metrics (Chap. 3).

Part II is composed of three chapters. This part presents the various engineering principles behind the cybersecurity and privacy of TCPS, including privacy-aware computing (Chap. 4), trust management (Chap. 5), and secure data dissemination (Chap. 6).

Part III includes several tools and practices available to TCPS (Chap. 7).

This book will enable readers to update their knowledge of state-of-the-art approaches, technologies, and solutions to the issue of cyber security and privacy in TCPS. As the book includes several works from different researchers, experts, and professionals, it also provides the audience with an efficient channel for obtaining

ideas, learning various methodologies, and even building up communications in the future . For those readers with different research interests, the security and privacy issues introduced in this book may also be extended to other interdisciplinary subjects.

This book would not have been possible without the help of many people. First, we would like to thank all the contributors of each of the book's chapters as well as reviewers all over the world. Second, we would like to thank Xiaolan Yao and Celine Lanlan Chang, both at Springer , who guided us through the book-editing process. Third, we sincerely acknowledge the support of the China Information Technology Security Evaluation Center.

This book is sponsored by the National Natural Science Foundation of China (No. 61371185) and China Postdoctoral Science Foundation (No.2015M571231).

Beijing, China — Yunchuan Sun
Daytona Beach, USA — Houbing Song
February 2017

Steering Committee

Chair
Shizhong Wu

Members
Shengtao Zhu
Shoupeng Li
Changqing Jiang
Guiqing Zhang
Li Zhang
Tao Zhang

Contents

Part I
Foundations

Guaranteed Security and Trustworthiness in Transportation Cyber-Physical Systems

Lei Wu and Yunchuan Sun

Abstract Transportation cyber-physical systems (CPSs) have the potential to improve traffic safety, mobility, and environmental protection. However, they are subject to threats stemming from increasing reliance on information and communication technologies (ICT). Cybersecurity threats exploit the increased complexity and connectivity of the transportation-critical infrastructure system, placing the transportation at risk. This chapter reviews the state of the art and the state of the practice of CPS in various transportation sectors, including highway, railway, and air. This chapter also examines various cybersecurity threats to the transportation CPS and the current countermeasures to enhance cybersecurity of these CPS. It then discusses several challenges and opportunities in achieving secure and trustworthy transportation CPS.

1 Transportation Cyber-Physical Systems

> "The left wheel can produce strong winds, and the right wheel can burn fire. Wearing it means getting the power of flying anywhere as fast as light."
>
> "Monkey King is able to move thousands of miles away in an instant by this Tumbling Cloud."
>
> *Journey to the West*

In my childhood, my grandparents liked to tell me bedtime fairy stories. Every night at that time we always shared a small bedroom in a mountain village. In these ancient Chinese fictions, there are always some heroes or miraculous figures who are endowed with supernatural gifts on traveling. They can always reach any place

L. Wu · Y. Sun (✉)
Beijing Normal University, Beijing, China
e-mail: yunch@bnu.edu.cn

L. Wu
e-mail: araleii@mail.bnu.edu.cn

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_1

easily and freely in a moment by some different and extraordinary magical tools such as *Nezha*'s Hot Wheels, *Monkey King*'s Tumbling Cloud, and sometimes a piece of cloth with a magic spell, and so on. The fascinating story about the Goddess *ChangE* flying to the moon is also one of the most popular legends in China. These stories tell us about our ancestors' desire for quick and secure transport tools with which they can travel here and there, as they pleased, flying in the sky, traveling in the sea, even in the earth. What wonderful dreams!

In our long history, our ancestors have always been struggling hard to make their dreams come true. After the Wright Brothers made their first powered flights in 1903, the aviation industry has been developing in a surprising way. In December 2016, Boom Technology reported a new supersonic aircraft named XB-1 with a breakthrough aerodynamic design using state-of-the-art engine technology and advanced composite materials, which enables an ultrafast airliner to be as efficient and affordable as business class in today's subsonic wide-body airliners. The flight from New York to Beijing would be no longer than five hours by the XB-1. The first steam locomotive was invented at the end of the eighteenth century with the longest travel of several hundred miles. Today, in China, a proposed high-speed train line would operate at a speed of 350 km/h from Inner Mongolia's Baotou to Haikou in Hainan and the journey is about 3000 km. Moreover, we have deep submarines to explore the floor of the ocean and spacecraft to reach the stars and the moon. In addition, we can't imagine what our life would be without cars, which are the most popular transportation today.

Up to now, we really have the quickest transportation systems which our ancestors didn't dare to imagine. Yet, it is never enough. In addition to the faster speed and bigger scale, trustworthiness and security are always the most important issues to be taken into account for transportation systems.

In the past decade, with the rapid development of information and communication technologies (ICT), the transportation system has gone through the process from traditional transportation systems to intelligent transportation systems, which integrate cyberspace, physical space, and human society into a converged system. Such a transportation system can enhance traffic efficiency, avoid accidents, ensure road safety, and improve driving and passenger experiences using new ICT in a green way.

1.1 Cyber-Physical Systems

A cyber-physical system (CPS) is a novel complex embedded system integrating sensing, computing, communication, networking, and control. The computing and physical processing in an open environment realize continuous interaction and deep fusion for open embedded computing, real-time communication, remote control, and so on. As a complex system integrating cyber space and the physical space, CPS uses embedded sensing devices to acquire data and information, transfer data via the connected network systems, store and process the data and information with

intelligent transportation systems (ITS) in cyberspace, and make decisions according to the results of information processing. Therefore, CPS could realize the deep fusion and seamless interaction between cyberspace and physical space.

CPS is a controllable, credible, and extensible networked physical system that integrates the computing, communication, and control capabilities on the basis of environmental perception. It implements deep integration and real-time interaction between the physical world and the cyber world through the real-time feedback loop of computing process and physical sensing. The communication network subsystem includes the sensor network, the ubiquitous communication network and so on, which are used to complete the functions of data acquisition, transmission, and communication in CPS. The computing subsystem completes the storage, analysis, and processing of various data. The control subsystem determines the control strategy for the physical world and coordination of the various actuators of the physical world object operation.

CPS has brought a more comprehensive and in-depth demand for global information technology, which is a new stage of information technology. Globally, CPS is gradually becoming a hot spot in the past decade. In February 2006, the US Academy of Sciences made clear the CPS as an important research direction. In 2007, the President's Council of Advisors on Science and Tech (PCAST) made CPS the first proposal in the field of networking and information technology [1]. The US CPS Steering Group, established in 2008, puts CPS applications in the areas of transportation, defense, energy, health care, agriculture, and large-scale construction facilities. In addition, the US National Science Foundation (NSF) and EU 7th Framework Program (FP7) heavily supported many CPS projects [2].

1.2 Transportation Cyber-Physical Systems

The transportation CPS is the application of CPS in the transportation sector. Commonly, it generally involves perceptual layer, communication layer, computing layer, control layer, and service layer in hierarchy (see Fig. 1).

Perceptual Layer

In perceptual layer, there are thousands or millions of sensor nodes and sink nodes to sense some physical attributes of the physical world in which users are interested. They mainly include the information perception of traffic elements such as traffic carrier, traffic participant, traffic infrastructure, traffic speed, traffic density, license plate number, driving time, and travel distance in the road network. The originally sensed data are transmitted to the information center after the fusion nodes are merged. The perception of traffic information is the foundation of transportation CPS.

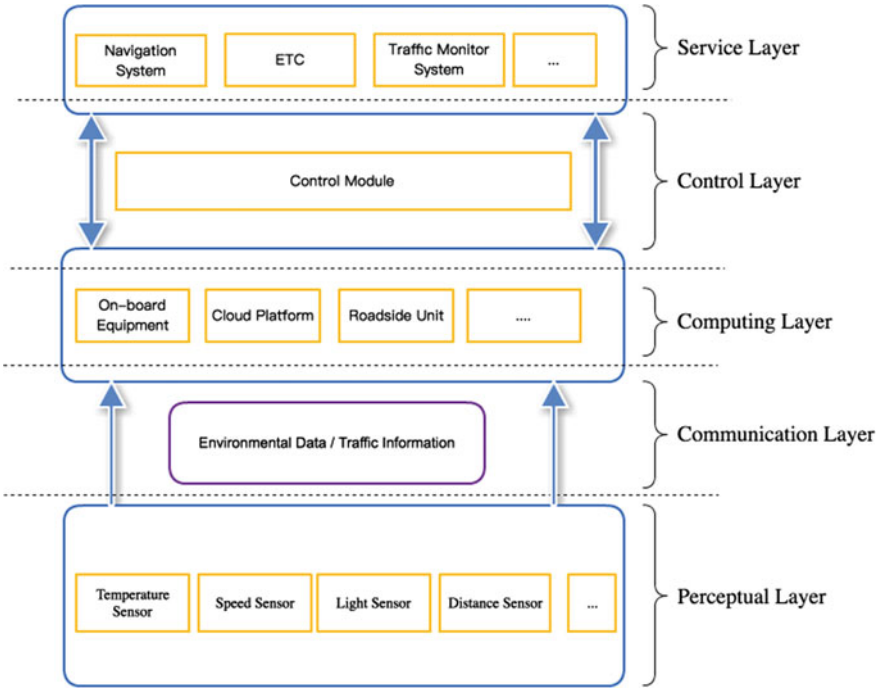

Fig. 1 Function layers of transportation cyber-physical systems

Communication Layer

The communication layer is composed of several communication base stations and network nodes. It is responsible for transmitting the original data perceived by the sensing layer to the information center while ensuring reliable communication between the vehicle, the roadside unit, and the roadside unit and the server. Available communication technologies include cable broadband, dedicated short-range communication technology (DSRC), 3G/4G, Wi-Fi, and so on [3]. In the actual transportation system, the occurrence of any traffic event is separated in time and space. Indeed, traditional sequential execution method cannot meet the requirement of transportation CPS. Therefore, a key problem of the communication layer is how to guarantee the high reliability of the information and effective transmission.

Computing Layer

Because of the volume of traffic data generated in transportation CPS, and the multiple interaction and feedback between the physical system and the cyber system, the requirements for analysis and simulation are very high, which poses a significant challenge to the computing capacity and storage capacity of the transportation CPS. Therefore, it is essential for the computing layer to have a transportation CPS platform with powerful computing power. These requirements cannot be satisfied

with the traditional centralized computing platforms. At the same time, cloud computing platforms with grid computing, distributed computing, parallel computing, utility computing, network storage, virtualization, and load balancing would be the primary option for the transportation CPS computing platform. It can help to obtain a strong computing and storage capacity by integrating a large number of distributed computing resources.

Control Layer

The control layer is used to enhance the ability to control the physical transportation system. The existing physical transportation system is relatively simple and always with fixed control mode and lack of flexibility, thus it is difficult to achieve systemwide optimal control. The distributed architecture of cloud computing is in accordance with the request of transportation CPS to realize the combination of centralized control and decentralized control. How to ensure the robustness and stability of transportation CPS is the key to effective control.

Service Layer

In the service layer, users have access to traffic objects, transport, transportation infrastructure, traffic information, and other types of states. The use of rich information for the user terminal to provide real-time traffic information service is the inevitable direction of the development of urban transport services. Some traditional and typical traffic services, such as ETC (Electronic Toll Collection), traffic guidance, and urban bus scheduling, can be improved due to the transportation CPS and the application of the control layer [4]. The difficulty lies in how to handle the uncertainty of traffic information, transmission, and so on effectively, in order to improve the accuracy and timeliness of traffic information.

2 Current Development of Transportation CPS

Transportation CPS can be classified into several types according to the transportation tools. In the last decades, there have been great developments in highway, railway, and aviation CPS.

2.1 Highway CPS

2.1.1 Development Status

The typical practice of highway CPS is the Internet of vehicles (IoV) which is a typical application of the Internet of things (IoT). It is a key point of intelligent life in the time of the mobile Internet. IoV provides a platform to exchange information

for people, vehicles, and roads. Security ensuring and privacy protecting are primary issues for such an information platform.

Highway CPS is a huge interactive system composed of various kinds of units. By GPS, RFID, sensors, camera image processing, and other devices, vehicles can complete the collection of their own environment and state information; through Internet technology, all vehicles can make their information transmission converge to the central processor; with data analytic technology, various data from a large number of vehicles can be analyzed and processed to derive the best routes plans for different vehicles, to report road conditions in a timely manner, and to schedule signal cycles.

In the last decades, highway CPS has occupied a great deal of market share. According to GSMA, global highway CPS market size was about 20 billion euros in 2014. By 2018, it will reach 39 billion euros. Japan's highway CPS market is dominated by Toyota G-Book and Honda Internavi, and the US highway CPS market is dominated by GM OnStar, the world's leading supplier of highway CPS products, including OnStar, Toyota G-Book, and BMW Internet Drives [5]. The highway CPS platform is characterized by cross-industry, involving chip equipment manufacturers, automobile manufacturers, traffic control departments, network operators, third-party service providers, and other industrial chains related to the main body. In the industry, there are four developed business models led by different participants including automobile manufacturers, telecom operators, third-party, and government and industry authorities. In the highway CPS application market, applications are dominated by vehicle manufacturers. Operators and third-party-led applications starting relatively late actively seize the market based on user needs; government and industry-led applications to enhance traffic safety and traffic efficiency as the starting point, are responsible for the establishment of nationwide traffic navigation services, which are also gradually occupying a small market.

2.1.2 Key Issues

There are a number of novel key issues for highway CPS for the purposes of meeting people's ever-increasing needs.

Intelligent Driving

Most existing intelligent driving technologies by advanced vehicle makers are still in the early stages of driver assistance or semi-automated driving, although automated cars by Google and Tesla have traveled several 1000 miles for testing in the last two years. Tesla's accident in 2016, in which the driver died in the first fatal crash while using autopilot mode, tells us that safety is the key to intelligent driving, and the technologies are yet on the way.

Emergency Rescue

Many sensors and devices can be set up in a vehicle to collect various data. When a traffic accident occurs, the emergency system will work immediately to notify the

roadside system and the cloud platform through the CPS. The rescue would be triggered in the most efficient way. Meanwhile, the accident information can be circulated to neighboring vehicles for the purpose of avoiding risk and traffic diversions.

Intelligent Traffic Management

Intelligent traffic management and control systems aim to alleviate adverse traffic conditions while ensuring mobility and accessibility. Many existing traffic management systems meet the technical capabilities only when the hardware components are of a specific brand. Some evolving traffic management technologies are necessary to meet present and future traffic needs, which would combine the knowledge and requirements in an efficient way by the transportation CPS.

In-Car Entertainment

An in-car system can help realize the cross-linking of mobile Internet and mobile devices. Drivers could have more convenient and comfortable experiences from in-car tablets and devices with various entertainment apps or friendly car-control services, such as the Audi MMI system, the Ford Applink, and the BMW iDrive [6].

2.1.3 Technologies

Highway CPS involves various kinds of information technologies, such as sensing technology, RFID technology, pervasive computing, and cloud computing. Intelligent sensor technology research involves AI, intelligent control, signal processing and identification, information fusion, and so on. Sensing technology is the key to realizing highway CPS comprehensive data acquisition. Communication technologies applied in highway CPS involve in-car communication, outside vehicle communication, vehicle–road communication, vehicle–vehicle communication, and so on. In detail, in-car communication technologies include CAN, LIN, MOST, FlexRAY, and Bluetooth, and all these feature short-distance and real-time high reliability [7]. The commonly used external technologies range from Boao to the expanded GSM, GPRS, 3G, GPS, and so on. Vehicle–road communication technologies are generally characterized with shorter distance and high mobility and commonly include microwave, infrared technology, and special short-range communications. The challenges for vehicle–vehicle communication mainly regard security and promptness. Microwave, infrared technology, and special short-range communications can be used in such a situation.

Furthermore, many applications of automotive positioning, communications, and charging are implemented in highway CPS by adopting DSRC (dedicated short-range communication) and VPS (vehicle positioning system) technology [8]. DSRC is an efficient wireless communication technology that can realize the

recognition and bidirectional communication of moving targets at high speed in a certain small area. At present, it is mainly used in electronic road pricing. VPS is a GPS + GSM technology, which can help to realize vehicle positioning, driving route query playback, and remote oil system. Furthermore in the field of car navigation, it helps voice communications and has other, wider applications. GPS has been mainly used in vehicle navigation, vehicle theft, emergency rescue, and other car security services.

2.2 Railway CPS

The railway CPS has evolved for several decades. In the early 1980s North America introduced an advanced train control system (ATCS) that attracted the attention of the developed countries. Some countries in Asia and Europe have successively developed similar train control systems, for example, ARES system in North America, ETCS system in Europe [9], ASTREE system in France, FZB system in Germany, and CARAT system in Japan. Around the 1990s, these train control systems were gradually implemented and applied in various countries, showing a strong vitality and great advantages.

Since 2000, the train control system has been a leap-style development. PTC (positive train control) was introduced in the United States. It aims to ensure the safe, reliable, and accurate operation of the train. It includes subsystems such as traffic command, train system, data exchange, and train information. The PTC system can effectively reduce the probability of train collision, accidental death of railway staff, railway and train equipment damage, and speeding accidents.

In the European Union, there are more than 20 railway control systems, each of which is independent and incompatible. They increase the total cost of cross-regional railway control systems for the safe travel of trains between European countries [10]. ERTMS/ETCS is a unified European train control system designed to replace the existing poorly compatible train control systems in European countries and to enhance the competitiveness of international passenger and freight transport. Since 2002, China has also started to revise the CTCS, China train control system, and relevant technical standards and promulgated a series of related technical documents. CTCS is a train operation control system that can meet the needs of different transportation to guarantee the safety of train operation, with the form of grading and different track lines. However, the PTC system in the United States, ERTMS/ETCS in Europe, and CTCS in China, are essentially CBTC (communication-based train control), which is a newly developed train control system [11]. It breaks through the boundaries of fixed occlusion, completely out of the traditional track circuit. It provides more accurate and reliable train control technology, such as speed protection and continuous train safety separation,

enabling the trains to operate in a shorter train operation interval with safe and reliable operation.

2.3 Aviation CPS

Similar to highway and railway, the aviation system is also a typical large-scale complex system. The wide range of aviation CPS can include different aircraft, airports, satellites, and the like. Especially, from a small view, the plane-airborne CPS comprises aircraft engine, landing gear, fuel tank, hydraulic, environmental control, power supply systems, and signal transmission. The airborne plane can be viewed as an embedded computer system which is a complex system of real-time and security. The airborne computer can be divided into two categories: one for the aircraft flight service, such as flight control and electromechanical devices; the other to complete the aircraft flight mission service, such as task management, digital map, communication, and navigation. These systems are interconnected through the real-time avionics network.

The key technologies for aviation CPS include the following aspects, which are different from other CPS.

- The distributed technology is implemented to separate platforms and applications in an airborne CPS system. Platforms are more closely integrated with aircraft physics, whereas applications are always functionally related. Distributed technology is built on platform hardware and primary software. It provides the management mechanism for available resources, fault-tolerant reconfiguration, time, security, and communication for application. Meanwhile, distributed technology enables CPS with the advantages of centralized computing resources for the purpose of enhancing capabilities and performance.
- Data-oriented communication middleware in aviation CPS help to realize the separation of computing resources and IO resources. Various kinds of sensors and actuators don't depend on remote computers and units. Data-oriented communication is utilized to simplify system communication and to enhance communication efficiency for the aviation CSP by avoiding the connection-oriented communication that would lead to a very complex system and degrade the system's scalability.
- Also, the aviation CPS involves many trustworthy configurable remote components. Herein, remote components can be remote interface units, remote electronic units, remote power controllers, or a combination of their functions. The high-confidence methods of the remote unit include cross-communication and closed-loop monitoring. The configurability of remote components addresses the standardization of remote components and reduces the lifecycle cost of components.

3 Threats and Attacks in Transportation CPS

Compared with other cyber-physical systems such as smart cities, the vehicle nodes in transportation CPS are always moving here and there; the network is dramatically changing constantly. There are several characteristics for such a real-time changing transportation CPS.

Dynamic Topological Structures

With high mobility and a short connection cycle, the topological structures of TCPS are intrinsically dynamic and thus difficult to predict and model. Compared with other networks such as smart home devices, vehicles are highly mobile, which leads to the frequent changes of vehicles in the network. Because a vehicle may have different drivers, V2H will change. The neighbors of vehicles on the road will change frequently, thus the V2V will also change, and a vehicle will run on different roads, and again the V2R will also change. The different actions of drivers will lead to the changes of sensors, thus the V2S will change as well. Therefore the network will change frequently according to the changes of vehicles, drivers, roads, and sensors.

Large-Scale Network

A transportation network may consist of millions of vehicles equipped with wireless communication capabilities which are decided by the scale of a city. The network should be scalable according to the entering or leaving of vehicles. With the advance of vehicle manufacturing and the construction of roads, more vehicles are running on the roads. The scale is drastically changing, especially regarding the time when people go to work in the morning or go home in the afternoon.

Nonuniform Distribution of Nodes

The distribution of vehicles is affected by many factors including the road network topological structure, geographical location, and driver's driving habits among others. The connectivity of the network can be totally different, for example, in the downtown of a metropolis and a rural area in a developing country. Thus the structure of the subnetwork keeps on changing continuously, although vehicles are in the whole network. A vehicle may enter different subnetworks according to the changes of its locations.

Different Granularities

Vehicles on the same road, in the same district, city, province, or country formulate different networks with different granularities. Transportation CPS with smaller granularities will formulate with larger granularities.

Mobile Limitation

Vehicles are connected via a wireless communication network. Therefore the transportation CPS is heavily limited by the wireless communication network

signals. If the distance is too great, the wireless network would not work, the signals would be weak, and the CPS would be difficult to be formulated. Because nodes in the network are expected to move on the road with a determined track to some extent, their predictability is better than those of free running, which is a benefit.

Unlike CPS in other fields, traffic disasters caused by erroneous information from transportation CPS directly cause the loss of people's lives. Hence, threats and security issues, as well as privacy in the transportation CPS are always more serious than those in other fields. Once an intrusion happens in the CPS, the vehicles could be controlled by hackers with ulterior motives, and would lead to traffic accidents. At the same time, driving records are the privacy of people. People may not want to let others know where and when they have been. However, the CPS could capture and monitor the driving track of the vehicles, which can reveal that privacy. What's more, as vehicles access the cloud more and more, security and trust are facing more challenges (see Table 1).

In information security, attacks and threats are classified into six main categories in the STRIDE Threat Model [12], including spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. Specially, an IoV system may be attacked from various aspects by different methods including jamming, interference, and eavesdropping, which decrease the stability, robustness, real-time, security, and privacy of the IoV and make it lose the ability to provide effective services, even cause serious accidents due to its characteristics of dynamic topology, bandwidth limitations, transmission power limitations, abundant resources, mobile limitation, nonuniform distribution of nodes, and perception of data depending on the vehicle trajectory and large-scale network.

3.1 Threats to Highway CPS

Security issues have become increasingly important with the development of the transportation CPS. Threats to highway CPS include inadequate authentication, eavesdropping in data transmission, information disclosure, and the like, caused by the attacks discussed above.

Inadequate authentication results in the easy manipulation of highway CPS through the remote control service. Remote control is a convenient function provided by the car manufacturers, including starting the engine, turning on air-conditioning, and braking cars. However, this function carries a potential risk. In July 2015, two US hackers broke through the network Jeep Free Light U Connect Highway CPS system by invading the integrated entertainment system chip using the vulnerability of the wireless communication module that provides remote control services of the car. They could easily achieve vehicle deceleration, shut down the engine, and even render the car's brakes failing. The event forced the Fiat–Chrysler Group to recall about 1.4 million vehicles. During the design stage, the security issues had not been addressed, which led to an inadequate

Table 1 Threats and attack type

Threats and attack type	Description	Examples
Attacks on authentication	This type attacks target and attempt to exploit the authentication process of the transportation CPS to verify the identity of a user, service, or application.	Sybil attack, GPS deception, Masquerading attack, Wormhole attack
Availability attacks	Attacks such as denial of service and channel interference are common types of attacks on availability. This type of attack mainly utilizes the limitations of bandwidth and transmission power to make the IoV system collapse. Most major significant components of IoV are exposed outside and have deficient protection; as a result they are easy to be interfered with, controlled, and totally destroyed. The influence of an availability attack depends on which type of nodes are attacked: damage to a core unit will have larger impacts on an IoV system than a destroyed vehicle	
Secrecy attacks	The data and resources are always the most important parts of a system, and secrecy is needed to guarantee that these sensitive data can only be accessed by rightful nodes that are authorized correctly. The secrecy attacks steal data by eavesdropping or interception. In most cases, an attacker compromises a normal entity such as a vehicle or a RSU. This gives the attacker the ability to access the secret resources through eavesdropping on this entity, causing the leakage of the users' privacy	
Routing attacks	Routing algorithm and its quality imply the effect of IoV communications among RSUs, vehicles, and other TPMs, and the routing mechanisms of IoV are always relatively complex due to the IoV's limitations of bandwidth, transmission power, and mobility. Subsequently, this complication brings about the loopholes and vulnerability of the IoV routing process	Eavesdropping, Denial of service, Masquerading, modification

(continued)

Table 1 (continued)

Threats and attack type	Description	Examples
Data authenticity attacks	The property of openness makes IoV dataflow easy to be captured, fabricated, and forwarded, especially in routing and wireless communication. Data authenticity attacks make the applications of IoV not credible and this destruction may have profound and lasting effects on IoV	Replay attack, Camouflage attack, Fabricating and tampering with messages, Illusion attack

authentication access to the CAN bus. The missing authentication to the CAN bus systems further led to the illegal manipulation by hackers.

The data transmission in highway CPS can easily be intercepted, eavesdropped on, or tampered with due to carelessness. In August 2015, some hackers announced that they broke through GM's OnStar highway CPS successfully [13]. By intercepting the communication of the OnStar Remote Link app and Anji Star, the attackers could take full control and behave as the legal user indefinitely. Many apps are provided for convenient services by the highway CPS. Not all providers could address the security issues in the development stage, which leads to control signals being easily intercepted or eavesdropped on. The intruders can even use the identity to send the wrong signaling to query or operate.

Disclosure of sensitive and personal information is generally caused by poor data management and storage. Location information and driving tracks are usually stored in the storage devices of the highway CPS. Users can access (registration or query) this information through Web services. Obviously, poor data management would lead to the disclosure of this personal information. There are many loopholes in existing highway CPS, such as the weak Cadillac password, the BMW database registration loopholes, and the Mercedes-Benz ultra vires, and so on. Some hackers can directly obtain the owner name, cell phone number, car models and other information by invading through these loopholes. In addition, highway CPS lacks the management policies for dataflow, which causes the risk of illegal cross-border movements.

3.2 Threats to Railway CPS

As with highway CPS, railway CPS also has to face various threats from different aspects. The main security threats faced by the railway CPS are listed as follows.

Physical Threat

Physical security is the prerequisite for the security of information systems. Railway CPS face physical threats, such as earthquake, floods, fires, and other environmental accidents caused by system failure, power failure caused by equipment failure resulting in the loss of database information, stolen equipment, destroyed data, loss or information leakage, and electromagnetic interference caused by data communication interruption.

Virus Threat

The spread of a virus through the network is the main form of computer virus transmission. As the railway CPS involves a wide range of network access points and requires more difficult network management, the consequences of a virus for railway CPS could be catastrophic. Any access point, such as the onboard Wi-Fi network, infected with a virus, is likely to spread it to the entire network. The virus could consume network resources, damage the running programs, steal sensitive data, and destroy the entire information system.

Malicious Attacks

Malicious attacks include two categories: attacks within the system and attacks from outside. According to one survey, about 70% of malicious attacks come from the internal network. Malicious attacks are mainly through the operating system or database vulnerabilities on the network. Examples are malicious tampering or theft of sensitive data, or even directly causing system paralysis.

4 Countermeasures

Most of the countermeasures to attacks for general computer networks can work for attacks in transportation CPS. However, the characteristics of the attacks in TCPS lead to special requirements for countermeasures. Much work has been done in this area in the last decades.

4.1 Threat Model

Modeling different attacks is important for understanding and analyzing their impacts on TCPS. Microsoft's STRIDE is a popular threat-modeling technique commonly used to find the security weakness of various systems. Graph-based approaches and mathematical modeling approaches are two main methods for describing modeling network attacks [14, 15].

Both static and dynamic graph-based techniques are well known for attack modeling. They provide graphics to describe the relationships between different

parts so that people who use them could conveniently make the model clear and easy to focus on the behavior of the attack in the network. Petri net modeling approaches [16], for example, have been used in modeling network attacks in large cyber-physical infrastructures, such as smart grids, as a more flexible method. Hierarchical methods for constructing large Petri nets from smaller size Petri nets have also been proposed for such a complex TCPS. Although graph-based approaches have many advantages for engineering applications in designing attack detection methods for improving security analysis and security design in large-scale TCPS, they are too complex to be used in industrial fields. Mathematical approaches for modeling the attacks in supervisory control and data acquisition have been used for IoV.

4.2 Intrusion Detection Systems (IDS)

Intrusion detection systems (IDS) are an important supplementary measure of network security. IDS provide protection against internal and external attacks by collecting and analyzing information from internal network systems to check if system behavior exists that violates security strategy or shows signs of attack. Signature-based detection and anomaly-based detection are the two main classes of detection methods.

Signature-Based Detection

This type of detection will build up a database to store various signatures of known attacks for retrieving and making comparisons. Signature-based detection identifies an attack by comparing the signatures in the database with the TCPS states. The IDS based on the signature will trigger the corresponding resistance measures when a network state matches an attack stored in the database. The detection results are always accurate for recorded attacks, however, when new, unknown attacks take place, this type of detection will have high false negative (FN) rates, which makes the detection lag behind indicators. In CPS, with the fast development of onboard applications, more sensors and more types of devices are integrated in vehicles, causing signature-based detection sometimes to be invalid.

Anomaly-Based Detection

Anomaly-based detection predefines the baseline of normal environment attributes in a system, and it can detect new types of attacks through the observed data that show abnormal information beyond the baseline. This detection method has high false positive (FP) rates, is costly, and it is hard to find proper metrics to determine the baseline. More accurate data analysis algorithms are needed for current and future use.

4.3 Honeypot

Spitzner [17] defined a honeypot as a security resource whose value lies in being probed, attacked, or compromised. Honeypots complement most other security mechanisms by running as normal system computing resources to tempt attackers. Honeypots aim at diverting attackers' attention away from the vital system resources and analyzing the behavior of attackers to create signatures for intrusion detection systems so the real targets, the important system services and data, can be protected by the attraction of attackers, and this is why IDS need honeypots. In CPS, the authorization module and communication module are the components that are attacked more often, and these related parts have components with the role of honeypot to absorb damage and record the attack data. Because they consume system resources, these functions should be switched off in some relatively safe situations.

4.4 Secure Routing Protocols

In order to resist attacks such as eavesdropping, denial of service, counterfeiting, route modification, black hole, and the like effectively, a series of security routing protocols are presented based on traditional routing protocols. These security routing protocols can achieve normal routing functions and can effectively resist common routing attacks at the same time. There are three most common security routing protocols: SAODV [18], Ariadne [19], and SRP [20].

4.5 Routing Privacy Protection Mechanism

To ensure that the routine nodes' data won't be leaked during the routing process, a routing privacy protection mechanism is necessary for IoVs. Hiding the value of each utility using the idea of "The Millionaire's Problem" [21] can be a feasible method that is designed to compare two objects without leaking their actual values. SLPD [22], ALAR [23], and STAP [24] are three algorithms to protect the location privacy of mobile nodes in DTNs. SLPD makes a node's location information circumvent the social friends of this node to prevent service providers from obtaining the location data of the node. ALAR divides the source packet into different parts, uses different keys to encrypt them, and forwards them separately. After these treatments, it is almost impossible for the attackers to figure out the private information of the nodes from the packets. STAP uses the idea of the cache and caches packets for a node on locations where it appears frequently. Then, other nodes that meet with it do not need to know the node's location to send their packets to it.

4.6 Key Management

Encryption is the fundamental means to ensure information security. Encryption technology can meet the requirements of authentication, message confidentiality, data integrity of vehicular ad hoc networks, and nonrepudiation. Effective encryption requires appropriate key management.

The goal of key management is to ensure the security of the key, that is, authenticity and validity. Key management includes key generation, distribution, transmission, preservation, destruction, and backup. In traditional networks, the distribution and management of keys are generally completed by the key distribution center (KDC) or certificate authentication center (CA).

5 Challenges to Transportation CPS Security

This section discusses the future trends of the security and privacy issues in transportation CPS. There are several different trends to be addressed for more efforts in future.

- *Intrusion Detection System.* There are many differences between transportation CPS and other networks. In traditional networks, intrusion detection technologies can rarely be applied to transportation CPS due to the unavailability of fixed basic network architecture. Network-based intrusion detection systems in wired networks rely on real-time traffic analysis. Traffic monitoring is usually implemented on the switches, routers, and gateway nodes. However, there are no centralized flow monitoring points available to collect the entire network data in transportation CPS. It is difficult to identify the true invasion and temporary system failure for intrusion detection systems.
- *Trust and verification of the data center.* The data center provides the security of data communication through the trust and audit of the data. The trust and verification of the data center protect the vehicles in the transportation CPS from network threats and attacks, but the standard is not unified and this disunity hinders the further integration of transportation CPS. The social network in transportation CPS is an important aspect in view of trust management [25, 26]. How to verify trust-based recommendation in social network is also a challenge [27].
- *Cross-layer transmission.* The connections between nodes in transportation CPS may end abruptly for some nodes due to the mobile and dynamic characteristics. It is very difficult to obtain stable traffic safety. Designing a cross-layer transmission protocol is really important for transportation CPS to ensure real-time and multimedia applications.
- *Privacy protection.* Mobile cloud computing would be an important technology for transportation CPS due to its dynamic and mobile architecture. How to protect the data of mobile cloud participants and how to meet the user's

requirements for information protection are two primary goals for mobile cloud computing. Some mobile nodes often become temporarily disconnected, and the data can be delegated to mobile cloud computing. Attackers could penetrate the devices to access data illegally from mobile cloud computing. However, protection mechanisms always mean negative impact on functions; for example, how to determine the right lifetime of a certificate can be difficult, fixed lifetime, location-dependent, or speed-dependent can have various effects in different situations. In addition, privacy protection in routing is another serious problem. In the package routing processing of transportation CPS, meeting frequency, social closeness, and network centrality and other social attributes of routing nodes play important roles in routing. Correct and efficient routing needs the genuine utility information to be revealed and shared between the two nodes and most of the routing algorithms cannot be executed properly if such data are concealed from the two nodes. Here comes the paradox: how to protect the private routing information, that is, a node's routing utilities and selected reasonable forwarders at the same time in transportation CPS routing while guaranteeing the correct routing operations are big challenges to be adequately addressed.

- *Big data oriented threats and countermeasures.* With the rapid development of data technologies, more and more opportunities and challenges are emerging on the big data issues. There is no doubt that we can benefit much more than ever from big data in transportation CPS. However, the risk is also increasing. Transportation CPS faces the challenge of handling large quantities of data generated by millions of vehicles to maintain the security and privacy of customer information. Novel data models and analytic methods are really necessary to be developed to manage and utilize the big data for security purposes in transportation CPS. How to model and extract useful knowledge from big data is a big challenge for transportation CPS [28].

6 Summary

Security and privacy issues in transportation CPS applications have always been in the spotlight though each aspect of transportation CPS technology has made great progress in the past decade. Security and privacy still have to face technical challenges in transportation CPS. There is a long list of unresolved problems in this area. Inevitably, issues of security and privacy will determine the promotion and implementation of transportation CPS, which are also the crucial premise and foundation for the practices of transportation CPS. All the transportation CPS participants including vehicle users, vehicle manufacturers, insurance companies, government, and anyone relevant play important roles in the implementation of transportation CPS.

In this chapter, we give a brief introduction to transportation CPS, describe the characteristics and development of three transportation CPS systems, which show the differences between transportation CPS and other CPSs. In addition, we summarize the typical attacks on transportation CPS systems, and also discuss the issues of security and current countermeasures in transportation CPS. Furthermore, we also discuss the challenges for the security of transportation CPS.

Acknowledgements This research is sponsored by the National Natural Science Foundation of China (No. 61371185) and China Postdoctoral Science Foundation (No. 2015M571231).

References

1. Antsaklis, P. J., et al. (2012). Cyber-physical systems design using dissipativity. *Control conference (CCC), 31, 2012*. Chinese, IEEE.
2. Ma, H.-D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer science and Technology, 26*(6), 919–924.
3. Rawat, D. B., Bajracharya, C., & Yan, G. (2015). Towards intelligent transportation cyber-physical systems: Real-time computing and communications perspectives. *SoutheastCon 2015*. IEEE.
4. Crowcroft, J., & Oechslin, P. (1998). Differentiated end-to-end internet services using a weighted proportional fair sharing TCP. *ACM SIGCOMM Computer Communication Review, 28*(3), 53–69.
5. Lu, Y., et al. (2013). On the application development of 3G technology in automobiles. In *Proceedings of the FISITA 2012 world automotive congress*. Berlin Heidelberg: Springer.
6. Becker, T., et al. (2006). Natural and intuitive multimodal dialogue for in-car applications: The SAMMIE system. *Frontiers in Artificial Intelligence and Applications, 141*, 612.
7. Zheng, B., et al. (2015). Design and verification for transportation system security. In *Proceedings of the 52nd annual design automation conference.* ACM.
8. Qureshi, K. N., & Abdullah, A. H. (2013). A survey on intelligent transportation systems. *Middle-East Journal of Scientific Research, 15*(5), 629–642.
9. Schoitsch, E., & Skavhaug, A. (2014). Introduction: ERCIM/EWICS/ARTEMIS workshop on dependable embedded and cyberphysical systems and systems-of-systems (DECSoS' 14) at SAFECOMP 2014. *International conference on computer safety, reliability, and security*. Springer International Publishing.
10. Platzer, A. (2009). Verification of cyberphysical transportation systems. *IEEE Intelligent Systems, 24*(4), 10–13.
11. Bu, L., et al. (2012). Demo abstract: Bachol-modeling and verification of cyber-physical systems online. In *Proceedings of the 2012 IEEE/ACM third international conference on cyber-physical systems*. IEEE Computer Society.
12. Yampolskiy, M., et al. (2012). Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In *5th international symposium on resilient control systems (ISRCS), 2012*. IEEE.
13. Brenwald, J. (2011). Vehicle data acquisition. *Group 14*, 11–7.
14. Cohen, F. (1999). Simulating cyber attacks, defences, and consequences. *Computers and Security, 18*(6), 479–518.
15. Cheung, S., Lindqvist, U., & Fong, M. W. (2003). Modeling multistep cyber attacks for scenario recognition. *DARPA information survivability conference and exposition, 2003. Proceedings* (Vol. 1). IEEE.

16. Chen, T. M., Sanchez-Aarnoutse, J. C., & Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid 2.4*, 741–749.
17. Spitzner, L. (2003). *Honeypots: tracking hackers* (Vol. 1). Reading: Addison-Wesley.
18. Lu, S., et al. (2009). SAODV: a MANET routing protocol that can withstand black hole attack. *International conference on computational intelligence and security, 2009. CIS' 09* (Vol. 2). IEEE.
19. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks, 11*(1-2), 21–38.
20. Wu, T. D. (1998). The secure remote password protocol. *NDSS* (Vol. 98).
21. Yao, C. C. (1982). Protocols for secure computations (extended abstract), Pcr—O(1/n) = O (1) points from P Pcr in Si, since Pr[p Si] = (n 1/c) is, 160–164.
22. Zhang, X., Wang, X., Liu, A., Zhang, Q., & Tang, C. (2012). Pri: A practical reputation-based incentive scheme for delay tolerant networks. *Ksii Transactions on Internet and Information Systems, 6*(4), 973–988.
23. Lu, X., Hui, P., Towsley, D., Pu, J., & Xiong, Z. (2010). Anti-localization anonymous routing for delay tolerant network. *Computer Networks the International Journal of Computer and Telecommunications Networking, 54*(11), 1899–1910.
24. Lin, X., Lu, R., Liang, X., & Shen, X. (2011). Stap: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets. *Proceedings IEEE INFOCOM, 28*(6), 2147–2155.
25. He, Z., Cai, Z., & Wang, X. (2015). Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks. *The 35th IEEE international conference on distributed computing systems* (pp. 205–214).
26. Wang, Y., Cai, Z., Yin, G., Gao, Y., & Pan, Q. (2016). A game theory-based trust measurement model for social networks. *Computational Social Networks*.
27. Wang, Y., Yin, G., Cai, Z., Dong, Y., & Dong, H. (2015). A trust-based probabilistic recommendation model for social networks. *Journal of Network and Computer Applications, 55*, 59–67.
28. Sun, Y., & Jara, A. J. (2014). An extensible and active semantic model of information organizing for the internet of things. *Personal and Ubiquitous Computing, 18*(8), 1821–1833.
29. Lee, E. A. (2010). CPS foundations. In *Proceedings of the 47th design automation conference.* ACM.

Smart Transportation Systems: Architecture, Enabling Technologies, and Open Issues

Hansong Xu, Jie Lin and Wei Yu

Abstract With the development of smart sensors, smart vehicles, and vehicular communication technologies, the smart transportation system is proposed and considered to be the future of the transportation critical infrastructure system, aiming to improve traffic efficiency, safety, and security. All vehicles and roadside infrastructures will be deployed with integrated smart sensors and communication units in order that traffic states can be measured and shared via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication networks. With the smart transportation system, diversified services can be provided to customers, including traffic and transportation management, safety management, and others. In addition, the optimal travel for users (e.g., drivers) can be achieved, travel safety can be realized, and road congestion can be reduced in the smart transportation system. Nonetheless, security issues, including illegal access, attacks, unauthorized information sharing, and so on, become challenging in the smart transportation system. In order to understand smart transportation systems such that techniques can be designed to make them secure, this chapter conducts a review of smart transportation systems with respect to architecture, enabling technologies, and open issues. To be specific, a three-layer architecture is first presented for the smart transportation system, including the physical layer, communication layer, and service layer. Then, the detailed components and enabling technologies in each layer are described. Finally, we present some open issues related to security, big data, performance, and evaluation platforms in the smart transportation system.

H. Xu · W. Yu (✉)
Towson University, Towson, MD, USA
e-mail: wyu@towson.edu

H. Xu
e-mail: hxu2@students.towson.edu

J. Lin
Xi'an Jiaotong University, Xi'an, Shaanxi, People's Republic of China
e-mail: Jielin@mail.xjtu.edu.cn

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_2

1 Introduction

The smart transportation system, also known as the intelligent transportation system (ITS) or transportation-based cyber-physical system (CPS), has been rapidly developing with the advancement of smart sensors, smart vehicles, vehicular communication, and the like [8, 102, 103]. As the future transportation infrastructure system, the smart transportation system is capable of connecting smart vehicles and roadside units via vehicle-to-vehicle (V2V) communications and vehicle-to-infrastructure (V2I) communications, integrating information, computation, communication, and control technologies to enable the sharing of real-time traffic data and road information to users (drivers, etc.), and providing efficient and reliable services to improve traffic efficiency and safety in the transportation system [18, 20, 77]. Unlike the traditional transportation system, users (travelers, etc.) in the smart transportation system technology play an active role, and participate in the management and operations of the transportation system. Objectives of resources are to provide services to users, different from the conventional focus on system operations [8]. With the support of the smart transportation system, users can be provided with real-time and accurate traffic information, along with the corresponding services to mitigate road congestion and improve traffic safety [63]. In addition, the smart transportation system can efficiently improve the use of traffic resources and reduce environmental pollution [44]. Thus, growing attention has been devoted to the development of smart transportation systems in many different countries [8].

The basic concept of the smart transportation system was initially introduced by the United States [8]. Subsequently, countries such as Japan and the European Union also began developing smart transportation systems [21]. To provide an efficient and safe smart transportation system, the US Department of Transportation (DoT) outlined the following key services that the smart transportation system should consider [94]: (i) travel and traffic management, (ii) public transportation management, (iii) electronic payment, (iv) commercial vehicle operations, (v) emergency management, (vi) advanced vehicle safety systems, (vii) information management, and (viii) maintenance and construction management. With all of these services, users can gain benefits during travel, including the improvement of travel safety, the reduction of travel time and gas use, and others.

To ensure that the aforementioned services can be efficiently and securely provided by the smart transportation system, related enabling technologies should be developed and challenges should be addressed. In recent years, various efforts have reviewed the smart transportation system from different aspects [8, 20, 44, 59, 66, 102, 103, 115]. For example, An et al. in [8] reviewed smart transportation projects in the United States, Japan, the European Union, and other countries, and compared the international research efforts on the smart transportation system. Yan et al. in [103] discussed the development of smart transportation systems in China. Zhu et al. in [102] investigated the basic functions of smart transportation systems and designed a system from the viewpoint of IoT (Internet-of-things) to make urban traffic intelligent and efficient. Zhang et al. in [115] considered the smart transportation

system as a powerful multifunctional data-driven system and presented a survey on the development of the data-driven smart transportation system. Elkosantini et al. in [20] presented a review to introduce the smart public transportation system and corresponding enabling technologies. In addition, some existing efforts were focused on reviewing the special technologies to support services that smart transportation can provide. For instance, Li et al. in [59] reviewed traffic coordination control technologies and discussed several key topics in this field. Liu et al. in [66] comprehensively reviewed video-processing technologies for vehicle detection and tracking. Khanjary et al. in [44] reviewed the existing route guidance schemes and categorized these schemes based on their structures and communication techniques.

In addition, some survey papers focused on security challenges for the smart transportation system [4, 22, 42, 50, 89, 119]. For example, Zhao et al. in [119] reviewed the risks of proposed security solutions in vehicular networks and found that existing solutions could not have practical usage and satisfy security requirements. ALkahtani et al. in [4] presented possible security attacks in vehicular ad hoc networks (VANET) and also discussed corresponding defensive schemes. Faezipour et al. in [22] reviewed the progress and challenges in the system that consists of smart vehicles. Although a number of survey papers have been executed, most existing efforts have only focused on specific aspects of the smart transportation system, and have reviewed the security attacks and challenges only limited to the security and privacy issues on VANET. This calls for a survey in which a full vision of the smart transportation system, including architecture, enabling technologies, security, big data, and performance and evaluation platforms, should be presented.

Distinct from existing efforts, this chapter reviews the recent efforts on the smart transportation system and provides an overview of the smart transportation system with respect to architecture, enabling technologies, and issues related to security, big data, performance, and platforms. First, a three-layer architecture is considered in the smart transportation system, including the physical layer, the communication layer, and the services layer (also known as the application layer). In the physical layer, the physical components, including smart sensors, smart vehicles, roadside units, and others, are considered. In the communication layer, the V2V and V2I communication networks are used to enable the sharing and delivery of real-time traffic information among the physical components. The service or application layer is used to provide services to users, including transportation and traffic management, safety management, and so on.

Second, enabling technologies in each layer of the three-layer architecture are presented. For example, one of the most important services for users, namely route guidance, is presented in detail. With the support of route guidance, users can obtain real-time and accurate traffic state information in time and alter or reschedule their routes to destinations during travel. By doing this, travel time can be reduced, road congestion can be avoided, and travel safety can be improved.

Third, some open issues are presented. Particularly, security issues with respect to information security are presented. Although major research efforts have been conducted in improving traffic efficiency and reliability of smart transportation systems by using information communication technologies, the risks of cyberspace breaches

in the system need to be seriously investigated before a massive deployment of smart transportation technologies can be realized. The impact of attacks on the smart transportation system is severe by nature, and can significantly affect the safety, as well as the efficiency, of the transportation system by hampering system performance (energy- or fuel-efficient driving, etc.), leading to traffic jams or even life-threatening road accidents. There have been growing security concerns in the smart transportation system. For example, in 2015, researchers demonstrated the feasibility of hacking a Jeep that was driving in traffic, taking over key functions (dashboard, steering, transmission, and brakes), the result of which led to Chrysler issuing a recall for 1.4 million vehicles [29]. Particularly, the adversary can manipulate traffic information and control commands shared among physical components and disrupt the effectiveness of services provided by the smart transportation system, placing on-road vehicles in unsafe situations. To defend against security challenges, potential countermeasures are discussed. In addition, the big data issues and performance in V2X, as well as evaluation platforms in the transportation system, are discussed.

The remainder of the chapter is organized as follows: we present the architecture of the smart transportation system in Sect. 2. We present the enabling technologies of the smart transportation system in the physical layer, the communication layer, and the service layer in Sects. 3, 4 and 5, respectively. We discuss some open issues on security, big data, and performance and evaluation platforms in Sect. 6. Finally, we conclude the chapter in Sect. 7.

2 Architecture

Generally speaking, the architecture of the smart transportation system can be divided into three basic layers, including the physical layer, the communication layer, and the services/application layer, as shown in Fig. 1.

- *Physical layer:* It is composed of physical components or physical subsystems used to support the smart transportation system, including smart sensors, smart vehicles, traffic lights, traffic signs, and others. Sensor units, control units, and communication units are integrated, in which sensor units are used to measure local traffic state information, control units are used to process the state information, and communication units are used to transmit the processed information into the upper layer (i.e., the communication layer).
- *Communication layer:* It is comprised of wired or wireless communication links to support efficient and secure information sharing among physical components and physical subsystems in the smart transportation system. Generally speaking, the communication structures in the communication layer can be divided into two basic categories: vehicle-to-vehicle communication and vehicle-to-infrastructure communication. Particularly, in V2V communication, all smart vehicles will communicate with each other and share real-time traffic information via communication units deployed in each smart vehicle. However, in V2I communication, smart

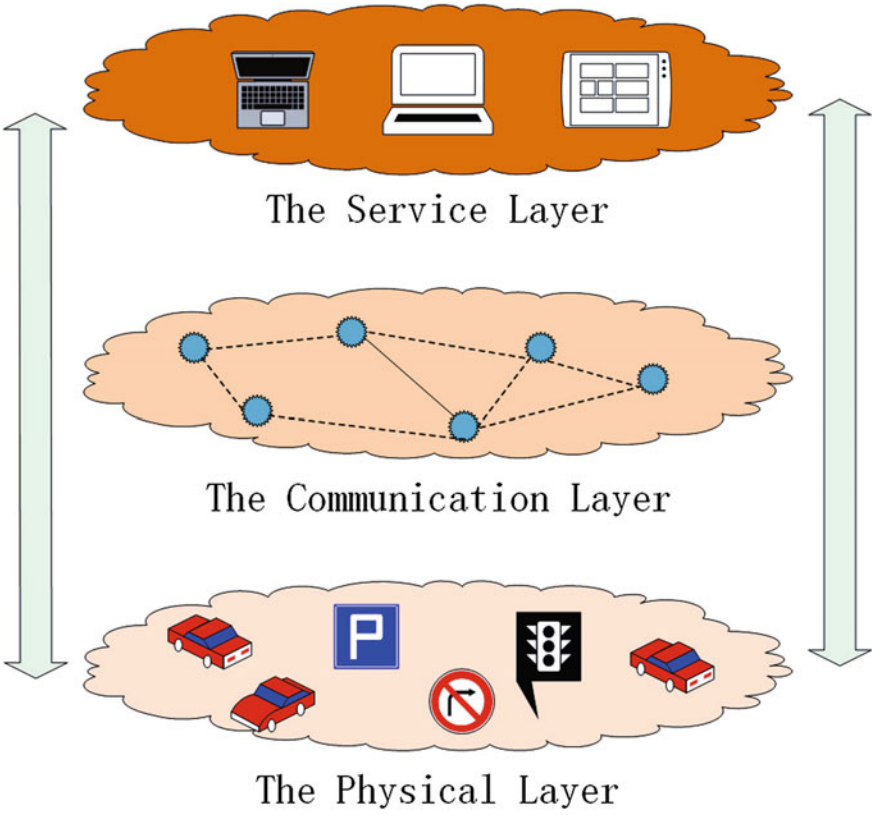

Fig. 1 Three-layer architecture for smart transportation

vehicles will not communicate with each other directly, but through the help of roadside units (RSU; access points, base station, etc.). In addition, in the communication layer, various physical components (routers, etc.) and various communication technologies (Bluetooth, WiFi, long-term evolution (LTE), etc.) are integrated to provide efficient and secure information transmission and delivery.

- *Service layer:* This is also known as the application layer, and is the top layer of the smart transportation system. The service layer receives the real-time traffic state information and requests from users via the communication layer and uses the collected data to provide the requested services or operations. For example, based on local real-time traffic state information, the service layer can provide the information to users who can reduce vehicle speed and keep a safe distance from the front vehicle to improve traffic safety, or determine a best travel route for users to avoid road congestion and reduce travel time.

Notice that the three-layer architecture is the basic architecture for the design of the smart transportation system. In each layer, various and distinct sublayers may

exist. For example, the communication layer can be divided into several sublayers, where the perception layer is used to perceive the state information of physical components, the network layer is used to transmit the information, and the interface layer is used to manage services. In the service or application layer, a service-oriented architecture (SoA) can be leveraged to enable the reuse of software and hardware components and improve the feasibility of the design and implementation of the smart transportation system.

3 Physical Layer

In the physical layer, the physical components and subsystems used to support the smart transportation system are included. Generally speaking, the physical components can be divided into three key categories: smart devices, smart vehicles, and roadside units, all of which are further described in this section.

3.1 Smart Devices

In the smart transportation system, a large number of smart devices should be deployed to measure the traffic state, detect nearby objects, and share the real-time information to assist vehicle control. The two typical smart devices used in the smart transportation system are sensors [68, 74] and RFID [118]. In the smart transportation system, a large number of sensors should be deployed in vehicles to measure vehicle traveling information, or in roadside units to measure the traffic state information. The deployed sensors can be organized as a sensor network via wireless communication links to share real-time information. With the support of wireless sensor networks, monitoring and tracking the status of devices and processing and sharing the status data among physical components can be realized.

Another important smart device used in the smart transportation system is RFID, which is a noncontact device and can be used to identify and track objects without contact. RFID can support the information exchange within a short distance [118]. RFID has been widely used in the transportation system to identify and track vehicles. For example, RFID is composed of several RFID tags and a RFID reader [49], where the information is stored in the RFID tags, and users can obtain the information via scanning the tags using the RFID readers. In addition, RFID can be divided into three categories based on the power supply mechanism, including active RFID, passive RFID, and semi-passive RFID [97]. In active RFID, tags have their own power supply, such as a battery. An example of active RFID used in the smart transportation system is the EZPASS card, which is used for highway toll charging. In passive RFID, tags do not have their own power supply, and they can only harvest power from signals transmitted by RFID readers. An example of passive RFID in the smart transportation system is the “Oyster” card, which is used in public bus fee

charging. In semi-passive RFID, although tags have their own power supply, they can only obtain the power from their own power supply when they receive signals transmitted from RFID readers.

Notice that both sensors and RFID are important devices in the smart transportation system. The main objective of sensors is to measure data relevant to the current state, whereas the main objective of RFID is to identify objects nearby. In addition to sensors and RFID, other smart devices, including GPS (global positioning system) used to carry out positioning, interface devices used to achieve the interactions between users and vehicles, and others, have been widely used in smart transportation to improve efficiency and safety.

3.2 Smart Vehicles

The smart vehicle can be considered an integrated system (or an intelligent robot) in which advanced technologies (communication, computation, sensing, information fusion, artificial intelligence, control, etc.) are integrated to achieve the functionality of environment perception, automatic decision-making, multiscale auxiliary driving, and the like. The main objective of smart vehicles is to improve vehicle safety and comfort, and to provide friendly interfaces between users and vehicles.

In the smart transportation system, the smart vehicle is an essential component and can use the deployed sensors to measure nearby traffic states and suggest a safe speed for users in travel. A GPS, sensors, and a large number of electronic control units (ECUs) will be integrated in smart vehicles. With the support of GPS, a smart vehicle can obtain the current position and determine the travel direction via comparing the current location and destination [102]. Sensors can be used to detect and track objects. ECUs are used to monitor and control subsystems in the vehicle and can be connected via an internal network to share information associated with the vehicle [89]. In addition, smart vehicles use the enabling wireless communication units, which are used to provide the V2V and V2I communications.

In the recent past, the development of smart vehicles has drawn growing attention from government, industry, and academia alike. For example, in the United States, four states and Washington, DC have passed laws that allow the operation of driverless cars and autonomous cars [51]. Self-driving cars have been developed by Google, and can detect objects around them and choose a safe speed during travel without the aid of users, via the deployed map, sensors, and software [27].

3.3 Roadside Units

Roadside units, also known as roadside equipment, are another essential component in the smart transportation system [1]. These units are deployed on the two sides of roads and embedded with smart devices to detect and track vehicles and relay

the information sent by vehicles. Generally speaking, roadside units consist of static traffic assistant equipment (traffic lights, traffic signs, street lamps, beacons, and others). Traffic lights can be used to schedule the traffic flow and reduce congestion at road intersections. To achieve a greater efficiency of traffic flows through the traffic lights, advanced schemes to schedule traffic lights need to be developed. Traffic signs are used to alert vehicles about the prospective traffic environment, aiming at improving travel safety. Street lamps are used to improve the visibility of vehicles while traveling in a dark environment.

In addition to the functions mentioned above, roadside units are deployed with sensing devices and communication devices [39, 47]. Sensing devices are used to detect and track vehicles and send the corresponding signals to assist vehicles in choosing proper operations. For example, when a "Stop" sign is in front of a vehicle, the ECUs embedded in the vehicle will receive the signal of "stop" sent by "Stop" sign, and the vehicle will automatically stop traveling and detect the traffic environment ahead. By doing this, increased safety in traveling can be achieved. Communication devices deployed in roadside units can be integrated with communication devices in vehicles to establish V2I communication. In comparison with V2V communication, V2I communication can achieve greater stability, higher throughput, and a larger communication range. Thus, V2I can have greater efficiency in delivering information over a long distance. As we can see, with the assistance of roadside units, the smart transportation system can achieve greater efficiency in traffic management and information delivery.

4 Communication Layer

In the communication layer, we present protocols, communication standards, and techniques that support the information exchange via the V2V and V2I communications. In the following, we first give an overview of the communication layer and then, briefly, the standard activities, followed by the detailed techniques in the different sublayers of the communication layer.

4.1 Overview

With the increasing number of vehicles operated in urban areas, the complexity of road conditions raises the problems of driving safety and efficiency within the transportation system (e.g., traffic congestion). The techniques have been advanced to support the communication layer in the smart transportation system, enabling efficient information sharing in user-to-user and user-to-vehicle communication. Particularly, by leveraging the wireless communication techniques deployed in the vehicle network, the functions of traffic sensing, surrounding observation, and information sharing can be provided to assist users in the complex driving environment.

By doing this, road accidents can be reduced and route management and efficiency can be improved.

Generally speaking, V2X, which stands for the communication of vehicles to everything, consists of V2V and V2I communication, and so on. In particular, information sharing among vehicles and/or RSUs (i.e., infrastructures) can improve accident avoidance, congestion awareness, and efficient operation of vehicles in the transportation system, where the vehicles have more knowledge about the surroundings and nearby vehicles, as well as potential risks.

In the V2V, the vehicles (cars, trucks, buses, etc.) exchange the information (direction, speed, acceleration, vehicle size, etc.) to predict and warn of safety threats and potential accidents (e.g., collisions) [31]. Sometimes, the vehicles may initiate protective actions or mechanisms ahead of the human response in some extreme cases so that the injury risk or property loss can be reduced or avoided. Notice that each vehicle should be equipped with a transceiver to transmit and receive information and the response action, and multiple sensors to collect information.

In the V2I, the RSUs (traffic signal, road sign, road lights, and others) as infrastructure elements can be used to support the information exchange among vehicles, which not only enables driving environment awareness, but also extends the communication range. The V2I can assist users in the information collection of the roadway, such as warning of curve speed, signal violation, and the acknowledgment of road signs, to name a few.

4.2 Standardization Activities

To develop and promote the techniques related to V2X, there have been standardization efforts to establish rules, legal information, and policy. In this section, we review one standardization development that seeks to realize dedicated short-range communication (DSRC) in V2X. The DSRC that enables two-way communication in short/medium range has been developed for improving the performance (i.e., transmission delay, communication reliability, and security) of V2V and V2I communications. In addition, the 75 MHz frequency spectrum in the 5.9 GHz band have been allocated for the applications in the smart transportation system, including vehicle safety, traffic management, and infotainment [54, 72, 76, 88, 101]. In addition to DSRC, using cellular communication techniques such as LTE was proposed by the 3rd Generation Partnership Project to support V2X [69] because the wide deployment of an LTE network can be leveraged to support high data rates and meet QoS (quality of service) requirements.

The standardization activities provide profound and widespread impacts on the development of the V2V and V2I communication in the smart transportation system. For example, the standardization of the MAC and PHY layer were established by the IEEE 802.11p-part 11 in [88], which mainly addresses the link establishment latency in V2V and the connection establishment delay in V2I via tuning the PHY and MAC parameters [38]. On top of the PHY and MAC layers, the standardizations in the

network and transport layers were realized via the IEEE 1609 Working Group (WG), which specified the protocols, network service, and management, among others [25, 43]. The IEEE 1609 WG consists of 1609.0, 1609.2, 1609.3, 1609.4, 1609.11, and 1609.12 and range from 2006 to 2016 [54]. For instance, the 1609.0 specifies the architecture of the vehicular network, the 1609.4 specifies the multichannel operation, and the 1609.12 is for the allocation of identifiers, and so on.

4.3 Technique Approaches

The communication requirements for the diverse and comprehensive V2X scenarios include low connection latency, low transmission latency, high network capacity, and security. To satisfy the communication requirements, various techniques in the different communication sublayers have been developed to carry out communication latency reduction, congestion avoidance, interference suppression, resource management, and the like.

4.3.1 PHY

The IEEE 802.11p specifies the frequency bands and operation channel bandwidth on the PHY layer, as well as the physical layer convergence protocol (PLCP) and physical medium access (PMD); whereas the PLCP connects the MAC layer with packets, the PMD connects to the physical communication channel and data links [2, 70].

The investigation of the PHY layer in IEEE 802.11p is to understand the impact and correlation of the parameters associated with the PHY layer. For example, Jiang et al. [38] conducted the analysis of the PHY layer and performance evaluation of the IEEE 802.11p, where V2V communication scenarios in both highway and urban areas were considered. To obtain propagation performance such as the bit error rate (BER) of high-mobility vehicles with respect to different PHY layer parameters (packet size, channel models, etc.), Sassi et al. [81] conducted the modeling analysis on vehicular communication, and provided the BER analysis on the channel models with the consideration of different modulation schemes (i.e., BPSK, QPSK, 16 QAM, and 64 QAM), as well as channel noises (i.e., AWGN (additive white Gaussian noise), Rayleigh fading, and Rician fading). Their results show that the transmission quality is relevant not only to the vehicle speed, but also to the signal-to-noise ratio (SNR) variance, modulation scheme, channel type, and others.

In addition, the power control mechanism is one effective technique to reduce end-to-end delay [23, 92, 93]. Adapting the transmission power and/or transmission rate is effective in dealing with the channel congestion problem when the density of vehicles is largely increased. Tielert et al. [92] investigated the relationship between the performance of optimal receivers and the power/rate parameters when the communication distance is provided. Their results show that the optimal transmit power is

independent of the node density in the network, but is relevant to the communication distance, whereas the transmit rate is related to the channel load. Furthermore, Fallah et al. [23] proposed a stateful utilization-based power adaption (SUPRA) scheme to improve the stability and fairness of the power use in the network.

4.3.2 MAC

The design of MAC protocols that support the V2V and V2I is critical and complex due to the mobility of vehicles in the network, the dynamic network topology, and high QoS requirements from diverse applications. The classic MAC layer design (i.e., carrier sense multiple access with collision avoidance, CSMA/CA), which provides the random access and collision avoidance for associated devices in the cluster, as the key mechanism in the IEEE 802.11p leverages the carrier sensing and packet management mechanism to reduce the collision from "hidden" nodes [123].

Nonetheless, the IEEE 802.11p may not be able to meet the latency requirements for some safety-related applications due to the channel access delay in CSMA. Thus, the decentralized self-organized mechanism (self-organizing time division multiple access, STDMA) provides timely and predictable channel access by sharing channel information via geolocation systems. The TDMA can assign and schedule frequency resources and time slot based on the vehicle and access priority. As shown by Hadded et al. [30], with knowledge of the vehicle's geolocation information, the TDMA-based MAC protocol could achieve overall higher performance (collision rate, access delay, packet loss, etc.) than the CSMA/CA-based MAC protocols.

Directional antenna-based MAC layer techniques in V2V/V2I communication were also studied to obtain high throughput and low latency via the high channel spatial reuse from directional transmission [26, 37, 55]. Other techniques such as cellular-assisted D2D (device to device) communication [33] and ad hoc based D2D communication were studied to support V2V communications. For instance, Hu et al. [34] proposed a D2D-based MAC protocol, which can conduct the modes' switching operation (cellular assisted D2D mode or ad hoc D2D mode) under different coverage scenarios. The main objective of the proposed protocol is to reduce end-to-end latency and improve connection reliability via the mode switching operations, as well as the radio resource allocation schemes.

4.3.3 Routing

The variety in packet size in V2X communications, dynamic network topology, and high vehicle mobility challenge the design and implementation of resource efficiency and delay awareness routing protocols. To address the issue, the routing protocols were studied [7, 12, 19, 58, 81, 104, 108, 120] to support V2X.

In a typical ad hoc network, routing protocols such as dynamic source routing (DSR) and ad hoc on-demand distance vector (AODV) [28, 52, 53, 75] were investigated. Due to the low scalability of the AODV, enhanced versions of AODV, such

as prediction-based AODV (PRAODV and PRAODVM) were proposed by Namboodiri and Gao [75]. The PRAODV and PRAODVM leverage the node speed and location information to estimate or predict the link connection lifetime and select the link with maximum lifetime.

Furthermore, due to the geolocation constraints of the physical streets, the bidirectional movement of vehicles could improve the performance of routing protocols when the geolocation information of streets (e.g., maps or navigation system) is considered. With the assistance of location information, the position-based routing scheme can be more effective in V2V communication, compared to the topology-based routing scheme. For example, the greedy perimeter stateless routing (GPSR) scheme, as one representative position-based routing scheme, which adopts both greedy forwarding and face routing to forward packets, could outperform the ad hoc routing scheme and DSR in open spaces or highway areas [41, 58].

The cluster-based routing protocols perform the communication between clusters (intercluster communication) or inside individual clusters (intracluster communication), coordinated by cluster heads. Clustering in the vehicle network leads to benefits such as high scalability and low control overhead. Nonetheless, the stability of clusters is one of the major issues that could significantly affect the delay and controlling overhead. As stated in [5, 6], the clustering in vehicle networks needs to consider factors such as vehicle position, mobility, and behavior.

The location-based routing protocols were also designed to find the statistical information of the end-to-end delay of multiple paths, and then select the path with the best performance. The examples include VADD [117], and D-Greedy and D-MinCost [86]. To be specific, the VADD carried out the packet carrying and forwarding with consideration of the vehicle mobility and the delivery delay, whereas D-Greedy and D-MinCost were designed to minimize the transmission cost and satisfy the overall delay bound.

4.3.4 Cross-Layer

The schemes designed for individual layers can lead to improvements in network performance with respect to end-to-end delay, packet loss rate, and others. Nonetheless, the conflicts or tradeoffs between different schemes may pose another issue. For instance, the automatic repeat request (ARQ) retransmits the packet when packet loss occurs, and forward error correction (FEC) provides the ability to correct the errors with introduced redundant data. The problem is that when the packet size is small, the FEC may have limited ability to correct the packet. In contrast, when the packet size is large, there will be retransmission overhead on the ARQ. Thus, finding the optimal packet size should not be constrained by only the MAC or PHY layers, but the MAC and PHY layers. The cross- layer design can provide the balance among multilayer tradeoffs, leading to improvement of the overall network performance [35, 36, 65, 80].

5 Service Layer

The service layer provides diverse services for users to maintain safe and efficient travels. In this section, the services that the smart transportation system can provide are presented first, and then the major application requirements are identified. Finally, one of the most important services, called the route guidance service, is presented in detail.

5.1 Services

To ensure the efficiency and safety of the smart transportation system, a number of services have been developed in recent years. In order to simplify and clarify the development and deployment of these services, the US Department of Transportation released the National Intelligent Transportation Architecture (NITA) and bundled these services into eight major categories [94]. In the following, we describe these major services in detail.

- *Travel and Traffic Management.* It focuses on the collection and sharing of traffic information, travel assistance, traffic and incident management, and others. Services in this category consist of pre-trip travel information, en route driver information, route guidance, ride matching and reservation, traveler service information, traffic control, incident management, travel demand management, emissions testing and mitigation, and highway rail intersection.
- *Public Transportation Management.* It focuses on improving the efficiency and safety of public transportation in the smart transportation system. Services in this category consist of public transportation management, en route transit information, personalized public transit, and public travel security.
- *Electronic Payment.* It focuses on the charging of travel, such as highway charging, bus charging, and others. The electronic payment service is listed in this category.
- *Commercial Vehicle Operation.* It focuses on monitoring and managing commercial vehicles. Services in this category consist of commercial vehicle electronic clearance, automated roadside safety inspection, on-board safety and security monitoring, commercial vehicle administrative processes, hazardous materials security and incident response, and freight mobility.
- *Emergency Management.* It focuses on dealing with the emergency events and consists of the services of emergency notification and personal security, emergency vehicle management, and disaster response and evacuation.
- *Advanced Vehicle Safety System.* It focuses on ensuring traffic safety while traveling. Services in this category consist of longitudinal collision avoidance, lateral collision avoidance, intersection collision avoidance, vision enhancement for crash avoidance, safety readiness, pre-crash restraint deployment, and automated vehicle operation.

- *Information Management.* It focuses on processing and storing traffic data and information, and the only service, namely archived data, is included in this category.
- *Maintenance and Construction Management.* It focuses on maintaining and monitoring the operation of the smart transportation system. The services of maintenance and construction operations are listed in this category.

In addition, the infotainment services on the vehicle focus on multimedia streaming (audio, video, etc.) to improve the driving experience or passenger's travel experience. The vehicle's location-based services, which enrich the driving experience and driving fatigue prevention are typical applications of vehicle infotainment, including navigation, attraction advisory, and others. It is worth noting that we only present the key services that the smart transportation system can provide, and further detailed descriptions of these services can be found in [94].

5.2 V2X Service Requirements

With the diverse and comprehensive applications supported by the vehicular network, the V2X communication has many specific requirements for network performance. The requirements of V2X communication, which consist of transmission frequency, transmission mode, latency constraints, packet size, communication range, and so on, can be provided by the services listed in Sect. 5.1.

In the safety-related applications, the transmission mode of the safety warning information can be identified as either event-driven or periodic [3, 32, 85]. The information is transmitted periodically in some applications, and require frequent data collection from vehicles or RSUs (curve speed warning, lane change assist, left turn assist, and so on). In addition, the information transmission in some safety applications are event-driven, where the warning is launched upon satisfying a certain condition or threshold (emergency stopping, vehicle distance, etc.), including precrash sensing and emergency brake lights.

Due to the high mobility of vehicles and high performance requirements, the end-to-end delay is one of the key metrics for the vehicular network. The latency requirements for safety-related applications are at maximum 100 ms, which is considerably higher than nonsafety-related services (i.e., 500 ms) [40]. The transmission frequency requirement for the related applications (media downloading, location-based services, etc.) is mostly a minimum 10 Hz, which is higher than other application categories (i.e., 1 Hz) for traffic management.

The requirements on the communication type (broadcast, co-operative awareness, or direct messaging) may vary based on the specific application. For example, the collision warning and emergency vehicle warning in safety-related services, the adaptive speed control and congestion avoidance control in traffic management, and the location-based service and attraction advisory in the infotainment service may broadcast the information for wide acknowledgment. Meanwhile, the lane change

assist, collision risk warning, and multimedia services are based on co-operative awareness for direct communication.

To satisfy the aforementioned communication requirements, the latency becomes one key challenge for the vehicular network, due to the high mobility of vehicles in both V2V and V2I communication scenarios. Furthermore, the high vehicle mobility poses additional challenges to the reliability of connections, dynamic network topology, and network capacity, among others [122].

5.3 Route Guidance

Route guidance is an essential service in transportation and traffic management in the smart transportation system. It is a service that requires interactions with users, in which users input their destinations and route guidance can automatically determine the optimal guided routes for users based on real-time traffic information, aiming at completing their travels with low traffic congestion and great traffic efficiency [44, 63].

To improve traffic efficiency in the smart transportation system, a number of efforts have been developed on route guidance. Based on the information used to determine guided routes, existing route guidance schemes can be divided into two main categories: static route guidance schemes, and dynamic route guidance schemes, which are described.

5.3.1 Static Route Guidance Schemes

Static route guidance schemes are the earliest guidance schemes used to determine the guided route from the current location to the user's destination. Generally speaking, the static route guidance scheme usually determines the optimal routes depending on the road map information, which is advance-stored in a database [87]. When determining guided routes, the static route guidance scheme first reads the stored map information and then converts static criteria, such as road length or travel time, obtained via dividing limited speed by road length, as the road weight, and finally determines the optimal guided route via the shortest distance algorithms (e.g., Dijkstra [24, 98] and Floyd [16, 96]).

Until now, a limited number of static route guidance schemes have been developed. For example, Selamat et al. [84] proposed a static route guidance scheme that can find the best shortest path from the current location to the destination in the road network, leading to lower cost in comparison with the Dijkstra algorithm. Anagnostopoulos et al. [9] proposed a static route guidance system, namely PAN-DRIVE, that can determine the shortest itineraries between two points by abstracting map topology as a graph. PAN-DRIVE can efficiently achieve system functionalities of navigation, routing, and route guidance.

In fact, the static route guidance scheme can be easily developed via algorithms that compute the shortest distance between source and destination. Because the static route guidance scheme only uses static criteria to determine an optimal route, low traffic efficiency can be achieved when road congestion occurs. Thus, the static route guidance schemes are not suitable for the smart transportation system.

5.3.2 Dynamic Route Guidance Schemes

Dynamic route guidance schemes were developed to overcome the limitation of static route guidance schemes, and can determine the optimal route from the current location to the destination based on real-time traffic information, leading to the reduction of road congestion and travel time. One of the most important components in the dynamic route guidance scheme is the sharing of real-time traffic information. In the smart transportation system, each vehicle or roadside unit can perceive local traffic information and share the information via V2V or V2I communications. Based on the mechanism used to share and deliver traffic information, dynamic route guidance schemes can be divided into two categories: dynamic infrastructure-based route guidance schemes, and dynamic infrastructure-free route guidance schemes.

Dynamic Infrastructure-Based Route Guidance Schemes. In the dynamic infrastructure-based route guidance scheme, the real-time traffic information measured by vehicles is shared and delivered by V2I communication, in which the roadside infrastructure is established by a number of devices or components deployed on roads and streets, and used as a relay node to achieve communication between vehicles and control centers.

Recently, a number of dynamic infrastructure-based route guidance systems have been developed [10, 45, 46, 91, 107, 116]. For example, Chahbi et al. [10] proposed a dynamic route guidance based on the MVDR beamforming technique that can achieve optimal coverage and connectivity of drivers and roadside units to exchange information and ultimately achieve great efficiency on route guidance. Ye et al. [107] proposed the maximum flow theory-based dynamic route guidance, which aims at balancing the traffic load of the road network, avoiding network congestion, and improving traffic efficiency. Zhang et al. [116] proposed the backpressure theory-based traffic dispersion route algorithm, namely BPR-US, which can meet both users' satisfaction and traffic load simultaneously. Khanjary et al. [45] proposed a dynamic route guidance system, namely PersianGulf. Combining traffic signal controllers and route guidance, PersianGulf could derive the optimal route in traffic signal controllers and autonomously work without the assistance of other traffic supervisors. Evaluation results demonstrated that PersianGulf could efficiently improve the average speed of vehicles.

Although the infrastructure-based route guidance schemes that use V2I communication to share real-time traffic information can achieve great efficiency on information delivery and transmission leading to greater traffic capability in the smart transportation system, the deployment of roadside infrastructure would incur high costs with low scalability.

Dynamic Infrastructure-Free Route Guidance Schemes. To reduce the cost of deploying roadside infrastructure, dynamic infrastructure-free route guidance schemes were developed in which real-time traffic information is shared and delivered via V2V communications and roadside infrastructure does not need to be involved.

A number of infrastructure-free route guidance schemes were developed [15, 17, 56, 57, 79, 90, 99]. For example, Ding et al. [15] proposed a real-time vehicle route guidance scheme based on V2V communications, namely V2R2, that can effectively determine better routes to destinations with less travel time. Li et al. [57] proposed a multicriteria combination system, namely AHP-FUZZY, in which a fuzzy inference technique-based analytical hierarchy process was designed to be integrated with the route guidance to determine the weights of the attributes, and then, based on these weights, the optimal guided routes can be determined. Dong et al. [17] proposed a framework to determine the optimal route in a stochastic time-dependent network. In their proposed scheme, real-time information was used to investigate the path travel time indeterminacy and correlation between adjacent paths, and a mathematical formalization was proposed to update the path travel time and assist users in determining optimal routes.

Although the infrastructure-free route guidance schemes can reduce the cost of deploying roadside infrastructure, unstable connectivity of information communication may occur. For example, if a road has no vehicle traveling on it, the real-time traffic information of the road cannot be delivered and shared with the outside, because there may be no available vehicle around the road to forward the information. Thus, developing an infrastructure-free route guidance scheme with great connectivity remains an unsolved issue.

6 Open Issues

In the following, we discuss several open issues related to the smart transportation system, including security, big data, and performance and evaluation platforms.

6.1 Security

The real-time traffic state information measured and shared via V2I and V2V communication is essential for providing efficient and secure services in the smart transportation system. Nonetheless, V2V and V2I communications are deployed in an open environment and the topologies change over time. This means that in each time slot, a number of vehicles will leave or enter the smart transportation system, making it difficult to identify and authenticate whether each vehicle is legitimate. Malicious attacks may be easily launched in the smart transportation systems to disrupt services provided, leading to low traffic efficiency and safety [11, 89].

One of the serious malicious attacks in the smart transportation system is the information-related attack, which focuses on modifying and faking the real-time traffic state information and sharing the forged information with other on-road vehicles through V2V and V2I communications [11, 64]. With the forged information, vehicles will make erroneous determinations about the traffic environment and request improper services, which may lead to an unsafe traveling environment. In fact, this kind of information-related attack can be considered as the integration of data integrity attacks [62, 105, 106] and malicious code propagation attacks [109, 110], in which the data integrity attack is used to compromise measured traffic state information via compromised components by the adversaries, and the malicious code propagation attack is used to propagate the malicious code to other vehicles in a large area. In this way, a large number of vehicles can be compromised in a similar manner as Internet worm propagation [111]. Therefore, before deploying the smart transportation system, security challenges should be investigated in detail. In addition, the privacy of users in the transportation system needs to be considered [78].

With respect to the secure smart transportation system, a number of research efforts have been conducted [14, 48, 60, 61, 67, 71, 73, 83, 121]. For example, Sedjelmaci et al. [83] proposed an intrusion detection and prevention scheme to detect and predict the malicious behavior of an adversary, and the proposed scheme can achieve a high detection rate and low false positive rate in vehicular networks. Tyagi et al. [95] investigated the security and vulnerabilities of vehicular networks, aiming to develop secure and efficient broadcasting and routing services. Li et al. [60] proposed an attack-resistant trust management scheme to detect and cope with malicious attacks via evaluating the trustworthiness of both data and mobile vehicles in the smart transportation system. With enhanced trustworthiness, the proposed scheme can achieve improvement of traffic safety, mobility, and environmental protection. Morais et al. [71] proposed a distributed intrusion detection scheme that can categorize malicious activities and behaviors of vehicles with great efficiency via exchanging events between participating vehicles.

Although a number of efforts have been developed to secure the smart transportation system, the majority focus on securing data dissemination in vehicular networks, and few efforts focus on investigating the impact of malicious attacks on services, such as route guidance, in the smart transportation system. Therefore, efforts on the modeling of impact of attacks and the design of efficient schemes to mitigate attacks against services (such as the information attack combined with the data integrity attack and malicious code propagation attack) should be developed in the future.

6.2 Big Data

In the smart transportation system, a large amount of data needs to be collected from physical and cyber components and transmitted to computing cores via V2X communications so that the efficient and secure operations of the transportation system can be enabled. Particularly, in a safe and reliable smart transportation system,

various sensors should be installed on vehicles and deployed on roadsides to collect information and transmit it to the operation center. With a large number of vehicles dynamically running in the smart transportation system, by constantly monitoring variations in traffic characteristics (traffic densities, speeds, vehicles, etc.), high-volume data streams (big data) are generated by monitoring sensors over time for timely processing and analysis. Thus, the mounting volume of data stored and processed, along with a continuously increasing storage and processing capacity, poses significant challenges that hinder the effectiveness of the smart transportation system.

To address this issue, we study cloud computing and fog computing techniques to assist in designing a secure and efficient transportation system. The proposed system consists of monitoring sensors, a cloud infrastructure, and an operation center [100, 112]. Monitoring sensors can be deployed on devices in the smart transportation system to collect the component information and transmit it (e.g., raw data or alerts) to the cloud or the fog computing infrastructure. A cloud or fog computing infrastructure is a distributed system deployed with a number of servers, providing both storage and computational resources. There are two types of servers in the cloud and fog computing infrastructures: storage servers and application servers. The collected streams of data will be pushed and stored in storage servers in real-time whereas application servers will provide data analysis. MapReduce is one type of technique used to speed up data processing by separating and processing data streams concurrently. Notice that to improve the scalability of the cloud further, fog computing, which supports the smart transportation system, should be explored, where some computation and storage can be conducted by roadside devices. There have been a number of research efforts on the MapReduce framework used for various applications [13, 100]. The operation center plays the intelligence role that can dynamically update requests from users, operation policies and configurations, and monitor system security.

6.3 Performance and Platforms

As we mentioned, V2X is the core in the communication layer, enabling effective and efficient information sharing in vehicular networks. The diverse applications supported by V2X that range from safety to infotainment require high network performance (latency, capacity, stability, etc.). Although various techniques and standardization activities have been developed, to accomplish and realize the services from the various applications fully, the following challenges need to be addressed. First, the latency bounds of the information delivery may vary based on QoS requirements of a specific application. To satisfy the latency requirement of various applications with high vehicle mobility, dynamic channel conditions, rapid dynamic topology, and the design of effective V2X communication infrastructures and protocols need further research. For example, the ultra-dense network [113, 114], as part of next-generation wireless networks, can be one possible solution for supporting diverse QoS requirements of applications. Second, attention has been increasingly

focused on the cross-layer design in order to obtain an overall optimal network performance. However, challenges to the measurement and evaluation of the interaction and information exchange among different layers of the cross-layer design remain. For example, the upper layer design may need feedback information from the lower layer and vice versa. In addition, the complexity of cross-layer design implementation may pose further challenges in V2X. Third, due to the dynamics of the network topology, the addressing of the moving vehicles becomes an issue for packet delivery. The geographical addressing is one possible enabling solution for logical addressing, which leverages the feature of physical geolocation of a vehicle or a region. Nonetheless, how to extend the IP addressing with geoaddressing remains an open challenge to the implementation and realization of the smart transportation system.

In addition, in the smart transportation system, various cyber and physical components exist and interact, and many research efforts have given rise to unique schemes and systems. To evaluate the effectiveness of the proposed schemes, we need to design cost-effective modeling and simulation platforms that combine traffic, application, communication, events, and so on. The performance metrics from the transportation operation aspect include effectiveness and accuracy (routing correctness, etc.), scalability, efficiency (travel time, gas usage, etc.), and other factors. Considering the problems of flexibly coupling simulators, synchronizing them, and enabling them to interact with each other, a framework that integrates both traffic and network simulators will be needed. One platform is using the V2X simulation run-time infrastructure (VSimRTI) [19, 82], which has the capability of coupling various simulators. For communication networks, different types of network architectures such as V2I communication, V2V communication, and a combination of both (called hybrid) need to be integrated. Performance metrics (e.g., throughput, packet delivery ratio, latency, delay, jitter, etc.) need to be considered to evaluate the performance of V2X. Performance metrics in physical components include traffic congestion, travel time, fuel consumption, and environmental emissions (such as carbon dioxide [CO_2]). Metrics for computing cores include computing resources and time, among others.

7 Conclusion

In this chapter, an overview of the smart transportation system has been presented, including architecture, enabling technologies, and related open issues. Particularly, a three-layer architecture was introduced for the smart transportation system, specifically comprising the physical layer, communication layer, and service layer. To construct a full-vision of smart transportation, the components, enabling technologies, and services included in these three layers have been presented in detail. Ongoing and unresolved concerns surround the topics of security, big data, and performance and evaluation platforms for the smart transportation system. The main purpose of this chapter was to establish basic knowledge of the architecture and techniques in the smart transportation system, which can be used to further investigate and evaluate techniques that seek to address security issues in the smart transportation system.

Acknowledgements This work was supported in part by US National Science Foundation (NSF) under grant: CNS 1350145 and USM Wilson H. Elkins Professorship fund. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the agencies.

References

1. Abbassi, S.H., Qureshi, I.M., & Abbasi, H. (2014). Performance of uni-directional road side units in vehicular adhoc networks. In: *Proceedings of World Congress on Computer Applications and Information Systems (WCCAIS)*.
2. Abdelgader, A., & Lenan, W. (2014). The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges. In: *Proceedings of the world congress on engineering and computer science*.
3. Ahmed-Zaid, F., Bai, F., Bai, S., Basnayake, C., Bellur, B., Brovold, S., Brown, G., et al. (2011). Vehicle safety communications–applications (vsc-a) final report: appendix volume 1 system design and objective test. Technical Report.
4. Al-kahtani, M.S. (2012). Survey on security attacks in vehicular ad hoc networks (vanets). In: *Proceedings of 6th International Conference on Signal Processing and Communication Systems (ICSPCS)*.
5. Al-Rabayah, M., & Malaney, R. (2010). A new hybrid location-based ad hoc routing protocol. In *Proceedings of ieee global telecommunications conference (GLOBECOM)*.
6. Al-Rabayah, M., & Malaney, R. (2012). A new scalable hybrid routing protocol for vanets. *IEEE Transactions on Vehicular Technology (TVT)*, *61*(6), 2625–2635.
7. Altayeb, M., & Mahgoub, I. (2013). A survey of vehicular ad hoc networks routing protocols. *International Journal of Innovation and Applied Studies*, *3*(3), 829–846.
8. An, S.H., Lee, B.H., & Shin, D.R. (2011). A survey of intelligent transportation systems. In *Proceedings of third international conference on computational intelligence, communication systems and networks (CICSyN)*.
9. Anagnostopoulos, P., Papapanagiotakis, G., & Gonos, F., (1992). Pan-drive: A vehicle navigation and route guidance system. In *Proceedings of the 3rd International Conference on Vehicle Navigation and Information Systems*.
10. Chahbi, I., Ben Amara, D., & Belghith, A., (2013). A novel route guidance algorithm using beamforming techniques for vehicular networks. In *Proceedings of IEEE 38th conference on local computer networks workshops (LCN Workshops)*.
11. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., et al. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of 20th USENIX security symposium (SEC)*.
12. Chen, W., Guha, R. K., Kwon, T. J., Lee, J., & Hsu, Y. Y. (2011). A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, *11*(7), 787–795.
13. Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A cloud computing based network monitoring and threat detection system for critical infrastructures. *International journal of big data research (elsevier)-special issue on big data from networking perspective 3*:10–23.
14. Deng, H., Zeng, Q.A., & Agrawal, D.P. (2003). Svm-based intrusion detection system for wireless ad hoc networks. In *Proceedings of IEEE 58th vehicular technology conference*, VTC 2003-Fall.
15. Ding, J. W., Wang, C. F., Meng, F. H., & Wu, T. Y. (2010). Real-time vehicle route guidance using vehicle-to-vehicle communication. *IET Communications*, *4*(7), 870–883.
16. Djojo, M., & Karyono, K. (2013). Computational load analysis of dijkstra, a*, and floyd-warshall algorithms in mesh network. In *Proceedings of IEEE international conference on robotics, biomimetics, and intelligent computational systems (ROBIONETICS)*.

17. Dong, W., Vu, H., & Vo, Q. (2011). Real time route guidance with correlated link cost. In *Proceedings of IEEE 14th international conference on intelligent transportation systems (ITSC)*.
18. D'Orey, P., & Ferreira, M. (2014). Its for sustainable mobility: A survey on applications and impact assessment tools. *IEEE Transactions on Intelligent Transportation Systems*, *15*(2), 477–493.
19. Ekedebe, N., Lu, C., & Yu, W. (2015). On experimental evaluation of intelligent transportation system (its) safety and traffic efficiency. In *Proceedings of IEEE international conference on communication (ICC)*.
20. Elkosantini, S., & Darmoul, S. (2013). Intelligent public transportation systems: A review of architectures and enabling technologies. In *Proceedings of international conference on advanced logistics and transport* (ICALT).
21. Ezell, S. (2010). Explaining international it application leadership: Intelligent transportation systems.
22. Faezipour, M., Nourani, M., Saeed, A., & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communication of ACM*, *55*(2), 90–100.
23. Fallah, Y. P., Nasiriani, N., & Krishnan, H. (2016). Stable and fair power control in vehicle safety networks. *IEEE Transactions on Vehicular Technology*, *65*(3), 1662–1675.
24. Fan, D., & Shi, P. (2010). Improvement of dijkstra's algorithm and its application in route planning. In *Proceedings of seventh international conference on fuzzy systems and knowledge discovery (FSKD)*.
25. Festag, A. (2015). Standards for vehicular communication-from ieee 802.11 p to 5g. e & i. *Elektrotechnik und Informationstechnik*, *132*(7), 409–416.
26. Gillani, S.A., Shah, P.A., Qayyum, A., & Hasbullah, H.B. (2015). Mac layer challenges and proposed protocols for vehicular ad-hoc networks. In Vehicular ad-hoc networks for smart cities, Springer, pp. 3–13.
27. Google (2016). Google self-driving car. In http://www.google.com/selfdrivingcar/how/.
28. Goyal, M.K., Verma, Y.K., Bassi, P., & Misra, P.K. (2013). Performance analysis of ad hoc on-demand distance vector routing and dynamic source routing using ns2 simulation. In *Mobile communication and power engineering*, Springer, pp. 390–396.
29. Greenberg, A. (2015). After jeep hack, chrysler recalls 1.4 m vehicles for bug fix. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.
30. Hadded, M., Muhlethaler, P., Laouiti, A., Zagrouba, R., & Saidane, L. A. (2015). Tdma-based mac protocols for vehicular ad hoc networks: A survey, qualitative analysis, and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(4), 2461–2492.
31. Harding, J., Powell, G., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M. et al. (2014). Vehicle-to-vehicle communications: Readiness of v2v technology for application. Technical Report.
32. Hartenstein, H., & Laberteaux, L. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, *46*(6), 164–171.
33. Hematian, A., Yu, W., Lu, C., Griffith, D., & Golmie, N. (2016). Clustering-based device-to-device communication to support diverse applications. In *Proceedings of ACM International Conference on Reliable & Convergent Systems (RACS)*.
34. Hu, L., Eichinger, J., Dillinger, M., Botsov, M., & Gozalvez, D. (2016). Unified device-to-device communications for low-latency and high reliable vehicle-to-x services. In *Proceedings of IEEE Vehicular Technology Conference* (VTC Spring), 2016 IEEE 83rd.
35. Huang, Y., Yang, X., Yang, S., Yu, W., & Fu, X. (2011). A cross-layer approach handling link asymmetry for wireless mesh access networks. *IEEE Transactions on Vehicular Technology (TVT)*, *60*(3), 1045–1058.
36. Jarupan, B., & Ekici, E. (2011). A survey of cross-layer design for vanets. *Ad Hoc Networks*, *9*(5), 966–983.
37. Ji, S., Kim, J., & You, C. (2015). An efficient directional mac protocol for vehicular ad-hoc networks. *Journal of the Institute of Electronics and Information Engineers*, *52*(4), 9–16.
38. Jiang, D., & Delgrossi, L. (2008). Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Proceedings of ieee vehicular technology conference, 2008. VTC Spring 2008*. IEEE.

39. Jo, Y., & Jeong, J. (2016). Rpa: Road-side units placement algorithm for multihop data delivery in vehicular networks. In *Proceedings of 30th international conference on advanced information networking and applications workshops (WAINA)*.
40. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., et al. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys & Tutorials*, *13*(4), 584–616.
41. Karp, B., & Kung, H.T. (2000). Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking (ACM)*.
42. Kastell, K. (2014). Security requirements in communication networks for transportation systems. In *Proceedings of 16th international conference on transparent optical networks (ICTON)*.
43. Kenney, J. B. (2011). Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, *99*(7), 1162–1182.
44. Khanjary, M., & Hashemi, S. (2012). Route guidance systems: Review and classification. In *Proceedings of 6th euro american conference on telematics and information systems (EATIS)*.
45. Khanjary, M., Faez, K., Meybodi, M., & Sabaei, M. (2011). Persiangulf: an autonomous combined traffic signal controller and route guidance system. In *Proceedings of IEEE vehicular technology conference (VTC Fall)*.
46. Khosroshahi, A., Keshavarzi, P., KoozehKanani, & Z., Sobhi, J. (2011). Acquiring real time traffic information using vanet and dynamic route guidance. In *Proceedings of IEEE 2nd International Conference on Computing, Control and Industrial Engineering (CCIE)*.
47. Kim, D., Velasco, Y., Yang, Z., Wang, W., Hussain, R., & Uma, R.N. (2016). Cost effective mobile and static road side unit deployment for vehicular adhoc networks. In *Proceedings of international conference on computing, networking and communications (ICNC)*.
48. Kim, R., Lim, H., & Krishnamachari, B. (2015). Prefetching-based data dissemination in vehicular cloud systems. *IEEE Transactions on Vehicular Technology (TVT)* PP(99):1–1.
49. Klaus Finkenzeller, D.M. (2010). *RFID Handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*, 3rd edn. Wiley.
50. Kleberger, P., Olovsson, T., & Jonsson, E. (2011). Security aspects of the in-vehicle network in the connected car. In *Proceedings of IEEE intelligent vehicles symposium* (IV).
51. Knapp, A. (2011). Nevada passes law authorizing driverless cars. In: Forbes.
52. Kukreja, D., Dhurandher, S. K., & Reddy, B. (2015). Enhancing the security of dynamic source routing protocol using energy aware and distributed trust mechanism in manets. In *Intelligent distributed computing* (pp. 83–94). Springer.
53. Kumar, P. N., et al. (2013). A novel method to avoid stale route cache problem of dynamic source routing protocol for mobile ad hoc network. In *Proceedings of the IEEE International Conference On Current Trends in Engineering and Technology (ICCTET)*.
54. Kurihara, T. (2013). Dedicated short range communication working group. https://standards.ieee.org/develop/wg/1609-WG.html.
55. LeLann, G. (2015). Safety in vehicular networks–on the inevitability of short-range directional communications. In *Proceedings of the International Conference on Ad-Hoc Networks and Wireless* (Springer).
56. Leontiadis, I., Marfia, G., Mack, D., Pau, G., Mascolo, C., & Gerla, M. (2011). On the effectiveness of an opportunistic traffic management system for vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), 1537–1548.
57. Li, C., Anavatti, S., & Ray, T. (2014). Analytical hierarchy process using fuzzy inference technique for real-time route guidance system. *IEEE Transactions on Intelligent Transportation Systems*, *15*(1), 84–93.
58. Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, *2*(2), 12–22.
59. Li, S. (2012). A survey of urban traffic coordination controls in intelligent transportation systems. In *Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*.

60. Li, W., & Song, H. (2016). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(4), 960–969.
61. Li, W., Joshi, A., & Finin, T. (2010). Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach. In *Proceedings of the Eleventh International Conference on Mobile Data Management*.
62. Lin, J., & Yu, W. (2014). Yang X (2016a) On false data injection attack against multistep electricity price in electricity market in smart grid. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, *27*, 286–302.
63. Lin, J., Yu, W., Yang, X., Yang, Q., Fu, X., & Zhao, W. (2016b). A real-time en-route route guidance decision scheme for transportation-based cyber-physical systems. *IEEE Transactions on Vehicular Technology* (TVT) PP(99), 1–1.
64. Lin, J., Yu, W., Zhang, N., Yang, X., & Ge, L. (2017). On data integrity attack against route guidance in transportation-based cyber-physical systems. In *Proceedings of Annual IEEE Consumer Communications and Networking (CCNC)*.
65. Liu, J., Wan, J., Wang, Q., Zeng, B., & Fang, S. (2016). A time-recordable cross-layer communication protocol for the positioning of vehicular cyber-physical systems. *Future Generation Computer Systems*, *56*, 438–448.
66. Liu, Y., Tian, B., Chen, S., Zhu, F., Wang, K. (2013). A survey of vision-based vehicle detection and tracking techniques in its. In *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES)*.
67. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*.
68. Mello, L. D., & Kubota, L. T. (2002). Review of the use of biosensors as analytical tools in the food and drink industries. *Food Chemistry 77*(2), 237–256. http://www.sciencedirect.com/science/article/pii/S0308814602001048.
69. MirEmail, Z. H., & Filali, F. (2014). Lte and ieee 802.11p for vehicular networking: a performance evaluation. *EURASIP Journal on Wireless Communications and Networking*, *2014*(89).
70. Mittag, J., Papanastasiou, S., Hartenstein, H., & Strom, E. G. (2011). Enabling accurate cross-layer phy/mac/net simulation studies of vehicular communication networks. *Proceedings of the IEEE*, *99*(7), 1311–1326.
71. Morais, A., & Cavalli, A. (2012). A distributed intrusion detection scheme for wireless ad hoc networks. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*.
72. Morgan, Y. L. (2010). Notes on dsrc & wave standards suite: Its architecture, design, and characteristics. *IEEE Communications Surveys & Tutorials*, *12*(4), 504–518.
73. Mostefaoui, A., Melkemi, M., & Boukerche, A. (2014). Localized routing approach to bypass holes in wireless sensor networks. *IEEE Transactions on Computers (TC)*, *63*(12), 3053–3065.
74. Nakamura, J. (2005). Image sensors and signal processing for digital still cameras. In Optical science and engineering: CRC Press.
75. Namboodiri, V., & Gao, L. (2007). Prediction-based routing for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology (TV)*, *56*(4), 2332–2345.
76. Oh, H., Yae, C., Ahn, D., & Cho, H. (1999). 5.8 ghz dsrc packet communication system for its services. In *Proceedings of IEEE Vehicular Technology Conference*.
77. Owojaiye, G., & Sun, Y. (2012). Focal design issues affecting the deployment of wireless sensor networks for intelligent transport systems. *IET Intelligent Transport Systems*, *6*(4), 432–432.
78. Pingley, A., Yu, W., Zhang, N., Fu, X., & Zhao, W. (2009). Cap: A context-aware privacy protection system for location-based services. In *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*.
79. Qing, S., & Xiaofan, W. (2011). An efficient route computation approach for large graphs. In *Proceedings of the 30th Chinese Control Conference (CCC)*.

80. Ratwani, V., & Shah, A. (2015). Network coding and cross-layer approach for reliability and optimization of routing in vanet: A survey. *International Journal of Computer Applications*, *113*(13).
81. Sassi, A., Charfi, F., Kamoun, L., Elhillali, Y., & Rivenq, A. (2014). Ofdm transmission performance evaluation in v2x communication. arXiv:14108039.
82. Schnemann, B. (2016). V2x simulation runtime infrastructure vsimrti: An assessment tool to design smart traffic management systems. *Computer Networks*, *55*(14), 3189–3198.
83. Sedjelmaci, H., Bouali, T., & Senouci, S. M (2014) Detection and prevention from misbehaving intruders in vehicular networks. In *Proceedings of IEEE Global Communications Conference (GLOBECOM)*.
84. Selamat, A., Zolfpour-Arokhlo, M., Hashim, S., & Selamat, M. (2011). A fast path planning algorithm for route guidance system. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.
85. Shulman, M., & Deering, R. (2007). Vehicle safety communications in the united states. In *Proceedings of the Conference on Experimental Safety Vehicles*.
86. Skordylis, A., & Trigoni, N. (2008). Delay-bounded routing in vehicular ad-hoc networks. In *Proceedings of the 9th ACM International Symposium on Mobile ad hoc Networking and Computing*.
87. Song, Q., & Wang, X. (2011). Efficient routing on large road networks using hierarchical communities. *IEEE Transactions on Intelligent Transportation Systems*, *12*(1), 132–140.
88. Standards I (2010) 802.11 p-2010-ieee standard for information technology - local and metropolitan area networks-specific requirements-part 1 : Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6 : Wireless access in vehicular environments. https://www.standardsieeeorg/findstds/standard/80211p-2010html.
89. Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaaniche, M., Laarouchi, Y. (2013). Survey on security threats and protection mechanisms in embedded automotive networks. In *Proceedings of 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*.
90. Sun, W., Hu, L., Li, P., & Wang, H. (2012). A bi-level optimal control approach to route guidance problem considering travelers' stochastic compliance. In *Proceedings of the of Proceedings of International Conference on Modelling, Identification Control (ICMIC)*.
91. Tian, D., Yuan, Y., Zhou, J., Wang, Y., Lu, G., Xia, H. (2013). Real-time vehicle route guidance based on connected vehicles. In *Proceedings of IEEE International Conference on and IEEE Cyber, Physical and Social Computing*.
92. Tielert, T., Jiang, D., Hartenstein, H., & Delgrossi, L. (2013). Joint power/rate congestion control optimizing packet reception in vehicle safety communications. In *Proc. of the tenth ACM international workshop on Vehicular inter-networking, systems, and applications (ACM)*.
93. Torrent-Moreno, M., Mittag, J., Santi, P., & Hartenstein, H. (2009). Vehicle-to-vehicle communication: fair transmit power control for safety-critical information. *IEEE Transactions on Vehicular Technology (TVT)*, *58*(7), 3684–3703.
94. Transportation UDO, (2011). Executive summary national its architecture version 6.1. https://www.iteris.com/itsarch/html/user/userservhtm.
95. Tyagi, P., & Dembla, D. (2014). Investigating the security threats in vehicular ad hoc networks (vanets): Towards security engineering for safer on-road transportation. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*.
96. Wang, J., Sun, Y., Liu, Z., Yang, P., Lin, T. (2007a). Route planning based on floyd algorithm for intelligence transportation system. In *Proceedings of the IEEE International Conference on Integration Technology (ICIT)*.
97. Wang, Y., Wu, Y., Liu, Y., Tang, A. (2007b). The application of radio frequency identification technology on tires tracking. In *Proceedings of the 2007 IEEE International Conference on Automation and Logistics*.
98. Wei, M., & Meng, Y. (2014). Research on the optimal route choice based on improved dijkstra. In *Proceedings of IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)*.

99. Wu, C., Zhang, X., Dong, Y. (2013). Route guidance systems based on real-time information. In *Proceedings of International Conference on Connected Vehicles and Expo (ICCVE)*.
100. Xu, G., Yu, W., Chen, Z., Zhang, H., Moulema, P., Fu, X., & Lu, C. (2015). A cloud computing based system for cyber security management. *International Journal of Parallel, Emergent and Distributed Systems (IJPEDS) 30*(1), 29–45.
101. Xu, Q., Mak, T., Ko, J, Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in dsrc. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*.
102. Y Z, X Z, S Z, s G. (2012). Intelligent transportation system based on internet of things. In *Proceedings of World Automation Congress (WAC*).
103. Yan, X., Zhang, H., Wu, C. (2012). Research and development of intelligent transportation systems. In *Proceedings of 11th International Symposium on Distributed Computing and Applications to Business, Engineering Science (DCABES)*.
104. Yang, Q., Lim, A., Li, S., Fang, J., & Agrawal, P. (2010). Acar: Adaptive connectivity aware routing for vehicular ad hoc networks in city scenarios. *Mobile Networks and Applications*, *15*(1), 36–60.
105. Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., & Zhao, W. (2014). On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Transactions on Parallel and Distributed System (TPDS)*, *25*(3), 717–729.
106. Yang, X., Lin, J., Yu, W., Moulema, P., Fu, X., & Zhao, W. (2015). A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. *IEEE Transactions on Computers (TC)*, *64*(1), 4–18.
107. Ye, P., Chen, C., Zhu, F. (2011). Dynamic route guidance using maximum flow theory and its mapreduce implementation. In *Proceedings of 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*.
108. Yu, W., Lee, J. (2002). Dsr-based energy-aware routing protocols in ad hoc networks. In *Proceedings of IEEE International Conference on Wireless Network (ICWN)*.
109. Yu, W., Boyer, P.C., Chellappan, S., Xuan, D. (2005). Peer-to-peer system-based active worm attacks: Modeling and analysis. In *Proceedings of the IEEE International Conference on Communications (ICC)*.
110. Yu, W., Wang, X., Calyam, P., Xuan, D., Zhao, W. (2006). On detecting camouflaging worm. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*.
111. Yu, W., Zhang, N., Fu, X., & Zhao, W. (2010). Self-disciplinary worms: Modeling and countermeasures. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, *21*(10), 1501–1514.
112. Yu, W., Xu, G., Chen, Z., & Moulema, P. (2013). A cloud computing based architecture for cyber security situation awareness. In: *Proceedings of 4th International Workshop on Security and Privacy in Cloud Computing (SPCC)*.
113. Yu, W., Xu, H., Hematian, A., Griffith, D., & Golmie, N. (2016a). Towards energy efficiency in ultra dense networks. In *Proceedings of IEEE International Performance Computing and Communications Conference (IPCCC*).
114. Yu, W., Xu, H., Zhang, H., Griffith, D., & Golmie, N. (2016b). Ultra dense networks: State of art and future directions. In *Proceedings of IEEE International Conference on Computer Communication and Networks (ICCCN)*.
115. Zhang, J., Wang, F. Y., Wang, K., Lin, W. H., Xu, X., & Chen, C. (2011). Data-driven intelligent transportation systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), 1624–1639.
116. Zhang, R., Li, Z., Feng, C., & Jiang, S. (2012). Traffic routing guidance algorithm based on backpressure with a trade-off between user satisfaction and traffic load. In *Proceedings of IEEE Vehicular Technology Conference (VTC Fall)*.
117. Zhao, J., & Cao, G. (2008). Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE transactions on vehicular technology (TVT)*, *57*(3), 1910–1922.
118. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Proceedings of 2013 9th International Conference on Computational Intelligence and Security (CIS)*.

119. Zhao, M., Walker, J., & Wang, CC. (2012). Security challenges for the intelligent transportation system. In *Proceedings of the First International Conference on Security of Internet of Things*.
120. Zhao, P., Yang, X., Yu, W., & Fu, X. (2013). A loose virtual clustering based routing for power heterogeneous manets. *IEEE Transactions on Vehicular Technology (TVT)*, *62*(5), 2290–2302.
121. Zheng, B., Li, W., Deng, P., Grardy, L., Zhu, Q., Shankar, N. (2015a). Design and verification for transportation system security. In *Proceedings of 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*.
122. Zheng, K., Zheng, Q., Chatzimisios, P., Xiang, W., & Zhou, Y. (2015b). Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *17*(4), 2377–2396.
123. Zhu, J., & Roy, S. (2003). Mac for dedicated short range communications in intelligent transport system. *IEEE Communications Magazine*, *41*(12), 60–67.

Properties, Principles, and Metrics in Transportation CPS

Syed Hassan Ahmed and Murad Khan

Abstract During the past decades, we have witnessed tremendous advancements in the field of wireless communications, while supporting a wide range of applications. Nevertheless, wireless access has also been shifted towards transportation research and development centers. The integration of embedded devices to transverse heterogeneity into homogeneity, cyber-physical systems (CPS) have been introduced as a subset of the Internet of things (IoT). For example, sensors/actuator systems became responsive to the physical world by enabling real-time control emanating from conventional embedded systems also known as CPS. Likewise, we have several onboard sensors installed inside the vehicles, responsible for sensing different activities within the vehicle and its surroundings such as temperature, intruder detection, and so on. In addition to the general applications for CPS, we have the vehicular cyber-physical systems (VCPS) that is not a new concept. For now, VCPS may refer to a wide range of transportation management systems that are heavily integrated and should be highly accurate, real-time, and efficient. This chapter provides readers with the details of the term "VCPS" followed by the historical overview of this new emerging field including research challenges and future aspects of the VCPS.

Keywords CPS · Vehicular networks · Future research · Architectures

1 Introduction

Transportation systems of the modern world cause several challenges due to lack of reliability and robustness as stated in a recent report by the Transportation Research Board (Washington, DC, 2013). Consequently, the world faces a considerable

S.H. Ahmed (✉) · M. Khan
School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea
e-mail: s.h.ahmed@ieee.org

M. Khan
e-mail: muradkhan23@gmail.com

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_3

amount of accidents and deaths daily. Moreover, the transportation system affects the environment, climate, and energy availability [1]. In the United States, the number of deaths due to road accidents reaches beyond 37,000 per year. Road traffic wastes 2.8 billion (UNIT) in fuel and 4.2 billion hours, while costing 87.2 billion US dollars of the US economy [2]. Thus, it creates a crucial demand to revise the existing transportation system into a more flexible one that can reduce injuries and mortalities caused by road crashes, simultaneously addressing the unnecessary and avoidable environmental impact. The cyber-physical system (CPS) is a suitable candidate to solve a majority of the problems existing in transportation systems. The following section explains CPS modeling.

Computers and software play a vital role in processing raw data to obtain valuable information that helps in decision making. In a car, a variety of computers are used, including engine, seatbelts, brake system, airbags, and steering system, even though they are invisible. Similarly, in a mobile phone the human voice is encoded into digital format and the digital signals converted into radio signals in order to send the signals from the mobile phone to the base station. The washing machine, deep freezer, dishwasher, and printer are some of the household appliances that operate with invisible computers as well as computers and software model robots, power grids, traffic lights, and healthcare services. The creation of toys that can respond to human voice and touch is another application of computers and software. In the modern world, computers are involved in almost all aspects of life. With this popularity, these less noticeable computers and software are called embedded systems and embedded software, respectively. Despite their effect, they have widespread occurrences, but they are only viewed as an information processing source, just like an ordinary computer system.

In the recent past, researchers have identified that embedded systems are in need of specific design and analysis techniques. The embedded systems were considered as minor models of computers since their invention in the 1970s. The major concern with these systems is the resource restriction in terms of memory, energy, and processing speed. The experts focused on improving the system designs to optimize the performance of these embedded systems. In other words, embedded computing is similar to conventional computers in many respects. However, applying conventional computing optimization techniques will not help the optimization of embedded systems.

The researchers revealed that embedded systems mainly suffer from limited resources and incompatibilities with other physical processes. CPS emerged as a solution for these challenges. Figure 1 presents the modeling of a generic CPS. The term CPS was initially coined by Hylen Gill as a core research area. In 2006, the National Science Foundation of the United States introduced fusing computation processes with physical processes. A complete CPS is different from a typical embedded system because it acts as a network that connects the physical devices, that is, input devices and output devices. Technological expansions strengthen the bond between computation and physical elements owing to intelligent mechanisms that subsequently, increase the adaptability, functionality, reliability, usability, security, and independence of CPS.

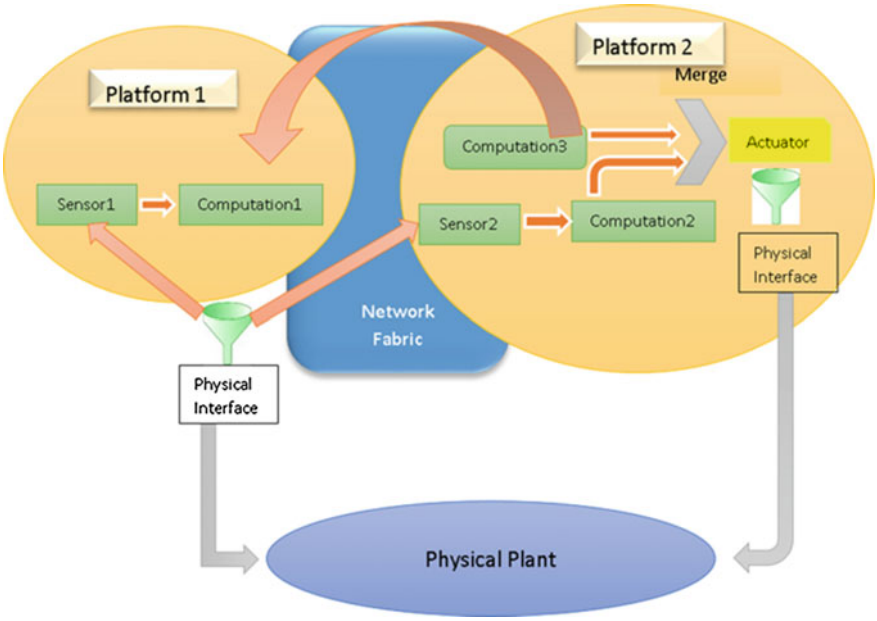

Fig. 1 CPS generic architecture

CPS can be described in a functional as well as formational perspective. In the functional point of view, CPS controls the physical environment with the aid of feedback tools. According to the formation perspective, CPS can be described as a collection of embedded systems and network components. Modern cars create a network environment to communicate with others using over 100 electronic components including FlexRray and CAN bus.

Modern vehicles enable a variety of control functions including engine control, body control, chassis control, and safety features. Engine control is the most important, and is liable for speed and throttle control. Air-conditioner control, mirror, and lock controls are sub-features of body control. The safety features include warning of lane patrol control. A majority of the functionalities are associated with sensors, controllers, and physical devices. CPS in the vehicles are known as vehicular CPS (VCPS) and they use a closed round feedback algorithm.

Traditional cars use an amalgamated software model so that each ECU performs one function. Therefore, the number of ECUs increases by using such an architecture, which not only increases the cost of the car, but makes the maintenance of the car harder. Moreover, different vendors provide most of the car interior components. It forms an embedded computing environment that consists of heterogeneous subsystems. Thus it is difficult to design an architecture that effectively and reliably manages the whole system [3].

Automotive component suppliers and manufacturers began to understand the need of a unified model after the proposal of models such as AUTOSAR and OSGI. At the start automotive software was considered services in order to improve the

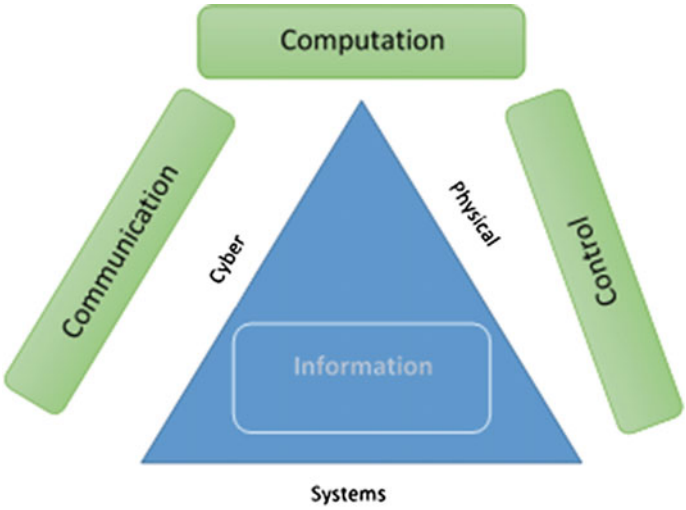

Fig. 2 3C modeling for CPS

reusability and maintainability of the software that appears [4]. According to the new software development model, services are independent of software and hard; this is known as service-oriented architecture (SOA). It has grabbed the attention of both researchers and industry. The proposed architecture has many advantages in distributed software development and heterogeneous system integration. In recent years, the architecture has been applied to e-commerce, a business process model, and enterprise information construction, but it has a limited use in real-time systems, Internet of things, and embedded systems development.

Generally, CPS is the interaction of the physical and cyber worlds. CPS receives the data from a physical component through sensors, processes the data, and then accordingly affects and changes the physical component. The authors in [5] discussed the concept of the CPS as "3C": communication, computation, and control, whereas "information" resides in the center of 3C. The blending of 3C provides sensing of real-time, active control and information in large-gauge systems such as illustrated in Fig. 2.

CPS are closely related to wireless sensor embedded systems and wireless networks, but they have their own distinctive features as well, for example, the demand of high trustworthiness in the system, the changing aspects, and complications involved in the environment.

2 Principles of CPS in Transportation

CPS transform the way people interact with transportation systems, which include aeronautics, rail, and automobile. They ensure the best possible communication between physical devices. For example, in the case of a driverless car, they securely

communicate with each other on smart roads, and airplanes coordinate with each other to minimize delay. In the following section, we explain the role of CPS in vehicular communication.

2.1 Highway Transportation Cyber-Physical Systems

They provide efficient, safe, and reliable highway transportation systems, which consist of connected vehicles, infrastructures, people, and goods in an energetic and inexpensive budget. In highway transportation CPS are connected automated vehicles (CAVs), the combination of both connected vehicles (CV) and automated vehicle systems.

2.2 Metrics for Integration of CPS in Vehicular Networks

CPS facilitate development of a variety of applications and services owing to communication, computation, authentication, sensing, and actuation devices [6]. CPS are the real-time integration of computational capabilities into physical systems. Thus, they enable the physical system to offer the best services to the recipients. Healthcare, aerospace, transportation, environmental control, and weather forecasting systems are some of the potential applications.

As our emphasis is to explain ITS (intelligent transportation systems), therefore, vehicular communication is considered to explain the issues in ITS, because they have proven their mettle in the field of comfort and safety applications built on the top of them. Vehicular ad hoc networks (VANET) or connected vehicles or Internet of vehicles are the networking infrastructure for the transportation of highway CPS. CV are formed by the combination of fast-moving vehicles connected by a self-manageable network. This has the most potential and is one of the most researched areas of ITS. It mostly prefers the following two types of wireless communication: vehicle to vehicle (V2V) communication (this type of communication occurs between vehicles), and vehicle to infrastructure (V2I) communication (this type of communication takes place between vehicles and the units installed at the roadside). In CV the network topology changes rapidly due to the high speed of vehicles. This mobility affects the lifetime of the link and the density of the network as well. Consequently, these challenges make the job of CV difficult to maintain their proximity information with minimum information interchange. CV are an ad hoc type of network; they don't have any pre-established network infrastructure. Therefore, the fast-moving vehicles, nodes, and the roadside units create the highly dynamic and large network infrastructure. In the network, each vehicle is equipped with wireless technology to exchange or broadcast its information to other nodes in the network. Wireless technology, which has been used by the vehicles, is dedicated

Table 1 Categorization of connected vehicles

Category	Application
Safety	V2V communications for safety
	V2I communications for safety
Mobility	Real-time data capture and management
	High mobility applications
Environmental	Applications for the environment: real-time information synthesis (AERIS)
	Road weather applications for CV

short-range communications (DSRC) or wireless access in vehicular environment (WAVE) [7], WiMAX, cellular, and satellite [8].

The CV-based applications are categorized as safety, mobility, and environmental applications [9]; see Table 1 for a brief discussion.

It is a specialized type of generic MANET, in which vehicles move randomly and at high speed as well. This feature makes VANET less static, but more reliable for applications running over it. These factors force us to differentiate VANET from MANET; consequently, it demands precise protocols, model, tools, and applications to handle the issues efficiently.

2.3 Reliability in VCPS

Vehicles have onboard computers as well as mobile devices such as smartphones and tablets. Deployed mobile sensors can determine travel delay along the travel path. In addition to wireless communication devices dedicated to Wi-Fi, WiMAX, 3G, and 4G-LTE, vehicles in VANETs have a DSRC device. Thus, we can assume that future smart vehicles will be well equipped with multiple smart devices, wireless communication devices, cameras, accelerometer, gyroscope, and a vehicle computer. By the end of 2018, the marketing giants of vehicle manufacturing are planning to release vehicles that include DSRC devices. The importance of a DSRC-equipped vehicle is that they can act as packet forwarders and packet carriers when transmitting a data packet to a relay node or a destination vehicle.

2.3.1 Distributed VCPS Applications

VANET improve the safety of passengers by enabling the development of a wider range of applications to support passengers to avoid risks such as fog, rain, icy roads, and the like. In addition to emergency conditions, it enhances safety by facilitating safety entrance, safety exit, safety turns, dangerous obstacle avoidance, adaptive traffic signals, and traffic rerouting during rush hours. In the following case study, VANET avoid accidents by assisting drivers to take care regarding the dangers or obstacles on the road ahead; moreover, in case an accident takes place,

Fig. 3 Generic VANET scenario

they perform analysis of the cause, and provide reasons behind the occurrence of the accident, as illustrated in Fig. 3.

By using more imagination, passengers can seamlessly switch between different transportation models such as air, bus, car, train, motorcycle, or taxi as per their requirements to reach their destination. This type of transportation helps to save both money and time of passengers.

Suppose A wants to travel to B by car. CV make A aware of a traffic jam on the way to the destination, which could not only waste time but money also. It suggests A to park the car at "Par" for X Euros/hours, take a train at nearby station S which departs at Y PM, then from the next nearby station take a bus that departs at M PM, which will lead to the destination B. This kind of approach leads to a better experience for passengers [10].

In the application, CV consist of a number of distributed applications. They use different communication paradigms simultaneously, including peer-to-peer, client-server, and publish-subscribe.

(1) It should run on different networks with different devices.
(2) It should offer time- and location-based services.

2.3.2 Driverless Vehicles

Driverless vehicles are also known as autonomous vehicles and self-driving vehicles. They can perform steering, braking, and accelerating operations without the driver's input. Therefore, drivers do not have to monitor the road continuously when the vehicle is operating in self-driving mode. Five levels of self-driving modes have been defined by the National Highway Traffic Safety Administration (NHTSA), as presented in Table 2.

Table 2 NHTSA definitions of automation levels

Level Index	Level name	Definition
Level 0	No automation	Driver performs all the operations of vehicle manually—all the time
Level 1	Function-specific automation	This level of automation performs one or more specific control functions
Level 2	Combined function automation	This level of automation performs one or more specific control functions to work in coordination, and allows the driver to take care of those
Level 3	Limited self-driving automation	At this level control is relinquished under certain environmental and traffic conditions for safety-critical functions. Thus in those conditions the driver has to trust the vehicle to take care of changes and relinquish control to the driver after the transition. Control is occasionally offered to the driver, but with adequate transition time. The Google car is an example of limited-self driving automation
Level 4	Full self-driving automation	This monitors the road and performs safety measures of driving autonomously. Initially, the driver has to provide the destination. The rest of the operations throughout the journey are controlled by the automated driver. It includes both occupied and unoccupied vehicles

2.3.3 Aviation Cyber-Physical Systems

In 2003, the United States proposed a satellite-based new-generation air transportation system [11]. The beauty of this technology is that it precisely informs pilots about the positioning of other aircraft around them to allow safe flying for more aircraft. Moreover, this technology enables pilots to reach an airport more professionally. Once the planes are on the ground, using this technology helps planes get to the gate sooner [4, 12, 13].

Air traffic administration has integrated the physical world, which includes the airplane and the environment in which it resides, with the control algorithm, traffic control managers, and pilots [14]. MIT researchers proposed an algorithmic solution in order to make flying more efficient by reducing the time spent by flights on engines while taxiing to the runway and avoiding congested conditions at the surface of airport on arriving [9, 15].

2.3.4 Cloud Computing for Transportation Cyber-Physical Systems

Cloud computing presents various new factors in the design and operation of CPS, which offers economic growth, reducing the risk involved in gathering and disaggregating behaviors dynamically. It also helps to amalgamate and share physical hardware among different applications in order to reduce power utilization, autoscaling, communication, heat generation, and sensing and actuation resources

on demand. It ensures that CPS could use an optimal number of resources without experiencing cost when resources are idle [16]. To get the full benefits of both CPS and cloud computing, the architecture of the cyber-physical cloud computing (CPCC) framework integrating the characteristics of CPS and cloud computing in a single framework, has been perceived. The framework consists of a system environment that can be built, modified, and facilitated into auto scale CPS grouping of a set of cold-based processing, sensor, data, and processing services. The CPCC framework supports the development of enterprise-scale and data-intensive systems. It involves a complex decision-making, distributed system, which helps to achieve the vision of smart networked systems and societies (SNSS) or CCPS. The objectives of using a CCPC framework are: efficient utilization of resources, modular design helping to provide modularizeability, scalability, rapid development, adapting to the environment smartly, resiliency, reliability, and providing user-demanded performance [17]. Cloud computing supported by an elastic infrastructure is proposed for the development of large-scale CPS [18].

3 Future Research Roadmap

3.1 Reliability Challenges in CPS Communication

All the ITS-based applications are built on the top of VC, nevertheless, VC is more unreliable and unstable due to high mobility and movement of the nodes.

It imposes obstacles for the safety and comfort applications based on ITS. The comfort applications include video streaming or finding the desired location nearby and demanding a stable network underneath it, whereas safety applications such as emergency alert need real-time quality of service. Due to the high speed of vehicles, there is a very short interaction time between them, especially when they are moving in opposite directions. It has proven that they interact for a couple of seconds if each vehicle has a communication range of 100 m and moving with the speed of 40 m/h, especially when they are moving in opposite directions [19, 20].

Hence, it is concluded that only V2V communication is enough to establish a network for the application, which we presented earlier. It forces the researcher to develop multihop communication in a VC, where the VC is not only based on V2V communication, but also on V2I and vehicle-to-broadband cloud communication (V2B) [11]. In the communication of V2I, fixed infrastructure has been implanted. Apart from implanting new infrastructure, existing traffic control systems can be used for V2I communication.

CV use heterogeneous networks seamlessly, such as Wi-Fi 802.11 (a/b/g) through hotspots, cellular networks (e.g., 2G, 3G, or 4G), and dedicated infrastructure including RSUs through 802.11p and WAVE. In order to perform such seamless connectivity between different networks brings challenges to researchers to develop reliable applications that can switch without causing any delay and

overhead to the application itself. Following are the list of challenges faced by reliable and stable CV communication for ITS applications:

- V2V communication alone is not sufficient for reliable communication therefore it needs V2I communication as well for achieving reliability among the applications.
- Inasmuch as traffic is highly dynamic VC protocols should be adaptive enough to manage high traffic dynamicity. Most of the mobile ad hoc network protocols are designed by considering dense traffic situations, which make them unreliable and even more vulnerable to sparse network traffic; for example, the CAR protocol will not work if it doesn't experience a dense traffic environment. Nevertheless the car should have alternative ways to send the data packets in case it experiences space or no traffic conditions at any point in time [21, 22].
- The problem of seamless interoperating among heterogeneous networks needs to be addressed in network protocol design; currently traditional protocols consider either Wi-Fi (802.11 a/b/n/g) or DSRC 802.11p alone. Therefore, protocols need to be designed that are independent of the network types, so that they can switch to any network type at any point in time, in order to achieve better reliability [20].

3.2 Challenges Involved in Verification and Validation of Distribution Applications

It is very complex to model traffic mobility by using a single model. It requires different traffic situations that occur in real traffic systems, are missing and should be addressed while designing the protocol for traffic mobility. It also requires testbeds or a testing platform to validate and verify the reality of the protocol. The dream comes true by integrating real-world maps and traffic traces with the model [23, 24].

3.3 Challenges for Transportation Cyber-Physical Systems

The CPS complexity is rapidly increasing due to advancements in the requirements. In order to provide improvements and elasticity, it is essential to understand the role of software in terms of hardware operation, which is an important task. Adding additional lines of code might be observed as essentially free, hence the development with the fixed cost payback over many systems and many years. Nevertheless, the additional complexity does achieve at a huge cost, particularly if the certification budget of the safety-critical application is taken into account [25–27]. Transportation CPS, by nature, are safety critical, and current practices, which are

considered the best for development of safety-critical and certification systems are not capable of handling the desires to add networks, adaption, and distribution to CPS.

4 Conclusion

Transportation is an important application domain of CPS, where the physical processes are tightly bound with networked computing. As the Internet has changed the interaction patterns between information and people, VCPS have changed the interaction patterns between people and transportation systems. The optimum VCPS should offer safe, secure, reliable, lucrative, and flexible solutions in rapidly changing environments. The efficiency of VCPS relies on data-intensive computing. Cloud computing has the capability to enable optimal operation of VCPS compared to a conventional network of a local server and personal computers used for data storing, managing, and processing. Conclusively, we believe that many academic and industrial projects will be initialized to bring vehicular CPS into reality likewise the traditional ad hoc networks. In future, it is expected that vehicular CPS will play a vital role in developing smart cities.

References

1. Ahmed, S. H., Kim, G., & Kim, D. (2013, November). Cyber Physical System: Architecture, applications and research challenges. In *Wireless Days (WD), 2013 IFIP* (pp. 1–5). IEEE.
2. Broy, M., Kruger, I. H., Pretschner, A., & Salzmann, C. (2007). Engineering automotive software. *Proceedings of the IEEE, 95*(2), 356–373.
3. Broy, M. (2005, July). Automotive software and systems engineering. In *Proceedings. Third ACM and IEEE International Conference on Formal Methods and Models for Co-Design, 2005. MEMOCODE'05.* (pp. 143–149). IEEE.
4. Abid, H., Phuong, L. T. T., Wang, J., Lee, S., & Qaisar, S. (2011, October). V-Cloud: vehicular cyber-physical systems and cloud computing. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (p. 165). ACM.
5. Ahmed, S.H., Bouk, S.H., Kim, D., & Sarkar, M., (2015). Cyber-physical systems: Basics and fundamentals. In *Cyber-Physical System Design with Sensor Networking Technologies*, p. 21.
6. Korkmaz, G., Ekici, E., & Özgüner, F. (2006). A cross-layer multihop data delivery protocol with fairness guarantees for vehicular networks. *IEEE Transactions on Vehicular Technology, 55*(3), 865–875.
7. Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE, 99*(7), 1162–1182.
8. Benslimane, A., Taleb, T., & Sivaraj, R. (2011). Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G heterogeneous wireless networks. *IEEE Journal on Selected Areas in Communications, 29*(3), 559–570.

9. Ganti, R. K., Ye, F., & Lei, H. (2011). Mobile crowdsensing: current state and future challenges. *IEEE Communications Magazine, 49*(11), 32–39.
10. Ran, B., Jin, P. J., Boyce, D., Qiu, T. Z., & Cheng, Y. (2012). Perspectives on future transportation research: impact of intelligent transportation system technologies on next-generation transportation modeling. *Journal of Intelligent Transportation Systems, 16* (4), 226–242.
11. Saad, W., Han, Z., Hjørungnes, A., Niyato, D., & Hossain, E. (2011). Coalition formation games for distributed cooperation among roadside units in vehicular networks. *IEEE Journal on Selected Areas in Communications, 29*(1), 48–60.
12. Jaworski, P., Edwards, T., Moore, J., & Burnham, K. (2011, October). Cloud computing concept for intelligent transportation systems. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)* (pp. 391–936). IEEE.
13. Li, Z., Chen, C., & Wang, K. I. (2011). Cloud computing for agent-based urban transportation systems. *IEEE Intelligent Systems, 26*(1), 73–79.
14. Poovendran, R. A. D. H. A. (2010). Cyber–physical systems: Close encounters between two parallel worlds [point of view]. *Proceedings of the IEEE, 98*(8), 1363–1366.
15. Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. *Communications of the ACM, 51*(1), 107–113.
16. Simmon, E., Kim, K. S., Subrahmanian, E., Lee, R., De Vaulx, F., Murakami, Y., et al. (2013, August). *A vision of cyber-physical cloud computing for smart networked systems*. NIST.
17. Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014, June). Elastic infrastructure to support computing clouds for large-scale cyber-physical systems. In *2014 IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC)* (pp. 56–63). IEEE.
18. Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications, 40,* 325–344.
19. He, W., Yan, G., & Da Xu, L. (2014). Developing vehicular data cloud services in the IoT environment. *IEEE Transactions on Industrial Informatics, 10*(2), 1587–1595.
20. Yan, G., Wen, D., Olariu, S., & Weigle, M. C. (2013). Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems, 14*(1), 284–294.
21. Wan, J., Zhang, D., Zhao, S., Yang, L., & Lloret, J. (2014). Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. *IEEE Communications Magazine, 52*(8), 106–113.
22. Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014, March). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 241–246). IEEE.
23. Bakar, K. A., Ghafoor, K. Z., Mohammed, M. A., Sadiq, A. S., & Lloret, J. (2013). Vehicular cloud computing: trends and challenges. *Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications, 262*.
24. Hussain, R., Son, J., Eun, H., Kim, S., & Oh, H. (2012, December). Rethinking vehicular communications: Merging VANET with cloud computing. In *2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 606–609). IEEE.
25. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587–1611.
26. Kumar, K., & Lu, Y. H. (2010). Cloud computing for mobile users: Can offloading computation save energy? *Computer, 43*(4), 51–56.
27. Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems, 29*(1), 84–106.

Author Biographies

Syed Hassan Ahmed completed his B.S in Computer Science from Kohat University of Science & Technology (KUST), Pakistan and Masters combined Ph.D. Degree from School of Computer Science and Engineering (SCSE), Kyungpook National University (KNU), Republic of Korea. In summer 2015, he was also a visiting researcher at the Georgia Institute of Technology, Atlanta, USA. Collectively, Dr. Hassan authored/co-authored over 90 International Journal articles, Conference Proceedings, Book Chapters, and 2 Springer brief books. From the year 2014 to 2016, he consequently won the Research Contribution awards by SCSE at KNU, Korea. In 2016, he also won the Qualcomm Innovation Award at KNU, Korea. His research interests include Sensor and Ad hoc Networks, Cyber-Physical Systems, Vehicular Communications and Future Internet.

Dr. Murad Khan received his BS degree in Computer Science from the University of Peshawar Pakistan in 2008. He completed his PhD degree in Computer Science and Engineering from the School of Computer Science and Engineering in Kyungpook National University, Daegu, Korea. Dr. Khan has published over 40 international conference and journal papers along with two book chapters in Springer and CRC Press. He also served as a TPC member in world-reputed conferences and as a reviewer for numerous journals such as *Future Generation Systems* (Elsevier) and *IEEE Access*, among others. In 2016, he was awarded the Qualcomm Innovation Award at Kyungpook National University for designing a Smart Home Control System. He was also awarded a Bronze Medal at ACM SAC 2015, Salamanca, Spain, for his distinguished work in Multicriteria Based Handover Techniques. He is a member of various communities such as ACM and IEEE, CRC Press, and so on. His area of expertise includes ad hoc and wireless networks, architecture designing for Internet of things, and communication protocols designing for smart cities and homes, and big data analytics.

Part II
Principles

Privacy Issues for Transportation Cyber Physical Systems

Meng Han, Zhuojun Duan and Yingshu Li

Abstract Transportation Cyber-Physical Systems (TCPS) developed a lot with the advancement of the transportation industry worldwide. The rapid proliferation of TCPS provides rich data and infinite possibilities for us to analyze and understand the complex inherent mechanism that governs the novel intelligence world. Also, TCPS open a range of new application scenarios, such as vehicular safety, energy efficiency, reduced pollution, and intelligent maintenance services. However, while enjoying the services and convenience provided by TCPS, users, vehicles, and even the systems might lose privacy during information transmission and processing. This chapter summarizes the state-of-art research findings on TCPS in a broad sense. First, we introduce the typical TCPS model and their basic mechanism of data communication. Secondly, considering the privacy issues of TCPS, we give a bird's-eye view of the up-to-date literature on the problems and privacy protection approaches. Thirdly, we point out the most recently emerging challenges and the potential resolutions for privacy issues in TCPS.

1 Introduction

Cyber-physical systems (CPS) are integrations of computation, networking, and physical processes [1]. CPS research has formally commenced since the National Science Foundation (NSF) awarded large amounts of funds to a project titled, "Science of Integration for Cyber Physical Systems" in 2006. More than 300 research and development CPS projects covering the theories, methods, tools, platforms, and the like were launched along with the support of the NSF. Then IBM proposed their

M. Han
Department of Information Technology, Kennesaw State University, Marietta, Georgia
e-mail: menghan@kennesaw.edu

Z. Duan · Y. Li (✉)
Department of Computer Science, Georgia State University, Atlanta, Georgia
e-mail: yili@gsu.edu

Z. Duan
e-mail: zduan2@student.gsu.edu

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_4

"smart planet" as one strategic solution of CPS application practice in 2009 [2]. In Europe, correspondingly, 658 million euros were invested by the European Union in 2013 to support the "Smart Cyber-Physical Systems" program, targeted at improving the quality and performance of the products and services with innovative embedded information communication technology components and systems [3]. All these programs indicate the huge potential and the development space of CPS.

Transportation represents the movement of people, animals, and goods from one location to another. All automotive, aviation, and rail systems, which belong to transportation systems, play a crucial role in the communication and interaction of our society. The transportation system, formed by automotive, aviation, and rail systems with structural components, has a direct impact on a nation's productivity, environment, and energy consumption. As shown in Fig. 1, modes, elements, and functions are the three main components of transportation. All infrastructure, vehicles, and operation provide freight and passengers the movement by air, rail, road, and water. The integration of traditional transportation systems and CPS gave birth to transportation cyber-physical systems (TCPS). In a typical CPS, physical components are controlled or monitored continuously by discrete computing. A transportation system provides an ample supply of examples of CPS because all automotive, aviation, and rail systems are controlled and monitored by corresponding communications and computations. Therefore, TCPS has become one of the most important CPS to improve our society's efficiency, safety, and stability.

Along with the development of TCPS, more information is generated, transferred, and analyzed within and without a TCPS. All these data are shared and used in more and more applications such as collision avoidance, intelligent traffic control, health-

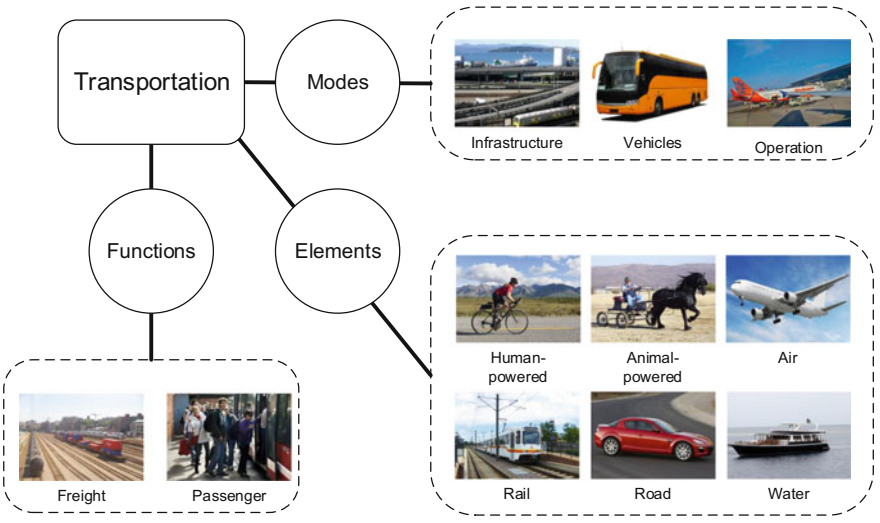

Fig. 1 Transportation represents the movement of people, animals, and goods from one location to another: modes, elements, and functions

care monitoring, and even self-driving vehicles. However, although users are enjoying the convenience and functions brought by TCPS, the security and privacy issues have become important fundamental challenges with respect to usability and safety. Trains, subways, vehicles, and traffic lights are all managed or monitored by some TCPS. That means an electronic intruder potentially could affect vehicle speeds or even cause a horrible collision. It is also conceivable that adversaries or hackers could disrupt all the traffic in a major city and cause chaos by attempting to control all the traffic lights simultaneously to red or to green. With the development of more and more complex TCPS, opportunities and challenges regarding the privacy issues in TCPS are emerging. Therefore, security and privacy of TCPS are attracting more and more attention from both industry and academia. Up to now, NSF in 2016 continued its commitment to securing cyberspace by awarding US$74.5 million in research grants through the NSF Secure and Trustworthy Cyberspace (SaTC) program.

As far as we know, unfortunately, few works comprehensively expound upon and analyze the privacy issues in TCPS. Considering road safety, traffic management, and driver convenience, the work of [4] summarized the security and privacy issues of smart vehicles equipped with recording, processing, positioning, and location devices. This work only considers the very earlier stage of TCPS, and many advanced techniques are not considered. As to the message privacy problems in vehicle-to-vehicle communications, Wu et al. [5] tried to balance safety, privacy, and trustworthiness. Although the concern of privacy is taken into account in [5], it is still communication-oriented research. Most recently, Xiong et al. [6] surveyed the intelligent transportation of CPS and CPSS (cyber-physical social systems) addressing the characteristics, applications, constraints, and challenges. They incorporated social features into traditional TCPS and pointed out several potential research directions. But the work in [6] focuses on the social features, not the privacy issues.

In this chapter, we focus on the latest problems and techniques regarding the privacy issues in TCPS. We not only provide a comprehensive analysis from the viewpoint of computer science, but also in an interdisciplinary way illustrate the various aspects of privacy issues in TCPS. Firstly, we give a bird's-eye view of the development of TCPS and some examples of the typical problems as an introduction in Sect. 1. Secondly, some preliminary knowledge regarding TCPS including fundamental concepts and TCPS architecture are presented in Sect. 2. Thirdly, in Sect. 3, we introduce the general privacy problems, the progress in traditional CPS, and the emerging privacy issues in TCPS. Afterward, we illustrate the most typical privacy goal in TCPS. Then by introducing the features and applicability of different models, we summarize the up-to-date literature in Sect. 4. Then we point out some new challenges and opportunities in this new digital era, and propose a taxonomy that summarizes the state of the art. We also put forward some future directions and possible solutions of the privacy issues in TCPS. Finally, Sect. 5 concludes this chapter.

2 Preliminaries

In this section, we first define a CPS and a TCPS. Then we explain the typical architecture of a TCPS and the corresponding terminologies.

2.1 Cyber-Physical Systems

CPS generally represent physical engineered systems in which the embedded operations are monitored, coordinated, and controlled by a computation and communication center. Similar to the Internet, which transforms interaction and communication among humans through information, CPS attempt to transform the interaction and control of the physical world around us through information. Medical devices, aerospace systems, robotic systems, factory automation, and transportation vehicles with intelligent highways could all be considered as CPS.

As shown in Fig. 2, CPS bring the discrete and powerful logic of computing to the communication and control of the dynamics of physical and engineered systems. The control part of CPS is a predominantly continuous-time system modeled by means of algebraic or trajectories. The communication part is predominantly an

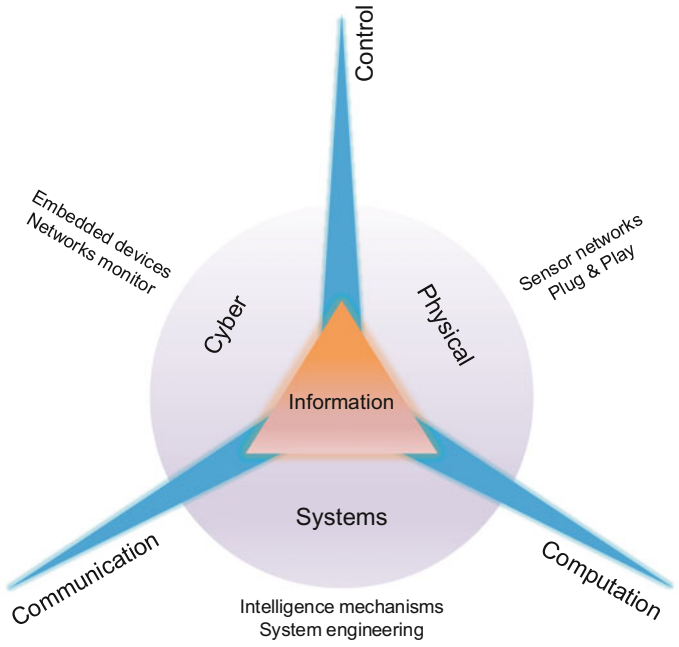

Fig. 2 Three main parts of CPS: communication, computation, and control.eps

interaction system connecting the physical devices, information platform, and the involved people. The computation part is usually predominantly a discrete-event system. Information, as the core of CPS, is the platform and materials for communication, computation, and control. The promise of CPS is also a natural product of the development of several recent trends: (1) the low-cost and increasingly smaller sensors; (2) the low-power, high-performance computing devices; (3) the ubiquitous wireless communication revolution; and (4) the increasing demand for not only interaction and communication among humans but also the control and interaction between the physical world and humans [7]. As well as the further development of all the above, potentialities and challenges of CPS are increasing.

2.2 Transportation Cyber-Physical Systems

We consider physical systems such as automotive, aviation, and rail systems involving communication, computation, control, and physical devices as transportation cyber-physical systems. As an indispensable category of CPS, TCPS focus on monitoring, control, and coordination of all kinds of transportation. Typically, applications, cyberspace, and physical space together construct TCPS as shown in Fig. 3. Cyberspace is a notional environment in which communications over computer networks occur, and the physical space more considers the physical existence in the real world. Based on both cyber and physical spaces, rich applications provide the intuitive recognition to researchers and customers. In this chapter, we pay more attention to the most common transportation on land, and other types of transportation follow similar techniques.

Another very popularly used term related to TCPS is "vehicular ad hoc networks (VANETs)". A VANET could be considered as the precursor of TCPS to a certain extent, but the difference is also significant: (1) TCPS are essentially CPS upon the foundation and application of transportation, whereas a VANET actually is an ad hoc network; (2) MANETs are wireless multihop networks that lack infrastructure, and are decentralized and self-organizing, but TCPS are not limited to any special architecture, and as well as CPS, are very diverse; (3) faithful to the Internet model, VANET applications require point-to-point (unicast) with fixed addressing; that is, the recipient of a message is another node in a network specified by its IP address. TCPS do not just consider connections but also consider the whole system-

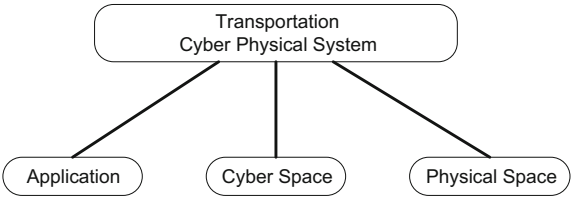

Fig. 3 Application, cyberspace, and physical space construct typical TCPS

level application. However, much research, especially the privacy-related research in VANETs, is also very meaningful to TCPS. VANETs build up the foundation of the communication and computation systems of TCPS, thus most privacy protection mechanisms are worthy of reference in TCPS. The mobility, dynamic, and organization pattern in VANETs are also very similar to those in TCPS, thus the progress in both academia and industry is also valuable for the TCPS study.

2.2.1 Infrastructure of TCPS

All infrastructures such as automotive, aviation, and rail systems could be considered as the foundation of TCPS. These physical manifestations of transportation provide a broad range of infrastructure to support TCPS. Specifically, from land, air to water, different kinds of cars, trains, planes, and watercraft construct the modes of transportation. Roads, bridges, parking places, kinds of stations, airports, and shipyards provide the immobilized support and sustenance to all kinds of motions. The interaction between the mobile and immobile are the infrastructure of cyber networks. Video detectors, microwave detectors, radar detectors, and magneto detectors cause the monitor, control, and communication to happen within TCPS. Multiple sensors employed in roads, bridges, and fixed decks further improve the system ability of transportation.

In TCPS, there are three entities to support control, communication, and computation:

- **Onboard Units (OBUs)**. An OBU is a device, sometimes also called in-vehicle equipment (IVE), installed in a vehicle. An OBU allows the built-in system to collect data through identification of the vehicle and process the collected data that are stored in the OBU's memory. Generally, each OBU is configured or personalized for a specific vehicle.
- **Roadside Units (RSUs)**. RSUs are infrastructure nodes with fixed base stations deployed along the roadside with the goal of increasing the overall coverage of a vehicular network. When a vehicle enters the coverage area of an RSU, it registers with the RSU and receives messages from the RSU. An RSU could be equipped with better hardware than an OBU without strict power and cost constraints. RSUs are expected to enhance network performance and improve propagation delay of messages among several disconnected vehicles.
- **Transportation Control Platform (TCP)**. The TCP actually is a supporting system for both OBUs and RSUs, as shown in Fig. 4. During the communication process, data and information are collected and transferred over the TCP. Without the limitations of time, data, and resources, the TCP could provide comprehensive support to make an optimal decision and apply the optimized strategies to the TCPS.

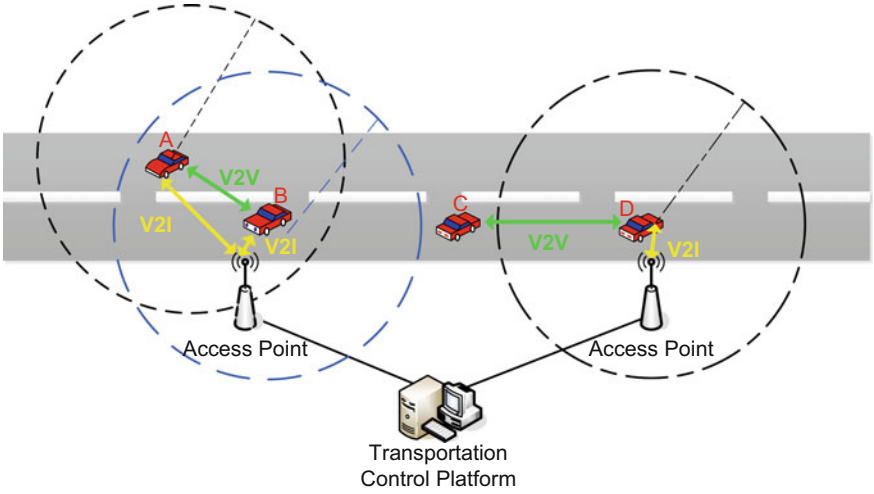

Fig. 4 Three entities in TCPS: the transportation control platform (TCP), the onboard units (OBUs) equipped on vehicles, and the roadside units (RSUs) including the access points

2.2.2 Communications in TCPS

The development of wireless networks is pushing the progress of transportation systems. WAVE/802.11p and ZipBee/802.15.4 are two very typical communication protocols for data collection and transportation because of their improved abilities of data exchange among high-speed vehicles and between the vehicles and the roadside infrastructure. Traditional wireless sensor networks (WSNs) in TCPS play a very important but not conspicuous role. Intuitively, WSNs consist of spatially distributed autonomous sensors to monitor physical conditions such as temperature, sound, pressure, and the like, and to transfer sensed data co-operatively through wireless networks to sink nodes then return to the control unit. The communications in TCPS, in fact, are processed as in a traditional WSN, but should concern mobility. Traditionally, there have been two types of TCPS communications for decades: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. Most recently, more and more mobile devices are installed in a vehicle or carried by a driver. The third type of communication channel is built upon V2I and V2V based on long- distance wireless communication with the support of vehicle manufacturers (Ford, BMW, Tesla, etc.) or mobile service carriers (AT&T, T-Mobile, Verizon, etc.). We call the third type of communication device-to-device (D2D) communication. Different from V2V and V2I, D2D is a multidimension channel that not only provides simple information exchange but also supports the interaction of images, sounds, and GPS location information. Furthermore, with the assistance of smartphone platforms (iOS, Android) based on the mobile service carriers, many location-based services also benefit from the third type of communication and produce many applications (Google Map, Apple Map, etc.). As shown in Fig. 5, in addition to V2I

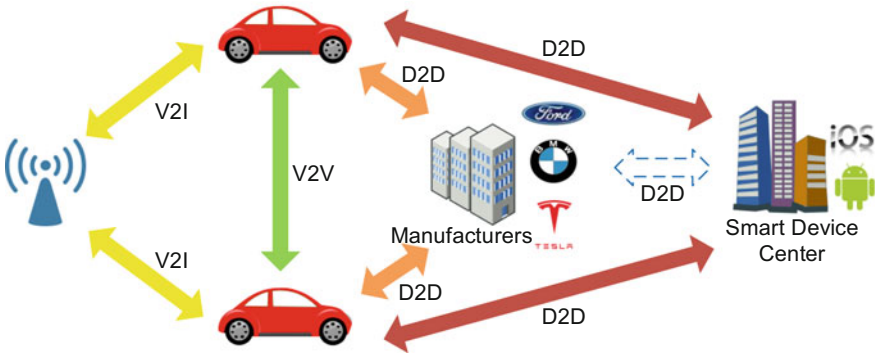

Fig. 5 Three TCPS communications: V2V, V2I, and D2D

and V2V, D2D communication emerges because of the popularization of many kinds of mobile devices (mobile phones, wearable devices).

- **Vehicle-to-Infrastructure (V2I)**. V2I communication allows infrastructure to communicate with vehicles by short-distance touching or monitoring. The infrared-ray sensors or the cameras built into the infrastructure collect data from vehicles. According to the collected data, drivers can be informed regarding weather, traffic conditions, work zones, and even potholes. V2I communication could also be used to co-ordinate signal timing and enhance parking systems for improving traffic flow in urban areas.
- **Vehicle-to-Vehicle (V2V)**. V2V communication allows nearby vehicles to exchange data regarding their positions and use these data to warn drivers of potential collisions. V2V technologies are also capable of warning drivers of potential collisions that are not visible to sensors, such as a stopped vehicle blocked from view, or a moving vehicle at a blind intersection. It is worth mentioning that the term "intervehicle communication (IVC)" system is widely used in industry. Similar to V2V communication, IVC systems are completely infrastructure-free with only OBUs equipped.
- **Device-to-Device (D2D)**. D2D communication is still relatively new in TCPS. But the potential and prospects are great. One reason is more and more vehicle manufacturers try to provide more intelligence support to their product. Tesla, for example, provides many artificial intelligence applications to their customers. The direct connection between a vehicle and the manufacturer allows the monitoring of vehicle health status and the tracking of accidents or theft.

2.2.3 Computation in TCPS

Once monitored and sensed data have been returned to the control unit, more computations are required to direct transportation. Generally, there are two kinds of com-

putations, one carried out online by remote devices or stations such as traffic lights and GPS assistants, and another much more complicated and accomplished in a data collecting center or central control board such as a city traffic control center, airport terminal, and so on. Such decision-support centers comprehensively investigate all the information related to the transportation, then produce excellent and optimal strategy suggestions and decision commands. As shown in Fig. 5, D2D communication and TCPS computation are intimately related. Manufacturers and smart device servers provide computation support with D2D communication.

2.2.4 Applications of TCPS

Generally speaking, the applications of TCPS could be divided into three categories in view of the real-time, resource cost, and computation usage: vehicle-oriented CPS applications, vehicle-infrastructure CPS applications, and infrastructure-oriented CPS applications (Fig. 6).

- **Vehicle-Oriented CPS Applications**. Such applications include collision avoidance, anti-skid control, and autonomous driving among others. All the applications are real-time and safety-critical. Particularly, such an application depends on the requirements from a vehicle itself, and the decisions are also common from a single unit without many communications and computations interacting with other units.

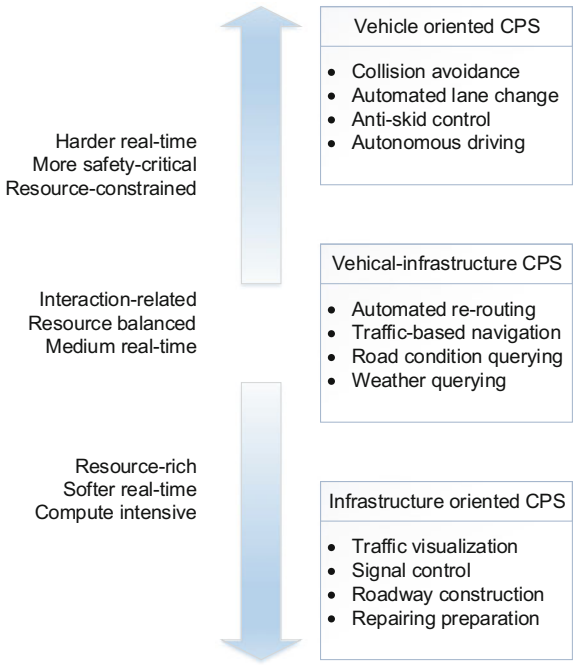

Fig. 6 Three categories of TCPS applications: vehicle-oriented, vehicle-infrastructure, and infrastructure-oriented applications. (*1*) Vehicle-oriented applications have faster reaction ability, and the computation and resource cost need to be very limited due to the constraints of a vehicle. (*2*) Vehicle-infrastructure applications trade off position for mobility and comprehensiveness. (*3*) Infrastructure-oriented applications could take advantage of full usage of data and computation, but it is hard to guarantee the real-time requirement

- **Infrastructure-Oriented CPS Applications**. Correspondingly, such applications emphasize the intensive computations and high-resource cost to produce more advantages and optimal resolutions for a system. Typical applications include traffic visualization, signal control, roadway construction, repairing preparation, and the like.
- **Vehicle-Infrastructure CPS Applications**. In between the above two categories, the third type of application considers both real-time ability and computation comprehensibility. Commonly, communication is emphasized by this category. Example applications include real-time roadway condition queries and weather condition queries.

3 Privacy Issues in TCPS

3.1 General Privacy Issues in CPS

Addressing the privacy requirements in CPS, the work of [8] describes a security engineering method PriS, which incorporates the privacy requirement early in the system development process. The works of [9, 10] present the relative practical frameworks for assessing security risks in CPS. When information is less than perfect, their frameworks could be used to benchmark the security risks. Considering the situation where a motivated and highly skilled attacker may use a multivector attack that exploits the weaknesses of individual components, a framework addressing the combined vector attacks and synchronization/localization issues is proposed in [11]. This framework models the security of CPS in which the behaviors of an adversary are controlled by a threat model that captures the cyber aspects and the physical aspects of the CPS.

The works of [12, 13] discuss the limitations of the current automotive CPS. They particularly propose the privacy issue of georeference data. Although they point out the research direction regarding how to structure data collection and communication in a privacy-preserving environment to enable a functioning human-centric CPS, this issue has not been well investigated till now.

Recently, the work of [14] explores the solutions for the design of CPS through three aspects: models, abstractions, and architectures. Two case studies based on the authors' own experiences are used to analyze the requirements of CPS. The authors point out that the challenges in large-scale CPS applications can be solved by a combination of different disciplines. In a survey work [15], some recent advances in the filtering and control problem for CPS are reviewed under the security and resource constraints. The authors first discuss the security issues: DoS attacks, reply attacks, and deception attacks. Then resource constraints including energy, timing, and communications are surveyed.

3.2 Emerging Privacy Issues in TCPS

Considering the mobility, dynamics, and complexity of TCPS, many privacy issues in TCPS are emerging. We summarize the most typical concerns and problems addressed in the latest literature in the following.

The work of [4] investigates the security and privacy issues in smart vehicles, including road safety, traffic management, and privacy-preserving driver convenience.

The work of [5] proposes a privacy- preserving system considering the balance of trustworthiness, safety, and privacy for VANETs. The innovative idea of the vehicle-to-vehicle communication system in [5] considers a prior countermeasure and an a posteriori countermeasure at the same time. The former could avoid fraudulent messages generated by attackers and a context-aware threshold authentication is proposed to implement it. The latter is able to identify the vehicles that originate and endorse malicious messages. In addition, a batch verification algorithm is applied in message validation that makes the system in this paper outperform previous works. Another related work is the vehicle safety communication technologies, which have many safety benefits in practical applications. The surveillance threats of the VSC technologies aim to make the VSC development community aware of the potential privacy issues. The objective in this type of work is to remind the designers and developers of VSC to consider the value of privacy in the development process.

The work of [16] is the first to study the privacy-preserving traffic volume measurement covering more than two locations instead of only one location as in previous literature. The authors propose a two-location traffic measurement scheme and eventually extend it to a multilocation traffic measurement framework. All the schemes in this paper are based on the combination of VCPS automatic traffic collection and rigorous statistical MLE methodology. Consider the RSU, a secure communication system for TCPS, where a lightweight authentication scheme is designed for vehicles to RSUs and V2V, is proposed [17]. The authors of [17] claim that Sybil attacks could be protected effectively with their secure communication system but it is hard to keep their communication performance with this protection. The work of [18] designs a privacy-enhanced traffic-monitoring framework (SPETM), where RSUs are used to sense information from moving vehicles, threshold-based VMs are able to authenticate vehicles and trace malicious vehicles, and TM is responsible to collect and validate traffic reports. With a threshold-based guarantee trust, many RSUs connecting with vehicles could provide better scalability, but the RSU is still a requested assumption in some other situations. Zhou et al. [19] designed a threshold credit-based incentive mechanism (TCBI) for CV-DTNs (cloud-based vehicular DTNs) which is able to enhance data confidentiality and reliability, prevent node compromise attacks, and resist the layer-adding attack. However, even though the intermediate nodes will receive rewards, they are still a bottleneck. Credit cannot satisfy them.

Most recently, to preserve the privacy of the communications for VANETs according to the conditional anonymous ring signature algorithm, the work of [20] proposes

a protocol that achieves efficient authentication and dispute tracking. Furthermore, the authentication of vehicles does not rely on the RSU or any fully trusted authority.

Based on signatures, which could provide the basic message integrity, authentication, and nonrepudiation, the first category of privacy protection mechanisms is developed as follows. The authors of [21], and also [22], provided a detailed threat analysis and devised an appropriate security architecture. The authors also described some major design decisions still to be made, which in some cases have more than mere technical implications. In [23], the authors proposed a method that uses a set of anonymous keys that change frequently according to driving speed. Each key has a specific lifestyle which only allows one-time usage and expires after its usage. To hamper commonality between pseudonyms and restrict vehicles that cannot hear messages from other groups, the work in [24] proposed a silent period to protect privacy. To further investigate the advantage of signatures, short-lived anonymous certificates are necessary to be developed with the digital signatures. Each vehicle in a TCPS needs to load anonymous certificates in advance to achieve TCPS privacy. In an accident, the signature-based conditional anonymity of pseudonymous authentication could help determine the liability of drivers. However, this category of techniques suffers from the burden of a heavy certificate management and optimization problem. The generation, delivery, storage, and verification of certificates for all the keys result in unaffordable pressure on TCPS.

To mitigate the heavy overhead of signature management, the second category of mechanisms was developed with the help of group signatures. A novel group signature-based security framework was proposed by [25], which relied on tamper-resistant devices for stopping adversarial attacks on TCPS. The authors of [26] presented a security and privacy-preserving protocol for VANETs that integrates group signatures and identity (ID)-based signatures (GSIS). In [26], by integrating the techniques of group signatures and identity-based signatures, a similar framework was proposed to preserve privacy. However, the group member revocation problem becomes a main deficiency in this category. The verification, transmission, and storage costs of group signatures are even higher than traditional signatures. Zhang et al. [27] tried to solve the member revocation problem with an on-the-fly approach, but the assumption that the RSUs need to be fully trusted is not practical.

Some other privacy-preserving methods try to use an identity-based cryptography strategy [28, 29]. A recognizable identity is used by an entity as its public key and a trusted authority will use a master secret to generate a private key for each agent. With replaced pseudonyms for the identity of an entity, privacy is preserved. To achieve unsinkable privacy, in [30], an ideal device that does not allow any attacker to extract any stored data is proposed. But the assumption is too strong to be applied in practice. Even if the assumption could be established that no attackers can probe the inside of an ideal tamper-proof device, as shown in [31], an attacker could still collect substantial information to launch side-channel attacks.

Drawing lessons from the above methods, the one-time identity-based aggregate signature [32] was proposed. The application of information-theoretic measures to anomaly detection was also studied [32, 33]. In [34], the authors assumed that the

simplest explanation of some inconsistency in the received information has the highest probability to be correct; then they proposed a method that could handle both detection and correction of malicious data.

3.3 Privacy Goals in TCPS

In this section, we summarize the following seven privacy goals to be considered in real TCPS design and development. These privacy goals are general outlines for privacy concerns in TCPS, but it is not required to satisfy every goal in a single application. Actually, some of the privacy goals are regarded as interconstraint measures.

- **Identity**. The identity of a vehicle should be protected. It is required that a vehicle should not be traced without all trusted authorities all agreeing to disclose their identities, and the trajectory privacy of vehicles should also be ensured. Different from other privacy goals we illustrate, identity is involved in most other privacy goals, inasmuch as most privacy disclosures are with identity disclosure.
- **Authentication**. Authentication represents privacy protection against impersonation attacks or adversary attacks. Messages in a TCPS should be generated only by the authenticated senders whether the messages are sent by RSUs or OBUs. A typical mechanism of authentication is evaluated by a threshold. The threshold authentication requires a message in a TCPS to be endorsed by at least the number of threshold vehicles' times. The a priori threshold strategy ensures improvement of the confidence of other vehicles in a sensitive message.
- **Anonymity**. Identified entities would result in the loss of vehicles' privacy. If a message originator cannot be identified by communication monitoring, the anonymity goal is achieved. Without an anonymity mechanism, public identity such as the public access key or license plate of a vehicle would be revealed. The lack of anonymity would result in serious privacy disclosure.
- **Traceability**. Anonymity might be utilized by vehicles or other malicious instances to release messages without the worry of being tracked. The authority should allow the identification of a vehicle if necessary. As an opposite role of anonymity, traceability has to reduce anonymity. The balance and tradeoff always exist in our privacy goals.
- **Revocability**. Similar to traceability, revocability represents the feature that an originator and the endorsers of any hazardous message may be identified. Without a valid revocability mechanism, anonymous fake messages could be broadcast to any other vehicle without the possibility of being caught, which would damage public safety.
- **Scalability**. Scalability represents that a system is scalable and can host different levels of data access and workload. Take monitoring as a typical application: the scalability goal requires privacy to be preserved no matter how many vehicles are being monitored in a system.

- **Robustness**. In a dynamic TCPS, robustness requires a system to allow the joining and leaving of any number of vehicles, and privacy could be kept during the whole dynamic process. A system should also be functional even if some vehicles or infrastructure units are compromised or broken.

4 Challenges and Future Directions of the Privacy Issues in TCPS

4.1 Challenges of the Privacy Issues in TCPS

Private information related to any data emitted, collected, or stored should be considered in TCPS.

4.1.1 Personal Identifiable Information

First, a key concept in privacy analysis is personal identifiable information (PII). PII is any information that can be used to distinguish or trace an individual's identity. Therefore, a TCPS needs to determine the extent to which the system will collect or store PII and PII-related information, ensure that there is a legitimate need for this information to meet the goals of the system, and that the data are only accessible and used for these legitimate purposes.

4.1.2 Communication Privacy in TCPS

Communication privacy plays a very important role in TCPS privacy because most data and information are always transmitted from vehicles, infrastructures, or some other terminal devices. The communication process becomes more and more important to protect the privacy of sensitive information.

All V2V, V2I, and D2D messages must be trusted for a system to work. That is, all three types of the received messages must (1) be real and from a vehicle, infrastructure, or personal device in proximity; and (2) convey accurate data about the vehicle, infrastructure, or personal device but with privacy protection. Therefore, considering communication privacy, two emerging challenges are how to develop: (1) methods to validate that the original sender of the message is trusted (authenticity) without compromising privacy of end-users; and (2) methods to prevent the messages from being spoofed or altered (integrity) without compromising privacy of end- users [35, 36]. However, the trusted authorization is hard to develop because we always want to use identity to guarantee truthfulness.

4.1.3 Location Privacy in TCPS

Localization and tracking techniques enable accurate location estimation and tracking of vehicles in TCPS. The benefit of advanced location identification, the information of a vehicle's location history becoming available, raises a new challenge regarding the privacy of a user and a vehicle [37, 38]. Furthermore, the private information of the vehicle's user is also accessible to location-based applications. The work of [39] studies the problem of providing location privacy in TCPS by allowing vehicles to prevent tracking of their broadcast communications. However, as well as the development of modern device applications, only interdicting communication and privacy leaks of vehicle broadcast communication is not enough anymore. How to protect location privacy not only from the V2V and V2I communications but also from the D2D communications becomes an emerging challenge.

4.2 Potential Directions of Privacy Issues in TCPS

Traditionally, TCPS only have two information sources: transportation networks and CPS. With the development of smartphones and wearable devices, as shown in Fig. 7, online social networks become a third information source and this source has taken effect in the integration of a whole TCPS. With online social networks, applications could combine traffic data, weather information, and social event information to provide a comprehensive update to all vehicles and vehicle drivers. These applications

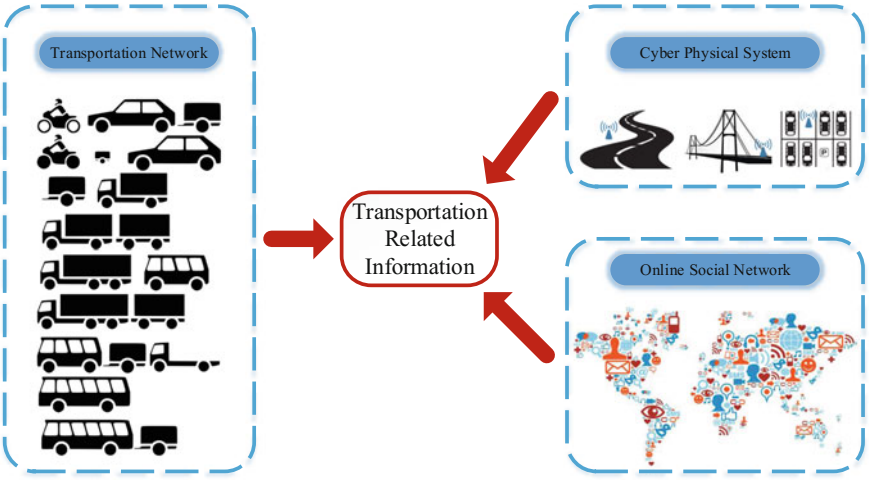

Fig. 7 Transportation networks, CPS, and online social networks are three main sources for transportation-related information

could significantly improve the performance of navigation applications, traffic prediction systems, and strategy decision systems.

4.2.1 Communication Privacy in TCPS

Generally, there are two research directions of the communication privacy problem in TCPS. The first is related to V2I communications, and two main issues need to be taken care of: the privacy of all participating vehicles should be preserved as well as the sensitive information in RSUs; and the communication with infrastructure might result in a large-scale vehicular network, which requires a privacy protection scheme that should efficiently process the big data. Compared with V2V communications, few efforts have been made to protect V2I communications. Without comprehensive information about driving environment changes for drivers, the emerging problems (e.g., highway accidents and traffic jams) are still difficult to be well solved. Most recently, Liu et al. [18] tried to investigate the traffic monitoring application with the consideration of V2I communications. Cryptographic technologies are applied in their system, but still relies on a good communication infrastructure. In real-world situations, however, the communication quality is questionable. Therefore, how to collect in-time information precisely about the driving status of numerous vehicles and the corresponding spatiotemporal occupations on the road in TCPS is still a very challenging issue.

4.2.2 Social-Based Privacy in TCPS

With the emerging of social networks, social media, and social applications, humans are connected and it is much easier to share and get useful information than ever before. Thus, TCPS have increasing influence over an individual's travel decisions and behavior. There are some notable attempts at implementing social transportation systems: (1) Uber, which fulfills over one million rides on a daily basis and currently has over eight million users, is a very popular mobile phone application to help users get a taxi, private car, or rideshare; (2) TCPS are CPS applied to transportation. However, TCPS generally do not quantitatively estimate the impacts from humans, organizations, and societies, which are uncertain, diverse, and complex [6]. Although the CPSS have been proposed by integrating the social components into the CPS [40], the development of the social scenario is still not sufficient to address the many emerging challenges especially the privacy issues in TCPS. The social-based privacy in TCPS involves the right of mandating personal privacy concerning storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the TCPS and Internet. Therefore, social-based privacy in TCPS is a broad direction for future study.

4.2.3 Evaluation of TCPS Privacy

Lastly, the evaluation metrics are also open problems in TCPS. Differential privacy, borrowed from the database field, aims to provide the means to maximize the accuracy of query results while minimizing the chances of identifying privacy and has been investigated for several years in data privacy. However, the limitations of differential privacy are apparent: (1) Differential privacy guarantees that the results of queries on two adjacent query pools cannot be distinguished very well. Although it is a very strong privacy guarantee, it ensures that the presence or absence of any user in the database cannot affect the results very much. In practice, an adjacent query pool is not easy to build or formalize. (2) An important consequence of differential privacy is that composing a differentially private function with any other function that does not depend on the database yields a function that is again differentially private. This assumption requires that even with unknown auxiliary information, an adversary cannot lessen the differential privacy guarantee. However, this is not easy to be guaranteed either. The correlation of many different queries could provide a very high probability to de-anonymize the sensitive information. Therefore, how to evaluate a privacy protection mechanism in TCPS is also a very important future research direction.

4.2.4 More Potential Research Directions

In addition to all the aforementioned directions, there are more potential research directions due to the complexity, dynamics, and uncertainty of TCPS.

- **Complexity and Dimensionality Protection**. Scaling to the full complexity and dimensionality of transportation data is one of the most pressing needs today for privacy protection in TCPS. Research in this area requests a comprehensive understanding of the mechanism and deep insight of privacy issues in TCPS. Thus far, there is still no comprehensive research that considers the complexity and dimensionality in TCPS yet.
- **Verification Architectures of Large-Scale TCPS Privacy Data**. The architecture design is always a big issue, but the solution would resolve the issue fundamentally. Rather than verifying each new transportation system from scratch, developing domain-specific verification frameworks to speed up the verification process with good scalability properties for the industrial setting would be a very valuable topic in the near future.
- **Probabilistic Effects in TCPS**. Taking the probability distribution of the corresponding TCPS into account for the automatic stochastic message communication would be another potential research direction. The likelihood of a certain event would create many novel models to analyze privacy and information transmitting. All these new models could also provide many research opportunities in the next several years.

5 Conclusion

In this chapter, we summarize the up-to-date privacy issues in TCPS. We introduce the pivotal concepts and the architecture of typical TCPS. Overall, the development of reliable transportation cyber-physical innovations and products will continue for a very long time. The privacy issues in all these systems could be more and more important. The debate between privacy attacks and defense schemes will last even longer. There are still many opportunities alongside the challenges.

References

1. http://cyberphysicalsystems.org/.
2. http://www.ibm.com/smarterplanet/us/en/.
3. https://ec.europa.eu/programmes/horizon2020/en/h2020section/smart-cyber-physical-systems.
4. Hubaux, J.-P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine 2* (LCA-ARTICLE-2004-007), 49–55.
5. Wu, Q., Domingo-Ferrer, J., & Gonzalez-Nicolas, U. (2010). Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology*, *59*(2), 559–573. doi:10.1109/TVT.2009.2034669.
6. Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., & Chen, S., et al. (2015). Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica*, *2*(3), 320–333. doi:10.1109/JAS.2015.7152667.
7. Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution (2010).
8. Kalloniatis, C., & Evangelia, K. (2008). Addressing privacy requirements in system design: the pris method. *Requirements Engineering*, *13*(3), 241–255. doi:10.1007/s00766-008-0067-3.
9. Amin, S., Schwartz, G. A., & Hussain, A. (2013). In quest of benchmarking security risks to cyber-physical systems. *IEEE Network*, *27*(1), 19–24. doi:10.1109/MNET.2013.6423187.
10. Amin, S., Schwartz, G. A., & Sastry, S. S. (2013). Security of interdependent and identical networked control systems. *Automatica 49*(1), 186–192. doi:10.1016/j.automatica.2012.09.007.
11. Burmester, M., Magkos, E., & Chrissikopoulos, V. (2012). Modeling security in cyber physical systems. *International Journal of Critical Infrastructure Protection 5*(3), 118–126. doi:10.1016/j.ijcip.2012.08.002.
12. Work, D., Bayen, A., & Jacobson, Q. (2008). Automotive cyber physical systems in the context of human mobility (2008).
13. Work, D., & Bayen, A. (2008). Impacts of the mobile internet on transportation cyberphysical systems: Traffic monitoring using smartphones.
14. Balaji, B., Al Faruque, M. A., Dutt, N., Gupta, R., & Agarwal, Y. (2015). Models, abstractions, and architectures: The missing links in cyber-physical systems.
15. Wang, D., Wang, Z., Shen, B., Alsaadi, F. E., & Hayat, T. (2016). Recent advances on filtering and control for cyber-physical systems under security and resource constraints. *Journal of the Franklin Institute 353*(11), 2451–2466. doi:10.1016/j.jfranklin.2016.04.011.
16. Zhou, Y., Chen, S., Zhou, Y., Chen, M., & Xiao, Q. (2015). Privacy-preserving multi-point traffic volume measurement through vehicle-to-infrastructure communications. *IEEE Transactions on Vehicular Technology*, *64*(12), 5619–5630. doi:10.1109/TVT.2015.2487985.
17. Ashritha, M., & Sridhar, C. S. (Jan 2015). Rsu based efficient vehicle authentication mechanism for vanets.

18. Liu, Y., & Jie, L. (2016). Scalable privacy-enhanced traffic monitoring in vehicular ad hoc networks. *Soft Computing*, *20*(8), 3335–3346. doi:10.1007/s00500-015-1737-y.
19. Zhou, J., Dong, X., Cao, Z., & Vasilakos, A. V. (2015). Secure and privacy preserving protocol for cloud-based vehicular dtns. *IEEE Transactions on Information Forensics and Security*, *10*(6), 1299–1314. doi:10.1109/TIFS.2015.2407326.
20. Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., & Hu, C. (2016). Distributed aggregate privacy-preserving authentication in vanets. *IEEE Transactions on Intelligent Transportation Systems* (99), 1–11. doi:10.1109/TITS.2016.2579162.
21. Raya, M., & Hubaux, J.P. (2005). 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).
22. Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.
23. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., & Hubaux, J.-P. (2007). Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, *25*(8), 1557–1568.
24. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). *CARAVAN: Providing location privacy for VANET*. ESCAR: Proc.
25. Guo, J., Baugh, J. P., & Wang, S. (2007). A group signature based secure and privacy-preserving vehicular communication framework. In P*roceedings of the Mobile Network Vehicle Environment* (pp. 103–108).
26. Lin, X., Sun, X., Ho, P. H., & Shen, X. (2007). GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, *56*(6), 3442–3456.
27. Zhang, L., Wu, Q., Solanas, A., & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions on Vehicular Technology*, *59*(4), 1606–1617.
28. Li, J., Lu, H., & Guizani, M. (2015). ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*, *26*(4), 938–948.
29. Zhang, L., Hu, C., Wu, Q., Domingo-Ferrer, J., & Qin, B. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. In *IEEE Transactions on Computers, to be published*. doi:10.1109/TC.2015.2485225.
30. Zhang, C., Lu, R., Lin, X., Ho, P. H., & Shen, X. (2008). An efficient identity-based batch verification scheme for vehicular sensor networks, In *The 27th Conference on Computer Communications INFOCOM 2008*.
31. Kiltz, E., & Pietrzak, K. (2010). Leakage resilient elgamal encryption, In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 595–612).
32. Eiland, E., & Liebrock, L.: An application of information theory to intrusion detection. In Proceedings of the IWIA (pp. 119–134).
33. Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003). Statistical approaches to DDoS attack detection and response. In *Proceedings DARPA Information Survivability Conference & Exposition* (pp. 303–314).
34. Golle, P., Greene, D., & Staddon, J. (2004). Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad HOC Networks* (pp. 29–37).
35. He, Z., Cai, Z., Cheng, S., & Wang, X. Approximate Aggregation for Tracking Quantiles in Wireless Sensor Networks. The 8th Annual International Conference on Combinatorial Optimization and Applications (COCOA2014).
36. Cheng, S., Cai, Z., Li, J., & Fang, X. (2015). Drawing dominant dataset from big sensory data in wireless sensor networks. In *The 34th Annual IEEE International Conference on Computer Communications (INFOCOM 2015)*.
37. Han, M., Li, J., Cai, Z., & Han, Q. (2016). Privacy reserved influence maximization in GPS-enabled cyber-physical and online social networks ieee international conference on social computing and networking. In IEEE SocialCom 2016, Atlanta, GA, USA, October 8–10 (pp. 284–292).

38. Han, M., Han, Q., Li, L., Li, J., & Li, Y. (Accepted). Maximizing influence in sensed heterogenous social network with privacy preservation. *International Journal of Sensor Networks (IJSNet)*.
39. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). Caravan: Providing location privacy for vanet. Technical report, DTIC Document.
40. Wang, F. Y. (2010). The emergence of intelligent enterprise: from CPS to CPSS. *IEEE Intelligent Systems*, *25*(4), 85–88.

Toward More Secure and Trustworthy Transportation Cyber-Physical Systems

Wenjia Li, Houbing Song, Yehua Wei and Feng Zeng

Abstract Cyber-physical systems (CPS) and cyber infrastructure are key elements of the national infrastructure, and securing them is of critical importance to national security. There is ample evidence that these systems are vulnerable to disruption and damage due to natural disasters, social crises, and terrorism. CPS applications are becoming more widespread, ranging from healthcare with patient monitoring systems to autonomous vehicles to integrated electrical power grids. Within these various application domains, transportation cyber-physical systems (TCPS) have become a very important application of CPS, in which various sensing, computing, and control components, such as in-vehicle onboard sensors, traffic surveillance cameras, smartphones carried by pedestrians, and so on, are tightly coupled to enhance the safety and efficiency of the transportation system. There have been security and safety concerns for the deployment of TCPS, such as the Jeep hack in 2015 and Tesla accident in 2016, which clearly demonstrate the urgent need to secure TCPS better. This chapter discusses how to better safeguard TCPS by means of trust management. We first describe the basic concept of trust management, and summarize its application in generalized wireless networks. Then we discuss in detail how the trust management mechanism can benefit the TCPS in particular.

W. Li (✉)
Department of Computer Science, New York Institute of Technology,
New York, NY 10023, USA
e-mail: wli20@nyit.edu

H. Song
Department of Electrical, Computer, Software, and Systems Engineering,
Embry-Riddle Aeronautical University,
Daytona Beach, FL 32114, USA

Y. Wei
School of Physics and Information Science, Hunan Normal University,
Hunan, Changsha, China

F. Zeng
School of Software, Central South University, Hunan, Changsha, China

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_5

1 Introduction

There are over 1.2 billion vehicles on the roads worldwide, and in 2015, the number of electric vehicles just passed the milestone of 1 million [1]. However, according to the 2012 Urban Mobility Report [2], we are facing a very serious transportation management issue: in 2011, traffic congestion caused Americans to travel 5.5 billion hours more and to purchase an extra 2.9 billion gallons of fuel, costing $121 billion. To make things worse, according to a report released by the World Health Organization [3], the number of road traffic deaths globally has plateaued at 1.25 million a year, which makes road traffic injuries a leading cause of death globally. Hence, it is critical to improve road safety and enhance the efficiency of transportation systems. For instance, the exchange of traffic-related information in a timely and accurate fashion in a road transportation system is critical to accident prevention because prior knowledge of future collisions in as little as one-half second before an actual impact, could lead to a decrease in traffic accidents by as much as 60% [4]. However, the exchange of information also makes the system prone to attacks and more general security-related issues.

There are several major challenges in a transportation system. First, the system is highly distributed and complicated, and manages and controls geographically dispersed assets [5]. The inherent complexity, heterogeneity, and sensitivity to system performance lead to various modeling and design challenges. Unfortunately, there is a lack of an integrated modeling framework to understand traffic management with the consideration of diversified actors and applications. Second, the system inherently operates in the presence of uncertainties or unpredictable behaviors due to intrinsic and extrinsic causes. Uncertainties can be raised by benign faults, malicious attacks, and the like. In addition, weather conditions and other factors can lead to great uncertainty in traffic management. Therefore, the identification and treatment of both faults and malicious attacks must be developed to achieve useful and effective infrastructure. Third, before massively deploying technologies in the field, the security and cost-effectiveness of the developed technologies need to be evaluated and tested. A large number of individual components simulated by different tools must synchronously and mutually exchange information in a collaborative manner. Synchronizing two completely different systems: a continuous time-based simulator (e.g., transportation system) and a discrete event-based simulator (e.g., network simulator) are challenging.

To address these urgent needs, the concept of transportation cyber-physical systems (TCPS) naturally emerged in recent years. Thus far, transportation has already become one of the most important application domains of cyber-physical systems (CPS), which are systems in which physical components are tightly coupled with cyber components such as networking, sensing, computing, and control. The application of CPS in the transportation sector, called transportation CPS, will transform the way people interact with transportation systems, just as the Internet has transformed the way people interact with information.

One TCPS application will be vehicle prognostics, which allows vehicle owners to assess how long the parts in their vehicles will last by continuously monitoring the state of each part via the onboard prognostic systems [6]. In this way, the vehicle owners can be more confident that they will not have any car trouble whenever they start their car. Moreover, drivers today can also get real-time traffic information with the help from TCPS and can thus avoid traffic jams so that they can predict their schedule in a more precise fashion. More important, the drivers can be alerted to an accident occurring in front of them by other vehicles or roadside units (RSUs) nearby so that they can avoid a fatal accident [7]. Finally, in TCPS context, searching for a vacant parking space in a congested area or a large parking lot will no longer be an issue because a smart parking service can provide the drivers with a real-time parking navigation service and the drivers can even reserve parking spots ahead of time [8].

Despite the fact that TCPS is a very promising paradigm that can significantly enhance the overall efficiency and safety of transportation systems, there have been various security concerns that exist in TCPS. For example, in July of 2015, automotive cyber security researchers Charlie Miller and Chris Valasek demonstrated to Wired Magazine how they could remotely hack into a Jeep Cherokee from 10 miles away while it was on the highway [9]. By scanning the US Sprint network for the car's IP address, they were able to access the car's Internet-connected Uconnect service. Uconnect is Chrysler's hands-free communication system, which connects Bluetooth passengers' cellphones, the car's satellite radio, and a number of user-interface systems in the car's dashboard. Unfortunately, Uconnect is connected both to the Internet and to the car's controller area network (CAN) bus control system, exposing the 30–70 unprotected component system controllers to attack. The researchers were able to override the head nodes' firmware and from there they could issue commands to essentially any system in the vehicle. Far beyond the annoyance level of merely toying with the radio, the adversary could issue commands to disable the steering, abruptly engage the brakes, and even turn off the engine. Their demonstration led Chrysler to recall 1.4 million affected vehicles, the first known automotive recall for a cybersecurity vulnerability [10].

Furthermore, the impact of cyber-attacks on transportation systems is severe: it will significantly influence the safety as well as efficiency of the vehicular transportation system. Figure 1 shows one such example. From Fig. 1 we can find that the traffic monitoring and alerting services are very vulnerable to various security attacks, such as the demonstrated jamming attack, which deliberately aims to block, jam, or interfere with legitimate wireless communications. More specifically, the malicious attacker (who can also be called the jammer in this case) can prevent the urgent traffic alert to be disseminated to vehicles on the same road where an accident just occurred by jamming the wireless communication channel, which can lead to severe outcomes such as a widespread traffic jam or even a life-threatening multi-vehicle pileup. Therefore, it is important to secure transportation systems.

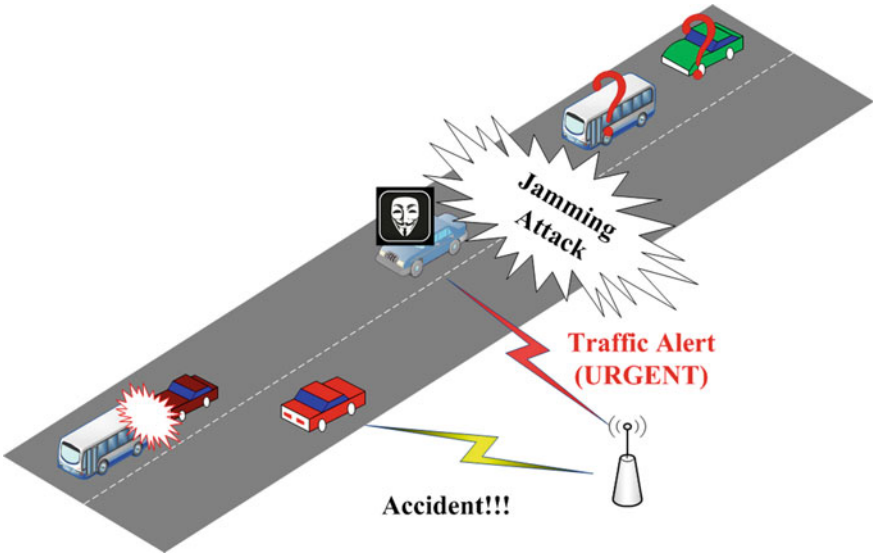

Fig. 1 Example of security threats in vehicular transportation systems

2 Trust Management for Transportation Cyber-Physical Systems

In this section, we aim to provide a comprehensive literature review on various trust management schemes that have been proposed for general wireless networks, which is the key enabling technology for TCPS, and then we summarize some specific research efforts on trust management for TCPS.

2.1 Basics of Trust Management

In general, the goal of trust management is to evaluate different behaviors of other nodes and build a reputation for each node based on the observations made for behavior assessment of other nodes. The reputation can then be utilized to determine trustworthiness for other nodes, make choices on which nodes to work with, and even isolate an untrustworthy node if necessary. The trust management system has been studied for various self-organized systems, such as ad hoc networks [11–13], peer-to-peer systems [14–16], and wireless sensor networks [17–19]. More specifically, trust management in wireless networks can be utilized in the following aspects: (1) node behavior evaluation, (2) misbehaving node identification, and (3) proper response to node misbehavior.

In practice, the trust management system generally depends on two types of evidences to evaluate node behavior. The first kind of observation is called *first-hand* observation, or in other words, direct observation [20]. First-hand observation is the observation that is directly made by a node itself, and the first-hand observation can be collected either passively or actively. If a node promiscuously observes its neighbors' actions, the local information will then be collected passively. On the other hand, the trust management system can also rely on some explicit evidence to assess the neighbor's behavior, such as an acknowledgment packet during the route discovery process. The other kind of observation is called *second-hand* observation or indirect observation. Second-hand observation is generally obtained by exchanging first-hand observations with other nodes in the same network. The main issues of second-hand observations are related to overhead, false report, and collusion [21, 22].

Trust management has been proven to be an important security solution to cope with various misbehaviors in wireless networks, which act as the primary key enabling technology for transportation cyber-physical systems. Therefore, we begin with reviewing the widely used trust management schemes for wireless networks.

2.2 Trust Management for Wireless Networks

In general, wireless networks is compose of a *dynamic* set of nodes that rely on each other to relay packets. Compared with traditional wired networks, wireless networks are more susceptible to malicious attacks and random failures due to their unique features such as limited node energy supply, error-prone communication media, and dynamic network topology. Therefore, security is a key concern for the wide deployment of wireless networks. To address these growing security concerns, various trust management schemes have been studied for wireless networks.

In [23], Buchegger et al. proposed a protocol, namely CONFIDANT (co-operation of nodes, fairness in dynamic ad hoc networks), to promote node co-operation and punish misbehaving nodes. Basically, CONFIDANT has four components in each node: a monitor, a reputation system, a trust manager, and a path manager. The monitor is used to observe and identify abnormal routing behavior. The reputation system calculates the reputation for each node according to the observed behavior. The trust manager exchanges alerts with other trust managers regarding node misbehavior. The path manager maintains path rankings, and properly responds to various routing messages. The main issue with CONFIDANT is that an attacker may intentionally spread false alerts to other nodes that a node is misbehaving while it is actually a well-behaved node. Therefore, it is important for a node in CONFIDANT to validate an alert it receives before it accepts the alert.

In [24], the effect of rumors on the timely detection of malicious nodes and also effectiveness of trust management system was studied. To address the rumor spreading effect, a Bayesian based approach was proposed. In addition, a mechanism was

studied to detect and exclude the possible rumors from the trust management systems.

Michiardi et al. [25] presented a mechanism named CORE to first identify selfish nodes, and then enforce them to co-operate in the following routing activities. Similar to CONFIDANT, CORE uses both a surveillance system and a reputation system to observe and evaluate node behavior. Nevertheless, although CONFIDANT allows nodes to exchange both positive and negative observations of their neighbors, only positive observations are exchanged among the nodes in CORE. In this way, malicious nodes cannot spread fake charges to frame the well-behaved nodes, and consequently avoid denial-of-service attacks toward the well-behaved nodes. The reputation system maintains reputations for each node, and the reputations are adjusted upon receiving new evidence. Because selfish nodes may refuse to cooperate in some cases, their reputations are lower than other nodes. To encourage node co-operation and punish selfishness, if a node with a low reputation sends a routing request, the request will be ignored and consequently the selfish node with bad reputation cannot use the regular network services any longer.

Patwardhan et al. [26] studied an approach in which the reputation of a node in wireless networks is determined by data validation. In this approach, a few nodes, called anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are treated as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Malicious nodes can be identified if the data they present are invalidated by the validation algorithm.

Ren et al. [12] proposed a node evaluation method for Mobile Ad-hoc Networks (MANETs) with the help of trustworthy neighboring nodes, which allows a mobile node to evaluate its neighbors more effectively based on the additional trust information from selected neighboring nodes.

In [27], the authors proposed a cluster-based hierarchical trust management scheme for wireless sensor networks to cope with selfish or malicious nodes, in which the authors consider trust attributes derived from both communication and social networks to evaluate the overall trust of a sensor node. To demonstrate the effectiveness of the proposed hierarchical trust management protocol, the authors apply it to both trust-based geographic routing and trust-based intrusion detection applications. For each application, the authors identify the best trust composition and formation to maximize the performance.

He et al. proposed ReTrust, an attack-resistant and lightweight trust management approach for medical sensor networks [28]. In this approach, the authors delegate the trust calculation and management functionality to master nodes (MNs) which are special nodes with more computational capabilities in medical sensor networks, so that there will be no additional computational overhead for resource-constrained sensor nodes (SNs), which is a critical factor for medical sensor networks. Moreover, the authors also discuss the possibility to use the ReTrust approach to detect and fight against two types of malicious attacks in medical sensor networks, namely on-off attacks and bad mouth attacks.

Chen et al. [29] studied a dynamic trust management protocol for secure routing optimization in delay-tolerant networks (DTNs) in the presence of well-behaved,

selfish, and malicious nodes, in which the concept of dynamic trust is highlighted in order to determine the best operational settings at run-time in response to dynamically changing network conditions to minimize trust bias and to maximize routing application performance. Furthermore, the trust-based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio.

In [30], Wei et al. presented a unified trust management scheme that enhances the security in MANETs using uncertain reasoning which originated from the artificial intelligence community. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, which is also called second-hand information that is obtained from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory (DST), which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method.

Ren et al. [31] proposed a novel trust management scheme for unattended wireless sensor networks (UWSNs), which are characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party means that the existing WSN trust management schemes are not applicable to UWSNs. To address this limitation, the authors studied a trust management scheme for UWSNs to provide efficient and robust trust data storage and trust generation. For trust data storage, the authors employed a geographic hash table to identify storage nodes and to decrease storage cost significantly. In addition, the authors used subjective logic-based consensus techniques to mitigate trust fluctuations caused by environmental factors. Finally, the authors exploited a set of trust similarity functions to detect trust outliers and to cope with trust pollution attacks.

In [32], an energy-efficient collaborative spectrum sensing (EE-CSS) protocol, based on trust management, was proposed. The protocol achieved energy efficiency by reducing the total number of sensing reports exchanged between the honest secondary users (HSUs) and the secondary user base station (SUBS) in a traditional collaborative spectrum sensing (T-CSS) protocol.

2.3 Trust Management for Transportation CPS

Recently, there have been some research efforts that primarily focus on trust establishment and management for vehicular networks which serve as the primary underlying enabling technology for TCPS.

In general, vehicular networks have their own unique features in addition to those features that are common to the generalized wireless networks. For instance, the traveling velocity for nodes in vehicular networks is generally much higher than those in generalized wireless networks, which makes it even more challenging for

those vehicular nodes to exchange information successfully (such as which nodes are trustworthy or untrustworthy according to their prior interactions and observations) before they move out of the wireless communication range between each other [33]. Moreover, the outcome of successful security attacks in vehicular networks is generally severe or even life-threatening. For example, one compromised vehicle may transmit false hazard warnings to all neighboring vehicles, which can cause a chaotic situation such as traffic jams or even an accident if the false warnings are not properly handled. Moreover a compromised vehicle can forge messages to masquerade as an emergency vehicle so that it can mislead other vehicles to slow down and yield [33].

To address these unique security challenges that are imposed to vehicular networks, various trust management schemes have been studied in recent years. In [34], the authors attempted to address the presence of both malicious and selfish nodes in vehicular networks via the trust management approach. More specifically, a distributed trust model named DTM^2 was proposed based on the Spence's Job Market model which originated from economics. In this model, a sender node transmits a special *signal* with the message that it wants to send. This signal indicates that the message is authentic for the potential receivers. The sender node will have to pay a cost to utilize the signal, which is determined on both the value of the signal and its own behavior. In other words, the more unco-operative or malicious the behavior of the sender node, the more costly the signal will be. By this means, the proposed model discourages sender nodes from behaving in a malicious fashion. Similarly, cooperation of the sender nodes will be rewarded proportionally to the signal's value. By this means, the nodes will be encouraged to cooperative, and the uncooperative behaviors will also be discouraged. This research idea was extended in [35].

Liao et al. proposed a trust-based approach to decide the likelihood of the accuracy of V2V incident reports considering the trustworthiness of the report originator and those vehicles that have forwarded it [36]. In particular, the approach leverages the existing V2I communication facilities to collect vehicle behavior information in a crowdsourcing fashion in order to build a more comprehensive view of vehicle trustworthiness.

The authors in [37] identified that the problems of information cascading and oversampling, which are generally common research problems in social networks, also adversely impact trust management schemes in VANETs. Moreover, the authors also demonstrated that a simple voting approach for decision making can lead to oversampling and yield incorrect results in VANETs. To address this issue, the authors proposed a new voting scheme, in which each vehicle has different voting weight according to its distance from the event. In other words, the vehicle that is closer to the event possesses a higher weight.

Rawat et al. [38] proposed to apply both probabilistic and deterministic approaches to estimate trust for securing vehicular networks. First, the probabilistic approach determined the trust level of the peer vehicles based on received information. The trust level would then be used to determine legitimacy of the message, which would be used to decide whether the message would be considered for further transmission over the VANET or should be discarded. Second, the deterministic approach measured the trust level of the received message by using distances calcu-

lated using the received signal strength (RSS) and the vehicle's geolocation (position coordinate). Overall, the combination of probabilistic and deterministic approaches produce better results compared to individual approaches.

In a recent study conducted by Li et al. [7], an attack-resistant trust management scheme (ART) was proposed for vehicular ad hoc networks in which the trustworthiness in vehicular networks was evaluated separately in multiple dimensions: data trust was evaluated based on the data sensed and collected from multiple vehicles; node trust was determined in two aspects, that is, functional trust and recommendation trust, which indicate how likely it is that a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively.

In recent years, Vehicular Social Networks (VSNs) have become an emerging paradigm in the transportation domain, in which vehicular communication can facilitate large-scale data sharing between drivers and their neighbors. However, malicious users of VSNs can also disseminate false information over the network. To address the security challenges in VSNs, a trust management mechanism is introduced to secure vehicular social data in [39]. More specifically, the authors studied a layered trust management mechanism which benefits from the efficient use of various resources (such as computing, storage, communication), and also explored its deployment in a VSN scenario based on a three-layer cloud computing architecture.

3 Conclusion

In recent years, transportation cyber-physical systems have emerged as a new research paradigm to help improve the overall safety and efficiency for transportation systems. However, TCPS is also very vulnerable to various attacks and security threats. Thus it is critical to secure TCPS. In this chapter, we studied a variety of trust management approaches and their application to TCPS.

References

1. Lutsey, N. (2015, September). Global milestone: The first million electric vehicles.
2. Schrank, D., Eisele, B., Lomax, T., & Tti's (2012). *Urban mobility report* (p. 2012). Texas A&M Transportation Institute: The Texas A&M University System.
3. W. H. Organization (2015). Global status report on road safety 2015.
4. Wang, C., & Thompson, J. (1997, March 18) Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network. US Patent 5,613,039.
5. Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010). Security issues and challenges for cyber physical system. In *Proceedings of the 2010 IEEE/ACM Int'L Conference on Green Computing and Communications & Int'L Conference on Cyber, Physical and Social Computing*, GREENCOM-CPSCOM '10, Washington, DC, USA, (pp. 733–738). IEEE Computer Society.

6. Fleming, B. (2015). Advances in automotive electronics [automotive electronics]. *IEEE Vehicular Technology Magazine*, *10*, 4–11. Sept.
7. Li, W., & Song, H. (2016). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*, 960–969. April.
8. Lu, R., Lin, X., Zhu, H., & Shen, X. (2009, April). Spark: A new vanet-based smart parking scheme for large parking lots. In *INFOCOM 2009, IEEE* (pp. 1413–1421).
9. Greenberg, A. (2015). Hackers remotely kill a jeep on the highway.
10. Greenberg, A. (2015) After jeep hack, chrysler recalls 1.4m vehicles for bug fix.
11. Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J. -P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *Proceedings of the IEEE INFOCOM 2008* (pp. 1238–1246). IEEE.
12. Ren, Y., & Boukerche, A. (2009, June). Performance analysis of trust-based node evaluation schemes in wireless and mobile ad hoc networks. In *Proceedings of 2009 IEEE International Conference on Communications, ICC '09.* (pp. 1–5).
13. Li, W., Joshi, A., & Finin, T. (2010, May) Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach. In *Proceedings of the 11th International Conference on Mobile Data Management. MDM '10.* (pp. 112–121). IEEE Computer Society.
14. Aberer, K., & Despotovic, Z. (2001) Managing trust in a peer-2-peer information system. In *Proceedings of the Tenth International Conference on Information and Knowledge Management* (pp. 310–317). ACM.
15. Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003) The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International Conference on World Wide Web, WWW '03* (pp. 640–651). ACM.
16. Wang, Y., & Vassileva, J. (2003, September). Trust and reputation model in peer-to-peer networks. In *Third International Conference on Peer-to-Peer Computing, 2003. (P2P 2003). Proceedings* (pp. 150–157).
17. Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*(11), 2413–2427.
18. Shaikh, R., Jameel, H., d'Auriol, B., Lee, H., Lee, S., & Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *20*, 1698–1712. Nov.
19. Lopez, J., Roman, R., Agudo, I., & Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: Best practices. *Computer Communications*, *33*(9), 1086–1093.
20. Buchegger, S., Boudec, J. -Y. L. (2003). A robust reputation system for mobile ad-hoc networks. In *Proceedings of P2PEcon*.
21. He, Q., Wu, D., & Khosla, P. (2004, March). Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks. In *Proceedings of 2004 IEEE Wireless Communications and Networking Conference, WCNC '04.* (Vol. 2, pp. 825–830).
22. Buchegger, S., & Boudec, J. -Y. L. (2003). The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In *Proceedings of WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*.
23. Buchegger, S., & Le Boudec, J. -Y. (2002). Performance analysis of the confidant protocol. In *MobiHoc '02: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, New York, NY, USA (pp. 226–236). ACM.
24. Buchegger, S., & Le Boudec, J. (2003). The effect of rumor spreading in reputation systems for mobile Ad-hoc Networks. In Proceedings of WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks. Sophia Antipolis, France.
25. Michiardi, P., & Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, Deventer, The Netherlands, The Netherlands (pp. 107–121). Kluwer, B.V.
26. Patwardhan, A., Joshi, A., Finin, T., & Yesha, Y. (2006, July). A data intensive reputation management scheme for vehicular ad hoc networks. In *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems—Workshops, Mobiquitous '06.* (pp. 1–8).

27. Bao, F., Chen, I. R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management*, *9*, 169–183. June.
28. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). Retrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine*, *16*, 623–632. July.
29. Chen, I. R., Bao, F., Chang, M., & Cho, J. H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems*, *25*, 1200–1210. May.
30. Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology*, *63*, 4647–4658. Nov.
31. Ren, Y., Zadorozhny, V. I., Oleshchuk, V. A., & Li, F. Y. (2014). A novel approach to trust management in unattended wireless sensor networks. *IEEE Transactions on Mobile Computing*, *13*, 1409–1423. July.
32. Mousavifar, S. A., & Leung, C. (2015). Energy efficient collaborative spectrum sensing based on trust management in cognitive radio networks. *IEEE Transactions on Wireless Communications*, *14*, 1927–1939. April.
33. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine*, *46*, 100–109. November.
34. Haddadou, N., & Rachedi, A. (2013, June). Dtm2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks. In *2013 IEEE International Conference on Communications (ICC)* (pp. 1827–1832).
35. Haddadou, N., Rachedi, A., & Ghamri-Doudane, Y. (2015). A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *64*, 3657–3674. Aug.
36. Liao, C., Chang, J., Lee, I., & Venkatasubramanian, K. K. (2013, June). A trust model for vehicular network-based incident reports. In *2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC)* (pp. 1–5).
37. Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., & Nayak, A. (2014). A social network approach to trust management in vanets. *Peer-to-Peer Networking and Applications*, *7*(3), 229–242.
38. Rawat, D. B., Yan, G., Bista, B. B., & Weigle, M. C. (2015). Trust on the security of wireless vehicular ad-hoc networking. *Ad Hoc & Sensor Wireless Networks*, *24*(3–4), 283–305.
39. Chen, X., & Wang, L. (2017). A cloud-based trust management framework for vehicular social networks. In *IEEE Access, 5*, 2967–2980.

Secure Data Dissemination for Intelligent Transportation Systems

Li Sun and Qinghe Du

Abstract Intelligent transportation systems (ITS) integrate communications and information technology into the transportation systems to provide a safer and more efficient driving experience. Transmission security is of vital importance for the deployment of ITS systems in practice. In this chapter, secure data dissemination techniques are studied for relay-assisted vehicular communications towards ITS applications. We first briefly review the state of the art of vehicular networking research. Afterwards, we investigate the secure data dissemination issues for both vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) scenarios exploiting the physical-layer security approach. For the V2I scenario, a distributed source-relay selection scheme with anti-eavesdropping capabilities is proposed, for which a source-relay pair is jointly selected to maximize the achievable secrecy rate. For the V2V scenario, a fountain-coding aided relaying scheme is developed. By using this scheme, transmission security is guaranteed as long as the legitimate receiver can accumulate the required number of fountain-coded packets before the eavesdropper does. To satisfy this condition, a constellation-rotation aided cooperative jamming method is utilized to deteriorate the received signal quality at the eavesdropper. To evaluate the performance of the proposed strategy, a novel metric called QoS violating probability (QVP) is further proposed and analyzed. Finally, in the concluding remarks, we summarize the main contributions of our work, and point out some topics that are worthy of investigation in future studies.

1 Background and Motivations

In the past few years, we have witnessed a large increase in the number of vehicles and critical traffic accidents as well. This calls for the development of intelligent transportation systems (ITS), which integrate communications and information

L. Sun (✉) · Q. Du (✉)
Xi'an Jiaotong University, Xi'an, China
e-mail: lisun@mail.xjtu.edu.cn

Q. Du
e-mail: duqinghe@mail.xjtu.edu.cn

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_6

technology (CIT) into the transportation systems to provide a safer and more efficient driving experience. The vehicular network, as an embodiment of ITS, is a promising application-oriented network for enhancing driving safety, improving traffic management efficiency, and providing infotainment services [1]. The interest in vehicular networking dates back to the late 1980s. Since then, the idea of leveraging wireless technologies for vehicular communications has fascinated researchers around the globe, and great efforts have been made to develop new architectures, protocols, algorithms, and applications for vehicular networks. Many governmental projects or plans have been set up to explore the potential of vehicular wireless communication (VWC), including VSC and VII in the United States, eSafety in Europe, and the ASV series in Japan [1]. From the industrial perspective, several standards have been created, among which the most important ones are the IEEE 802.11p and IEEE 1609 protocol suite. IEEE 802.11p specifies the physical layer (PHY), the medium access control (MAC) layer has features such that the existing IEEE 802.11 can work in vehicular environments, and IEEE 1609 mainly deals with multichannel operation, routing, security issues, and the like. Academic research in the field of VWC is also fruitful, ranging from the modeling of vehicular channels [2] to the development of MAC and routing algorithms [3–7]. In addition, some field trials have also been carried out in many countries for objective performance evaluation [8].

There are basically two types of data dissemination modes in vehicular networks, namely V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure). For the former, vehicles communicate with each other directly through a single-hop or a multihop connection, whereas for the latter, vehicles exchange the information with the fixed infrastructure (called the roadside unit or RSU) that is installed along the roadside. In practice, the data transfer for any source-destination pair can be performed in V2V, V2I, or in a hybrid manner. The proposed ideas and schemes in this chapter can be applied to both V2V and V2I communications.

Although many communication technologies have been devised thus far for wireless networks, it is nontrivial to design a highly efficient data dissemination protocol for vehicular communications. The main challenge comes from the unique feature of the vehicular networks. First, due to the fast movement of vehicles, the connectivity among the vehicle nodes may change frequently, and the resulting network topology is highly dynamic. Second, the propagation conditions for vehicular communications is more complicated compared to traditional wireless systems. The existence of the obstacles such as buildings, trees, and traffic lights will lead to poor channel quality. These two factors make wireless communications for vehicular networks errorprone, which indicates the necessity for developing novel protocols to support the stringent quality-of-service (QoS) requirements in vehicular environments.

To achieve this goal, more and more efforts have been made to enhance the performance of the physical layer (PHY) of the vehicular networks. Among many candidates of physical layer techniques, co-operative communication is widely recognized as a powerful solution. The key idea of co-operative communication is to let the neighboring terminals relay information for each other. In this way, the spatial diversity gain as well as the spatial multiplexing gain can be harvested without the deployment of multiple antennas. Research in co-operative communications was

pioneered by Sendonaris et al. [9]. In [10], several basic co-operative relaying protocols were proposed and their outage performances were analyzed. Since these two seminal papers, a large body of literature has appeared dealing with the relaying protocol design for various systems, and many co-operative techniques have been proposed, including distributed space-time code (DSTC), relay selection, coded co-operation, and collaborative beamforming, among others [11–15]. In vehicular communications, the destination node (either the RSU or a vehicle node) may be outside the transmission range of the source node, however, there are often many intermediate vehicles that can serve as relays. Therefore, the application of co-operative relaying in vehicular communications is an appealing solution to provide reliable end-to-end data delivery. In [4], a relay-aided distributed MAC protocol was proposed to optimize the system throughput and extend the service range of vehicular networks. The key idea is to select the relay node and the co-operative mode adaptively according to the channel quality and the relay positions. In [16], co-operative communication was exploited to improve the performance of routing algorithms, and a path selection criterion was developed to obtain a better tradeoff between end-to-end reliability and energy efficiency. The main drawback of the works [4, 16] is that they did not take into account the impact of some network parameters (such as vehicle density, road structure, etc.) in the protocol design. Aiming at this problem, [17] investigated the collective impact of the internode distance, vehicle density, and transmission range of the vehicles on the access and connectivity probability for vehicular relay networks. In [18], a co-operative data dissemination mechanism was introduced. The authors explored the symbol-level network coding to enhance reception reliability and the content downloading rate.

Common to the aforementioned works is that they mainly focused on the use of co-operative relaying to enhance transmission reliability, improve the end-to-end throughput, or extend the service coverage of vehicular networks. However, the openness of the wireless vehicular channels makes the transmitted data available to unauthorized users as well as the intended receiver. For example, Vehicle A wants to transmit a confidential message to Vehicle B via some trusted relays. Meanwhile, there is some malicious entity within the transmission range that attempts to extract this information. Therefore, guaranteeing the secrecy of the data transmission process is also of vital importance. Existing approaches to securing communications rely heavily on data encryption at the upper layers of the protocol stack. Taking vehicular networks as an example, IEEE 1609.2 specifies the formats for the secure messages and the corresponding encryption/decryption procedure. However, the management and distribution of the secret keys often require a trusted third party as well as complex protocols and system architectures, which is hard to be satisfied in practical vehicular networks. In contrast to the traditional cryptography-based paradigm, physical-layer security (PLS) [19] exploits the characteristics of wireless channels and realizes secrecy via signal design and signal-processing approaches, which have great potential in securing co-operative transmissions for vehicular networks.

Since the pioneering work of [20, 21], more and more attention has been paid to PHY security from an information-theoretic point of view [22–25]. Recently, the secrecy problem was considered under the framework of co-operative networks.

Dong et al. [26] studied the use of decode-and-forward (DF) and amplify-and-forward (AF) relays to enhance the PLS, and [26–28] discussed the co-operative jamming (CJ) technique with sending artificial noise as its core. To reduce the implementation complexity without sacrificing the achievable secrecy performance, relay selection was introduced as an efficient mechanism to fulfill secure co-operation. In [29], an opportunistic selection technique was reported to minimize the secrecy outage probability. Following the idea of jamming, the authors of [30] proposed several schemes to select two relays to protect the legitimate receiver from being eavesdropped, significantly enhancing the performance. Liu et al. [31] also adopted the relay selection and co-operative jamming to secure communications, but the jamming signal was sent from the destination rather than the selected relay.

Although the developed PLS methods in the literature have been shown to be effective in improving the secrecy performance of relay systems, the application of these methods to vehicular networks is not straightforward. First, few of them took the unique characteristics of the vehicular networks into consideration. Second, most of the existing works assumed that there was only one source node having a message to transmit, which simplifies the protocol design but may not be realistic for vehicular applications. Third, almost all of the proposed PLS schemes aim at minimizing the secrecy outage probability (SOP) or maximizing the secrecy capacity (SC). This methodology only focuses on the system secrecy performance from an information-theoretic perspective, ignoring the diverse QoS requirements of data delivery in vehicular applications such as delay, throughput, and so on.

To address the aforementioned issues, we in this chapter propose two schemes for secure data dissemination in vehicular relaying networks. Our contributions are summarized as follows.

- For the V2I communications scenario, we propose a novel source-relay selection scheme with anti-eavesdropping capabilities. Specifically, prior to any frame transmission, a source-relay pair is jointly selected to maximize the achievable secrecy rate. After that, the selected relay assists the source in delivering its data to the destination. The proposed selection scheme can be realized in a fully distributed manner, and the security is guaranteed without using any encryption techniques at the upper layers. The closed-form expressions for the secrecy outage probability and the intercept probability are derived, and the achievable diversity order is also analyzed. Simulation results show that the proposed scheme outperforms the competing counterparts in terms of both the secrecy outage probability and the average secrecy rate.
- For the V2V communications scenario, we develop a fountain-coding aided relaying scheme, for which all the source packets are first encoded with fountain codes and then transmitted over the channels. Based on the characteristic of fountain-coded transmissions, a sufficient number of coded packets have to be successfully received to recover the original data. Therefore, transmission secrecy is guaranteed if the legitimate receiver can accumulate the required number of fountain-coded packets before the eavesdropper does. To satisfy this condition, a co-operative jamming method is utilized to worsen the received signal quality at the

eavesdropper. By applying the constellation rotation approach, the information-bearing signal and the jamming signal are designed carefully to reduce the negative effect of the jamming procedure on the legitimate receiver. To evaluate how the scheme behaves in wireless fading channels, we propose a novel performance metric, the QoS violating probability (QVP), and derive its closed-form expression. Compared to the commonly used metrics in physical-layer security such as secrecy outage probability, QVP can give a more comprehensive performance evaluation for the system, including the delay, the reliability, and the security level.

The rest of this chapter is organized as follows. Section 2 presents the distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks. Section 3 presents the fountain-coding aided strategy for secure vehicular communications in intelligent transportation systems. Finally, we summarize our work and deliver the concluding remarks in Sect. 4.

2 Distributed Source-Relay Selection Scheme for Vehicular Relaying Networks Under Eavesdropping Attacks

2.1 Introduction

During the past few years, vehicular networks have received increasing attention due to their potential in enhancing road safety, improving traffic efficiency, and providing mobile infotainment services [32, 33]. In vehicular networks, the information exchange among the vehicles can typically be performed in two modes, namely V2V and V2I. The V2V communications do not rely on the existence of the central unit, and the vehicles can communicate with each other directly via either single-hop or multihop connections. Comparably, in V2I communications, data are transferred between the vehicle and the fixed infrastructure deployed along the roadside, which is often called the roadside unit in the literature. The co-existence of these two modes makes the vehicular networks a hybrid network that supports both the infrastructure-based and ad hoc communications.

Since the late 1980s, there has been increasing research interest in the field of vehicular networks, from both industry and academia. Thus far, simple and basic solutions at almost all layers have been devised for vehicular communications. Among many candidates of VWC technologies, co-operative communication is widely regarded as a promising solution to enhance the performance of vehicular networks from various layers. Till now, a large body of literature has been devoted to the design, analysis, and implementation of co-operative schemes for various scenarios. In [34], the authors proposed a constellation reassignment scheme at the relay to minimize the symbol error rate at the destination node. In [35], a link adaptive regeneration strategy was developed for decode-and-forward (DF) systems. These works, however, are concerned with the simple scenario where there is only one source and

one relay. For multiple-relay systems, advanced relaying mechanisms such as distributed space-time coding [11], relay selection [36], network coding [37], and collaborative beamforming [15] were investigated to further benefit the co-operative systems. Based on the work of [36], the joint source-relay selection schemes were proposed by [13, 38] for multisource multirelay networks to exploit both co-operative and multiuser diversity.

In vehicular networks, there are often a large number of vehicles that can serve as relays to facilitate both the V2V and V2I communications. Therefore, the application of co-operative relaying in vehicular communications is a natural choice. In [39], a dual-hop intervehicular transmission with relay selection was considered, and the outage performance as well as the achievable diversity order was analyzed. By incorporating a highway mobility model, the authors of [40] proposed a scheme for locating and selecting the optimal relay station for multihop vehicular networks. Whereas [39, 40] mainly focused on the PHY-layer issues, [4] dealt with the relay-aided MAC protocol design for vehicular communications. In [16], the cross-layer routing was studied using a co-operative relaying technique. It was found that co-operative transmission can yield more efficient routes than the competing counterparts in terms of both reliability and energy consumption.

Although there are plenty of schemes proposed thus far to take full advantage of co-operative communications to improve link reliability, increase achievable throughput, extend service coverage, and lower energy consumption, very few works address the security issue for relay-aided vehicular networks, which is also critically important due to the openness of wireless channels. Recently, the secrecy problem in co-operative communications networks has emerged as a hot research topic. For a single-user scenario, a security-embedded opportunistic user co-operation scheme was proposed by Niu et al. [41] to determine jointly whether and with whom to co-operate. In [42], a co-operative jamming strategy was developed, where the artificial noise was sent from the destination node to protect the source message from being captured by the malicious user. For the multiuser scenario, [43] proposed three criteria to select the best user-relay pair to combat eavesdropping attacks. In [44], the impact of both co-operative beamforming and user selection on the security level was investigated. Common to the works [41–44] is that they all assumed there was only one eavesdropper within the considered area. In comparison, [45] studied the relay selection issue for dual-hop networks with multiple eavesdroppers.

Although the aforementioned works have exhibited the potential of physical-layer techniques in securing wireless co-operative networks, all of them assumed that there is only one node having a message to transmit. This assumption simplifies the protocol design and the performance analysis, but may not be realistic for vehicular networks. Different from these works, we in this section consider a more practical scenario where there are multiple sources sharing the same pool of multiple relays. For this scenario, a source-relay selection strategy with anti-eavesdropping capabilities is proposed. The selected source-relay pair is the one that offers the maximum secrecy rate. A significant advantage of the proposed scheme is that it can be implemented in a distributed manner, which is attractive for vehicular networks.

The rest of this section is organized as follows. Section 2.2 presents the system model and introduces the basic assumptions. In Sect. 2.3, we give a detailed description of the proposed source-relay selection scheme. In Sect. 2.4, we evaluate the system performance in terms of the secrecy outage probability, the intercept probability, and the achievable diversity order. Simulation results are shown in Sect. 2.5, from which the superiority of our scheme can be observed. Finally, we conclude our work in Sect. 2.6.

2.2 System Model

As shown in Fig. 1, we consider a V2I communications scenario where K vehicles (source nodes) want to deliver their confidential messages to the RSU (the destination), which is located beyond the transmission range of the vehicles, and thus the direct links between the sources and the destination do not exist. However, there are M trusted vehicles that do not have a message to transmit and can serve as relay nodes to help the sources. Meanwhile, near the destination there exists a malicious node (eavesdropper) that tries to intercept the information intended for the destination. The sources, the relays, the destination, and the eavesdropper are denoted by $S_k(k = 1, 2, \ldots, K)$, $R_m(m = 1, 2, \ldots, M)$, D, and E, respectively. It is noted that $K \geq 1$; that is, there might be several sources having data to transmit at any time instant.

To avoid intervehicle interference and reduce the implementation complexity, we employ a TDMA-based scheduler that selects a single source-relay pair to access the channel during one scheduling unit. (The selection criterion is given in the next subsection.) To facilitate the presentations, we denote the selected source and selected relay as S_{k^*} and R_{m^*}, respectively. After the scheduling is completed, the transmission is carried out in a two-phase manner. Specifically, S_{k^*} transmits its data to R_{m^*}

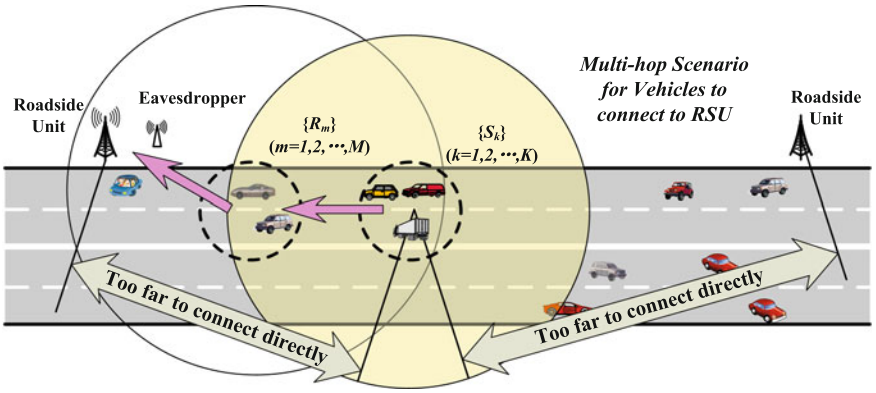

Fig. 1 System model. K sources communicate with the destination via the help of M relays

in the first phase, and R_{m^*} retransmits the received signal to D using the standard AF protocol [10] in the second phase. The destination as well as the eavesdropper can hear the transmission from R_{m^*} and will perform decoding at the end of the second phase. Here we assume that the first phase is secure and the information leakage only occurs during the second phase, which is attributed to the fact the eavesdropper is near the destination and outside the transmission range of the first hop. It is further assumed that the channel state information (CSI) pertaining to the eavesdropper's channels is available at the legitimate nodes. This assumption is commonly adopted in the PHY-security literature such as [22, 26, 46], and can be satisfied in cases where the eavesdropper is active and its transmission can be monitored.

Each node is equipped with a single antenna and operates in a half-duplex mode. All channels are assumed to be independent and modeled as flat block fading, which remain constant within one frame (a two-phase duration) and vary independently from frame to frame. The channel coefficient between node i and node j is represented by h_{ij}, which is a complex circularly symmetric Gaussian variable with mean zero and variance μ_{ij}. That is, $h_{ij} \sim CN(0, \mu_{ij})$. The average transmit powers at the selected source and the selected relay are denoted by P_S and P_R, respectively, and we assume $P_S = P_R = P$ for simplicity. The additive noise at each receiver is modeled as a complex Gaussian variable with mean zero and variance N_0. The notation $\rho = P/N_0$ is used to represent the average signal-to-noise ratio (SNR) of the system.

2.3 *Distributed Source-Relay Selection Under Eavesdropping Attacks*

2.3.1 Selection Criterion

As mentioned above, a single source-relay pair is selected for any frame transmission. According to the principle of the AF protocol and the considered system model, the kth ($1 \le k \le K$) source's received SNR at the destination, with the help of the mth ($1 \le m \le M$) relay, can be expressed as

$$\gamma_{k,m}^{(d)} = \frac{\gamma_{s_k r_m} \gamma_{r_m d}}{1 + \gamma_{s_k r_m} + \gamma_{r_m d}}, \tag{1}$$

where $\gamma_{s_k r_m} = P|h_{s_k r_m}|^2/N_0$ and $\gamma_{r_m d} = P|h_{r_m d}|^2/N_0$ are the instantaneous received SNR at the mth relay from the kth source and that at the destination of the mth relay, respectively.

Similarly, the received SNR at the eavesdropper can be calculated as well by simply replacing $\gamma_{r_m d}$ in (1) by $\gamma_{r_m e}$, where $\gamma_{r_m e} = P|h_{r_m e}|^2/N_0$ is the instantaneous SNR of the link $R_m \to D$. Therefore, the instantaneous secrecy rate, defined as the difference between the achievable rate of the source-destination link and that of the source-eavesdropper link, can be formulated as

$$C_S^{(k,m)} = \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}\right) - \frac{1}{2}\log_2\left(1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}\right)\right]^+, \tag{2}$$

where $[x]^+ = \max(0, x)$. In order to minimize the secrecy outage probability, defined as the probability that the instantaneous secrecy rate falls below a target secrecy rate, our criterion is to select such a source-relay pair (k^*, m^*) that can maximize the secrecy rate in (2). That is,

$$(k^*, m^*) = \underset{1\le k\le K, 1\le m\le M}{\arg\max} \left\{\frac{1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}}\right\} \triangleq \underset{1\le k\le K, 1\le m\le M}{\arg\max} \left\{\gamma_{e2e}^{(k,m)}\right\}. \tag{3}$$

With this criterion, the achievable secrecy outage probability can be expressed as

$$P_{out}^S = \Pr\left[C_S^{(k^*,m^*)} < R_S\right] = \Pr\left[\frac{1}{2}\log_2\left(\gamma_{e2e}^{(k^*,m^*)}\right) < R_S\right] = \Pr\left[\gamma_{e2e}^{(k^*,m^*)} < v\right], \tag{4}$$

where R_S represents the target secrecy rate, and $v = 2^{2R_S}$. Because R_S is positive, v should be larger than 1.

If the global CSI is available at some node, for example, the RSU, the criterion in (3) can be implemented in a centralized manner. However, it is nontrivial to obtain the CSI of all the involved links, especially for the networks with a large number of nodes. This motivates us to develop the distributed algorithm with low complexity, the details of which are given in the next subsection.

2.3.2 Low-Complexity Distributed Scheme

The proposed low-complexity design is based on the observation of (3), which tells us that the achievable secrecy rate is determined by $\gamma_{e2e}^{(k^*,m^*)}$, the maximum of $K \times M$ $\gamma_{e2e}^{(k,m)}$'s. According to the selection criterion in Sect. 2.3.1, $\gamma_{e2e}^{(k^*,m^*)}$ can also be viewed as $\gamma_{e2e}^{(k^*,m^*)} = \max_{1\le m\le M}\{\gamma_{e2e}^m\}$, where γ_{e2e}^m is defined as

$$\gamma_{e2e}^m = \max_{1\le k\le K}\left\{\frac{1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}}\right\}. \tag{5}$$

With the above observation in mind, we can divide the overall selection procedure into three steps. First, every relay node independently evaluates its eligibility for co-operation. After that, each eligible relay selects an appropriate source to maxi-

mize its contribution to the achievable secrecy rate. In this way, all the candidate source-relay pairs are generated. Finally, a single pair with the maximum $\gamma_{e2e}^{(k,m)}$ is screened out from the candidate pairs to access the channel. The details of these steps are given in what follows.

Step1: Generating the Set of Eligible Relays

For any relay node R_m, it can be deduced from (3) that, if $\gamma_{r_m d} < \gamma_{r_m e}$, then $\gamma_{e2e}^{(k,m)}$ will be less than 1 irrespective of the source index k. In other words, the system will be in outage if this relay node is selected to access the channel, no matter which source is chosen to form the pair.

Furthermore, when $\gamma_{r_m d} \geq \gamma_{r_m e}$, the secrecy outage probability, with R_m being the selected relay, can be expressed as

$$\begin{aligned} P_{out}^{S} &= \Pr\left[\gamma_{e2e}^{(k^*,m)} < v\right] \\ &\overset{(a)}{\geq} \Pr\left[\frac{\frac{\gamma_{s_{k^*} r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m d}}}{\frac{\gamma_{s_{k^*} r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m e}}} < v\right] \\ &= \Pr\left[\frac{\gamma_{r_m d}}{\gamma_{r_m e}} \times \frac{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m e}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m d}} < v\right] \\ &= \Pr\left[\gamma_{s_{k^*} r_m}(\gamma_{r_m d} - v\gamma_{r_m e}) < v\gamma_{r_m e}(1+\gamma_{r_m d}) - \gamma_{r_m d}(1+\gamma_{r_m e})\right], \end{aligned} \tag{6}$$

where (a) stems from the fact that $\frac{b+1}{a+1} < \frac{b}{a}$ for $a < b$. If $\gamma_{r_m e} < \gamma_{r_m d} < v\gamma_{r_m e}$, we have $v\gamma_{r_m e}(1+\gamma_{r_m d}) - \gamma_{r_m d}(1+\gamma_{r_m e}) > 0$ and $\gamma_{s_{k^*} r_m}(\gamma_{r_m d} - v\gamma_{r_m e}) < 0$. Therefore, the probability provided by (6) equals 1, implying that the outage event definitely occurs if we choose such a relay to co-operate.

Summarizing the discussions above we can conclude that, to support the target secrecy rate, the selected relay has to satisfy the following condition.

$$\gamma_{r_m d} > v\gamma_{r_m e}. \tag{7}$$

In other words, if the channel gains regarding R_m do not meet (7), R_m cannot be selected. In Steps 2 and 3, we only focus on the eligible relays satisfying (7).

It should be emphasized that the eligibility determination process requires the knowledge of $\gamma_{r_m d}$ and $\gamma_{r_m e}$ at R_m. However, this can be guaranteed because we have assumed that both the RSU and the eavesdropper are active entities that will transmit control information or messages, and the corresponding channel gains can be estimated at the relays using the pilots from the received signals.

Step2: Source Selection at Eligible Relays

After Step 1 has finished, all the relays satisfying (7) broadcast flag signals to declare their eligibility for co-operation. Upon receiving the flag signals, all the sources will send an ACK to respond. With the received ACKs, any eligible relay R_m can estimate $\gamma_{s_k r_m}$ for all $k's$. After that, R_m supposes itself to be the selected relay,

and chooses the "best" source that can contribute most to $\gamma_{e2e}^{(k,m)}$. To elaborate on how to find such a source node, a lemma is introduced first.

Lemma *The function*

$$f(\gamma) = \frac{1 + \frac{\gamma_1 \gamma}{1+\gamma_1+\gamma}}{1 + \frac{\gamma_2 \gamma}{1+\gamma_2+\gamma}}, \tag{8}$$

where γ_1 and γ_2 are two constants with γ_1 being larger than γ_2, is an increasing function of γ.

Proof By taking the derivative of $f(\gamma)$ with respect to γ, we can obtain

$$f'(\gamma) = \frac{(1+\gamma_1)(\gamma_1 - \gamma_2)}{(1+\gamma+\gamma_1)^2(1+\gamma_2)}, \tag{9}$$

which is obviously larger than 0 for $\gamma_1 > \gamma_2$. Therefore, $f(\gamma)$ is an increasing function of γ.

Based on this *lemma*, the "best" source for R_m, that is, $S_{k^*(m)}$, should be the one with the property:

$$\begin{aligned} k^*(m) &= \arg\max_{1\le k\le K} \left\{ \frac{1 + \frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1 + \frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}} \right\} \\ &= \arg\max_{1\le k\le K} \gamma_{s_k r_m}. \end{aligned} \tag{10}$$

Undoubtedly Step 2 also enjoys a distributed implementation inasmuch as the source selection is performed at the eligible relays, and there is no information exchange among different relay nodes.

Step3: Distributed Source-Relay Pair Selection

Upon completion of Steps 1 and 2, we can formulate the expression for the maximum achievable secrecy rate by utilizing the mth relay as

$$C_S^m = \frac{1}{2}\log_2 \left\{ \frac{1 + \frac{\gamma_{s_{k^*(m)} r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*(m)} r_m}+\gamma_{r_m d}}}{1 + \frac{\gamma_{s_{k^*(m)} r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*(m)} r_m}+\gamma_{r_m e}}} \right\}. \tag{11}$$

To select the optimal source-relay pair, we adopt the method based on the distributed timer [36]. Specifically, after calculating C_S^m, each eligible relay R_m will start its timer with the initial value inversely proportional to C_S^m. Therefore, the relay with the largest C_S^m, namely R_{m^*}, has its timer expired first. R_{m^*} then broadcasts the flag signal and the rest of the relays will back off after receiving the flag signal. Noticing

the fact that the "best" source for R_{m^*} has already been determined to be $S_{k^*(m*)}$ in Step 2, we now have the selected source-relay pair.

Remark The proposed source-relay selection scheme has two advantages. It can be realized in a distributed way, yielding a low implementation complexity. This is of practical significance for vehicular networks. In addition, the distributed method, despite its simplicity, is an optimal solution in the sense that it can select the "best" source-relay pair to minimize the system secrecy outage probability.

2.4 Performance Analysis

2.4.1 Secrecy Outage Probability

The secrecy outage probability (SOP) is widely adopted as a performance metric to evaluate the PHY-security protocol in wireless fading channels. As previously mentioned, it is defined as the probability that the instantaneous secrecy rate falls below a target secrecy rate $R_S > 0$. By noticing that the M γ_{e2e}^m's are independent random variables, the SOP can be expressed as

$$P_{out}^S = \Pr\left[\gamma_{e2e}^{(k^*,m^*)} < v\right] = \prod_{m=1}^{M} \Pr\left(\gamma_{e2e}^m < v\right). \tag{12}$$

By combining (5) and (10), γ_{e2e}^m can be expressed as

$$\gamma_{e2e}^m = \frac{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_m d}}}{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_m e}}}, \tag{13}$$

where $\gamma_{s_{k^*(m)}r_m} = \max\limits_{1\le k\le K}\{\gamma_{s_k r_m}\}$.

Therefore, denoting $\gamma_{s_{k^*(m)}r_m}$, $\gamma_{r_m d}$, and $\gamma_{r_m e}$ by X, Y, and Z, respectively, the probability $\Pr(\gamma_{e2e}^m < v)$ can be calculated as

$$\begin{aligned}\Pr\left(\gamma_{e2e}^m < v\right) &= \Pr\left[\frac{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_m d}}}{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_m e}}} < v\right] \\ &= \int_{y<vz} f_Y(y) f_Z(z) dy dz + \\ &\quad + \int_{y>vz} \Pr\left[\frac{1 + \frac{Xy}{1+X+y}}{1 + \frac{Xz}{1+X+z}} < v\right] f_Y(y) f_Z(z) dy dz, \end{aligned} \tag{14}$$

where $f_X(x)$ is the probability density function (PDF) of the random variable X. The intractability of the PDF of γ_{e2e}^m makes it rather difficult to calculate the accurate result of the integral in the second part of (14). Therefore, we resort to the approximation $\frac{\gamma_1\gamma_2}{1+\gamma_1+\gamma_2} \approx \min\{\gamma_1, \gamma_2\}$, which is rather tight for large values of γ_1 and γ_2 [47]. Then, the second part of the right-hand side of (14), denoted by I, is approximated as

$$\begin{aligned} I &\approx \int_{y>vz} \Pr\left[\frac{1+\min(X,y)}{1+\min(X,z)} < v\right] f_Y(y) f_Z(z) dydz \\ &= \int_{vz<y<vz+v-1} f_Y(y) f_Z(z) dydz \\ &\quad + \int_{y>vz+v-1} \Pr\left[X < v(1+z)-1\right] f_Y(y) f_Z(z) dydz. \end{aligned} \tag{15}$$

Combining (14) and (15), the approximate expression for the probability $\Pr\left(\gamma_{e2e}^m < v\right)$ can be given by

$$\begin{aligned} \Pr\left(\gamma_{e2e}^m < v\right) \approx & \overbrace{\int_{y<vz+v-1} f_Y(y) f_Z(z) dydz}^{I_1} \\ & + \overbrace{\int_{y>vz+v-1} \Pr\left[X < v(1+z)-1\right] f_Y(y) f_Z(z) dydz}^{I_2}. \end{aligned} \tag{16}$$

For the considered Rayleigh fading channels, γ_{ij} follows the exponential distribution with the rate parameter $\lambda_{ij} = (\rho\mu_{ij})^{-1}$. Therefore, I_1 in (16) can be obtained as

$$\begin{aligned} I_1 &= \int_0^{\infty} \int_0^{v(z+1)-1} \lambda_{r_m d} \lambda_{r_m e} e^{-\lambda_{r_m d} y - \lambda_{r_m e} z} dydz \\ &= 1 - \frac{\lambda_{r_m e} e^{-\lambda_{r_m d}(v-1)}}{\lambda_{r_m d} v + \lambda_{r_m e}}. \end{aligned} \tag{17}$$

On the other hand, $X = \gamma_{s_{k^*(m)} r_m}$ is the maximum of K independently and nonidentically distributed exponential random variables. According to the order statistics, I_2 in (16) can be simplified as

$$I_2 = \int_{v-1}^{\infty} \int_0^{\frac{y+1-v}{v}} \prod_{k=1}^{K} \left(1 - e^{-\lambda_{s_k r_m}(v(1+z)-1)}\right) \lambda_{r_m e} e^{-z\lambda_{r_m e}} dz \lambda_{r_m d} e^{-y\lambda_{r_m d}} dy$$

$$= \int_{v-1}^{\infty} \int_{0}^{\frac{v+1-v}{v}} \sum_{n=0}^{K} \sum_{\substack{1\le p_1,p_2,\ldots,p_K\le K \\ p_i\neq p_j,\forall i\neq j \\ p_1<p_2<\cdots<p_n \\ p_{n+1}<p_{n+2}<\cdots<p_K}} (-1)^{K-n} e^{-\left(\sum_{k=n+1}^{K} \lambda_{s_{p_k} r_m}\right)\left(v(1+z)-1\right)} \times \left(\lambda_{r_m e} e^{-\lambda_{r_m e} z}\right) dz \times \left(\lambda_{r_m d} e^{-\lambda_{r_m d} y}\right) dy, \tag{18}$$

where we have utilized the multinomial expansion identity given by [48, Eq. (7)]. After some tedious calculations, I_2 can be finally simplified as

$$I_2 = \sum_{n=0}^{K} \sum_{\substack{1\le p_1,p_2,\ldots,p_K\le K \\ p_i\neq p_j,\forall i\neq j \\ p_1<p_2<\cdots<p_n \\ p_{n+1}<p_{n+2}<\cdots<p_K}} (-1)^{K-n} e^{-\sum_{k=n+1}^{K} \lambda_{s_{p_k} r_m}(v-1)} \frac{\lambda_{r_m e} e^{-\lambda_{r_m d}(v-1)}}{\lambda_{r_m e} + \sum_{k=n+1}^{K} \lambda_{s_{p_k} r_m} v} \times \left[1 - \frac{v\lambda_{r_m d}}{v\lambda_{r_m d} + \lambda_{r_m e} + \sum_{k=n+1}^{K} \lambda_{s_{p_k} r_m} v}\right]. \tag{19}$$

Substituting (17) and (19) into (16), the closed-form expression for $\Pr\left(\gamma_{e2e}^{m} < v\right)$ is obtained, and the SOP of the system can also be derived by substituting this result into (12). However, we omit these expressions here due to space limitation. In the next subsection, we show through simulations that the derived theoretical result is tight enough for medium to high SNR values.

2.4.2 Intercept Probability

The intercept probability, which is also a key metric in evaluating the performance of PHY-layer security schemes, is defined as the probability that the capacity of the legitimate link falls below that of the wiretap link [46]. Mathematically speaking, the intercept probability can be expressed as

$$P_{intercept} = \Pr\left[\gamma_{e2e}^{(k^*,m^*)} < 1\right] = \prod_{m=1}^{M} \Pr\left(\gamma_{e2e}^{m} < 1\right). \tag{20}$$

According to the expression for γ_{e2e}^{m} in (13), the event $\gamma_{e2e}^{m} < 1$ is equivalent to

$$\frac{\gamma_{r_m d}}{\gamma_{r_m e}} \times \frac{1 + \gamma_{s_{k^*} r_m} + \gamma_{r_m e}}{1 + \gamma_{s_{k^*} r_m} + \gamma_{r_m d}} < 1. \tag{21}$$

Therefore, $\Pr\left[\gamma_{e2e}^{m} < 1\right]$ can be calculated as

$$\Pr\left(\gamma_{e2e}^{m} < 1\right) = \int_{y<z} f_Y(y) f_Z(z) dy dz + \int_{y>z} \Pr\left[\frac{y(1+X+z)}{z(1+X+y)} < 1\right] f_Y(y) f_Z(z) dy dz, \tag{22}$$

where $X = \gamma_{s_{k^*(m)} r_m}$, $Y = \gamma_{r_m d}$, and $Z = \gamma_{r_m e}$. The probability in the second integral in (22) can be rewritten as

$$\begin{aligned} \Pr\left[\frac{y(1+X+z)}{z(1+X+y)} < 1\right] &= \Pr\left[X(y-z) < z(1+y) - y(1+z)\right] \\ &= \Pr\left[X(y-z) < z-y\right], \end{aligned} \tag{23}$$

which is always zero for $y > z$. By inserting this result into (22), we have

$$\Pr\left(\gamma_{e2e}^{m} < 1\right) = \int_{y<z} f_Y(y) f_Z(z) dy dz = \frac{\lambda_{r_m d}}{\lambda_{r_m d} + \lambda_{r_m e}}. \tag{24}$$

Combining (24) with (20), the exact expression for the intercept probability can be given by

$$P_{intercept} = \prod_{m=1}^{M} \frac{\lambda_{r_m d}}{\lambda_{r_m d} + \lambda_{r_m e}}. \tag{25}$$

2.4.3 Diversity Order

In order to gain some useful insights into system performance, we proceed to analyze the achievable diversity order. Because the intercept probability is not a function of the average SNR, the traditional definition of diversity order is not applicable here. Instead, we adopt the definition of generalized diversity order given in [46], which is formulated as

$$d \triangleq -\lim_{\kappa_{de} \to \infty} \frac{\log P_{intercept}}{\log \kappa_{de}}, \tag{26}$$

where $\kappa_{de} = \mu_{sd}/\mu_{se}$ is known as the main-to-eavesdropper ratio (MER), defined as the ratio of the average channel gain of the source-destination link to that of the source-to-eavesdropper link.

To simplify the discussions, we assume that there is only one source node. Denoting $\mu_{r_m d} = \mu_{sd} \alpha_{r_m d}$ and $\mu_{r_m e} = \mu_{se} \alpha_{r_m e}$, the intercept probability in (25) can be rewritten as

$$P_{intercept} = \prod_{m=1}^{M} \frac{\frac{1}{\rho\mu_{sd}\alpha_{r_m d}}}{\frac{1}{\rho\mu_{sd}\alpha_{r_m d}} + \frac{1}{\rho\mu_{se}\alpha_{r_m e}}}$$
$$= \prod_{m=1}^{M} \frac{1}{1 + \frac{\mu_{sd}}{\mu_{se}}\alpha_m}$$
$$= \left(\frac{1}{\kappa_{de}}\right)^{M} \prod_{m=1}^{M} \frac{1}{\frac{1}{\kappa_{de}} + \alpha_m}, \tag{27}$$

where we have introduced α_m to represent $\frac{\alpha_{r_m d}}{\alpha_{r_m e}}$.

Based on the calculations above, the diversity order can be derived as

$$d = \lim_{\kappa_{de}\to\infty} \frac{M \log \kappa_{de} + \sum_{m=1}^{M} \log\left(\frac{1}{\kappa_{de}+\alpha_m}\right)}{\log \kappa_{de}} = M. \tag{28}$$

2.5 Simulation Results and Discussions

In this subsection, we present the simulation results to validate the proposed source-relay selection scheme. In the following simulations, all the nodes (including the sources, relays, destination, and eavesdropper) are distributed in a 2-D plane. The direct links of $S_k \to D$ and $S_k \to E$ are assumed to be absent for all k's, and the channel gains are modeled according to the system model in Sect. 2.2. To be specific, $h_{ij} \sim CN(0, \mu_{ij})$, where $\mu_{ij} = d_{ij}^{-\theta}$ with d_{ij} being the distance between any node pair (i,j) and θ being the path loss exponent. In our simulations, θ is fixed as 3. Unless otherwise stated, the target secrecy rate R_S is set to be 0.1 bit/s/Hz, and the notation "SNR" is used to represent the ratio of P versus N_0, that is, ρ in the previous sections.

In Figs. 2 and 3, we consider the system with 3 sources and 2 relays: $K = 3$ and $M = 2$. These nodes are uniformly generated in the circle with center (0, 0) and radius 1. The destination and the eavesdropper are located at (2, 0) and (2, 2), respectively. Figure 2 shows the SOP-SNR curves for the proposed anti-eavesdropping selection scheme and the conventional joint source-relay selection scheme [13]. The theoretical result is also given to verify the correctness of the analysis in Sect. 2.4.1. From Fig. 2 it can be seen that, by taking the security constraints into account, the proposed scheme brings nonnegligible gains compared to the conventional scheme, which only considers the channel qualities regarding the legitimate links. In addition, there is an excellent match between the theoretical curve and the simulated one for medium to high SNR values, implying the soundness of the theoretical analysis.

In Fig. 3a, we compare the ergodic secrecy capacity of the proposed scheme (C_1) and that of the conventional scheme (C_2). To illustrate the capacity loss incurred

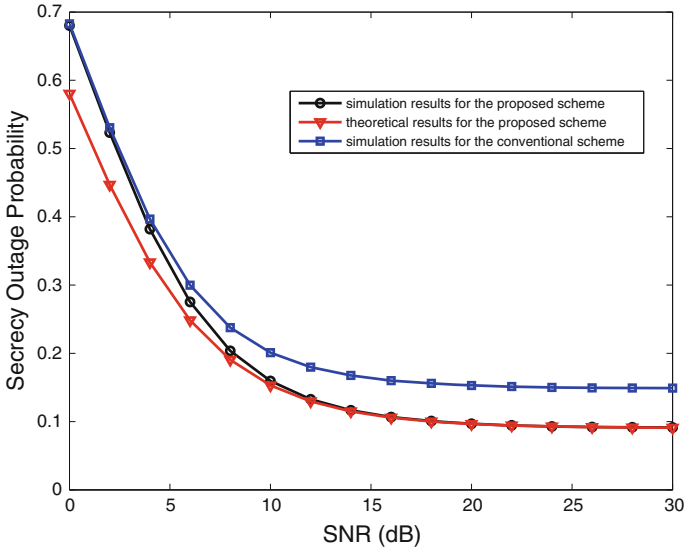

Fig. 2 The secrecy outage probability versus the system average SNR. $K = 3, M = 2, R_s = 0.1$ bit/s/Hz

by the secrecy constraint, we calculate the ergodic capacity for the system without eavesdroppers (C_0), and present the differences $C_0 - C1$ and $C_0 - C2$ in Fig. 3b.[1] One can observe from Fig. 3a that the proposed scheme outperforms the conventional scheme in terms of the secrecy capacity. However, the secrecy capacities of both schemes almost saturate as the SNR tends to infinity. This is because as SNR gets larger, the achievable rate of the legitimate link as well as the eavesdropper link increases. Comparably, without the existence of the eavesdroppers, the system capacity increases linearly with SNR, which is due to the multiuser diversity gain [13]. This explains the phenomenon in Fig. 3b, which clearly reflects the capacity penalty to support the secrecy constraints.

Figure 4 plots the system intercept probability as a function of the MER κ_{de}. In this figure, we assume $K = 1$ and fix SNR to be 20 dB. The source node and destination node are located at (0, 0) and (2, 0), respectively. The location of the eavesdropper is determined according to the value of κ_{de}. Other simulation parameters are the same as those for producing the results in Figs. 2 and 3. From Fig. 4, it can be seen that, for various values of M, the theoretical results exactly match the simulated ones, indicating the correctness of the performance analysis in Sect. 2.4.2. In addition, the slopes of the curves illustrate that the diversity order of M is achieved by our protocol, which is in accordance with the analysis in Sect. 2.4.3.

[1]For the multisource multirelay network without eavesdroppers, the best source-relay pair is selected according to the method in [13].

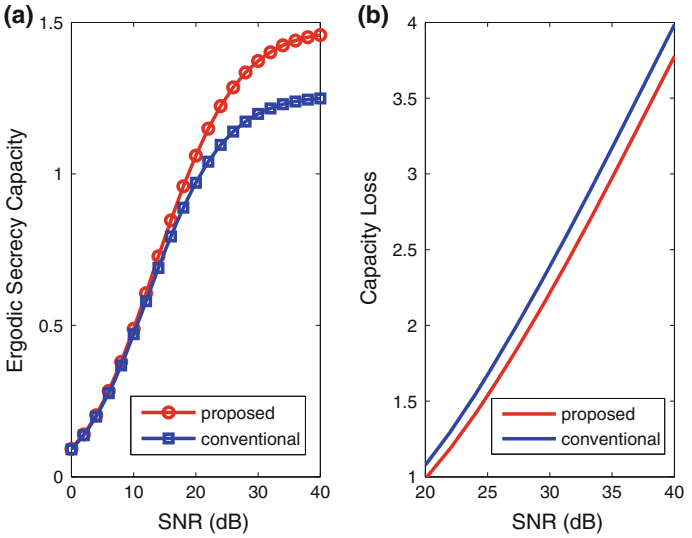

Fig. 3 The ergodic secrecy capacity of the system: **a** the secrecy capacity comparison between the proposed and the conventional scheme. **b** The capacity loss relative to the system without eavesdroppers. $K = 3, M = 2$

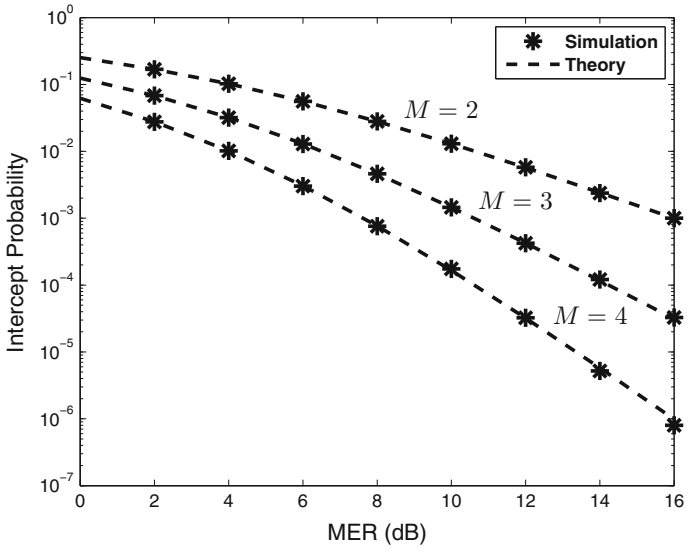

Fig. 4 The intercept probability versus the main eavesdropper ratio (MER). $K = 1, M = 2, 3, 4$, SNR = 20 dB

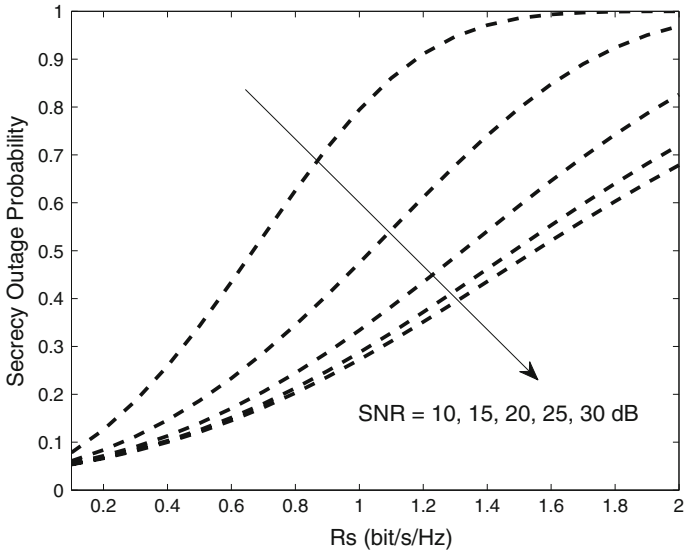

Fig. 5 The secrecy outage probability versus the target secrecy rate R_S. $K = 3, M = 2$, SNR = 30 dB

In Figs. 5, 6, 7 and 8, the impact of some key parameters on the system secrecy performance are examined. In these figures, we locate the $K = 3$ sources at $(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$, $(-\frac{1}{\sqrt{2}}, 0)$, and $(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$. The $M = 2$ relays are distributed at $(\frac{1}{2}, \frac{1}{2})$ and $(\frac{1}{2}, -\frac{1}{2})$. In Figs. 5 and 6, the positions of the destination and the eavesdropper are fixed as (2, 0) and (2, 2), respectively. In Figs. 7 and 8, the destination is also located at (2, 0) whereas the eavesdropper's position varies within the rectangular region $[-3, 3] \times [-3, 3]$.

Figure 5 presents the curve of the system secrecy outage probability, and exhibits how it varies with the target secrecy rate R_S. In this figure, five representative SNR values are considered. As expected, when the target rate increases, the SOP increases as well.

In Fig. 6, the effect of the power allocation ratio on the achievable SOP is investigated. Specifically, given the total transmit power P_{tot}, we allocate αP_{tot} to the selected source and $(1 - \alpha)P_{tot}$ to the selected relay. As α changes from 0 to 1, the SOP as a function of α is shown in Fig. 6. Here we plot a set of SOP curves, each corresponding to a specific SNR value. It should be pointed out that in Fig. 6, the notation "SNR" represents the ratio of the total transmit power for two phases versus N_0, which is different from the previous figures. An important observation from Fig. 6 is that, in order to optimize the system performance, α should be neither too large nor too small. The reasons can be briefly given as follows. If α is too large, the relay-destination link will be in poor channel quality, which significantly limits the achievable rate at the destination. On the other hand, if α is too small, implying

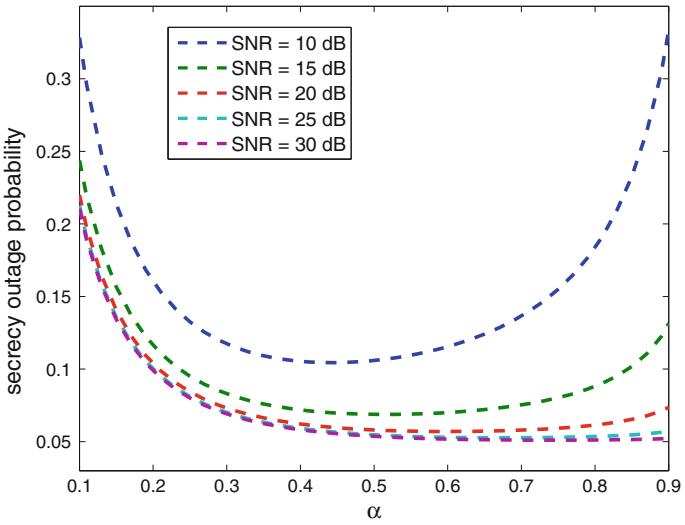

Fig. 6 The secrecy outage probability versus the power allocation factor α. $K = 3, M = 2, R_s = 0.1$ bit/s/Hz

that more power is allocated to the relay node, the eavesdropper will benefit from the improved quality of the relaying channel, which also decreases the secrecy rate. From Fig. 6 we can also find that the system performance is satisfactory for $\alpha = 0.5$. Therefore, the equal power allocation scheme, which is assumed in our work, is near-optimal despite its simplicity.

Figure 7 shows the relationship between the eavesdropper's location and the intercept probability. From this figure, we can observe that the intercept probability increases significantly when the eavesdropper moves toward the relay nodes. This is obvious because the closer the eavesdropper is to the relays, the better the channel quality of the relay-eavesdropper link. Figure 8 presents the secrecy outage probability versus the eavesdropper's location. As expected, the impact of the eavesdropper's location on the SOP is similar to that on the intercept probability.

2.6 Conclusions

In this section, a joint source-relay selection scheme is proposed for vehicular networks under eavesdropping attacks. The proposed scheme maximizes the instantaneous secrecy rate of the system, and hence can minimize the achievable secrecy outage probability. We present the selection criterion, and also give a low-complexity method to realize this criterion in a distributed manner. The system performance is analyzed in terms of the secrecy outage probability, the intercept probability, and the achievable diversity order. Finally, the effectiveness of the proposed scheme and the correctness of the theoretical analysis are verified through extensive simulations.

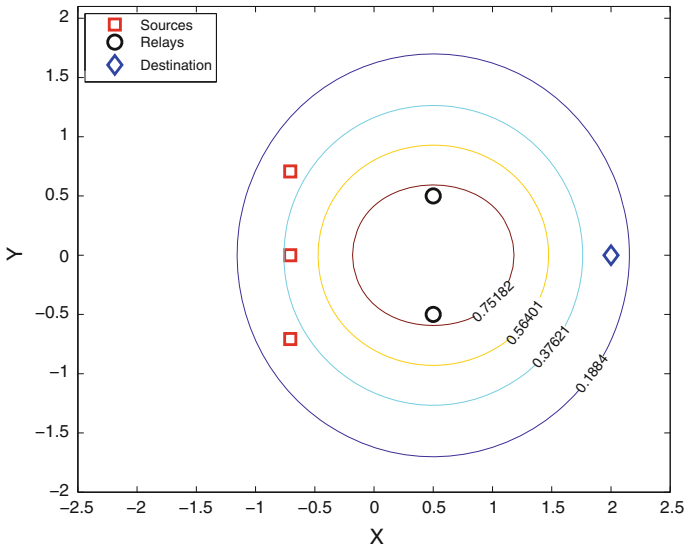

Fig. 7 The intercept probability versus the location of the eavesdropper. $K = 3, M = 2$, SNR $= 20$ dB. The numbers on the curves represent the achievable intercept probabilities

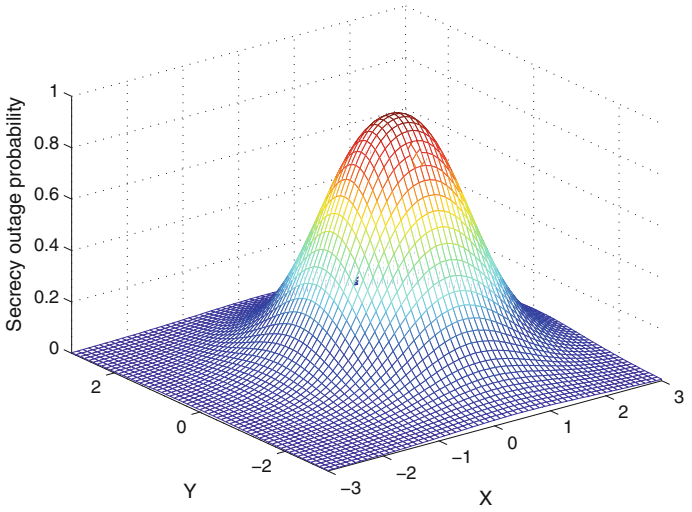

Fig. 8 The secrecy outage probability versus the locations of the eavesdropper. $K = 3, M = 2$, SNR $= 20$ dB

3 Fountain-Coding Aided Strategy for Secure Vehicular Communications in Intelligent Transportation Systems

3.1 Introduction

With the development of advanced wireless networking technologies that are being designed exclusively for use in a vehicular context, it becomes possible to establish connections between vehicles to exchange information, promising novel and fantastic V2V applications. For example, by exploiting the intervehicle communications capabilities, safety-relevant information can be exchanged, creating opportunities not only to increase traffic safety but also to improve the driving experience. Moreover, the drivers might even be able to enjoy fully automated rides on the highway.

Applications for V2V communications often have very stringent requirements on communication reliability and transmission delay. Nevertheless, the harshness of wireless environments poses severe challenges to the design of efficient V2V protocols. First, wireless channels are subject to multipath fading and interuser interference, which makes it extremely difficult to satisfy the QoS requirements of the data transmission. Second, in intervehicle communications, the highly dynamic feature of the network topology, resulting from the fast movement of the vehicles, also has adversary impacts on the reliability of end-to-end transmissions.

Among the existing candidates that tackle these technical challenges, co-operative relaying is widely regarded as a powerful tool [49, 50]. As mentioned in the previous section, the use of co-operative relaying techniques in the context of V2V communications has been intensively studied in recent years, and currently more and more attention has been paid to secure the co-operative relaying transmission using physical-layer approaches. In contrast to the traditional cryptography-based paradigm, physical-layer security (PLS) [19] exploits the characteristics of wireless channels and realizes secrecy via signal-processing approaches, which have great potential in guaranteeing V2V communications security.

Typical PLS approaches include the artificial noise injection [51], secure beamforming/precoding [52], co-operative jamming [53], power control [54], and signal alignment techniques [55]. For co-operative communication systems, [56] proposed an opportunistic relay selection strategy to improve the security-reliability tradeoff (SRT) of end-to-end transmissions. In [46], the optimal relay selection schemes were developed to maximize the secrecy rate for both AF and DF systems. In [57], an alternate jamming approach was adopted to prevent information leakage to the untrusted relays, and a low-complexity relay selection method was given to optimize system secrecy performance. In [58], a signal alignment scheme was devised for co-operative device-to-device (D2D) transmissions, which keeps the information exchange between cellular users and that between D2D users confidential from each other.

Till now, most existing PLS schemes aimed at minimizing the secrecy outage probability or maximizing the secrecy capacity (SC). This methodology, however, may not be appropriate for vehicular applications. First, SOP dictates the probability with which the achievable secrecy rate is lower than the target transmission rate. To satisfy a predefined SOP requirement, the transmission rate of the legitimate user has be kept at a very low level. This results in an intolerable delay, which may violate the delay requirement of real-time services. Second, SC gives the maximum rate below which the legitimate receiver can successfully decode while the eavesdropper cannot obtain any information from the received signal. To guarantee this *perfect secrecy*, any transmission rate above SC is prohibited. From a practical point of view, it is not always necessary to satisfy this requirement. If the transmitted file is composed of correlated packets, the eavesdropper cannot extract useful information even though a small number of the packets are received.

The aforementioned issues can be addressed by introducing fountain codes into PLS protocol design. Fountain codes (FC), such as LT codes or Raptor codes, were first proposed to realize reliable communications without retransmission [59]. In fountain-coded data transmissions, the source file is first divided into K packets. Then, a potentially infinite number of fountain-coded packets are generated, each of which is the XOR of distinct source packets chosen randomly. The transmitter sprays these coded packets at the destination continuously. Once the receiver has correctly received N packets, where N is slightly larger than K, the source file can be recovered and the transmission terminates. This characteristic of fountain codes can be exploited to realize physical-layer security. Specifically, by using fountain codes, the transmission link between the legitimate transceivers can be secured if the legitimate receiver successfully accumulates the N coded packets before the eavesdropper does. In other words, the source information is not leaked as long as the source obtains the required N packets first, even though some packets may be obtained by the eavesdropper. Compared to the existing PLS strategies based on the secrecy rate optimization, the fountain-coding aided approach can significantly increase the data rate of the system, which is only bounded by the Shannon capacity of the legitimate link.

The fountain codes have been widely used in point-to-point communications, multicast systems, and co-operative relay networks as a low-complexity transmission approach towards enhanced reliability [59–61]. However, the use of FC in PLS has not been well studied. In [62], the FC-aided secure communications were discussed for the basic wiretap channel, for which the power control technique was used to lower the intercept probability. However, the proposed scheme in [62] cannot be directly applied to co-operative relaying networks, where the information leakage needs to be dealt with within the first hop as well as the second hop. Additionally, the adopted performance metric therein (i.e., intercept probability) does not fully reflect the requirements of vehicular applications.

In this section, a novel FC-aided PLS scheme is proposed for two-hop relay transmission in V2V scenarios. The proposed scheme has two significant advantages compared to the state-of-the-art techniques. First, it offers lower implementation complexity and thus lower cost than traditional cryptography-based security pro-

tocols. Second, it provides a higher transmission rate and thus reduced transmission delay than the existing physical-layer security protocols. Because low complexity and low latency are both crucial for intelligent transportation systems, the scheme developed in this section is very suitable for V2V applications. The main contributions of this work can be summarized as follows.

- A novel transmission framework is developed for DF-based two-hop cooperative networks. The new approach combines fountain coding at the application layer and cooperative jamming at the physical layer. In this way, with high probability the legitimate receiver can accumulate the enough fountain packets before the eavesdropper does, thereby enhancing the transmission secrecy.
- A constellation-rotation based method is designed to realize effective cooperative jamming. By rotating the signal constellation and exploiting the intrinsic orthogonality between the real and the imaginary component of a complex signal, the received signal-to-noise-plus-interference ratio (SINR) at the eavesdropper is greatly deteriorated, whereas the adversary impact of jamming on the received signal quality at the legitimate terminals can be significantly reduced.
- A novel metric called QoS Violating Probability (QVP) is proposed to evaluate the system performance. The closed-form expression for QVP is derived, and its correctness is verified through simulations. Compared to the well known performance metrics in PLS research such as SC or SOP, QVP gives a more comprehensive characterization of the system performance, including the delay, the reliability, and the security level as well.

The rest of this section is organized as follows. Section 3.2 presents the system model. Section 3.3 gives a detailed description of the proposed scheme. In Sect. 3.4, the new performance metric, the QVP, is defined, and the closed-form expression of QVP for the proposed scheme is derived. Simulation results are shown in Sect. 3.5. Finally, concluding remarks and future works are given in Sect. 3.6.

3.2 System Model

As shown in Fig. 9, this section considers a system consisting of one source (S), one destination (D), one eavesdropper (E), and a group of intermediate nodes. In practical vehicular networks, the source corresponds to the vehicle having data to transmit, and the destination is the vehicle to receive the message. The eavesdropper, whose location is unknown to the legitimate parties, is an malicious entity that attempts to extract the source information. The intermediate nodes are some idle vehicles, and they can act as helpers to assist the source transmission. Two idle vehicles are assumed to be selected as the relay (R) and the friendly jammer (J), respectively. The relay node helps the source deliver its message to the destination, while the jammer generates artificial noise to deteriorate the received signal quality at the eavesdropper. For simplicity, it is supposed that these two helpers have already been selected

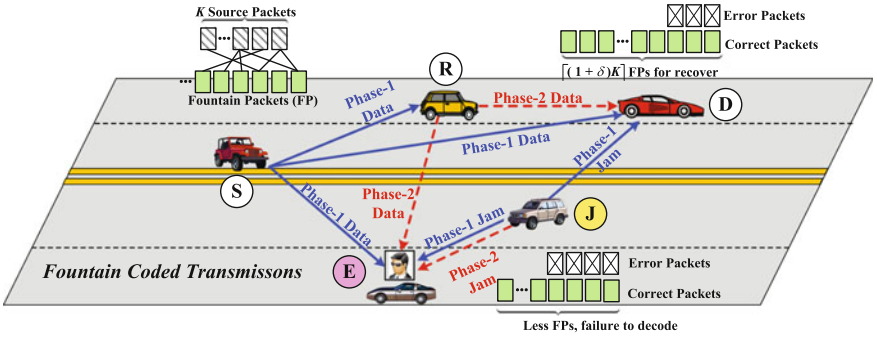

Fig. 9 System model

prior to communications, and the discussion on how to select these nodes is beyond the scope of our work.

S wants to deliver a confidential data file securely to D. To achieve this goal, S first divides its file into K packets denoted by $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K)$. Then, fountain coding is employed to encode these original packets into a potentially infinite number of fountain packets $(\mathbf{v}_1, \mathbf{v}_2, \ldots)$, each of which is a binary addition of a random subset of the K source packets. After that, every fountain packet is further encoded by a capacity-approaching code at the physical layer. Finally, the output of the encoder is modulated and sent to the wireless channel. The transmitted packets are denoted $(\mathbf{p}_1, \mathbf{p}_2, \ldots)$.[2]

The end-to-end delivery of each packet is completed within a transmission round (TR) composed of two phases. During the first phase (broadcast phase), S broadcasts its message, while R and D operate in the receive mode. To combat the eavesdropping behavior at E, J performs co-operative jamming by sending artificial noises. At the end of this phase, R does channel decoding on the received packet, and D stores the received packet for further processing. If the channel decoding at R is correct, the packet will be forwarded to D during the second phase (relaying phase); meanwhile, the jamming signal is transmitted from J to worsen the SINR at E. At the end of the second phase, D as well as E combines the received signals from the two phases and performs channel decoding. On the other hand, if the channel decoding at R is in failure, R will not retransmit this packet and all the terminals will keep silent within the second phase. Correspondingly, the channel decoding at D and E is based on the received signal during the first phase only. The correctly received fountain packets are stored for future fountain decoding. According to the basic characteristics of fountain codes, when the destination accumulates $N = \lceil (1 + \delta)K \rceil$ fountain packets, the whole file can be recovered and an acknowledgment (ACK) packet is fed back to the source to terminate the transmission, where δ represents the decoding overhead

[2] We emphasize that in this section, "source packets," "fountain packets," and "transmitted packets" have different meanings.

and $\lceil x \rceil$ is the ceiling function. The security of data delivery is guaranteed if the eavesdropper has not accumulated enough (i.e., N) fountain packets at this time.

Each node is equipped with a single antenna and is operative in a half-duplex mode (i.e., it cannot transmit and receive simultaneously). The channel coefficient between any node pair (i,j) $(i,j \in \{\mathrm{S},\mathrm{D},\mathrm{R},\mathrm{E}\})$ is represented by h_{ij}, which is modeled as a complex circularly symmetric Gaussian variable with mean zero and variance μ_{ij}. The amplitude and phase of h_{ij} are denoted by $|h_{ij}|$ and $\angle h_{ij}$, respectively. We presume that each node only has the local channel state information (CSI), that is, the channel coefficients of the links connecting this node and its neighboring nodes. It is further assumed that D also knows h_{SR}. All the channels are independent and follow the flat block fading model, and remain constant within one TR (a two-phase duration) and vary independently among different TRs. The average transmit power at each terminal is constrained by P, and the additive noise at each receiver is modeled as a complex Gaussian variable with mean zero and variance N_0. $\rho = P/N_0$ is introduced to represent the average signal-to-noise ratio of the system. For the considered channel model, $\gamma_{ij} \triangleq \rho|h_{ij}|^2$ obeys an exponential distribution with rate parameter $\lambda_{ij} = (\rho\mu_{ij})^{-1}$. The target transmission rate is R bits per channel use (bpcu). Throughout this section, $\Pr(A)$ is the probability of event A, $\log(\cdot)$ stands for the base-2 logarithm, $\mathrm{E}(\cdot)$ denotes the expectation operator, x^*, $\mathfrak{R}\{x\}$, and $\mathfrak{I}\{x\}$ are used to represent the complex conjugate, the real component, and the imaginary component of x, respectively.

3.3 Scheme Descriptions

From Sect. 3.2 it was learned that the secure delivery of the source messages can be realized if the destination can accumulate enough fountain packets before the eavesdropper does. Towards this purpose, a co-operative jamming technique is applied at the physical layer to ensure a high outage probability at E.[3] However, without careful design, the jamming signal also does harm to the received signal quality at R and D. To overcome this difficulty, a constellation-rotation based approach is proposed at the physical layer, which can weaken the adversary impact of the jamming procedure on the legitimate users, while effectively decreasing the SINR at E.

Constellation rotation was first proposed by [63] as a diversity approach over fading channels. The basic principle of constellation rotation is as follows. Let d represent the original complex constellation, taking values from an alphabet $\mathscr{X}$. Then the rotated symbol is $t = e^{j\theta}d$, where θ is the rotation angle chosen in such a way that no two symbols have the same coordinate. That is, for any $i \neq k$,

$$\mathfrak{R}\{t^i\} \neq \mathfrak{R}\{t^k\}, \quad \mathfrak{I}\{t^i\} \neq \mathfrak{I}\{t^k\}, \ \forall t^i, t^k \in e^{j\theta}\mathscr{X}. \tag{29}$$

[3] In this section, the outage probability is defined as the probability that the channel capacity falls below a specified target transmission rate. This definition is the same as the one used in the information-theoretic literature.

In the proposed scheme, constellation rotation is applied to every symbol output from the modulator.[4]

The transmission details for each TR are now presented. Because the physical-layer processing is the same for all the symbols in each transmitted packet, it only needs to focus on the transmission procedure on a symbol basis. During the first phase, the transmitted signals from S and J are designed as

$$x_{\mathrm{S}} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}e^{-j\angle h_{\mathrm{SR}}} \tag{30}$$

and

$$x_{\mathrm{J}}^{(1)} = j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(1)}\}e^{-j\angle h_{\mathrm{JR}}}, \tag{31}$$

respectively, where $t_{\mathrm{S}} = e^{j\theta}d_{\mathrm{S}}$ is the information-bearing signal from S, and $w_{\mathrm{J}}^{(1)}$ is the artificial noise sent from the friendly jammer during the first phase.[5] The receive signal at R can be expressed as

$$y_{\mathrm{R}} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}|h_{\mathrm{SR}}| + j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(1)}\}|h_{\mathrm{JR}}| + n_{\mathrm{R}}^{(1)}, \tag{32}$$

where $n_k^{(m)}$ is the additive noise at node k during phase m ($k \in \{\mathrm{R}, \mathrm{D}, \mathrm{E}\}, m \in \{1, 2\}$). R extracts the real component of y_{R} and estimates $\Re\{t_{\mathrm{S}}\}$ using the maximum likelihood (ML) criterion. According to Eq. (29), there is a one-to-one correspondence between the rotated constellation and its real (or imaginary) part. Therefore, t_{S} can be recovered from $\Re\{t_{\mathrm{S}}\}$. Here, by rotating the constellation, the signal detection at R is made free of the interference from the friendly jammer. Also, thanks to the characteristic given by Eq. (29), the information of the complex signal can be fully represented by its real (or imaginary) part. Therefore, the transmission rate (measured by bits per channel use) is not reduced despite the fact that only half of the dimensions are utilized.

Based on Eq. (32), the received SNR of the source-relay link can be derived as $\gamma^{(\mathrm{S}\to\mathrm{R})} = 2\gamma_{\mathrm{SR}}$, and the achievable rate can be calculated as

$$\mathscr{R}^{(\mathrm{S}\to\mathrm{R})} = \frac{1}{2}\log\left(1 + 2\gamma_{\mathrm{SR}}\right), \tag{33}$$

where the pre-log factor is due to the half-duplex constraint at the terminals.

---

[4] In practice, the value of the rotation angle affects system performance such as the bit error rate. However, this work is dedicated to information-theoretic analysis. Therefore, any angle value satisfying Eq. (29) can be used and the specific choice for this parameter has no influence on the results.

[5] It is assumed that the power of the information-bearing signal as well as the jamming signal is normalized such that $\mathrm{E}[|t_{\mathrm{S}}|^2] = 1$ and $\mathrm{E}[|w_{\mathrm{J}}^{(1)}|^2] = 1$. This assumption also holds for the transmitted signals during the second phase.

The received signals at D and E can be separately written as

$$y_{\mathrm{D}}^{(1)} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}e^{-j\angle h_{\mathrm{SR}}}h_{\mathrm{SD}} + j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(1)}\}e^{-j\angle h_{\mathrm{JR}}}h_{\mathrm{JD}} + n_{\mathrm{D}}^{(1)} \tag{34}$$

and

$$y_{\mathrm{E}}^{(1)} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}e^{-j\angle h_{\mathrm{SR}}}h_{\mathrm{SE}} + j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(1)}\}e^{-j\angle h_{\mathrm{JR}}}h_{\mathrm{JE}} + n_{\mathrm{E}}^{(1)}, \tag{35}$$

yielding the SINRs at these two nodes to be

$$\mathrm{SINR}_{\mathrm{D}}^{(1)} = \frac{\gamma_{\mathrm{SD}}}{\gamma_{\mathrm{JD}} + 1} \tag{36}$$

and

$$\mathrm{SINR}_{\mathrm{E}}^{(1)} = \frac{\gamma_{\mathrm{SE}}}{\gamma_{\mathrm{JE}} + 1}, \tag{37}$$

respectively.

If $\mathscr{R}^{(\mathrm{S}\to\mathrm{R})} < R$ or equivalently $\gamma_{\mathrm{SR}} < \frac{2^{2R}-1}{2}$, the physical-layer decoding (channel decoding) at R is in failure. In this case, packet re-transmission will not be activated, and D (E) has to decode the transmitted packet based on $y_{\mathrm{D}}^{(1)}$ ($y_{\mathrm{E}}^{(1)}$) only. Otherwise, the decoded packet is re-encoded using the same codebook and then forwarded to D during the second phase. To be specific, the transmitted signals from R and J are given by $x_{\mathrm{R}} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}e^{-j\angle h_{\mathrm{RD}}}$ and $x_{\mathrm{J}}^{(2)} = j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(2)}\}e^{-j\angle h_{\mathrm{JD}}}$, respectively. The received signal at D can be expressed as

$$y_{\mathrm{D}}^{(2)} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}|h_{\mathrm{RD}}| + j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(2)}\}|h_{\mathrm{JD}}| + n_{\mathrm{D}}^{(2)}. \tag{38}$$

Similar to what R does during the first phase, D extracts the real part of $y_{\mathrm{D}}^{(2)}$ to obtain the source information. Obviously, the signal detection at D is interference-free, and the resulting SINR of this phase is

$$\mathrm{SINR}_{\mathrm{D}}^{(2)} = 2\gamma_{\mathrm{RD}}. \tag{39}$$

The received signal at E has the form of $y_{\mathrm{E}}^{(2)} = \sqrt{2P}\Re\{t_{\mathrm{S}}\}e^{-j\angle h_{\mathrm{RD}}}h_{\mathrm{RE}} + j\sqrt{2P}\Im\{w_{\mathrm{J}}^{(2)}\}e^{-j\angle h_{\mathrm{JD}}}h_{\mathrm{JE}} + n_{\mathrm{E}}^{(2)}$. Because the source information is contained in both the real and the imaginary components of the signal, E has to perform channel decoding while being interfered with by the jamming signal from J.[6] After some simple derivations, the SINR at E can be expressed as

[6] According to the assumptions about the available CSI at each node, h_{JR} and h_{JD} are unknown at E, and the impact of the jamming signals cannot be removed by the eavesdropper.

$$\mathrm{SINR}_{\mathrm{E}}^{(2)} = \frac{\gamma_{\mathrm{RE}}}{\gamma_{\mathrm{JE}} + 1}. \tag{40}$$

At the end of the second phase, both D and E combine the received signals during the two phases and make a decision about the transmitted packet within this TR. If the packet can be decoded correctly at the physical layer, it will be kept for future fountain coding; otherwise, this packet is discarded.

3.4 Performance Analysis

3.4.1 Performance Metric

To evaluate the performance of the developed FC-aided PLS strategy, a novel metric called QoS violating probability is proposed, which is defined as

$$\begin{aligned} p^{\mathrm{vio}} &= \Pr(T_{\mathrm{tot,D}} > T_{req}) \\ &\quad + \sum_{k=N}^{T_{\mathrm{req}}} \Pr(T_{\mathrm{tot,D}} = k)\Pr(T_{\mathrm{tot,E}} \leq k), \end{aligned} \tag{41}$$

where T_{req} is the number of TRs allowed to finish the file delivery, and $T_{\mathrm{tot,D}}$, and $T_{\mathrm{tot,E}}$ are the number of TRs needed by D and E to recover the file, respectively. It is obvious that $T_{req} \geq N$ because fountain code is employed.

In Eq. (41), the first term defines the *delay violating probability*, that is, the probability with which the file cannot be successfully transferred from S to D within the given delay bound. The second term calculates the probability of the event that the eavesdropper obtains the N fountain packets before the destination does, or they complete the packet accumulation simultaneously. For the proposed FC-aided scheme, this corresponds to the *information intercept probability*, meaning that the data delivery is not secured although the delay constraint is satisfied. The sum of the two terms in Eq. (41) characterizes the probability with which the QoS requirement is violated. Compared to the well-adopted SOP metric, QVP has the following advantages.

First, QVP gives a more comprehensive description about the system performance. To be specific, 1-SOP characterizes the probability with which the file is reliably received at D, without any information leakage at E. Comparably, 1-QVP defines the probability with which the file is reliably received at D within the given delay constraint, without any information leakage at E. Therefore, QVP can reflect the reliability, security, and delay performances of a protocol, which is more appropriate for practical V2V applications.

Second, QVP provides a guideline of designing the transmission strategies for a broad class of services. To illustrate this, let's consider two extreme cases that $T_{req} = N$ and $T_{req} = \infty$. When $T_{req} = N$, Eq. (41) becomes

$$p^{\text{vio,N}} = \Pr(T_{\text{tot,D}} > N) + \Pr(T_{\text{tot,D}} = N)\Pr(T_{\text{tot,E}} = N), \tag{42}$$

which indicates that, for delay-sensitive services, that is, the services with tight delay bound, QVP is determined by both the delay violating probability and the information intercept probability. However, it can be easily verified that the latter is much smaller than the former. Therefore, QVP is dominated by the delay violating probability. This implies that, for delay-sensitive services with secrecy constraints, it suffices simply to increase the channel quality of the legitimate link. On the other hand, when $T_{req} = \infty$, QVP can be written as

$$p^{\text{vio},\infty} = \sum_{k=N}^{\infty} \Pr(T_{\text{tot,D}} = k)\Pr(T_{\text{tot,E}} \leq k), \tag{43}$$

which is fully determined by the information intercept probability. Equation (43) indicates that, for nondelay-sensitive services under eavesdropping attacks, the system designer should try to enlarge the difference in channel qualities between the legitimate link and the eavesdropping link. In this manner, the packet accumulation at D will be faster than that at E, and the information intercept probability can be decreased.

3.4.2 Derivation of the QoS Violating Probability

Now, the closed-form expression for QVP is derived. $T_{\text{tot,D}}$, which is a discrete random variable taking values from $\{N, N+1, N+2, \ldots\}$, can be rewritten as

$$T_{\text{tot,D}} = N + N_{\text{out}}, \tag{44}$$

where N_{out} is the number of outage events for the source-destination transmissions (with or without the assistance of the relay node, depending on the channel quality of the source-relay link). Here, the outage event is defined as the event that the achievable rate is below the target transmission rate. For the proposed protocol, the transmission terminates as long as N fountain packets have been correctly received at D. Therefore, by denoting the outage probability for the legitimate link as α, N_{out} can be modeled as a random variable following the negative binomial distribution $\mathcal{NB}(N;\alpha)$, whose probability mass function (PMF) is given by

$$\begin{aligned} f_{N_{\text{out}}}(k) &= \Pr(N_{\text{out}} = k) \\ &= \binom{N+k-1}{k} \alpha^k (1-\alpha)^N, \quad k = 0, 1, 2, \ldots \end{aligned} \tag{45}$$

Thus, the PMF of $T_{\text{tot,D}}$ can be calculated as

$$f_{T_{\text{tot,D}}}(k) = \Pr(N_{\text{out}} = k - N) = \begin{cases} \binom{k-1}{k-N}\alpha^{(k-N)}(1-\alpha)^N, & k \geq N \\ 0 & k < N \end{cases} \tag{46}$$

As a result, $\Pr(T_{\text{tot,D}} > T_{req})$ can be derived as

$$\Pr(T_{\text{tot,D}} > T_{\text{req}}) = 1 - \Pr(T_{\text{tot,D}} \leq T_{\text{req}}) = 1 - \sum_{k=N}^{T_{\text{req}}} \binom{k-1}{k-N}\alpha^{k-N}(1-\alpha)^N. \tag{47}$$

The PMF of $T_{\text{tot,E}}$, that is, $f_{T_{\text{tot,E}}}(k)$, has the same form as Eq. (46) with α replaced by β, where β is the outage probability for the source-eavesdropper transmission. By exploiting this PMF result, it can be deduced that

$$\Pr(T_{\text{tot,E}} \leq k) = \sum_{p=N}^{k} \Pr(T_{\text{tot,E}} = p) = \sum_{p=N}^{k} f_{T_{\text{tot,E}}}(p) = \sum_{p=N}^{k} \binom{p-1}{p-N}\beta^{p-N}(1-\beta)^N. \tag{48}$$

Substituting Eqs. (46)–(48) into Eq. (41) leads to the QVP expression. To complete the analysis, one only needs to derive the outage probabilities α and β, which are dealt with in what follows.

The Derivation of α:

The outage probability for the transmission between the legitimate users, that is, α, can be expressed as

$$\alpha = \Pr\left(\gamma_{\text{SR}} < \frac{2^{2R}-1}{2}\right)\Pr\left(\frac{1}{2}\log\left(1 + \text{SINR}_{\text{D}}^{(1)}\right) < R\right) + \Pr\left(\gamma_{\text{SR}} > \frac{2^{2R}-1}{2}\right)\Pr\left(\frac{1}{2}\log\left(1 + \text{SINR}_{\text{D}}^{(1)} + \text{SINR}_{\text{D}}^{(2)}\right) < R\right). \tag{49}$$

For the considered channel model, γ_{ij} follows an exponential distribution with rate parameter λ_{ij}. Thus,

$$\Pr\left(\gamma_{\text{SR}} < \frac{2^{2R}-1}{2}\right) = 1 - e^{-\frac{1}{2}\lambda_{\text{SR}}\left(2^{2R}-1\right)}, \tag{50}$$

and

$$\Pr\left(\gamma_{\text{SR}} > \frac{2^{2R}-1}{2}\right) = e^{-\frac{1}{2}\lambda_{\text{SR}}\left(2^{2R}-1\right)}. \tag{51}$$

$\Pr(\frac{1}{2}\log(1+\mathrm{SINR}_{\mathrm{D}}^{(1)})<R)$ can be derived as

$$\begin{aligned}\Pr\left(\frac{1}{2}\log(1+\mathrm{SINR}_{\mathrm{D}}^{(1)})<R\right)&=\Pr\left(\mathrm{SINR}_{\mathrm{D}}^{(1)}<2^{2R}-1\right)\\&=\int_0^{\infty}\Pr\left(\gamma_{\mathrm{SD}}<(2^{2R}-1)(1+x)\right)f_{\gamma_{\mathrm{JD}}}(x)dx\\&=\int_0^{\infty}\left[1-e^{-\lambda_{\mathrm{SD}}(2^{2R}-1)(1+x)}\right]\lambda_{\mathrm{JD}}e^{-\lambda_{\mathrm{JD}}x}dx\\&=1-\frac{\lambda_{\mathrm{JD}}}{\lambda_{\mathrm{JD}}+\lambda_{\mathrm{SD}}(2^{2R}-1)}e^{-\lambda_{\mathrm{SD}}(2^{2R}-1)}.\end{aligned}\tag{52}$$

Let $\mathrm{SINR}_{\mathrm{D}}^{(1)}\triangleq X$ and $\mathrm{SINR}_{\mathrm{D}}^{(2)}\triangleq Y$. Then, the cumulative distribution function (CDF) of X and the probability density function (PDF) of Y can be expressed by

$$F_X(x)=1-\frac{\lambda_{\mathrm{JD}}}{\lambda_{\mathrm{JD}}+\lambda_{\mathrm{SD}}x}e^{-\lambda_{\mathrm{SD}}x},\tag{53}$$

and

$$f_Y(y)=\frac{\lambda_{\mathrm{RD}}}{2}e^{-\frac{\lambda_{\mathrm{RD}}}{2}y},\tag{54}$$

respectively. By utilizing Eqs. (53) and (54), $\Pr(\frac{1}{2}\log(1+\mathrm{SINR}_{\mathrm{D}}^{(1)}+\mathrm{SINR}_{\mathrm{D}}^{(2)})<R)$ in Eq. (49) can be derived as

$$\begin{aligned}&\Pr\left(\frac{1}{2}\log(1+X+Y)<R\right)\\&\quad=\Pr(X+Y<2^{2R}-1)\\&\quad=\int_0^{\infty}\Pr(X<2^{2R}-1-y)f_Y(y)dy\\&\quad=\int_0^{2^{2R}-1}\Pr(X<2^{2R}-1-y)f_Y(y)dy\\&\quad=\int_0^{2^{2R}-1}\left[1-\frac{\lambda_{\mathrm{JD}}e^{-\lambda_{\mathrm{SD}}(2^{2R}-1-y)}}{\lambda_{\mathrm{JD}}+\lambda_{\mathrm{SD}}\left(2^{2R}-1-y\right)}\right]\frac{\lambda_{\mathrm{RD}}}{2}e^{-\frac{\lambda_{\mathrm{RD}}}{2}y}dy\\&\quad=1-e^{-\frac{\lambda_{\mathrm{RD}}}{2}(2^{2R}-1)}-\left(\frac{\lambda_{\mathrm{RD}}\lambda_{\mathrm{JD}}}{2}e^{-\lambda_{\mathrm{SD}}(2^{2R}-1)}\right.\\&\qquad\left.\times\int_0^{2^{2R}-1}\frac{e^{-\left(\frac{\lambda_{\mathrm{RD}}}{2}-\lambda_{\mathrm{SD}}\right)y}}{\lambda_{\mathrm{JD}}+\lambda_{\mathrm{SD}}\left(2^{2R}-1-y\right)}dy\right).\end{aligned}\tag{55}$$

Letting $2^{2R}-1-y=t$ and utilizing [64, Eq. (3.352.1)], Eq. (55) can be simplified as

$$\Pr\left(\frac{1}{2}\log(1+X+Y)<R\right) = 1-e^{-\frac{\lambda_{\mathrm{RD}}}{2}\left(2^{2R}-1\right)} = -\frac{\lambda_{\mathrm{RD}}\lambda_{\mathrm{JD}}}{2\lambda_{\mathrm{SD}}}e^{-\frac{\lambda_{\mathrm{RD}}}{2}\left(2^{2R}-1\right)+\lambda_{\mathrm{JD}}\left(1-\frac{\lambda_{\mathrm{RD}}}{2\lambda_{\mathrm{SD}}}\right)}\times A, \quad (56)$$

where

$$A = \mathrm{Ei}\left(-\left(\left(2^{2R}-1\right)+\frac{\lambda_{\mathrm{JD}}}{\lambda_{\mathrm{SD}}}\right)\left(\lambda_{\mathrm{SD}}-\frac{\lambda_{\mathrm{RD}}}{2}\right)\right)-\mathrm{Ei}\left(-\frac{\lambda_{\mathrm{JD}}}{\lambda_{\mathrm{SD}}}\left(\lambda_{\mathrm{SD}}-\frac{\lambda_{\mathrm{RD}}}{2}\right)\right). \quad (57)$$

In Eq. (57), $\mathrm{Ei}(x)$ is the exponential integral function defined in [64, Eq. (8.21)]. By combining Eqs. (50)–(52), and (56), the closed-form expression for α can be deduced. However, its explicit expression is omitted due to page limit.

The Derivation of β:

Based on the proposed protocol, β can be expressed as

$$\beta = \Pr\left(\gamma_{\mathrm{SR}}<\frac{2^{2R}-1}{2}\right)\Pr\left(\frac{1}{2}\log(1+\mathrm{SINR}_{\mathrm{E}}^{(1)})<R\right) + \Pr\left(\gamma_{\mathrm{SR}}>\frac{2^{2R}-1}{2}\right)\underbrace{\Pr\left(\frac{1}{2}\log\left(1+\mathrm{SINR}_{\mathrm{E}}^{(1)}+\mathrm{SINR}_{\mathrm{E}}^{(2)}\right)<R\right)}_{B}. \quad (58)$$

In Eq. (58), $\Pr(\gamma_{\mathrm{SR}}<\frac{2^{2R}-1}{2})$ and $\Pr(\gamma_{\mathrm{SR}}>\frac{2^{2R}-1}{2})$ have already been derived as Eqs. (50) and (51), respectively, and $\Pr(\frac{1}{2}\log(1+\mathrm{SINR}_{\mathrm{E}}^{(1)})<R)$ is of the same form as Eq. (52), with λ_{SD} and λ_{JD} being replaced by λ_{SE} and λ_{JE}, respectively. Therefore, it only needs to focus on the derivation of B in Eq. (58), which can be rewritten as

$$\begin{aligned} B &= \Pr\left[\gamma_{\mathrm{SE}}+\gamma_{\mathrm{RE}}<\left(2^{2R}-1\right)\left(\gamma_{\mathrm{JE}}+1\right)\right] \\ &= \int_0^{\infty}\Pr\left[\gamma_{\mathrm{SE}}+\gamma_{\mathrm{RE}}<\left(2^{2R}-1\right)(x+1)\right]f_{\gamma_{\mathrm{JE}}}(x)dx \\ &= \int_0^{\infty} I_1 f_{\gamma_{\mathrm{JE}}}(x)dx, \end{aligned} \quad (59)$$

with

$$\begin{aligned} I_1 &= \int_0^{\infty}\Pr\left[\gamma_{\mathrm{SE}}<\left(2^{2R}-1\right)(x+1)-y\right]f_{\gamma_{\mathrm{RE}}}(y)dy \\ &= \int_0^{2^{2R}-1}\Pr\left[\gamma_{\mathrm{SE}}<\left(2^{2R}-1\right)(x+1)-y\right]\lambda_{\mathrm{RE}}e^{-\lambda_{\mathrm{RE}}y}dy \end{aligned}$$

$$= \begin{cases} 1 - e^{-\lambda_{\mathrm{RE}}(2^{2R}-1)(x+1)} - \dfrac{\lambda_{\mathrm{RE}}\left(2^{2R}-1\right)(x+1)}{e^{\lambda_{\mathrm{RE}}(2^{2R}-1)(x+1)}}, \\ \qquad\qquad \text{if } \lambda_{\mathrm{SE}} = \lambda_{\mathrm{RE}}; \\ 1 - e^{-\lambda_{\mathrm{RE}}(2^{2R}-1)(x+1)} + \dfrac{\lambda_{\mathrm{RE}}}{\left(\lambda_{\mathrm{SE}} - \lambda_{\mathrm{RE}}\right)} \\ \qquad \times \dfrac{1 - e^{(\lambda_{\mathrm{SE}}-\lambda_{\mathrm{RE}})(2^{2R}-1)(x+1)}}{e^{\lambda_{\mathrm{SE}}(2^{2R}-1)(x+1)}}, \\ \qquad\qquad \text{if } \lambda_{\mathrm{SE}} \neq \lambda_{\mathrm{RE}}. \end{cases} \tag{60}$$

Substituting Eq. (60) into Eq. (59) and making use of [64, Eq. (3.351.2)], B can finally be derived as

$$B = \begin{cases} 1 - \dfrac{\lambda_{\mathrm{JE}} e^{-\lambda_{\mathrm{RE}}(2^{2R}-1)}}{\lambda_{\mathrm{JE}} + \lambda_{\mathrm{RE}}(2^{2R}-1)} - \dfrac{\lambda_{\mathrm{RE}}\lambda_{\mathrm{JE}}(2^{2R}-1)\Gamma(2,\Lambda)}{e^{-\lambda_{\mathrm{RE}}}\Lambda^2}, \\ \qquad\qquad \text{if } \lambda_{\mathrm{SE}} = \lambda_{\mathrm{RE}}; \\ 1 + \dfrac{\lambda_{\mathrm{JE}}}{\lambda_{\mathrm{SE}} - \lambda_{\mathrm{RE}}} \left(\dfrac{\lambda_{\mathrm{RE}} e^{-\lambda_{\mathrm{SE}}(2^{2R}-1)}}{\lambda_{\mathrm{SE}}(2^{2R}-1) + \lambda_{\mathrm{JE}}} - \dfrac{\lambda_{\mathrm{SE}} e^{-\lambda_{\mathrm{RE}}(2^{2R}-1)}}{\lambda_{\mathrm{RE}}(2^{2R}-1) + \lambda_{\mathrm{JE}}} \right), \\ \qquad\qquad \text{if } \lambda_{\mathrm{SE}} \neq \lambda_{\mathrm{RE}}. \end{cases} \tag{61}$$

where $\Lambda = \lambda_{\mathrm{JE}} + \lambda_{\mathrm{RE}}(2^{2R}-1)$, and $\Gamma(a,x)$ is the upper incomplete gamma function [64, Eq. (8.350.2)]. Substituting Eq. (61) into Eq. (58) leads to the expression of β, which is also omitted here due to space limitation. Having obtained both α and β, the QoS violating probability can be derived in closed form.

3.5 Simulation Results and Discussions

This subsection presents the simulation results to validate the proposed scheme. In the following simulations, all nodes are distributed in the first quadrant of the 1×1 rectangular coordinate system. Unless otherwise stated, the source, relay, jammer, destination, and eavesdropper are located at (0, 0), (0.4, 0.6), (0.6, 0.4), (1, 1), and (1, 0), respectively. The small-scale fading coefficients follow the channel model given in Sect. 3, that is, $h_{ij} \sim \mathcal{CN}(0, \mu_{ij})$. It is assumed that $\mu_{ij} = d_{ij}^{-\eta}$, where d_{ij} is the distance between node i and j, and $\eta = 3$ is the path loss exponent. In what follows, the notation "SNR" stands for the ratio of P to N_0, that is, ρ in Sect. 3.2. The fountain decoding overhead is set to be $\delta = 0.05$, which is a typical value for fountain-coding based transmissions [62].

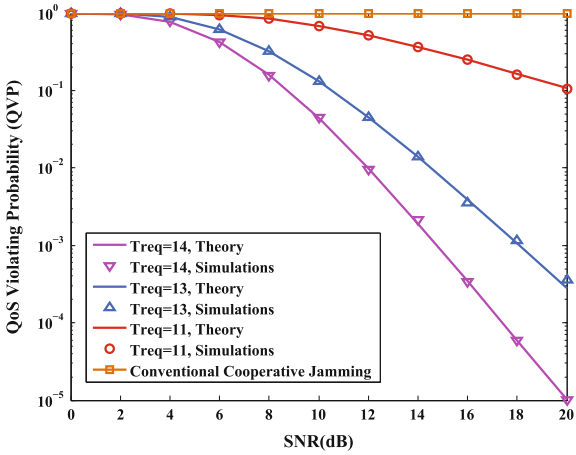

Fig. 10 QoS violating probability versus the average SNR of the system, where $R = 1$ bpcu, $K = 10$, and $\delta = 0.05$

The QVP-SNR curve is depicted in Fig. 10, where $R = 1$ bpcu and $K = 10$. Three values of T_{req} are considered. As is observed from Fig. 10, the QVP falls off with SNR as a waterfall shape, and the simulation results perfectly match the theoretical ones, verifying the correctness of the analysis. Also, T_{req} has a significant impact on the system performance. For the system with the most stringent delay constraint, that is, $T_{req} = 11 = \lceil (1+\delta)K \rceil$, the QVP remains as high as 10^{-1} even when SNR is 20 dB. However, if the system can tolerate a certain amount of delay, for example, $T_{req} = 14$, the QVP can be reduced to below 10^{-4} for high SNR regimes. As a comparison, the QVP curve for the conventional co-operative jamming scheme is also shown. This scheme also employs the fountain-coding based transmission framework; however, it does not adopt the constellation-rotation technique for signal design at the physical layer. As a result, the jamming signal does great harm to the legitimate terminals, thus making it difficult for the destination to accumulate the required number of fountain packets within the delay bound. This is why the QVP for the conventional co-operative jamming scheme keeps as high as 1 regardless of the SNR values.

The impact of T_{req} on the achievable QVP performance is further investigated in Fig. 11, where $R = 1$ bpcu and $K = 10$. In this figure, the QVPs are obtained from the theoretical results given in Sect. 3.4. The "asymptotic results" are obtained from the QVP expression by letting $T_{req} = \infty$, which corresponds to the information intercept probability. It can be seen from Fig. 11 that, when T_{req} is small, the system QVP can be reduced quickly as T_{req} increases. This is because, for small T_{req}'s, QVP is dominated by the delay violating probability. Therefore, the larger T_{req} is, the easier the system can accumulate the N fountain packets within the delay bound. However, when increasing T_{req} further, the system QVP cannot be significantly improved and will finally converge to a constant. This is because the system performance is mainly determined by the information intercept probability for the large T_{req} case. The information intercept probability, which reflects the system secrecy performance, cannot be improved by relaxing the delay constraint.

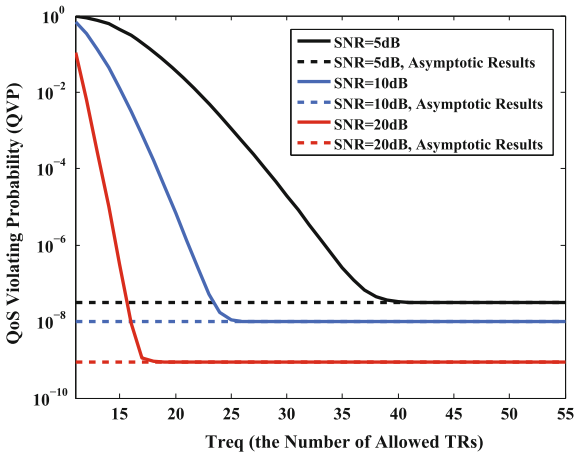

Fig. 11 QoS violating probability versus the number of allowed TRs (T_{req}), where $R = 1$ bpcu, $K = 10$, and $\delta = 0.05$

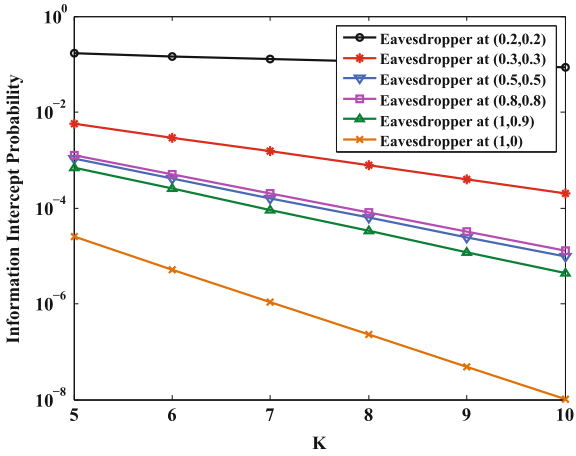

Fig. 12 Information intercept probability versus the number of source packets in each file (K), where $R = 1$ bpcu, $\delta = 0.05$, and SNR = 15 dB

Figure 12 plots the information intercept probability as a function of the value of K (i.e., the number of source packets contained in each file to be transmitted), where $R = 1$ bpcu and SNR = 15 dB. In this figure, the intercept probabilities for various eavesdropper positions are presented and compared. An important observation from Fig. 12 is that the information intercept probability is reduced to zero near-exponentially with K increasing. Therefore, a desired security level can be satisfied by selecting an appropriate value of K. For example, when the eavesdropper is located at (1, 0), the system intercept probability is below 10^{-8} for $K = 10$, which can be neglected in practice. In real-world V2V communications, there might be a need to transmit video data, for which each file consists of a large number of packets. Therefore, the large K condition is easy to satisfy, and the proposed scheme can be used to realize secure data delivery.

Finally, the average secure throughput of the system is examined, which is defined as,[7]

$$\eta = \frac{K}{\mathrm{E}[T_{secu}]}. \tag{62}$$

In the above definition, $\mathrm{E}[T_{secu}]$ is the average number of TRs that is needed to deliver the file *securely*, which can be calculated as

$$\mathrm{E}[T_{secu}] = \sum_{k=N}^{\infty} k\Pr(T_{\mathrm{tot,D}} = k,\ T_{\mathrm{tot,E}} > k). \tag{63}$$

The average secure throughput characterizes the average number of source packets that can be securely transmitted during each TR. Clearly, the average secure throughput cannot be larger than 1. Figure 13 exhibits the relationship between the average secure throughput and the value of K, with $R = 2$ bpcu. As observed from this figure, the average secure throughput is an increasing function of K, which implies that the transmission efficiency can be improved by choosing a larger value of K. To make a comparison, the average secure throughput curve is also plotted for the system without using the FC-based transmission strategy. For this benchmark system, the source packets are directly transmitted through the wireless channels, and only the physical-layer jamming approach (shown in Sect. 3.3) is adopted to secure the communications. The average secure throughput of such systems simply equals one minus the secrecy outage probability, which is irrelevant with K. It can be seen from Fig. 13 that, for SNR = 10 and 12 dB, the average secure throughput achieved by the conventional method is obviously smaller than that achieved by the proposed design. When SNR = 15 dB, the conventional scheme outperforms that proposed for $K \leq 7$. However, by choosing a larger K, the superiority of the proposed scheme can be observed. Moreover, the performance gap becomes larger when increasing the value of K.

3.6 Conclusions

In this section, a fountain-coding aided strategy is proposed for secure co-operative transmission in vehicular networks. The proposed scheme combines fountain coding at the application layer and co-operative jamming at the physical layer. By adopting fountain codes, the security of data delivery can be realized as long as the legitimate user can accumulate enough fountain packets before the eavesdropper does. To satisfy this condition, a constellation-rotation based jamming approach is designed

[7]This metric can be viewed as a modification of the average end-to-end throughput defined in [61] which is suitable for evaluating the transmission efficiency of the fountain-coding based strategy. Here the original definition is modified to make it applicable to the eavesdropping environments.

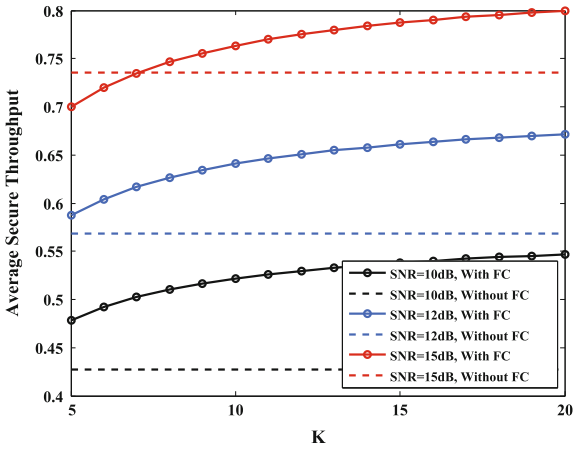

Fig. 13 Average secure throughput versus the number of source packets in each file (K), where $R = 2$ bpcu and $\delta = 0.05$

to increase the difference in channel qualities between the source-destination and source-eavesdropper transmissions. Furthermore, a novel metric called the QoS violating probability is developed, which gives a comprehensive characterization for the performance of the protocols, including reliability, security, and delay as well. The closed-form expression for the QoS violating probability is derived, and the effectiveness of the theoretical analysis is verified through simulations.

4 Summaries

This chapter discussed secure data dissemination for relay-assisted vehicular communications towards future intelligent transportation systems. The main contributions of our work are twofold. For theV2V communications scenario, a distributed source-relay selection scheme with anti-eavesdropping capabilities was proposed, where a source-relay pair is selected to maximize the achievable secrecy rate. The proposed scheme can be realized in a fully distributed manner, thereby enjoying a low implementation complexity. The performance of this scheme was evaluated in terms of the secrecy outage probability, the intercept probability, and the diversity order. Second, for the V2I communications scenario, a cross-layer approach was developed to secure the end-to-end transmissions. In the proposed approach, fountain coding is applied at the application layer, and the constellation-rotation aided co-operative jamming is utilized at the physical layer. By combining these two techniques, the security of data delivery can be guaranteed. Furthermore, a novel metric called QoS violating probability was proposed to evaluate the system performance from the security-delay-reliability tradeoff perspective. The effectiveness of our theoretical achievements is verified via numerical simulations.

Physical layer security and vehicular networking are each separate hot research topics. However, the application of PLS techniques to real-world vehicular

communications is rather challenging, for which several technical issues have to be addressed. In the following, we briefly summarize some problems that are worthy of further investigation.

First, in vehicular networks, due to the fast movement of the vehicles, the communications environment varies the network topology and is highly dynamic. This poses nonnegligible difficulties for the design of PLS schemes. To be more specific, in our proposed strategies, security is achieved by exploiting the co-operation among neighboring vehicles. However, the frequent changes of the network topology make it extremely difficult to select an appropriate co-operating node in practice. In addition, the high-speed moving characteristic of the vehicles makes the channel coefficients change quickly with time. This requires the developed relay selection policy as well as the signal-processing algorithms to be executed in real-time. Otherwise, the channel state information collected at the nodes might be outdated, which yields significant performance degradation.

Second, all the vehicles are operated by drivers, whose behavior will no doubt affect the data transmission performance of vehicular communication systems. For instance, if the drivers of two vehicles, say A and B, have a very close social relationship, they might trust each other, and the data exchange between them will be very frequent as well. This motivates us to develop socially aware user co-operation mechanisms and secrecy enhancement schemes. From a theoretical point of view, the mutual impact between social relationships and system security performance is also of great research value.

Last but not least, in this work we only focus on the scenario where the V2V or V2I communication is subjected to external eavesdropping attacks. However, in practical vehicular communications, malicious users can attack the system in various manners. For example, the adversary might launch the active jamming attack to interrupt the communication sessions, or conduct the pilot contamination attack during the channel training phase to deteriorate the channel estimation results at the legitimate users. Therefore, it would be very important to design the PLS strategies to combat various types of attacks.

References

1. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys and Tutorials*, *13*(4), 584–616, 4th Quarter.
2. Mecklenbrauker, C. F., Molisch, A. F., Karedal, J., Tufvesson, F., Paier, A., Bemado, L., et al. (2011). Vehicular channel characterization and its implications for wireless system design and performance. *Proceedings of the IEEE*, *99*(7), 1189–1212.
3. Zhang, J., Zhang, Q., & Jia, W. (2009). VC-MAC: A cooperative MAC protocol in vehicular networks. *IEEE Transactions on Vehicular Technology*, *58*(3), 1561–1571.
4. Zhou, T., Sharif, H., Hempel, M., Mahasukhon, P., Wang, W., & Ma, T. (2011). A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks. *IEEE Journal on Selected Areas in Communications*, *29*(1), 72–82.

5. Nzouonta, J., Rajgure, N., Wang, G., & Borcea, C. (2009). Vanet routing on city roads using real-time vehicular traffic information. *IEEE Transactions on Vehicular Technology*, *58*(6), 3609–3626.
6. Harigovindan, V. P., Babu, A. V., & Jacob, L. (2012). Ensuring fair access in IEEE 802.11p-based vehicle-to-infrastructure networks. *EURASIP Journal on Wireless Communications and Networking*. doi:10.1186/1687-1499-2012-16.
7. Eiza, M. H., & Ni, Q. (2013). An evolving graph-based reliable routing scheme for VANETs. *IEEE Transactions on Vehicular Technology*, *62*(4), 1493–1504.
8. Lin, J. C., Lin, C. S., Liang, C. N., & Chen, B. C. (2012). Wireless communication performance based on IEEE 802.11p R2V field trails. *IEEE Communications Magazine*, *50*(5), 184–191.
9. Sendonaris, A., Erkip, E., & Aazhang, B. (2003). User cooperation diversity-Part I: System description. *IEEE Transactions on Communications*, *51*(11), 1927–1938.
10. Laneman, J. N., Tse, D. N. C., & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory*, *50*(12), 3062–3080.
11. Zhang, W., & Letaief, K. B. (2008). Full-rate distributed space-time codes for cooperative communications. *IEEE Transactions on Wireless Communications*, *7*(7), 2446–2451.
12. Bletsas, A., Shin, H., & Win, M. Z. (2007). Cooperative communications with outage-optimal opportunistic relaying. *IEEE Transactions on Wireless Communications*, *6*(9), 3450–3460.
13. Sun, L., Zhang, T., Lu, L., & Niu, H. (2010). On the combination of cooperative diversity and multiuser diversity in multi-source multi-relay wireless networks. *IEEE Signal Processing Letters*, *17*(6), 535–538.
14. Janani, M., Hedayat, A., Hunter, T. E., & Nosratinia, A. (2004). Coded cooperation in wireless communications: Space-time transmission and iterative decoding. *IEEE Transactions on Signal Processing*, *52*(2), 362–371.
15. Zeng, M., Zhang, R., & Cui, S. (2011). On the design of distributed beamforming for two-way relay networks. *IEEE Transactions on Signal Processing*, *59*(5), 2284–2295.
16. Ding, Z., & Leung, K. K. (2011). Cross-layer routing using cooperative transmission in vehicular ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, *29*(3), 571–581.
17. Ng, S. C., Zhang, W., Zhang, Y., Yang, Y., & Mao, G. (2011). Analysis of access and connectivity probabilities in vehicular relay networks. *IEEE Journal on Selected Areas in Communications*, *29*(1), 140–150.
18. Li, M., Yang, Z., & Lou, W. (2011). CodeOn: cooperative popular content distribution for vehicular networks using symbol level network coding. *IEEE Journal on Selected Areas in Communications*, *29*(1), 1–14.
19. Mukherjee, A., Fakoorian, S. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys and Tutorials*, *16*(3), 1550–1573, Third quarter.
20. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal*, *54*(8), 1355–1387.
21. Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348.
22. Tekin, E., & Yener, A. (2008). The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, *54*(6), 2735–2751.
23. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory*, *54*(6), 2515–2534.
24. Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, *7*(6), 2180–2189.
25. Vilela, J. P., Pinto, P. C., & Barros, J. (2011). Position-based jamming for enhanced wireless secrecy. *IEEE Transactions on Information Forensics and Security*, *6*(3), 616–627.
26. Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, *58*(3), 1875–1888.
27. Zheng, G., Choo, L.-C., & Wong, K.-K. (2011). Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Transactions on Signal Processing*, *59*(3), 1317–1322.

28. Sun, L., Zhang, T., Li, Y., & Niu, H. (2012). Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *IEEE Transactions on Vehicular Technology*, *61*(8), 3801–3807.
29. Krikidis, I. (2010). Opportunistic relay selection for cooperative networks with secrecy constraints. *IET Communications*, *4*(15), 1787–1791.
30. Krikidis, I., Thompson, J. S., & McLaughlin, S. (2009). Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, *8*(10), 5003–5011.
31. Liu, Y., Li, J., & Petropulu, A. P. (2013). Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Transactions on Information Forensics and Security*, *8*(4), 682–694.
32. Zhao, H., Lu, L., Song, C., Wu, Y. (2012). IPARK: Location-aware-based intelligent parking guidance over infrastructures VANETs. *International Journal of Distributed Sensor Networks*, Article ID: 280515. doi:10.1155/2012/280515.
33. Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, *46*(6), 164–171.
34. Seddik, K. G., Ibrahim, A. S., & Liu, K. J. R. (2008). Trans-modulation in wireless relay networks. *IEEE Communications Letters*, *12*(3), 170–172.
35. Wang, T., Giannakis, G. B., & Wang, R. (2008). Smart regenerative relays for link-adaptive cooperative communications. *IEEE Transactions on Communications*, *56*(11), 1950–1960.
36. Bletsas, A., Khisti, A., Reed, D. P., & Lippman, A. (2006). A simple cooperative diversity method based on network path selection. *IEEE Journal on Selected Areas in Communications*, *24*(3), 659–672.
37. Ding, Z., Leung, K. K., Goeckel, D. L., & Towsley, D. (2009). On the study of network coding with diversity. *IEEE Transactions on Wireless Communications*, *8*(3), 1247–1259.
38. Ding, H., Ge, J., da Costa, D. B., & Jiang, Z. (2011). A new efficient low-complexity scheme for multi-source multi-relay cooperative networks. *IEEE Transactions on Vehicular Technology*, *60*(2), 716–722.
39. Seyfi, M., Muhaidat, S., Liang, J., & Uysal, M. (2011). Relay selection in dual-hop vehicular networks. *IEEE Signal Processing Letters*, *18*(2), 134–137.
40. Ge, Y., Wen, S., Ang, Y.-H., & Liang, Y.-C. (2010). Optimal relay selection in IEEE 802.16j multihop relay vehicular networks. *IEEE Transactions on Vehicular Technology*, *59*(5), 2198–2206.
41. Niu, H., Zhu, N., Sun, L., Vasilakos, A. V., & Sezaki, K. (2015). Security-embedded opportunistic user cooperation with full diversity. *Wireless Networks*. doi:10.1007/s11276-015-1044-7.
42. Park, K.-H., Wang, T., & Alouini, M. (2013). On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE Journal on Selected Areas in Communications*, *9*(31), 1741–1750.
43. Fan, L., Lei, X., Duong, T. Q., Elkashlan, M., & Karagiannidis, G. K. (2014). Secure multiuser commucations in multiple amplify-and-forward relay networks. *IEEE Transactions on Communications*, *62*(9), 3299–3310.
44. Hoang, T. M., Duong, T. Q., Suraweera, H. A., Tellambura, C., & Poor, H. V. (2015). Cooperative beamforming and user selection for improving the security of relay-aided systems. *IEEE Transactions on Communications*, *63*(12), 5039–5051.
45. Bao, V., L-Trung, N., & Debbah, M. (2013). Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. *IEEE Transactions on Wireless Communications*, *12*(12), 6076–6085.
46. Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, *31*(10), 2099–2111.
47. Ikki, S., & Ahmed, M. H. (2007). Performance analysis of cooperative diversity wireless networks over Nakagami-m fading channel. *IEEE Communications Letters*, *11*(4), 334–336.
48. Xu, F., Lau, F. C. M., Zhou, Q. F., & Yue, D. W. (2009). Outage performance of cooperative communication systems using opportunistic relaying and selection combining receiver. *IEEE Signal Processing Letters*, *16*(4), 237–240.

49. Pappi, K. N., Diamantoulakis, P. D., Otrok, H., & Karagiannidis, G. K. (2015). Cloud compute-and-forward with relay cooperation. *IEEE Transactions on Wireless Communications*, *14*(6), 3415–3428.
50. Sun, L., Zhang, T., & Niu, H. (2011). Inter-relay interference in two-path digital relaying systems: Detrimental or beneficial? *IEEE Transactions on Wireless Communications*, *10*(8), 2468–2473.
51. Zhang, X., McKay, M. R., Zhou, X., & Heath, R. W. (2015). Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Transactions on Wireless Communications*, *14*(5), 2742–2754.
52. Jayasinghe, K., Jayasinghe, P., Rajatheva, N., & Latva-aho, M. (2014). Secure beamforming design for physical layer network coding based MIMO two-way relaying. *IEEE Communications Letters*, *18*(7), 1270–1273.
53. Luo, S., Li, J., & Petropulu, A. P. (2013). Uncoordinated cooperative jamming for secret communications. *IEEE Transactions on Information Forensics and Security*, *8*(7), 1081–1090.
54. Wang, X., Tao, M., Mo, J., & Xu, Y. (2011). Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks. *IEEE Transactions on Information Forensics and Security*, *6*(3), 693–702.
55. Mo, J., Tao, M., Liu, Y., & Wang, R. (2014). Secure beamforming for MIMO two-way communications with an untrusted relay. *IEEE Transactions on Signal Processing*, *62*(9), 2185–2199.
56. Zou, Y., Wang, X., Shen, W., & Hanzo, L. (2014). Security versus reliability analysis of opportunistic relaying. *IEEE Transactions on Vehicular Technology*, *63*(6), 2653–2661.
57. Sun, L., Ren, P., Du, Q., Wang, Y., & Gao, Z. (2015). Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Communications Letters*, *19*(3), 463–466.
58. Sun, L., Du, Q., Ren, P., & Wang, Y. (2016). Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation. *IEEE Transactions on Vehicular Technology*, *65*(10), 8767–8774.
59. MacKay, D. J. C. (2005). Fountain codes. *IEE Proceedings of the Communications*, *152*(6), 1062–1068.
60. Zhang, X., & Du, Q. (2006). Adaptive low-complexity erasure-correcting code-based protocols for QoS-driven mobile multicast services over wireless networks. *IEEE Transactions on Vehicular Technology*, *55*(5), 1633–1647.
61. Wang, X., Chen, W., & Cao, Z. (2011). SPARC: Superposition-aided rateless coding in wireless relay systems. *IEEE Transactions on Vehicular Technology*, *60*(9), 4427–4438.
62. Niu, H., Iwai, M., Sezaki, K., Sun, L., & Du, Q. (2014). Exploiting fountain codes for secure wireless delivery. *IEEE Communications Letters*, *18*(5), 777–780.
63. Boutros, J., & Viterbo, E. (1998). Signal space diversity: A power- and bandwidth-efficient diversity technique for the Rayleigh fading channel. *IEEE Transactions on Information Theory*, *44*(4), 1453–1467.
64. Gradshteyn, I. S., & Ryzhik, I. M. (2007). *Table of integrals, series, and products* (7th ed.). New York: Academic Press.

Part III
Practices

Tools and Practices

Xuerong Cui and Juan Li

Abstract In recent years, along with the rapid development of the GNSS (global navigation satellite system), cellular network, and IoT (Internet of things), vehicle networking has entered into a wireless interconnected and intelligent era that makes remote-operating vehicles or sharing information convenient. However, the vehicle wireless networks connected to physical components of vehicles make it possible for hackers to engage in wireless sabotage. This chapter presents various vulnerable physical components, reactions from government and industry against the cyber-attacks, attacking tools, attacking practices, and some mitigation strategies.

Keywords Vehicle networking · Cyber-attack tools · Cyber-attack practices

1 Introduction

Vehicle networking has entered into a wireless interconnected and intelligent era. "About one in five vehicles on the road worldwide will have some form of wireless network connection by 2020, amounting to more than 250 million connected vehicles," [1] reported Gartner, the world's leading information technology research and advisory company. It is possible for hackers to engage in wireless sabotage no matter whether it is IEEE 802.11p [2] WAVE (wireless access in the vehicular environment), cellular wireless network, Bluetooth, or Wi-Fi network. "Reports of hackers gaining remote access to the latest car models from manufacturers such as Land Rover, Jeep, Toyota, Chrysler, BMW, Ford and General Motors have flooded the Internet" [3].

X. Cui (✉) · J. Li
Department of Computer and Communication Engineering,
China University of Petroleum (East China), Qingdao 266580, China
e-mail: cuixuerong@163.com

J. Li
e-mail: lijuanlijuan@sina.com

Y. Sun and H. Song (eds.), *Secure and Trustworthy Transportation Cyber-Physical Systems*, SpringerBriefs in Computer Science, DOI 10.1007/978-981-10-3892-1_7

2 Vulnerable Physical Components of Vehicles

The Summary of Findings [4] from Intel Automotive Security Research Workshops describes some of the IVI potential threat areas as shown in Fig. 1. Totally vulnerable physical components of vehicles include the electronic control unit (ECU), controller area network (CAN), GNSS, and software.

2.1 ECU

ECU is a generic term for any of a wide array of embedded computer modules that receive input from electronic sensors and control different electrical functions by actuators.

The ECU of a vehicle is akin to the brain of a person, which is used to regulate the engine and maintain optimal performance. Some vehicles have more than 80 ECUs and types of these ECUs include the engine control module (ECM), powertrain control module (PCM), brake control module (BCM), transmission control module (TCM), central control module (CCM), central timing module (CTM), general electronic module (GEM), body control module (BCM), suspension control module (SCM), and so on. These modules often consist of a microprocessor, random access memory (RAM), read only memory (ROM), and an input/output interface.

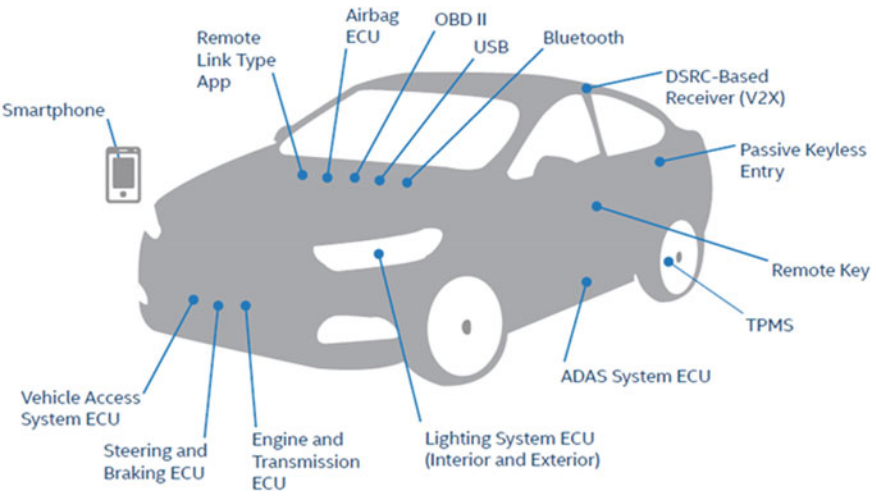

Fig. 1 Potential threats

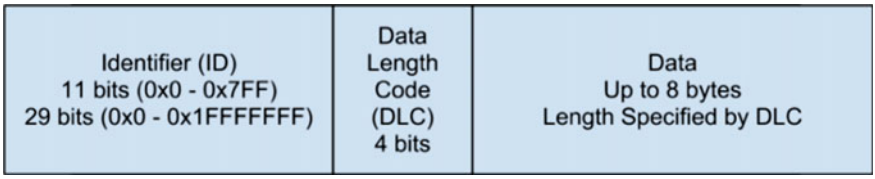

Fig. 2 Structure of CAN packet

2.2 CAN

CAN is a serial bus system that was originally designed for the communication system between ECUs in vehicles, but has also become a popular bus in industrial automation as well as other applications. It is a two-wire, half-duplex, high-speed network system and is well suited for high-speed applications using short messages. A single CAN packet consists of identifier, data length code, and data, shown in Fig. 2.

CAN frames are limited to 8 bytes of data. To overcome this limitation, the ISO 15765-2 standard, often called ISO-TP is used. This standard provides a way of packaging longer data into multiple frames.

Using CAN, peer stations (controllers, sensors, and actuators) are connected via a serial bus. Typically, many of today's modern vehicles' CANs are able to be accessed via wireless communication. CAN-based systems typically assume that anyone accessing the network is trusted. Once a device is placed on a CAN it is able to read all traffic, send fraudulent messages, or perform a denial of service attack. Thus, once a hacker gains access to the vehicle's CAN which is connected to all of the ECUs, the only challenge to the hacker is just the vehicle discovering the functions of each CAN message.

2.3 OBD-II

The OBD-II [5] (on-board diagnostic) standard is used for basic vehicle diagnostics. During the 1970s and early 1980s manufacturers started using electronic means to control engine functions and diagnose engine problems. This was primarily to meet EPA emission standards. Through the years on-board diagnostic systems have become more sophisticated. OBD-II, a new standard introduced in the mid-1990s, provides almost complete engine control and also monitors parts of the chassis, body, and accessory devices, as well as the diagnostic control network of the car.

At first there were few standards and each manufacturer had its own systems and signals. In 1988, the Society of Automotive Engineers (SAE) set a standard connector plug and set of diagnostic test signals. The EPA adapted most of their standards from the SAE on-board diagnostic programs and recommendations.

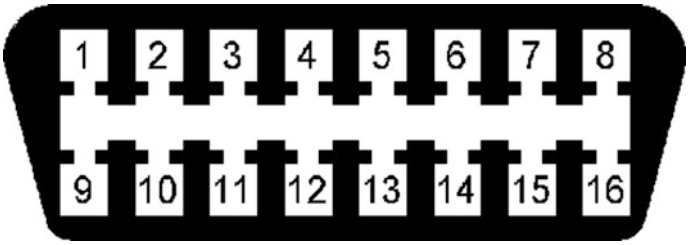

Fig. 3 OBD II connector [5]

OBD-II is an expanded set of standards and practices developed by SAE and adopted by the EPA and CARB (California Air Resources Board) for implementation by January 1, 1996.

The connector of SAE J1962 is shown in Fig. 3.

- Pin 4—Chassis Ground
- Pin 5—Signal Ground
- Pin 6—CAN High (J-2284)
- Pin 7—ISO 9141-2 K Line
- Pin 10—J1850 Bus
- Pin 14—CAN Low (J-2284)
- Pin 15—ISO 9141-2 L Line
- Pin 16—Battery Power

2.4 GNSS

Most advanced vehicles have infotainment systems whose wireless security and wireless access points are all connected into the navigation system. Navigation systems are more susceptible to be hacked because GNSS cheating may exist.

Nowadays, there exist four main global navigation satellite systems: GPS (global positioning system) of the United States, GLONASS (global navigation satellite system) of Russia, Galileo of the European Union, and BDS (Beidou system) of China. However, the GNSS is susceptible to both intentional and unintentional interference, including jamming and spoofing; therefore the latter may be used by a hacker.

2.5 Software

Driven by consumer expectations for convenience and interoperability, vehicles' in-vehicle software is getting more and more complex, such as Wi-Fi access points,

the ability to play MP3s, touchscreens, feature-rich operating systems, and consumer device interoperability.

A common approach to hacking the software is to replace trusted software components with malicious software that can be used to affect the confidentiality, integrity, and availability of the system. This can be done either by a persistent change (such as installing new binaries) or dynamically (with in-memory changes, perhaps) [4].

3 Reactions Against Cyber-Attacks

3.1 Intel

In order to lessen and address cybersecurity risks associated with connected automobiles and create long-term research roadmaps and facilitate specific projects, Intel established the Automotive Security Review Board (ASRB) [6] in 2016 which is an open and independent global research organization and is composed of some top experts from the automotive, security, and information technology industries across the globe. Moreover, ASRB's research arm is tasked to perform continuous security tests and inspections, which will serve as the basis for best practices and design recommendations for vehicle cybersecurity solutions and products that will benefit both the industry and driver. Chris Young, Intel senior vice president and general manager for security, said. We can, and must, raise the bar against cyberattacks in automobiles. With the help of the ASRB, Intel can establish security best practices and encourage that cybersecurity is an essential ingredient in the design of every connected car. Few things are more personal than our safety while on the road, making the ASRB the right idea at the right time.

Intel also announced that it has already published the first white paper version, "Automotive Security Best Practices: Recommendations for Security and Privacy in the Era of the Next-Generation Car" [7], which the company will continue to update based on the findings of ASRB. The study in this white paper breaks down the risks involved with connected vehicles and makes the appropriate recommendations to address the security problem.

3.2 United States

The *Moving Ahead for Progress in the 21st Century Act* (MAP-21) Division C, Title I, Subtitle D, Section 31402 requires that the agency examine the need for safety standards with regard to electronic systems in passenger motor vehicles. NHTSA (National Highway Traffic Safety Administration) released four automotive cybersecurity reports in October 2014: *Assessment of the Information Sharing and Analysis Center Model* [8], *A Summary of Cybersecurity Best Practices* [9], *Characterization of Potential Security Threats in Modern Automobiles: A*

Composite Modeling Approach [10], and *National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles* [11].

The Electronic Systems Safety (ESS) Research Division of the NHTSA Vehicle Research and Test Center (VRTC) conducts research to ensure the safety, security, and reliability of the interconnected, complex electronic systems.

It was reported by *Computerworld* [12] that on July 21, 2015 two US senators filed a bill [13] that would require the federal government to establish standards to ensure that automakers secure a driver against vehicle cyber-attacks. In this way, consumers may know how well the vehicle protects drivers' security and privacy beyond the proposed federal minimum standards.

3.3 VisualThreat

VisualThreat is a leading connected-car security vendor based in Silicon Valley. The company offers a vehicle cybersecurity protection framework (FUSE) to minimize penetration from cyber-attacks.

In 2015, VisualThreat established VisualThreat Auto Cybersecurity Testing Lab, the first comprehensive connected-car security testing lab in the industry to cover TSP cloud service, telematics control unit, OBD dongle, and an auto mobile app.

The Lab's Security Testing Matrix contains the following testing categories.

(1) Communication security
(2) Telematics service
(3) Functional security
(4) Privacy leakage assessment
(5) Intelligent device
(6) Auto mobile app security vulnerabilities
(7) Comprehensive security testing report

Why the VisualThreat Auto Cybersecurity Testing Lab?

VisualThreat has helped car makers, TSP providers, car-sharing companies, OBD dongle manufacturers, and mobile app developers to find security vulnerabilities in their products and services. There is a high demand for an auto security testing service while designing a new telematics unit, Car OS, and telematics cloud platform. Instead of focusing on interior device security, such as ECU and gateway, their point of differentiation lies in securing the "edge" between the car and its exterior communications, where the most auto cyber-attacks originate. More than 60 testing checkpoints will be applied through the testing:

(1) Telematics unit
(2) TSP cloud platform
(3) OBD dongle
(4) Auto mobile app

4 Tools

4.1 Carwall

Karamba Security has released Carwall [14], an in-vehicle security software that can automatically secure connected cars against cyber-attacks and is the automotive industry's first autonomous security solution. Carwall hardens the ECU's software run-time environment to detect and prevent all attempted attacks. Carwall doesn't fix the security bugs in your code; it prevents their exploitation by permitting only the running of operations that comply with the ECU's factory settings.

Carwall seamlessly integrates into the software development environment and automatically seals the software against cyber-attacks. Its lightweight embedded software contains multiple security layers, which are:

- Validate in-memory functional flows to avoid in-memory attacks.
- Inspect and enforce programs so they load according to factory settings.
- Control ECU Internet connectivity to avoid architectural flaws.
- Control input from external devices to eliminate malware implants by a peripheral device.

Karamba's software seals the car's electronic control units by automatically creating security policies, based on factory settings. In real-time, Carwall detects and prevents anything not explicitly allowed to load or run on the ECU, including in-memory attacks.

4.2 Vector Solutions

The company of Vector Software GmbH provides OEMs and suppliers of automotive and related industries a professional and open development platform of tools, software components, and services for creating embedded systems [15].

Vector supports with professional tools, basic software, and services as shown in Fig. 4.

What should be mentioned is the CANoe which is a comprehensive software tool for development, testing, and analysis of entire ECU networks and individual ECUs. It supports throughout the entire development process: from planning up to final system-level tests.

The CANoe user interface with control and display panels, analysis windows, and the Trace Window is shown in Fig. 5.

(1) Analysis
This covers the analysis of the multibus communication of ECUs and entire systems at the development workplace as well as directly in the vehicle.

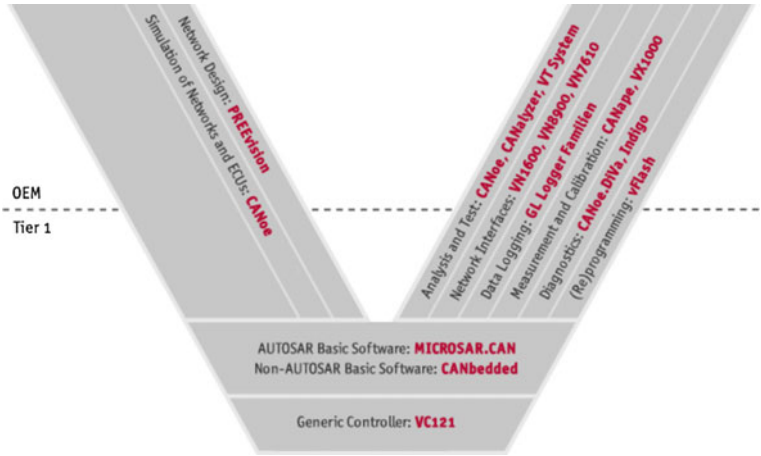

Fig. 4 Vector solutions [15]

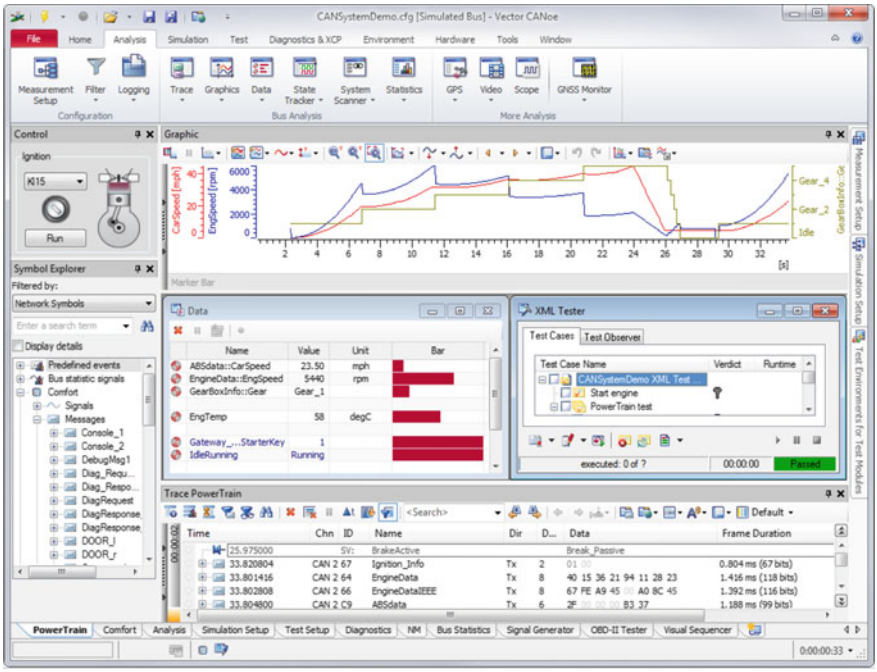

Fig. 5 CANoe user interface

(2) Simulation
Manual or automatical simulation from the underlying communication database is supported in CANoe. This remaining bus simulation of communication behavior is the basis for the subsequent analysis and testing phases. Via specific OEM packages the CANoe simulation can be adjusted to the requirements of the respective OEM. Real-time relevant simulation and test functions in combination with the hardware CANoe RT Rack are executed on a dedicated platform, that is, separate from the graphic user interface. CANoe offers many different ways to stimulate ECUs in the network: the bandwidth ranges from pre-defined user interfaces to different programming options.
(3) Testing
CANoe represents the state-of-the-art test environment. It is the ideal testing tool as well for the entire system.
(4) Diagnostics/Diagnostic Tester
CANoe may be used both as a diagnostic tester and to simulate ECU diagnostics. In addition a complete OBD-II Tester is integrated.

4.3 FUSE

FUSE [16] is the cybersecurity protection framework of VisualThreat Inc., which includes F—Firewall, U—Umbrella Policy, S—Security-Over-The-Air (SOTA), and E—Event Intelligence.

Visual Threat's patent-pending firewall technology adds protection on the vehicle to minimize penetrations from cyber-attacks. The Firewall API provides a simple and REST-based interface to take connected-car security to a whole new level. OEMs and tier providers can use scalable APIs to integrate VisualThreat security features on their platforms.

(1) Umbrella: Security Policy Enforcement

By providing an in-line protection function coupled with flexible security policy enforcement, VisualThreat's policy deployment solution enables car OEMs to discover various attack scenarios in real-time.

(2) Security Over-The-Air

VisualThreat's SOTA solution facilitates on-the-fly preventions of car hackings. Instead of tedious updating works, SOTA makes security deployment a seamless and invisible process.

(3) Event intelligence: auto data threat analytics

VisualThreat meets security demands by leveraging event analytics that are scalable and perform threat correlations across heterogeneous attack vectors. Their real-time intelligent portal gives access to all threat-related information and scan-at-a-glance risk status in one streamlined user interface.

4.4 CANtact

CANtact [17], shown in Fig. 6, is an open source CAN to USB interface for computers developed by Eric Evenchick, a former employee of Tesla. It can connect to any CAN-enabled car using a standard OBD-II cable. The device can be connected to Windows, Linux, or an Apple computer. When it is plugged into the OBDII port of a car, what is going on in the car can be found.

It is an open source and full source code and hardware design files are available on Github (http://github.com/cantact).

4.5 CANard Toolkit

CANard [18] is software that can send and receive messages and encode and decode data. It is a Python library for communicating with CAN bus systems, released by Eric Evenchick at the Black Hat Asia 2015 Conference.

Providing hardware abstraction, CANard achieves a variety of CAN adapter support, and provides a unified call interface. At the same time, CANard supports many kinds of upper layer protocol communication, such as CAN-TP (Controller Area Network Transport Protocol), OBD-II, and UDS (Unified Diagnostic Services).

Fig. 6 A first batch v1.0 CANtact tool

It is capable of sending and receiving frames on a network, and includes support for protocols that are commonly used on CAN. This toolkit has a few goals:

- Hardware abstraction
- Protocol implementation
- Ease of automation
- Sharing of information

CANard encapsulates CAN frames as Python objects. These frame objects can be sent, received, logged, and inspected. The following codes create a standard CAN frame with identifier 0x123, data length code 5, and data bytes 1, 2, 3, 4, 5. This example frame can now be sent using a hardware device. This simple interface makes it easy to generate and send payloads, or analyze frames received from the bus.

```
from canard import can

f = can.Frame(0x123)
f.dlc = 5
f.data = [1,2,3,4,5]
```

Because traditional PCs lack a CAN bus interface, an external adapter is required. A variety of adapters exists to provide a CAN bus interface over USB. Each has its own drivers and tools. CANard allows developers to build utilities that deal with raw CAN data and standard protocols. Due to the hardware abstraction provided by the library, scripts can be used across various operating systems and with a multitude of CAN bus adapters. A simple script using CANard is shown in listing 5. This script performs a denial of service attack by sending a message with identifier 0 at a high rate. In this example, a CANtact device is used.

```
from canard import can
from canard.hw import cantact

# create and start device
dev = cantact.CantactDev('/dev/cu.usbmodem14514')
dev.start()

# create our payload frame
frame = can.Frame(id=0)
frame.dlc = 8

# spam!
while True:
    dev.send(frame)
```

The CANard library provides a UdsInterface class that deals with packaging UDS messages, sending them, receiving a response, and parsing the response data. This makes it easier to write scripts to fuzz and exploit diagnostic systems. For example, the following example attempts to discover UDS-enabled devices by requesting a diagnostic session on a range of IDs.

```
import sys

from canard.proto.uds import UdsInterface
from canard.hw.cantact import CantactDev

d = CantactDev(sys.argv[1])
d.set_bitrate(500000)
d.start()

p = UdsInterface(d)

# DiagnosticSessionControl Discovery
for i in range(0x700, 0x800):
    # attempt to enter diagnostic session
    resp = p.uds_request(i, 0x10, [0x1], timeout=0.2)
    if resp != None:
        print("ECU response for ID 0x%X!" % i)
```

Using CANard can enable users to understand how their connected cars work in order to see if there is any tweak they can make to enhance the system further. It can also be used to check whether there are any security vulnerabilities where hackers can take advantage. On top of that, it also can be used to modify the data to an insurance OBDII port device as well as to change the emission test results which can break the law.

4.6 RollJam

"RollJam," shown in Fig. 7, is a device that can intercept and store keyless entry codes and allow its user unfettered access to the automobile or garage. The concept is fairly simple [19], as shown in the following three steps (Figs. 8, 9 and 10).

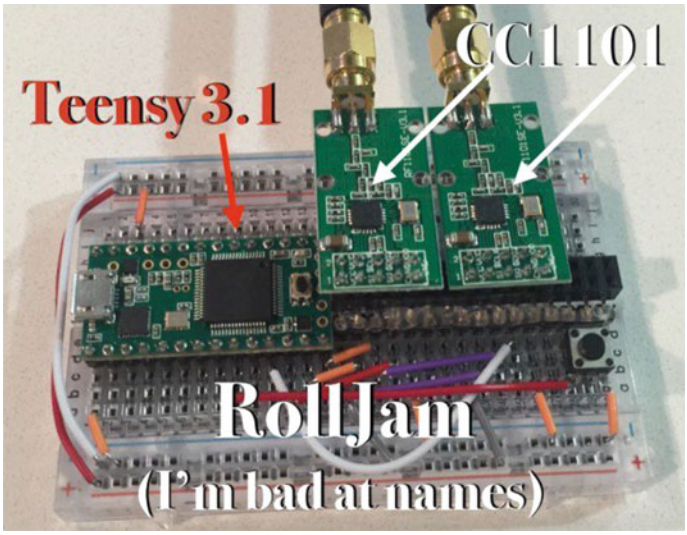

Fig. 7 Picture of RollJam [19]

Fig. 8 Step 1

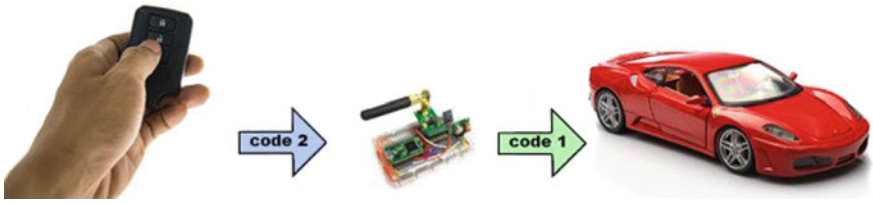

Fig. 9 Step 2

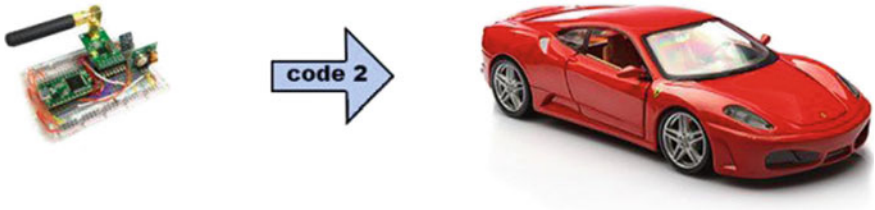

Fig. 10 Step 3

The RollJam, detecting a signal, jams the vehicle's frequency. The code is intercepted and stored [19].

The user clicks the button again and the RollJam broadcasts the old code while simultaneously capturing the new one. The car unlocks [19].

The RollJam device is retrieved, still holding the new unused code. The code can then be transmitted later to unlock the car [19].

5 Practices

5.1 Hacking the Software

As we know, OnStar software is GM's subscription-based, invehicle service that provides vehicle security, hands-free calling, turn-by-turn navigation, and remote

diagnostics. RemoteLink is the OnStar mobile app that allows users to unlock and remote-start their vehicles from almost anywhere. RemoteLink also can turn on headlights, sound the horn, and manage an equipped vehicle's Wi-Fi hotspot.

Samy Kamkar has posted a video on YouTube [20] demonstrating how a device he made could intercept wireless communications between OnStar RemoteLink and the OnStar cloud service [21].

After opening the RemoteLink on a mobile phone, Kamkar's device, called OwnStar, can intercept the communication and send "specially crafted" data packets to the mobile device to acquire additional credentials. The OwnStar device then notifies the attacker about the new vehicle that he has access to for an indefinite period of time, including its location, make, and model. And at that point, the hacker can use the RemoteLink app to control the vehicle. For example, he could locate, unlock, and remotely start GM vehicles. "Fortunately, the issue lies in the mobile software and is not a problem with the vehicles themselves," Kamkar said.

Kamkar has also proved that Fiats and Chryslers with early model versions of the UConnect Infotainment system could be broken into electronically, and the UConnect system used to control vital vehicle functions. Thus hackers would be able to control vehicle acceleration, braking, and ignition systems, among others (Fig. 11).

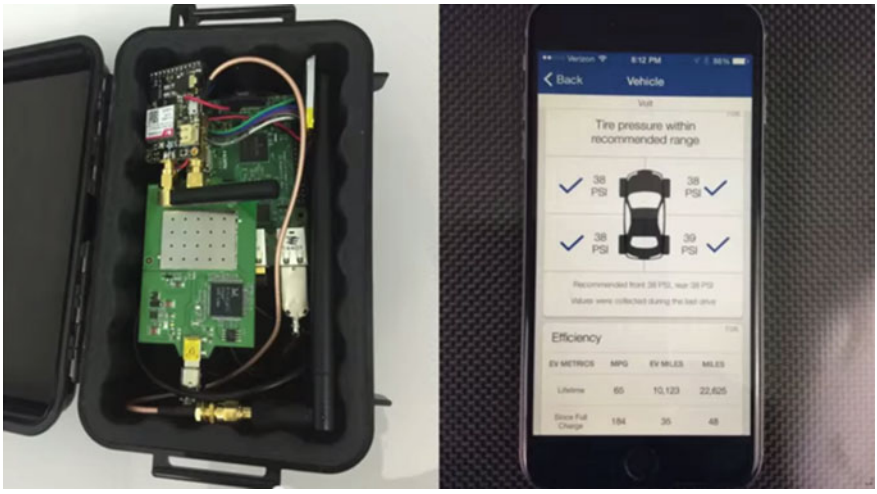

Fig. 11 On the left is Kamkar's "OwnStar" device that he used to intercept a "nearby" mobile phone using the OnStar RemoteLink app. The right shows his own phone linked to the other user's RemoteLink app [21]

5.2 Hacking the CAN

WIRED has posted a video on YouTube [22] demonstrating two security experts, Charlie Miller and Chris Valasek, who successfully hacked a 2015 Jeep Cherokee's CAN via a cellular connection; that is, physical access was not required for the vehicle hack. The two hackers were 10 miles away from the car with the *WIRED* reporter driving. In the video, the hackers were able to manipulate its radio and windshield wipers and even shut the car down. Almost everything from steering and braking to seatbelts and the radio could be remotely controlled.

The hackers are able to use the cellular connection to the Jeep's entertainment system or head unit to gain access to other systems that are commonly connected to various electronic control units located throughout a modern vehicle. There can be as many as 200 ECUs in a vehicle [23] (see Fig. 12).

Miller said the vulnerability that allowed the attack is exclusive to Chrysler's UConnect head unit, but there are likely similar types of security holes on other vehicles' telematics systems.

After this hack event, Chrysler issued a recall notice for 1.4 million vehicles in order to fix this software hole that allowed hackers to break into some vehicles wirelessly and electronically control vital functions.

Fig. 12 On the left is the hacking tool that they used. The right, shows how the hackers can control the steering [22]

References

1. Gartner Says By 2020. A quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities, 2016-10-25. http://www.gartner.com/newsroom/id/2970017.
2. IEEE 802.11p-2010 (2010). 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.
3. Intel launches automotive security review board to ensure cybersecurity of cars, 17 Sept 2015.
4. Intel automotive security research workshops—Summary of findings. https://www-ssl.intel.com/content/dam/www/public/us/en/documents/product-briefs/automotive-security-research-workshops-summary.pdf.
5. OBD-II Background. http://www.obdii.com/background.html.
6. Automotive security review board. https://asrb.org/.
7. Automotive cybersecurity best practices white paper. http://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf.
8. McCarthy, C., Harnett, K., Carter, A., Hatipoglu, C. Assessment of the information sharing and analysis center model. https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812076-AssessInfoSharingModel.pdf.
9. McCarthy, C., Harnett, K., Carter, A. A summary of cybersecurity best practices. https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf.
10. McCarthy, C., Harnett, K., Carter, A. Characterization of potential security threats in modern automobiles: A composite modeling approach. https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf.
11. National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles.
12. Senators propose bill to tighten vehicle security, privacy standards. http://www.computerworld.com/article/2950520/data-privacy/senators-propose-bill-to-tighten-vehicle-security-privacy-standards.html.
13. A BILL To protect consumers from security and privacy threats to their motor vehicles, and for other purposes. http://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf.
14. Carwall—Autonomous security for autonomous and connected cars. https://www.karambasecurity.com/product.
15. Vector solutions for CAN and CAN FD. http://vector.com/vi_can_solutions_en.html.
16. PRODUCTS: 3 + 1 cyber security protection framework—FUSE. http://www.visualthreat.com/UIproducts.action.
17. Evenchick, E. CANtact. http://www.evenchick.com/post/cantact/.
18. Evenchick, E. An introduction to the CANard toolkit. http://blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus-wp.pdf.
19. Anatomy of the RollJam Wireless Car Hack. http://makezine.com/2015/08/11/anatomy-of-the-rolljam-wireless-car-hack/.
20. OwnStar—Hacking cars with OnStar to locate, unlock and remote start vehicles. https://www.youtube.com/watch?v=3olXUbS-prU.

21. Hacker shows he can locate, unlock and remote start GM vehicles. http://www.computerworld.com/article/2954668/telematics/hacker-shows-he-can-locate-unlock-and-remote-start-gm-vehicles.html.
22. Hackers remotely kill a jeep on the highway—With me in it. https://www.youtube.com/watch?v=MK0SrxBC1xs.
23. Hacker: 'Hundreds of thousands' of vehicles are at risk of attack. http://www.computerworld.com/article/2951489/telematics/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html.