Trust and reputation management in vehicular ad hoc networks

Hu, Hao

2016

Hu, H. (2016). Trust and reputation management in vehicular ad hoc networks. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/69403>

<https://doi.org/10.32657/10356/69403>

NANYANG
TECHNOLOGICAL
UNIVERSITY

Trust and Reputation Management in Vehicular Ad Hoc Networks

Hu Hao
School of Electrical and Electronic Engineering

2016

Trust and Reputation Management in Vehicular Ad Hoc Networks

Hu Hao

(Supervised by: Asst Prof. Lu Rongxing)

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirement for the degree of
Doctor of Philosophy

2016

This Thesis Is Dedicated With Love And Affection To
My Grandma
Parents And Girlfriend
You Mean The Whole World To Me

Acknowledgments

My P.hD career is like taking a roller coaster, two years ago, it was at its bottom. It was that hard time when I met my supervisor, Dr. Rongxing Lu, who, if not changes my life, changes my P.hD career. Dr. Lu shows me a way into the magical world of security and cryptography, a world he had long endeavored with all of his passion and intelligence, a world filled with wonders and fantasies. By keeping a firm grasp on the emerging research trends in this field, he widens my visions greatly. A teacher for a day is a father for a lifetime. The days that I worked with Dr. Lu will be the most memorable days in my life, and this thesis is a faithful record of those days.

My appreciations go to my previous supervisor Dr. Tan Soon Yim who brought me to NTU. I also greatly acknowledge my co-authors: Dr. Zonghua Zhang, Dr. Jun Shao and Mr. Cheng Huang who provide valuable suggestions for me and help me polish and improve my work. Especially Dr. Zhang, who is always the first reader of my work. His original and insightful comments and excellent language skills lift my papers to a higher level. Besides, I own many thanks to my oral defense panel members: Dr. Xiao Gaoxi, Dr. Li Kwok Hung and Dr. Gunawan Erry. Last but not the least, I would like to thank Dr. Ma Maode without whom things will not go so smoothly after my thesis submission.

I am indebted to my colleagues in Dr. Lu's research group. Among them, Dr. Haiyong Bao, Dr. Changlu Lin, Mr. Cheng Huang, Dr. Ximeng Liu, Dr.

Le Chen, Mr. Shuo Chen, Dr. Ruilong Deng, Miss Qinglei Kong, Mr. Beibei Li, Mr. Guoming Wang, Dr. Chen Li, Dr. Lichun Li, Dr. Yali Liu, Mr. Rakesh, Dr. Chang Xu are notable. I can not imagine how hard and lonely my research will be without support from such a big team of talented researchers. Simple relations in the group make me feel comfortable, as a result, widely open discussions become the source of my ideas. Many appreciations go to my labmates in INFINITUS Lab, who create a dynamic living and working environment that makes my life more interesting.

I would like to thank Miss Meng Sun, my Miss Right, who is of course always right, for her encouragements and dedication. Finally, I am deeply grateful to my grand parents and parents for their unconditional love and support throughout my pursuit of my dream. To all of them I dedicate this thesis.

Contents

Acknowledgments	i
Contents	iii
Summary	x
List of Tables	xiii
List of Figures	xiv
List of abbreviations	xvii
1 Introduction	1
1.1 Overview	1
1.2 Vehicular Ad Hoc Networks	2
1.2.1 Architecture of VANETs	2
1.2.2 Characteristics of VANETs	3
1.2.3 Security Requirements in VANETs	4
1.2.4 Comparisons between MANETs and VANETs	6
1.2.5 Classification of Attacks on VANETs	6

1.3	Motivation	12
1.4	Objectives	13
1.5	Research Contributions	14
1.6	Outline of the Thesis	15
2	Background and Related Works	16
2.1	Preliminaries	16
2.1.1	Beta Distribution	16
2.1.2	Dirichlet Distribution	18
2.1.3	Trust and Reputation	19
2.1.4	Bilinear Pairing	19
2.2	Review of Existing Trust and Reputation-based Systems	20
2.2.1	Background for Trust and Reputation Systems	20
2.2.2	Bio-inspired Trust and Reputation Model	20
2.2.3	Reputation-based Framework for High Integrity Sensor Net- works	24
2.2.4	EigenTrust	26
2.2.5	TRIP: Trust and Reputation Infrastructure-based Proposal for VANETs	29
2.2.6	Data-centric Trust Establishment	31
2.3	Summary	34
3	Trust-based Platoon Service Query via Vehicular Communication- s	35
3.1	Introduction	36

3.2	System Model, Trust Model and Design Goal	39
3.2.1	System Model	39
3.2.2	Trust Model	41
3.2.3	Design Goals	45
3.3	Proposed TPSQ Scheme	46
3.3.1	System Initialization	46
3.3.2	Platoon Service Request	47
3.3.3	Request Preprocessing	48
3.3.4	Trust-based Platoon Selection	50
3.3.5	Platoon Service Quality Feedback	50
3.4	Trust Management	54
3.5	Performance Evaluation	58
3.5.1	Vehicle Behaviors	58
3.5.2	Simulation Setup	59
3.5.3	Simulation Results	62
3.6	Related Work	66
3.7	Summary	68
4	Reliable Trust-based Platoon Service Recommendation Scheme	69
4.1	Introduction	69
4.2	System Model, Trust Model and Design Goal	72
4.2.1	System Model	72
4.2.2	Trust Model	74

4.2.3	Design Goals	75
4.3	Proposed REPLACE Scheme	77
4.3.1	System Initialization	77
4.3.2	Quality of Feedbacks	78
4.3.3	Dirichlet-based Model	82
4.3.4	Trustworthiness of a User Vehicle	84
4.3.5	Reputation of PH Vehicles	85
4.4	Security Analysis	86
4.5	Performance Evaluation	87
4.5.1	Simulation Settings	88
4.5.2	Modeling the PH Vehicles and User Vehicles	88
4.5.3	Modeling Attackers in User Vehicles	90
4.5.4	Reputation Scores of PH Vehicles	91
4.5.5	Trust Scores of User Vehicles	92
4.5.6	Robustness of Our Proposed Scheme	93
4.6	Related Work	96
4.7	Summary	97
5	Privacy-Preserving Trust-based Relay Selection Scheme	99
5.1	Introduction	99
5.2	Problem Statement	102
5.2.1	System Model	103
5.2.2	Trust Model	104

5.2.3	Threat Model	105
5.2.4	Design Goal	106
5.3	Proposed PTRS Scheme	107
5.3.1	Initialization	107
5.3.2	Privacy-preserving Relay Selection Protocol	109
5.3.3	Performance Report	112
5.3.4	Trust Management	112
5.4	Security Analysis	116
5.4.1	Resilience to Reputation Link Attack	116
5.4.2	Resilience to Packets Dropping Attack	117
5.4.3	Resilience to Packets Analysis Attack	117
5.4.4	Resilience to Fake Reputation Attack	117
5.5	Performance Evaluation	118
5.5.1	Simulation Setup	118
5.5.2	Simulation Results	120
5.6	Related Work	124
5.7	Summary	127
6	Trust-based Vehicular Platoon Crowdsensing Scheme with Privacy Preservation	129
6.1	Introduction	130
6.2	Problem Statement	133
6.2.1	System Model	133
6.2.2	Security Model	135

6.2.3	Design Goal	137
6.3	Proposed TripSense Scheme	138
6.3.1	System Initialization	138
6.3.2	Trust-based Privacy-preserving Sensing Vehicle Selection . .	140
6.3.3	Privacy-preserving Sensed Data Aggregation	142
6.3.4	Aggregated Sensed Data Retrieval	143
6.3.5	Privacy-preserving Sensed Data Accuracy Evaluation	144
6.3.6	Dirichlet-based Trust Management	145
6.4	Security Analysis	148
6.4.1	The proposed TripSense scheme is privacy-preserving for PM vehicles	148
6.4.2	The proposed TripSense scheme achieves robustness against attacks launched by adversary	149
6.5	Performance Evaluation	150
6.5.1	Simulation Settings	151
6.5.2	Modeling the Sensing Behaviors of PM Vehicles	151
6.5.3	Simulation Results	152
6.6	Related Work	154
6.7	Summary	156
7	Conclusions and Future Work	158
7.1	Contributions	158
7.2	Future Work	160

List of publications	161
Bibliography	164

Summary

We have never lived in such an era when vehicles are so indispensable before. The number of vehicles worldwide has been keeping increasing despite it had already broken one billion in 2011. A survey reported that in U.S. people stay in vehicles daily for 3 hours on average. It has become a lifestyle. Like in any other venues, people in vehicles also have the need to communicate and access information resources. So the networks designed specifically for vehicles were born. These networks are called VANETs (vehicle ad-hoc networks), aiming at providing communications between vehicles or between vehicle and infrastructures along the roads.

In VANETs, each vehicle is regarded as a mobile node or a wireless router. Vehicles are connected with each other once they are within the transmission range, they may join in or drop out of the range of the networks intermittently which makes the networks highly dynamic. Besides, in some places like rural areas the networks are quite sparse while in urban districts they are dense. Recently, IEEE 802.11p has been approved as an amendment to IEEE 802.11 standard which fully supports Intelligent Transportation Systems (ITS) applications with data exchanges between high-speed vehicles. The effective information sharing within the networks partially mitigates the problems which we have suffered from, like traffic jams, and also decreases the possibility of traffic accidents by informing drivers the bad road conditions in advance.

Like any other types of wireless networks, security plays a vital role in VANETs. The reason is the information communicated in VANETs can be about entertainment or some advertisements, it can also be location information which should be protected or real-time road conditions which should be verified. The security requirements are even higher in the future as automatic driving systems have already been developed by motor car companies like BMW and GM. Traditional cryptographic methods like encryption and digital signature are introduced to ensure security and privacy of data and entity in VANET. However, that is far from enough since the accuracy and reliability of those widespread information are still unverified. Hence the trust and reputation management system specifically for VANET needs to be proposed and developed.

The ultimate goal of our research is to develop a trust and reputation based model to ensure that those “well-behaved” vehicles are always selected to provide a service or contribute data. Specifically, in this thesis, we first study the platoon formation problem given that there are “badly-behaved” platoon head vehicles which provide low quality services in the vehicular platooning system. We propose a reliable trust-based platoon service recommendation scheme to help the user vehicles distinguish well-behaved vehicles from badly-behaved vehicles and then avoid choosing those badly-behaved platoon head vehicles. Another study is to make sure that information can be delivered without deliberately dropping when passing through relay vehicles. To reach this goal, we propose a robust trust-based relay selection scheme based on Dirichlet distribution with an objective to effectively differentiate the trust levels of the vehicles, and meanwhile, preserving robustness. Besides, the location privacy of vehicles are preserved in this proposed scheme by using the technique of pseudonyms and trust levels instead of accurate reputation scores.

In a nutshell, trust and reputation systems are necessary to solve the “insider” problems which traditional cryptographic methods cannot solve in vehicular ad hoc

networks (VANETs). However, it does not mean that trust and reputation systems will take the place of cryptographic methods. On the contrary, they serve as the complement to traditional cryptographic methods to make the whole network more secure and robust.

List of Tables

1.1	Comparisons between VANETs and MANETs	6
1.2	Attacks on Individual Layers	7
3.1	Trust Table Maintained by the Server	42
3.2	Traveling Parameter Table	42
3.3	Notations	43
3.4	Traveling Parameter Initialization	47
3.5	Simulation settings	61
3.6	Reputation score in $\text{beta}(1, \beta)$ of $ph_i(\text{bmr}=10\%)$	62
4.1	Simulation Parameter Settings	89
5.1	SIMULATION SETTINGS	120
6.1	Simulation Parameter Settings	151

List of Figures

1.1	Architecture of VANET.	2
1.2	Characteristics of VANET.	3
1.3	The Attacker Node May Forge Many Fake Identities to Launch Sybil Attack, thus the whole reputation system is disrupted.	10
2.1	PDF beta distribution with variable α and β	17
2.2	Architecture of RFSN system.	25
2.3	Data-centric trust establishment framework.	33
3.1	System model under consideration	39
3.2	Preprocessing Diagram	49
3.3	Evaluation questions and evaluation vector	51
3.4	Satisfaction State Machine	52
3.5	State Transitions from Real Performance State to Random-mouth Evaluation States	61
3.6	Satisfaction Level of a PH Vehicle with Different HQSR values in 200 Trips	63
3.7	Reputation scores of different PH vehicles in various numbers of trips	64

3.8	False positive rate versus various numbers of trips	65
4.1	System model under consideration	72
4.2	Architecture of REPLACE Scheme	77
4.3	Tables that are established and updated by the server	79
4.4	User vehicles give feedbacks on trips	80
4.5	Reputation scores comparison between PH vehicle with $l_{ph} = 0.8$ and $l_{ph} = 0.92$	91
4.6	Trust scores comparison between honest user vehicles with $l_v = 0.92$, $l_v = 1$ and malicious attackers	92
4.7	Trust score comparison of the same on-off attacker under REPLACE scheme with adaptive forgetting factor and under another scheme with fixed forgetting factor	93
4.8	Trust scores comparison of a newcomer attacker with different c_0 values	94
4.9	Resilience to badmouth attacker and ballot-stuffing attack by com- paring detection rate between REPLACE scheme with and without iterative filtering algorithm	95
5.1	Reputation scores are associated despite the change of pseudonyms	101
5.2	System model under consideration	103
5.3	Privacy-preserving relay selection protocol	109
5.4	Map for simulation	119
5.5	Relay ratio versus specific time period with different trust level thresholds	121

5.6	Total number of messages generated in 3 hours with different relay selection policies	122
5.7	Detection ratio versus time with trust level threshold $L=8$	123
5.8	Detection ratio varies with time under different malicious vehicle proportions	123
6.1	platoon head vehicle associates a platoon member vehicle's trust scores even when its pseudonym has been changed	131
6.2	System model under consideration	133
6.3	Trust scores comparison between honest platoon member vehicles with $l_v = 0.7$, $l_v = 0.95$ and malicious PM vehicles with $l_v = 0.05$, $l_v = 0.2$	153
6.4	Detection ratio comparison between sensing system with / without trust system	154

List of Abbreviations

VANET	Vehicular Ad Hoc Network
MANET	Mobile Ad Hoc Network
OBU	On board Unit
RSU	Road Side Unit
ITS	Intelligent transportation systems
V-2-V	Vehicle-to-Vehicle Communication
V-2-I	Vehicle-to-Infrastructure Communication
TA	Trust Authority
PK	Public Key
QoS	Quality of Service
PH	Platoon Head
PM	Platoon Member
TPSQ	Trust-based Platoon Service Query Scheme
REPLACE	Reliable Trust-based Platoon Service Recommendation Scheme
PTRS	Privacy-Preserving Trust-based Relay Selection Scheme
TripSense	Trust-based Vehicular Platoon Crowdsensing Scheme with Privacy Preservation
MLE	Maximum likelihood estimation
ETA	Estimated time of arrival
PDF	Probability density function
HQSR	High quality service rate

RMR	Random mouth rate
PQL	Performance quality level
FAL	Feedback accuracy level
PID	Pseudo identification
AoI	Area of Interest
SP	Service Provider
CS	Cloud Server
SAL	Sensing Accuracy Level

Chapter 1

Introduction

1.1 Overview

Our driving experience will be revolutionized by the emergence of vehicular ad hoc networks (VANETs) in the near future [1]. In VANETs, each vehicle will be equipped with wireless communication devices, known as on board units (OBUs). With the help of those OBUs, the vehicles can communicate with each other within the transmission range. At the same time, road side units (RSUs) are spread along the roads or at the intersections of the roads. They are connected with each other and the remote server through reliable wires or optical cables. The network can be used to spread real-time location information about vehicles on the road, real-time road conditions as well as entertainment information. Alternatively, the vehicles can also exchange information with nearby RSUs through protocols based on IEEE 802.11 standards [2]. One important application of VANET is that it can be used to enhance road safety and mitigate traffic congestion. Some prototypes like Network-On-Wheels (NOW) project, PreVent and Car-to-Car Consortium have already been developed by vehicle companies to meet the requirements above [3].

1.2 Vehicular Ad Hoc Networks

VANET has been studied a lot by both industry and academia [4] due to its high potential in a wide range of applications being deployed in aid of consumers and commercial establishments. In this section we will introduce some of the basic concepts and characteristics regarding VANETs as well as its main characteristics, and then we will deploy its comparisons with MANETs. Through the comparisons, we understand that those attacks targeted on MANET may happen in VANET, but there are also some special attacks on VANET, therefore security requirements for VANET are formed. Then we analyse those different types of attacks in detail.

1.2.1 Architecture of VANETs

As an important component of VANETs, V2V communication enables vehicles to communicate with other vehicles which may be located out of the range of line of sight (LOS) where a multi-hop scenario is needed. Another way of communication is vehicle-to-infrastructure (V2I). In this context, the infrastructures act as access points and gateways to the Internet and provide real-time information to vehicles. Using the minimum density of infrastructures to achieve the maximum information dissemination performance had been discussed in [5]. When those two ways of communications are combined together, VANETs become a hybrid architecture [6], which is shown in Figure 1.1.

Figure 1.1: Architecture of VANET.

1.2.2 Characteristics of VANETs

As a special case of mobile ad hoc networks (MANETs), VANETs resemble MANETs in many aspects. However, since VANETs are equipped with more powerful OBUs which are linked to RSUs, it shows a few special characteristics, outlined in Figure 1.2. On the other hand, those characteristics lead to lots of challenges [7].

Figure 1.2: Characteristics of VANET.

1. *Large scale:* VANETs are likely to be among the largest ad hoc network containing hundreds of vehicles. It requires scalable solutions for adequate availability and sufficient performances. Also, security and privacy policies differ among regions owing to the worldwide deployment of this network. In such a case, coordination of VANETs in different regions will be difficult which would require specific relationships between various regions.
2. *High mobility:* Vehicles travel at a high speed up to 150 kilometers per hour, at the same time, their routes are dynamic. In an extreme case, when two cars are moving toward two opposite directions, the connection time in between is very short. Facing such an ephemeral network, the time delay factor should be taken as an important issue. Also, most of the interactions are between vehicles who had never met before.

3. *Rapidly changing topology:* The topology of VANETs changes constantly due to the fast-moving characteristic of vehicles [8]. During the peak hours in urban areas, the network nodes could be denser than usual. However, sometimes the topology could be predicted according to the road layouts and conditions.
4. *No power constraint:* The batteries are charged by vehicles, which breaks the power bottleneck of traditional MANETs. As a result, vehicles fully support complex computing devices that are competent for onerous cryptographic calculations.

1.2.3 Security Requirements in VANETs

Vehicle communication (VC) systems can be disrupted or disabled even by some relatively unsophisticated attacks [9], so a security architecture that provides a comprehensive and practical solution is needed. The security requirements [1, 10, 11, 12, 13] are categorized below:

1. *Authentication:* Authentication is a major requirement for VANETs, since it ensures that a message is sent by the actual vehicle rather than a vehicle representing multiple identities or impersonating as another vehicle [14]. Through authentication, Sybil attack can be avoided since a malicious vehicle cannot send messages to nonexistent vehicles.
2. *Message integrity:* It assures that the messages sent between vehicles are not modified in transit. Coupled with authentication, integrity ensures that messages received by vehicles in VANET are not false.
3. *Message confidentiality:* Confidentiality can be utilized when certain vehicles want to communicate with others in private, which will be useful in cases when law enforcement vehicles communicate with each other for dis-

seminating private information regarding suspected locations of criminals or speed check points.

4. *Access control*: Access control is required to ensure that all nodes function according to the roles and privileges authorized to them in the network. Misbehaving nodes should be revoked from the network to ensure the safety of other legitimate entities in the network; otherwise the whole network will become malfunctional.
5. *Availability*: Due to the rapid changing topology, VANET is required to be kept available at all times so that it is resistable to attacks like DoS when vehicles refuse to provide services.
6. *Non-repudiation*: It is the ability to prevent an authorized vehicle from denying having sent a message. It urges the vehicles to be responsible for its actions as well as finding the source of a message. It can also prevent an attacker from denying the attacks it has launched.
7. *Privacy protection*: Privacy is important to prevent the unauthorized parties from accessing the information [15], neither should they be able to track the trace of the vehicles as it offends the privacy of those vehicles. It prevents the information from leaking outside. However, that information should be transparent to liable authorities. This kind of security requirement is also called “conditional privacy preserving”. Currently, an approved amendment called wireless access in vehicular environments (WAVE) [16] has been added to IEEE 802.11 standard, forming a security standard specifically for vehicular communication system: IEEE 802.11p standard [17].

1.2.4 Comparisons between MANETs and VANETs

VANET is a special case of MANET which can be used to provide communications between nearby vehicles as well as between vehicles and fixed infrastructures on the roadside. While MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.

In MANETs, mobile devices are free to move independently towards any direction slowly, whereas in VANETs, vehicles move along the road in a high speed (up to 150km/h) whose trails can be predicted in advance due to the geometric topology of roads.

Routing protocols in MANETs also have to be modified to be adapt to the VANETs environment because the vehicles in VANETs are moving along predefined roads and their trails are predicable. In [18], the author analyses and proposes an optimized routing protocol for VANETs. The comparisons is shown in Table 1.1 below.

Table 1.1: Comparisons between VANETs and MANETs

	<i>MANET</i>	<i>VANET</i>
Speed	Fixed or slow	up to 150km/h
Topology	Predefined, fast changing, streets in the real world	random way point, relative stable
Resource	Limited by battery, computational ability	almost no limit
Architecture	Node to node	V2V, Vehicle-to-RSU
Scalability	50-100 nodes	Very huge
Protocols	DSDV, FSR, AODV	DSR, FSR, TORA

1.2.5 Classification of Attacks on VANETs

As a specific type of MANETs, VANETs are vulnerable to various types of attacks which also happen in MANETs. Those attacks may happen in different layers,

varying from routing attacks to physical compromises. Since the study of attacks in MANETs is not the main focus of this section, we generalize it into a table below. The main focus of this section is to survey the attacks specifically for VANETs. Later, we will present a survey of those attacks, attempting to study and classify those attacks and the ways of mitigating them [19].

There are some general ways of classifying the attacks. One way is to classify those attacks by *insiders* and *outsiders* way. Outsiders attacks come from unauthorized vehicles or nodes outside the network, it can be solved in traditional cryptographical ways. Insiders attacks are mounted by vehicles inside the network. Insiders attacks are difficult to handle using cryptography since each vehicle shares the common secrets within the network. That is the reason we would like to introduce trust and reputation models. Alternatively, we can also classify attacks into *active* attack and *passive* attack. An active attacker modifies, fabricates or deletes the content of the packets [20], whereas the passive attacks include eavesdropping and traffic analysis attacks [21]. The schematic of classification is shown in Table 1.2. We will introduce more details below.

Table 1.2: Attacks on Individual Layers

<i>Network Layer</i>	<i>Types of Attacks</i>
Application	Malicious node, repudiation
Transport	Session hijacking, SYN flooding
Network	Flooding, blackhole, greyhole, wormhole, link spoofing, link withhold, byzantine, replay
MAC	Malicious behavior, selfish behavior,
Physical	Interference, jamming

VANET is a special kind of MANET, it has some characteristics which make it different from MANET like highly dynamic and volatile topology, intermittent connections and fast changing neighbouring environments. Those characteristics make it vulnerable to some of the attacks specifically for VANETs. As described

before, the security requirements for VANET are typical and have contradicting requirements in terms of privacy, anonymity, authentication and non-repudiation [22].

Adversary Models

Before classifying the types of attacks on VANETs, firstly we analyze the adversaries [7] in an increasing order of threat severity:

1. *Selfish drivers*: Traffic condition information like congestion, accidents or construction could be spread among the drivers through V2V communications so that other drivers can avoid those roads. Though most of the drivers obey the rules of the VANETs to generate and spread traffic condition information, there are still selfish drivers who may intentionally mislead other drivers to a congested way so that they themselves can avoid the crowd. It is easy to deal with this kind of attack by introducing an authentication system to trace the source and put heavy legal punishments. Those selfish drivers will be afraid of law enforcement next time if they realize that there is a high probability to get caught.
2. *Eavesdroppers*: Those adversaries may collect the information passively and analyse them to understand the drivers' behaviors and traffic patterns. For instance, the thieves may use the vehicular network to detect which garages then which houses are empty. Companies would like to buy those vehicular trace information to see the consumers' shopping habits. After all, the VANET users will not be happy if their information is divulged to third parties.
3. *Pranksters*: Pranksters could be hackers who try to find bugs and utilize them to disrupt the network just for fun.

4. *Insiders*: The insiders could be vehicles inside the VANETs, or it could be the people working in the car companies or software companies, they are capable of injecting the mal-software or compromise the public keys in the PKI system since they are the key distributors.
5. *Malicious attackers*: Malicious attackers cause the most severe damages to the VC systems. The attackers use more sophisticated tools or methods to launch attacks, disrupting the system for crimes.

Types of Attacks on VANETs

1. *Sybil attack*: As described by Douceur [23], Sybil attack may seriously impair the functionality of VANET. In this attack, a malicious vehicle may forge many fake identities and send messages by those identities. Except for that, the attackers may also spoof the identities of other vehicles, which is shown in Figure 1.3. A Sybil attacker can make an illusion of traffic jam or accident on a specific road by spreading false information using these identities so that all the other vehicles receiving the message may avoid the road, hence the Sybil attacker benefits from it. Sybil attack can be further classified into three categories based on types of communication, identity and participation [24]. Golle et al. propose some general techniques such as registration, radio resource testing and position verification to mitigate Sybil attack [25]. Some authors propose other techniques for position verification using temporal links [26]. Harsch et al. [27] propose a comprehensive position-based routing protocol using cryptographic primitives to partially mitigate bogus information attack.
2. *Jamming attack*: Jamming attack is launched by introducing radio interferences. Those attackers are called jammers. The jammers may remain silent when there are no activities on the channel and start interfering as soon as

Figure 1.3: The Attacker Node May Forge Many Fake Identities to Launch Sybil Attack, thus the whole reputation system is disrupted.

they detect a transmission. Those jammers' communications are not compliant with MAC protocols. There are many different types of attacking strategies for jammers according to their different attacking goals. Those types of attacks have different levels of effectiveness and need different detection methods. For example, a constant jammer continuously emits radio signals by using normal wireless devices or a waveform generator which keeps emitting radio signals. A deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. A random jammer alternates between sleeping and jamming continuously [28]. Those jammers above are all active jammers because they try to block the channel irrespective of traffic patterns on the channel. For reactive jammers, they only transmit radio signals as soon as they sense activities on the channel so they target on the reception of a message, which makes it harder to detect. Some basic factors of detecting jamming attacks include signal strength, carrier sensing time and packet delivery ratio (PDR). Xu et al. propose two enhanced detection protocols that employ consistency checking

[28].

3. *DoS attack*: In a DoS attack, the attacker may try to exhaust the network resources or jam the channel so that information cannot be delivered [29]. However, this attack can be detected and warned to the drivers [29].
4. *Bogus information attack*: The attackers may intentionally spread false information in the network in order to disrupt the other vehicles for their own benefits. One way to mitigate is by using the position verification approach [30]. Raya propose a data-centric trust establishment in VANET [31]. In this system, when a message is spreading, it will be burdened an evaluation score according to the reporter's location and time to finally form a trust value, each forwarding vehicle is qualified to give an evaluation. The receivers can decide to trust the message according to the score attached. Other approaches include digital signatures and some cryptographic methods to ensure non-repudiation.
5. *Identity disclosure attack*: As a peculiar type of attack in VANETs, identity disclosure attack occurs once the attacker has the vehicle's identity. Because after getting vehicle's identity, the attacker can easily know the driver's mobility pattern by tracking its location and do spoofing. Technique like pseudonyms is used to mitigate [32].
6. *Illusion attack*: Described in [22], the adversary intentionally deceives the sensor or other detecting devices in its own vehicle to produce a wrong reading which will be broadcast later. The attack cannot be mitigated with those traditional methods like message authentication, message integrity check. A novel plausibility validation network model was proposed which takes help of some predetermined rule set and analyses the message contents on these rules to decide the authenticity of the message [33].
7. *Repudiation attack*: Repudiation denial of participation happens in all parts

of communication, which cannot be verified in the transport layer even when the entire connections are encrypted end-to-end. Louridas has derived a non-repudiation protocol to mitigate [34].

Different types of attacks may occur in different layers of different wireless networks. As a special type of mobile ad hoc network, VANETs has its own characteristics which makes it vulnerable to not only the attacks on wireless networks but also attacks specifically on VANETs. At the same time, the cryptographic or network methods can be utilized to solve some of the “outsider” attacks in VANETs but not the “insider” attacks. Therefore, we need to introduce the trust and reputation models which will be explained in the next section.

1.3 Motivation

Security has always been of the highest importance in VANETs. To secure VANETs, some cryptographic methods like encryption algorithms have been used widely to ensure the security and preserve the privacy of data [35] [15], digital signature algorithms can not only be used to verify the messages generated by a specific vehicle but also to prevent from any tampering of the messages to achieve non-repudiation.

Although cryptographic methods are very effective against attacks coming from outside, it becomes ineffective when the attackers are malicious drivers in VANET who intend to disrupt the network or mislead others for their own benefits. The reason is that those attacks are mainly from those “insiders” who have the legal identification and key certificates in the system. Therefore, we are motivated to study and mitigate the “insider” attack existed in VANETs.

1.4 Objectives

In this research, we would like to establish a trust and reputation model to resist against badly-behaved vehicles that are inside VANETs. In order to meet the requirements of VANETs, the following design objectives should be achieved by our system:

1. Light and fast. Since the topology of VANET is fast changing, even after a short time, the former topology will be replaced by a new one, hence the method proposed should be very fast and light for a quick reaction.

2. Low-delay. Because of the fast changing topology, a message may become meaningless in a short time, it requires those road condition information or congestion information to be real-time and messages to be conveyed quickly as we cannot tolerate much delay.

3. Scalable. The number of vehicles in the network can be very huge, we need to consider the size of the network when designing the protocols. Furthermore, the distribution of vehicles may be unbalanced in time and location: in urban areas or office hours the network will be dense while in rural areas or off-office hours the network will be sparse.

4. Robust. Traditional cryptographic methods are robust against outside attacks while trust and reputation methods are robust against inside attacks, e.g., collusion attack, badmouth attack. Our method is robust against both types of attacks.

In VANETs, location information is widely used in the design and implementation of trust and reputation systems. However, drivers' location privacy will be disclosed with the use of their trust scores. It has become a challenging issue to preserve the drivers' privacy in VANET. In this thesis, we will study the vehicular platooning formation, crowdsensing and vehicular relay selection with the exis-

tence of “insider” attackers of VANETs, and devote ourselves to establishing a few trust-based schemes to mitigate the attacks and preserve the privacy of drivers.

1.5 Research Contributions

The research in this thesis focuses on developing a suite of trust-based schemes to deal with the challenging security and privacy-preserving issues in vehicular ad hoc networks. Specifically, the main contributions lie in the following aspects:

First, to deal with untrusted “insider” attacker in vehicular platooning system, we propose a practical trust-based platoon service query scheme, called TPSQ [36], for vehicular communications in VANETs. This proposed scheme helps user vehicles differentiate between well-behaved and badly-behaved head vehicles in platooning system, and finally enhances the road safety and user comfort. A trust and reputation system is developed to distinguish platoon head vehicles according to their historical service qualities. By adopting our proposed scheme, querying vehicles are able to choose the most reliable platoon head vehicle to follow. In addition, to deal with the badmouth attackers launched by platoon members in evaluation, a reliable trust-based platoon service recommendation scheme, called REPLACE [37], is presented, which enhances the trust system’s robustness.

Second, to make the two-hop vehicle-to-infrastructure communications reliable and secure in vehicular ad hoc networks, a robust trust-based relay selection scheme, called PTRS [38], is improved from TPSQ scheme to ensure that only the trustworthy vehicles are selected as relays between a vehicle and infrastructure. Besides, the location privacy of vehicles are preserved in PTRS scheme by using the technique of pseudonyms and trust levels instead of explicit reputation scores.

Third, to preserve the location and data privacy of vehicles in crowding sensing scenario while ensuring the sensed data quality at the same time, we propose a

TripSense scheme [39], which focuses on establishing a trust model to improve the sensed data reliability and accuracy of the whole system. By using the pseudonyms and trust levels, the proposed TripSense scheme can not only achieve vehicle's identity privacy, location privacy and data privacy, but also resists against adversary attacks on malicious sensing reports.

1.6 Outline of the Thesis

The organization of the remainder of this thesis is as follows:

Chapter 2 recalls some related work, including basic concepts of trust and reputation, Beta distribution, Dirichlet distribution and bilinear pairing. Chapter 3 presents a trust-based platoon service query scheme (TPSQ) when choosing platoon head vehicles with an objective to differentiate the well-behaved and badly-behaved vehicles. In Chapter 4, we propose a reliable trust-based platoon service recommendation scheme (REPLACE) aiming at distinguishing well-behaved and badly-behaved platoon head vehicles according to their reputation scores and then recommends a reliable platoon head vehicle to the user vehicle. Chapter 5 proposes a privacy-preserving trust-based relay selection scheme (PTRS) to help requesting vehicle choose the most reliable relay vehicle while preserving candidate relay vehicle's location privacy at the same time. Chapter 6 introduces a trust-based vehicular platoon crowdsensing scheme (TripSense) to evaluate vehicles' sensing abilities and then selects those more capable vehicles in order to improve sensing results accuracy. Chapter 7 concludes our present work and proposes future research directions.

Chapter 2

Background and Related Works

2.1 Preliminaries

In this chapter, we will briefly outline the beta distribution, Dirichlet distribution [40] and the concept of trust and reputation, which will serve as the basis of our proposed schemes.

2.1.1 Beta Distribution

The beta distribution is a family of continuous probability distributions which is defined on the interval of $[0,1]$ indexed by two parameters α and β . A random variable X beta-distributed with parameters α and β will be denoted by: $X \sim Beta(\alpha, \beta)$. The probability density function (PDF) $f(x|\alpha, \beta)$ can be expressed by using gamma function Γ as:

$$f(x|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1} (1 - x)^{\beta-1} \quad (2.1)$$

where $0 \leq x \leq 1$, $\alpha > 0$, $\beta > 0$. Gamma function is an extension of the factorial function. To be specific, if α is an integer, gamma function can be expressed as

$\Gamma(\alpha) = (\alpha - 1)!$; otherwise $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx$. The probability expectation value of the beta distribution is given by:

$$E(x) = \frac{\alpha}{\alpha + \beta} \quad (2.2)$$

The reputation system can be based on the beta PDF to represent the binary events [41]. In this case, we can denote s and u the positive and negative event times respectively, let $\alpha = s + 1$, $\beta = u + 1$ [42]. The mean of the PDF in Eq. (2.1) can accurately model trust metrics given by:

$$E(x) = \frac{r + 1}{r + s + 2} \quad (2.3)$$

Figure 2.1: PDF beta distribution with variable α and β

Figure 2.1 shows the PDF of beta distribution with different parameters α and β . It expresses the uncertain probability that a process will produce positive

outcomes in future. Take an example, when $\alpha = 8$, $\beta = 2$, according to Eq. (2.2), the probability expectation value of this type of beta distribution is $E(x) = 0.8$, which can be interpreted as the relative frequency of positive outcome is somewhat uncertain and that the most likely value is 0.8. When nothing is known, $r = s = 0$, a priori distribution is the uniform beta PDF with $\alpha = r + 1 = 1$ and $\beta = s + 1 = 1$ as illustrated by solid lines in Figure 2.1.

2.1.2 Dirichlet Distribution

The Dirichlet distribution is a family of continuous multivariate probability distributions parameterized by a priori parameter vector $\vec{\alpha}$. It is the conjugate prior distribution for the parameters of the multinomial distribution. In case of a binary state space, it is determined by the Beta distribution [43]. Generally, we can use the Dirichlet distribution to describe the probability distribution over a k -component random variable $\vec{X} = \{X_1, X_2, \dots, X_k\}$. If $\vec{p} = \{p_1, p_2, \dots, p_k\}$ is the probability distribution vector of X , it satisfies $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i$ ($1 \leq i \leq k, \theta_i \in [0, 1], \theta_{i+1} > \theta_i$). The Dirichlet distribution captures a sequence of observations of k possible outcomes; those observations serve as the prior parameters $\vec{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_k)$, which denote the cumulative observations and initial beliefs of X . $\vec{p}$ is a k -dimensional random variable and $\vec{\alpha}$ is a k -dimensional random observation variable. The probability density function is given by:

$$f(\vec{p}|\vec{\alpha}) = \frac{\Gamma(\sum_{i=1}^k \alpha_i)}{\prod_{i=1}^k \Gamma(\alpha_i)} \prod_{i=1}^k p_i^{\alpha_i-1} \quad (2.4)$$

where $0 \leq p_1, p_2, \dots, p_k \leq 1$; $\sum_{i=1}^k p_i = 1$; $\alpha_1, \alpha_2, \dots, \alpha_k > 0$. The expected value of the probability that X to be x_i given the observations vector $\vec{\alpha}$ is given by: $E(p_i|\vec{\alpha}) = \frac{\alpha_i}{\sum_{i=1}^k \alpha_i}$. Furthermore, if we let $\alpha_0 = \sum_{i=1}^k \alpha_i$, the variance of the event of X to be x_i is given by: $Var[X = x_i] = \frac{\alpha_i(\alpha_0 - \alpha_i)}{\alpha_0^2(\alpha_0 + 1)}$. If $i \neq j$, the covariance is: $Cov[X = x_i, X = x_j] = \frac{-\alpha_i \alpha_j}{\alpha_0^2(\alpha_0 + 1)}$.

2.1.3 Trust and Reputation

Trust: Trust is defined as a particular level of subjective probability with which an agent assesses another agent or a group of agents who will perform a particular action before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action [44]. When we say someone is trustworthy, we implicitly mean that it will perform an action within our expectation so that we can cooperate with it. It can be represented as a particular expectation regarding the behaviors.

Reputation: The term reputation can be described as a long term collective measure of trust which can be used to decide whether a vehicle is malicious or honest. It is a loose definition that reflects the observations of all members in a particular entity.

2.1.4 Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of the same composite order n . Then, a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ will satisfy the following properties: i) Bilinear: Let $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_n^*$, then $e(g^a, h^b) = e(g, h)^{ab}$, ii) Non-degenerated: Let $g \in \mathbb{G}$ be a generator in $\mathbb{G}$, then $e(g, g) \neq 1_{\mathbb{G}_T}$, and iii) Computable: Let $g, h \in \mathbb{G}$, then $e(g, h)$ can be efficiently computed.

Definition 2.1 (Bilinear Parameter Generator). *A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter κ as its input, and outputs a 6-tuple $(p, q, g, \mathbb{G}, \mathbb{G}_T, e)$, where p, q are κ -bit prime numbers, $n = p \cdot q$, $(\mathbb{G}, \mathbb{G}_T)$ are two multiplicative groups of the same order n , $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map.*

2.2 Review of Existing Trust and Reputation-based Systems

It was recent years that trust and reputation models are applied specifically in VANETs. In this section, we will firstly introduce some background knowledge of the trust and reputation systems, then their applications in wireless networks and in VANETs.

2.2.1 Background for Trust and Reputation Systems

Trust and reputation are very useful tools in network when making decisions. They are related but different. Here are the definitions of both:

Definition 2.2. *Trust is a particular level of subjective probability with which an agent assesses that another agent or group of agents will perform a particular action [44].*

Definition 2.3. *Reputation is what is generally said or believed about a person's or thing's character or standing.*

So reputation can be considered as a collective measure of trustworthiness based on the referrals or ratings from members in the community. The main difference between trust and reputation can be described as follows: a trust score is produced to reflect the subjective view of a relying party over an entity, while reputation score is produced by the whole system and to be seen by the whole system.[45].

2.2.2 Bio-inspired Trust and Reputation Model

BTRM (Bio-inspired Trust and Reputation Model) was proposed by Gomez [46] which is used in Wireless Sensor Network (WSN). The model is used to help a node

requesting a certain service in the network to find the most trustworthy route leading to the node providing that specific service based on ant colony system (ACS) [47]. However, due to specific restrictions and limitations in WSN, the ACS needs to be changed to be applied to WSN.

In the model, every node maintains a pheromone trace for each of its neighbour, this pheromone trace $\tau \in [0, 1]$ will determine the probability for the ants to choose a certain route over another, which can be also regarded as the trust of a node given to another one. The heuristic value $\eta \in [0, 1]$ is defined as the inverse of the distance between two nodes.

Algorithm

The algorithm is shown below:

Algorithm 1 BTRM

```

1: While (condition) do
2: for k=1 to Number_of_ants do
3:  $S_k \leftarrow$  initial sensor (client)
4: Launch ant k
5:
6: do
7: for every returned ant k do
8: if ( $Q(S_k) > Q(\text{Current\_Best})$ ) then
9:  $\text{Current\_Best} \leftarrow S_k$ 
10: while (timeout does not expire) and
11:  $\text{Num\_returned\_ants} \leftarrow \% \text{Number\_of\_ants}$ 
12:
13: if ( $Q(\text{Current\_Best}) > Q(\text{Global\_Best})$ ) then
14:  $\text{Global\_Best} \leftarrow \text{Current\_Best}$ 
15: Pheromone_global Updating
16: ( $\text{Global\_Best}, Q(\text{Global\_Best}), \rho$ )
17:
18: Return Global_Best.

```

The algorithm consists of four steps: 1. Each ant adds the node it departs from as its solution, then the ant decides which next node to move on according to the transition rule (lines 2-4). 2. For each returned ant, the client compares its

solution and keeps the best one. In WSN it is impossible for all of the ants to come back, so the round can be finished when a timeout expires or a certain percentage of all the ants has returned (lines 6-11). 3. The best solution found by some ants issued in the iteration is compared with the global best solution and swapped if it's appropriate (lines 13-14). 4. A pheromone global updating is performed over the paths belonging to the global best path (line 16).

Then we need to describe those features in detail and provide equations.

Path Quality

Each time a returned ant carries a solution, the client may compare the path quality in the way:

$$Q(S_k) = \frac{\bar{\tau}_k}{Length(S_k)} \cdot \%A_k \quad (2.5)$$

where $\bar{\tau}_k$ is the average pheromone of the path found by ant k and $\%A_k$ represents the percentage of ants who choose the same solution as ant k . From the equation above, we can find that the more ants choosing a specific path, the shorter the path distance is, the higher quality the path is.

Ants Transition and Stop Condition

Let ant k be at node c in a certain moment in searching, $Ne(c)$ is the set of neighbours of node c which ant k has not visited yet, τ_{cn} represents the pheromone value and η_{cn} is a heuristic value, both of which are associate with each edge $e(c, n)$ between two nodes c and n , α and β are two coefficients used to balance the influence of pheromone value and heuristic value to the probability to be calculated. The probability of node n chosen by ant k is:

$$p_k(c, n) = \frac{(\tau_{cn})^\alpha \cdot (\eta_{cn})^\beta}{\sum_{u \in Ne(c)} (\tau_{cu})^\alpha \cdot (\eta_{cu})^\beta} \quad (2.6)$$

We can easily see that the bigger τ_{cn} (which is given by Eq. (2.7)) and η_{cn} is, the more possible node n is chosen by ant k .

Pheromone Updating

After ants have passed through a route, they update the pheromone value accordingly. The local pheromone is updated when ants transit from one node to another. For example, let ant k be at node s_1 . When it moves according to the transition scheme explained in the last section, it decides to go to node s_2 (the neighbour of s_1). So the pheromone between the nodes s_1 and s_2 is updated as Eq. (2.7):

$$\tau_{s_1 s_2} = (1 - \varphi) \cdot \tau_{s_1 s_2} + \varphi \cdot \Omega \quad (2.7)$$

where $\Omega = (1 + (1 - \varphi) \cdot (1 - \tau_{s_1 s_2}) \cdot \eta_{s_1 s_2}) \cdot \tau_{s_1 s_2}$ is the convergence value of $\tau_{s_1 s_2}$ when time $t \rightarrow \infty$.

On the other hand, the pheromone global updating value is performed over the best path found by all ants in each iteration of Algorithm 1 (line 16). The modification is performed by expression Eq. (2.8):

$$\tau_{rs} = (1 - \rho) \tau_{rs} + \rho (1 + \tau_{rs} \eta_{rs} Q(S_{Global_{Best}})) \tau_{rs} \quad (2.8)$$

Therefore, the higher the pheromone trace, the heuristic value, and the quality of the path are, the higher the additional pheromone contribution over the best route is.

Punishment and Reward

If the client is satisfied, the reward will be given to the selected path; otherwise the punishment will be applied in .

$$\tau_{rs} = (\tau_{rs} - \varphi \cdot df_{rs}) \cdot Sat \cdot (1 - df_{rs}) \quad (2.9)$$

where $Sat \in [0, 1]$ represents the satisfaction of the client with received service and $df_{rs} \in (0, 1]$ is a distance factor.

2.2.3 Reputation-based Framework for High Integrity Sensor Networks

Ganeriwal and Srivastava proposed a distributed, symmetric reputation-based framework for high-integrity sensor network which is called Reputation-based Framework for High Integrity Sensor Networks (RFSN) [48].

The architecture of RFSN is shown in Figure 2.2. The method uses watchdog mechanism to collect the first-hand information and mutual evaluation as second-hand information to compute an integrated reputation value. Beta-distribution is used for reputation representation, update and integration. The trust level is then computed by reputation value, then the nodes make decisions of whether to cooperate with a node on the basis of its trust level, if the trust level is higher than a specific threshold, then this node chooses to cooperate and vice versa.

For each node j , the reputation value R_{ij} is computed and maintained by its neighbour node i through a beta-reputation model:

$$R_{ij} = Beta(\alpha_{ij} + 1, \beta_{ij} + 1). \quad (2.10)$$

where α_{ij} represents the number of successful transactions that node i has with

Figure 2.2: Architecture of RFSN system.

node j , and β_{ij} represents the number of unsuccessful transactions. Therefore, for each node i , there is a data structure termed reputation table RT_i which is defined by those reputation values node i stored:

$$RT_i = R_{ij} \quad (2.11)$$

The trust is defined as the expected value of reputation shown as:

$$T_{ij} = E(R_{ij}) = E(\text{Beta}(\alpha_{ij} + 1, \beta_{ij} + 1)) = \frac{\alpha_{ij} + 1}{\alpha_{ij} + \beta_{ij} + 2} \quad (2.12)$$

For the second-hand information, $(R_{ij})_{ID}$ is presented by node k who is the neighbour of both nodes i and j . Node i may receive a reputation value R_{kj} from node k over node j , in the form of two parameters α_{kj} and β_{kj} , after combining the direct and indirect information together, the integrated trust value $(R_{ij})^{new}$ is formed:

$$(R_{ij})^{new} = \text{Beta}((\alpha_{ij})^{new}, (\beta_{ij})^{new}) \quad (2.13)$$

where $(\alpha_{ij})^{new}$ and $(\beta_{ij})^{new}$ are given by the followings:

$$(\alpha_{ij})^{new} = \alpha_{ij} + \frac{2\alpha_{kj}\alpha_{kj}}{(\beta_{ik} + 2)(\alpha_{kj} + \beta_{kj} + 2)(2\alpha_{ik})} \quad (2.14)$$

$$(\beta_{ij})^{new} = \beta_{ij} + \frac{2\alpha_{kj}\alpha_{kj}}{(\beta_{ik} + 2)(\alpha_{kj} + \beta_{kj} + 2)(2\alpha_{ik})} \quad (2.15)$$

It's important to note that bigger weights should be given to more reputable nodes when collecting second-hand information. Before a decision is made, node i judges from j 's reputation whose behaviour has a binary value:

$$B_{ij} = \begin{cases} cooperate, \forall T_{ij} \geq B_{ij} \\ notcooperate, \forall T_{ij} < B_{ij} \end{cases} \quad (2.16)$$

The assumption of RFSN is that the majority of the nodes in WSN are trustworthy and the trust assessment can be used to flush out bad nodes. The nodes are only allowed to exchange good reputation information which eliminates bad-mouth attack.

2.2.4 EigenTrust

Eigen trust was firstly developed by Kamvar [49] to judge whether a peer is malicious based on the peer's history of uploading in P2P file-sharing networks and thus minimizing the risk of sharing and distributing inauthentic files.

The basic idea is to give each peer a trust value based on its previous behaviors. Through those distributed local trust values, a global trust value will be computed by iterations. Here are the detailed steps:

Local Trust Values

In the distributed environment, each peer i may update the number of satisfactory and unsatisfactory transactions with another peer j , storing as $sat(i, j)$ and $unsat(i, j)$ respectively. Then the **local trust value** s_{ij} can be defined as:

$$s_{ij} = sat(i, j) - unsat(i, j) \quad (2.17)$$

In order to aggregate the local trust values in the next step, we need firstly to normalize those values. Also, it prevents a malicious peer from assigning a low trust value to a good peer to subvert the system. The **normalized local trust value**, c_{ij} can be expressed as follows:

$$c_{ij} = \frac{max(s_{ij}, 0)}{\sum_j max(s_{ij}, 0)} \quad (2.18)$$

Aggregating Local Trust Values

In order for peer i to have an overall view of peer k , a natural way is to ask the opinions from peer i 's friends who have interacted with k before. Also, before asking, i should give weight to those peers who have different trust values too.

$$t_{ij} = \sum_j c_{ij} c_{jk} \quad (2.19)$$

where t_{ik} represents the opinion from peer i over peer k based on asking his fiends. We can present peer i 's opinions over all of its friends in the matrix form. Let $\vec{t}_i$ be the vector containing all values of t_{ik} , then we have $\vec{t}_i = (C^T)^n \vec{c}_i$, which is

presented as:

$$\vec{t}_i = \begin{pmatrix} t_{i1} \\ t_{i2} \\ \vdots \\ t_{im} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1m} & c_{2m} & \cdots & c_{mm} \end{pmatrix} \cdot \begin{pmatrix} c_{i1} \\ c_{i2} \\ \vdots \\ c_{im} \end{pmatrix}$$

Through this way peer i can get the knowledge of peer j in a more comprehensive way. However, it's still not enough so we can keep asking friend's friend ($\vec{t}_i = (C^T)^2 c_i$), and so on. After keeping asking for n times (n is a very large value), $\vec{t} = (C^T)^n c_i$, vector $\vec{t}$ tends to converge which means for arbitrary i , the trust value over a specific peer is the same value, this value can be regarded as the reputation value of that peer in this distributed network.

Algorithm of EigenTrust

Note that we assume that some of the peers in the network are pre-trusted. If those peers are in the set P , we define that p_i is the initial trust value for all peers and $p_i = 1/|P|$ if $i \in P$, and $p_i = 0$ otherwise. This $\vec{p}$ will generally converge faster in the presence of malicious peers.

It's possible for some malicious collectives who give high local trust values to each other and low values to others in order to subvert the system. The problem can be addressed by assigning a trust value to pre-trust peers:

$$\vec{t}^{k+1} = (1 - a)C^T \vec{t}^k + a\vec{p} \quad (2.20)$$

where $a \in [0, 1]$ is a weight value from pre-trusted peers, by assigning a trust value from pre-trust peers compulsorily, the malicious collectives will be broken. Here is the algorithm:

Algorithm 2 Eigentrust Algorithm

```

 $\vec{t}^{(0)} = \vec{p};$ 
repeat
 $\vec{t}^{(k+1)} = C^T \vec{t}^{(k)};$ 
 $\vec{t}^{(k+1)} = (1 - a)\vec{t}^{(k+1)} + a\vec{p};$ 
 $\delta = \|t_{(k+1)} - t_{(k)}\|;$ 
until  $\delta < \epsilon;$ 

```

2.2.5 TRIP: Trust and Reputation Infrastructure-based Proposal for VANETs

Developed by Gomez [50], TRIP is a method to quickly and accurately distinguish malicious or selfish nodes who spread false or bogus information throughout VANETs.

Theories

When a vehicle receives a traffic warning or message from another vehicle, according to the trust level of the sender, it has three choices: reject and drop, accept but not forward, accept and forward.

Besides, each message or warning has an associated severity. This is easy to understand since it is not equally harmful to accept a false accident report and a false advertisement.

Moreover, a reputation score can be computed by combining three different sources of information, namely: direct previous experiences with the vehicle, recommendations from nearby vehicles, recommendations provided by central authority through Road Side Unit (RSU). The assumption we have for direct experience is that a vehicle usually circulates over the same roads at the same time of the day so that it has a good chance to meet vehicles it had seen before.

Like in the other systems, there is a trade-off between computational accuracy and computing time needed to make a decision.

Trust Scores Computing

As described before, each vehicle v_i computes a trust score for another vehicle v_j when receiving a message. The trustworthiness can be computed as follows:

$$Rep_{ij}^t = \alpha_i Rep_{ij}^{t-1} + \beta_i \sum_{k=1}^{n^t} \omega_k Rec_{kj} + \gamma_i Rec_{RSU_j} \quad (2.21)$$

where $Rep_{ij}^{t-1} \in [0, 1]$ represents the reputation score from node v_i over node v_j in the last time $t - 1$, and $Rep_{ij}^t \in [0, 1]$ represents the reputation score from node v_i over node v_j at this time t , n^t is the number of vehicles nearby to whom node v_i requests opinions about v_j at the time t , $\omega_k \in [0, 1]$ represents the reliability of recommendations provided by each vehicle v_k , $Rec_{kj} \in [0, 1]$ represents the recommendation score given to v_j by v_k , the same to RSU recommendation $Rec_{RSU_j} \in [0, 1]$. Finally, $\alpha_i, \beta_i, \gamma_i \in [0, 1]$ represent the weights given to those three components respectively. For example, if those recommenders have high reputation values, β_i deserves a high value. To be noticed, $\alpha_i + \beta_i + \gamma_i = 1$ and $\sum_{k=1}^n \omega_k = 1$.

Also, there is a rewarding and punishing system: if the message sent by v_j is confirmed, then those supporting vehicles will get an increment of weight ω_k in the next recommendation and those who provide bad recommendations will get a decreased weight of ω_k .

Decision Making

When a reputation score Rep_{ij}^t has already been computed, a decision will be made based on fuzzy sets [51]. Three fuzzy sets will be given to three different levels: “Not Trust”, “+/- trust”, “Trust”. The probability of accepting a message sent by a vehicle placed in the “+/- trust”, $\mathbb{P}_{+/-T}$ can be obtained as:

$$\mathbb{P}_{+/-T} = \mu_{+/-T} - \mu_{NT} - \sigma_{NT} \quad (2.22)$$

where μ_{TK_k} and σ_{TK_k} are mean and standard deviation respectively of trust level TL_k .

2.2.6 Data-centric Trust Establishment

Traditional notion of trust is entity-centric which is based on a priori trust relations already established in those entities who produced data. It is not feasible in VANETs since it is hard to establish prior trust because the network is ephemeral and vehicles had never even met before, meanwhile it is very slow for such a trust to establish. Hence Raya proposed a model to establish data trustworthiness [31]. This model mainly focuses on trustworthiness on data rather than reflecting trust attributed to data-reporting entities.

This method can be divided into a few steps below:

System Model

Define a set $\Omega = \alpha_1, \alpha_2, \dots, \alpha_I$ of mutually exclusive *basic events*. Composite events γ are unions or intersections of basic events. V is the set of nodes v_k , classified according to a system-specific set of node types, $\Theta = \theta_1, \theta_2, \dots, \theta_N$. The function τ is defined by $\tau : V \rightarrow \Theta$ returning the type of node v_k . *Reports* are statements by nodes on events including related time and geographic coordinates where applicable.

Default Trustworthiness

Default trustworthiness of a node v_k of type θ_n is defined as a real number which depends on the attributes related to the designated type of node v_k . There exists a trustworthiness ranking of $0 < \theta_1 < \theta_2 < \dots < \theta_N < 1$.

Event- or Task-Specific Trustworthiness

Let Λ be the set of all relevant system tasks, then for nodes v_1 and v_2 with types $\tau(v_1) = \theta_1$ $\tau(v_2) = \theta_2$ and default trustworthiness rankings $t_{\theta_1} < t_{\theta_2}$, v_1 is more trustworthy than v_2 with respect to task $\lambda \in \Lambda$.

The *event-specific trustworthiness* function f can be defined as $f : \Theta \times \Lambda \rightarrow [0, 1]$. f incorporates the type $\tau(v_k)$ of the reporting node v_k and task λ_j .

Dynamic Trustworthiness Factors

The nodes may become faulty or be comprised by attackers hence we need to revoke them. To reach the goal we define a *security status* function $s : V \rightarrow [0, 1]$. $s(v_k) = 0$ implies node v_k is revoked, and $s(v_k) = 1$ implies that the node is legitimate. Besides, we define a set of *dynamic trust metric* functions $M = \mu_l : V \times \Lambda \rightarrow [0, 1]$ indexed by a selector l indicating different node attributes (e.g., location) that dynamically change. A different metric μ_l is defined for each attribute. μ_l takes node $v_k \in V$ and task $\lambda_j \in \Lambda$ as inputs and returns a real value in $[0, 1]$.

Location and Time

Among the possible values of l for metric μ_l , proximity either in *time* or *geographic location* are attributes of particular importance which can be used to increase the trustworthiness of a report: The closer the reporter is to the location of an event, the more likely it is to have accurate information on the event. Similarly, the more recent and the closer to the event occurrence time a report is generated, the more likely it is to reflect the system state.

Figure 2.3: Data-centric trust establishment framework.

Scheme Overview

Here is the scheme to compute the trustworthiness of a report e_k^j by vehicle v_k to provide supporting evidence for event α_j by using both static or slow-evolving evidence on trustworthiness and dynamically changing information:

$$F(e_k^j) = G(s(v_k), f(\tau(v_k), \lambda_j), \mu_l(v_k, \lambda_j)) \quad (2.23)$$

where $s(v_k)$ reflects whether the vehicle v_k is legitimate or evoked for evaluation, if it is legitimate then $s(v_k) = 1$; otherwise it equals 0. $\tau(v_k)$ and λ_j are the types of reporting vehicle v_k and task respectively. f will be given a default trustworthiness $t(\tau(u_k))$. $\mu_l(v_k, \lambda_j)$ represents a trust metric function evaluating the trustworthiness of a node considering the location of vehicle v_k spotting the event or time when it reported. Then the method uses a weighted voting and Bayesian Interference for determination. The scheme is illustrated in Figure 2.3.

This method shows its advantages in a fast-changing and sparse environment

where vehicles never met before, but when vehicles often meet each other it will be very slow without an entity-based trust.

In this section, we have reviewed the trust and reputation models developed in P2P network, wireless sensor network (WSN) and vehicular ad hoc network (VANET) respectively. These models solve some of the problems including trust establishment, trust calculation and broadcasting, etc. But none of them have utilized the RSUs in VANET, nor have they considered the message delivery and relay in the fast changing topology in VANET.

2.3 Summary

In this chapter, we have discussed some background information and related works of existing trust and reputation schemes, including basic concepts of vehicular ad hoc networks (VANETs), bilinear pairing and some distributions. In the following chapters, we will present several schemes or protocols one by one to address some security and privacy challenges in VANETs.

Chapter 3

Trust-based Platoon Service Query via Vehicular Communications

Future requirements for safer and more comfortable travel experience will lead to significant changes in the way we see vehicles driving on the road in the years to come. Hence, highway platooning of vehicles is identified as a promising framework because of its enhanced safety, increased comfort and improved highway utility. However, since the platoon service quality relies completely on the platoon head vehicles' driving skills and manners, the platoon service users will be less comfortable or even be put in danger once they choose badly-behaved platoon head vehicles. To tackle this problem and help the platoon service users avoid badly-behaved vehicles, in this chapter, we propose a trust-based platoon service query scheme for platoon head vehicles choosing with an objective to differentiate the well-behaved and badly-behaved vehicles [36]. The scheme integrates the unique features and requirements of user vehicles, e.g., location, destination and estimated time of arrival. Performance analysis through extensive simulations demonstrates the correctness and accuracy of the scheme.

3.1 Introduction

With the advancement of automobile technology, our driving experience will be revolutionized in the near future by the emergence and development of vehicle highway platooning [52]. A platoon is a line of vehicles that drive together at the same speed and with a close distance to each other. It has been proved that platooning can not only enhance the road safety, improve the traffic efficiency but also save the fuel due to air drag reduction [53]. For individual drivers, after long-term driving, platoon provides them a best chance to rest without pulling up their vehicles, which increases their comfort and enhances safety as well. In addition, supported by vehicular ad hoc network (VANET), platooning can be executed through a hybrid and more dynamic framework, which speeds up its application.

Because of those promising applications in the future, vehicle platooning has been investigated practically by Europe, U.S. and Japan. SARTRE [54] supported by European Commission is a project aiming at reducing fuel consumption, increasing safety, efficiency and driver convenience and comfort. In this project, a platoon head vehicle is a manually driven heavy vehicle, the user vehicles may join and leave the platoon dynamically. Once they join the platoon, they follow the platoon head vehicle automatically both laterally and longitudinally. PATH [53] is a California traffic automation program which is motivated by the need to produce a significant increase in the capacity of a highway lane to meet the increasing travel demand with a minimum new infrastructure construction. PATH platooning research is focused on heavy truck vehicles because of the potential for energy saving. The research also studies the gap between two trucks and its fuel consumption rate. Energy ITS [55] is a national ITS project by Japanese Ministry of Economy, Trade and Industry in 2008 with the main goal of mitigating the lack of skilled drivers. Lane marker detection based on computer vision controls the lateral distance and the radars make gap measurement to achieve the longitude

control. The experiment demonstrates that the project reduces the energy by 15% and CO2 emission by 2.1%. More projects are introduced and compared in [56].

However, some of the security problems haunted the platooning system, they jeopardize the highways and impede vehicle platooning's further application. Take an example, since the platoon service providers' performance are not equal due to their different driving styles or manners, some badly-behaved or malicious vehicles may jeopardize the system by providing low quality services to user vehicles if they are chosen as a platoon head vehicle. The problem can never be solved by the traditional authentication methods [57, 58] since they are all authorized vehicles, neither can it be solved by any privacy-preserving protocols [59] or incentive protocols [60].

In this chapter, in order to help the platoon member vehicles to avoid badly-behaved platoon head vehicles and ensure that they receive high quality platoon service, we propose a trust-based platoon service query (TPSQ) scheme to distinguish between well-behaved and badly-behaved platoon head vehicles according to their service qualities. In the TPSQ scheme, a pre-selection process which integrates factors like location, destination and estimated time of arrival is included to minimize the choosing range of the platoon head vehicles. Besides, trust and reputation system based on beta distribution is incorporated in the scheme with the aim to measure the reliability of a platoon head vehicle. In this system, the evaluations on the platoon head vehicle's historical performance are collected to determine the reputation score of that platoon head vehicle. As such, the query vehicle can always choose the highly reliable platoon to join. Specifically, the main contributions of this chapter are threefold:

- First, we take advantage of the unique features of VANET, e.g., high dynamics, hybrid architecture, V-2-I and V-2-V communications, to propose our TPSQ scheme. Specifically, the high dynamics ensure the real-time update

of reputation scores and traveling parameters. Then, the hybrid architecture, which includes vehicles, RSUs and server (TA), enables the computation and calculation of reputation scores and traveling parameters. Finally, vehicular communications lay a foundation for platoon service requests and platoon control.

- Second, to guarantee the feasibility of our method as well as reducing the communication cost, the classification method is developed to narrow the selection range of platoon head vehicles. With this classification method, the querying vehicle can conveniently select and then join the platoon which is within its range and shares the same or nearby destination with it.
- Third, we take performance evaluations provided by member vehicles as a trust metric to measure the quality of service (QoS) for platoon head vehicles. To the best of our knowledge, it is the first attempt to develop a trust and reputation system for describing the QoS of platoon head vehicles as well as providing an evidence for platoon head vehicle selection. Besides, the utilization of the beta distribution and maximum-likelihood estimation (MLE) helps to achieve the high accuracy and high dynamics of our trust and reputation system.

The remainder of this chapter is organized as follows. In Section 3.2, we formalize the system model and trust model considered in our work, and identify the design goals. In Section 3.3, the TPSQ scheme is presented in detail and the explanations of how TPSQ can help the query vehicles choose the highly reliable platoon vehicle are provided. Followed by the proposed scheme, trust management is introduced in Section 3.4 and the performance analysis of the proposed TPSQ scheme is described in Section 3.5. Finally, we give the related work in Section 3.6 and draw conclusions in Section 3.7.

3.2 System Model, Trust Model and Design Goal

In this section, we formalize the system model, trust model and identify our design goals.

3.2.1 System Model

We consider a flourish stage of VANETs where road side units (RSUs) are widely deployed, and each vehicle is equipped with an on board unit (OBU). In particular, the system model of our proposed TPSQ scheme consists of a top trusted authority (TA), a server, stationary road side units (RSUs) and vehicles traveling on the roads equipped with OBUs, as shown in Figure 3.1.

Figure 3.1: System model under consideration

TA: Trust authority plays a significant role in the whole system, it takes charge of registration of the server, all RSUs and vehicles.

Server: In general, server has a high storing and computational capability. As a result, it maintains the trust table which includes satisfaction levels and reputation scores for all platoon head vehicles as well as those platoon head vehicles' driving parameter vectors. Specifically, every time when an individual vehicle

requests to join a platoon, server will respond to this request by returning the most matching and trusted platoon head vehicle.

RSUs: On the one side, RSUs are connected through wired lines and secured channels to the server or TA. On the other side, they provide wireless connections to vehicles. The individual vehicles' queries, PH vehicles' responds and information updates are all forwarded through RSUs to TA or server. Hence, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, road side units are widely deployed along the roads and in the rest areas to cover the whole area, ensuring that the vehicles are able to update the information timely when driving on the roads. In some areas where RSUs are sparsely deployed, the update of the trust scores and traveling information of PH vehicles are delayed, the efficiency of our proposed TPSQ scheme may be decreased to some extent.

Vehicles: The vehicles $\mathcal{V}$ are a set of highly mobile nodes that are traveling on the roads; those vehicles are all equipped with on board units(OBUs) which allow them to communicate with other vehicles or RSUs. In platoon, V-2-V communication is not only utilized by platoon head vehicles to control the whole platoon and to process the requests from the member vehicles, but also applied for traffic or entertainment information sharing between vehicles. A vehicle frequently updates its own traveling information and evaluation scores to server when passing through RSUs via V-2-I communication. The drivers on the vehicles can choose either to drive individually or to join a platoon. According to their roles and current states, the vehicles can be further divided into three categories as follows.

- *PH Vehicles:* Platoon head vehicles $\{ph_1, ph_2, ph_3, \dots, ph_n\}$ form the set $\mathcal{P}$. Apparently, $\mathcal{P} \subset \mathcal{V}$. Since platoon head vehicles take the full control of the whole platoon when driving on the road, they are responsible for the safety and user experiences for all of the platoon member vehicles. What's

more, their behaviors even affect the whole road's condition and operation efficiency. It is easy to imagine that such vital roles in the platoon system can only be played by some specific qualified vehicles which are driven by experienced and capable drivers.

- *Individual Vehicles*: Except for the PH vehicles, all the other vehicles can be regarded as individual vehicles once they drive on the road until they decide to join a platoon. It is important to note that individual vehicles are not a specific type of vehicles, they are just a state of vehicles.
- *Platoon Member Vehicles*: Alternatively, in order to reach the destination in a more comfortable and energy saving way, those individual vehicles have the option to join a platoon via our proposed TPSQ mechanism and enter another state: platoon member vehicle. After that, they split the platoon and become individual vehicles again.

3.2.2 Trust Model

In the trust model, the trust level of different roles are defined. The tables and vectors which are maintained by different roles are also described in details.

- TA: Since trust authority is maintaining the public and private keys of the whole network, it is always trusted and can never be compromised by the adversaries at any time.
- Server: Similar to the trust authority (TA), server is a highly centralized facility with strong protection so it is impossible to be compromised by the adversaries. In particular, the main responsibilities of the server can be divided into two parts: maintaining trust table and traveling parameter table, computing traveling parameter similarity and trust scores.

Table 3.1: Trust Table Maintained by the Server

PH vehicle	Evaluation value	Beta value	Reputation score
ph_1	$c_{11} , c_{12} , \dots , c_{1m_1}$	β_1	r_1
ph_2	$c_{21} , c_{22} , \dots , c_{2m_2}$	β_2	r_2
ph_3	$c_{31} , c_{32} , \dots , c_{3m_3}$	β_3	r_3
$\vdots$	$\dots , \dots , \dots , \dots$	$\vdots$	$\vdots$
ph_n	$c_{n1} , c_{n2} , \dots , c_{nm_n}$	β_n	r_n

Table 3.1 shows the trust table maintained by the server. It includes the trust information of all PH vehicles $ph_1, ph_2, ph_3, \dots, ph_n$. Since a PH vehicle may serve as platoon head for many times, after each trip, the server will collect the evaluations from all platoon member vehicles in that specific trip and compute the satisfaction level for that trip. After a period of time, the server will get a few satisfaction levels for corresponding trips and store them in the row of the trust table. For example, for PH vehicle ph_1 , values $c_{11}, c_{12}, c_{13}, \dots, c_{1m_1}$ stands for the satisfaction levels of ph_1 after $1^{st}, 2^{nd}, \dots, m_1^{th}$ trip respectively. Using those c_{ij} ($j = 1, 2, 3, \dots, m_1$) values, the beta value β_i in the beta distribution of PH vehicles ph_i can be estimated and the corresponding reputation score r_i will be easily calculated from β_i and then be stored in the last two columns of the trust table.

Table 3.2: Traveling Parameter Table

	f	CL	DL	T_e	T_a
ph_1	0				
ph_2	0				
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
ph_n	0				

There are many traveling parameters to describe the driving statues for both PH vehicles and individual vehicles. However, in our proposed scheme, we only consider five most dominant parameters, which are listed in Table 3.2, and their notations and the corresponding meanings are listed in Table 3.3.

The traveling parameters of vehicles in the whole set $\mathcal{P}$ are documented in

Table 3.3: Notations

Notation	Descriptions
f	Traveling factor
CL	Current location of vehicle
DL	Destination location of vehicle
T_e	Estimated time to reach the destination
T_a	Accumulated driving time of PH vehicle

this table. Since not all vehicles are moving at all time, traveling factor f is necessary to indicate whether the vehicle is moving or static with the value $f = 0$ and $f = 1$ respectively. It saves computation resources during the travel similarity matching since the vehicle will be excluded once its $f = 0$. Following this, the current location of vehicle CL is prior to the other factors since it is too time-consuming and hence almost impossible for a querying individual vehicle to join a platoon too far away from itself. Besides, destination locations of querying individual vehicles and PH vehicle DL have to be the same or close, which ensures that the PH vehicle takes the querying individual vehicle to the place it desires. Furthermore, the estimated time of arrival (ETA) to the destination location T_e is a promise given by the PH vehicle, it has to be announced to the server in advance. Though the PH vehicle can decide when and where to stop for a rest and the speed for platoon, it must obey its promised estimated time of arrival (ETA) to the destination. At the same time, the querying individual vehicle will also submit an estimated time of arrival, only when these two T_e are close within a threshold will the PH vehicle be selected. Ultimately, the accumulated driving time T_a is another factor we consider; it represents the duration of driving for PH vehicle. Apparently, the longer driving duration is, the greater chance PH vehicle is in danger since T_a reflects the tiredness of driving in one aspect. In this way, T_a has to be considered in PH matching. As shown in the Table 3.2, all of the traveling factors f remain 0 at the beginning until the PH vehicles report that they are traveling. All those traveling parameters

will be updated once the platoon head vehicles pass through RSUs, since the RSUs are deployed widely, the update can be almost regarded as real-time.

- **RSUs:** RSUs are subordinated to TA and server via reliable communication. Hence the RSUs are trusted in the model, but they still need the authentication mechanism to be protected from the rogue attackers.
- **PH Vehicles:** Even though PH vehicles are driven by experienced and capable drivers, it cannot guarantee that they will provide reliable service at all time because they may provide poor PH service on the halfway due to poor, careless driving habits or even deliberate behaviors that leads to poor customer experience. For example, a PH vehicle may brake suddenly due to its driving habit or in another case, it just dismisses the platoon before arriving at the final destination.
- **Individual Vehicles:** By using the authentication system, it is reasonable to assume that the evaluations from individual vehicles towards PH vehicles are trusted.
- **Platoon member vehicles:** After each trip, a platoon member vehicle is required to provide a trust evaluation on the PH vehicle's performance in that trip. Besides, before requesting for platoon service, individual vehicles keep the traveling parameter vector which includes four parameters. Thanks to authentication schemes, these platoon member vehicles are trusted when providing the trust evaluations. Nevertheless, we do not exclude a minority of vehicles may evaluate randomly in the trust evaluation, which will be discussed later.

3.2.3 Design Goals

Since VANET is a large-scale wireless network, it faces serious security and computational problems in platoon service. Under the above models, we aim at developing a trust-based platoon service query mechanism where individual vehicles are able to choose the most reliable platoon to join via vehicular communications. Specifically, two desirable goals will be achieved:

1. **Communication cost reduction between PH vehicles and querying**

individual vehicles. When an individual vehicle requests to join a platoon, the request will be sent to the server, then the server will query and communicate with all of the PH vehicles in the trust table and finally returns a most reliable one to the querying individual vehicle. Since the network is very large, it will be time consuming and resource wasting to do so. Besides, due to the physical limitations and other restrictions, only a few PH vehicles are eligible to provide the platoon service to the querying vehicle. For example, a querying individual vehicle may not be able to follow a PH vehicle instantly if its 1000 kilometers away no matter how reliable the PH vehicle is. Therefore, to tackle the problem of physical limitation and reduce the communication cost, a preprocessing step is critical to the applicability of our proposed scheme.

2. **Accurate differentiation between well-behaved and badly-behaved**

PH vehicles. There are always badly-behaved and well-behaved PH vehicles on the road. The reason why PH vehicles behave badly can be explained as: in the real scenario, PH vehicles may sometimes speedup or brake suddenly due to poor driving habits, reaching destination later than the estimated time schedule, or even dismiss the platoon personally on half way. All of those behaviors may downgrade the participant experience to certain extents. Hence under such situation where reliable and unreliable vehicles are mixed, the

querying individual vehicle will be put in danger if it selects the PH vehicle arbitrarily. To help the querying individual vehicle avoid badly-behaved vehicles, it is significant for our scheme to distinguish between well-behaved and badly-behaved PH vehicles. In addition, the proposed scheme should be accurate and scalable.

3.3 Proposed TPSQ Scheme

In this section, we propose our TPSQ scheme which consists of five parts: system initialization, platoon service request, request processing, trust-based platoon selection, platoon service quality feedback.

3.3.1 System Initialization

For the proposed system, it can be assumed that all roles share the same parameters. Specifically, given the security parameters, trust authority (TA) first generates and publishes its own public key PK_{TA} , the public keys of RSUs and vehicles are their IDs. Although RSUs are trusted and subordinated by the TA, TA still needs to assign a private key for each RSU deployed at roadside to prevent potential rogue RSU issue launched by malicious guys. In particular, for each deployed roadside unit RSU_j , TA generates its private key SK_{RSU_j} . Besides RSUs, for each vehicle v_i , TA also generates its private key SK_{v_i} .

In addition, if vehicle $v_m \in \mathcal{V}$ uses the platoon service provided by PH vehicle $ph_i \in \mathcal{P}$, each of them is required to give an evaluation over ph_i after the trip. This evaluation score has to be uploaded to the server through RSUs once v_m encounters an RSU. After receiving all platoon member vehicles' evaluations on the j th trip, the score $c_{ij} \in [0, 1]$ can be computed which reflects the satisfaction level on the ph_i 's service in the j th trip with the value 0 indicating that platoon member vehicles

are completely unsatisfied and 1 indicating completely satisfied. Initially, server sets up the trust table shown in the Table 3.1 to store those satisfaction levels. In the table, the satisfaction levels will be kept vacant if no corresponding services are provided. At the very beginning, beta values $\beta_i (i \in [1, n])$ are defined as 1, they will be updated according to the satisfaction level c_{ij} .

Except for the evaluation scores, the PH vehicles ph_i upload their destination locations DL and current locations CL to the server using rectangular coordinates (x_j, y_j) and (X_j, Y_j) respectively at the beginning of the trip. Besides, the estimated time of arrival (ETA) to the destination T_e and the time to start the trip also need to be submitted. All of the information is stored in the traveling parameter table, the PH vehicles keep reporting their current locations CL once they encounter RSUs. Those PH vehicles who have not uploaded their information stay in the “static” state and all the information is kept vacant. The initialization step is shown in Table 3.4 below:

Table 3.4: Traveling Parameter Initialization

	f	CL	DL	T_e	T_a
ph_1	1	X_1, Y_1	x_1, y_1	T_1	t_1
ph_2	1	X_2, Y_2	x_2, y_2	T_2	t_2
ph_3	0				
ph_4	1	X_4, Y_4	x_4, y_4	T_4	t_4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
ph_n	0				

3.3.2 Platoon Service Request

After the system is established, each individual vehicle $v_j \in \mathcal{V}$ that is running on the road is able to communicate with an RSU within its transmission range through V-2-I communication. When a querying individual vehicle v_0 wants to request a platoon service, it submits its traveling vector $\vec{I}_0$ to the server. This traveling vector includes its own traveling parameters: current location (X_0, Y_0) ,

destination location (x_0, y_0) , expected time of arrival T_0 and expected accumulated driving time for PH vehicle t_0 so that $\vec{I}_0 = [X_0, Y_0; x_0, y_0; T_0; t_0]$. Besides, v_0 also submits the distance requirements for CL and DL, denoted by Th_1 and Th_2 . For example, $Th_1 = 10km$ means querying individual vehicle wants to find the PH vehicle within 10 kilometers. Similarly, the time requirement of T_e and T_a are also decided by v_0 using Th_3 and Th_4 respectively.

3.3.3 Request Preprocessing

The platoon service request will be submitted to the server together with individual vehicle v_0 's traveling vector $\vec{I}_0$, then preprocessing is done by the server with the goal of minimizing the candidate size of PH vehicles and make a preparation for trust-based platoon selection. It includes four steps: vehicle location matching, destination location matching, estimated ToA matching and accumulated driving time matching. The flow diagrams of request preprocessing is shown in Figure 3.2. Detailed descriptions are provided below:

1. **Vehicle location matching:** For simplicity, we use Euclidean distance as location matching metric. In the real scenario, a dynamic map information should be incorporated when calculating distance because of different road conditions. For each PH vehicle $ph_i \in \mathcal{P}$, the Euclidean distance between querying individual vehicle v_0 and ph_i 's current location, denoted by D_{CL_i} , will be calculated by using the equation:

$$D_{CL_i} = \sqrt{(X_i - X_0)^2 + (Y_i - Y_0)^2} \quad (3.1)$$

p_i will be selected if $D_{CL_i} < Th_1$. Those selected PH vehicles form a new set $\mathcal{P}_1$.

2. **Destination location matching:** Each PH vehicle $v_j \in \mathcal{P}_1$ will be selected

Figure 3.2: Preprocessing Diagram

to do the destination matching using Euclidean distance:

$$D_{DL_j} = \sqrt{(x_j - x_0)^2 + (y_j - y_0)^2} \quad (3.2)$$

when $D_{DL_j} < Th_2$, v_j will be selected and all of those selected vehicles form a new set $\mathcal{P}_2$.

3. **Estimated ToA matching:** For each PH vehicle $ph_k \in \mathcal{P}_2$, $(D_{Te})_k = |T_k - T_0|$ will be calculated to measure the distinction of estimated time of arrival between PH vehicles and querying individual vehicle. If $D_{Te_k} < Th_3$, then ph_k will be selected and finally form set $\mathcal{P}_3$.

4. **Accumulated driving time matching:** For each PH vehicle $ph_l \in \mathcal{P}_4$, by calculating $(D_{Ta})_l = |t_l - t_0|$, the expected and actual tiredness of PH vehicle drivers will be measured. If it meets the requirement of querying individual

vehicle such like $(D_{T_a})_l < Th_4$, the PH vehicle ph_l will be selected to form $\mathcal{P}_4$.

After the preprocessing, the server gets a very small PH vehicle set $\mathcal{P}_4$ which satisfies the request vehicle's need for destination location, estimated time of arrival and accumulated driving time at the same time. The preprocessing achieves the goal of reducing communication cost for PH vehicle choosing and lays a foundation for trust-based PH vehicle selection in the next step.

3.3.4 Trust-based Platoon Selection

For those selected PH vehicles in $\mathcal{P}_4$, server will rearrange the trust table according to their reputation scores. Then the server will query from the first PH vehicle in the table to the last until one accepts to provide the platoon service. Finally, proposed merging location and proposed merging time will be obtained by the server and then forwarded to the querying individual vehicle.

3.3.5 Platoon Service Quality Feedback

After the platoon member vehicle leaves the platoon, it is asked to provide a feedback about the quality of service provided by the PH vehicle. If the platoon member vehicle fails or refuses to provide feedback, the server will refuse to provide service next time. The evaluation will be uploaded via RSUs to server to output a satisfaction level between 0 and 1. In this section, we describe the process how the service evaluating system is operated and how the satisfaction level is calculated.

1. *Service Evaluations*

The service evaluations should be easy and straightforward for the platoon member vehicles to handle. Hence we design such a system including a few

questions for the evaluators. After each trip, those questions will be presented on the screen of the OBUs in the vehicles, the drivers only need to choose “Yes” or “No” on each question.

The design of the questions should be concise and straightforward; otherwise the user vehicles may be reluctant to give evaluations or may get confused about them. Without losing generality, we design four questions which is shown in Figure 3.3 below:

Figure 3.3: Evaluation questions and evaluation vector

The first two questions regarding the scheduled destination accuracy and punctuality are most significant since they are the basic requirements of a platoon service. By contrast, the last two questions are relatively subjective. Specifically, question 3 asks about the riding comfort, there are many behaviors that lead to the uncomfortable experience of the ride. For example, sudden speed-up or brake, frequent or unnecessary lane changes and so on. For question 4, it gives the user vehicles a chance to punish the PH vehicles whose behaviors may cause more severe consequences than those in question 3. The dangerous behaviors could be tailgating, aggressive driving, making phone calls when driving or even drunk driving.

After the evaluator gives answers to the questions, an evaluation vector will be generated by the OBU of the evaluator vehicle which stores the evaluations as the binary string in the evaluation vector. For the first three questions, the answer “Yes” is denoted by “1” and “No” denoted by “0” in the evaluation

vector; for the last question, the answer “Yes” is denoted by “0” and “No” denoted by “1”.

2. Transforming Evaluations to Satisfaction State Machines

After a trip, all of the platoon member vehicles will submit their evaluation vectors to the server. Theoretically, there will be many possible cases. To a specific trip, each evaluation vector specifies one state, either it is satisfied state in which a satisfied evaluation is given, normal states or unsatisfied state in which an unsatisfactory evaluation is given. An evaluation to the trip has a number of state variables depending on the number of the evaluating vehicles indicating whether the service quality of the PH vehicle in that trip is high or low.

Figure 3.4: Satisfaction State Machine

Figure 3.4 illustrates the evaluation satisfaction machine for a random evaluating vehicle in a trip. The state machine consists one satisfied state, three normal states and one unsatisfied state based on the number of “0”s in the evaluation vector. We label these states as S_1, S_2, S_3, S_4, S_5 respectively. The

satisfied state is defined when all of the questions are chosen as “1”, it is also the preferred situation. We can further classify those evaluation cases according to the number of “0”s in the vector and apparently, the worst case is defined as unsatisfied state when all “0”s appear in the vector.

3. *Calculation of Satisfaction Level*

Satisfaction level is the metric to indicate the PH vehicle’s performance in one trip, it is the extent to which a PH vehicle behaves safely and punctually to meet the requirements of the evaluation questions. In order to calculate the satisfaction level of a PH vehicle in a trip, we will collect those evaluations from all of the platoon member vehicles in that trip. Since evaluating vehicles are mutually dependent, all of those evaluations from them are dependent.

We model the dependent evaluations from those platoon member vehicles by a stochastic process such that it may be in state S_1, S_2, S_3, S_4, S_5 in the satisfaction state machine with π_i indicating the probability the stochastic process is in state S_i . Since we have five states, we can easily get: $\sum_{i=1}^5 \pi_i = 1$. The physical meaning of π_i is the probability that an evaluation is in state S_i .

Let p_i denote a PH vehicle, c_{ij} is the satisfaction level of p_i in the j th trip. There are m platoon member vehicles in this trip, according to their evaluation vectors, the number of platoon member vehicles is m_i with evaluation vectors respect to the S_i state. The probability that an evaluation is in state π_i can be easily expressed as:

$$\pi_i = \frac{m_i}{m}, i = 1, 2, 3, 4, 5 \quad (3.3)$$

With the above formulation, the satisfaction level c_{ij} can be calculated as the sum of the products of each state’s grade and probability:

$$c_{ij} = \sum_{k=1}^5 \pi_k c^k \quad (3.4)$$

where c^k is the “grade” assigned to state S_k , measuring the closeness between the observed evaluation state and the specified “satisfied” state S_1 . The closer the evaluation state to the “satisfied” state, the greater satisfaction level it is. We denote $\vec{I}_k$ as the evaluation vector of state S_k so that we can get:

$$\begin{matrix} \vec{I}_1 = [1, 1, 1, 1] \\ \vec{I}_5 = [0, 0, 0, 0] \end{matrix} \quad \vec{I}_2 = \begin{cases} [0, 1, 1, 1] \\ [1, 0, 1, 1] \\ [1, 1, 0, 1] \\ [1, 1, 1, 0] \end{cases} \quad \vec{I}_3 = \begin{cases} [0, 0, 1, 1] \\ [1, 0, 0, 1] \\ [1, 1, 0, 0] \\ [0, 1, 1, 0] \\ [0, 1, 0, 1] \\ [1, 0, 1, 0] \end{cases} \quad \vec{I}_4 = \begin{cases} [1, 0, 0, 0] \\ [0, 1, 0, 0] \\ [0, 0, 1, 0] \\ [0, 0, 0, 1] \end{cases} \quad (3.5)$$

To evaluate the closeness between $\vec{I}_k$ and $\vec{I}_1$, we let $\vec{I}_{k,t}$ denote the t th element in the vector $\vec{I}_k$. Since the dimension of all evaluation vectors are 4, so $\vec{I}_{k,t} \in [0, 1]$ with $1 \leq t \leq 4$. The closeness between $\vec{I}_k$ and $\vec{I}_1$ can be evaluated as:

$$c^k = \frac{\sum_{t=1}^4 \vec{I}_{1,t} \cdot \vec{I}_{k,t}}{\sqrt{\sum_{t=1}^4 \vec{I}_{1,t}^2} \sqrt{\sum_{t=1}^4 \vec{I}_{k,t}^2}} \quad (3.6)$$

3.4 Trust Management

After getting enough satisfaction level values c_{ij} , we need to calculate the reputation of PH vehicle Ph_i . In this section, we introduce the method of calculating reputation scores of a PH vehicle.

Since c_{ij} are a set of actual data, we cannot use the existing distributions to describe it, so we use the most likelihood estimation (MLE) to estimate the distribution. Hence the beta distribution is an ideal description of the satisfaction level because: first, it is a distribution that comprises many different distributions controlled by parameters α and β ; second, the domain of the beta reputation can be viewed as a probability so that it can be used to describe the prior distribution over the probability which models the satisfaction level. By applying the Bayesian inference, the beta distribution can be used as the posterior distribution of the probability after getting sufficient instances [61].

1. MLE of β

The beta distribution is an ideal description of the satisfaction level c_{ij} distribution for a specific PH vehicle ph_i in the j th trip ($j \in [1, m_i]$). m_i stands for the number of trips that vehicle ph_i receives the evaluations. The evaluation values c_{ij} can be modeled as a random variable X_i that follows beta distribution with the value 0 indicating unsatisfaction and value 1 indicating satisfaction. The PDF of beta distribution is expressed as:

$$f(c_{ij}|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} c_{ij}^{\alpha-1} (1 - c_{ij})^{\beta-1} \quad (3.7)$$

since c_{ij} are independent and identically distributed, the joint density function is:

$$\begin{aligned} f(c_{i1}, c_{i2}, \dots, c_{im_i}|\alpha, \beta) \\ = f(c_{i1}|\alpha, \beta) \times f(c_{i2}|\alpha, \beta) \times \dots f(c_{im_i}|\alpha, \beta) \end{aligned} \quad (3.8)$$

α and β are to be estimated based on the maximum likelihood estimation (MLE):

$$\begin{aligned}
& \mathcal{L}(\hat{\alpha}, \hat{\beta} | c_{i1}, c_{i2}, \dots, c_{im_i}) \\
& = f(c_{i1}, c_{i2}, \dots, c_{im_i} | \hat{\alpha}, \hat{\beta}) = \prod_{k=1}^{m_i} f(c_{ij} | \hat{\alpha}, \hat{\beta})
\end{aligned} \tag{3.9}$$

In practice, we use the log-likelihood:

$$\begin{aligned}
\ln \mathcal{L}(\hat{\alpha}, \hat{\beta} | c_{i1}, c_{i2}, \dots, c_{im_i}) & = \sum_{j=1}^{m_i} \ln f(c_{ij} | \hat{\alpha}, \hat{\beta}) \\
& = \sum_{j=1}^{m_i} [\ln \Gamma(\hat{\alpha} + \hat{\beta}) - \ln \Gamma(\hat{\alpha}) - \ln \Gamma(\hat{\beta}) + \\
& (\hat{\alpha} - 1) \ln c_{ij} + (\hat{\beta} - 1) \ln(1 - c_{ij})]
\end{aligned} \tag{3.10}$$

The maximum likelihood estimates of α and β can be attained by solving the partial differential equation set:

$$\begin{aligned}
\frac{\partial \ln \mathcal{L}(\hat{\alpha}, \hat{\beta} | c_{i1}, c_{i2}, \dots, c_{im_i})}{\partial \hat{\alpha}} & = \frac{m_i \frac{\partial \Gamma(\hat{\alpha} + \hat{\beta})}{\partial \hat{\alpha}}}{\Gamma(\hat{\alpha} + \hat{\beta})} \\
- \frac{m_i \frac{\partial \Gamma(\hat{\alpha})}{\partial \hat{\alpha}}}{\Gamma(\hat{\alpha})} + \sum_{j=1}^{m_i} \ln c_{ij} & = 0
\end{aligned} \tag{3.11}$$

$$\begin{aligned}
\frac{\partial \ln \mathcal{L}(\hat{\alpha}, \hat{\beta} | c_{i1}, c_{i2}, \dots, c_{im_i})}{\partial \hat{\beta}} & = \frac{m_i \frac{\partial \Gamma(\hat{\alpha} + \hat{\beta})}{\partial \hat{\beta}}}{\Gamma(\hat{\alpha} + \hat{\beta})} \\
- \frac{m_i \frac{\partial \Gamma(\hat{\beta})}{\partial \hat{\beta}}}{\Gamma(\hat{\beta})} + \sum_{j=1}^{m_i} \ln(1 - c_{ij}) & = 0
\end{aligned} \tag{3.12}$$

where

$$\frac{\partial \Gamma(\hat{\alpha} + \hat{\beta})}{\partial \hat{\alpha}} = \int_0^\infty (\ln x) x^{\hat{\alpha} + \hat{\beta} - 1} e^{-x} dx \quad (3.13)$$

Generally, we can consider the single parameter β with $\alpha = 1$, in that case, the partial differential equation could be written as:

$$\frac{\partial \ln \mathcal{L}(1, \hat{\beta} | c_{i1}, c_{i2}, \dots, c_{im_i})}{\partial \hat{\beta}} = m_i \frac{1}{\hat{\beta}} + \sum_{j=1}^{m_i} \ln(1 - c_{ij}) \quad (3.14)$$

The maximum likelihood estimate of PH vehicle ph_i 's β is:

$$\hat{\beta}_i = \frac{m_i}{\sum_{j=1}^{m_i} \ln(\frac{1}{1-c_{ij}})} \quad (3.15)$$

The expected value of the value X_i is given by:

$$E_B[X_i] = \int_0^1 c_{ij} \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) + \Gamma(\beta)} c_{ij}^{\alpha-1} (1 - c_{ij})^{\beta-1} dc_{ij} \quad (3.16)$$

Once the MLE of β_i is calculated, the beta distribution of the PH vehicle ph_i is known, $X_i \sim \text{Beta}(1, \hat{\beta}_i)$.

2. The reputation score

Let X_i represent the PH vehicle ph_i 's satisfaction level c_{ij} , then the function defined by

$$r_i = E[\text{beta}(X_i | 1, \hat{\beta}_i)] = \frac{1}{1 + \hat{\beta}_i} \quad (3.17)$$

is called PH vehicle ph_i 's reputation score. The reputation score r_i can be interpreted as measure of reputation, or in other words an indication of how a particular PH vehicle is expected to behave in the future [42].

3.5 Performance Evaluation

We will evaluate the performance of our proposed TPSQ scheme. The numerical data are generated in Matlab. The performance metrics used in the evaluation are: i) Satisfaction levels in terms of the trip number with different service qualities, which is defined by the probability to provide a specific service that satisfies the platoon member vehicles; ii) Reputation scores in terms of the total number of trips with different random-mouth rates, which is defined by the proportion of a platoon members who give random evaluation towards a specific service; iii) False positive rate versus the total number of trips.

3.5.1 Vehicle Behaviors

For PH vehicles and member vehicles, we use two parameters to describe their manners respectively:

High quality service rate (HQSR): As described in Section 3.3.5, there are four metrics for evaluating the service quality of the PH vehicles, each metric is presented by a question displayed to the platoon member vehicle at the end of the trip, the answer to each question could either be “Yes” or “No” indicating whether the PH vehicle provides that specific satisfactory service or not. In the ideal case, the PH vehicle’s service satisfies all of the four metrics, which means it takes the platoon members to the scheduled destination punctually and comfortably without any dangerous driving manners. However, this is impossible in the real scenario due to the limitation of PH vehicle drivers’ driving skills and driving habits, or simply because they are selfish. Moreover, some of the malicious PH vehicle drivers even plan to overturn the whole system by providing low quality services deliberately. Their service performance are distinguished by “High quality service rate” denoted by p , where $p \in [0, 1]$. It stands for the probability that a PH vehicle provides a satisfactory service; alternatively, it measures the probability

that “1” appears in each blank of the evaluation vector. Apparently, when a well-behaved PH vehicle will always be punctual and arrive the destination accurately, it has a lower probability to drive dangerously or makes the user vehicles less comfortable. As a result, a well-behaved PH vehicle is more reliable, which could be described by a higher “p” value.

Random-mouth rate (RMR): At the same time, platoon members may not always provide evaluations that reflects the real service quality of the PH vehicles. This could be caused by many factors: each platoon member vehicle has its own opinions which is a little bit different from the real case, or the platoon member vehicle is not cooperative in giving an accurate evaluation after the service. In either case, their evaluations can be modeled as random. Hence a Random-mouth rate (RMR) always exists in the feedback, it is denoted by q measuring the proportion of platoon member vehicles’ who give random evaluations to the PH vehicles after each platoon service. It should be noted that our TPSQ scheme performs well with the existence of the random-mouth rate, detailed analysis will be provided in the next section.

3.5.2 Simulation Setup

In our simulation, we study the long-term reputation evaluation for each PH vehicle who has already served as a platoon head for $N = 200$ trips. For every trip, there are n platoon member vehicles who use the service and give evaluations. Although in the real project, the maximum platoon size is 15 vehicles at one time [62], considering the platoon member vehicles’ behaviors of joining and splitting in the halfway, $n = 100$ is a reasonable assumption in one trip.

We generate the data of performance vectors by means of Monte Carlo simulation. It allows us to generate independent and repeated random sampling following the stochastic process of a PH vehicle’s performance in a few trips. Then, we sim-

ulate the procedure described in Section 3.3.5 to construct the state machines and then collect satisfaction level data, finally the reputation score will be calculated using those satisfaction level data.

Specifically, we generate a total number of $N = 200$ performance vectors reflecting the performance qualities in 200 trips for a PH vehicle. Apparently, for a PH vehicle with a specific HQSR value p , the probability that a performance vector is in state S_j , denoted by P_{b-S_j} , $j \in [1, 5]$, follows the binomial distribution with parameters 4 and p , $P_{b-S_j} \sim B(4, p)$:

$$P_{b-S_j} = \binom{4}{5-j} p^{5-j} (1-p)^{j-1} \quad (3.18)$$

Given a performance vector in state S_1 and the RMR of q , Figure 3.5 shows the state transitions from PH vehicle's real performance state S_1 to random-mouth evaluators' evaluation states. Since the random-mouth vehicles evaluate randomly, it has possibilities to all of the five states with transition possibilities of $t_{11}, t_{12}, t_{13}, t_{14}, t_{15}$ respectively. Similarly, when the performance states are S_2, S_3, S_4, S_5 , we can also get a state transition graph. Considering all of the five states and their mutual transitions, the transition matrix T is denoted as:

$$T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{15} \\ t_{21} & t_{22} & \dots & t_{25} \\ \vdots & \vdots & \ddots & \vdots \\ t_{51} & t_{52} & \dots & t_{55} \end{pmatrix} \quad (3.19)$$

It is not hard to calculate the transition matrix T from Figure 3.5. Apart from the random transition evaluations, there are percentage of $1 - q$ evaluations that reflects the real performance of PH vehicle. We can calculate the probability π_i that an evaluation is in state $S_i, i \in [1, 5]$ by combining all above together:

Figure 3.5: State Transitions from Real Performance State to Random-mouth Evaluation States

$$\pi_i = \sum_{j=1}^5 P_{b-S_j} \cdot t_{ji} + (1 - q) \cdot S_i \quad (3.20)$$

The detailed settings of simulation are shown in the Table 3.5.

Table 3.5: Simulation settings

Parameter	Settings
Number of trips for each PH vehicle	N=200
Number of platoon member vehicles in each trip	n=100
High quality service rate for PH vehicles in each trip	p=0; 0.2; 0.4; 0.6; 0.8; 1
Random-mouth rate for platoon member vehicles	q=1%; 10%; 20%; 40%

3.5.3 Simulation Results

The simulation results demonstrate that our system is correct, convergent and accurate.

1. *Correctness:* Figure 3.6 shows the variation of satisfaction level values $c_{ij}, j \in [1, 200]$ in $N = 200$ trips for a PH vehicle ph_i in terms of HQSR values. From the figure, as can be seen, the satisfaction level c_{ij} remains steady for 200 trips. As p increases, c_{ij} also increases. The reason is that with a larger p value, ph_i is more possible to provide high quality service, the satisfaction level from the platoon member vehicles are hence higher. From the figure, it can also be seen that the well behaved and badly behaved PH vehicles are clearly distinguished, which justifies the correctness of our proposed scheme. In addition, when q increases from 1% to 40%, the six clouds of satisfaction levels get closer to each other and the distinguishability decreases. That is because when q increases, it means more vehicles evaluate randomly and the evaluations deviate from the true performance. The results match with the analysis perfectly. With all of the satisfaction level c_{ij} , we use the Eq. (3.17) to calculate the reputation scores of ph_i in different cases, the results are shown in Table 3.6. The system will be subverted when random mouth rate $q \geq 50\%$.

Table 3.6: Reputation score in beta(1, β) of ph_i (bmr=10%)

PH vehicle with various high quality service rate	Estimated Beta Value	Reputation Score
$ph_i(p = 1)$	$\beta_1 = 0.2854$	$r_1 = 0.7780$
$ph_i(p = 0.8)$	$\beta_2 = 0.5039$	$r_2 = 0.6650$
$ph_i(p = 0.6)$	$\beta_3 = 0.7301$	$r_3 = 0.5780$
$ph_i(p = 0.4)$	$\beta_4 = 1.1423$	$r_4 = 0.4668$
$ph_i(p = 0.2)$	$\beta_5 = 2.1715$	$r_5 = 0.3153$
$ph_i(p = 0)$	$\beta_6 = 15.0367$	$r_6 = 0.0624$

2. *Convergency:* Figure 3.7 shows the reputation scores $r_i, i \in [1, 100]$ of 100

(a) Random-mouth Rate $q=1\%$ (b) Random-mouth Rate $q=10\%$ (c) Random-mouth Rate $q=20\%$ (d) Random-mouth Rate $q=40\%$

Figure 3.6: Satisfaction Level of a PH Vehicle with Different HQSR values in 200 Trips

(a) Random-mouth Rate $q=1\%$ (b) Random-mouth Rate $q=10\%$ (c) Random-mouth Rate $q=20\%$ (d) Random-mouth Rate $q=40\%$

Figure 3.7: Reputation scores of different PH vehicles in various numbers of trips

different PH vehicles $ph_i, i \in [1, 100]$ after the total number of N trips. For every PH vehicle ph_i , the HQSR value $q_i = 0.9 + (i - 1) \cdot (0.97 - 0.9)/99$. From the figure, we can see that when N is small, the reputation scores fluctuate seriously with the increasing of N . That is because when the total number of trips is of a small value, the reputation score is affected seriously by the arbitrary performance so it is very unstable. As trip number increases, the reputation scores are accumulated and become convergent. When the random-mouth rate increases, the reputation score face decreases due to the random evaluations.

(a) Random-mouth Rate $q=1\%$ (b) Random-mouth Rate $q=10\%$ (c) Random-mouth Rate $q=20\%$ (d) Random-mouth Rate $q=40\%$

Figure 3.8: False positive rate versus various numbers of trips

3. *Accuracy*: In order to calculate the accuracy of our proposed scheme, we define that the top 20 PH vehicles with the highest p values as “good PH vehicles” while the others as “bad PH vehicles”, after the simulation we rank the reputation score of all the PH vehicles and count the number of “bad PH vehicles” n_b among the highest 20 reputation scores, the ratio $f_p = n_b/20$ is defined as “false positive rate”. Figure 3.8 shows the false positive rate of the of our proposed scheme with the increasing of the total number of trips. We can see that when N is a small value, the false positive rate is very big since the reputation score is not convergent and the evaluations do not reflect the true performance of the PH vehicle, as N increases, f_p falls to a very small value, the accuracy of our proposed scheme is verified.

3.6 Related Work

Our work is related to the platoon formation which is the first part of platoon management. In this section, we explore some of the existing platoon management protocols [63]. In [64], the authors propose a disturbance-adaptive platoon architecture by considering the intra platoon dynamics, then the driving strategy for platoon head vehicles which exploit V-2-V communications are discussed. In order to solve the problem of sharp acceleration and deceleration which significantly consumes more fuel and results in more exhaust, the metric of acceleration noise [65] is utilized. Furthermore, a filter-multicast protocol was proposed in [66] which realizes the function of allocating dynamic platoon-ID, and achieves dynamic management and platoon multicast. In [67], the analysis of interferences caused by non-automated vehicles during a JOIN maneuver is proposed. An application layer protocol is defined to support the maneuver, together with situations that can prevent successful termination, and describe how they can be detected. Since maximizing the platoon size and lifetime are both important factors in platoon [68], [69] presents an approach to lane assignment for highway vehicles that increases traffic throughput while ensuring vehicles can exit successfully at their destinations.

Regarding the stability of the platoon, [70] investigates a practical string stability of both homogeneous and heterogeneous platoons of adaptive cruise control (ACC) vehicles, the constant time headway spacing policy is applied by considering the parasitic time delays and lags of the actuators and sensors when building the vehicle longitudinal dynamics model. Furthermore, three characteristic modeling approaches are summarized in [71]: reaction time, update time and adaption time. Y.Zhang etc. have proposed a vehicle-platoon-aware data access solution to address the problem of poor performance of data access in VANET due to high mobility of vehicles and unreliable wireless communications. The work does not rely on a centralized vehicular mobility observation or analysis, instead, its proto-

col is able to quickly identify the platoon and predict split process in a distributed manner [72]. In order to control the vehicle platooning in the VANET, a platoon management protocol based on wireless communication for Cooperative Adaptive Cruise Control (CACC) vehicles is developed [73]. The protocol includes three basic platooning maneuvers which are common scenarios in the highway: merge, split and lane change. Moreover, a set of micro-commands are defined in the application layer to accomplish those maneuvers. Finite State Machines (FSM) are implemented to describe the protocol operations. Another modular approach targeted on mitigating the interferences caused by non-automated vehicles during a maneuver is proposed in [74].

The vehicular communication system security has also been studied by many researchers [9, 75, 11]. In [9], the threats and types of adversaries including active and passive attackers are analyzed in vehicular communication context, security and privacy requirements are identified as message authentication and integrity, non-repudiation, authentication, access control and confidentiality with a spectrum of mechanisms presented to secure the vehicular communication systems. In [75], Matthias proposed a vehicular security architecture which integrates existing individual solutions for vehicle registration, data integrity and authentication. Various issues related to the implementation and deployment aspects of secure vehicular communication systems have been discussed in [11]. Besides, service query issue has also been explored in web service [76].

All of the above efforts on the platoon management focus on the controlling system of platoon management or in the area of communication security. However, they never take the human factors of drivers into consideration, neither do they consider a service query issue when multiple platoons are available to be selected from.

3.7 Summary

In this chapter, we have proposed a practical trust-based platoon service query (TPSQ) scheme in order to enhance the road safety and user comfort. By adopting our scheme, querying vehicles are able to choose the most reliable PH vehicle to follow. In particular, we integrate the parameters in the real scenario, e.g., the location of querying vehicles and PH vehicles, targeted destination and estimated time of arrival for the querying vehicles to make the scheme more applicable as well as minimizing the computing time. Besides, the trust and reputation system is developed to distinguish PH vehicles according to their historical service qualities. Through extensive performance evaluation, we have demonstrated that the TPSQ scheme can achieve much higher accuracy in terms of distinguishing reliable PH vehicles. In the future work, we intend to take into account more factors to evaluate the trust and reputation in vehicular platooning scenarios.

Chapter 4

Reliable Trust-based Platoon Service Recommendation Scheme

In the previous chapter, we introduced TPSQ, a trust-based platoon service query scheme when choosing platoon head vehicles with an objective to differentiate the well-behaved and badly-behaved vehicles. However, the user vehicles may give untruthful feedbacks for platoon head vehicles, and as a result, the TPSQ scheme is subject to badmouth attack or ballot-stuffing attack [77]. In this chapter, we will focus on how to distinguish badmouth or ballot-stuffing attackers' and then exclude their untruthful evaluations in vehicular platooning [37].

4.1 Introduction

With the advance of automobile technology, vehicle manufactures and research academia are heavily engaged in the blueprint of highway vehicular platooning [56]. By linking vehicles into a train-like group, the platooning liberates drivers from the tedium of driving. Besides, this newly emerging highway platooning technique is characterized by enhanced road safety, improved traffic efficiency and less energy consumption due to air drag reduction [78]. Compared to the way of constructing

roads, platoon-based driving pattern is a more sustainable and less costly way to alleviate traffic congestion and reduce accidents, which envisions one of the future intelligent transportation systems (ITS). With so significant innovative benefits to achieve, many researchers have shown great interests in the initiative: as a California traffic automation program, PATH [53] is motivated by the need to produce a significant increase in the capacity of a highway lane to meet the increasing travel demand with a minimum new infrastructure construction. SARTRE [54], supported by European Commission, is a project aiming at reducing fuel consumption, increasing safety, efficiency and driver convenience and comfort. Energy ITS [55] is a national ITS project by Japanese Ministry of Economy, Trade and Industry in 2008 to mitigate the problem of lacking skilled drivers.

Though much effort has been invested by engineers and researchers to make such a platooning system work, the challenge of ensuring the security of the system still remains to be tackled before the beauty of platooning can be fully appreciated by its large audience [79]. Without security guarantee, some badly-behaved or malicious platoon head vehicles may jeopardize the system by providing low quality services or even put the user vehicles in dangerous situations [36]. Therefore, how to identify those badly-behaved or malicious platoon head vehicles has become a fundamental requirement in securing vehicular platooning.

In this chapter, we propose a reliable trust-based platoon service recommendation scheme, which is termed REPLACE, to rank the platoon head vehicles by establishing a trust and reputation system. In this system, the server uses the feedbacks collected from user vehicles to compute the reputation scores of platoon head vehicles. By doing so, the well-behaved and badly-behaved platoon head vehicles are clearly distinguished according to their reputation scores and then the server will recommend a reliable platoon head vehicle to the user vehicle. However, the system is potentially subject to malicious user vehicles who might give untruthful feedbacks. To mitigate the negative impacts of those malicious user vehicles, we

design an iterative filtering algorithm for our REPLACE scheme to exclude their feedbacks. Specifically, the main contributions of this chapter are threefold:

- First, we take advantage of the unique features of VANET [80, 81, 82], e.g., high dynamics, hybrid architecture, vehicle-to-infrastructure (V-2-I) and vehicle-to-vehicle (V-2-V) communications, to propose our REPLACE scheme. Specifically, the high dynamics ensure the real-time update of feedbacks. The hybrid architecture, i.e., vehicles, road side units (RSUs), server and trust authority (TA), enables the storage of feedbacks and computation of reputation scores. Besides, vehicular communications also lay a foundation for platooning service requests and platoon control.
- Second, we design an evaluation mechanism by utilizing performance feedbacks provided by user vehicles as the trust metrics to measure the quality of services of platoon head vehicles. To the best of our knowledge, it is the first attempt to develop a trust and reputation system for describing the services of platoon head vehicles, eventually leading to the optimal selection of platoon head vehicles. In particular, the system is developed on the Dirichlet distribution, ensuring high accuracy and dynamics.
- Third, we mitigate the effect of malicious user vehicles' feedbacks by proposing an iterative filtering algorithm to exclude those attackers from our evaluation mechanism. In doing so, the evaluation of the behavior of platoon head vehicles becomes more accurate, ultimately enabling REPLACE to be resistant against some sophisticated attacks.

The remainder of this chapter is organized as follows. In Section 4.2, we formalize the system model and trust model considered in our work, and identify our design goals. In Section 4.3, the REPLACE scheme is presented in detail, along with the rationale that it can help the query vehicles to choose the highly reliable platoon head vehicles. Security analysis is then introduced in Section 4.4,

and the performance evaluation is in Section 4.5. Finally, we give the related work in Section 4.6 and draw conclusions in Section 4.7.

4.2 System Model, Trust Model and Design Goal

In this section, we formalize the system model, trust model and identify our design goals.

4.2.1 System Model

We consider a flourish stage of VANETs where road side units (RSUs) are widely deployed, and each vehicle is equipped with an on board unit (OBU). In particular, the system model of our proposed REPLACE scheme consists of a top trust authority (TA), a server, some stationary road side units (RSUs) and vehicles traveling on the roads equipped with OBUs, as shown in Figure 4.1.

Figure 4.1: System model under consideration

TA: Trust authority plays a significant role in the whole system, which takes charge of registration of the server, all RSUs and vehicles.

Server: In general, the server has a high storing and computational capability

to store the feedback data table, trust table and reputation table for the whole system. Using the data in the tables, the server also calculates the trust scores for user vehicles and reputation scores for platoon head vehicles. Specifically, every time when a potential user vehicle requests to join a platoon, server will respond this request by recommending the most trusted platoon head vehicle.

RSUs: RSUs are connected through wired lines and secured channels to the server and TA, meanwhile, they provide wireless connections to the vehicles. Both the feedbacks of user vehicles and trip information updates of platoon head vehicles will be forwarded through RSUs to TA or server. From this point of view, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, we assume that RSUs are widely deployed along the roads to cover the whole area which ensures that the vehicles are able to update the information timely when driving on the roads. In some areas where RSUs are sparsely deployed, the update of the feedbacks and traveling information of platoon head vehicles are delayed, the accuracy of our proposed REPLACE scheme will be decreased. But in the long run, the scheme is still efficient.

Vehicles: The vehicles can be regarded as a group of highly mobile nodes equipped with OBUs which allow them to communicate with other vehicles or RSUs. Through V-2-I communication, a vehicle updates its own traveling information or uploads feedback scores to the server when passing RSUs. The drivers on the vehicles can choose either to drive individually or to join a platoon. Vehicles can be further divided into three categories as follows:

- *PH Vehicles:* In the system, there are a number of m_k platoon head vehicles who form a set $\mathcal{P} = \{ph_1, ph_2, \dots, ph_{m_k}\}$. The platoon head vehicles take the full control of the whole platoon when driving on the road, they are responsible for the safety, user experience of all platoon user vehicles. More importantly, their behaviors affect the whole road's condition and operation

efficiency. It is easy to imagine that such vital roles in the platoon system can only be played by some qualified vehicles which are driven by experienced and capable drivers.

- *Potential user Vehicles:* Except for the PH vehicles, all the other individually driving vehicles can be regarded as potential user vehicles once they drive on the road until they decide to join a platoon.
- *User Vehicles:* In order to reach the destination in a more comfortable and energy saving way, those potential user vehicles have the option to join a platoon via our proposed REPLACE scheme to be a user vehicle v_j . A total number of m_j user vehicles the road form a set $\mathcal{V}$, where $\mathcal{V} = \{v_1, v_2, \dots, v_{m_j}\}$.

4.2.2 Trust Model

In our trust model, we make some assumptions and define the trust levels of different roles in the system model.

- TA: Trust authority maintains the public and private keys of the network which is fully trusted by all roles in the system.
- Server: We assume that server is under so strong physical protection that it is impossible for any attacker to compromise.
- RSUs: RSUs are subordinated to server via reliable communication channel, it will never disclose any internal information without permissions. However, we do not rule out the possibility that a portion of RSUs at the road side are compromised or the attackers even deploy bogus RSUs. Nevertheless, the TA can inspect all RSUs at high level: once the RSUs are compromised, they will be recovered or revoked in the next time slot by TA.
- PH Vehicles: Although PH vehicles are driven by experienced drivers, it does

not mean that we can trust them equally since their performances vary for different drivers. Even for the same PH vehicle, its performance changes in different periods and different trips. Besides, PH vehicles may also be compromised by adversaries and provide poor platoon service deliberately. However, we assume that the future behaviors of PH vehicles can be expected according to its historical performances.

- **User vehicles:** A user vehicle is required to provide a feedback on the PH vehicle's performance after each trip. However, we cannot directly use their opinions at all times. The reasons are: first, user vehicles have different capabilities of providing feedbacks, even in the same trip, some of them are able to provide more accurate feedbacks than others; second, some of the user vehicles are compromised to make biased feedbacks, with an intention to disrupt the whole system, while others may collude with each other to give untruthful feedbacks for their own benefits.

4.2.3 Design Goals

Different from traditional wireless networks, VANET is heavily involved in human factors; on the other hand, it is affected by human factors. In other words, the behaviors of platoon head vehicles are unpredictable, which makes it hard for potential user vehicles to choose a reliable platoon service when facing multiple platoon head vehicles nearby. To tackle this challenge, three design goals are desirable in the development of our REPLACE scheme. Specifically,

1. **Accurate PH vehicle performance evaluation:** Judging from the platoon service qualities of PH vehicles, there are always relatively badly-behaved PH vehicles on the road. Some of those behaviors may downgrade the user vehicles' experience, others may even put the platoon members in danger. In practice, many reasons lead to the poor performance of PH vehicles, such as

poor driving habits, selfishness or intentional attacks. Sometimes PH vehicles drive carelessly or provide bad service only because of the lack of supervision in the system. In all the above cases, a performance evaluation scheme is expected to either punish the attackers or motivate careless drivers to provide as best service as they can. In addition, to make the results more accurate, the evaluating scores given by user vehicles should be sufficiently fine-grained and smooth.

2. **Reliable platoon service recommendation:** Under such situation where reliable and unreliable vehicles are mixed, the selection of PH vehicle is a significant issue. To help the potential user vehicles avoid badly-behaved vehicles, our scheme should be able to accurately distinguish between well-behaved and badly-behaved PH vehicles so as to recommend the most reliable PH vehicles.

3. **Robustness against malicious user vehicles:** To build the reputation of PH vehicles, the platoon user vehicles are asked to provide the feedbacks about the performance of PH vehicles in a series of trips. However, some malicious user vehicles can intentionally manipulate the feedbacks or collude with each other to provide bogus feedbacks deliberately. Such attacks will eventually subvert the evaluation process of PH vehicles, resulting in the untruthful evaluations on PH vehicles. Other malicious user vehicles may behave well and badly alternatively. After accumulating high trust value, they start doing bad things. Our proposed scheme should be able to filter out those unfair feedbacks and resist against those malicious attacks.

4.3 Proposed REPLACE Scheme

In this section, we propose our REPLACE scheme which consists of five parts: system initialization, quality of feedbacks calculation, Dirichlet-based model, trustworthiness of user vehicles and reputation of PH vehicles. The architecture of our proposed scheme is shown in Figure 4.2.

Figure 4.2: Architecture of REPLACE Scheme

4.3.1 System Initialization

Given the security parameters, TA first generates and publishes its own public key PK_{TA} , the public keys of RSUs and vehicles are their IDs. Before an RSU or a vehicle registers itself to the system, it submits its identity to TA to obtain its private key SK_{RSU} or SK_v .

Let $\mathcal{T}$ be the set of trips with the total number of m_i so that $\mathcal{T} = \{Tr_1, Tr_2, \dots, Tr_{m_i}\}$. After a user vehicle $v_j \in \mathcal{V}$ uses the platoon service provided by a PH vehicle $ph_k \in \mathcal{P}$ in trip $Tr_i \in \mathcal{T}$, it is required to provide a feedback of that trip Tr_i ,

which is denoted by $f_j^i (\in [0, 1])$. This feedback together with the PH vehicle ID ph_k , trip ID Tr_i and trip time t_i will be uploaded to server, where i denotes the sequence number of trips, t_i is the beginning time of Tr_i . We note that since the feedback data keeps being updated, m_i , m_j and m_k increase by time. However, when calculations are conducted, the server collects the data in a time window so that at that time the feedback data table can be regarded as static without any new records coming in.

As shown in the Figure 4.3(a), the server will establish such a feedback data table which stores the feedbacks from all user vehicles in each trip Tr_i . The trips will be arranged in sequence, e.g., $\{Tr_1, Tr_2, \dots, Tr_i, \dots\}$, this table will be updated once a new piece of record is uploaded. Another trust table is also established by the server to record all of the user vehicle identities $v_j \in \mathcal{V}$ and their trust scores T_j ($j = 1, 2, \dots, m_j$), which is shown in Figure 4.3(b). Those trust scores are used to describe the reliability and accuracy of v_j 's feedbacks. We will describe the calculation of these trust scores later, but initially, $T_j = T_0$ ($j = 1, 2, \dots, m_j$). T_0 will not be given a high value to resist against newcomer attack. The reputation scores Rep_k of PH vehicles are also initialized as $Rep_k = Rep_0$.

4.3.2 Quality of Feedbacks

In order to evaluate the quality of user vehicle v_j 's feedback in trip Tr_i , we first calculate the integrated feedback of the trip Tr_i , denoted by TR_i , which could be regarded as a real performance of the PH vehicle in Tr_i by combining all feedbacks about Tr_i together. Then TR_i will be compared to f_j^i , a greater difference leads to a lower quality value of this feedback f_j^i . It is obvious that the accuracy of TR_i determines the accuracy of the quality value on feedback.

However, due to the existence of badmouth or ballot-stuffing attackers in the user vehicles who always give untruthful feedbacks, those feedbacks in the feedback

Trip	User Vehicle	PH Vehicle	Time	Feedback
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Tr_i	v_j	ph_k	t_i	f_j^i
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

(a) Feedback Data Table

User Vehicle ID	Trust Score
$\vdots$	$\vdots$
v_j	T_j
$\vdots$	$\vdots$

(b) User Vehicle Trust Table

PH Vehicle	Trip ID	User Vehicle ID	Feedback
ph_k	$\vdots$	$\vdots$	$\dots$
	Tr_i	$\vdots$	$\dots$
		v_j	f_j^i
		$\vdots$	$\dots$
	$\vdots$	$\vdots$	$\dots$

(c) PH Vehicle Data Table

Figure 4.3: Tables that are established and updated by the server

data table can never be used directly to compute TR_i . Therefore, before calculating the quality values of feedbacks, we develop an iterative filtering algorithm which is able to exclude the feedbacks from attackers. Specifically, we achieve our goals in two steps:

1. *Filtering out untruthful feedbacks:* The relationship between the user vehicles and the trips is depicted in Figure 4.4.

Inspired by the work of [83], in our proposed iterative filtering algorithm, we

Figure 4.4: User vehicles give feedbacks on trips

use the circles and squares to represent the user vehicles and trips respectively. Assume that the feedback graph has m_i trips and m_j user vehicles in total. If a user vehicle v_j gives a feedback on trip Tr_i , we place an arrowed solid line from v_j to Tr_i . At each iteration, the collection of all feedbacks of a trip will be combined to estimate the value of integrated feedback on the trip in that round. Once the values of integrated feedbacks are estimated, in next iteration, those values will be used to determine the quality values of the user vehicles' feedbacks.

Each trip comprises different user vehicles. We use $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{m_i}$ to represent the sets of user vehicles of trip $Tr_1, Tr_2, \dots, Tr_{m_i}$ respectively. The sets will be updated after each iteration because some of the user vehicles will be in blacklist after iteration. We denote ν to be the round number of the iteration. $\mathcal{A}_i^{(\nu)}$ denotes the set of user vehicles of trip Tr_i after the ν^{th} round. In the very beginning, we can easily get $\mathcal{A}_i^{(0)}$, $i \in \{1, 2, \dots, m_i\}$ from the feedback data table. Similarly, for each user vehicle who takes part in different trips, we use $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_{m_j}$ to represent the set of trips that

the user vehicles $v_1, v_2, \dots, v_{m_j}$ take part in. At the ν^{th} round, the iterative algorithm will be executed, we compute the integrated feedback of Tr_i as:

$$TR_i^{(\nu+1)} = \frac{\sum_{v_j \in \mathcal{A}_i^{(\nu)}} T_j \cdot f_j^i}{\sum_{v_j \in \mathcal{A}_i^{(\nu)}} T_j} \quad (4.1)$$

where $\mathcal{A}_i^{(\nu)}$ is the set of all user vehicles in trip Tr_i at the ν^{th} round. T_j represents the trust score of a user vehicles v_j .

Then we compute the inconsistency factor $C_j^{(\nu+1)}$ for each user vehicle v_j using the integrated feedbacks of each trip $TR_i^{(\nu+1)}$. For v_j , since it gives feedbacks to different trips at different times, the time factor should be incorporated as well:

$$C_j^{(\nu+1)} = \frac{\sum_{Tr_i \in \mathcal{B}_j^{(\nu)}} \lambda^{t-t_i} \cdot |f_j^i - TR_i^{(\nu+1)}|}{\sum_{Tr_i \in \mathcal{B}_j^{(\nu)}} \lambda^{t-t_i}} \quad (4.2)$$

where λ and t_i are the fading parameter and the beginning time of the trip Tr_i . After computing the inconsistency factors of all user vehicles, we select those whose inconsistency factors are greater than a specific threshold $C_{threshold}$ and remove them from the $\mathcal{A}_i$ in the next round. The iteration stops when the difference between $TR_i^{(\nu+1)}$ and $TR_i^{(\nu)}$ is smaller than a threshold $TR_{threshold}(\in [0, 1])$.

2. *Quality value calculation of feedbacks:* To measure the quality of feedback quantitatively, we use a function $QVal(\in [0, 1])$ to represent the quality values of feedbacks. For a user vehicle v_j in trip Tr_i , its feedback is given by f_j^i , we assume that the trips's integrated feedback TR_i converges at the ν^{th} round. The quality value of v_j 's feedback f_j^i can be represented as:

$$QVal = 1 - |f_j^i - TR_i^{(\nu)}|^{\nu \cdot c_1} \quad (4.3)$$

Note that ν is the number of rounds to get a convergent integrated feedback, the larger is ν , the more malicious user vehicles exist, the more difficult it

Algorithm 3 Iterative filtering**Input:** Records in the feedback data table**Output:** Trip Tr_i 's integrated feedback TR_i

```

 $\nu \leftarrow 0$ 
 $difference \leftarrow 100$ 
while  $difference \geq TR_{threshold}$  do
  for  $Tr_i \in \mathcal{T}$  do
    calculate  $TR_i^{(\nu+1)}$ 
  end for
  for  $v_j \in \mathcal{A}_i^{(\nu)}$  do
    calculate  $C_j^{(\nu+1)}$ 
  end for
  for  $Tr_i \in \mathcal{T}$  do
    for  $v_j \in \mathcal{A}_i^{(\nu)}$  do
      if  $C_j^{(\nu+1)} > C_{threshold}$  then
        remove  $v_j$  from  $\mathcal{A}_i^{(\nu)}$  to form  $\mathcal{A}_i^{(\nu+1)}$ 
      end if
    end for
  end for
   $difference = TR_j^{(\nu+1)} - TR_j^{(\nu)}$ 
   $\nu = \nu + 1$ 
end while
return  $TR_i^{(\nu+1)}$ 

```

is to give a feedback accurately. Hence ν can be used as an award to the quality value of feedback when there are more malicious user vehicles. c_1 controls the award sensitivity, with larger values representing more awards to the quality values.

4.3.3 Dirichlet-based Model

A Dirichlet distribution is based on initial belief on an unknown event according to prior distribution. It provides a solid mathematical foundation for measuring the uncertainty of feedbacks based on historical data. Compared to Beta distribution which is more appropriate in a binary satisfaction level [42], Dirichlet distribution is more appropriate for multi-valued satisfaction levels [84]. In our case, the evaluation trustworthiness of user vehicles are described by continuous trust values. Therefore, we use Dirichlet distribution to estimate the quality values of user

vehicle' feedbacks in the future and then build our trust model accordingly.

For a specific user vehicle v_j , let X ($0 \leq X \leq 1$) be the continuous random variable denoting the quality value of v_j 's feedback. In order to classify the historical and future quality values, we also denote a number of l satisfaction levels of feedbacks as a set $\{\theta_1, \theta_2, \dots, \theta_l\}$ ($\theta_i \in (0, 1], i \in [1, l], \theta_i < \theta_{i+1}$). Let $\vec{p} = \{p_1, p_2, \dots, p_l\} (\sum_{i=1}^l p_i = 1)$ be the probability distribution vector of X with respect to satisfaction levels, so that we have $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i$ ($i = 1, 2, \dots, l$). To make it more mathematically precise, we define $\theta_0 = 0$ when $i = 1$, $X_i = 0$ is categorized into θ_1 .

Following the steps in Section 4.3.2, the server is able to calculate the quality values of v_j 's historical feedbacks, then we let $\vec{\gamma} = \{\gamma_1, \gamma_2, \dots, \gamma_l\}$ denote the vector of cumulative historical data and initial belief of X . With a posterior Dirichlet distribution, $\vec{p}$ can be modeled as:

$$f(\vec{p}|\xi) = Dir(\vec{p}|\vec{\gamma}) = \frac{\Gamma(\sum_{i=1}^l \gamma_i)}{\prod_{i=1}^l \Gamma(\gamma_i)} \prod_{i=1}^l p_i^{\gamma_i-1} \quad (4.4)$$

where ξ denotes the background information represented by $\vec{\gamma}$. Let: $\gamma_0 = \sum_{i=1}^l \gamma_i$. The expected value of the probability of $X_i \in (\theta_{i-1}, \theta_i]$ with the historical distribution of quality values is given by:

$$E(p_i|\vec{\gamma}) = \frac{\gamma_i}{\gamma_0} \quad (4.5)$$

Consider the time factor of historical quality values, we introduce a forgetting factor β to give a greater weight to more recent quality values:

$$\vec{\gamma}^{(n)} = \begin{cases} \vec{S}^{(0)} & (n = 0) \\ \sum_{i=1}^n \beta^{t-t_i} \vec{S}^{(i)} + c_0 \vec{S}^{(0)} & (n \geq 1) \end{cases} \quad (4.6)$$

where n is the total number of historical quality values; $\vec{S}^{(0)}$ is the initial belief

vector when $n = 0$. Since no prior information is available, all elements of $\vec{S}^{(0)}$ have equal probability which makes $\vec{S}^{(0)} = (\frac{1}{l}, \frac{1}{l}, \dots, \frac{1}{l})$. Parameter $c_0 > 0$ is a weight on the initial beliefs. In the i^{th} trip of v_j ($Tr_i \in \mathcal{B}_j, 1 \leq i \leq n$), $\vec{S}^{(i)}$ denotes the satisfaction level of its quality value, which contains only one element set to 1 corresponding to the selected satisfaction level and all the other $k - 1$ elements set to 0. t_i stands for the beginning time when the i^{th} trip took place and t is the moment of running the algorithm. The forgetting factor is $\beta \in [0, 1]$; from Eq. (6.12), we can easily see that smaller β means that the system is easier to forget the historical records, and vice versa. In order to defend against on-off attack [85], we choose β as an adaptive value:

$$\beta = c_3 \cdot (1 - T_j) \quad (4.7)$$

c_3 is a parameter to control the forgetting factor, the larger value of c_3 makes the system more forgettable about the historical behaviors and vice versa. From the Eq. (4.7) we can see that when v_j has a high trust value, its forgetting factor is small, which means that those good behaviors of giving truthful feedbacks will be easily forgotten. On the contrary, once v_j performs as a malicious attacker, its trust value gets lower and forgetting factor becomes larger. This means that all of those bad behaviors will be memorized and it takes even longer time for v_j to build up a high trust value again.

4.3.4 Trustworthiness of a User Vehicle

For an arbitrary user vehicle v_j , to evaluate its trustworthiness when giving feedbacks, we assign the weight ω_i to each satisfaction level $\theta_i (i \in [1, k])$. Let p_i denote the probability that the quality value of v_j 's feedback is categorized into the satisfaction level of θ_i . $\vec{p} = (p_1, p_2, \dots, p_k) | \sum_{i=1}^k p_i = 1$. We model $\vec{p}$ using equations in Section 4.3.3. Let Y be the random variable denoting the weighted average of

the probability of each satisfaction level in $\vec{p}$, the trust score T_j of v_j is represented as:

$$T_j = E[Y] = \sum_{i=1}^k \omega_i E[p_i] = \frac{1}{\gamma_0} \sum_{i=1}^k \omega_i \gamma_i \quad (4.8)$$

where γ_i is the cumulated evidence that v_j 's feedback's quality value is with a satisfaction level of θ_i . Using the trust scores of user vehicles, the server updates the trust table in Figure 4.3.

4.3.5 Reputation of PH Vehicles

In order to calculate the reputation of a PH vehicle which reflects the opinions from all user vehicles, a feedback table specifically for each PH vehicle is designed. As shown in Figure 4.3(c), for a PH vehicle ph_k in the system, it records all trips of ph_k and the feedbacks from each user vehicle in the corresponding trip. Let $\mathcal{C}_k$ be the set of all trip IDs for ph_k . For a specific trip $Tr_i \in \mathcal{C}_k$, as defined before, $\mathcal{A}_i$ is the set of all user vehicle IDs in that trip.

The reputation of ph_k can be calculated by aggregating all the feedbacks of ph_k 's user vehicles based on the trustworthiness of those user vehicles. Using the weight majority method, ph_k 's reputation score is given by:

$$Rep_k = \frac{\sum_{Tr_i \in \mathcal{C}_k} \sum_{v_j \in \mathcal{A}_i, T_j \geq T_{TH}} \eta^{t-t_i} \cdot T_j \cdot f_j^i}{\sum_{Tr_i \in \mathcal{C}_k} (\sum_{v_j \in \mathcal{A}_i, T_j \geq T_{TH}} \eta^{t-t_i} \cdot T_j)} \quad (4.9)$$

where η is the forgetting factor of the outdated feedbacks in accumulation. To make the aggregated evaluation more accurate, the requesting vehicle applies a threshold $T_{threshold}$ on choosing user vehicles' feedback for ph_k .

4.4 Security Analysis

In this section, we analyze the security properties of our proposed REPLACE scheme. Specifically, some attack strategies will be described followed by the resilience analysis against those attacks:

Resilience to badmouth attack: In the proposed REPLACE scheme, a badmouth attack is meant that a collective of user vehicles always give lower feedback scores to the well performed PH vehicles. In some cases the badmouth user vehicles originate by selfish drivers who attempt to lower the high reputation of well performed PH vehicles with the hope of improving their own chances to be PH vehicles. To prevent those attacks, the proposed REPLACE scheme incorporates an iterative filtering algorithm to find out the untruthful feedback providers and then remove their feedbacks.

Resilience to ballot-stuffing attack: Similar to the badmouth attack, another group of malicious user vehicles may collude to increase the reputation values of PH vehicles with low reputations by always giving them good feedbacks no matter what their performances are. It could be mounted by a group of malicious vehicles to favor their allies. Similar to the badmouth attack, our defense against ballot-stuffing attacks relies on the iterative filtering algorithm to exclude the feedbacks from ballot-stuffing attackers.

Resilience to rough RSU attack: Although all the deployed RSUs are trusted in the system, an adversary could place rogue RSUs along the roads which intentionally drop the feedback data that should be uploaded to the server to degrade the trustworthy environment of VANET. In our proposed REPLACE scheme, V-2-I communication implicitly achieves mutual authentication by establishing a non-interactive session key. If an RSU is a rogue RSU, it cannot successfully generate the session key. Therefore, rogue RSU attack can be countered in the REPLACE scheme.

Resilience to newcomer attack: The newcomer attacks occur when a malicious user vehicles abandon their low trusted old IDs and register new IDs to launch new attacks [86]. This type of attack is mitigated in two ways: on one hand, our proposed scheme assigns low initial trust scores to the new IDs so it requires a longer time for the new user vehicles to accumulate high trust scores; on the other hand, in VANET, the user vehicle ID is connected to the driving license in real world, which makes it harder for a malicious driver to spoof ID easily.

Resilience to on-off attack: User vehicles may behave well and badly alternatively with the hope to hide themselves by building up high trust or reputation scores before launching attacks. Those attackers exploit the forgetting factor of the system to launch attacks. Specifically, user vehicles may give truthful feedbacks at first, in order to accumulate trustworthiness. When their trust scores get high enough, they launch attacks and remain silent thereafter. Since the system forgets about the past behaviors gradually, their trust scores recover slowly and they repeat the steps above. Those attackers are hard to be detected using the traditional method, but we handle this problem by adopting an adaptive forgetting factor in our proposed REPLACE scheme. The method is inspired by a common human nature: it takes long time to build up trust among others and only a few bad behaviors will ruin it. The method is effective in mitigating the on-off attacker in our VANET system.

4.5 Performance Evaluation

We will evaluate the performance of our proposed REPLACE scheme in this section. The numerical data are generated in Matlab. The performance metrics used in the evaluation are: i) trust scores in terms of the round for different user vehicles; ii) reputation scores' variations with round for PH vehicles with different performances; iii) detection rate variations with round of badmouth and ballot-stuffing

attackers. We define “round” as a period when all PH vehicles provide the same number of service to all PM vehicles; when one “round” is finished, in the next “round”, all PH vehicles provide service to another group of PM vehicles compared with the previous one.

4.5.1 Simulation Settings

We design a simulation to evaluate our proposed REPLACE scheme in which only a set of key factors are considered and specified in order to validate the performance of platoon head vehicles and the feedback accuracy of user vehicles. It is worth noting that the selected factors are not related to the movement of vehicles and the packets collision problems. In this case, we simulate the proposed scheme in the environment of MATLAB where there are a total number of m_j user vehicles and m_k PH vehicles. To ensure the fairness, we suggest that each PH vehicle provides n times of service in each round, and in each service the same amount of user vehicles take part in the trip. This assumption is reasonable because in real scenario in the same local area, when a large number of services are provided, a PH vehicle has equal chance to serve other PM vehicles. A total number of N rounds will be run for evaluation.

4.5.2 Modeling the PH Vehicles and User Vehicles

Due to the lack of real data, we need to model the malicious behaviors of not only PH vehicles but also user vehicles in order to test the performance of our system.

- **Performance quality level (PQL) of PH vehicles:** We define a parameter as performance quality level (PQL) $l_{ph} \in [0, 1]$ to describe the capability of a PH vehicle to provide high quality services. A PH vehicle with higher l_{ph} may provide higher quality services. Specifically, given a PH vehicle with

Table 4.1: Simulation Parameter Settings

Notation	Definition	Value
m_j	user vehicle number	100
m_k	PH vehicle number	20
n	service times per vehicle per round	4
N	number of rounds	50, 100
c_0	initial belief weight	1
c_1	award sensitivity	1
c_2	variance sensitivity	10
c_3	forgetting factor parameter	0.5
$C_{threshold}$	inconsistency threshold	0.3
$TR_{threshold}$	stability threshold	0.1
$T_{threshold}$	trust threshold	0.3
T_0	initial trust score	0.5
Rep_0	initial reputation score	0.5
q_{bm}	percentage of badmouth attackers	10%, 40%
q_{bs}	percentage of ballot-stuffing attackers	5%, 20%
l_{ph}	performance quality level	0.8, 0.98
l_v	feedback accuracy level	0.92, 1

l_{ph} , we use the beta distribution to describe the performance quality variable X of that PH vehicle, the probability density function of beta distribution can be expressed as:

$$f(x|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1} (1-x)^{\beta-1} \quad (4.10)$$

where $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx$. $f(x|\alpha, \beta)$ is the probability that a PH vehicle with PQL of l_{ph} provides a service with the quality value of $x \in [0, 1]$. Higher values of l_{ph} imply that the PH vehicle provides a higher quality service. To achieve this goal, we define α and β as follows:

$$\begin{aligned} \alpha &= c_2 \cdot l_{ph} \\ \beta &= c_2 \cdot (1 - l_{ph}) \end{aligned} \quad (4.11)$$

where c_2 is the parameter to control the variance of the distribution: when c_2 is given a larger value, the performance quality values will have a larger

variance and vice versa. For a PH vehicle with PQL of l_{ph} , the above model has the property of generating a service quality score which follows a beta distribution with the expectation $E(X) = l_{ph}$. We assume that all of the PH vehicles are relatively experienced drivers so that we set l_{ph} with the range from 0.8 to 1. If there are malicious PH vehicles, we give lower l_{ph} values to them and the performance of our proposed scheme will be better.

- **Feedback accuracy level (FAL) of user vehicles:** The capability of a user vehicle to give an accurate feedback regarding the performance of a PH vehicle can be determined by another parameter l_v : feedback accuracy level (FAL). Given a performance score of x , the user vehicle with FAL of l_v gives evaluation as follows:

$$eva = x \pm 10\% \cdot x \cdot (1 - l_v) \quad (4.12)$$

From the experience we find that the evaluation errors always exist which could be regarded as random noises added to the real performance score with the mean value of x . As shown in the equation, the errors are controlled by l_v . When there are no attackers, all of those user vehicles are honest, so $l_v \in [0.8, 1]$.

4.5.3 Modeling Attackers in User Vehicles

- **Badmouth/Ballot-stuffing attackers:** In the simulation, the badmouth attackers always evaluate the PH vehicles with the score of “0” while ballot-stuffing attackers give “1” to all PH vehicles. The ratio of badmouth attackers and ballot-stuffing attackers in all user vehicles are q_{bm} and q_{bs} respectively.
- **On-off attackers:** The on-off attackers accumulate a high trust score before they launch the badmouth attacks, at round 20 they turn on until round 40,

later their trust scores recovery to a high level gradually and then they repeat the step above.

4.5.4 Reputation Scores of PH Vehicles

In the first experiment, we study the effectiveness of our proposed REPLACE scheme regarding reputation scores without any attackers. That says, all user vehicles are honest to provide truthful feedbacks though their evaluating abilities vary. We do simulation in the whole system for 50 rounds and track the reputation scores of two different PH vehicles with different performance quality levels. Figure 4.5 shows the reputation changes with round. The PH vehicles with different PQLs are able to be distinguished by our scheme.

Figure 4.5: Reputation scores comparison between PH vehicle with $l_{ph} = 0.8$ and $l_{ph} = 0.92$

4.5.5 Trust Scores of User Vehicles

The goal of this experiment is to compare the trust scores of malicious and honest user vehicles with different feedback accuracy levels. For a better comparison, we choose two honest users with FAL of $l_v = 1$ and $l_v = 0.92$ respectively. Besides, another two attackers who launch badmouth and ballot-stuffing attacks are also put in the system. After “50” rounds, we plot their trust scores in Figure 4.6.

Figure 4.6: Trust scores comparison between honest user vehicles with $l_v = 0.92$, $l_v = 1$ and malicious attackers

We notice that the trust scores of all user vehicles converge after “20” rounds. It is obvious that the honest user vehicles with $l_v = 1$ and $l_v = 0.92$ get the highest trust scores after the experiments. On the contrary, both of the attackers get the low trust scores. We also notice that a user vehicle with a larger FAL will achieve a higher trust score, which shows the effectiveness of our trust model to identify user vehicles according to their actual FALs. Besides, the converged

trust scores of badmouth attacker is a little lower than ballot-stuffing attacker, the reason is that PH vehicles in the system provide service with PQL between 0.8 and 1, so that badmouth attackers who always give “0” to all services will suffer more punishments.

4.5.6 Robustness of Our Proposed Scheme

In this experiment, we study the robustness of our proposed scheme against different types of attackers. One possible threat is the on-off attack when a user

Figure 4.7: Trust score comparison of the same on-off attacker under REPLACE scheme with adaptive forgetting factor and under another scheme with fixed forgetting factor

vehicle is compromised. In this scenario, the compromised vehicle will perform as usual to gain high trust score and then suddenly turn to badmouth vehicle and launches attacks. We simulate this case by putting an on-off attacker in our system, the attacker with an initial trust $T = 0.5$ behaves honestly in the first 20 rounds. After that, it launches badmouth attack for another 20 rounds and then

turns off the attack. Figure 4.7 shows the trust scores of one on-off attacker with a fixed forgetting factor and another with an adaptive forgetting factor which is utilized in our proposed scheme. From the figure, we can find that the system with a fixed forgetting factor is more vulnerable to on-off attackers since the attacker recovers after only 10 rounds once it stops launching attacks. On the contrary, in our proposed scheme, when the attacker builds up high trust score at first, its forgetting factor is a small value, resulting in a steep decrease of its trust score once the attacker starts launching attacks. With the decrease of the trust score, its forgetting factor will increase, which means it remembers more of the previous performance. As a result, the recovery of the attacker's trust score will be very slow. From the figure, we can see that to beat the proposed adaptive forgetting factor with parameter $c_1 = 0.5$, the on-off attacker spends five times of rounds to recover than the fixed forgetting factor. The method is very effective in protecting the system against on-off attackers.

Figure 4.8: Trust scores comparison of a newcomer attacker with different c_0 values

Figure 4.8 shows the robustness of our scheme against newcomer attacks. As

described in Section 4.3.3, c_0 is the constant to control the initial prior feedback quality value. $c_0 = 0$ means no initial values. In this case the newcomer will gain trust very fast and converge soon, and the system will also be vulnerable to newcomer attack. When we give higher initial prior feedback quality value c_0 to the user vehicles in the trust system, it takes a longer time for a newcomer to accumulate a converged trust value. By choosing c_0 properly, the system is able to resist against newcomer attacks without affecting the trust evaluation of the other user vehicles.

Figure 4.9: Resilience to badmouth attacker and ballot-stuffing attack by comparing detection rate between REPLACE scheme with and without iterative filtering algorithm

To demonstrate the robustness of our proposed scheme against badmouth and

ballot-stuffing attacks, we simulate these two cases separately. We define the top 20% of the total number of user vehicles with the highest l_v as “good user vehicles”. After the service, all user vehicles will be re-ranked, then the detection rate can be defined as the ratio of “good user vehicles” who still remain top 20% in the new ranking list.

We set the percentage of badmouth attackers q_{bm} in the system as 10% and 40% respectively, the results are shown in Figure 4.9(a) and 4.9(b). From the figures, we can find that the scheme with the iterative filtering (IF) algorithm performs better than the system without the IF algorithm. The detection rate reaches 90% even when the badmouth ratio is 10%. Similarly, in Figure 4.9(c) and Figure 4.9(d), our system still performs better given that the ballot-stuffing ratio q_{bs} are 5% and 20%. Comparing the two experiments, we may find that our system is more tolerable against badmouth attack than ballot-stuffing attack. This finding can be explained as follows: the PH vehicle always provides services with high qualities, hence the strategy of badmouth attacker is more easily exposed. In a word, the experiments show that our scheme is very robust against both badmouth and ballot-stuffing attacks.

4.6 Related Work

Platoon-based driving pattern attracts much attention due to its potential to improve the road capacity and energy efficiency [87]. Among all of issues in platooning technique, how to manage the platooning system has always been an urgent topic [63].

However, none of the platoon management models solve the problem of reliable PH vehicle selection. To solve the problem of reliable PH vehicle selection and then help user vehicles avoid badly-behaved PH vehicles, a possible solution could be evaluating the trustworthiness of the PH and user vehicles. Trust and

reputation models in VANET have been studied by many researchers [88, 31, 89]. Patwardhan et al. [88] present a distributed reputation management scheme for VANET, which enables vehicles to quickly adapt to changing local conditions and provides a bootstrapping method for establishing trust relationships. However, the lack of scalability and robustness makes it hard to be applied in the platoon scenario. Different from traditional entity-based trust model, Raya et al. [31] suggest a data-oriented trust establishment framework. By combining trust values of each piece of data together, their framework deals well with ephemerality and functions well in sparse areas. However, in the platoon scenario, the large amount of feedback data makes their framework less efficient. Chen et al. [89] propose a trust-based message propagation and evaluation framework in VANET, however, the lack of robustness is its weakness.

Combining the above platoon management models and trust models together, our proposed REPLACE scheme is focused on evaluating the platoon head vehicles based on their performances. Specifically, there are several aspects which make our proposed scheme different: first, we establish a reputation system as a long-term evaluation metric of evaluation. Second, a recommendation scheme is developed to solve the problem of distrust on unknown platoon head vehicles. Third, our proposed scheme is resistable against several sophisticated attacks for reputation systems, such as badmouth attacks, newcomer attacks and on-off attacks.

4.7 Summary

In this chapter, we have proposed a recommendation scheme for user vehicles to select platoon head vehicle before joining a platoon. Considering the uncertainties of human behaviors, the scheme is reputation-based using the weighted majority method by adding up all of the historical feedbacks from the user vehicles together. It is well perceived that the feedbacks from the user vehicles could also be untrusted.

Concretely, we establish a trust system to evaluate the reliability of user vehicles by adapting the Dirichlet density function to deal with the uncertainties of user vehicles' feedbacks and then to estimate their future behaviors. Furthermore, the iterative filtering algorithm is incorporated to resist against badmouth and ballot-stuffing attacks, and the adaptive forgetting factor protects the system against on-off attacks. The main results of this chapter demonstrated that the scheme is effective in distinguishing platoon head vehicles even when their performances have slight differences. Our simulations also suggest that the proposed REPLACE scheme is robust against different types of attackers. In the future work, we will target on preserving the privacy of feedback data and trust data that are stored and computed in the server.

Chapter 5

Privacy-Preserving Trust-based Relay Selection Scheme

In the previous chapter, we presented a reliable trust-based platoon service recommendation scheme, which is called REPLACE, to help the user vehicles avoid choosing badly behaved platoon head vehicles. However, the location privacy of the vehicles is not preserved though it is of great significance. In this chapter, we will focus on how to protect candidate relay vehicle's location privacy in relay selection application [38] in VANET.

5.1 Introduction

Significant efforts have been made recently for enabling safety, traffic management, and commercial applications in VANET [1]. Envisioned as one of the most promising approaches to implement intelligent transportation systems (ITS), VANET has the potential to enhance road safety and reduce traffic congestion due to its hybrid infrastructure [90, 82, 37]. This hybrid infrastructure includes road side units (RSUs) deployed along the roads and on board units (OBUs) equipped in mobile vehicles, which enables not only vehicle-to-vehicle (V-2-V) but also vehicle-

to-infrastructure (V-2-I) communications.

Due to the high cost of RSUs, they can only be deployed in some of the downtown areas where many vehicles pass by. We consider a scenario when a vehicle is traveling in a rural area and no RSUs are deployed nearby, and this vehicle would like to send an urgent message to RSU by asking other vehicles nearby to relay the message. However, vehicles are not always reliable when relaying messages. For example, they may relay the messages after a long delay or even drop the messages, leading to low relay ratio. The problem can be settled by incorporating trust which allows each vehicle to detect malicious relay vehicles who drop messages deliberately, and to give incentives to encourage reliable vehicles [3].

Meanwhile, location privacy has always been a concern in VANET since the locations of the vehicles are actually the locations of drivers [91]. To achieve location privacy, a very popular approach in VANET is that vehicles periodically change their pseudonyms when broadcasting messages [1, 92, 14], since the pseudonyms make the location information in a period unlinkable to a specific vehicle. However, pseudonyms do not always ensure privacy, as an example shown in Figure 5.1, a requesting vehicle (the red vehicle) is asking another vehicle for relaying its message among a few candidate vehicles nearby. At time t , two candidate vehicles V_i and V_j respond to the requesting vehicle by sending their own pseudonyms together with their reputation scores, then after a short while at time $t + \Delta t$, their pseudonyms are changed from PID_A and PID_C to PID_B and PID_D respectively, the requesting vehicle can still link V_i and V_j by associating their reputation scores even though their pseudonyms have been changed. Because the reputation update interval is long enough so that in the period before update, the reputation score of a vehicle can be regarded as unchanged. Hence, candidate vehicles' location privacy are exposed. Therefore, it is compelling for us to build a trust system through which vehicles take its advantages without sacrificing their privacies.

In this chapter, to facilitate vehicles to improve relay ratio while achieving lo-

Figure 5.1: Reputation scores are associated despite the change of pseudonyms

cation privacy, we propose a privacy-preserving trust-based relay selection scheme, called PTRS. This scheme can help a vehicle to efficiently detect the malicious or selfish vehicles who drop packets deliberately by establishing a trust model to measure the reliability of a vehicle when relaying a message. Meanwhile, the proposed scheme is characterized by its ability to preserve the location privacy of vehicles. Specifically, our work features the follows:

- First, our designed scheme takes advantages of the already-existing centralized infrastructure in VANET by considering its unique characteristics: high mobility, hybrid infrastructure and ephemeral link. It allows us to design a secure and efficient relay selection scheme.
- Second, we build a trust-based relay selection scheme through which a requesting vehicle is able to quickly decide whether a candidate vehicle is reliable to relay a message by verifying whether its trust level meets a threshold which is set by this requesting vehicle. This trust level reflects the extent to which a candidate vehicle has been a successful relay in the past. It also reflects the likelihood that it will relay a message successfully in the future.

- Finally, we design a request-response scheme using pseudonyms combined with trust-based system that allows a requesting vehicle to authenticate the candidate vehicle anonymously, and then judge whether this candidate vehicle's reputation score satisfies its requirement without knowing the exact reputation score. In this way, the candidate vehicle's reputation score is concealed and its location privacy is preserved in the process of reputation score sharing. Besides, to deal with the cheating behavior of candidate vehicles in sharing their reputation scores, the TA is able to check whether a candidate vehicle cheats the requesting vehicle by submitting an exaggerated reputation score afterwards. The candidate vehicle will be punished once their cheating behavior is detected. .

The remainder of this chapter is organized as follows. In Section 5.2, we formalize the system model, trust model and threat model considered in our work, and identify our design goals. In Section 5.3, the PTRS scheme is presented in details, together with the rationale how it can help the requesting vehicles to choose a highly reliable relay vehicle without knowing its reputation score. Security analysis is then presented in Section 5.4, and the performance analysis is given in Section 5.5. Finally, we present the related work in Section 5.6 and draw conclusions in Section 5.7.

5.2 Problem Statement

In this section, we define the problem by formalizing the system model, threat model and design goal.

Figure 5.2: System model under consideration

5.2.1 System Model

The system model is illustrated in Figure 5.2.1, which consists of three roles: the top TA (trust authority), the immobile RSUs (road side units) at the road side and the mobile vehicles equipped with OBUs (on board units). Specifically, we consider a scenario when a vehicle wants to transmit a packet to the destination in VANET without the existence of RSUs, which is common in rural areas or highways.

TA: TA takes charge of the registration of all RSUs and the vehicles, which also maintains the evaluation records and trust values of all vehicles in the system model. TA is assumed to have sufficient computation and storage capability.

RSUs: The RSUs are subordinated by the TA, which are connected to the TA through wired lines and secured channels. Equipped with wireless devices, RSUs are able to exchange data with the passing-by vehicles. However, due to the high cost of RSU installment and maintenance, especially in the early stage of VANET, no RSUs are deployed at the crossroads where traffic flow is small.

Vehicles: The vehicles can be regarded as a group of highly mobile nodes equipped with OBUs which allow them to communicate with other vehicles or with

RSUs. Through V-2-I communication, a vehicle retrieves the updates of its own trust levels or uploads feedbacks to the server when passing by RSUs. Through V-2-V communication, a vehicle broadcasts the relay requirement to nearby vehicles and transmits the messages to a chosen relay vehicle. In this case, the vehicles can be further divided into two categories:

- *Requesting Vehicle*: After authentication in the system through TA, any authorized vehicle can be a requesting vehicle whenever it wants to relay a message through the nearby vehicles to a specific destination.
- *Candidate Vehicle*: A candidate vehicle is the vehicle within the transmission range of the requesting vehicle, whenever a requesting vehicle broadcasts its relaying request, the candidate vehicle will firstly respond if it is interested to relay the message. This response message includes the candidate vehicle's pseudo identity and reputation score. Later, the requesting vehicle will decide which candidate vehicle to chose as a relay vehicle according to its reputation score.

5.2.2 Trust Model

In our trust model, we make some assumptions and define the trust levels of different roles in the system model, besides, we also define the attack models

- *TA*: Trust authority maintains the public keys, private keys and trust records of the network, we assume that it is fully trusted by all roles in the system since it is under strong physical protection.
- *RSUs*: RSUs are subordinated to server via reliable communication channel, it will never disclose any internal information without permissions. However, we do not rule out the possibility that a portion of RSUs at the road side are compromised or the attackers even deploy bogus RSUs. Nevertheless,

the TA can inspect all RSUs at high level: once the RSUs are compromised, they will be recovered or revoked in the next time slot by TA.

- *Requesting Vehicles:* We assume that the requesting vehicles are honest but curious about the privacy of the candidate vehicles. Besides, they are also honest when evaluate the relay vehicles who have accomplished their tasks.
- *Candidate Vehicles:* The candidate vehicles are driven by human, which means that the behaviors of vehicles are actually the behaviors of human beings. As a result, some of the vehicles will be selfish when asked to relay a message due to their limited storage space and energy. To make things worse, a small fraction of vehicles may even be compromised by the adversaries who drop the packets deliberately when they promise to relay the message. Because of those selfish or malicious behaviors, the relay ratio of the system will decrease greatly.

5.2.3 Threat Model

Specifically, we consider the adversary can launch the following types of attacks to either invade the privacy of vehicles or degrade the message relay efficiency of the whole VANET.

- *Impersonation attack:* The adversary impersonates a candidate vehicle to ask for relaying the message. However, this candidate vehicle may not be qualified in the system. Once chosen as relays, these unqualified vehicles may drop the messages intentionally.
- *Packets dropping attack:* The adversary is able to control a small fraction of the vehicles in the system who ask for taking the responsibility to relay the messages and then drop the packets deliberately.

- *Packets analysis attack:* The adversary eavesdrops the transmission of a message and tries to analyze the message.
- *Reputation link attack:* We assume that the requesting vehicles are honest but curious. If the reputation score of a candidate vehicle is directly given to the requesting vehicle, the location privacy and traveling path and of this candidate vehicle will be exposed since the requesting vehicle can still derive that it belongs to the same vehicle from the same reputation score collected in different locations even though the pseudo-id has changed.

5.2.4 Design Goal

Based on the given models, our goal is to design a trust-based relay selection scheme in VANET which is effective in distinguishing the malicious or selfish vehicles who drop relay messages deliberately, and finally improve the relay ratio. At the same time, the proposed scheme preserves the location privacy of the vehicles. Specifically, the following objectives need to be achieved:

- *The relay ratio improvement:* In the VANET, vehicles are selfish, they could firstly promise to relay a message but then drop it in order to save energy and communication cost. Besides, another possible case is that when a vehicle requests to relay a message, no vehicle responds even they are able to relay the message. In addition, packets dropping attacks exist due to malicious vehicles controlled by adversary. With the existence of those vehicles, if a requesting vehicle chooses a relay vehicle randomly from candidate vehicles, the relay ratio may be low, finally leading to the failure of the system. Therefore, the proposed scheme should be able to improve the message relay ratio of the system by helping the requesting vehicle choose a more reliable candidate vehicle as a relay as well as defending against the aforementioned attacks.

- *Achieving the location privacy preservation:* The location privacy of a vehicle is very sensitive since it is closely related to the location its driver. For example, if the adversary is able to track the location of a vehicle, it may probably infer that the driver is not at home. More serious results will be caused when the adversary studies the path of a vehicle and learns the living pattern of that driver. The scheme should be able to resist against privacy-related attack and preserve the location privacy of vehicles.
- *Anonymous authentication to participant vehicles:* As introduced before, the impersonation attack decreases the relay ratio in the system. To tackle this problem without disclosing the privacy of vehicles, the scheme employs an anonymous authentication mechanism to resist against impersonation attack and ensure that the participant vehicles are all qualified.

5.3 Proposed PTRS Scheme

In this section, we propose PTRS scheme, a privacy-preserving trust-based relay selection scheme in VANET, which is mainly comprised of four phases: system initialization, privacy-preserving relay selection protocol, performance report and trust management.

5.3.1 Initialization

The trust authority (TA) takes charge of bootstrapping the whole system and generating the public and private keys for vehicles and road side units (RSUs). Specifically, the bootstrapping steps are executed as follows:

- Given a security parameter κ , the TA firstly generates the bilinear parameters $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{Gen}(\kappa)$. Then TA chooses a random number

$p \in \mathbb{Z}_q^*$ as its master key. In addition, TA chooses a secure symmetric encryption algorithm $E(\cdot)$, such as AES encryption and a secure asymmetric encryption algorithm $Enc(\cdot)$, such as ElGamal encryption. After that, the system parameters will be published, including $(q, g, \mathbb{G}, \mathbb{G}_T, e)$.

- Afterwards, when a vehicle $v_i \in \mathcal{V} = \{v_1, v_2, \dots, v_n\}$ with real identity ID_i wants to register itself in the system, TA generates a set of m pseudonyms and their corresponding public and secret key pairs in this way:

1. TA randomly chooses a set of m numbers $\{x_{i1}, x_{i2}, \dots, x_{im} \in \mathbb{Z}_q^*\}$ as the secret keys of m pseudonyms. To compute their corresponding public keys, TA chooses a set of random values $\{s_{i1}, s_{i2}, \dots, s_{im} \in \mathbb{Z}_q^*\}$, and computes certificates $\theta_{i1} = e(g, g)^{p^2 \cdot s_{i1}^2}, \theta_{i2} = e(g, g)^{p^2 \cdot s_{i2}^2}, \dots, \theta_{im} = e(g, g)^{p^2 \cdot s_{im}^2}$, then computes $y_{i1} = \theta_{i1}^{x_{i1}}, y_{i2} = \theta_{i2}^{x_{i2}}, \dots, y_{im} = \theta_{im}^{x_{im}}$. For any pseudo-id PID_{i1} with a secret key x_{i1} , its public key comprises two parts: $\theta_{i1} = e(g, g)^{p^2 \cdot s_{i1}^2}$ and $y_{i1} = \theta_{i1}^{x_{i1}}$.

2. TA chooses a symmetric key k_0 and the secure symmetric encryption algorithm $E_{k_0}()$ with the secret key k_0 to compute the set of m pseudo-id for v_i : $\{PID_{i1} = E_{k_0}(ID_i || x_{i1}), PID_{i2} = E_{k_0}(ID_i || x_{i2}), \dots, PID_{im} = E_{k_0}(ID_i || x_{im})\}$. Then TA assigns the whole set of pseudo-ids and their corresponding public and secret key pairs to v_i . Besides, TA also passes a set of specific certificates $\{g^{p \cdot s_{i1}}, g^{p \cdot s_{i2}}, \dots, g^{p \cdot s_{im}}\}$ corresponding to the set of pseudo-ids to v_i .

- In addition, for each vehicle $v_i \in \mathcal{V}$, TA assigns an initial reputation score $R_i = R_0$ and an initial trust level $T_i = T_0$ to it.

5.3.2 Privacy-preserving Relay Selection Protocol

In order to achieve the relay selection without revealing the vehicles' privacy, the scheme uses pseudo-ids and trust level instead of real IDs and accurate reputation scores. To be specific, a requesting vehicle v_B would like to choose a relay vehicle from the nearby candidate vehicles. If there is a candidate vehicle v_A with pseudo-id PID_A , trust level T_A and private-public key pair $(x_A; \theta_A = e(g, g)^{p^2 \cdot s_A^2}, y_A = \theta_A^{x_A})$ who wants to relay the message, it follows the request-response protocol shown in Figure 5.3.

Figure 5.3: Privacy-preserving relay selection protocol

Step 1: Before relaying a message, the candidate vehicle v_A firstly needs to verify itself for v_B to show that it is an authorized vehicle by TA. Therefore, v_A chooses a random number $r \in \mathbb{Z}_q^*$ and uses current time stamp t and the certificate $g^{p \cdot s_A}$, which is awarded by TA, to compute $C_1 = g^{p \cdot r \cdot (H(t) + x_A) \cdot s_A} \in \mathbb{G}$ and $C_2 = g^{p \cdot r^{-1} \cdot s_A} \in \mathbb{G}$ and sends **req1** := $\{C_1; C_2\}$.

Step 2: After receiving **req1** := $\{C_1; C_2\}$, v_B verifies the eligibility of v_A by checking the equation $e(C_1, C_2) \stackrel{?}{=} \theta_A^{H(t)} \cdot y_A$, where t is the current time and y_A is public key of vehicle v_A . If it holds, v_B responds to v_A in the next step. Otherwise, v_B neglects v_A 's request.

Step 3: Once v_B verifies that v_A is authorized, it responds to v_A by checking whether v_A 's trust level matches v_B 's requirement. Specifically, v_B chooses a threshold T_1 as its requirement. Since the trust level is a set of discrete values, any trust level which is no smaller than T_1 could be included in the vector: $(T_1, T_2, \dots, T_n)$. By checking whether v_A 's trust level is in this vector, v_B is able to see whether v_A meets its requirement even without knowing v_A 's trust level. To achieve this, v_B chooses a random value $r_0 \in \mathbb{Z}_q^*$, a random variable $y \in \mathbb{Z}_q^*$ and conducts the computation:

$$\begin{aligned}
& f(y) \\
&= \prod_{i=1}^n (y - T_i) + r_0 \\
&= y^n + \sum_{i=1}^n (-T_i) y^{n-1} + \dots + (-1)^n \prod_{i=1}^n T_i + r_0 \\
&= a_n \cdot y^n + a_{n-1} \cdot y^{n-1} + \dots + a_1 \cdot y + a_0
\end{aligned} \tag{5.1}$$

Then v_B sends **res1** := $\{(g^{a_0}, g^{a_1}, g^{a_2}, \dots, g^{a_n}); T_1\}$ back to v_A .

Step 4: v_A checks whether its own trust level T_A satisfies the threshold T_1 provided by v_B , if $T_A \geq T_1$, v_A computes $C = \prod_{i=0}^n (g^{a_i})^{T_A^i}$ and sends **req2** := C to

v_B to ask for relaying the message.

Step 5: Upon receiving **req2**:= C , v_B checks the relation $C \stackrel{?}{=} g^{r_0}$. If it holds, v_B accepts the request from v_A and responds to v_A in the next step.

Step 6: To ensure the confidentiality and integrity of the relayed message m , v_B encrypts it using the symmetric encryption algorithm $E()$ and a randomly chosen symmetric key k_r to form $E_{k_r}(m)$, and attaches its signature $\sigma_B = Enc_{x_B}(m)$. The symmetric key k_r is encrypted with the receiver's public key y_r to form $Enc_{y_r}(k_r)$ and combined in the message. Besides, the destination location L and a deadline t_0 are also attached, if v_B relays the message to the receiver in destination location within t_0 , the relay is successful; otherwise it fails. Hence v_B responds **res2**:= M where $M = (E_{k_r}(m) || Enc_{y_r}(k_r) || \sigma_B || t_0 || L)$.

Correctness Analysis: Due to the bilinear paring property, the equation will hold on the following relations:

$$\begin{aligned}
& e(C_1, C_2) \\
&= e(g^{p \cdot r \cdot (H(t) + x_A) \cdot s_A}, g^{p \cdot r^{-1} \cdot s_A}) \\
&= e(g, g)^{p^2 \cdot s_A^2 \cdot (H(t) + x_A)} \\
&= [e(g, g)^{p^2 \cdot s_A^2}]^{H(t)} \cdot [e(g, g)^{p^2 \cdot s_A^2}]^{x_A} \\
&= \theta_A^{H(t)} \cdot y_A
\end{aligned} \tag{5.2}$$

$$\begin{aligned}
C &= \prod_{i=0}^n (g^{a_i})^{T_A^i} \\
&= g^{a_n \cdot y^n + a_{n-1} \cdot y^{n-1} + \dots + a_1 \cdot y + a_0} \\
&= g^{(T_A)^n + \sum_{i=1}^n (-1) \cdot T_i \cdot (T_A)^{n-1} \dots + (-1)^n \prod_{i=1}^n T_i} \\
&= g^{\prod_{i=1}^n (T_A - T_i) + r_0}
\end{aligned} \tag{5.3}$$

For any T_i , if $T_A = T_i (i = 1, 2, \dots, n)$, then $C = g^{r_0}$.

5.3.3 Performance Report

When v_A is selected as a relay vehicle, it manages to relay the message as quickly as possible. Once the message is successfully relayed to the destination, the requesting vehicle v_B will be notified immediately. Then v_B gives a report regarding the performance of v_A at this time. Once v_B passes by an RSU, it uploads this report about this task by submitting $(PID_A || T_1 || f)$ to TA, where $f \in [0, 1]$ is the feedback score to evaluate how successful the relay is by considering factors like the delay and distance. If the relay fails, $f = 0$.

5.3.4 Trust Management

In this section, we will first introduce how the feedbacks of vehicles are verified and then how the reputation scores are computed based on those feedbacks; later we describe how to convert reputation scores to trust levels and how to update trust levels.

Feedback Verification

Upon receiving a performance report $(PID_A || T_1 || f)$ in 5.3.3, TA will perform the following procedure to verify the feedback score f :

- (a) TA searches for the real ID of v_A from PID_A and finds its corresponding trust level T_A .
- (b) TA compares T_A with the threshold T_1 chosen by v_B , if $T_A \geq T_1$, the submitted feedback score f is accepted; otherwise $f = 0$.

In our proposed scheme, for simplicity, we assume that f is accurate and can be trusted. However, feedbacks from requesting vehicles may not always be accurate though they are authenticated. Those requesting vehicles may launch badmouth attacks by giving untruthful feedbacks deliberately. In this case, we can establish a trust system for requesting vehicles when they give feedbacks and use methods like iterative filtering to exclude their untruthful feedbacks [37]. However, in this chapter, we do not consider this issue as it is not the main focus of our work.

Feedback Aggregation

A Dirichlet distribution is based on initial belief on an unknown event according to prior distribution. It provides a solid mathematical foundation for measuring the uncertainty of feedbacks based on historical data. Compared to Beta distribution which is more appropriate in a binary satisfaction level [42], Dirichlet distribution is more appropriate for multi-valued satisfaction levels [84]. In our case, the evaluation trustworthiness of user vehicles are described by continuous trust values. Therefore, we use Dirichlet distribution to estimate the performance of candidate vehicles in the future and then build our trust model accordingly.

For a specific candidate vehicle v_A , let X ($0 \leq X \leq 1$) be the continuous random variable denoting the feedback score of v_A 's performance. In order to classify the historical and future feedback scores, we also denote a number of l satisfaction levels of feedbacks as a set $\{\theta_1, \theta_2, \dots, \theta_l\}$ ($\theta_i \in (0, 1], i \in [1, l], \theta_i < \theta_{i+1}$). Let $\vec{p} = \{p_1, p_2, \dots, p_l\}$ ($\sum_{i=1}^l p_i = 1$) be the probability distribution vector of X with respect to satisfaction levels, so that we have $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i$ ($i = 1, 2, \dots, l$). To make it more mathematically precise, we define $\theta_0 = 0$ when $i = 1$, $X_i = 0$ is categorized into θ_1 .

As described in Section 5.3.3, once v_A finishes many tasks, the TA is able to collect v_A 's historical feedback scores from its performance reports, then we let

$\vec{\gamma} = \{\gamma_1, \gamma_2, \dots, \gamma_l\}$ denote the vector of cumulative feedback score and initial belief of X . With a posterior Dirichlet distribution, $\vec{p}$ can be modeled as:

$$f(\vec{p}|\xi) = Dir(\vec{p}|\vec{\gamma}) = \frac{\Gamma(\sum_{i=1}^l \gamma_i)}{\prod_{i=1}^l \Gamma(\gamma_i)} \prod_{i=1}^l p_i^{\gamma_i-1} \quad (5.4)$$

where ξ denotes the background information represented by $\vec{\gamma}$. Let: $\gamma_0 = \sum_{i=1}^l \gamma_i$. The expected value of the probability of $X_i \in (\theta_{i-1}, \theta_i]$ with the historical distribution of feedback scores is given by:

$$E(p_i|\vec{\gamma}) = \frac{\gamma_i}{\gamma_0} \quad (5.5)$$

Consider the time factor of historical feedback scores, we introduce a forgetting factor β to give greater weight to more recent feedback scores:

$$\vec{\gamma}^{(n)} = \begin{cases} \vec{S}^{(0)} & (n = 0) \\ \sum_{i=1}^n \beta^{t-t_i} \vec{S}^{(i)} + c_0 \vec{S}^{(0)} & (n \geq 1) \end{cases} \quad (5.6)$$

where n is the total number of historical feedback scores, $\vec{S}^{(0)}$ is the initial belief vector when $n = 0$. Since no prior information is available, all elements of $\vec{S}^{(0)}$ have equal probability which makes $\vec{S}^{(0)} = (\frac{1}{l}, \frac{1}{l}, \dots, \frac{1}{l})$. Parameter $c_0 > 0$ is a weight on the initial beliefs. In the i^{th} task of v_A ($i \in [1, n]$), $\vec{S}^{(i)}$ denotes the satisfaction level of its feedback score, which contains only one element set to 1 corresponding to the selected satisfaction level and all the other $l - 1$ elements set to 0. t_i stands for the time when the i^{th} task took place and t is the moment of running the algorithm. The forgetting factor is $\beta \in [0, 1]$, a smaller β means that the system is easier to forget the historical records and vice versa. In order to defend against on-off attack [85], we choose an adaptive value as β :

$$\beta = c_0 \cdot (1 - R_A) \quad (5.7)$$

c_0 is a parameter to control the forgetting factor, the larger value of c_0 makes the system more forgetful about the historical behaviors and vice versa. From the equation we can see that when v_A has a high reputation score, its forgetting factor is small, which means that those good performances will be easily forgotten. On the contrary, once v_A provides a low quality relay or drops the packet, its reputation score gets lower and forgetting factor becomes larger. This means that all of those poor performances will be memorized and it takes an even longer time for v_A to build up a high reputation score again.

Reputation Score of a Candidate Vehicle

For an arbitrary candidate vehicle v_A , to evaluate its trustworthiness when serving as relay vehicle, we assign the weight ω_i to each satisfaction level θ_i ($i \in [1, l]$). Let p_i denote the probability that v_A 's feedback score is categorized into the satisfaction level of θ_i . $\vec{p} = (p_1, p_2, \dots, p_l) | \sum_{i=1}^l p_i = 1$. We model $\vec{p}$ using Eq. (5.4), Eq. (5.5) and Eq. (5.6). Let Y be the random variable denoting the weighted average of the probability of each feedback score in $\vec{p}$, the reputation score R_A of v_A is represented as:

$$R_A = E[Y] = \sum_{i=1}^l \omega_i E[p_i] = \frac{1}{\gamma_0} \sum_{i=1}^l \omega_i \gamma_i \quad (5.8)$$

where γ_i is the cumulated evidence that v_A 's feedback score is with satisfaction level of θ_i .

Trust Level of a Candidate Vehicle

As explained in Section 5.1, the system will suffer from reputation link attack if vehicles use the reputation scores directly in the vehicular communications. In the PTRS scheme, a discrete trust level is used instead of accurate reputation score, in this section, we describe how to convert reputation score to trust level: first, TA chooses the total number of trust levels, m . Then, for a candidate vehicle v_A with

reputation score of R_A , its trust level T_A can be easily calculated as: $T_A = i$, for $(i - 1)/m < R_A \leq i/m$, where integer $i \in [1, m]$.

Trust Update

The trust update frequency is decided by TA, when there are more tasks in the system, TA will ask the vehicles to update their trust levels more frequently, and vice versa. When vehicle v_A drives into the wireless range of an RSU, it retrieves its own updated trust level T_A from TA via RSU. v_A uses it in task request, as shown in Section 5.3.2, before the next update.

5.4 Security Analysis

In this section, we analyze the security properties of the PTRS scheme. Specifically, some attack strategies will be described followed by the resilience analysis against those attacks:

5.4.1 Resilience to Reputation Link Attack

We consider the honest but curious requesting vehicles who know the reputation score of a candidate vehicle. Although pseudo-id makes the candidate vehicle anonymous, and the different locations of a candidate vehicle are unlinkable once it changes its pseudo-id. There still exists a risk that a candidate vehicle can be linked by a requesting vehicle according to its reputation score given that the reputation score remains unchanged in a long period. Clearly, in this case, the location information is disclosed and the candidate vehicle could be tracked. In the PTRS scheme, when requesting vehicle v_B wants to know whether a candidate vehicle v_A 's reputation score satisfies its requirement, it does not ask for reputation score directly. Instead, it provides the reputation score requirement to v_B and let v_B

compute $C = \prod_{i=0}^n (g^{a_i})^{T_A^i}$. Then, by checking $C \stackrel{?}{=} g^{r_0}$, v_B is able to know whether v_A meets its reputation requirement even without knowing the exact reputation score of v_A . In addition, r is randomly chosen from $\mathbb{Z}_q^*$, $C_1 = g^{p \cdot r \cdot (H(t) + x_A) \cdot s_A}$ and $C_2 = g^{p \cdot r^{-1} \cdot s_A}$ are unlinkable.

5.4.2 Resilience to Packets Dropping Attack

Due to the existence of feedback scheme, the selfish or malicious vehicles who drop packets when relaying messages will get negative feedbacks, if they keep behaving in that way, those negative feedbacks will accumulate and finally lead to a low trust score and trust level. Thus, it will be less likely for them to be chosen to relay messages in the future since they will hardly meet the trust level requirement by a requesting vehicle. In this way, those reliable vehicles who seldom drop packets will be chosen to relay the messages, thus the scheme is resistable against packet dropping attack.

5.4.3 Resilience to Packets Analysis Attack

In the PTRS scheme, the requesting vehicle v_B has encrypted the message m into $M = (E_{k_r}(m) || Enc_{y_r}(k_r) || \sigma_B || t_0 || L)$. Without knowing the receiver's secret key x_r , the adversary is unable to recover m from the packet analysis. In addition, because the pseudo-id is used in the scheme, no identity information will be disclosed. Therefore, the PTRS scheme is resistant against packet analysis attack.

5.4.4 Resilience to Fake Reputation Attack

In Section 5.3.2 *step 4*, v_A integrates its own trust level T_A into C . However, a small fraction of vehicles controlled by the adversary may cheat by using T_A' . In this case, our proposed scheme is still efficient in tracking those dishonest vehicles and punish

them. The inspection is executed by TA; when a performance report is submitted, as shown in Section 5.3.4, TA firstly finds the real ID of the relay vehicle v_A from its pseudo-id PID_A , then retrieves the trust level T_A and compares it with the threshold T_1 . If $T_A < T_1$, which means that v_A launches a fake reputation attack by using an untruthful trust level in task request, TA will punish v_A by recording this task as an unsuccessful relay no matter how successful this relay is.

5.5 Performance Evaluation

In this section, we study the performance of PTRS scheme using a custom simulator built in Java. The performance metrics used in our proposed scheme are: *message delivery ratio* defined as the ratio of messages successfully relayed to the destination with respect to total number of messages generated by vehicles in a period, and *detection ratio* defined as the ratio of the number of detected malicious vehicles with respect to the total number of malicious vehicles in a specific time period.

5.5.1 Simulation Setup

To simulate the vehicular network, an area of $10km \times 10km$ is created with roads that are equally laid with distance of $2km$ in between. Later, one RSU with transmission radius of $1000m$ is deployed at an intersection of the map denoting the urban area. Finally, a total number of N vehicles with transmission radius of 300 meters are deployed, as shown in Figure 5.4. We also choose $m = 10$ as the total number of trust levels, and let all vehicles choose relay vehicles using the trust level threshold L .

Mobility model. Since vehicles are driven along the roads, we can model the mobility of the vehicles in this way: vehicles firstly randomly choose a destination and then follow the shortest path map based movement [60] at a constant speed of

Figure 5.4: Map for simulation

36km/h. After reaching the destination, they stop for 5 minutes, and then choose a new random destination to repeat the above. During the random walk, once a vehicle is selected as the relay vehicle, it changes its route immediately and follows the shortest path to the RSU for relaying the message. After that, it recovers to drive following the random walk model.

Adversary model. We assume that the malicious vehicles follow the same mobility model as the normal vehicles, and the only difference is that after they accept to relay the message, they drop the relayed messages with a probability ρ . The proportion of malicious vehicles, defined as the number of malicious vehicles to the total number of vehicles, is another variable in the simulation.

The detailed parameter settings are summarized in Table 5.1. We conduct the simulations with different L and compare it with random selection under different N , and then we perform the simulation with different ρ and malicious proportion. For each case, we run the simulation for 3 hours, and the average performance

Table 5.1: SIMULATION SETTINGS

Parameter	Setting
<i>Simulation</i>	
area	$10000 \times 10000 \text{ m}^2$
duration	3 hours
number of trust levels	$m = 10$
<i>RSU</i>	
number	1
transmission radius	$1000m$
<i>Vehicles</i>	
total number	$N = 50, 100, 200, 400$
transmission radius	$300m$
velocity	$36km/h$
trust level threshold	$L = 5, 8$
message generation interval per vehicle	1 piece / 6 min
malicious vehicles proportion	30%, 40%, 50%, 60%
drop probability	$\rho = 20\%, 30\%, 40\%, 50\%$

results over 10 runs are reported.

5.5.2 Simulation Results

Relay Ratio

In Figure 5.5, we compare the relay ratio of the vehicular ad hoc network with different relay selection policies, i.e., random selection, PTRS scheme with trust level threshold $L = 5$ and $L = 8$, under different vehicle number $N = 50, 100, 200, 400$ and malicious proportion of 50% with dropping probability of 50%. From the figure, we can see that the relay ratio is very low when relay vehicles are chosen randomly. By contrast, after adopting the PTRS scheme, the relay ratio can be improved from 75% to 95%, which demonstrates the effectiveness of our proposed scheme in improving the message relay ratio. From the figure, it also can be seen that the relay ratio increases with the increase of vehicle number N and trust level threshold L . The reason is that when there are more vehicles, more messages will be generated and the malicious vehicles have more chances to relay messages and

(a) $N=50$ (b) $N=100$ (c) $N=200$ (d) $N=400$

Figure 5.5: Relay ratio versus specific time period with different trust level thresholds

Figure 5.6: Total number of messages generated in 3 hours with different relay selection policies

then be detected by the scheme, which finally makes them be excluded in the relay selection. At the same time, when trust level threshold L is higher, better behaved vehicles are chosen and they increase the relay ratio of the network. However, from Figure 5.6, we find that the total number of generated messages will decrease when trust level threshold increases because in this case, the requesting vehicles have less chances to meet a qualified relay vehicle among its nearby candidate vehicles when their requirements are higher. Combining the above two figures together, we can find that there is always a trade-off between the utility and efficiency of our proposed scheme.

Detection Ratio

Figure 5.7 depicts the detection ratio variations within 3 hours for different total number of vehicles. From the figure, we can see that the detection ratio converges

Figure 5.7: Detection ratio versus time with trust level threshold $L=8$ (a) Dropping probability $\rho=20\%$ (b) Dropping probability $\rho=30\%$ (c) Dropping probability $\rho=40\%$ (d) Dropping probability $\rho=50\%$

Figure 5.8: Detection ratio varies with time under different malicious vehicle proportions

to nearly 100% as time increases; at the same time, it converges faster when the total vehicle number increases. The reason is similar to the above: more vehicles generate more messages which gives malicious vehicles more chances to relay messages and then be detected by the scheme.

The last experiment is done when the dropping probability and malicious proportion are fixed. In the next experiment, we further compare the detection ratios with different malicious proportion in terms of various dropping probabilities. The results are shown in Figure 5.8. From the comparisons, we can see that with the same malicious proportion, detection ratio increases as dropping probability increases because malicious vehicles with higher dropping probabilities are more easily detected. Intuitively, when malicious proportion is higher, the detection ratio is higher. However, by observing the figure, we find that the detection ratio reaches its highest as malicious proportion increases to 50%. After that, the detection ratio decreases as the malicious proportion increases. The reason is that when malicious proportion exceeds 50%, the system will be overturned.

5.6 Related Work

To date much research effort has been paid to preserve the privacy of vehicles in vehicular communications [91, 93, 59]. Similar to our work, a simple method is to use pseudonyms, which however may cause many issues. In [91], Lu et al. consider a scenario when the pseudonyms are changed at improper location or time, for example, on the road. In this way, the location and velocity information embedded in the safety messages could still provide a clue for an adversary to link the pseudonyms, which leads to privacy leakage. To cope with this issue, they propose a strategy to change the pseudonyms at social spots where many vehicles gather, e.g., intersections when the traffic light turns red and parking lots near a shopping mall. This solution is reasonable because when vehicles gather at those

social spots, their velocities and locations are the same and the location privacy will be achieved. However, this method is not applicable to our scenario because unlike velocity and location, the reputation score of a vehicle is unchangeable in a period. In [93], Lu et. al propose a social-based privacy-preserving packet forwarding protocol for vehicular DTN. In this protocol, a road side unit is used to help store and forward packets for vehicles. This proposed protocol, based on conditional privacy-preserving authentication (CPPA) technique, is robust against packet analysis, packet tracing and black hole attacks. The experimental results show that the SPRING protocol efficiently improves the delivery ratio, lowers the average delay and preserves the privacy of vehicles. This work has the same idea on “packet forwarding” to improve the delivery ratio like ours. However, it does not consider the reliability of relays. Another efficient conditional privacy preservation protocol is proposed in [59], to address the issue of anonymous authentication with authority traceability. The work is characterized by short-time anonymous key generation to solve the problem of key storage, fast safety message verification and efficient tracking algorithm.

Another recent group of papers focus on how to ensure the trustworthiness of messages in propagation or incentives in delay tolerant networks [94, 95, 96, 97, 98, 99, 100] or reliability of vehicle relay [82]. One way to address this problem is to collect the opinions or endorsements on the message in its propagation. For example, Li and Malip proposed a message announcement scheme [94]. In this scheme, the message receiver is able to evaluate the message reliability based on sender’s reputation. Upon receiving each message, the receiver will evaluate by giving a feedback report. Later the sender vehicle’s reputation will be aggregated based on those feedback reports from receivers. The system takes advantages of a centralized structure in VANET, which is similar to our proposed scheme. This work is also robust against both external and internal adversaries to a reasonably good level. Zhang proposes a message propagation model [95] to collect and prop-

agate peers' opinions. The peers are able to make local decisions on whether to follow the information by evaluating both its trust level and others' opinions. Since the framework is manipulated in a distributed and collaborative way, it shows great scalability. Experimental results also show the effectiveness of the proposed scheme. However, neither of these works consider the privacy issue of vehicles in message exchange, and the assumption that a cluster leader is always reliable in forwarding messages is not always practical in the real world. Another direction to this problem is laid on the technique of group signature and secret sharing. In [96], Daza proposes a privacy-preserving vehicle-generated announcement scheme to protect the system against both internal and external attacks. Specifically, a prior approach is used to thwart fake announcement launched by internal attacks and reduces the verification cost of endorsed messages to one signature verification. A (t, n) -threshold signature is used to verify an announcement only when at least t out of n vehicles endorse the message. Finally, a compound protocol is proposed combining three privacy-preserving variants together. Wu et al. propose a privacy-preserving system to guarantee message trustworthiness in vehicle-to-vehicle communications [97]. When a message-linkable group signature (MLGS) is produced and attached which ensures the vehicle anonymity. Later, after the endorsements for a message are aggregated, a threshold authentication mechanism will be executed to help vehicles decide whether to trust the message. To speed up the validation of authenticated messages, a batch message processing approach is used. Though the privacy issue has been considered, the misbehaviors of vehicles are not taken into account, neither do the system provide any incentives to the vehicles participating in the evaluations of messages.

From the investigations above, we see that how to achieve anonymity and trust at the same time has been a challenging research issue which attracts researchers' attention, some of the works have been done in the context of participatory sensing [101, 102, 103, 104]. In [101], Wang et al. propose an anonymous repu-

tation management protocol to solve the problem of “trust without identity” in mobile sensing. In this protocol, the blind signature technique is used to achieve anonymity. Besides, by issuing a reputation certificate, the server will only know who wants to participant without knowing its actual sensing report. In [102], the authors present a way to transfer the reputation values belonging to the same user between its different pseudonyms. This kind of transfer is manipulated by a trusted server, which also maintains a list of mappings between real user identities and all the associated pseudonyms. Another similar solution is proposed in [103], called IncngniSense. In this framework, blind signature is used to generate periodic pseudonyms and a reputation transfer based on cloaking mechanism is presented.

In contrast to the existing solutions, though our work relies on a trust authority to update and manage reputation scores and trust levels, anonymous authentication and verification are conducted between two parties to meet the dynamic requirements of VANET. Our trust model is developed on existing technique of trust management scheme. In particular, the work directly related to the ours is the Dirichlet-based trust model proposed by Josang in [43] and Fung et al. in [84]. However, both of their works have not considered about the privacy issues in the application of trust model, which has been solved in our work.

5.7 Summary

In this chapter, we have developed a scheme in order to help a vehicle choose another reliable vehicle for relaying a message. By establishing a Dirichlet-based trust model, the proposed PTRS scheme improves the relay ratio of the whole network. In addition, we introduced a trust-based request-response scheme when a requesting vehicle wants to select a relay among candidate vehicles which is able to preserve the privacy of a candidate vehicle. Detailed security analyse have shown that the PTRS scheme is resistant against most attacks launched by self-

ish or malicious attackers. Through extensive performance evaluations, we have demonstrated that the proposed PTRS scheme can improve the relay ratio with the presence of selfish or malicious attackers.

Chapter 6

Trust-based Vehicular Platoon Crowdsensing Scheme with Privacy Preservation

In the previous chapter, we presented a robust trust-based relay selection scheme, called PTRS, which is based on Dirichlet distribution to make two-hop vehicle-to-infrastructure communications reliable and secure. Though the location privacy of vehicles are preserved, the communication cost efficiency is high. In this chapter, we will propose a more efficient scheme: a trust-based vehicular platoon crowdsensing scheme, named as TripSense, in VANET [39]. The proposed TripSense scheme introduces a trust-based system to evaluate vehicles' sensing abilities and then selects those more capable vehicles in order to improve sensing result accuracy. Besides, the sensing tasks are accomplished by platoon member vehicles and preprocessed by platoon head vehicles before the data are uploaded to server. As a result, it is less time-consuming and more efficient compared with the way where the data is submitted by individual platoon member vehicles. Therefore, it is more suitable in ephemeral network like VANET. Moreover, our proposed TripSense scheme integrates unlinkable pseudo-ID technique to achieve PM vehicle identity

privacy, and employs a privacy-preserving sensing vehicle selection scheme without involving the PM vehicle's trust score to keep its location privacy. Detailed security analysis shows that our proposed TripSense scheme not only fulfills desirable privacy requirements but also can resist against attacks launched by adversaries. Extensive simulations are conducted to show the correctness and effectiveness of our proposed scheme.

6.1 Introduction

Envisioned as one of the most promising applications to implement intelligent transportation systems (ITS), vehicular platooning [56, 37] has the potential to enhance road safety, improve traffic efficiency and reduce energy consumption due to air drag reduction [78]. At the same time, with the increasing popularity of mobile devices and sensing technologies, a new sensing paradigm, mobile crowdsensing, attracts attention from both academia and industry [105]. Different from traditional sensor networks, this new sensing paradigm leverages the power of crowds for large scale sensing tasks and fuels the evolution of the Internet of Things [106]. Many factories are built in remote areas where the sensor resources are limited, if the authority needs to inspect those factories, it can hardly collect information with the existing traditional sensor networks. However, given the fact that many highways go through the remote areas. One solution to this problem is to invite vehicles passing by those areas to take part in the crowdsensing tasks and utilize their sensed data (e.g., temperature, humidity, noise level, air pollution level, etc.).

However, due to the inherent openness of this platform, it is easy for vehicles to contribute corrupted data [107]. Several research efforts have been made on ensuring the trustworthiness of the sensed data [101, 108]. One possible solution is to establish the reputation system for evaluating the trustworthiness of volunteer contributions in participatory sensing applications [107].

Furthermore, this new data aggregation way may also bring in privacy concerns into the networks. For example, the sensed data could reveal the capacity of a vehicle's sensor and hence reveal the personal information of the vehicle. Another factor that has always been a concern is the location privacy, since the locations of the vehicles are closely related to the drivers of those vehicles [91]. To achieve location privacy, one approach is to use unlinkable pseudonyms that are periodically changed when broadcasting messages [1, 92, 14]. However, pseudonyms do not always ensure privacy, as an example shown in Figure 6.1, a platoon head vehicle is asking its platoon member vehicle V_i for participating in the sensing task. When V_i responds by sending its own reputation score ts_i at Day-1 and Day-2 respectively, the platoon head vehicle can still associate V_i in different days by associating its trust scores even when its pseudonym has been changed. The unchanged trust score of a vehicle reveals its location privacy and the platoon head vehicle can even derive the driving pattern of the platoon member vehicle. Therefore, it is compelling for us to build a trust system through which vehicles take its advantages without sacrificing their privacies and a data aggregation mechanism to ensure data privacy.

Figure 6.1: platoon head vehicle associates a platoon member vehicle's trust scores even when its pseudonym has been changed

Based on the observations above, we propose a trust-based vehicular platoon

crowdsensing scheme, called TripSense, to improve sensing accuracy while achieving location and data privacy. This scheme is based on vehicular platooning technique to collect and aggregate data. At the same time, by establishing a trust model to measure the accuracy of a vehicle's sensed data, the service provider (SP) efficiently detects and then excludes the malicious or selfish vehicles who submit corrupted sensed data. Meanwhile, the proposed scheme is characterized by its ability to preserve the location privacy and data privacy of sensing vehicles. With assistance of platoon head vehicles, the communication overhead and computational cost can be greatly reduced. Specifically, our work features the followings:

- First, we establish the trust system based on Dirichlet distribution to evaluate the sensing accuracy of all sensing vehicles in our proposed TripSense scheme. The historical sensed data will be evaluated and finally form a reputation score. Therefore, the sensing accuracy will be improved greatly when the data are always collected from those high reputation sensing vehicles.
- Second, we propose the TripSense scheme by taking advantages of the unique features of vehicular platooning. In this scheme, platoon head vehicles firstly authenticate all sensing vehicles inside the platoon and then select some of them according to their trust values. Later, the sensed data from sensing vehicles will be collected and aggregated by platoon head vehicles before they are finally uploaded to the server. Compared with previous works, our proposed scheme reduces the communication overhead and hence is more suitable for the dynamic and ephemeral vehicular ad hoc network.
- Third, we design a privacy-preserving sensing vehicle selection scheme based on our trust system and a privacy-preserving data aggregation scheme based on the efficient commitment scheme in [109] such that platoon head vehicles can collect the data without leaking sensing vehicles' privacy.

The remainder of this chapter is organized as follows. In Section 6.2, we formalize the system model, trust model and threat model considered in our work, and identify our design goals. In Section 6.3, the TripSense scheme is presented in details, together with the rationale how it can help the requesting vehicles to choose a highly reliable relay vehicle without knowing its reputation score. Security analysis is then presented in Section 6.4, and the performance analysis is given in Section 6.5. Finally, we present the related work in Section 6.6 and draw conclusions in Section 6.7.

6.2 Problem Statement

In this section, we define the problem by formalizing the system model, security model and design goal.

6.2.1 System Model

Figure 6.2: System model under consideration

In our model, the service provider (SP) wants to inspect an area of interest

(AoI) located near a highway where many platoons pass by. As illustrated in Figure 6.2, our system model consists of three roles: the service provider (SP), a cloud server (CS), the immobile roadside units (RSUs) along the highway and mobile vehicles traveling on the highway which are equipped with onboard units (OBUs) and powerful sensors.

Service Provider (SP): The SP is fully trusted because it is normally controlled by the authority who wants to inspect an area of interest by collecting the data of this AoI. The data collected is a vector of readings regarding, for example, air pollution level, noise level, temperature, humidity and so on. The duty of SP is to initialize the whole system, and distributes key materials to RSUs and vehicles. It is also responsible for storing and updating trust values for all vehicles.

Roadside Units (RSUs): The RSUs are subordinated by the SP, which are connected to the CS and SP via reliable communication channels. Equipped with wireless devices, RSUs are able to exchange data with the passing-by vehicles. However, due to the high cost of RSU installment and maintenance, especially in the early stage of VANET, RSUs are sparsely deployed along the highway. The RSUs will never disclose any internal information without permissions. However, we do not rule out the possibility that a portion of RSUs at the road side are compromised or the attackers even deploy bogus RSUs. Nevertheless, the SP can inspect all RSUs at high level: once the RSUs are compromised, they will be recovered or revoked soon by SP.

Cloud Server (CS): CS collects data from RSUs, then aggregates them in a privacy-preserving way. Besides, CS also computes the sensed data evaluations for vehicles and returns the results to SP. CS are assumed to be honest but curious about the sensed data of vehicles, which means that it follows the proposed scheme faithfully, but tends to be curious and disclose vehicles' privacy.

Vehicles: The vehicles are regarded as a group of highly mobile nodes equipped

with OBUs which allow them to communicate with other vehicles or with RSUs. In the highway, vehicles follow a platoon head vehicles to form a platoon. With this driving pattern, the vehicles can be further divided into two categories:

- Platoon Head (PH) Vehicles $\mathcal{P}_0 = \{ph_1, ph_2, \dots\}$: PH vehicles take the full control of the whole platoon when driving on the highway, they are responsible for the safety, user experience of all platoon member vehicles. Apart from that, they also claim a sensing task and submit sensed data to RSUs through V-2-I communication. PH vehicles are also honest but curious about the privacy of platoon member vehicles. In fact, PH vehicles could be malicious and provides untruthful aggregated data to server in order to subvert the system, or they may even collude with a bunch of PM vehicles with an object to victimize other PM vehicles. However, in this work, we do not consider this issue since it is not the main focus of this work.
- Platoon Member (PM) Vehicles $\mathcal{V}_0 = \{v_1, v_2, \dots\}$: Each PM vehicle is equipped with various types of powerful sensors to meet the requirements of different tasks. Through V-2-V communication, a member vehicle authenticates itself and then submits its sensed data to the PH vehicles. Some of the PM vehicles compromised by adversaries launch attacks, other PM vehicles are all honest but curious.

Both PH vehicles and PM vehicles will get paid by the SP for leading a platoon or contributing their sensed data.

6.2.2 Security Model

In our security model, we assume that all roles, except the SP, RSUs and malicious PM vehicles, are honest-but-curious, i.e., they will faithfully follow the protocol, but could also snoop into other role's privacy on account of some sensitive infor-

mation available to them. In specific, we first consider the privacy requirements of PM vehicles.

Privacy requirements of platoon member vehicles: The privacy requirement of a PM vehicles include its data privacy, location privacy and identity privacy. Since the sensed data are private assets of a PM vehicle, which may reflect some sensitive information like the sensor accuracy or sensing ability, the PM vehicles will not disclose them to others. The location privacy requirement indicates that a PM vehicle will not let its PH vehicle know its past driving pattern, and the identity privacy means that the PM vehicle tries to keep his real identity secret. Meanwhile, each vehicle is also privacy-curious, i.e., it tends to disclose the privacy of other vehicles from other information available to him.

We assume that there are two kinds of adversaries according to their attacking abilities, the first kind tries to impersonate another authorized PM vehicle; the second kind is able to control a small portion of vehicles. Specifically, we list potential attacks as follows:

- *Impersonation attack:* The first kind of adversary may try to impersonate a PM vehicle to ask for a sensing task. However, this PM vehicle may not be qualified in the system. Once chosen to fulfil the task, these unqualified vehicles may submit inaccurate sensed data.
- *Malicious sensing attack:* The second kind more capable adversary is able to control a small fraction of the vehicles in the system who submit inaccurate sensed data deliberately to subvert the system. Another possible case is that the PM vehicle is selfish, so it report an arbitrary data without using sensors to save power.
- *Trust score association attack:* PH vehicles are honest but curious, in this case, if the trust score of a PM is directly given to its PH vehicle, its driving pattern will be disclosed. As described in Section 6.1, the reason is that since

every time the PH vehicle can associate a PM vehicle in platoon according to the same trust score collected in different trips even though the pseudo-id has been changed.

- *Data analysis attack:* Due to the curious characteristics of both PH vehicles and PM vehicles, they may eavesdrop the transmission of sensed data and try to analyze the data. On the other hand, cloud server (CS) is also curious about the sensed data. If the data is not encrypted, those attacker can easily analyze the data in transmission.

6.2.3 Design Goal

Our design goal is to develop a trust-based privacy-preserving scheme to not only improve the sensing accuracy, but also preserve the privacy of sensing vehicles while resisting against the attacks launched by adversary. Specifically, the following desirable objectives need to be achieved.

- *Ensuring the sensed data reliability and accuracy.* According to our adversary model, the existence of selfish and malicious vehicles who submit corrupted sensed data will make the final result inaccurate and unreliable. Hence, our proposed scheme should be able to improve the sensed data accuracy by excluding those selfish and malicious vehicles' data.
- *Achieving privacy-preserving sensing vehicle selection, sensed data aggregation and evaluation.* The proposed scheme should achieve privacy requirements of PM vehicles. Particularly, i) the real identity of PM vehicles will never be disclosed; ii) when a PM vehicle replies to the PH vehicle, the PH vehicle can never know the exact trust score of this PM vehicle; iii) when a PH vehicle collects and aggregates the sensed data, it can never know what the data is; iv) the CS can never know the aggregated sensed data and the

evaluations on those data.

- *Resisting against attacks launched by adversaries.* The proposed scheme should also be secure and reliable in VANET. Once an outside adversary launches some attacks, e.g., impersonation attack, data analysis attack, the proposed scheme should be able to detect them.

6.3 Proposed TripSense Scheme

In this section, we propose our TripSense scheme, which consists of six parts: system initialization, trust-based privacy-preserving sensing vehicle selection, privacy-preserving sensed data aggregation, aggregated sensed data retrieval, privacy-preserving sensed data accuracy evaluation, and Dirichlet-based trust management.

6.3.1 System Initialization

We assume that a service provider (SP) will bootstrap the whole system. Specifically, given a security parameter κ , SP first generates the bilinear parameters $(p, q, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{Gen}(\kappa)$ and then computes $h = g^q \in \mathbb{G}$. Next, SP chooses a secure symmetric encryption algorithm $\mathcal{Enc}()$, i.e., AES, and a collision-resistant cryptographic hash function $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_n^*$. In addition, SP chooses a random number $s \in \mathbb{Z}_n^*$ as the master key and computes $P_{pub} = g^s$, $n = pq$. Finally, SP keeps p, q secret and publishes $\{n, g, h, P_{pub}, \mathbb{G}, \mathbb{G}_T, e, \mathcal{H}, \mathcal{Enc}\}$

RSU REGISTRATION: For each RSU, SP first generates an identity, denoted by RID , and then calculates its private key and public key as $(s_r; S_r)$, where s_r is randomly chosen in $\mathbb{Z}_n^*$ and $S_r = g^{s_r}$.

PH VEHICLE REGISTRATION: For any platoon head (PH) vehicle $ph_i \in \mathcal{P}_0$ which wants to participate in the sensing task, it has to register itself to SP and

obtains a real identity RID_i . Then SP assigns the private key and public key to ph_i as (s_i, S_i) , where s_i is randomly chosen in $\mathbb{Z}_n^*$ and $S_i = g^{s_i}$.

PM VEHICLE REGISTRATION: For each platoon member (PM) vehicle $v_j \in \mathcal{V}_0$ who wants to take part in the sensing task and contributes its sensed data, it first registers itself in the system. The following steps between SP and v_j show the registration process.

- SP first chooses a random number $k_0 \in \mathbb{Z}_n^*$ and uses $\mathcal{Enc}()$ to compute pseudo-IDs $\mathcal{PID}_j = \{PID_{j1}, PID_{j1}, \dots\}$, where each pseudo-ID $PID_{jk} \in \mathcal{PID}_j$ is computed as $PID_{jk} = \mathcal{Enc}_{k_0}(ID_j || r_{jk})$ with a fresh random number $r_{jk} \in \mathbb{Z}_n^*$. Then, for each PID_{jk} , SP calculates its corresponding private key by $s_{jk} = \mathcal{H}(PID_{jk})^s$ and public key by $S_{jk} = g^{s_{jk}}$. Finally, SP sends $\mathcal{PID}_j$ and the corresponding public and private keys back to v_j via a secure channel.
- After receiving pseudo-IDs $\mathcal{PID}_j$ and their private keys, v_j verifies the correctness of each private key s_{jk} by checking $e(\mathcal{H}(PID_{jk}), P_{pub}) \stackrel{?}{=} e(s_{jk}, g)$.

TRUST REGISTRATION: Each registered PM vehicle v_j will be given a trust score ts_j by SP before it is able to take part in the sensing task, where $ts_j \in [0, 1]$ with the precision of two decimal places. Initially, $ts_j = ts_0$. Besides, SP also defines L trust levels $\{TL_1, TL_2, \dots, TL_L\}$ for all trust scores from 0 to 1. For instance, TL_1 is with $(0, 0.1]$, TL_2 is with $(0.1, 0.2]$, $\dots$, TL_{10} is with $(0.9, 1]$. Later, SP selects l random elements $\{y_1, y_2, \dots, y_L \in \mathbb{Z}_n^*\}$ as master keys, and publishes the public keys as $\{Y_1 = g^{y_1}, Y_2 = g^{y_2}, \dots, Y_L = g^{y_L}\}$.

- For a registered PM vehicle v_j with trust score $ts_j \in TL_x$, where $x \in [1, L]$, SP makes signatures for each of its pseudonym $PID_{jk} \in \mathcal{PID}_j$ as $A_{jk} = g^{\frac{1}{y_x + ts_j + s_{jk} + H(T_j)}}$, where T_j is the timestamp for updating the trust score of v_j .

TASK REGISTRATION: Before a task is broadcasted to PH vehicles, it should be registered by SP. First, the sensed data categories need to be decided, such as

air pollution level, noise level, temperature, humidity, and so on. Second, the the format could be defined as $\vec{d} = (d^A, d^B, \dots, d^Z)$, where each element denotes one category. Besides, SP also defines that each piece of data is with precision of two decimal places. In addition, the location of area of interest (AoI) is also included in the task. Finally, the SP will also decide a sensing vehicle trust level threshold TL_{TH} according to the accuracy requirements of the task to make sure that the sensed data only come from those more trusted vehicles.

6.3.2 Trust-based Privacy-preserving Sensing Vehicle Selection

We assume that there are a number of m PH vehicles in the system which would like to participate in the sensing task. They form a new set $\mathcal{P} = \{ph_1, ph_2, \dots, ph_m\}$. For a specific PH vehicle $ph_i \in \mathcal{P}$, it needs to collect sensed data from all registered PM vehicles in its platoon and then selects those which meet the trust level requirement. Therefore, a trust-based privacy-preserving sensing vehicle selection scheme has been proposed as follows.

Step 1: When the platoon approaches the AoI, ph_i broadcasts its sensing requests $\{PID_i || H(T)^{s_i} || T\}$ to all platoon members, where T is the current timestamp.

Step 2: In ph_i 's platoon, for each registered PM vehicle v_j , after receiving ph_i 's requests, it first verifies whether ph_i is a registered PH vehicle by checking $e(H(T)^{s_i}, g) \stackrel{?}{=} e(S_i, H(T))$. If it holds, v_j accepts the requests, otherwise, v_j rejects ph_i . Then v_j responds to ph_i with $\{PID_{jk} || H(T')^{s_{jk}} || TL_x || \Pi || T' || T_j\}$ by calculating as follows, where T' is the current timestamp and T_j is the latest timestamp for updating v_j 's trust score.

- Since the trust scores of PM vehicles are two decimal places, we need to

expand them by 100 times before it can be encrypted. If v_j 's trust score is with trust level TL_x where $x \in [1, L]$, v_j encrypts the expanded trust score ts_j as $C = g^{ts_j} h^r$, with a fresh random number $r \in \mathbb{Z}_n^*$.

- Similarly, the sensed data are all collected and expanded by 100 times. For one category in $\vec{d}$, v_j encrypts the expanded sensed data d_j as $D = g^{d_j} h^{r'}$, where r' is a random number in $\mathbb{Z}_n^*$.
- v_j chooses a pseudonym PID_{jk} and a random element $v \in \mathbb{Z}_n^*$ to calculate the following:

$$\begin{aligned} B &= A_{jk}^v = g^{\frac{v}{y_x + ts_j + s_{jk} + H(T_j)}} \\ E &= B^{-ts_j} \cdot g^v = g^{\frac{v(y_x + s_{jk} + H(T_j))}{y_x + ts_j + s_{jk} + H(T_j)}} \end{aligned} \quad (6.1)$$

- v_j randomly chooses ts_j'' , r'' , $v'' \in \mathbb{Z}_n^*$ and computes $C'' = g^{ts_j''} h^{r''}$, $E'' = B^{-ts_j''} g^{v''}$
- v_j calculates the proofs $\Pi = \{C, B, E, D, z_1, z_2, z_3, \phi\}$ as:

$$\begin{aligned} \phi &= H(C, B, E, D, C'', E'', H(T)^{s_j}) \\ z_1 &= ts_j'' + \phi \cdot ts_j \mod n \\ z_2 &= r'' + \phi \cdot r \mod n \\ z_3 &= v'' + \phi \cdot v \mod n \end{aligned} \quad (6.2)$$

Step 3: After receiving the response from v_j , ph_j first checks whether v_j is a registered PM vehicle by checking $e(g, H(T')^{s_{jk}}) \stackrel{?}{=} e(S_{jk}, H(T'))$. Then, ph_i checks whether the timestamp T' is relatively new. Next, ph_i checks whether v_j 's trust score ts_j is with TL_x by checking $e(E, g) \stackrel{?}{=} e(B, Y_x \cdot S_{jk} \cdot g^{H(T_j)})$. If it does hold, ph_i calculates $\hat{C} = g^{z_1} h^{z_2} C^{-\phi}$, $\hat{E} = B^{-z_1} g^{z_3} E^{-\phi}$ and checks $\phi \stackrel{?}{=} H(C, B, E, D, \hat{C}, \hat{E}, H(T)^{s_i})$. If it holds, ph_i will finally check whether $TL_x \geq TL_{TH}$, and accept v_j 's sensed data once its trust level satisfies the task requirement.

6.3.3 Privacy-preserving Sensed Data Aggregation

For each PH vehicle $ph_i \in \mathcal{P}$, where $i \in [1, m]$, we assume that a number of n_i PM vehicles meet the trust level threshold requirement, and those eligible PM vehicles form a set $\mathcal{V}_i = \{v_{i1}, v_{i2}, \dots, v_{in_i}\}$. After a PH vehicle ph_i receives the sensed data from its PM vehicles, it selects those eligible data and aggregates them locally before submitting to CS for global aggregation. Therefore, a privacy-preserving data aggregation scheme has been proposed.

Local Aggregation: Take one data category, d^A , in $\vec{d}$ as an example. For simplicity, we omit the superscript and use D_{in_i} instead of $D_{in_i}^A$. As described in Section 6.3.2, ph_i collects encrypted sensed data from n_i PM vehicles as $D_{i1} = g^{d_{i1}} \cdot h^{r'_{i1}}, D_{i2} = g^{d_{i2}} \cdot h^{r'_{i2}}, \dots, D_{in_i} = g^{d_{in_i}} \cdot h^{r'_{in_i}}$ together with their corresponding encrypted trust score: $C_{i1} = g^{ts_{i1}} \cdot h^{r_{i1}}, C_{i2} = g^{ts_{i2}} \cdot h^{r_{i2}}, \dots, C_{in_i} = g^{ts_{in_i}} \cdot h^{r_{in_i}}$. Then ph_i aggregates the encrypted data D_{ij} and trust score C_{ij} of each PM vehicle $v_{ij} \in \mathcal{V}_i$ where $j \in [1, n_i]$ using the paring:

$$\begin{aligned} e(D_{ij}, C_{ij}) &= e(g^{d_{ij}} \cdot h^{r_{ij}}, g^{ts_{ij}} \cdot h^{r'_{ij}}) \\ &= e(g, g)^{d_{ij}ts_{ij}} \cdot e(g, h)^{d_{ij}r_{ij}+ts_{ij}r'_{ij}} \cdot e(h, h)^{r_{ij}r'_{ij}} \end{aligned} \quad (6.3)$$

Later ph_i aggregates all aggregated data of all PM vehicles in $\mathcal{V}_i$ together as:

$$\begin{aligned} \phi_i &= \prod_{j=1}^{m_i} e(D_{ij}, C_{ij}) = \prod_{j=1}^{m_i} e(g^{d_{ij}} \cdot h^{r_{ij}}, g^{ts_{ij}} \cdot h^{r'_{ij}}) \\ &= \prod_{j=1}^{m_i} e(g, g)^{d_{ij}ts_{ij}} \cdot \prod_{j=1}^{m_i} e(g, h)^{d_{ij}r_{ij}+ts_{ij}r'_{ij}} \cdot \prod_{j=1}^{m_i} e(h, h)^{r_{ij}r'_{ij}} \\ &= e(g, g)^{\sum_{j=1}^{m_i} d_{ij}ts_{ij}} \cdot e(g, h)^{\sum_{j=1}^{m_i} (d_{ij}r_{ij}+ts_{ij}r'_{ij})} \cdot e(h, h)^{\sum_{j=1}^{m_i} r_{ij}r'_{ij}} \end{aligned} \quad (6.4)$$

Finally, when ph_i drives within the transmission range of an RSU, it submits ϕ_i together with all pseudo-IDs in $\mathcal{V}_i$ to CS via RSU.

Global Aggregation: Upon receiving reports from all PH vehicles in $\mathcal{P}$, CS

aggregates those data together as follows, and passes the final result Φ and all pseudo-IDs of PM vehicles to SP.

$$\begin{aligned} \Phi &= \prod_{i=1}^m \phi_i = e(g, g)^{\sum_{i=1}^m \sum_{j=1}^{n_i} d_{ij} \cdot ts_{ij}} \\ &\cdot e(g, h)^{\sum_{i=1}^m \sum_{j=1}^{m_i} (d_{ij} r_{ij} + ts_{ij} r'_{ij})} \cdot e(h, h)^{\sum_{i=1}^m \sum_{j=1}^{m_i} r_{ij} r'_{ij}} \end{aligned} \quad (6.5)$$

6.3.4 Aggregated Sensed Data Retrieval

Once SP receives the aggregated sensed data Φ from CS, it retrieves it using its secret key p :

$$\begin{aligned} \Phi^p &= e(g, g)^{p \sum_{i=1}^m \sum_{j=1}^{n_i} d_{ij} \cdot ts_{ij}} \\ &\cdot e(g, h)^{p \sum_{i=1}^m \sum_{j=1}^{m_i} (d_{ij} r_{ij} + ts_{ij} r'_{ij})} \cdot e(h, h)^{p \sum_{i=1}^m \sum_{j=1}^{m_i} r_{ij} r'_{ij}} \\ &= e(g, g)^{p \sum_{i=1}^m \sum_{j=1}^{n_i} d_{ij} \cdot ts_{ij}} \end{aligned} \quad (6.6)$$

Similarly, we have:

$$\begin{aligned} e(h, h)^{p \sum_{i=1}^m \sum_{j=1}^{m_i} r_{ij} r'_{ij}} &= e(h, h^p)^{\sum_{i=1}^m \sum_{j=1}^{m_i} r_{ij} r'_{ij}} \\ &= e(h, 1)^{\sum_{i=1}^m \sum_{j=1}^{m_i} r_{ij} r'_{ij}} = 1 \end{aligned} \quad (6.7)$$

Since the aggregated data $\sum_{i=1}^m \sum_{j=1}^{n_i} d_{ij} \cdot ts_{ij}$ is in small space, we can use the method of exhaustion to retrieve them. From the pseudo-IDs in $\mathcal{V}_i, i \in [1, m]$, SP is able to find their real identities and corresponding trust scores $ts_{ij}, i \in [1, m], j \in [1, n_i]$. Then SP computes the sensed data d_0 using a weighted majority method:

$$d_0 = \frac{\sum_{i=1}^m \sum_{j=1}^{n_i} d_{ij} \cdot ts_{ij}}{\sum_{i=1}^m \sum_{j=1}^{n_i} ts_{ij}} \quad (6.8)$$

For each category, there will be a sensed result, therefore the sensed result vector $\vec{d}_0$ will be $\vec{d}_0 = (d_0^A, d_0^B, \dots, d_0^Z)$. After shrinking 100 times, SP will get the final sensed result.

6.3.5 Privacy-preserving Sensed Data Accuracy Evaluation

We assume that all PM vehicles in each PH vehicle ph_i 's platoon contribute their sensed data in the task, where $ph_i \in \mathcal{P}, i \in [1, m]$. These PM vehicles form a set, denoted as $\mathcal{V} = \{v_1, v_2, \dots, v_n\}$, where n is the total number of these PM vehicles. After the sensed result is computed, SP would like to evaluate the sensed data accuracy in this task for each PM vehicle who contributes its data. Specifically, for $v_k \in \mathcal{V}$, from Section 6.3.3, we learn that CS stores v_k 's pseudo-ID and encrypted sensed data for sensing category A as: $D_k^A = g^{d_k^A} \cdot h^{r_k'^A}$. The evaluation score $f_k \in [0, 1]$ for v_k in this task can be calculated by following the steps below:

Step 1: Given that there are many sensing categories in the sensed data vector, SP first defines a tolerance value for each sensing category in sensed result vector $\vec{d}$. We denote these tolerance values as another vector $\vec{d}_t = (d_t^A, d_t^B, \dots, d_t^Z)$. The tolerance value can be explained in this way: if the difference between the sensed data and sensed result is larger than tolerance level, the sensed data accuracy is unacceptable and $f_k = 0$. Besides, SP also defines the weights for different sensing categories as $\omega_A, \omega_B, \dots$ which satisfies $\omega_A + \omega_B + \dots + \omega_Z = 1$.

Step 2: We take sensing category A as an example, SP needs to calculate the difference between sensed result and sensed data $\Delta d_k^A = |d_0^A - d_k^A|$. When there are many vehicles in the VANET, the computation cost are too large for SP so it should be done by CS in a privacy-preserving way as follows. Note that, in case d_0^A is not an integer, SP rounds it off to the nearest integer.

- SP encrypts the sensed result d_0^A as: $D_0^A = g^{d_0^A} \cdot h^{r_0'^A}$, where $r_0'^A \in \mathbb{Z}_n^*$, and sends D_0^A to CS.

- CS pairs the encrypted sensed data D_k^A from v_k and the inverse of encrypted sensed result, $D_k^{A^{-1}}$, as: $\alpha_k^A = e(D_0^A, D_k^{A^{-1}})$. In case that $d_0 < d_k$, CS also pairs the data as: $\beta_k^A = e(D_0^{A^{-1}}, D_k^A)$. After calculation, CS passes the results together with the v_k 's pseudo-ID $\{PID_k || \alpha_k^A || \beta_k^A\}$ to SP.
- Upon receiving CS's message, SP first finds the real identity of v_k according to its pseudo-ID PID_k , then retrieves $\Delta d_k^A = |d_0^A - d_k^A|$ using the same method of exhaustion proposed in Section 6.3.4.

Step 3: After calculating Δd_k^A , SP uses the similar way to calculate other sensing categories as: $\Delta d_k^B, \Delta d_k^C, \dots, \Delta d_k^Z$. Finally, the evaluation score for v_k in this task is calculated by:

$$f_k = \omega_A(1 - \frac{\Delta d_k^A}{d_t^A}) + \omega_B(1 - \frac{\Delta d_k^B}{d_t^B}) + \dots + \omega_Z(1 - \frac{\Delta d_k^Z}{d_t^Z}) \quad (6.9)$$

6.3.6 Dirichlet-based Trust Management

For a specific PM vehicle $v_k \in \mathcal{V}$, the SP would like to evaluate its trustworthiness from its evaluation scores. Since the trustworthiness of v_k reflects its performance in a long period, SP first collects v_k 's evaluation scores in many tasks, denoted by a continuous random variable X ($0 \leq X \leq 1$). From these collected historic records, SP can estimate X 's future distributions by using Dirichlet distribution. Since Dirichlet distribution is based on initial belief on an unknown event according to prior distribution. It provides a solid mathematical foundation for measuring the uncertainty of feedbacks based on historical data. Compared to Beta distribution which is more appropriate in a binary satisfaction level [42], Dirichlet distribution is more appropriate for multi-valued satisfaction levels [84]. In our case, the evaluation trustworthiness of user vehicles are described by continuous trust scores. Therefore, SP uses Dirichlet distribution to estimate the performance of candidate vehicles in the future and then build trust model accordingly.

In order to classify the historical and future evaluation scores, we also denote a number of l satisfaction levels of feedbacks as a set $\{\theta_1, \theta_2, \dots, \theta_l\}$ ($\theta_i \in (0, 1], i \in [1, l], \theta_i < \theta_{i+1}$). Let $\vec{p} = \{p_1, p_2, \dots, p_l\} (\sum_{i=1}^l p_i = 1)$ be the probability distribution vector of X with respect to satisfaction levels, so that we have $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i (i = 1, 2, \dots, l)$. To make it more mathematically precise, we define $\theta_0 = 0$ when $i = 1$, $X_i = 0$ is categorized into θ_1 .

As described in Section 6.3.5, once v_k finishes many sensing tasks, the SP is able to collect v_k 's historical evaluation scores, then we let $\vec{\gamma} = \{\gamma_1, \gamma_2, \dots, \gamma_l\}$ denote the vector of cumulative evaluation score and initial belief of X . With a posterior Dirichlet distribution, $\vec{p}$ can be modeled as:

$$f(\vec{p}|\xi) = Dir(\vec{p}|\vec{\gamma}) = \frac{\Gamma(\sum_{i=1}^l \gamma_i)}{\prod_{i=1}^l \Gamma(\gamma_i)} \prod_{i=1}^l p_i^{\gamma_i-1} \quad (6.10)$$

where ξ denotes the background information represented by $\vec{\gamma}$. Let: $\gamma_0 = \sum_{i=1}^l \gamma_i$. The expected value of the probability of $X_i \in (\theta_{i-1}, \theta_i]$ with the historical distribution of evaluation scores is given by:

$$E(p_i|\vec{\gamma}) = \frac{\gamma_i}{\gamma_0} \quad (6.11)$$

Consider the time factor of historical evaluation scores, we introduce a forgetting factor η and give greater weight to more recent evaluation scores:

$$\vec{\gamma}^{(n)} = \begin{cases} \vec{S}^{(0)} & (n = 0) \\ \sum_{i=1}^n \eta^{t-t_i} \vec{S}^{(i)} + c_0 \vec{S}^{(0)} & (n \geq 1) \end{cases} \quad (6.12)$$

where n is the total number of historical evaluation scores, $\vec{S}^{(0)}$ is the initial belief vector when $n = 0$. Since no prior information is available, all elements of $\vec{S}^{(0)}$ have equal probability which makes $\vec{S}^{(0)} = (\frac{1}{l}, \frac{1}{l}, \dots, \frac{1}{l})$. Parameter $c_0 > 0$ is a weight on the initial beliefs. In the i^{th} sensing task of $v_k (i \in [1, n])$, $\vec{S}^{(i)}$ denotes the

satisfaction level of its evaluation score, which contains only one element set to 1 corresponding to the selected satisfaction level and all the other $l - 1$ elements set to 0. t_i stands for the timestamp when the i^{th} task took place and t is the moment of running the algorithm. The forgetting factor is $\eta \in [0, 1]$, smaller η means that the system is easier to forget the historical records and vice versa. In order to defend against on-off attack [85], we choose an adaptive value as: $\eta = c_1 \cdot (1 - ts_k)$, where c_1 is a parameter to control the forgetting factor, the larger value of c_1 makes the system more forgettable about the historical behaviors and vice versa. From the equation we can see that when v_k has a high trust score, its forgetting factor is small, which means that those good performances will be easily forgotten. On the contrary, once v_k provides a low accuracy sensed data, its trust score gets lower and forgetting factor becomes larger. This means that all of those poor sensing performances will be memorized and it takes even longer time for v_k to build up a high trust score again.

To calculate v_k 's trust score when as sensing vehicle, we first assign the weight ω_i to each satisfaction level $\theta_i (i \in [1, l])$. Let p_i denote the probability that v_k 's evaluation score is categorized into the satisfaction level of θ_i . $\vec{p} = (p_1, p_2, \dots, p_l) | \sum_{i=1}^l p_i = 1$. We model $\vec{p}$ using Eq. (6.10), Eq. (6.11), Eq. (6.12). Let Y be the random variable denoting the weighted average of the probability of each evaluation score in $\vec{p}$, the trust score ts_k of v_k is represented as:

$$ts_k = E[Y] = \sum_{i=1}^l \omega_i E[p_i] = \frac{1}{\gamma_0} \sum_{i=1}^l \omega_i \gamma_i \quad (6.13)$$

where γ_i is the cumulated evidence that v_k 's evaluation score is with satisfaction level of θ_i .

6.4 Security Analysis

In this section, we discuss the security and privacy properties of the proposed TripSense scheme. In specific, following the design goals discussed early, we examine whether the proposed TripSense scheme can achieve the desirable security and privacy requirements.

6.4.1 The proposed TripSense scheme is privacy-preserving for PM vehicles

- *PM vehicle's identity privacy and location privacy are preserved in the proposed TripSense scheme:* In our proposed TripSense scheme, each PM vehicle $v_j \in \mathcal{V}_0$ uses pseudo-ID PID_{jk} instead of real identity in the network. Hence, the identity privacy can be achieved. In addition, to preserve the location privacy of the PM vehicle, v_j changes its unlinkable pseudo-IDs at different trips and locations to ensure that its past and future trip and location information will not be linked by pseudo-IDs.

However, as analyzed in Section 6.2.2, v_j still suffers from trust score link attack. Thus, in our proposed scheme, when a PH vehicle ph_i checks whether its PM vehicle v_j 's trust score satisfies the task requirement, it uses discrete trust levels TL_x in place of accurate trust scores. In other words, v_j can prove itself a highly trusted vehicle in front of ph_i without revealing its exact trust score. In addition, v_j 's trust score ts_j is encrypted as $C = g^{ts_j} h^r$ and its trust level is in PS's signature $A_{jk} = g^{\frac{1}{y_x + ts_j + s_{jk} + H(T_j)}}$, which make the other PM vehicles impossible to get either v_j 's trust score or trust level.

- *The sensed data privacy preservation is achieved:* Once the sensed data are aggregated by a PM vehicle v_j , they are encrypted as: $D = g^{d_j} \cdot h^{r'}$. In the whole process of local aggregation and global aggregation, those data are

all aggregated without decryption until it reaches SP, where SP is able to recover with its private key p . Therefore, unless the other vehicles know the private key p , the sensed data information will never be disclosed.

6.4.2 The proposed TripSense scheme achieves robustness against attacks launched by adversary

- Resilience to malicious sensing attack:* According to our proposed scheme, the selfish or malicious vehicles which submit arbitrary sensed data will get low evaluation score will get low evaluation scores in the trust system. Those low evaluation scores will be accumulated and finally lead to low trust scores if they keep behaving in that way. When their trust scores are lower than threshold TL_{TH} , their sensed data will be excluded from data aggregation or they will be given a low weight in data aggregation due to low trust scores. In both ways, the attacker will be mitigated in our proposed scheme.
- Resilience to Trust Score Spoofing Attack:* We assume that the majority of PM vehicles follow the scheme honestly, but we don't rule out a possibility that a small fraction of PM vehicles cheat PH vehicles by using the fake trust scores. There are two possible cases: one case is that the PM vehicle v_j spoofs a higher trust score ts'_j with the hope to participate in sensing task. However, in this case, when v_j is with pseudo-ID PID_{jk} , v_j 's trust score ts_j is signed by SP as $A_{jk} = g^{\frac{1}{y_x + ts_j + s_{jk} + H(T_j)}}$, where y_x , s_{jk} , $H(T_j)$ indicate the trust level, private key and updating timestamp respectively. Therefore, without knowing the spoofed trust score ts'_j 's master key y'_x , v_j is unable to launch attack. Another case is that v_j provides a fake trust score ts'_j after encryption as $C' = g^{ts'_j} h^{r'}$, $E' = B^{ts'_j} g^v$. To deal with this type of attack, PH vehicle needs to check $\phi \stackrel{?}{=} H(C, B, E, D, \hat{C}, \hat{E}, H(T)^{s_i})$, it won't hold once the original C and E are changed to C' and E' .

- *Resilience to Impersonation Attack:* Both PH vehicle and PM vehicle could be impersonated by unqualified vehicles which want to take part in the sensing tasks. Specifically, for an impersonated PM vehicle, it may submit false data and escapes punishments; for a PH vehicle, it may collect sensed data without submitting to CS and renders the sensed data result incomplete. However, this attack can be thwarted by our proposed scheme. In the initialization phase in Section 6.3.1, both PH and PM vehicles will be given a pair of private and public keys once they are registered. In Section 6.3.2, a PM vehicle v_j first checks PH vehicle ph_i by checking $e(H(T)^{s_i}, g) \stackrel{?}{=} e(S_i, H(T))$ before it accepts ph_i 's sensing task requirement. The timestamp $H(T)$ is used to resist against replay attack. Similarly, the PH vehicle ph_i also checks $e(g, H(T')^{s_{jk}}) \stackrel{?}{=} e(S_{jk}, H(T'))$ before accepting the sensed data from v_j . As a result, our proposed TripSense scheme is resistant against impersonation attacks.

6.5 Performance Evaluation

We will evaluate the performance of our proposed TripSense scheme in this section. The numerical data is generated in MATLAB. The performance metrics used in the evaluation are: i) *trust scores variations* for different PM vehicles in terms of the task number; ii) *detection ratio* defined as the ratio of the number of detected malicious vehicles with respect to the total number of malicious vehicles with the increase of task number. The detailed simulation parameter settings is in Table 6.1.

6.5.1 Simulation Settings

We design a simulation to evaluate our proposed TripSense scheme in which only a set of key factors are considered and specified in order to validate the PM vehicles' sensing accuracy. It is worth noting that the selected factors are related to the movement of vehicles and the packets collision problems. In this case, we simulate the proposed scheme in the environment of MATLAB where there are a total number of n registered PM vehicles. To ensure the fairness, we suggest that each PM vehicle provides m times of sensing report in totally m independent tasks.

Table 6.1: Simulation Parameter Settings

Notation	Definition	Value
n	registered PM vehicle number	500
ρ	malicious PH vehicle proportion	20%
l_v	sensing accuracy level (SAL)	0.05;0.2;0.7;0.95
m	number of tasks for each PM vehicle	50
c_0	initial belief weight	1
c_1	forgetting factor parameter	1
c_2	variance sensitivity	10
c_3	forgetting factor parameter	1
T_0	initial trust score	0.5

6.5.2 Modeling the Sensing Behaviors of PM Vehicles

Due to the lack of real data, we need to model the behaviors of not only PM vehicles who take part in the sensing tasks, especially for malicious vehicles, in order to test the performance of our proposed scheme.

Sensing accuracy level (SAL) of PM vehicles: We define a parameter as sensing accuracy level (SAL) $l_v \in [0, 1]$ to describe the capability of a PM vehicle to provide high accuracy sensed data. A PM vehicle with higher l_v may submit more accurate sensing reports. Specifically, given a PM vehicle with l_v , we use the beta distribution to describe the performance quality variable X of that PM

vehicle, the probability density function of beta distribution can be expressed as:

$$f(x|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1} (1-x)^{\beta-1} \quad (6.14)$$

where $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx$. $f(x|\alpha, \beta)$ is the probability that a PH vehicle with SAL of l_v provides a service with the quality value of $x \in [0, 1]$. Higher values of l_v imply that the PH vehicle provides a higher quality service. To achieve this goal, we define α and β as follows:

$$\begin{aligned} \alpha &= c_2 \cdot l_v \\ \beta &= c_2 \cdot (1 - l_v) \end{aligned} \quad (6.15)$$

where c_2 is the parameter to control the variance of the distribution, when c_2 is given a larger value, the performance quality values will have a larger variance and vice versa. For a PH vehicle with SAL of l_v , the above model has the property of generating a service quality score which follows a beta distribution with the expectation $E(X) = l_v$. We define that the malicious vehicles are vehicles with SAL $l_v \leq 0.2$.

6.5.3 Simulation Results

Correctness

In this experiment, we target on comparing the trust scores between malicious and honest sensing PM vehicles with different sensing accuracy levels (SALs). For a better comparison, we choose two honest PM vehicles with FAL of $l_v = 0.7$ and $l_v = 0.95$ respectively. Besides, another malicious PM vehicles who provide corrupt sensed data are also put in the system. After “50” number of tasks, we plot their trust scores in Figure 6.3.

We notice that the trust scores of all PM vehicles converge after “30” tasks. It

Figure 6.3: Trust scores comparison between honest platoon member vehicles with $l_v = 0.7$, $l_v = 0.95$ and malicious PM vehicles with $l_v = 0.05$, $l_v = 0.2$

is obvious that the honest PM vehicles with $l_v = 0.7$ and $l_v = 0.95$ get the highest trust scores after the experiments, on the contrary, both of the attackers get the low trust scores. We also notice that a PM vehicle with larger SAL will achieve higher trust score, which shows the correctness of our trust model to identify PM vehicles according to their actual SALs.

Effectiveness

To demonstrate the effectiveness of our proposed scheme in detecting malicious PM vehicles. We define a proportion of $\rho = 20\%$ number of PM vehicles with the lowest l_v as “malicious PM vehicles”. After the $m = 50$ tasks, all PM vehicles will re-ranked, so the detection ratio is defined as the ratio of “malicious PM vehicles” who remain lowest 20% in the new ranking list.

Figure 6.4 depicts the detection ratio between our proposed trust-based sensing

Figure 6.4: Detection ratio comparison between sensing system with / without trust system

system with a sensing system without trust. From the figure, we can see that our proposed system's detection ratio increases quickly with the increase of task numbers, and after around 5 tasks, it will be convergent to 92%. On the contrary, for a sensing system without a trust system, the selection of sensing PM vehicle is random and the detection ratio remains as low as 20%. Therefore, the effectiveness of our proposed scheme has been demonstrated.

6.6 Related Work

Recently, several research works have appeared on trust and reputation management in VANET [3, 88, 31, 82], privacy preserving data aggregation [110, 111, 112] and crowdsensing [113, 106], which are closely related to the techniques in our proposed TripSense scheme.

For trust and reputation management, Zhang et al. have done a survey for effective trust management in VANET in [3]. Specifically, it discusses challenging issues for trust management caused by the important characteristics of VANET environments, and points out that robustness should be drawn particular attention. Patwardhan et al. present a distributed reputation management scheme for VANET, which enables vehicles to quickly adapt to changing local conditions and provides a bootstrapping method for establishing trust relationships [88]. However, their scheme is not quite scalable and robust. Different from traditional entity-based trust model, Raya et al. suggest a data-oriented trust establishment framework [31]. By combining trust values of each piece of data together, their framework deals well with ephemerality and functions well in sparse areas. However, in dense urban area, due to large amount of data, their framework is less efficient.

There has also been extensive work on data aggregation schemes in VANET [114, 115]. These works share the same assumption that vehicles or servers are trusted and the communications are secure, which, however, is not the case in real scenario. In reality, data can be eavesdropped and disclosed. Therefore, a lot of works have been done in privacy-preservation data aggregation [110, 111, 112]. Xing et al. have proposed M-PERM, a mutual privacy-preserving regression modeling approach to address the issue of keeping both participants and users data private while still utilizing them for analysis [110]. In this chapter, data are aggregated at each node and each cluster, finally at the user with maximum privacy protection. He et al. present two privacy-preserving data aggregation schemes for additive aggregation functions, which bridges the gap between collaborative data collection and data privacy [111]. Bilogrevic et al. have proposed a state-of-art privacy preservation framework to preserve data utility and simultaneously provide user privacy [112]. Users in this framework only contribute encrypted and aggregated model of their files to the aggregator to tackle trust and incentive

challenges.

Burke was the first to introduce the concept of participatory sensing, and describes an initial architecture to enhance data credibility, quality, privacy, and ‘shareability’ [113]. Ganti gives an overview of crowdsensing by introducing existing mobile crowdsensing applications and explaining their unique characteristics, illustrating various research challenges, and discussing possible solutions [106].

Combining the above privacy preserving data aggregation techniques and trust models together, our proposed TripSense scheme is focused on evaluating the platoon member vehicles’ sensing ability based on the accuracy of their historical sensed data. Specifically, there are several aspects which make our proposed scheme different: first, we establish a trust system as a long-term evaluating metric. Second, we make use of platoon head vehicles for authentication local data aggregation, which greatly reduces the communication overhead between vehicles and infrastructures and hence very suitable in VANET. Third, our proposed scheme is privacy-preserving on platoon member vehicles’ identities, locations and data.

6.7 Summary

In this chapter, we have proposed a trust-based privacy-preserving scheme for vehicular platoon crowdsensing, called TripSense. The proposed scheme mainly focuses on establishing a trust model to improve the sensed data reliability and accuracy of the whole system, while preserving the location and data privacy of sensing vehicle in the process of sensing vehicle selection, sensed data aggregation and evaluation. Detailed security analysis shows that the proposed TripSense scheme can not only achieve vehicle’s identity privacy, location privacy and data privacy, but also resists against adversary attacks on malicious sensing reports. Moreover, through extensive performance evaluation, we have demonstrated that our proposed scheme can achieve better sensing accuracy. In our future work, we

will consider more scenarios in crowdsensing rather than data aggregation. Besides, we may also consider the collusion among PM and PH vehicles to launch attacks in order to victimize other vehicles.

Chapter 7

Conclusions and Future Work

In this chapter, we summarize our contributions in this thesis and propose our future research work.

7.1 Contributions

The major contributions of this thesis can be summarized as follows:

First, a practical trust-based platoon service query scheme, called TPSQ, is proposed for vehicular communications in VANETs, which aims at enhancing the road safety and user comfort. A trust and reputation system is developed to distinguish platoon head vehicles according to their historical service qualities. By adopting our proposed scheme, querying vehicles are able to choose the most reliable platoon head vehicle to follow. Besides, parameters in the real scenario, e.g., the location of querying vehicles and platoon head vehicles, targeted destination and estimated time of arrival for the querying vehicles are included in the proposed scheme to make it more applicable as well as minimizing the computing time. In addition, TPSQ has demonstrated a high accuracy in distinguishing reliable platoon head vehicles.

Second, to help the user vehicles avoid choosing badly-behaved platoon head vehicles, a reliable trust-based platoon service recommendation scheme, called REPLACE, is presented for VANETs, where we have designed a reputation system at the core of REPLACE for the platoon head vehicles to collect their user vehicle's feedbacks and then model them using Dirichlet distribution. In addition, an iterative filtering algorithm is designed to deal with the untruthful feedbacks from user vehicles. Through security analysis and extensive performance evaluation, we have demonstrated that our proposed REPLACE scheme is secure and robust against badmouth, ballot-stuffing, newcomer and on-off attacks existed in VANETs.

Third, to make the two-hop vehicle-to-infrastructure communications reliable and secure in vehicular ad hoc networks, a robust trust-based relay selection scheme, called PTRS, is designed to ensure that only the trustworthy vehicles are selected as relays between a vehicle and infrastructure. Meanwhile, the location privacy of vehicles are preserved in PTRS scheme by using the technique of pseudonyms and trust levels instead of explicit reputation scores. Detailed security analysis is conducted, which shows that the proposed PTRS scheme is secure and robust against several sophisticated attacks in VANETs. In addition, a set of extensive simulations are carried out, demonstrating its effectiveness and accuracy.

Forth, a trust-based privacy-preserving scheme for vehicular platoon crowd-sensing, called TripSense, is proposed which is focused on establishing a trust model to improve the sensed data reliability and accuracy of the whole system, while preserving the location and data privacy of sensing vehicle in the process of sensing vehicle selection, sensed data aggregation and evaluation. Detailed security analyses have shown that the proposed TripSense scheme can not only achieve vehicle's identity privacy, location privacy and data privacy, but also resists against adversary attacks on malicious sensing reports. Moreover, through extensive performance evaluation, we have demonstrated that the proposed PTRS scheme can achieve better sensing accuracy.

7.2 Future Work

The approaches proposed in this thesis have partly solved some of the challenging issues in securing vehicular ad hoc networks. However, since vehicular ad hoc network is a promising platform in pervasive environments, there still exist several directions in which current research can be extended. Therefore, the following research topics will be investigated as a continuation of my Ph.D. thesis work.

1. *Improving robustness of trust system:* Though trust models we proposed are effective against malicious insider attacks, these trust models themselves could be attacked by stronger and more complicated attackers. Therefore, the robustness of trust models should be emphasized as much as possible. To be specific, in vehicular platooning system, the collusion of platoon head vehicles and platoon member vehicles has been very challenging and not been considered yet. Nevertheless, the damage of collusion attack in vehicular platooning system is massive. For example, in TPSQ scheme proposed in Chapter 3, once the platoon member vehicles collude with platoon head vehicles, they always provide positive evaluations to exaggerate the performance of malicious platoon head vehicles, and the trust system will be overturned. In TripSense scheme proposed in Chapter 6, when collusion attack happens, platoon head vehicles will select their partners to take the sensing tasks without the trust system. As a result, the corrupted data will be injected, which makes the final sensing result inaccurate. Mitigating these types of attacks and increasing the robustness of trust system has been a very urgent area.

2. *Achieving privacy and trust tradeoff in a more efficient way:* Despite the robustness of trust and reputation models, another research direction is achieving the tradeoff between trust and location privacy without introducing too much computational and communication costs. In Chapter 5 and Chapter 6, we proposed a way to solve this problem by introducing trust levels instead of trust scores. However, both schemes suffer from high computational costs since bilinear pairing

requires large amount of computation. In a word, how to propose lighter and more efficient schemes to achieve both privacy and trust deserves further investigations.

3. *Achieving data privacy and data reliability in vehicular crowdsensing:* Last but not the least, in the scenario of crowdsensing, our proposed scheme in Chapter 6 achieves data privacy which only considers the data aggregation. In the practical case, those sensed data could be manipulated in more complex ways rather than simply aggregations. Therefore, it will be an interesting area to develop schemes to preserve the data privacy and enable the complex manipulations of those data.

List of Publications

Journal Papers

1. H. Hu, R. Lu, and Z. Zhang, “*TPSQ: Trust-based platoon service query via vehicular communications*”, *Peer-to-Peer Networking and Applications*, pp. 1–16, 2015.
2. H. Hu, R. Lu, Z. Zhang, and J. Shao, “*REPLACE: A reliable trust-based platoon service recommendation scheme in VANET*”, accepted in *IEEE Trans. Vehicular Technology*.
3. H. Hu, R. Lu, C. Huang, and Z. Zhang, “*PTRS: A Privacy-Preserving Trust-based Relay Selection Scheme in VANETs*”, *Peer-to-Peer Networking and Applications*, 2016: 1–15.
4. H. Hu, R. Lu, C. Huang, and Z. Zhang, “*TripSense: A Trust-based Vehicular Platoon Crowdsensing Scheme with Privacy Preservation in VANETs*”, *Sensors*, 2016, 16(6): 803.

Conference Papers

1. H. Hu, H. Bao, and R. Lu, “*A Trust Framework for Social Networking on Highway*”, in *ITS Singapore Summit, Best Student Paper Award*, Singapore, Feb 12-14, 2015.
2. H. Hu, R. Lu, and Z. Zhang, “*VTrust: A robust trust framework for relay selection in hybrid vehicular communications*”, in *Proc. IEEE Globecom’15*,

San Diego, CA, USA, Dec. 6-10, 2015.

3. C. Huang, R. Lu, H. Zhu, H. Hu, and X. Lin, “*PTVC: Achieving Privacy-Preserving Trust-Based Verifiable Vehicular Cloud Computing*,” in *Proc. IEEE Globecom’16*, Washington, DC USA, Dec. 4-8, 2016.

Bibliography

- [1] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007. [Online]. Available: <http://iospress.metapress.com/index/ch4d4dg8yl2qhr0w.pdf>
- [2] R. Lu, “Security and privacy preservation in vehicular social networks,” Ph.D. dissertation, University of Waterloo, 2012. [Online]. Available: <https://uwspace.uwaterloo.ca/handle/10012/6623>
- [3] J. Zhang, “A survey on trust management for vanets,” in *25th IEEE International Conference on Advanced Information Networking and Applications, AINA 2011, Biopolis, Singapore, March 22-25, 2011*, 2011, pp. 105–112. [Online]. Available: <http://dx.doi.org/10.1109/AINA.2011.86>
- [4] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WM-N, VANET*. CRC press, 2010.
- [5] V. Kone, H. Zheng, A. I. T. Rowstron, and B. Y. Zhao, “On infostation density of vehicular networks,” in *Proceedings of the 5th Annual International Conference on Wireless Internet, WICON 2010, Singapore, March 1-3, 2010*, 2010, pp. 1–9. [Online]. Available: <http://dx.doi.org/10.4108/ICST.WICON2010.8533>
- [6] M. Kakkasageri and S. Manvi, “Information management in vehicular ad hoc networks: A review,” *Journal of Network and Comput-*

-
- er Applications*, vol. 39, pp. 334–350, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1084804513001434>
- [7] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Workshop on hot topics in networks (HotNets-IV)*, 2005, pp. 1–6.
- [8] M. RAYA, “Data-centric trust in ephemeral networks,” Ph.D. dissertation, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2009.
- [9] P. Papadimitratos, L. Buttyán, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, “Secure vehicular communication systems: Design and architecture,” *CoRR*, vol. abs/0912.5391, 2009. [Online]. Available: <http://arxiv.org/abs/0912.5391>
- [10] F. Kargl, Z. Ma, and E. Schoch, “Security engineering for vanets,” *Proc. 4th Wksp. Embedded Sec. in Cars*, pp. 15–22, 2006.
- [11] F. Kargl, P. Papadimitratos, L. Buttyán, M. Müter, B. Wiedersheim, E. Schoch, T. V. Thong, G. Calandriello, A. Held, A. Kung, and J. Hubaux, “Secure vehicular communication systems: Implementation, performance, and research challenges,” *CoRR*, vol. abs/0912.5393, 2009. [Online]. Available: <http://arxiv.org/abs/0912.5393>
- [12] H. Hartenstein and K. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164–171, 2008.
- [13] R. R. Brooks, S. Sander, J. Deng, and J. Taiber, “Automobile security concerns,” *IEEE Vehicular Technology Magazine*, vol. 4, no. 2, pp. 52–64, 2009.
- [14] C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” *IEEE Trans. Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2008.928581>

-
- [15] X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho, and X. Shen, "TSVC: timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Communications*, vol. 7, no. 12-1, pp. 4987–4998, 2008. [Online]. Available: <http://dx.doi.org/10.1109/T-WC.2008.070773>
- [16] R. Uzcategui and G. Acosta-Marum, "Wave: A tutorial," *Communications Magazine, IEEE*, vol. 47, no. 5, pp. 126–133, 2009.
- [17] *IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 10: Mesh Networking*, IEEE Std. IEEE P802.11s/D7.0, July 2010, 2010. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5595635>
- [18] P. Ranjan and K. K. Ahirwar, "Comparative study of vanet and manet routing protocols," in *Proc. of the International Conference on Advanced Computing and Communication Technologies (ACCT 2011)*, 2011.
- [19] V. Gokhale, S. Ghosh, and A. Gupta, "Classification of attacks on wireless mobile ad hoc networks and vehicular ad hoc networks," *Security of Self-Organizing Networks, Auerbach Publications: MANET, WSN, WMN, VANET*, p. 195, 2010.
- [20] J. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2001, October 4-5, 2001, Long Beach, CA, USA*, 2001, pp. 146–155. [Online]. Available: <http://doi.acm.org/10.1145/501416.501437>

-
- [21] J. Kong, X. Hong, and M. Gerla, "A new set of passive routing attacks in mobile ad hoc networks," in *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, vol. 2. IEEE, 2003, pp. 796–801.
- [22] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on inter vehicle communication systems-an analysis," *Proc. WIT*, pp. 189–194, 2006.
- [23] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*. Springer, 2002, pp. 251–260.
- [24] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268. [Online]. Available: <http://dl.acm.org/citation.cfm?id=984660>
- [25] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 29–37. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1023881>
- [26] G. Yan, S. Olariu, and M. C. Weigle, "Providing vanet security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, 2008. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0140366408000273>
- [27] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for vanets," in *Proceedings of the 66th IEEE Vehicular Technology Conference, VTC Fall 2007, 30 September - 3 October 2007, Baltimore, MD, USA*, 2007, pp. 26–30. [Online]. Available: <http://dx.doi.org/10.1109/VETEFCF.2007.22>
- [28] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in

-
- Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing.* ACM, 2005, pp. 46–57. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1062697>
- [29] M. Raya and J.-P. Hubaux, “Security aspects of inter-vehicle communications,” in *5th Swiss Transport Research Conference (STRC)*, no. LCA-CONF-2005-012, 2005. [Online]. Available: <http://infoscience.epfl.ch/record/33742>
- [30] T. Leinmüller, E. Schoch, and F. Kargl, “Position verification approaches for vehicular ad hoc networks,” *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, 2006. [Online]. Available: <http://dx.doi.org/10.1109/WC-M.2006.250353>
- [31] M. Raya, P. Papadimitratos, V. D. Gligor, and J. Hubaux, “On data-centric trust establishment in ephemeral ad hoc networks,” in *INFOCOM 2008. 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA*, 2008, pp. 1238–1246. [Online]. Available: <http://dx.doi.org/10.1109/INFOCOM.2008.180>
- [32] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Proceedings of the Fourth International Workshop on Vehicular Ad Hoc Networks, VANET 2007, Montréal, Québec, Canada, September 10, 2007*, 2007, pp. 19–28. [Online]. Available: <http://doi.acm.org/10.1145/1287748.1287752>
- [33] N. W. Lo and H. C. Tsai, “Illusion attack on vanet applications - a message plausibility problem,” in *2007 IEEE Globecom Workshops*, Nov 2007, pp. 1–8.
- [34] P. Louridas, “Some guidelines for non-repudiation protocols,” *ACM SIGCOMM Computer Communication Review*, vol. 30, no. 5, pp. 29–38, 2000. [Online]. Available: <http://dl.acm.org/citation.cfm?id=505676>

-
- [35] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, 2008.
- [36] H. Hu, R. Lu, and Z. Zhang, "TPSQ: Trust-based platoon service query via vehicular communications," *Peer-to-Peer Networking and Applications*, pp. 1–16, to appear. [Online]. Available: <http://link.springer.com/article/10.1007/s12083-015-0425-0>
- [37] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Vehicular Technology*, no. 99, 2016. [Online]. Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7466806>
- [38] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: A privacy-preserving trust-based relay selection scheme in VANETs," *Peer-to-Peer Networking and Applications*, pp. 1–15, 2016.
- [39] —, "TripSense: A trust-based vehicular platoon crowdsensing scheme with privacy preservation in VANETs," *Sensors*, vol. 16, no. 6, p. 803, 2016. [Online]. Available: <http://www.mdpi.com/1424-8220/16/6/803>
- [40] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Rubin, *Bayesian data analysis*. Taylor & Francis, 2014, vol. 2.
- [41] A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in *Proc. 7th Int. Workshop on Trust in Agent Societies*, vol. 6, 2004, pp. 106–117.
- [42] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference, Bled, Slovenia*, vol. 5, June 17 - 19, 2002, pp. 2502–2511.

-
- [43] A. Jøsang and J. Haller, “Dirichlet reputation systems,” in *Proceedings of the The Second International Conference on Availability, Reliability and Security, ARES 2007, The International Dependability Conference - Bridging Theory and Practice, April 10-13 2007, Vienna, Austria*, 2007, pp. 112–119. [Online]. Available: <http://dx.doi.org/10.1109/ARES.2007.71>
- [44] D. Gambetta *et al.*, “Can we trust trust,” *Trust: Making and breaking cooperative relations*, vol. 13, pp. 213–237, 2000.
- [45] A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167923605000849>
- [46] F. G. Mármol and G. M. Pérez, “Providing trust in wireless sensor networks using a bio-inspired technique,” *Telecommunication systems*, vol. 46, no. 2, pp. 163–180, 2011. [Online]. Available: <http://link.springer.com/article/10.1007/s11235-010-9281-7>
- [47] M. Dorigo and L. M. Gambardella, “Ant colony system: a cooperative learning approach to the traveling salesman problem,” *IEEE Trans. Evolutionary Computation*, vol. 1, no. 1, pp. 53–66, 1997. [Online]. Available: <http://dx.doi.org/10.1109/4235.585892>
- [48] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 15, 2008. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1362546>
- [49] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The eigentrust algorithm for reputation management in p2p networks,” in *Proceedings of*

-
- the 12th international conference on World Wide Web.* ACM, 2003, pp. 640–651. [Online]. Available: <http://dl.acm.org/citation.cfm?id=775242>
- [50] F. Gómez Mármol and G. Martínez Pérez, “Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1084804511000828>
- [51] F. G. Mármol, J. G. Marín-Blázquez, and G. M. Pérez, “Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks,” in *10th IEEE International Conference on Computer and Information Technology, CIT 2010, Bradford, West Yorkshire, UK, June 29-July 1, 2010*, 2010, pp. 838–845. [Online]. Available: <http://dx.doi.org/10.1109/CIT.2010.158>
- [52] J. K. Hedrick, D. McMahnnon, and D. Swaroop, “Vehicle modeling and control for automated highway systems,” *California Partners for Advanced Transit and Highways (PATH)*, 1993.
- [53] F. Browand, J. McArthur, and C. Radovich, “Fuel saving achieved in the field test of two tandem trucks,” *California Partners for Advanced Transit and Highways (PATH)*, 2004.
- [54] C. Bergenhem, Q. Huang, A. Benmimoun, and T. Robinson, “Challenges of platooning on public motorways,” in *17th world congress on intelligent transport systems*, 2010, pp. 1–12.
- [55] S. Tsugawa, S. Kato, and K. Aoki, “An automated truck platoon for energy saving,” in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2011*. IEEE, 2011, pp. 4109–4114.

-
- [56] C. Bergenheim, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, "Overview of platooning systems," in *Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012)*, 2012.
- [57] P.-H. Ho, Z. Zhang, and R. Lu, "Special issue on security and privacy preservation in vehicular communications wiley's security and communication networks journal," *Security and Communication Networks*, vol. 1, no. 3, pp. 191–193, 2008.
- [58] H. Guo, F. Yu, Z. Zhang, W.-C. Wong, M. Ma, and Y. Wu, "Hasvc: An efficient hybrid authentication scheme for vehicular communication," in *IEEE International Conference on Communications (ICC), 2011*. IEEE, 2011, pp. 1–5.
- [59] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications*. IEEE, 2008.
- [60] R. Lu, X. Lin, H. Zhu, X. S. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483–1493, 2010.
- [61] R. Mitchell and R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013.
- [62] T. Robinson, E. Chan, and E. Coelingh, "Operating platoons on public motorways: An introduction to the sartre platooning programme," in *17th world congress on intelligent transport systems*, vol. 1, 2010, p. 12.
- [63] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications*

-
- Surveys and Tutorials*, vol. 18, no. 1, pp. 263–284, 2016. [Online]. Available: <http://dx.doi.org/10.1109/COMST.2015.2410831>
- [64] D. Jia, K. Lu, and J. Wang, “A disturbance-adaptive design for vanet-enabled vehicle platoon,” *IEEE Trans. Vehicular Technology*, vol. 63, no. 2, pp. 527–539, 2014. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2013.2280721>
- [65] A. Tapani, “Vehicle trajectory effects of adaptive cruise control,” *Journal of Intelligent Transportation Systems*, vol. 16, no. 1, pp. 36–44, 2012.
- [66] A. Uchikawa, R. Hatori, T. Kuroki, and H. Shigeno, “Filter multicast: a dynamic platooning management method,” in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. IEEE, 2010, pp. 1–5.
- [67] M. Segata, B. Bloessl, S. Joerer, F. Dressler, and R. Lo Cigno, “Supporting platooning maneuvers through ivc: An initial protocol analysis for the join maneuver,” in *11th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2014*. IEEE, 2014, pp. 130–137.
- [68] R. Hall and C. Chin, “Vehicle sorting for platoon formation: impacts on highway entry and throughput,” *Transportation Research Part C: Emerging Technologies*, vol. 13, no. 5, pp. 405–420, 2005.
- [69] T.-S. Dao, C. M. Clark, and J. P. Huissoon, “Distributed platoon assignment and lane selection for traffic flow optimization,” in *Intelligent Vehicles Symposium, 2008 IEEE*. IEEE, 2008, pp. 739–744.
- [70] L. Xiao and F. Gao, “Practical string stability of platoon of adaptive cruise control vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1184–1194, 2011.

-
- [71] A. Kesting and M. Treiber, “How reaction time, update time, and adaptation time influence the stability of traffic flow,” *Computer-Aided Civil and Infrastructure Engineering*, vol. 23, no. 2, pp. 125–137, 2008.
- [72] Y. Zhang and G. Cao, “V-PADA: vehicle-platoon-aware data access in vanets,” *IEEE Trans. Vehicular Technology*, vol. 60, no. 5, pp. 2326–2339, 2011. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2011.2148202>
- [73] M. Amoozadeh, H. Deng, C. Chuah, H. M. Zhang, and D. Ghosal, “Platoon management with cooperative adaptive cruise control enabled by VANET,” *Vehicular Communications*, vol. 2, no. 2, pp. 110–123, 2015. [Online]. Available: <http://dx.doi.org/10.1016/j.vehcom.2015.03.004>
- [74] M. Segata, F. Dressler, and R. L. Cigno, “A modular approach to platooning maneuvers,” *Fachgespräch Inter-Vehicle Communication*, vol. 36, 2014.
- [75] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch, “Security architecture for vehicular communication,” in *Workshop on intelligent transportation*, 2007.
- [76] A. Michlmayr, F. Rosenberg, P. Leitner, and S. Dustdar, “End-to-end support for qos-aware service selection, binding, and mediation in vresco,” *IEEE Trans. Services Computing*, vol. 3, no. 3, pp. 193–205, 2010. [Online]. Available: <http://dx.doi.org/10.1109/TSC.2010.20>
- [77] C. Dellarocas, “Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior,” in *EC*, 2000, pp. 150–157. [Online]. Available: <http://doi.acm.org/10.1145/352871.352889>
- [78] A. A. Alam, A. Gattami, and K. H. Johansson, “An experimental study on the fuel reduction potential of heavy duty vehicle platooning,” in *13th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 2010. IEEE, 2010, pp. 306–311.

-
- [79] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016. [Online]. Available: <http://dx.doi.org/10.1109/MNET.2016.7437026>
- [80] R. Du, C. Chen, B. Yang, N. Lu, X. Guan, and X. Shen, "Effective urban traffic monitoring by vehicular sensor networks," *IEEE Trans. Vehicular Technology*, vol. 64, no. 1, pp. 273–286, 2015. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2014.2321010>
- [81] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Vehicular Technology*, to appear.
- [82] H. Hu, R. Lu, and Z. Zhang, "Vtrust: A robust trust framework for relay selection in hybrid vehicular communications," in *2015 IEEE Global Communications Conference, GLOBECOM 2015, San Diego, CA, USA, December 6-10, 2015*, 2015, pp. 1–6. [Online]. Available: <http://dx.doi.org/10.1109/GLOCOM.2014.7417027>
- [83] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Trans. Mob. Comput.*, vol. 11, no. 9, pp. 1514–1531, 2012. [Online]. Available: <http://dx.doi.org/10.1109/TMC.2011.160>
- [84] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Network and Service Management*, vol. 8, no. 2, pp. 79–91, 2011. [Online]. Available: <http://dx.doi.org/10.1109/TNSM.2011.050311.100028>
- [85] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Com-*

- [86] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Reputation systems,” *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.
- [87] L. Xu, L. Y. Wang, G. G. Yin, and H. Zhang, “Communication information structures and contents for enhanced safety of highway vehicle platoons,” *IEEE Trans. Vehicular Technology*, vol. 63, no. 9, pp. 4206–4220, 2014. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2014.2311384>
- [88] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, “A data intensive reputation management scheme for vehicular ad hoc networks,” in *3rd Annual International ICST Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MOBIQUITOUS 2006, San Jose, California, USA, July 17-21, 2006*, 2006, pp. 1–8. [Online]. Available: <http://dx.doi.org/10.1109/MOBIC.2006.340422>
- [89] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, “A trust modeling framework for message propagation and evaluation in vanets,” in *2010 2nd International Conference on Information Technology Convergence and Services (ITCS)*. IEEE, 2010, pp. 1–8.
- [90] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” *Computer Communications*, vol. 44, pp. 1–13, 2014. [Online]. Available: <http://dx.doi.org/10.1016/j.comcom.2014.02.020>
- [91] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in vanets,” *IEEE Trans. Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2011.2162864>

-
- [92] L. Buttyán, T. Holczer, and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in vanets,” in *Security and Privacy in Ad-hoc and Sensor Networks*. Springer, 2007, pp. 129–141.
- [93] R. Lu, X. Lin, and X. Shen, “SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks,” in *INFOCOM 2010. 29th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 15-19 March 2010, San Diego, CA, USA*, 2010, pp. 632–640. [Online]. Available: <http://dx.doi.org/10.1109/INFCOM.2010.5462161>
- [94] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang, “A reputation-based announcement scheme for vanets,” *IEEE Trans. Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2012.2209903>
- [95] J. Zhang, C. Chen, and R. Cohen, “Trust modeling for message relay control and local action decision making in vanets,” *Security and Communication Networks*, vol. 6, no. 1, pp. 1–14, 2013.
- [96] V. Daza, J. Domingo-Ferrer, F. Seb, and A. Viejo, “Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks,” *IEEE Trans. Vehicular Technology*, vol. 58, no. 4, pp. 1876–1886, 2009. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2008.2002581>
- [97] Q. Wu, J. Domingo-Ferrer, and . Gonzlez-Nicols, “Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,” *IEEE Trans. Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2009.2034669>
- [98] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, “A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant

-
- networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 22–32, 2014. [Online]. Available: <http://dx.doi.org/10.1109/TPDS.2013.36>
- [99] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, “SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks,” *IEEE Trans. Vehicular Technology*, vol. 58, no. 8, pp. 4628–4639, 2009. [Online]. Available: <http://dx.doi.org/10.1109/TVT.2009.2020105>
- [100] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, “Mixzone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks,” *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 9, pp. 4565–4575, 2013.
- [101] X. O. Wang, W. Cheng, P. Mohapatra, and T. F. Abdelzaher, “Artsense: Anonymous reputation and trust in participatory sensing,” in *Proceedings of the IEEE INFOCOM 2013, Turin, Italy, April 14-19, 2013*, 2013, pp. 2517–2525. [Online]. Available: <http://dx.doi.org/10.1109/INFCOM.2013.6567058>
- [102] K. L. Huang, S. S. Kanhere, and W. Hu, “A privacy-preserving reputation system for participatory sensing,” in *37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, October 22-25, 2012*, 2012, pp. 10–18. [Online]. Available: <http://dx.doi.org/10.1109/LCN.2012.6423585>
- [103] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, “Incognisense: An anonymity-preserving reputation framework for participatory sensing applications,” *Pervasive and Mobile Computing*, vol. 9, no. 3, pp. 353–371, 2013. [Online]. Available: <http://dx.doi.org/10.1016/j.pmcj.2013.01.003>
- [104] Q. Li and G. Cao, “Providing efficient privacy-aware incentives for mobile sensing,” in *IEEE 34th International Conference on Distributed Computing*

-
- Systems, ICDCS 2014, Madrid, Spain, June 30 - July 3, 2014*, 2014, pp. 208–217. [Online]. Available: <http://dx.doi.org/10.1109/ICDCS.2014.29>
- [105] B. Guo, Z. Yu, X. Zhou, and D. Zhang, “From participatory sensing to mobile crowd sensing,” in *2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom 2014 Workshops, Budapest, Hungary, March 24-28, 2014*, 2014, pp. 593–598. [Online]. Available: <http://dx.doi.org/10.1109/PerComW.2014.6815273>
- [106] R. K. Ganti, F. Ye, and H. Lei, “Mobile crowdsensing: current state and future challenges,” *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011. [Online]. Available: <http://dx.doi.org/10.1109/MCOM.2011.6069707>
- [107] K. L. Huang, S. S. Kanhere, and W. Hu, “Are you contributing trustworthy data?: the case for a reputation system in participatory sensing,” in *Proceedings of the 13th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2010, Bodrum, Turkey, October 17-21, 2010*, 2010, pp. 14–22. [Online]. Available: <http://doi.acm.org/10.1145/1868521.1868526>
- [108] A. Dua, N. Bulusu, W.-C. Feng, and W. Hu, “Towards trustworthy participatory sensing,” in *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, ser. HotSec’09. Berkeley, CA, USA: USENIX Association, 2009, pp. 8–8. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1855628.1855636>
- [109] G. Arfaoui, J. Lalande, J. Traoré, N. Desmoulins, P. Berthomé, and S. Gharout, “A practical set-membership proof for privacy-preserving NFC mobile ticketing,” *CoRR*, vol. abs/1505.03048, 2015. [Online]. Available: <http://arxiv.org/abs/1505.03048>

-
- [110] K. Xing, Z. Wan, P. Hu, H. Zhu, Y. Wang, X. Chen, Y. Wang, and L. Huang, “Mutual privacy-preserving regression modeling in participatory sensing,” in *Proceedings of the IEEE INFOCOM 2013, Turin, Italy, April 14-19, 2013*, 2013, pp. 3039–3047. [Online]. Available: <http://dx.doi.org/10.1109/INFOCOM.2013.6567116>
- [111] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. F. Abdelzaher, “PDA: privacy-preserving data aggregation in wireless sensor networks,” in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 6-12 May 2007, Anchorage, Alaska, USA*, 2007, pp. 2045–2053. [Online]. Available: <http://dx.doi.org/10.1109/INFOCOM.2007.237>
- [112] I. Bilogrevic, J. Freudiger, E. De Cristofaro, and E. Uzun, “What’s the gist? privacy-preserving aggregation of user profiles,” in *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II*. Springer, 2014, pp. 128–145.
- [113] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, “Participatory sensing,” *Center for Embedded Network Sensing*, 2006.
- [114] B. Yu, J. Gong, and C. Xu, “Catch-up: a data aggregation scheme for vanets,” in *Proceedings of the Fifth International Workshop on Vehicular Ad Hoc Networks, VANET 2008, San Francisco, California, USA, September 15, 2008*, 2008, pp. 49–57. [Online]. Available: <http://doi.acm.org/10.1145/1410043.1410053>
- [115] C. Lochert, B. Scheuermann, and M. Mauve, “Probabilistic aggregation for data dissemination in vanets,” in *Proceedings of the Fourth International Workshop on Vehicular Ad Hoc Networks, VANET 2007, Montréal*,

Québec, Canada, September 10, 2007, 2007, pp. 1–8. [Online]. Available:
<http://doi.acm.org/10.1145/1287748.1287750>