2012

SECURITY, PRIVACY AND APPLICATIONS IN VEHICULAR AD HOC NETWORKS

Zhengming Li
Michigan Technological University

SECURITY, PRIVACY AND APPLICATIONS IN VEHICULAR AD HOC NETWORKS

By
Zhengming Li

A DISSERTATION
Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
(Electrical Engineering)

MICHIGAN TECHNOLOGICAL UNIVERSITY
2012

This dissertation, “Security, Privacy and Applications in Vehicular Ad Hoc Networks,” is hereby approved in partial fulfillment of the requirements for the Degree of DOCTOR OF PHILOSOPHY IN ELECTRICAL ENGINEERING.

Department of Electrical and Computer Engineering

Signatures:

Dissertation Advisor _____

Dr. Chunxiao (Tricia) Chigan

Department Chair

_____

Dr. Daniel R. Fuhrmann

Date

To My Wife and Daughter.

Table of Contents

List of Figures

List of Tables

Preface

This dissertation reports my research work in pursuing the degree of Ph.D. in Electrical Engineering at Michigan Technological University. This dissertation includes 2 previously published journal articles in Chapter 2 and Chapter 3. The other chapters contain original and unpublished work. Here, my individual contribution to each previously published article is briefly summarized. The motivations and major contributions of this dissertation, which aims to further enhance the security, privacy and applications of Vehicular Ad Hoc Networks (VANETs), will be discussed in detail in the introduction chapter (Chapter 1).

Chapter 2 contains an article previously published in the Elsevier Journal of Ad Hoc Networks. As the first author, I identified the research topic which was to ensure reliable and trustworthy multi-hop communications in VANETs. Then, with the guidance of my advisor (the second author of this article) I completed most parts of algorithm design, analysis and simulation. The article itself was completed by me and my advisor.

Chapter 3 is an article previously published in the journal of Security and Communication Networks. As the first author, I identified the research topic which was to ensure resource-aware message verification in VANETs. I also completed most parts of algorithm design, analysis and simulation, with the guidance of my advisor (the second author of this article). The article itself was completed by me and my advisor.

Acknowledgements

I would like to thank my advisor, Dr. Chunxiao (Tricia) Chigan, for her continuous encouragement and insightful guidance for the last four years. Her guidance and help are indispensible to the successful completion of this dissertation. I would also like to thank my committee members (Dr. Jindong Tan, Dr. Zhijun Zhao and Dr. Nilufer Onder) for reviewing my research work and dissertation. Besides, my lab-mates and friends at MTU have been supporting me in both my research work and daily life. Especially, Congyi Liu and Dr. Chunming Gao have provided valuable suggestions regarding the structure and writing of my dissertation. Above all, I want to thank my wife and my daughter for their love and patience during these challenging years.

Abstract

With wireless vehicular communications, Vehicular Ad Hoc Networks (VANETs) enable numerous applications to enhance traffic safety, traffic efficiency, and driving experience. However, VANETs also impose severe security and privacy challenges which need to be thoroughly investigated. In this dissertation, we enhance the security, privacy, and applications of VANETs, by 1) designing application-driven security and privacy solutions for VANETs, and 2) designing appealing VANET applications with proper security and privacy assurance.

First, the security and privacy challenges of VANETs with most application significance are identified and thoroughly investigated. With both theoretical novelty and realistic considerations, these security and privacy schemes are especially appealing to VANETs. Specifically, multi-hop communications in VANETs suffer from packet dropping, packet tampering, and communication failures which have not been satisfyingly tackled in literature. Thus, a lightweight reliable and faithful data packet relaying framework (**LEAPER**) is proposed to ensure reliable and trustworthy multi-hop communications by enhancing the cooperation of neighboring nodes. Message verification, including both content and signature verification, generally is computation-extensive and incurs severe scalability issues to each node. The resource-aware message verification (**RAMV**) scheme is proposed to ensure resource-aware, secure, and application-friendly message verification in VANETs.

On the other hand, to make VANETs acceptable to the privacy-sensitive users, the identity and location privacy of each node should be properly protected. To this end, a joint privacy and reputation assurance (**JPRA**) scheme is proposed to synergistically support privacy protection and reputation management by reconciling their inherent conflicting requirements. Besides, the privacy implications of short-time certificates are thoroughly investigated in a short-time certificates-based privacy protection (**STCP2**) scheme, to make privacy protection in VANETs feasible with short-time certificates.

Secondly, three novel solutions, namely VANET-based ambient ad dissemination (**VAAD**), general-purpose automatic survey (**GPAS**), and **VehicleView**, are proposed to support the appealing value-added applications based on VANETs. These solutions all

follow practical application models, and an incentive-centered architecture is proposed for each solution to balance the conflicting requirements of the involved entities. Besides, the critical security and privacy challenges of these applications are investigated and addressed with novel solutions. Thus, with proper security and privacy assurance, these solutions show great application significance and economic potentials to VANETs.

Thus, by enhancing the security, privacy, and applications of VANETs, this dissertation fills the gap between the existing theoretic research and the realistic implementation of VANETs, facilitating the realistic deployment of VANETs.

Chapter 1 Introduction

This chapter introduces the background and the state-of-the-art of VANET-related research, based on which the research motivations and major contributions of this dissertation are presented.

1.1 VANETs

Transportation has huge impacts on the economic and human assets in modern societies. For instance, in the USA, in 2009 alone traffic accidents resulted in totally 30,797 deaths [1], and traffic congestion caused an economic cost of about $115 billion [2]. Thus, it is meaningful to enhance transportation safety and efficiency. One especially promising approach to this end is to integrate transportation systems with information technology in intelligent transportation systems (ITS) [3], where vehicular ad hoc networks (VANETs) have been envisioned as an indispensible component.

VANETs are special mobile ad hoc networks (MANETs) formed by smart vehicles. It is envisioned that in the future vehicles will become smart, in the sense that each vehicle will be equipped with information processing devices (on-board CPU), information collection devices (on-board sensors), on-board display devices as well as wireless communication devices [4]. Based on the nature of involved communications, VANETs generally consist of two domains [5]-[7] as shown in Figure 1.1: an *ad hoc domain* and an *infrastructure domain*.

The ad hoc domain is formed by smart vehicles which wirelessly communicate with one another (V2V) via dedicated short range communication (DSRC) [8] and wireless access in vehicular environments (WAVE) [9] technologies. Each vehicle (also called vehicular node, or simply node) will periodically (with a period between 100ms and 500ms) broadcast beacons containing its driving state, such as its current location, speed, and heading direction, to support road safety applications [10]. To provide security, each node will carry one or more certificates issued by a certificate authority (CA) in VANETs. A Tamper-proof device (TPD) [11] exists in each node to keep its cryptographic elements, for example private keys, secure and confidential.

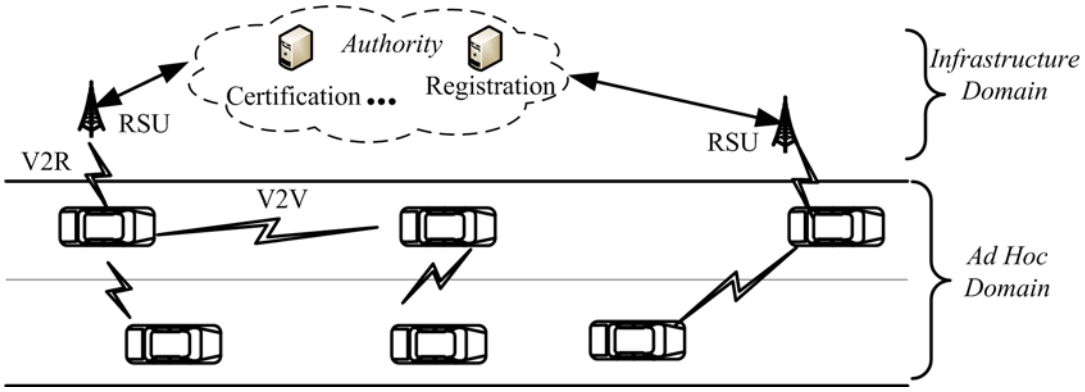

Figure 1.1 Exemplary VANET architecture

The infrastructure domain contains the managerial entities in charge of certification, registration, ID management, registration, and so on. Here, for brevity, all these entities are abstracted as the VANET *Authority*. The infrastructure domain also includes service providers for various applications, such as traffic management, traffic analysis, and location-based services (LBS) which are not shown in Figure 1.1 for brevity. Roadside units (RSUs) are deployed along road sides as vehicular nodes' access points to the infrastructure domain. Due to cost considerations, RSUs may be only sparsely deployed in VANETs, usually in road intersections or important downtown areas. Vehicle-to-roadside (V2R) communications are also based on DSRC [8] and WAVE [9]. The communications between RSUs and the infrastructure domain and within the infrastructure domain may adopt the existing mature communication technologies, such as WiMax, 3G, 4G, ATM and so on, which are out of the context of this dissertation.

With V2V and V2R communications, VANETs can greatly enhance traffic safety with applications such as collision avoidance, lane merge assistance, and so on [10]. Besides, VANETs provide an efficient approach to collect real-time traffic data from individual nodes [12], based on which traffic analysis and management can be further optimized. For instance, autonomous traffic control [13], [14] based on the real-time traffic data can be readily supported by V2R communications in VANETs. Eventually, VANETs provide a handy platform for information sharing among vehicles, based on which driving experience can be enhanced with applications such as ad dissemination [15], Internet on-the-wheel, on-road video game playing [16], and so on. Thus, VANETs open the door to numerous promising applications.

Due to VANET's application potentials, the Federal Communications Commission (FCC) specifically allocated 5,850 MHz to 5,925 MHz radio band to DSRC communications [17] in the USA, and in Europe the 5,725 MHz to 5,875 MHz Industrial, Scientific and Medical (ISM) band is allocated for DSRC communications [8]. Recently, US Department of Transportation (DoT), with various state DoTs, has been researching the technical and policy issues of VANETs in Vehicle-Infrastructure Integration (VII) [18] and later IntelliDrive [19]. The European Union also funds many research projects for VANETs, such as Secure Vehicular Communication (SeVeCom) [20], Cooperative Vehicle Infrastructure System (CVIS) [21], Adaptive Integrated Driver-vehicle InterfacE (AIDE) [22], E-safety Vehicle Intrusion Protected Applications (EVITA) [23], and Co-operative systems for intelligent road safety (COOPERs) [24], to name only a few. Among them, SeVeCom [20] aims to derive a threat model and a security architecture for VANETs; CVIS [21] aims to propose a universal communication module for VANETs based on Continuous Air Interface for Long and Medium Interface (CALM) [25], and propose realistic traffic safety applications. Japanese research mainly is focused on V2R communications [26]. Due to the relatively smaller area of European countries and Japan, their projects generally assume that V2R communications are pervasive in VANETs. However, in the USA RSUs may only be available in hot spots, such as downtown areas. Thus, the research projects in the USA generally are focused on V2V communications and only assume sparse V2R communications.

Recently, there is a trend of integrating various communication technologies in VANETs, as envisioned by CALM [25] and heterogeneous vehicular communications [27]. However, DSRC [8] and WAVE [9] are still commonly assumed to be the dominating technologies for V2V and V2R communications in VANETs. Thus, this dissertation only considers DSRC [8] and WAVE [9] in VANET communications.

1.2 Security and Privacy in VANETs

As distributed systems, VANETs also impose severe security and privacy challenges. Specifically, to fully realize the application potentials of VANETs, especially those of the traffic safety applications, security provisioning is necessary to ensure the proper functioning of VANETs. Otherwise, VANETs might become a handy tool to harm traffic

safety and traffic management [28]. For instance, by broadcasting false warnings about its emergent braking, one misbehaving vehicle may cause the vehicles behind itself to collide. Besides, the unique characteristics of VANETs, such as infrequent access to infrastructure, high node mobility, and precious assets at risk, to name only a few, make security provisioning more challenging than that of the general ad hoc networks [5].

Currently, many security schemes have been proposed for VANETs, among which the representative ones have been reviewed in our book chapter [5], as well as several existing surveys [4], [6], [7], [29]-[39]. Here, the existing security schemes are categorized and summarized according to their design goals. Detailed reviews on each individual scheme will be given later in the context of our proposed schemes.

Identity Management: In VANETs, to ensure message integrity, message authenticity, node authentication and node non-repudiation, identity management schemes are necessary to securely represent the identities of both vehicular nodes and RSUs. Briefly speaking, to prove its identity and its eligibility of participating in VANET communications, an entity needs a certificate issued by the VANET Authority. Besides the common public key cryptography techniques, several special digital signature techniques, such as group signature [40], ring signature [41], and identity-based signature [42], [43], can also be adopted in VANETs for identity management. For instance, [44] proposes an identity management framework for VANETs based on group signature. Still, many existing schemes [45]-[56] adopt a PKI-like approach to manage certificates, with various techniques to adapt to the unique characteristics of VANETs. In these schemes, certificate revocation list (CRL) distribution is necessary to evict the misbehaving nodes due to the relatively long lifetime of each certificate, which may incur heavy communication overhead. Thus, free of CRL distribution, short-time certificate schemes [57]-[60] are gaining popularity in VANETs. To ensure privacy-preserving node authentication, several anonymous authentication protocols [61], [62] have been proposed for VANETs. To detect the nodes which assume the identity of other nodes by launching the Sybil attack, several existing schemes [63], [64], [65] can be adopted.

Message Verification: To ensure message integrity and authenticity in VANETs, each node needs to verify the content [66]-[69] and digital signature of each received message. However, due to the numerous messages each node can receive, message verification

must be efficient and scalable. Among existing schemes, several schemes [45], [70], [71] attempt to reduce the resource required for verifying each message, while others [72]-[74] attempt to reduce the number of messages to be verified by each vehicle. So far, these schemes fail to ensure efficiency, security, and application-friendliness at the same time.

Cooperation Enhancement and Misbehavior Detection: In VANETs, it is necessary to detect the misbehaviors of any node to ensure reliable traffic safety applications and robust communications. Thus, several existing schemes [66]-[68], [75], [76] verify the content, for instance the location information, broadcasted by vehicular nodes; [77]-[81] rely on the watchdog mechanism to detect the routing and packet relaying behaviors in ad hoc networks, which may be adopted in VANETs. Besides, various incentives are adopted to encourage the cooperation of nodes in VANETs or general ad hoc networks, such as credit [82]-[84] and reputation [80], [85]-[88]. Several schemes [89]-[91] have been proposed to evict the misbehaving nodes from VANETs, usually with the cooperation of neighbors. So far, these schemes still fail to ensure reliable and faithful multi-hop communication in VANETs: watchdog-based schemes [77]-[81] generally perform badly in face of communication issues, while reputation or credit-based schemes [80], [85]-[88] cannot react fast enough to prevent the dissemination of invalid messages in VAENTs. Thus, a comprehensive solution to ensure reliable and faithful multi-hop communications is still needed to support various VANET applications.

Trust & Reputation: In VANETs and general networks, trust and reputation are a powerful tool to encourage node cooperation and punish node misbehaviors [92]. Currently, various trust model and metrics based on information theory [93]-[95], Bayesian theory [96]-[98], graph theory [99]-[101] and abstract algebra [102] have been proposed for general ad hoc networks and VANETs. The representative reputation schemes have been reviewed in [103], and in [104] the optimization of parameters in trust evaluation is discussed. Several trust schemes [105]-[107] for VANETs evaluate not only the cooperation of nodes but also the trustworthiness of the data itself, due to the importance of authentic data to VANETs.

In this direction, one remaining issue is to efficiently and reliably maintain the reputation history of vehicular nodes in the face of high node mobility and, potentially,

frequent pseudonym changes for privacy protection as discussed next. So far, only [108] begins to address this issue, with many issues still open.

Privacy Protection: The pervasive wireless vehicular communications and periodic beacons impose severe privacy issues [109]. By overhearing VANET communications, one powerful adversary may figure out the real identities of its interested nodes and profile them in terms of application accessing and personal information. Thus, several schemes [61], [62], [110] have been proposed to enable privacy-preserving node authentication in VANETs. Still, by overhearing the periodic beacons one adversary may collect the location history of any node. Thus, to protect the identity privacy of each node, each node may use pseudonyms instead of its real identity in VANET communications, as in [111]-[115]. Here, a pseudonym of one node is a temporary identifier without any obvious connection to its real identity, and a pseudonym usually consists of a certificate, a MAC address and an IP address. However, by collecting personal information and movement trajectory related to one pseudonym, an adversary may still derive the real identity of one node. Thus, frequent pseudonym change has been adopted in many schemes [116]-[127] to protect the location privacy of vehicular nodes and reduce the personal information revealed by any pseudonym. Briefly speaking, the major differences among these schemes [116]-[127] lie in the strategies of pseudonym changing. Especially, several schemes [128], [129] adopt the concept of mix [130], [131], so that vehicular nodes will change their pseudonyms to form mix zones for VANETs.

Besides pseudonym change, several special approaches for privacy protection exist in VANETs. For instance, [132] proposes that in contention-based forwarding each node should contend with a dummy distance to the destination, instead of its true locations, to protect location privacy. However, [132] ignores the periodic beacons in VANETs which will reveal the true location of each node anyway. [133] proposes that each node only sends out a fuzzy location in its beacons to protect its privacy, which may not be practical due to the safety risks. [134] proposes a pseudonym-less beaconing scheme for VANETs, based on secret keys shared by node groups. However, this scheme ignores the fact that the IP and MAC addresses of each node also form the pseudonym for this node.

Overall, the privacy protection for VANETs has been extensively studied. However, it is still necessary to investigate the interactions between privacy protection and other

security schemes, for instance reputation management. The conflicting requirements imposed by such schemes may make it challenging, if not impossible, for such schemes to coexist in VANETs. Besides, the existing privacy protection schemes mostly assume that each node has multiple pseudonyms at any time and can change them at will. However, privacy protection with other assumptions is still meaningful, since short-time certificates may still be implemented in VANETs in the future. Thus, it is meaningful to investigate privacy protection with short-time certificates.

General Security Topics: Besides the topics discussed above, several general security topics are still meaningful. For instance, [135] investigates the impact of VANET security on traffic safety, and [136] investigates geocast in VANETs and proposes a secure geocast protocol. [137] evaluates the performance of a basic VANET model implementing representative security schemes to identify new design issues for VANETs.

In summary, from the above reviews and discussions, several major open research issues for VANETs can be identified: reliable and trustworthy multi-hop communication, resource-aware and application-friendly message verification, as well as synergistic coexistence of multiple security schemes in VANETs. These open issues need to be investigated and properly solved to enable the imminent implementation of VAENTs, so they are the major concerns of this dissertation. Besides, existing security schemes and privacy protection schemes generally lack careful considerations of the realistic constraints imposed by VANETs. Thus, in this dissertation, special care will be taken to make our proposed schemes readily applicable to the realistic VANETs.

1.3 Envisioned Applications for VANETs

To exploit the pervasive vehicular communications, numerous applications have been proposed or envisioned for VANETs, including traffic safety applications, traffic management applications and value-added (commercial) applications.

Traffic safety applications are the primary justification for VANETs. Many traffic safety applications such as collision avoidance, lane change assistance, traffic light violation warning, and so on [10] have been proposed for VANETs. To support such applications, each node needs to periodically (with a period from 100ms to 500ms) broadcast beacons to indicate its driving states, including location, speed, driving

direction and so on, to its neighboring nodes [10]. Besides, warnings about traffic incidents should be disseminated to the vehicles which may be influenced by such incidents. Traffic safety applications and the incurred communications should be assigned the highest priority in VANETs.

Relying on V2V and V2R communications, real-time traffic statistics may be collected from vehicular nodes, based on which traffic monitoring and traffic management could be enhanced. For instance, autonomous traffic control [13], [14] can be cost-effectively supported with VANETs. The application of float car data collection [12] can also be cost-effectively supported with VANETs, where cellular communication from each vehicle to a central data center is not necessary. Smart traffic routing is envisioned in CVIS [21] based on V2V and V2R communications to improve traffic efficiency in downtown areas. Besides traffic statistics, VANETs provide a ready platform to collect environmental and weather information about the roads. For instance, Clarus [138] is a road weather management system proposed to this end.

Value-added (commercial) applications are gaining popularity in VANETs due to two reasons. First, such applications can attract more users to VANETs. Secondly, VANETs with V2V and V2R communications may enable more cost-effective solutions for such applications. For instance, in [139] a parking lot management system based on VANETs is proposed. On-road entertainment [16], [140], [141] is another promising value-added application for VANETs. With numerous nodes in VANETs, ad dissemination in VANETs [15] may be especially efficient and cost-effective.

In summary, VANETs show great application potentials, which will be further realized with new value-added applications in this dissertation.

1.4 Motivations and Contributions

As previously discussed, the open research issues form a great gap between the existing research and the realistic implementation of VANETs. Thus, the major research motivation of this dissertation is to fill this gap with 1) *application-driven security and privacy solutions* and 2) *applications with security and privacy assurance*. Driven by the realistic constraints of various VANET applications, we propose theoretically novel security and privacy solutions which are readily applicable to VANETs. On the other

hand, we propose new value-added applications for VANETs, which feature satisfying security provisioning and privacy protection. Thus, this dissertation greatly enhances the security, privacy and applications of VANETs.

Specifically, by identifying the root cause of unreliable multi-hop communications, we propose a lightweight reliable and faithful data packet relaying framework (LEAPER) [142] for VANETs. With LEAPER, reliable and faithful multi-hop communications, the basis of many VANET applications, can be ensured in various network scenarios. Additionally, by differentiating various messages, we propose a resource-aware message verification scheme (RAMV) [143], [144] to ensure secure and scalable message verification in VANETs which underlies the traffic safety applications.

To make privacy protection practical and compatible to other security schemes, we propose a joint privacy reputation assurance scheme (JPRA) [145], [146] to enable the efficient and synergistic coexistence of privacy protection and reputation management in VANETs. Besides, a short-time certificate-based privacy protection scheme (STCP2) [147] is proposed to protect the location privacy of vehicular nodes with short-time certificates. With JPRA and STCP2, privacy protection becomes both feasible and cost-effective in various VANET scenarios.

Three appealing solutions, namely general purpose automatic survey (GPAS) [148], [149], VANET-based ambient ad dissemination (VAAD) [150] and VANET-based vehicle performance monitoring and analysis (VehicleView) [151], [152] are proposed to support various value-added applications based on VANETs. Besides being efficient and cost-effective, these solutions all feature proper security and privacy assurance for the involved entities. Thus, being cost-effective, secure and privacy-preserving, these solutions can be readily implemented in VANETs.

Thus, by enhancing the security, privacy and applications of VANETs with both theoretic novelty and realistic solutions, this dissertation fills the gap between research and implementation, pushing VANETs further to the stage of massive deployment.

Chapter 2 Reliable and Trustworthy Multi-hop Communications[1]

In VANETs, reliable and trustworthy multi-hop communications are critical to many important applications. In this chapter, the root causes of unreliable and tampered multi-hop communications are identified, based on which a novel Adaptive Role Playing (ARP) strategy is proposed to tackle these issues with the cooperation of neighboring nodes. A Lightweight Reliable Faithful Data Packet Relaying Framework (LEAPER) [142] is proposed to implement the ARP strategy in each hop and ensure reliable and faithful multi-hop communications. In each hop the required security strength is configurable, making LEAPER flexible and adaptive to various application scenarios. Theoretical analysis and simulation studies show that LEAPER outperforms existing schemes in terms of communication overhead and security strength.

2.1 Introduction

Many VANET applications designed to enhance driving safety and convenience [10], [153], such as Accident Warning, Event Reporting, Car-to-Home Synchronization, and so on, rely on reliable and trustworthy multi-hop communications. However, in VANETs multi-hop communications (packet relaying) often suffer from various node misbehaviors and malfunctions such as packet tampering and packet dropping. For instance, the loss or tampering of a warning message about an accident may render the approaching vehicles unprepared for the potential dangers. Besides, tampered packets, once propagated throughout VANETs, are also a waste of the network resource.

Thus, *reliable* and *faithful* data packet relaying is vital to VANETs. Here, reliable relaying of a data packet means that this packet will be relayed by each intermediate relaying node; faithful relaying requires that the data packet will not be tampered. However, to our best knowledge, the existing schemes fail to meet both requirements as discussed in detail in section 2.2.

---

[1] The material contained in this chapter was previously published in the journal of *Ad Hoc Networks*. © 2011 Elsevier. See Appendix A for documentation of the permission to republish this material.

In this chapter a novel Adaptive Role Playing (ARP) strategy is proposed to allow the nodes in each hop to adaptively play the roles of a *relaying node* or *watchdog* monitoring the relaying node, based on their capabilities for such roles and their neighbors' behaviors. Thus, if one current role is not played honestly by a misbehaving or malfunctioning node, it will be taken over by the other honest nodes, so that the data packet will be faithfully relayed in each hop. As such, in principle ARP can prevent the malfunctioning and misbehaving nodes from directly affecting packet relaying in each hop, which is its major advantage over existing schemes. A **L**ightweight R**E**liable and F**A**ithful **P**acket R**E**laying F**R**amework (LEAPER) is proposed to securely implement the ARP strategy, organizing the nodes in each hop into a trust group where each node's behaviors are monitored by its neighbors. Thus, reliable and faithful data packet relaying can be ensured in each trust group, based on which end-to-end reliable and faithful packet relaying can be achieved.

Besides, a configurable *security threshold k* is adopted in LEAPER to determine the number of required watchdogs in each hop, tuning the tradeoff between the security strength and performance requirements in various application scenarios. Theoretic analysis and simulation studies prove LEAPER's salient merits compared to the existing schemes in face of misbehaving and malfunctioning VANET nodes.

2.2 Background & Related Work

2.2.1 Background

Here the problem of ensuring reliable and faithful packet relaying is considered in multi-hop communication scenarios where simplistic flooding [154] is not feasible due to the communication overhead involved. If one node needs to determine whether the received data packet is authentic or not, it has to depend on the information from its previous hop. Such a scenario is common in either urban areas or highways, so in this chapter the traffic models are not differentiated. Indeed, as we will show in section 2.5, the procedures of LEAPER in each hop will end within 100ms so that the network topology can be considered as being fixed during the concerned period. Thus, the merges and departures in the urban traffic model have no direct impact on the procedures of LEAPER and do not need to be considered.

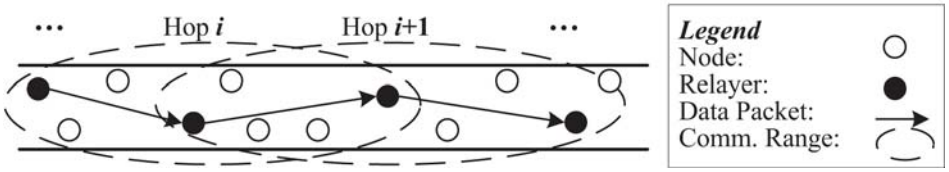

Figure 2.1 Exemplary relayers and watchdogs in VANETs

For brevity, following the conventions of [77], [155], in each hop the relaying node is called a *Relayer*. Due to the nature of wireless communications, the nodes within the communication range of the Relayer can overhear the data packet. Thus, as shown in Figure 2.1, the nodes within the communication ranges of both Relayers in hop i and hop (i+1) can verify whether the data packet sent by hop (i+1) is the same as that sent by hop i, functioning as the *watchdogs* for hop (i+1). These watchdogs can in turn inform the next hop of hop (i+1), namely hop (i+2), of their opinion about the data packet, so that hop (i+2) is able to know whether the data packet from hop (i+1) is authentic or not.

Thus, four *basic functions* critical to reliable and faithful data packet relaying can be abstracted in each hop: *data reception*, *data verification*, *data transmission* and *proof presenting*, as shown in Figure 2.2. In data reception, the nodes in one hop (say hop i) receive or overhear the data packet (D_{i-1}) from the previous hop. These nodes need to verify the authenticity of D_{i-1} based on the proof presented by the previous hop with the data verification function. D_{i-1}, if regarded as authentic, will be transmitted to hop (i+1) in the form of D_i by the Relayer in hop i. Similarly, in proof presenting the nodes in hop i need to present the proof of the authenticity of D_i, usually constructed and vouched for by the watchdogs of hop i, to hop (i+1). As such, these four basic functions can establish the trust of the data packet's authenticity between any two consequential hops. Thus, these basic functions are all indispensible, and the failure of any one may result in either data tampering or packet dropping in VANETs.

However, multiple node misbehaviors (attacks) may result in the failure of these basic functions, as shown in Figure 2.2. These common attacks have been thoroughly investigated in [155], with their impacts summarized in Table 2.1. VANET nodes may also fail to perform these basic functions due to malfunctions such as collision, interference and random errors in packet transmissions, as shown in Figure 2.2.

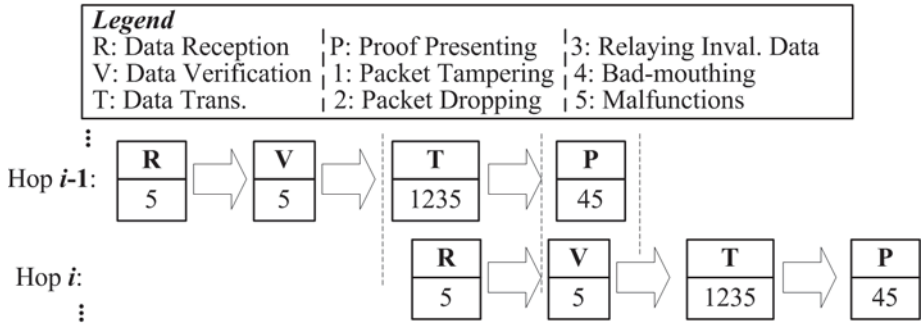

Figure 2.2 Basic functions, failures and attacks in each hop

Thus, in order to ensure reliable and faithful data packet relaying, the negative impacts of the individual node's misbehaviors and malfunctions on the four basic functions need to be prevented. To this end, a novel *Adaptive Role Playing* (*ARP*) strategy is proposed here. The core idea of ARP is to allow the nodes in each hop to contend to perform the four basic functions, adaptively playing the role of either Relayer or watchdog according to their capability and their neighbors' roles. Thus, if the current Relayer or watchdog fails to properly function, its role will be taken over by the other honest nodes in the same hop and the basic functions associated to this role will be successfully performed. As such, all basic functions in this hop will be successfully performed.

Table 2.1
Common attacks to data packet relaying

Attacks	**Impacts**
Packet Dropping	The Relayer simply refuses to relay the data packet.
Packet Tampering	The Relayer tampers the data packet before relaying it.
Relaying Invalid Data	The Relayer intentionally relays data packets tampered by its previous hop.
Badmouthing	Watchdog either gives positive evaluation to tampered data packets or negative evaluation to authentic data packets.

ARP will ensure more reliable and faithful data packet relaying than the commonly adopted strategy [77], [155]-[157] where the roles of Relayer and watchdog are rigidly assigned to specific nodes, as further discussed next.

2.2.2 Related Work

The routing protocols initially designed for general ad hoc networks, such as DSR [158] and AODV [159], are prone to performance degradation in VANETs due to the high node mobility. GPSR [156] selects the node nearest to the destination as the Relayer in

each hop, so any malfunction or misbehavior of the Relayer will result in packet loss or packet tampering. Thus, in GPSR neither reliability nor faithfulness is ensured.

Several routing schemes specifically proposed for VANETs, including PBF [157], CBF [160], [161], OPERA [162], and REAR [163], all ignore node misbehaviors, so faithful data packet relaying cannot be ensured in such schemes. Moreover, PBF [157], similar to GPSR [156], in each hop selects the node nearest to the destination as the specific Relayer, so it cannot ensure reliable data packet relaying either. CBF [160], [161] allows each node that overhear the data packet to set up a timer based on its distance to the destination, and the node with the shortest timeout period will serve as a Relayer. Thus, CBF could handle the packet dropping and nodes' malfunctions, ensuring reliable packet relaying. Similarly, in REAR [163] the nodes also contend to relay the data packets according to each node's reception probability, so reliable data packet relaying can also be achieved. OPERA [162] is focused on carrying data packets across network segmentations, without considering reliable and faithful data packet relaying in each hop.

Besides, several security schemes [77]-[80], [155] proposed to handle misbehaviors in data packet relaying generally fail to ensure reliable data packet relaying, relying on a specific Relayer in each hop. Specifically, the reputation schemes [78]-[80] update the reputation of each node based on its data packet relaying and routing behaviors with the help of watchdogs. These schemes may not be effective in VANETs, since 1) in VANETs nodes' reputation history is difficult to maintain, and 2) the tampered data packets can still get propagated during the reputation update periods. DTT [77] uses the previous hop of the Relayer as the watchdog to monitor the Relayer and detect data tampering. In each hop only one pre-selected watchdog exists, so DTT is prone to badmouthing attack, as discussed in [155]. To enhance DTT [77], AWF-NA [155] autonomously organizes several nodes around the Relayer as the watchdogs. It thus is resistant to the badmouthing attack. However, in AWF-NA [155] each node has to maintain the information of all neighbors within its 2 hops, which incurs heavy control overhead. Additionally, AWF-NA relies on the special connectivity model provided by RPB-MAC [164], which has not been commonly adopted in VANETs.

In summary, the existing schemes cannot ensure both reliable and faithful data packet relaying in VANETs, and LEAPER will achieve both goals with the ARP strategy.

2.3 LEAPER

2.3.1 Overview of LEAPER

LEAPER is proposed to enable the nodes in each hop to securely follow the ARP strategy to ensure reliable and faithful data packet relaying. To this end, LEAPER organizes the nodes in each hop into a trust group (*TG*), as shown in Figure 2.3. Each trust group (say TG_i) receives the data packet (D_{i-1}) and the total trust token (T_{i-1}) from its previous trust group (TG_{i-1}). Here T_{i-1} is the proof of the authenticity of D_{i-1} presented by TG_{i-1}. Thus, each node in TG_i knows both D_{i-1} and T_{i-1}, as shown in the bracket above TG_i in Figure 2.3. All nodes in TG_i can thus follow the ARP strategy to relay the data packet (denoted as D_i) and the associated total trust token (T_i) to the next hop. During this process, each node in TG_i is able to detect any malfunction or misbehavior of its neighbors, so that together the nodes in TG_i will ensure that only the authentic D_i and T_i will be sent out. Eventually, after D_i and T_i are received by the nodes in the next hop, such nodes can form a new trust group TG_{i+1} to further relay the data packet.

In the above process, the nodes in TG_i not only know that the Relayer in TG_i has already faithfully relayed the packet by comparing D_{i-1} with D_i, but also know in the first place that D_{i-1} itself is authentic with the help of T_{i-1}. Thus, by following the ARP strategy, each trust group can reliably and faithfully relay the data packet to the next hop. The relations between the four basic functions and the trust groups are self-evident: by relaying D_i to TG_{i+1}, TG_i is performing the *data transmission* function, and TG_{i+1} is performing the *data reception* function; while by relaying T_i to TG_{i+1}, TG_i is performing the *proof presenting* function, and TG_{i+1} is performing *data verification*.

Before introducing LEAPER in detail, the assumptions of this chapter will be clarified.

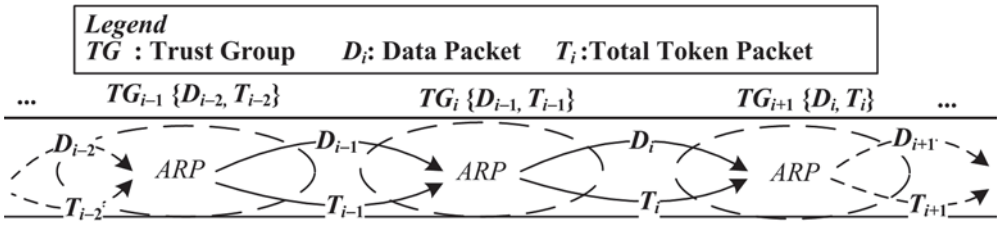

Figure 2.3 The relation of trust groups and ARP procedures

- The routing information is present in the data packet, as in geographic routing protocols and the source routing protocols, such as DSR [158].
- Each node is able to verify the IDs and the corresponding public keys of its neighbors, with the help of IBS [165] or any PKI-based key management schemes.
- From the source to the destination the node density is sufficient to support LEAPER. Network segmentations could be handled by adopting the robust message dissemination schemes, for example [162] and [166], into LEAPER.

2.3.2 Detailed Procedures

The detailed procedures of LEAPER are designed for the nodes in each trust group to collectively follow the ARP strategy. For clarity, the procedures in any trust group i are divided into three phases: *data packet relaying*, *single token collecting* and *total token relaying*. In these phases, t_S and t_E are used to indicate the start and end time, respectively. Each node will set up three distance-sensitive timers, namely Data Contention Timer (T_DCT), Single Token Timer (T_STT) and Total Token Timer (T_TTT), in these three phases respectively, to coordinate its interactions with the neighbors. The timing algorithms of these timers will be discussed in details in subsection 2.4.1.

Phase I: Data Packet Relaying.

In this phase the nodes contend to perform the *data transmission* function. As shown in t_S of Figure 2.4, nodes in TG_i have all received D_{i-1} and T_{i-1} from TG_{i-1} at the beginning of this phase. Each node in TG_i will set up its T_DCT timer with timeout period inversely proportional to its distance to the Relayer in TG_{i-1}. The timeout period of each timer is figuratively indicated by the length of the shadowed bar beside each node in Figure 2.4, Figure 2.5 and Figure 2.6. The node (say n_i) whose T_DCT expires first will send out the data packet (D_i) to next hop. Other nodes in TG_i can overhear D_i, and check D_i against D_{i-1}, as shown in t_E of Figure 2.4. If D_i is authentic, the role of Relayer has been faithfully played by n_i and the other nodes in TG_i will move on to contend to play the role of watchdogs. Specifically, the other nodes in TG_i will cancel their T_DCT timers and set up T_STT timers for Phase II. Otherwise, D_i will simply be discarded and Phase I will continue until one node finally relays an authentic data packet to the next hop.

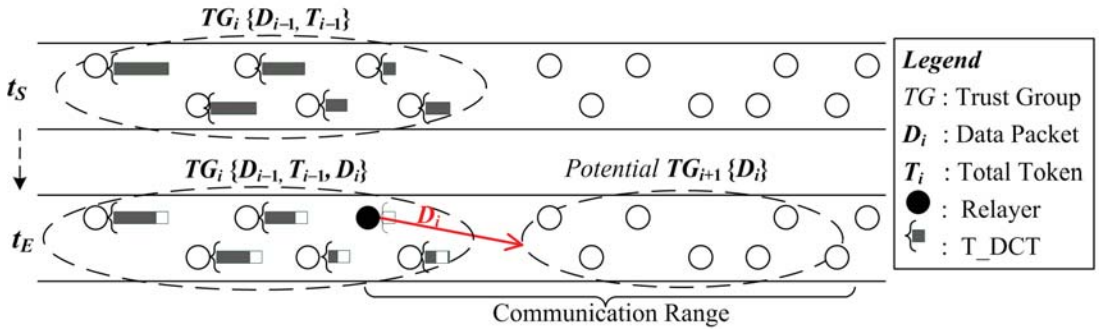

Figure 2.4 The procedures of Phase I (data packet relaying)

In Phase I, all the different copies of D_i from TG_i have been overheard by the nodes in the potential TG_{i+1}, as shown in t_E of Figure 2.4.

Phase II: Single Token Collecting.

In this phase, each node in TG_i will contend to send out its own proof of the authenticity of D_i, called *single trust token* here, based on which a total trust token T_i can be constructed by TG_i. At the beginning, each node in TG_i has already set up its own T_STT timer with timeout period proportional to its distance to the Relayer in TG_i, as shown in t_S of Figure 2.5. Whenever the T_STT timer of a node n_j expires, it will play the role of a watchdog and send its single token packet TS_j to the current Relayer, as shown in t_E. On the other hand, TS_j will be overheard and recorded by all the nodes in TG_i. After k such single token packets are thus generated, the still running T_STT timers will be cancelled and Phase II will come to an end.

Here k is the *security threshold* used to define the number of required watchdogs in each trust group, to handle the badmouthing attacks of individual watchdogs. The configuration of k will be discussed in detail in subsection 2.4.3.

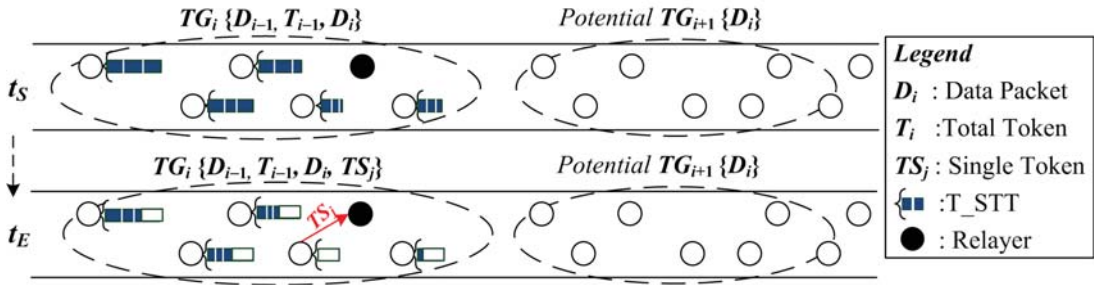

Figure 2.5 The procedures of Phase II (single token collection)

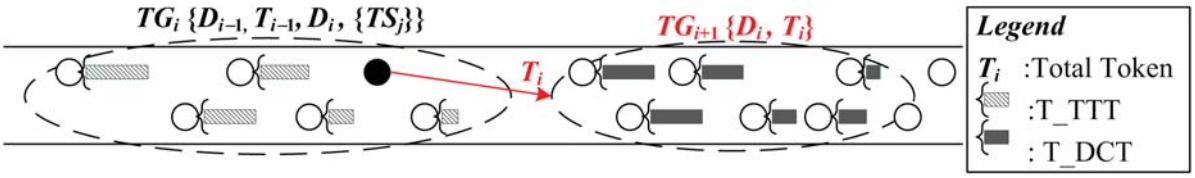

Figure 2.6 The procedures of Phase III (total token relaying)

Phase III: Total Token Relaying.

In this phase TG_i as a whole presents its total trust token T_i, as a combination of k single trust tokens, to the potential TG_{i+1}. At the beginning, each node in TG_i has overheard k single trust tokens, and each node will set up its own T_TTT timers with timeout periods proportional to its distances to the Relayer in TG_i, as shown in Figure 2.6 (with similar legends as Figure 2.5). Thus, the Relayer itself will set up a T_TTT timer with period 0, and it is supposed to send T_i to next hop immediately. If the Relayer fails to send out T_i when the T_TTT timer of another node expires, this node will send out T_i. Once T_i is sent out, Phase III in TG_i comes to an end. Meanwhile, TG_{i+1} is automatically formed by the nodes in the next hop which have overheard both D_i and T_i.

Thus, in Phase I TG_i performs the data transmission function and TG_{i+1} performs the data reception function; in Phase II and Phase III TG_i completes the proof presenting function and TG_{i+1} completes the data verification function. As such, by the cooperation of the neighboring node, reliable and faithful data packet relaying is ensured in each trust group. The packet dropping attack is effectively handled, and the tampered data packet will be stopped from being further propagated in VANETs.

2.4 Enabling Techniques

Several enabling techniques of LEAPER, including the distance-sensitive timers, the secure packet format and the security threshold k, will be described in detail here.

2.4.1 Distance-Sensitive Timers

As shown in subsection 2.3.2, the distance-sensitive timers T_DCT, T_STT and T_TTT serve to control the contention of the nodes in each trust group to relay data packet, generate single trust token and total trust token, respectively. Here the timing algorithms of these timers will be designed so that in each phase of LEAPER the desirable node interaction can be ensured.

Let R be the communication range of VANET nodes. For a node (n_i) in trust group i (TG_i), let d_1 and d_2 be the distances of n_i to the Relayers in TG_{i-1} and TG_i, respectively.

T_DCT Timer: In Phase I it is desirable that the node farthest from the Relayer in TG_{i-1} will relay the data packet, so that the data packet could geographically go as far as possible in one hop. With this consideration, the timeout period (T_{DCT}) of the T_DCT timer of n_i will be:

$$T_{DCT} = \begin{cases} \left[2 + uni(2)\right]\tau_0 & d_1 \le R/2 \\ \left[2 \times \left|d_1 - R\right| / R + uni(1)\right]\tau_0 & R/2 < d_1 < (3R)/4 \\ \left[\left|d_1 - R\right| / R + uni(1)\right]\tau_0 & d_1 \ge (3R)/4 \end{cases}. \quad (2.1)$$

Here $uni(x)$ is a uniform random function over [0, x], and τ_0 is the basic timeout period which should be set based on application requirements. Nodes with different d_1 are differentiated by three cases in (2.1), so that their timeout periods will be significantly different to avoid collisions in transmission. Thus, with (2.1) the node farthest to the Relayer in TG_{i-1} will be most likely to get the smallest T_{DCT} and relay the data packet first.

T_STT and T_TTT Timers: As shown in Phase II and Phase III, these timers should favor the nodes nearest to the Relayer in TG_i, so that in TG_{i+1} the nodes overhearing D_i will also overhear T_i and the size of TG_{i+1} can thus be maximized. Let T_{TT} be the timeout period of the T_STT or T_TTT timer of node n_i, and it could be determined as follows:

$$T_{TT} = \left[d_2 / r + uni(0.5)\right]\tau_0 \quad (2.2)$$

Equation (2.2) indicates that the nearer n_i is to the Relayer in TG_i, the smaller T_{TT} tends to be. $uni(0.5)$ is used to randomize the T_{TT} of the nodes with similar d_2. Thus, with (2.2) T_STT and T_TTT timers will ensure that the nodes nearer to the Relayer in TG_i are more likely to win the contentions in Phase II and Phase III of LEAPER.

VANET nodes may have different communication ranges, but even in such a case a Relayer and k watchdogs can still be adaptively selected in any trust group. Two nodes might have similar timeout periods for one timer, which may lead to duplicate packets or packet collision. However, the probability of this scenario is quite small and LEAPER could tolerate duplicate or lost data (token) packets. Besides, such a scenario could be ameliorated by the joint-layer design [167] of MAC and network layers.

2.4.2 Secure Packet Format

To prevent packet forging and packet replay in LEAPER, secure packet formats are proposed here for the data packet, single trust token and total trust token.

Data Packet: {*Payload* = {*R_ID, Type, TSP, S_ID, P_ID, M*}, {*Hash*(*Payload*)}PR_{R_ID}, $Cert_{R\_ID}$}.

Here, *R_ID* is the ID of the Relayer and *Type* indicates the packet type. *S_ID* is the ID of the source node of this data packet, and *P_ID* is the packet ID assigned by the source node. *TSP* is the timestamp generated by the Relayer, and *M* is the application-specific message contained in this data packet. {*Hash*(*Payload*)}PR_{R_ID} is the digital signature of the hash value of *Payload* generated with the Relayer's private key PR_{R_ID}. Here, *Hash*() is a standard hash function, such as SHA-2 [168]. $Cert_{R\_ID}$ is the certificate of the Relayer.

Single Trust Token: {*Payload* = {*G_ID, Type, TSP, DP_ID*}, {*Hash*(*Payload*)}PR_{G_ID}, $Cert_{G\_ID}$)}.

Here, *G_ ID* is the ID of the generator of this single trust token. *DP_ID*={*Rel_id, S_id, P_id*} of the data packet to be vouched for. The other items have similar meanings as those in the data packet. Thus, after receiving a single trust token any node can figure out its generator and the associated data packet.

Total Trust Token: {*Payload* = {*T_ID, Type, Tsp, K,* ST_1, …, ST_k}, {*Hash*(*Payload*)}PR_{T_ID}, $Cert_{T\_ID}$)}.

Here, *T_ID* is the ID of the generator of this total trust token. ST_i is the *i*th single trust token embedded in this packet. Thus, after receiving this packet, any node can easily figure out for which data packet this total trust token is generated and whether it contains enough single trust tokens.

The verification of the certificate and signature in these packets can be performed following the standard procedures in any common PKI schemes. Exemplary procedures can also be found in [77], [155], so for brevity they will not be discussed in detail here. Note here the pseudonyms, instead of real node IDs, of vehicular nodes can be used in these packets. Thus, LEAPER is also compatible to the common privacy protection schemes where each node usually uses a pseudonym in VANET communications and changes its pseudonym from time to time, as introduced in Chapter 1.

2.4.3 Security Threshold

The security threshold k mandates the number of required watchdogs in each trust group, so it has significant impact on the security strength and performance of LEAPER. Specifically, bigger k will make each trust group more resistant to the misbehaving watchdogs and meanwhile incur higher communication overhead with more single trust tokens collected. Thus, it is critical to set a proper k in LEAPER to achieve desirable tradeoff between the security strength and communication overhead.

Here we investigate the feasible range of k determined by the application requirements and VANET environments. Specifically, per-hop latency (T_d) and per-hop successful delivery ratio (SDR) P_S as application requirements, and the average node density (λ) as VANET parameter are carefully investigated here. The constraints of these factors on the feasible values of k are summarized in Table 2.2.

First, k must be fewer than the number of nodes in a typical trust group, which is determined by node density (λ), the length of the trust group (L) and number of lanes (n_l). For any specific application targeted at one specific area, λ, L and n_l all can be estimated and the feasible range of k can thus be obtained.

Secondly, each single packet will incur a certain latency, including average MAC access time (τ_m), signature creation time (τ_s) and signature verification time (τ_v). The total delay caused by 1 data packet ($\tau_m+\tau_v+\tau_s$), k single trust tokens ($k\tau_m+k\tau_v+\tau_s$) and 1 total trust token ($\tau_m+(k+1)\tau_v+\tau_s$) must be shorter than T_d. Thirdly, more than k+1 misbehaving nodes in a trust group could collude to relay a tampered data packet to the next hop. Thus, k must be big enough to make it practically impossible to have k+1 misbehaving nodes in a trust group.

Table 2.2
Constraints on security threshold k

Factors	**Constraints**
#. Neighbors	$k \le \lambda \times L \times n_l$
Delay per Hop (T_d)	$(k+2)\tau_m + (2k+2)\tau_v + 3\tau_s \le T_d$
Per-hop SDR(P_S)	$Pr\{$less than k+1 misbehaving nodes in a hop$\} \ge P_S$

Within the feasible range as determined above, the value of k has significant impacts on the tradeoff of the security strength and performance of LEAPER, as will be investigated in detail in section 2.5.

2.5 Performance Analysis and Evaluation

Here the salient security properties of LEAPER will be identified and justified, and the performance of LEAPER will be evaluated both analytically and based on simulation.

2.5.1 Trust Group Size

LEAPER requires that at least k+1 nodes (one Relayer and k watchdogs) exist in any trust group, so the trust group size has direct impacts on the performance of LEAPER. Here the trust group length will be estimated, since the trust group size is proportional to the trust group length given a node density. Additionally, the trust group length can also show geographically how far a data packet can be relayed in each hop.

As shown in Figure 2.7, let L_{i-1} and L_i be the lengths of two adjacent trust groups TG_{i-1} and TG_i, respectively. Then the Relayer (A) and the node (B) relaying the total trust token in TG_{i-1} must lie within aL_{i-1} from the joint point of TG_{i-1} and TG_i, where $a \in [0,1]$. Thus from the procedures of LEAPER we know that L_{i-1} and L_i have the following relation:

$$aL_{i-1} + L_i = R. \tag{2.3}$$

The expectations of both L_{i-1} and L_i should be equal, so it follows from (2.3) that

$$E[L_i] = R \times 1/(1+a). \tag{2.4}$$

Ideally, with the help of the distance-sensitive timers a can be 0, and $E[L_i] = R$ from (2.4). Even in the worst scenario where R and T are exactly at the opposite sides of TG_{i-1} (a=1), $E[L_i]$ is still $R/2$ from (2.4). Thus, $E[L_i]$ is between $R/2$ and R, ensuring at least the data packet geographically be relayed over a distance of $R/2$ in each hop. According to WAVE [9], R typically is 300m-1000m, which indicates the lower bound of $E[L_i]$ can allow each trust group to contain enough nodes given a reasonable node density.

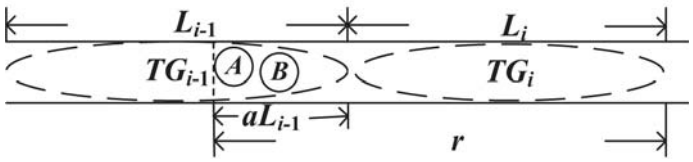

Figure 2.7 Estimation of the expected length of a trust group

2.5.2 Security Properties of LEAPER

With adequate nodes in each trust group, LEAPER shows salient security properties against the misbehaving or malfunctioning nodes. With the ARP strategy the nodes in each trust group contend to be the Relayer and watchdogs, so that the malfunctioning nodes have no direct impact on data packet relaying. Meanwhile, the common node misbehaviors in Table 2.1 can also be effectively handled by LEAPER.

In case of *packet dropping* by any node in a trust group (TG_i), the other honest nodes in TG_i can still relay the data packet to next hop, as discussed in Phase I of LEAPER. Similarly, if any node relays a tampered data packet in TG_i, this tampered packet can be detected and discarded by the honest nodes in TG_i. Thus, both *packet tampering* and *intentionally relaying tampered packet* can be effectively handled in each trust group.

In case of the *badmouthing* attack, the misbehaving watchdogs can generate single trust tokens for a tampered data packet. However, to convince the next hop, there must be k+1 misbehaving nodes (one Relayer and k watchdogs) in this trust group (TG_i), which will be quite unlikely with $k > 0$. Even if k+1 misbehaving nodes do exist in TG_i, the remaining honest nodes in TG_i can still relay the authentic data packet and the associated total trust token to the next hop. Besides, by monitoring the network environments, the applications could adaptively increase k in case of more misbehaving nodes, to make the badmouthing attack practically impossible.

Additionally, LEAPER is also effective in ensuring data validity in the source node, which is in trust group 0 (TG_0). In case of personal communications, it is sufficient for LEAPER to ensure reliable and faithful packet relaying in the intermediate hops. However, in case of data packets with public information, such as warnings about traffic jams or accidents, LEAPER can also ensure that TG_0 will only generate and send out data packets with valid content. Specifically, to send out invalid data packets and convince the next hop, the number of misbehaving nodes in TG_0 must be bigger than k+1 (one node to generate the data packet and k nodes to generate single trust tokens), which will be unlikely due to high node mobility in VANETs.

Even if a set of misbehaving nodes do succeed in sending out false warnings, the secure packet formats of LEAPER (as given in subsection 2.4.2) will ensure that the IDs

of the colluders (with their signatures present in the invalid data packets and tokens) can be verified with non-repudiation in the court. This court trial is also suitable to the badmouthing attacks as the ultimate aftermath countermeasure.

In summary, reliable and faithful data packet relaying can be ensured in LEAPER, with the misbehaving nodes and malfunctioning nodes effectively handled by the ARP strategy. Comparatively, the existing schemes, at best, can only ensure either reliability or faithfulness in data packet relaying, as discussed in subsection 2.2.2. The advantages of LEAPER over the existing schemes also include its flexibility and adaptability: by configuring k to different values, LEAPER can actually outperform, or at least perform as well as, the existing schemes in different application scenarios. For instance, when only malfunctioning nodes are of concern, LEAPER with k=0 can ensure reliable data packet relaying similar to CBF [160], [161] and REAR [163]. When misbehaving nodes exist, LEAPER with $k \geq 1$ can ensure faithful packet relaying as DTT [77] and AWF-NA [155], additionally ensuring reliable packet relaying.

2.5.3 Analytical Performance Estimation

Here, the per-hop performance of LEAPER will be analyzed with comparisons to a baseline protocol (BSL), namely GPSR [156]. As discussed before, GPSR [156] selects one specific Relayer and has no watchdog in each hop.

Per-hop SDR: Per-hop SDR (successful delivery ratio) is the probability that a data packet can be faithfully relayed in a certain hop, in face of misbehaving nodes and malfunctioning nodes. Thus, per-hop SDR actually is a comprehensive metric for both reliability and faithfulness in each hop.

In LEAPER, let N_i be the total number of nodes in trust group i (TG_i) and n_a be the number of *active* nodes. The other ($N_i - n_a$) malfunctioning nodes cannot take any active communication action. Let p_d and p_m be the probability of any node malfunctioning and misbehaving, respectively.

Thus, in hop i the average number of active nodes is $n_a = N_i \times (1 - p_d)$. Let $P(j)$ be the probability that j ($j \geq 0$) misbehaving nodes exist in trust group i. Thus,

$$P(j) = \binom{n_a}{j} p_m^j (1 - p_m)^{n_a - j}. \tag{2.5}$$

Then the probability that more than k misbehaving nodes exist in TG_i is

$$\Pr\{j \geq k\} = 1 - \sum_{l=0}^{k-1} P(l). \tag{2.6}$$

Let SDR_{LP} be the per-hop SDR of LEAPER, and SDR_{BSL} be the per-hop SDR of BSL. For LEAPER to ensure that the data packet can be faithfully relayed, there must be less than (k+1) misbehaving nodes in this trust group. Thus,

$$SDR_{LP} = 1 - \Pr\{j \geq k+1\}. \tag{2.7}$$

Comparatively, in BSL the data packet can be faithfully relayed only if the selected Relayer is not malfunctioning and there is no misbehaving node in this hop. Thus,

$$SDR_{BSL} = 1 - p_d - \Pr\{j \geq 1\}. \tag{2.8}$$

As shown in (2.5)-(2.7), in LEAPER p_d has no direct impact on SDR_{LP}. And with $k > 0$ the negative impact of misbehaving nodes on SDR_{LP} will be much smaller than that on SDR_{BSL}, as shown in (2.5), (2.6) and (2.8). Thus, given the same p_d and p_m, LEAPER can achieve much higher per-hop SDR than BSL.

Per-hop Latency: As already discussed in section 2.4.3, generally the per-hop latency of LEAPER is

$$T_{D,\,LP} = (k+2)\,\tau_m + (2k+2)\,\tau_v + 3\,\tau_s. \tag{2.9}$$

Let n_m be the number of misbehaving nodes in a trust group. In the worst case, these misbehaving nodes will all send out tampered data packet or invalid single trust tokens, and the per-hop latency of LEAPER becomes

$$T_{D,\,LP} = (k+2)\,\tau_m + (2k+2)\,\tau_v + 3\,\tau_s + (n_m\,\tau_m + n_m\,\tau_v). \tag{2.10}$$

Even in the worst case, $T_{D,\,LP}$ is acceptable for reasonable values of k. As defined in DSRC [8] and WAVE [9], the allowable latency for safety messages is 100ms. In this case, plug in the parameters from [155] (τ_m=5ms, τ_s=1.42ms, τ_v=0.07ms) and let n_m=k, we can get that $k \leq 7$ from (2.10). Meanwhile, with efficient message authentication schemes such [144], τ_v could be further reduced, and LEAPER can achieve smaller $T_{D,\,LP}$.

Tradeoff: To comprehensively compare the per-hop performance of BSL and LEAPER, the tradeoff between SDR and latency will be considered here. In BSL, in each hop there are only one signature generation, signature verification and MAC access for the data packet. Thus the per-hop latency of BSL is

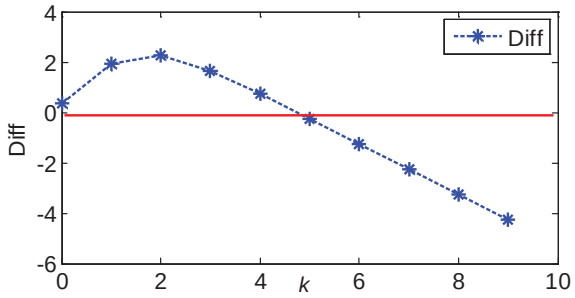

Figure 2.8 Difference between overall per-hop SDR of BSL and LEAPER

$$T_{D,\,BS} = \tau_m + \tau_v + \tau_s. \tag{2.11}$$

From (2.9) and (2.11), $T_{D,\,LP}$ is approximately k+2 times of $T_{D,\,BS}$, given that τ_m generally is much larger than τ_v and τ_s. Thus, if SDR_{LP} is (k+2) times higher than SDR_{BSL}, LEAPER will have a lower per-hop latency for each successful delivery than BSL, as shown in Figure 2.8. In Figure 2.8, *Diff* is defined as $Diff = SDR_{LP}/SDR_{BSL} - (k+2)$. Thus, when *Diff* is larger than 0, the overall performance of LEAPER is better than that of BSL. In this comparison p_m=0.1, p_d=0.2, and the time parameters for (2.10) are adopted.

As shown in Figure 2.8, *Diff* is above 0 when k is between 0 and 4. However, when k becomes larger than 2, the increase in k will bring down the overall performance of LEAPER. This is because SDR_{LP} is almost 100% when k is 2, and further increase in k can only bring additional latency without obvious increase in SDR_{LP}.

Thus, by tuning k carefully, LEAPER can achieve much better overall per-hop performance than BSL, which justifies the high per-hop latency of LEAPER to achieve higher per-hop SDR. Since with large k fewer tampered data packet will reach the destination, LEAPER will perform much better than BSL when security is taken into consideration. Actually, this reasoning is also meaningful for the end-to-end performance comparison between LEAPER and other schemes, as shown in our simulation studies.

2.5.4 Simulation Studies

To study LEAPER's performance, extensive NS2 [169] based simulations are conducted with vehicle mobility traces generated by MOVE [170]. The common simulation parameters are summarized in Table 2.3. The time required for signature generation and verification (RSA1024), and Hash function (SHA512) are adopted from one cryptographic benchmark [171].

Table 2.3
Simulation parameters of LEAPER

Parameters	***Values***	***Parameters***	***Values***
# of Nodes	142	Beacon Interval	200 ms
Road Length	3 Km	Communication Range	300 m
MAC Protocol	802.11	Node Velocity	40m/s
Bit Rate	6 Mbps	Simulation Time	900 seconds
τ_0	10 ms		

In these simulations, the source node and the destination node are placed at either end of a 3km road segment. The *malfunctioning* nodes will participate in neither data packet relaying nor token generation. The *misbehaving* nodes will tamper every data packet as Relayers. As watchdogs the *misbehaving* nodes will either refuse to generate token, or choose to collude with the misbehaving Relayer with a probability of 0.1, which is to reflect the fact that in VANETs collusions among misbehaving nodes are quite rare. For comparison, LEAPER, BSL and DTT [77] are implemented in the simulations.

Individual Metrics: Here three metrics are evaluated: end-to-end SDR (SDR_E), end-to-end latency (T_E) and ratio of tampered packets at the destination (R_b). Six protocols are implemented for comparison: BSL, DTT, LEAPER0 (k=0), LEAPER1 (k=1), LEAPER2 (k=2) and LEAPER3 (k=3). The performance differences among these protocols with different ratios of malfunctioning nodes (p_d) and misbehaving nodes (p_m) will be studied. Here, p_d is fixed to 0.1, and p_m changes from 0.0 to 0.1 with a step size of 0.01. The simulation is run 10 times and the metrics are averaged to reduce randomness effects.

As shown in Figure 2.9, LEAPER1 achieves the highest SDR_E with increasing p_m, which is almost stable as p_m increases. LEAPER2 and LEAPER3 also achieve stable SDR_E with increasing p_m, but their SDR_E are obviously lower than that of LEAPER1. In LEAPER2 and LEAPER3 more watchdogs are required in each trust group, so that they will face more network segmentations given the same mobility traces. This can also explain the fact that SDR_E of LEAPER2 is always higher than that of LEAPER3. The SDR_E of LEAPER0 is quite high when p_m is 0 but it decreases sharply with the increase of p_m, since LEAPER0 does not configure any watchdog and the packet authenticity cannot be ensured in each hop.

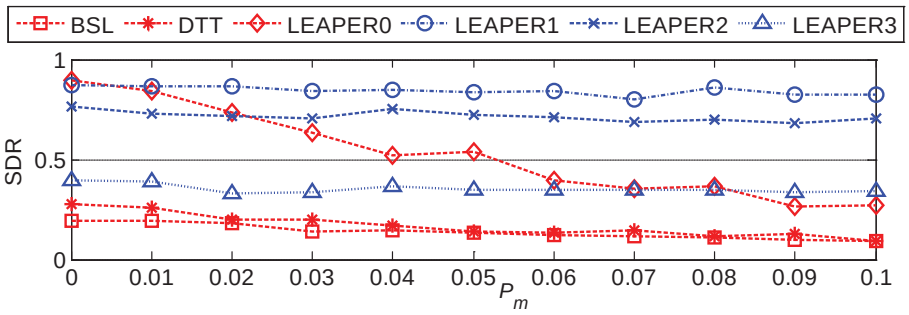

Figure 2.9 The end-to-end SDR statistics of BSL, DTT and LEAPER

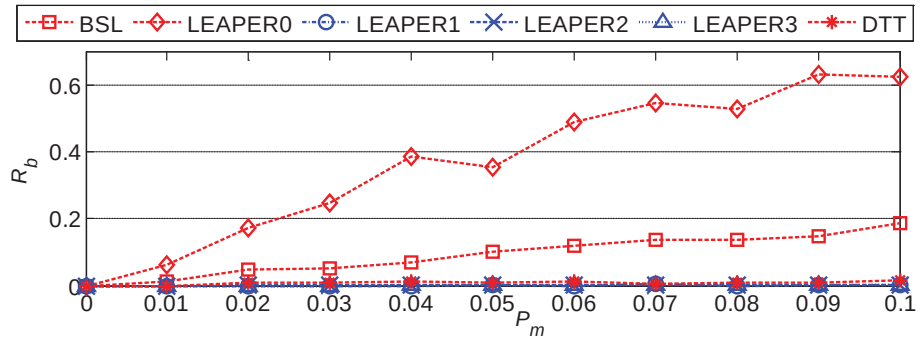

Figure 2.10 The ratios of tampered packets of BSL, DTT and LEAPER

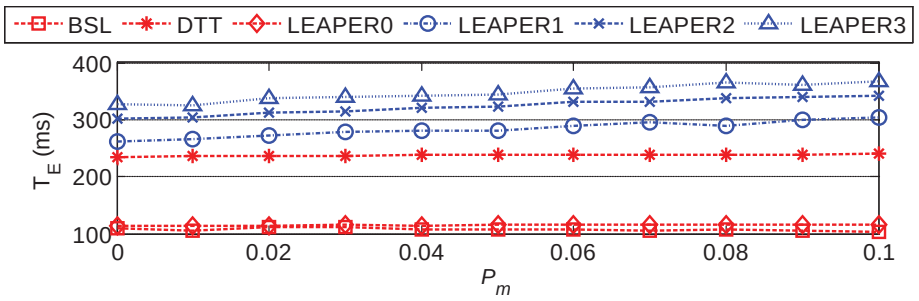

Figure 2.11 The end-to-end delays of BSL, DTT and LEAPER

Thus, in LEAPER0, with the increase of p_m more tampered data packets will arrive at the destination, as shown in Figure 2.10. Due to the impact of malfunctioning nodes, DTT and BSL only achieve very low SDR_E with any p_m values, which is consistent to our previous analysis. Meanwhile, BSL allows more tampered data packets at the destination than DTT, as shown in Figure 2.10. Comparatively, LEAPER0 allows most tampered data packets at the destination, as shown in Figure 2.10, since it ensures reliable packet relaying without detecting the tampered data packets. LEAPER1, LEAPER2, and LEAPER3 can actually achieves R_b=0 for increasing p_m.

In summary, LEAPER1 can ensure reliable and faithful packet relaying in face of malfunctioning nodes and misbehaving nodes, achieving the highest SDR_E and low R_b. Thus, LEAPER1 shows the merits and overcomes the disadvantages of both LEAPER0 (similar to REAR and CBF as discussed in subsection 2.5.2) and DTT. Though LEAPER2 and LEAPER3 show lower SDR_E than LEAPER1 in this simulation, their performance could potentially be enhanced once the network partitions can be handled by integrating the existing robust message dissemination schemes into LEAPER.

Figure 2.11 shows the end-to-end latency (T_E) of these various protocols. BSL and LEAPER0 have similar T_E, since they only transmit data packets in each hop. DTT, LEAPER1, LEAPER2, and LEAPER3 require the collection and relaying of trust tokens in each hop, so they incur higher latency in each hop. Figure 2.11 shows that bigger values of k (more tokens required in each hop) result in larger end-to-end latency, which is consistent to our previous analysis. However, the increased latency is still acceptable: the average hop number is 11, and T_E of LEAPER3 is still less than 400ms. Thus, the average per-hop latency of LEAPER3 is still less than 40ms in this simulation setting.

Thus it is arguable that the overall performance of LEAPER1, despite its higher T_E, can be better than that of LEAPER0, DTT and BSL due to its much higher SDR_E. The performance of these protocols will be comprehensively compared next. Note that LEAPER2 and LEAPER3 have lower SDR_E than LEAPER1 due to network segmentations, so they are not considered in the comprehensive comparisons.

Comprehensive Metrics: Here, a TCP-like end-to-end control protocol is implemented, where the source node will wait for an ACK from the destination node before it transmits the next data packet. If no ACK comes for 300ms, the source node will retransmit the data packet. Two metrics are designed here to indicate the comprehensive performance of LEAPER, DTT and BSL: expected overhead (O_E) and expected latency (T_L). O_E is the average communication overhead (including data packets, single trust tokens and total trust tokens) for each successfully received data packet at the destination; T_L is the averaged latency for each successfully received data packet. Here, p_d is set to 0.1 and p_m changes from 0.0 to 0.15 with step size 0.01. Again, the simulation is run 10 times and the metrics are averaged over all the simulation runs.

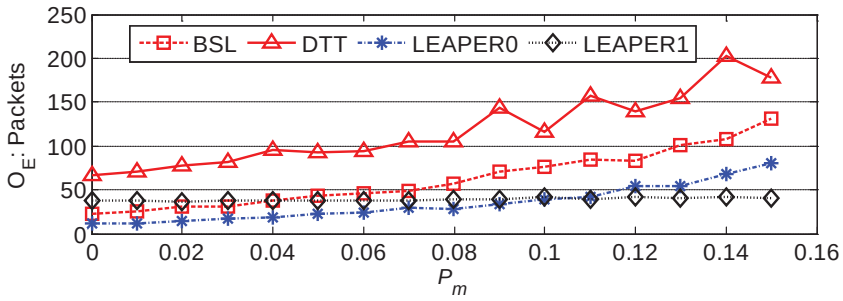

Figure 2.12 The overhead per successful delivery of DTT, BSL and LEAPER

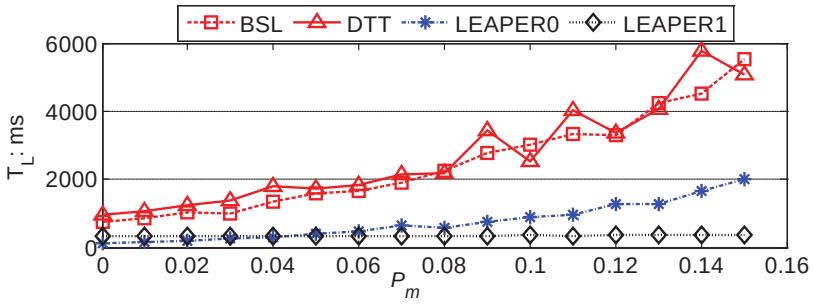

Figure 2.13 The latency per successful delivery of DTT, BSL and LEAPER

In Figure 2.12 the expected overhead is shown. LEAPER1 will outperform BSL and LEAPER0 when p_m is bigger than 0.04 and 0.1, respectively. LEAPER0 can always outperform BSL and DTT. Here, DTT has the highest O_E because it has SDR_E similar to BSL but has to generate tokens in each hop as LEAPER1 does.

The T_L statistics are shown in Figure 2.13. Due to the high SDR_E of LEAPER1, it can outperform BSL and DTT for any p_m, and can outperform LEAPER0 when p_m is larger than 0.04. LEAPER0 can always outperform BSL and DTT. This indicates that generally in face of misbehaving nodes LEAPER1 enables the destination to wait shorter for each authentic data packet. Meanwhile, the comprehensive performance of LEAPER1 is almost constant with the increase of p_m, as shown in Figure 2.12 and Figure 2.13, which shows the robustness of LEAPER in face of misbehaving nodes.

Moreover, LEAPER allows flexible configuration of k based on the specific application scenarios and desired tradeoff between security strength and performance. When there is no misbehaving node and only malfunctioning nodes in VANETs, k=0 is the best option. However, when misbehaving nodes exist k must at least be 1. When any tampered data packets cannot be tolerated by the destination, k can be set to 2 or higher in order to preclude any possibility of node collusions, at the cost of lower end-to-end SDR.

2.6 Summaries

In this chapter, insightful investigation into data packet relaying in VANETs identifies four *basic functions*. A novel Adaptive Role Playing (ARP) strategy is then proposed to enable the nodes in each hop to contend to perform the basic functions, so that reliable and faithful data packet relaying is still achievable in face of malfunctioning and misbehaving nodes. LEAPER enables the nodes in each hop to securely and efficiently follow the ARP strategy. With each honest node in each hop contending to relay the authentic data packet and to vouch for it with tokens, the misbehaving and malfunctioning nodes are effectively detected and handled. Thus, LEAPER achieves both reliable and faithful data packet relaying in each hop, which is its major advantage over existing schemes. Ensuring both reliable and faithful data packet relaying, LEAPER is appealing to VANETs, where many applications rely on trustworthy multi-hop communications. Especially, the configurable security threshold k makes LEAPER flexible and adaptive to various network environments and applications requirements.

In the future, the dynamic adjustment of k will be studied, so that LEAPER can achieve optimal tradeoff between security and performance in varying VANET environments. Another future work is to adopt the existing robust message dissemination schemes [162], [166] into LEAPER, so that LEAPER can effectively handle the network segmentations to achieve better end-to-end successful delivery ratio with $k \geq 2$.

Chapter 3 Resource-Aware Message Verification in VANETs[2]

Driven by various applications, verification of messages' content integrity and authenticity is indispensable for VANETs. However, due to the numerous message exchanges in VANETs, message verification often leads to excessive resource consumption and even resource depletion in vehicular nodes. To tackle this scalability issue, a novel Resource-Aware Message Verification (RAMV) [143], [144] scheme is proposed in this chapter. With application-specific differentiation of messages to better support traffic safety applications, RAMV streamlines existing message verification schemes to keep their resource consumption within the preset resource budget. Besides, the common security requirements for message verification are properly met by RAMV. Enabling resource-aware, application-friendly and secure message verification, RAMV is especially appealing to VANETs.

3.1 Introduction

It is critical to ensure message authenticity and integrity in various VANET applications, especially the traffic safety applications. Thus, content verification and source verification are critical to VANETs to ensure message authenticity and message integrity, respectively. Regardless of the implementation details, message verification, especially source verification which relies on digital signature verification, is resource demanding.

Thus, message verification may incur varying and excessive resource consumption in face of the massive message exchanges in VANETs. Such massive message exchanges result from the periodic messages broadcasted by each node to support traffic safety applications (Beacons) and various other applications (neighbor information for proactive routing [172], information abstract in epidemic routing [173], or message flooding [174]). Each node thus needs to verify numerous messages per second, the exact number of

[2] The material contained in this chapter was previously published in the Journal *of Security and Communication Networks*. © 2011 Wiley-Blackwell. See Appendix B for a copy of the copyright transfer agreement.

which changes linearly with the node density in the neighborhood. The resource consumed by message verification, given any algorithm adopted, tends to be huge and will make message verification non-scalable. Moreover, the variances in resource consumption will also negatively affect the resource available to other applications.

Thus, it is desirable to make message verification in each node *resource-aware*, in that its resource consumption in any circumstance will be bounded by the actual resource available to message verification, in form of a resource budget. For brevity, this chapter only explicitly considers the verification of Beacons, which, periodically broadcasted by each node to signal the driving status, may be the most prevalent messages in VANETs. However, as discussed throughout this chapter, the proposed scheme is also applicable to the verification of any kind of messages in VANETs.

In this chapter, a ***R***esource-***A***ware ***M***essage ***V***erification (***RAMV***) scheme is proposed to streamline the existing message verification algorithms to make them both *resource-aware* and *application-friendly*. Specifically, RAMV differentiates the Beacons based on their application relevance and latency requirements. Each node will mainly spend its resource budget in verifying the more important Beacons from the near-by neighbors or with safety-critical information, which are crucial to the traffic safety applications. This way, RAMV is also application-friendly by better supporting traffic safety applications given a limited resource budget. The less important Beacons generally will only be indirectly verified by the receiver with the help of its neighbors, at essentially no computation cost. Thus, even with a limited resource budget, RAMV still keeps the critical security strengths of message verification, in that 1) each Beacon will be verified by at least one receiver to timely disclose the misbehavior of data forging; and 2) each node is able to learn to validity/invalidity of each received Beacon to properly evaluate its neighbors, as in the reputation schemes [80], [86].

In short, by properly differentiating received Beacons, RAMV ensures resource-aware, application-friendly and secure message verification, which underlies many important applications in VANETs. Thus, RAMV is especially appealing to the approaching massive deployment of VANETs.

3.2 Background and Related Work

Here we will show the necessity of considering resource budget in message verification, as well as the drawbacks of the existing schemes in this light.

3.2.1 Resource Budget

A vehicular node is essentially a real-time system with limited (though abundant) resource in terms of memory, CPU time, I/O capabilities, and so on, to be shared by numerous applications. Here, we focus on the CPU time. The resource sharing usually is controlled by the resource allocation (scheduling) algorithms [175] which, simply put, provide each application with a certain resource in form of x CPU time out of y time units [175], [176]. Generally a *resource budget* is desirable to define the maximal resource consumption of each application and ensure reasonable resource sharing. Indeed, the traditional static priority scheduling [177] works well only when each task has a predictable workload, whereas the rate-based algorithms [175], [176], [178] actually enforce a resource budget for each application.

In the context of message verification, the resource consumption/requirement will be measured by the number of messages verified given a certain cryptographic technique and content verification algorithm. Thus, our algorithm and analysis will be generic and independent of the concrete message verification algorithms adopted in VANETs.

In VANETs, the resource requirement of message verification may vary greatly due to the wide range of the number of Beacons (n_m) received per second. It is commonly suggested in the VANET community, for example by DSRC [10], that the common beaconing period (T) is 100ms, and the common communication range (R) is 300m. Thus,

$$n_m=\rho R/T=10\rho R. \tag{3.1}$$

Here, ρ is the node density of the concerned neighborhood, in unit of node per meter. One node has ρR 1-hop neighbors within its communication range, each of which will broadcast 10 ($1/T$) Beacons per second. Thus, (3.1) follows. In urban scenarios it is common for one node to have tens of 1-hop neighbors and thus to receive hundreds of Beacons per second, resulting in the excessive resource consumption by message verification. Besides, ρ generally changes significantly in different geographic locations and time periods. The variances in n_m, and the variances in resource consumption thus

caused, will negatively affect the resource allocation algorithms as discussed in [175], and potentially harm other VANET applications in this way.

Thus, it is critical to ensure that message verification follows its resource budget, which can be expressed in the number of Beacons (N_M) one node is allowed to verify per second. It also can equivalently be expressed as the number of neighbors (N_B) one node can maintain if it verifies all Beacons from its neighbors. Thus,

$$N_M = N_B \times 1/T. \tag{3.2}$$

Equation (3.2) follows, since each neighbor will broadcast $1/T$ Beacons every second.

Two dimensions of resource budget will be investigated here: *hard* vs. *soft* and *static* vs. *dynamic*. The hard budget needs to be strictly met in any statistic period to prevent any application from violating its resource budget in a resource stringent environment. The soft one only needs to be statistically followed, serving as the application design guideline [179], [180]. The resource budget may remain static over a long period. Or it can be dynamically determined by the scheduler of the operation system [178] based on the runtime resource requirements of all applications. Hereafter, the types of resource budget will always be clarified whenever necessary.

3.2.2 Related Work

So far, the resource issue has been only insufficiently addressed in the existing schemes for message verification. First, the existing source verification and content verification algorithms generally focus on the functionalities, without systematically considering the overall resource consumption.

The well-known cryptographic techniques for message verification include ECDSA [181], RSA [182], group signature [40], etc. RSA and group signature may not be suitable for VANETs due to their excessively long signatures compared to ECDSA. ECDSA is recommended in WAVE [9] for VANETs, but it is computationally demanding as shown in various performance evaluations [171], [183]-[186]. For instance, an evaluation of ECDSA on a Pentium platform [185] shows that one signature verification requires 31ms and 47ms for ECDSA P224 and P256, respectively. Thus, one node with the same configuration can only verify 32 (in case of P224) and 21 (in case of P256) Beacons every second. Additionally, the computation platform installed in vehicles

is unlikely to be cutting-edge for cost considerations. Thus, if ECDSA is to be implemented in VANETs, its resource requirement must be brought under the control of resource budget. Exemplary content verification schemes include [66]-[68], which, though not so computation extensive as the cryptographic algorithms, still will incur significant resource consumption in face of massive message exchanges.

Besides, many schemes [45], [71], [187]-[191] have been proposed specifically for efficient message verification in VANETs. However, as we will show shortly, these schemes fail to be resource-aware, application-friendly and secure at the same time, and thus can be further improved by RAMV.

In both TESLA [187] and TDAS [188], each message contains a hashed value $hash(v)$, and v will be revealed in the next message from the same sender. The receiver can thus verify the received message by performing the relatively lightweight hash function. However, the receiver needs to wait for the next message to verify the current message, which will lead to high communication overhead and latency. Besides, any message loss will make its previous message unverifiable. The on-demand verification scheme [189] only verifies those messages which can raise an alert or warning to the applications, to reduce resource consumption. This, however, will leave most messages unverified so that the data forging attack cannot be detected in time. The batch verification schemes [190], [191] allow the receiver nodes to verify multiple messages in a batch. Their common drawback lies in the latency incurred by the accumulation of received messages, which is undesirable to the messages with high application significance.

[45] proposes group signature-based self-signing certificates to reduce the size of certificates, and further proposes only attaching certificate to every 1 out of α messages. Thus, the resource consumption of verifying certificate is significantly reduced. However, as stated in [45], the signature part of each message still needs to be verified. Thus, excessive resource consumption can still occur in [45]. Similarly, [71] proposes several approaches to reduce the resource consumption of beaconing in VANETs, including only attaching certificates and signature to 1 out of n messages at the sender's side, as well as only verifying 1 out of m messages at the receiver's side. So far, [71] is the most relevant scheme to RAMV. However, [71] does not investigate the impacts of these approaches

on the safety implications and security strengths of message verification, nor presents a systematic way to configure the relevant parameters.

In [192], the authors propose to solve the scalability issues in VANET communications with relevance-based message transmission. Each node estimates the application relevance of its messages and schedules the transmission of its messages accordingly. Thus, with limited bandwidth the messages with greater application relevance will be broadcasted first, ensuring maximal application benefits to the whole VANETs. Though the focus of this work is orthogonal to RAMV, the concept of application relevance is indeed useful to our work.

Thus, it is necessary for RAMV to ensure resource-aware, application-friendly and secure message verification in VANETs, which has not been satisfactorily addressed yet.

3.3 RAMV Overview

RAMV differentiates the received Beacons based on their application significance to meet the stringent resource and security requirements. As shown in Figure 3.1, this differentiation is performed by three modules: Distance-Based Resource-aware Verification (DBRV), Event Triggered Verification (ETV) and Piggybacked Invalid Message Notification (PIMN).

In DBRV, the application significance of each received Beacon will be ranked based on the distance between the receiver and the sender, since the Beacons from the near-by neighbors are more important to the driving safety of the receiver. DBRV will provide a strategy for message verification based on the current resource budget, with which the specific message verification algorithms such as ECDSA [181] will selectively verify the received Beacons. DBRV ensures that the more important Beacons will be directly verified with a higher probability, better supporting the traffic safety applications. The verification results will be adopted by the relevant reputation schemes or misbehavior detection schemes to update the evaluations on the corresponding senders. Among all received Beacons, the valid ones and the unchecked ones will be processed by the traffic safety applications.

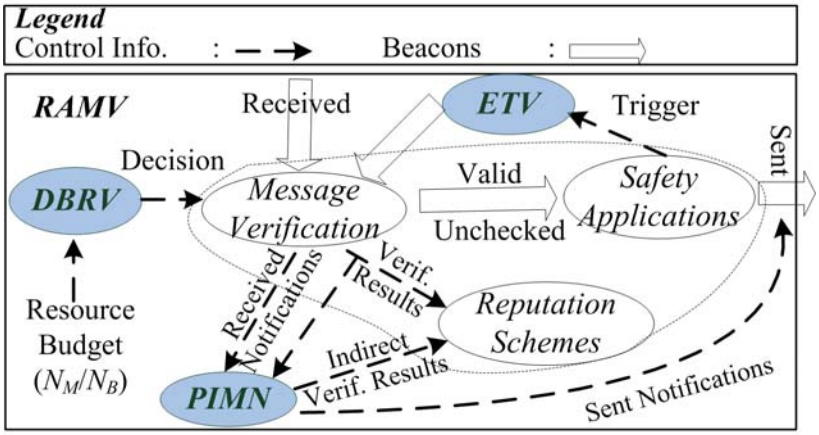

Figure 3.1 The overview of RAMV with message flows

If one traffic safety application regards one unchecked Beacon (B_C) as critical, the ETV module will signal the verification algorithms to immediately verify B_C. Thus, any critical Beacons, no matter how far their senders are, will be verified before they affect the traffic safety applications.

Whenever an invalid Beacon (B_I) is identified in DBRV, the PIMN module will construct a notification of B_I to broadcast the verification result of B_I by piggybacking it to the next outgoing Beacon. On the other hand, the notifications piggybacked in the received Beacons will be processed by PIMN to infer the properties of the previously unchecked Beacons. These indirect verification results will also be adopted by the reputation schemes.

Thus, by enabling each node to focus its resource on Beacons important to traffic safety, DBRV and ETV ensure reliable traffic safety applications while following the resource budget. PIMN enables each node to learn the property of each received Beacon either by direct verification or from the piggybacked notifications, ensuring security strengths. As such, RAMV streamlines the existing message verification algorithms to enable resource-aware, application-friendly and secure message verification in VANETs.

3.4 DBRV

As previously discussed, DBRV enables each node to spend its resource budget in verifying the Beacons with high application significance. A novel concept, *relevance rank*, is proposed in the first place to model the Beacons' application significance.

Figure 3.2 The exemplary relevance ranks in the single lane model

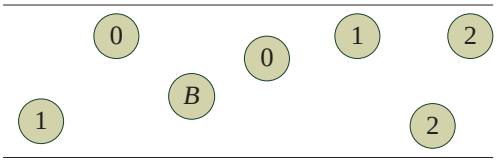

Figure 3.3 The exemplary relevance ranks in the multi-lane model

3.4.1 Distance-Based Relevance Rank

In the context of traffic safety applications, the Beacons from the nearby neighbors are more relevant to the receiver, since the driving states of such neighbors will potentially have bigger impact on the receiver. Thus, the concept of *relevance rank* is proposed based on the distances between the neighboring nodes.

Single-lane Model: In the single-lane scenario, node *A*'s relevance rank to node *B*, denoted as R_{BA}, can be calculated by node *B* as:

$$R_{BA} = \left| \left\{ X : X \in Nei(B), \left| \overline{XZ} \right| < \left| \overline{AB} \right| / 2 \right\} \right|. \tag{3.3}$$

In (3.3), *Nei*(*B*) is the set of *B*'s 1-hop neighbors, and *Z* is the middle point of line segment $\overline{AB}$. The operator | | either calculates the set cardinality or the line segment length, as defined by the context. Hence, R_{BA} is equal to the number of nodes between *A* and *B*, and indicates how relevant *A* is to *B* compared to *B*'s other neighbors. In single-lane scenarios, the relevance ranks of node *B*'s neighbors are shown in Figure 3.2.

Multi-lane Model: If node *B* is in a road junction or a road with multiple lanes, R_{BA} will be

$$R_{BA} = \left\lfloor \left| \left\{ X : X \in Nei(B) \,\&\&\, \left| \overline{BX} \right| < \left| \overline{AB} \right| \right\} \right| / 2 \right\rfloor. \tag{3.4}$$

In (3.4), R_{BA} is now determined by the absolute distance ranks of node *B*'s neighbors. (3.4) ensures that *B* will have exactly two neighbors with the same relevance rank, as shown in Figure 3.3. Similar to the single-lane model, this multi-lane model also considers the spatial symmetries of the neighborhood.

Both absolute distances and relative positions among the neighboring nodes are considered in relevance rank to comprehensively reflect the application relevance of

different senders' Beacons. Generally, only the sender and the receiver in the same driving direction are considered for relevance rank, except for the road junctions.

It is feasible for each node to calculate the relevance rank of each of its neighbors. In VANETs, each node can figure out its surrounding road layouts with the help of GPS, so it can choose the proper relevance rank model correspondingly. According to DSRC [10], Beacons contain the positions of the senders, with which each node can learn the current positions of all its 1-hop neighbors. Thus, each node can calculate the relevance ranks of its neighbors with (3.3) and (3.4). In case of other messages, relevance rank can be similarly defined based on their application-specific properties, as indicated by the application relevance concept in [192]. As another example, the messages for epidemic information broadcast may define the relevance rank based on the information similarities of such messages. That is, one receiver may assign the relevance rank 0 to the message with the most new information, assign the relevance rank 1 to the message with the second most new information, and so on.

With each received Beacon differentiated, the receiver can schedule its verification operations accordingly based on its current resource budget, either soft or hard.

3.4.2 Probabilistic Message Verification based on Soft Budget

A probabilistic message verification algorithm is proposed here to enable each node to schedule its message verification to meet its soft resource budget. If the receiver has fewer 1-hop neighbors than its resource budget N_B, it will verify all received Beacons without violating N_B. Otherwise, Beacons with relevance rank 0 will always be verified to ensure driving safety and other Beacons will be probabilistically verified to meet the resource budget.

This algorithm is performed with the help of a filtering probability p, which is decided based on N_B as we will discuss shortly. A node, say node A, will verify the Beacon from $X \in Nei(A)$, with a probability P_{AX} determined by the relevance rank R_{AX} and p as

$$P_{AX} = p^{R_{AX}} . \tag{3.5}$$

Specifically, as shown in Figure 3.4, when a Beacon is received its verification probability (*Thres*) is calculated based on p and the sender's relevance rank with (3.5). A random test will be performed to decide whether to verify it or not based on *Thres*.

```
/*This function probabilistically verify received Beacons.*/
1       Probabilistic_Authen(msg)
2          R = Find_Rank(msg);      //get the relevance rank
3          Thres = p^R;             //probability threshold
4          Coin = uniform();        //random number in [0, 1]
5          Flag = 0;                //indicator initialization
6          If Coin < Thres          //will verify msg
7             Flag = Authenticate(msg);
8          Else                     //will not verify
9             Set Flag to Unchecked ;    //regard msg as authentic
10         EndIf
11         If Flag is Valid or Unchecked
12            Update_Rank(msg);  //Update the relevance rank
13         Endif
14      EndofFunction
```

Figure 3.4 The detailed probabilistic verification algorithm

Here, for brevity the receivers verifying one Beacon are called the *active* receivers of this Beacon, while the receivers choosing not to verify it are called *idle* receivers. If one Beacon is detected to be invalid, it will be discarded. Otherwise, the sender's position will be updated, and the relevance ranks of all neighbors will be updated accordingly based on (3.3) or (3.4).

The filtering probability p is determined based on the resource budget N_B (or equivalently, N_M). The feasible values of R_{AX} are 0, 0, 1, 1, 2, 2, etc. as shown in Figure 3.2 and Figure 3.3. Therefore, on average the resource consumption of A is:

$$n_c = 2(1 + p + p^2 + p^3 + \ldots) \leq 2/(1-p). \tag{3.6}$$

The resource consumption n_c should be smaller than the resource budget, so

$$n_c \leq N_B. \tag{3.7}$$

To give the resource budget a margin, let the equation hold in (3.6). Thus, it follows:

$$p \leq (N_B-2)/N_B. \tag{3.8}$$

Thus, (3.8) can be used to derive p based on N_B. For instance, if N_B is 4, p can be set to any value no bigger than 1/2. With p derived as such, any node could perform probabilistic message verification without violating the soft resource budget (N_B).

3.4.3 Probabilistic Message Verification based on Hard Budget

To ensure that in any statistic period, say 10 seconds, each node's resource consumption n_c is strictly less than its resource budget N_B, the procedures shown in Figure 3.4 will be modified so that the probability in (3.5) will be strictly followed. Here,

each node maintains a counter vector *CV*, the *r*th element of which is $CV[r] = \lceil 1/p^r \rceil$. Thus, *CV* indicates how frequently the messages with different relevance ranks should be verified. Each node keeps track of how many messages with relevance rank *r* are unchecked with another vector *RV*.

The procedures in Figure 3.4 will be updated as follows. Once a Beacon with relevance rank *r* is received, *RV*[*r*] will be increased by 1. If *RV*[*r*] is equal to *CV*[*r*], this Beacon will be verified, and *RV*[*r*] is reset to 0. Otherwise, this Beacon will not be verified. In this process, the probability of the messages with relevance rank *r* being verified is strictly less than that indicated by (3.5). Thus, the resource consumption of each node will be strictly less than N_B as indicated by (3.6).

3.4.4 Simplistic Resource-Aware Message Verification

A simplistic algorithm for scheduling message verification according to the resource budget is proposed here. With this algorithm, each node will only verify the Beacons with a relevance rank less than or equal to $\left(\lfloor N_B/2 \rfloor - 1\right)$. Here, the hard (soft) resource budget can be met by any node, which will always have resource consumption of $2\lfloor N_B/2 \rfloor \le N_B$. Intuitive and simple to implement, this algorithm can serve as an alternative to the probabilistic algorithms.

3.5 PIMN

In DBRV, except when N_B and *p* are big enough or the node density is extremely low, idle receivers generally will exist for each Beacon. To enable such idle receivers to learn the validity/invalidity of each Beacon, a novel PIMN module is proposed here.

3.5.1 Detailed Procedures

The main procedures of PIMN consist of three parts, as shown in Figure 3.5.

Beacon Processing: The active receiver verifies the received Beacon with the help of DBRV, as shown in Figure 3.5. If one invalid Beacon (B_I) is detected, one notification to accuse B_I is constructed and added to the notification pool, which contains the pending notifications of all previously identified invalid Beacons.

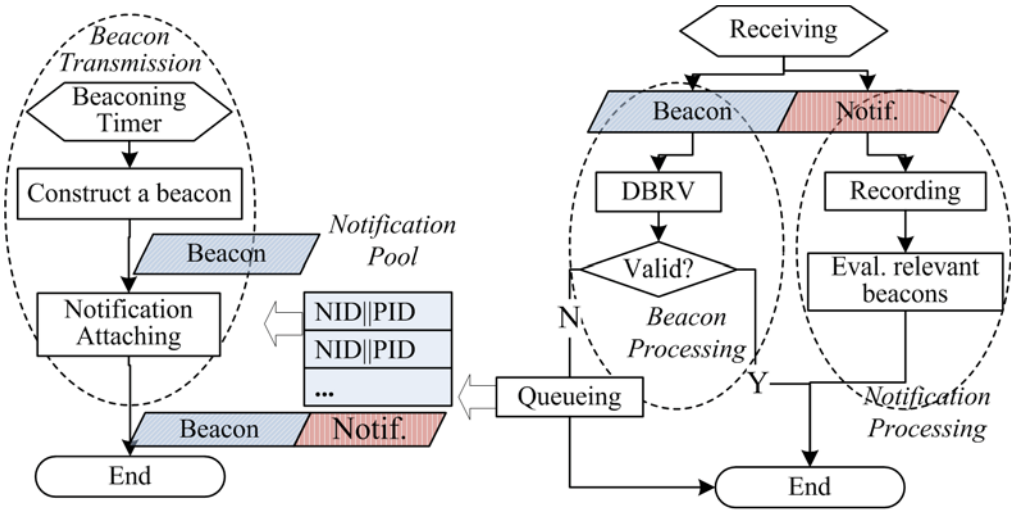

Figure 3.5 The detailed procedures of PIMN

Notification Processing: Upon receiving a Beacon (B_i), the receiver will process the notifications piggybacked, if any, in B_i as follows.

Case I: If one notification accuses a Beacon which has already been verified by this node, or has not been received yet, this notification will be disregarded.

Case II: If B_i has been (either directly or indirectly) verified as a *valid* Beacon, these piggybacked notifications are regarded as *acceptable*, and will be processed by the following approaches. Otherwise, if B_i has been verified (either directly or indirectly) as invalid, the notifications will simply be discarded.

For the *acceptable* notifications, the following approaches can be applied to determine the property of the accused Beacons, i.e. to indirectly verify the accused Beacons.

Approach I: The receiver evaluates the accused Beacon (B_a) based on all notifications about B_a. B_a is regarded as invalid if multiple (more than 2) notifications accuse it. Otherwise B_a is regarded as valid due to the lack of evidence.

Approach II: The receiver starts to verify the accused Beacon (B_a) even if only one acceptable notification about B_a is received. The property of B_a can thus be immediately figured out at the cost of one more message verification operation.

Both approaches allow the idle receivers to learn the invalid Beacons based on the received notifications. Their performance and security implications will be analyzed in details in section 3.7.

Beacon Transmission: When it is time to broadcast a new Beacon (B_n) based on the periodic beaconing timer, the node will first construct B_n based on its driving status. Then all the notifications in the notification pool will be piggybacked in B_n. The piggybacking approach is adopted here to reduce the bandwidth requirement.

3.5.2 Evaluation of Beacons and Notifications

The following strategies for evaluating Beacons and notifications are given to strictly define the terms of valid/invalid Beacons and acceptable notifications.

Without being directly verified by one receiver n_i, a Beacon B_i is regarded as valid by n_i if, 1) n_i has waited for a Beaconing period T without receiving any piggybacked notification about B_i, or 2) n_i receives one or more acceptable notifications $IN(B_i)$ but still confirms the validity of B_i with either Approach I or Approach II as discussed above.

Similarly, a Beacon B_i is indirectly verified as being invalid if n_i receives one or more acceptable notifications $IN(B_i)$ and confirms the invalidity of B_i with Approach I or Approach II as discussed above.

One notification $IN(B_i)$ is regarded as *acceptable* only if its bearer Beacon (B_j), the Beacon to which $IN(B_i)$ is piggybacked, is directly or indirectly verified to be valid.

Thus, any unchecked Beacon can be indirectly verified based on only *acceptable* notifications with a bounded latency. Given that in VANETs most Beacons are valid and most nodes are honest in sending out notifications, most unchecked Beacons will be regarded as being valid after T due to the absence of any notification. Only very few unchecked Beacons are invalid, which can be indirectly verified as being invalid after $2T$: the receiver only needs to wait for T to get the piggybacked notification, and at most another T to verify that the notification is acceptable. This latency is acceptable, since the unchecked Beacons are not quite relevant to the receiver as determined in DBRV.

3.5.3 Adaptive Organization of Notifications

A normal Beacon has the following packet format: {*NID*, *PID*, *Data*, *Signature*, *Cert*(*NID*)}. Here, *NID* is the sender's real identity, or pseudonym if privacy is concerned here. Adopted in privacy protection schemes [113], [125], a pseudonym is a temporary identifier without any obvious connection to the real identity of a node. If pseudonym is adopted here, RAMV can still successfully update the relevance ranks of the neighbors

without knowing their real identities. Actually, mainly concerning the locations of the neighbors, RAMV is oblivious to whether *NID* is a real identity or a pseudonym. Thus, RAMV is compatible to the common privacy protection schemes [113], [125] for VANETs, and will not pose any hurdles to privacy protection. *PID* is the packet ID of the Beacon, locally assigned by the sender. *Data* is the application specific data structure containing driving states. *Signature* is the sender's digital signature of the hash of the *NID*, *PID* and *Data* to ensure message integrity. The piggybacked notifications will also be included in this signature to ensure message integrity. *Cert*(*NID*) is the certificate of the *NID*, which may not be present in every Beacon according to [45], [71].

As shown in Figure 3.5, each notification of one Beacon (B_i) has the format {*NID*||*PID*}, since *NID* and *PID* concatenated together can uniquely identify B_i. The content of B_i is not needed in the notification, since the interested receivers of the notification are supposed to have received B_i. Each notification needs several bytes in the Beacon, and without loss of generality here both *NID* and *PID* are assumed to be 4 bytes. The number of pending notifications in each node may change greatly with the environments, so the space required for the piggybacked notifications will also change. This uncertainty in space requirement is undesirable for Beacon construction, so here an adaptive notification organization technique is proposed as shown in Figure 3.6 to ensure a relatively constant space requirement in various scenarios.

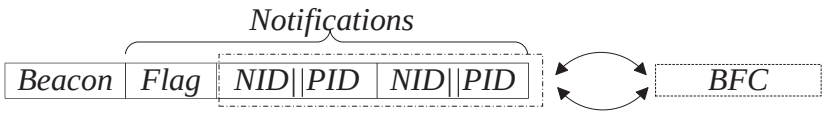

Figure 3.6 The format of piggybacked notifications

As shown in Figure 3.6, the 1-byte *Flag* field is used to indicate the format of the piggybacked notifications. If there are no more than 2 notifications, the attached notifications will be in the plain format. Here the piggybacked part will be no longer than 17 bytes long. If there are more notifications to attach, the bloom filter [193] coefficients (*BFC*) can be used instead to indicate the Beacons in this notification. The main idea is to hash the {*NID*||*PID*} of each notification, resulting in a value *v*. Each bit in *v* with value '1' will be used to set the corresponding bit in the *BFC*. On the receiver side, each {*NID*||*PID*} of the previously received Beacons will be hashed similarly, and the resulted

value v^* will be checked against *BFC*. If each '1' bit of v^* has a corresponding '1' bit in *BFC*, this Beacon is included in the notification. Thus, *BFC* with a specific size can indicate various numbers of Beacons. Here we set the filter (*BFC*) size m=128 bits and the hash round k=6, which is sufficient to indicate dozens of Beacons. The total length of the notification will also be 17 bytes in this case.

3.6 ETV

As previously discussed, DBRV ensures that the Beacons with high relevance ranks will be directly verified, while PIMN enables other Beacons to be indirectly verified with a bounded latency. This differentiation is proper to the routine Beacons containing normal driving states. However, the safety-critical Beacons, which may contain warning of abrupt braking or mechanical malfunctions of the sender, need to be verified by all receivers immediately to ensure driving safety. To this end, the Event-Triggered Verification (ETV) module is proposed.

As shown in Figure 3.1, ETV serves as a bridge between the safety applications and the message verification algorithms. Once the safety applications detect an unchecked Beacon (B_i) as safety-critical, ETV will pass B_i back to the message verification algorithms for immediate verification. Afterward, the safety applications will process B_i according to the verification result. In ETV, the detection of safety-critical Beacons can and only can be performed by the specific safety applications. With simple internal message buffer operation ETV can pass the safety critical Beacon to the message verification algorithms. The technical details may be too platform-specific to be elaborated on here. However, the feasibility of ETV is evident from the above reasoning, and also justified by the existing on-demand verification scheme [189].

Though the main idea of ETV is similar to that of the on-demand verification [189], ETV is actually more effective and powerful with the help of DBRV and PIMN. In [189] only the critical Beacons will ever be verified, thus the misbehaving nodes broadcasting invalid Beacons will not be detected in time if such Beacons are not regarded as critical by the receivers. Moreover, [189] actually has a security loophole. Suppose an adversary *A* broadcasts a sequence of invalid routine Beacons $\{B_i^*\}$, each with incrementally invalid data about its driving states, so they will not be verified by any receivers. As a result, *A*'s

neighbors will use $\{B_i^*\}$ to build an invalid model of *A*, $M_A(\cup B_i^*)$. In the end, if *A* sends out a safety-critical Beacon B_{i+1}^*, which is invalid but seems consistent with the preceding $\{B_i^*\}$, B_{i+1}^* will not be detected by [189] as being invalid due to the invalid model $M_A(\cup B_i^*)$. Comparatively, in RAMV with the help of DBRV and PIMN each node practically verifies both the signature and the content of each received Beacon, either directly or indirectly. The invalid Beacons $\{B_i^*\}$ will be identified and discarded once received, and the reputation of node *A* will be significantly decreased. Eventually, the false critical Beacon B_{i+1}^* will not be trusted by any receivers with ETV.

Regarding resource consumption, generally most Beacons are not critical Beacons and contain only routine information. Thus, no significant overhead will be incurred by ETV for additionally verifying the unchecked critical Beacons. Besides, the resource budget margin provided in DBRV will cover the overhead of ETV, if any. If in any case critical Beacons become prevalent, ETV can simply override the scheduling of DBRV and spend the resource budget mainly on the safety critical Beacons, so that the safety-critical Beacons will be always verified.

3.7 Analysis of RAMV

In subsections 3.4.2, 3.4.3 and 3.4.4, three algorithms have been proposed for DBRV: probabilistic message verification based on soft budget, probabilistic message verification based on hard budget, and simplistic resource-aware message verification. Hereafter, RAMV-S, RAMV-H and RAMV-SIM are used to denote RAMV adopting these algorithms, respectively. Whenever proper, RAMV will be compared to two alternative baseline schemes: BSL1 and BSL2. BSL1 represents the simplest best-effort message verification schemes, where each node attempts to verify all received Beacon. BSL2 adopts the main idea of [71], making each node verify 1 Beacon out of every n_t received Beacons. In both BSL1 and BSL2, in case of insufficient resource, after a period T_P the buffered Beacons will be simply discarded.

3.7.1 Quantitative Properties

Here we analyze RAMV's quantitative properties by comparison with BSL1 and BSL2.

3.7.1.1 Resource Consumption

Let n_{cb1}, n_{cb2}, n_{ch}, n_{cs} and n_{csim} denote the resource consumption per second of BSL1, BSL2, RAMV-H, RAMV-S and RAMV-SIM, respectively. Suppose one node has N_i 1-hop neighbors at time i. Further suppose this node has a total resource of N_A.

In case of BSL1, $n_{cb1}=N_i$ if $N_i \leq N_A$; $n_{cb1}=N_A$ if $N_i > N_A$. Thus, BSL1 results in varying resource consumption even when the resource is sufficient. When N_i becomes larger than N_A, resource depletion will happen to the VANET nodes.

In case of BSL2, $n_{cb2}=N_i/n_t$. BSL2 only rigidly scales down the resource consumption with a factor of $1/n_t$ without considering the available resource, and varying resource consumption can still be caused by the varying N_i.

Comparatively, from subsection 3.4 we have $n_{csim} \leq N_B$, $n_{cs}=2/(1-p) \leq N_B$, and $n_{ch}<N_B$. Besides, as we will show in subsection 3.7.3 and the simulation results, the additional message verification caused by ETV and PIMN is negligible compared to that of DBRV. Thus, overall RAMV results in relatively stable resource consumption bounded by the resource budget (N_B), which is more desirable than both BSL1 and BSL2.

3.7.1.2 Active Receivers of One Beacon

In RAMV, the number of active receivers (n_a) of a Beacon follows two theorems.

Theorem 1: Among all receivers at least one active receiver exists for any Beacon.

Proof: From both single-lane model and multi-lane model of relevance rank, any node A at least has 1 neighbor B such that $R_{BA}=0$. Meanwhile, all resource-aware algorithms in section 3.4 ensure that B will directly verify every Beacon from A if $R_{BA}=0$.

Theorem 2: In RAMV-S and RAMV-H, $E[n_a]$ also follows (3.6). In RAMV-SIM, $n_a=N_B$.

This theorem can easily be proven with the similar reasoning as shown in section 3.4.

Thus, RAMV ensures that any Beacon will be verified by at least 1 active receiver. Comparatively, BSL1 may actually leave a bunch of Beacons unchecked at the end of Tp, when resource is insufficient. In BSL2, one Beacon will be verified by any of its receivers with probability $(n_t-1)/n_t$. Thus, the probability that this Beacon is not verified by any receiver is $(n_t-1)^{N_i} / n_t^{N_i}$, which is non-zero as long as n_t is bigger than 1.

3.7.1.3 False Positive Ratio and False Negative Ratio

The false positive ratio is the probability that the receiver mistakes a valid Beacon as being invalid, and the false negative ratio is the probability that the receiver mistakes an invalid Beacon as being valid. The false positive ratio and false negative ratio are denoted as R_P and R_N, respectively.

In BSL1, the probability that one received Beacon will be verified by the receiver, Pr{Directly Verified}, is $\min(N_A/N_i, 1)$. Thus, if the receiver has sufficient resource it will verify all received Beacons, with $R_P=R_N=0$. When resource is insufficient, if the receiver regards all unchecked Beacons as invalid (let p_m denote the ratio of invalid Beacons), $R_P = (1-p_m)(N_i-N_A)/N_i$ and $R_N=0$; if the receiver regards unchecked Beacons as valid $R_P=0$ and $R_N = p_m(N_i-N_A)/N_i$. Thus, in BSL1, either R_P or R_N will be positive when the resource is insufficient. In case of BSL2, Pr{Unchecked}$=(n_t-1)/n_t$. Thus, with similar reasoning, R_P or R_N will also be quite large as long as n_t is bigger than 1, no matter whether the resource is sufficient or not.

In RAMV, with PIMN each Beacon is either directly verified by the receiver, or indirectly verified based on the presence or absence of notifications. Thus, R_P is the probability that one valid Beacon B_V is regarded as invalid due to the false notifications from some misbehaving neighbors. However, as discussed in section 3.5, with Approach II for indirect verification, this is impossible. With Approach I, R_P will be negligible, since the collusion among multiple misbehaving neighbors is required to successfully deceive the receiver.

In RAMV, R_N is the probability that one invalid Beacon B_I is regarded as valid due to the absence of any notifications. This is actually the probability that the notifications from n_a active receiver of B_I are all lost due to transmission collision or reception error, which generally is negligible when n_a is reasonably big. Thus, in RAMV, R_N is negligible as shown in the simulation results in section 3.8.

In summary, RAMV will result in much smaller R_N and R_P than both BSL1 and BSL2. Thus, RAMV can better support both traffic safety applications and reputation schemes in face of limited resource budget and high node density.

3.7.2 Security Properties

Given a resource budget, RAMV enables each node to directly verify as many important Beacons as possible to ensure reliable traffic safety applications. With PIMN each node can indirectly verify the Beacons which have not been directly verified, as discussed in subsection 3.5.2. Besides, RAMV also ensures that any Beacon will be verified by at least 1 neighbor, so that any invalid Beacon can be promptly detected by the receivers. Thus, RAMV shows salient safety and security properties while meeting the resource budget, as long as its design goals will not be disrupted by any potential attacks, which will be thoroughly investigated next.

In VANETs, it is reasonable to assume that most nodes will participate in RAMV honestly. The fact that a hardware security module (tampering-proof hardware) [36] can be used to protect the cryptographic materials implies that the Sybil attack will be quite impossible in VANETs. Even if one node somehow manages to launch the Sybil attack, the Sybil attack can be detected and handled by the existing schemes [64], and this node may be punished by the misbehaving node eviction schemes [90] or with reputation schemes [80], [86]. Thus, in RAMV we only consider the following attacks.

Invalid Data: One misbehaving node may intentionally send out Beacons with false position data. As discussed before, several neighbors of this node will work as active receivers and detect the invalid data through content verification. PIMN will ensure that most receivers of such Beacons will learn of their invalidity. Even based on the wrong positions, this node's Beacons will be verified as those of the normal nodes. Thus, it is impossible to allure any node into verifying more messages than its resource budget by broadcasting invalid positions.

One node may also send out numerous false safety-critical Beacons, which will incur additional resource consumption in the ETV module of the receivers and disrupt DBRV. Fortunately, ETV ensures that such fake critical Beacons will all be timely verified, so that the reputation of this node will be decreased sharply. After a while the Beacons from this node will be ignored and this node may be evicted from VANETs, as in [90].

Bad-mouthing: One node may send out a notification to wrongly accuse another node of broadcasting invalid Beacons in the bad-mouthing attack. As discussed in subsection

3.7.1, the false positive ratio of RAMV is negligible and the bad-mouthing attack can be effectively handled. Additionally, as discussed in PIMN, this node needs to attach its digital signature for the invalid notification, which can serve as proof to countermeasure against itself. In case of Approach II for indirect verification, one node may attempt to allure its neighbors into verifying more Beacons by attaching numerous invalid notifications to its Beacons. However, this attack can be easily detected by its neighbors, and its future notifications can be simply ignored. Thus, the resource consumption of any node will not be disrupted by the bad-mouthing attack.

3.7.3 Computation Complexity

To further corroborate the salient properties of RAMV in reducing resource consumption, the computation complexity of RAMV will be analyzed here.

In DBRV, the relevance ranks of all the (N_i) neighbors need to be updated upon receiving a Beacon. Thus, DBRV requires $10N_i \times N_i = O(N_i^2)$ comparisons for relevance rank updating each second. In PIMN, assuming that each node will send out invalid Beacons with probability p_m, $10N_i \times p_m$ piggybacking operations will be required per second. In reasonable scenarios p_m is small and this overhead is much smaller than the normal beaconing. In ETV, only 1 buffer operation will be incurred by each safety-critical Beacon, since the verification of the safety critical Beacon can be covered by the resource budget in DBRV. Assuming that the safety critical beacons are quite rare, this overhead of ETV is still acceptable.

Thus, DBRV incurs the biggest computation overhead among all modules of RAMV. However, most traffic safety applications also require regular update of the neighbor locations. Thus, the computation overhead of location and relevance rank update can actually be shared by RAMV and traffic safety applications. Even counting DBRV's computation overhead as it is, the overall computation overhead of RAMV may still be acceptable compared to the computation extensive cryptographic and mathematic operations of message verification algorithms.

3.7.4 Application Significance

RAMV makes message verification scalable and resource-aware in VANETs in face of increasing node density and massive message exchanges. Though proposed explicitly for

Beacons, RAMV is also easily applicable to other messages by slightly modifying the concept of relevance rank as discussed before. In VANETs, there will be many types of periodic messages necessitated by numerous applications, as discussed in section 3.1. Thus, RAMV is especially appealing to the realistic deployment of VANETs.

3.8 Simulations

A NS2 [169] based simulation with realistic vehicle mobility traces generated by MOVE [170] is constructed to evaluate RAMV. Totally 200 nodes are simulated within a 2000 by 3000 meters region. The simulation parameters are summarized in Table 3.1. In this simulation, each node on average has about 20 1-hop neighbors. Here for convenience, the resource consumption is measured with the unit of node as discussed in (3.2). RAMV will be compared with BSL1 and BSL2 in the following two scenarios.

Table 3.1
Simulation parameters of RAMV

Parameter	**Value**	**Parameter**	**Value**
# of vehicles	200	Bit-rate	6 Mbps
Road length	10km	T	100ms
R	300m	Average velocity	20m/s
MAC	802.11	Simulation Time	200s

3.8.1 Limited Resource Scenarios

In this scenario, VANET nodes do not have sufficient resource for message verification, either due to computation extensive cryptographic algorithms, or high node density. This scenario is common for realistic VANETs. Without struggling with technical details, we suppose that each node can only verify 120 Beacons or maintain 12 neighbors per second (N_A=12). As previously discussed, BSL1 and BSL2 will simply discard the Beacons pending for verification at the end of each second. In BSL2, we set n_t to 2, so that each node will verify every other received Beacon. In RAMV, resource budget N_B will be 2, 4, 5, 6, 7, 8, 10, 12, and filtering probability p will change accordingly.

Resource Consumption (N_C): In Figure 3.7, the N_C statistics for RAMV, BSL1, BSL2, as well as N_B, are shown. Figure 3.7 shows that all RAMV versions have N_C curves lower than the N_B curve and satisfyingly meet the resource Budget N_B. Note here that the resource consumption of RAMV includes that caused by PIMN and ETV.

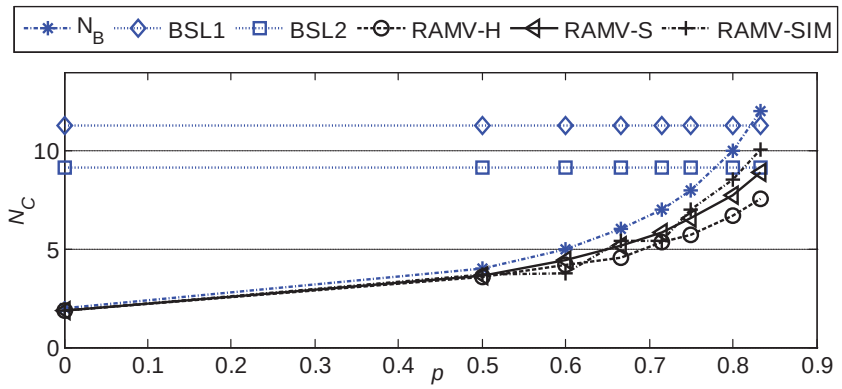

Figure 3.7 The resource consumption statistics of BSL and RAMV

As discussed in section 3.7, generally RAMV-SIM, RAMV-S and RAMV-H follow their resource budget increasingly more strictly. Thus, the differences between their N_C statistics in Figure 3.7 are reasonable. Comparatively, the resource consumption of BSL1 basically reaches N_A, so no sufficient resource is left for the other applications. BSL2, by only verifying one half of all received Beacons, leaves some resource for other applications. However, being not resource-aware, given higher node density even BSL2 will also face resource depletion.

In Figure 3.7, the fact that N_C of BSL1 is slightly smaller than 12 is caused by the Beacon loss in VANETs. The Beacon loss can be caused by the reception errors at the receiver side due to high vehicle mobility, or by MAC layer collisions of several simultaneously transmitting nodes. As indicated by the recent proof of concept tests [194] of the VII Consortium, Beacon loss is common in realistic VANETs. Thus, any receiver may only receive fewer than 10 Beacons from one neighbor per second, so the actual resource consumption of any node will be reduced. The Beacon loss also contributes to the gaps between the N_C curves of RAMV and the N_B curve in Figure 3.7.

Number of Active Receivers (n_a): As shown in Figure 3.8, the n_a data of all RAMV versions are larger than 1, and closely follow (3.6). Thus, the simulation results here corroborate Theorem 1 and Theorem 2 in subsection 3.7.1. In the lower sub-figure, the violation ratio (R_O) rigorously records the ratio of the Beacons with n_a=0 to all Beacons. Thus, R_O is the probability that one Beacon will not be verified by any receivers. For all RAMV versions, R_O is practically 0 (on the order of 10^{-4}), which is much lower than those of BSL1 and BSL2, as shown in Figure 3.8.

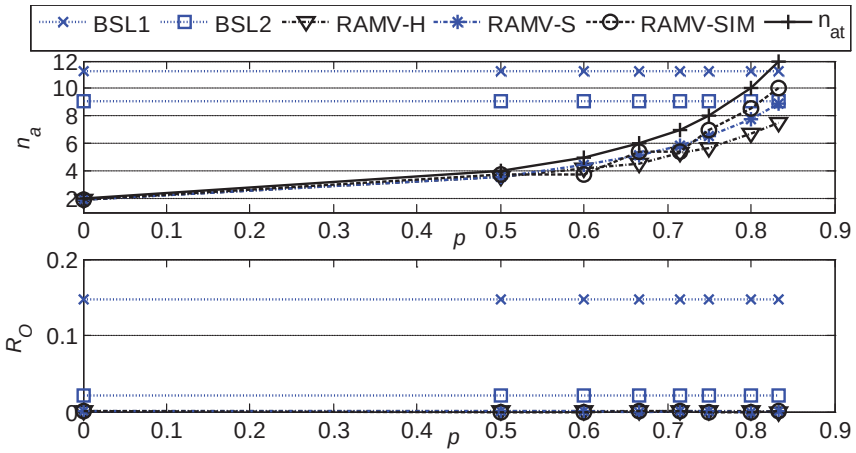

Figure 3.8 The numbers of active receivers of BSL and RAMV

Thus, with limited resource, RAMV practically ensures that any Beacon will be verified by at least one receiver, better supporting VANET applications than both BSL1 and BSL2. The theoretical n_a, n_{at}, is also shown in Figure 3.8, and the difference between n_{at} and the n_a curves of RAMV is also caused by Beacon loss in VANETs.

Ratio of Verification (R_V): In Figure 3.9, R_{V1} indicates the probability that one received Beacon will be *directly* verified in BSL1, BSL2 and RAMV. R_{V2} is the probability that one Beacon will be either *directly* or *indirectly* verified in RAMV. As shown in Figure 3.9, R_{V2} of RAMV-S, RAMV-H and RAMV-SIM is almost 1.0 for any N_B, while R_{V1} is generally smaller than 0.5. This shows that with limited resource budget only a portion of all received Beacons can be directly verified in RAMV. With the help of PIMN, almost all the remaining Beacons will be indirectly verified. Thus, in RAMV the false negative ratio R_N, which is equal to $p_m(1-R_{V2})$, is negligible, so RAMV ensures satisfying security strengths with limited budgets.

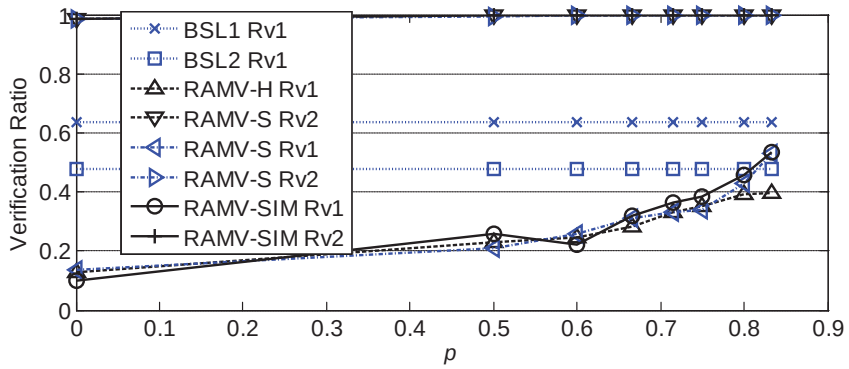

Figure 3.9 The ratios of verification of BSL and RAMV

Comparatively, both BSL1 and BSL2 need to rely on direct verification of the Beacons. When resource is not sufficient, as configured here, the R_{V1} curves of both BSL1 and BSL2 are about 70% and 50%, respectively. Thus in BSL1 and BSL2 about 30% and 50% received Beacons of any node will not be verified and their properties remain unknown, which is potentially harmful to the traffic safety applications and relevant security applications (e.g. reputation schemes).

3.8.2 Unlimited Resource Scenarios

In the idealistic scenario where each node always has unlimited resource to verify all received Beacons, the resource consumption variances (V_C) of BSL1, BSL2, and RAMV will be compared. Here, the resource consumption N_C of each node is calculated per 10 seconds. V_C is defined as $100(N_C - N_C^M)/N_C^M$, where N_C^M is the average of N_C over all periods. Basically, bigger V_C indicates higher variance of the resource consumption, and V_C=0 means that the resource consumption remains constant for every 10 seconds. As shown in Figure 3.10, both BSL1 and BSL2 have the same variances, which are much larger than those of RAMV in most periods. Basically, RAMV-H, RAMV-S and RAMV-SIM result in almost the same VC, which are within ±5% most of the time. Thus, RAMV, as previously discussed, can reduce the resource consumption variance of the individual nodes and better support the resource allocation algorithms.

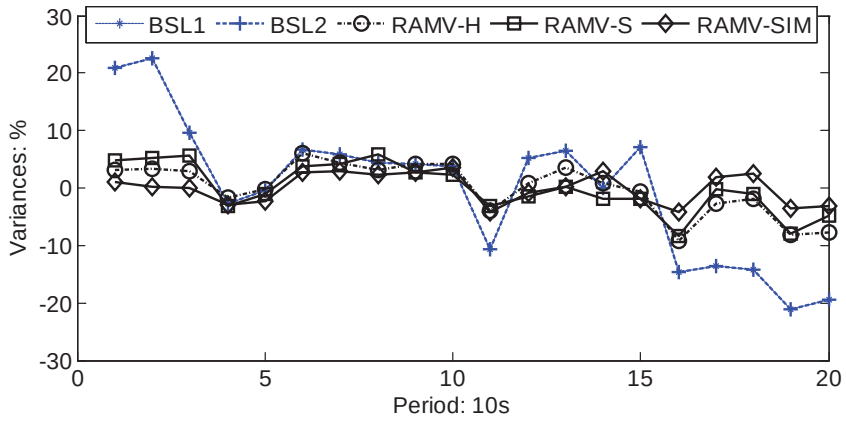

Figure 3.10 The resource consumption variances of BSL and RAMV

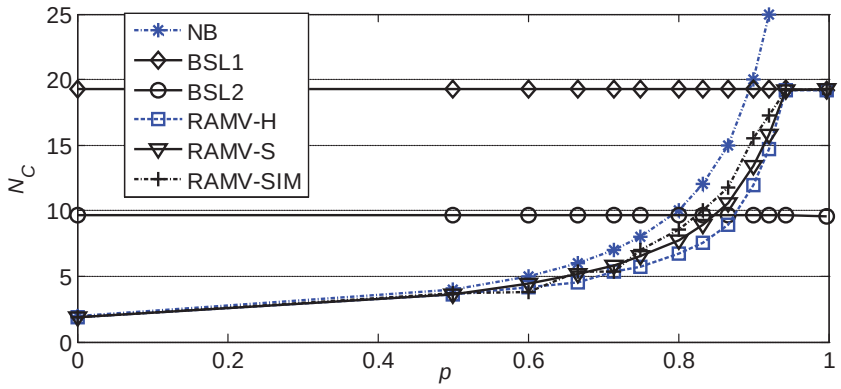

Figure 3.11 The full-fledged resource consumption statistics

In Figure 3.11, the full-fledged resource consumption (N_C) curves are shown, with N_B set to 2, 4, 5, 6, 7, 8, 10, 12, 15, 20, 25, 35, and 1000. Figure 3.11 proves again that RAMV can satisfyingly meet the preset resource budget N_B, resulting in configurable and predictable resource consumption. Although resource is assumed to be unlimited in this scenario, it is still meaningful to reduce the resource consumption as long as the relevant safety and security strengths will not suffer, as is the case with RAMV.

3.9 Summaries

Taking into consideration both the resource budget and the security requirements on message verification, RAMV is resource-aware, application-friendly and secure at the same time. Within RAMV, DBRV allows each node to spend its resource budget on the most relevant messages. ETV ensures that any critical messages which contain or raise a warning will be verified promptly, so that traffic safety will not suffer from DBRV and PIMN. The novel techniques in PIMN enable any node to learn the property of all received messages, so that the security of message verification is also ensured. Basically, RAMV allows the neighboring nodes to share the computation overhead in verifying the messages, and to share the message verification results. In this sense, the scalability issues in message verification are effectively handled.

Though only Beacons are explicitly considered in this chapter, RAMV can be easily applied to other types of messages in VANETs with the necessary modifications proposed in this chapter.

In conclusion, RAMV provides an efficient and secure solution to the verification of the numerous messages in VANETs, which threatens excessive resource consumption. RAMV can work in VANETs independently of the underlying cryptographic techniques, controlling the resource consumption of message verification to a desired budget. Besides, the safety and security requirements of message verification are all properly met. Thus, RAMV securely and realistically tackles the scalability issues in message verification in VANETs, which makes RAMV especially appealing to VANETs.

Chapter 4 Joint Privacy and Reputation Assurance[3]

In VANETs, privacy protection makes it challenging to maintain the reputation history of any node, while reputation management requires real-time reputation manifestation at risk of easier vehicle tracking. In this chapter, a Joint Privacy and Reputation Assurance (JPRA) scheme [145], [146] is proposed to reconcile these conflicts and support the synergistic coexistence of both schemes in VANETs. JPRA adopts a localized reputation management model where the behavior evaluation, reputation aggregation and reputation manifestation of each node are collectively performed by this node and its 1-hop neighbors. Within this model, a reputation relay algorithm and a neighbor-assisted reputation update algorithm support secure and efficient reputation management in face of node mobility and privacy protection. Besides, a conditional reputation discretization algorithm allows privacy-preserving reputation manifestation for the honest nodes. Theoretical analysis and simulations show that JPRA efficiently and synergistically supports reputation schemes and privacy schemes. Considering the necessity of both privacy protection and reputation management, JPRA is especially appealing to VANETs.

4.1 Introduction

As previously discussed, proper security provisioning is necessary [5], [20] to meet the critical security requirements of VANETs, such as data integrity, node authentication, reputation management, privacy protection, and so on. Extensive research has been conducted for each security requirement, as reviewed in our book chapter [5]. However, the conflicting requirements of different security schemes still call for thorough investigation to ensure their synergistic coexistence in VANETs.

This chapter is focused on jointly supporting reputation management and privacy protection in VANETs. Consisting of behavior evaluation, reputation aggregation and reputation manifestation, reputation management [103] serves to reward the

[3] The material contained in this chapter was submitted to *IEEE Transactions on Mobile Computing*. © 2012 IEEE. See Appendix C for a copy of the copyright permission from IEEE.

honest/complying nodes and punish the misbehaving ones in VANETs. Keeping the location and identity information of each node secret, usually with pseudonym changes, privacy protection is essential to the privacy-sensitive users [5] of VANETs. However, with different design goals, reputation management and privacy protection impose conflicting requirements to each other. Briefly speaking, reputation management requires that each node be continuously monitored to maintain a precise reputation history for this node. However, privacy protection mandates that each node, after changing its pseudonym, should not be recognized by its neighbors. Additionally, the manifested reputation of any node may provide an additional clue to the adversaries, potentially harming its privacy. These conflicting requirements, to be further discussed in section 4.2, have not been comprehensively investigated in literature. Thus, here a novel Joint Privacy and Reputation Assurance (JPRA) scheme is proposed to reconcile the inherent conflicts of these schemes and efficiently support both in VANETs.

JPRA adopts a localized reputation management model to facilitate efficient behavior evaluation, reputation aggregation and reputation manifestation in VANETs. In this model, each node uses a neighbor-certified reputation label to reflect its reputation history and its 1-hop neighbors [4] hold short-term reputation opinions for its recent behaviors. A novel *reputation relay* algorithm is proposed to ensure that the complete reputation information of any node is always locally maintained by itself and its neighbors, in face of frequent network topology changes caused by high node mobility and pseudonym changes. A *neighbor-assisted reputation label update* algorithm allows each node to honestly update its reputation label with the aid of its neighbors, which is made privacy-preserving with partially blind signature [195] based procedures. Moreover, to make reputation manifestation privacy-preserving, a *conditional reputation discretization algorithm* allows honest nodes to manifest a same reputation.

By comprehensively considering the unique characteristics of VANETs and the challenging conflicts of both schemes, JPRA supports the synergistic coexistence of both reputation management and privacy protection in VANETs. Extensive theoretical

[4] In this chapter, we only consider the 1-hop (direct) neighbors of each node. Thus, in this chapter each neighbor is a 1-hop neighbor, unless explicitly stated otherwise.

analysis and realistic simulations validate the effectiveness and efficiency of JPRA. Thus, JPRA is especially appealing to VANETs, considering the necessity of both schemes.

4.2 Related Work

In VANETs, *privacy protection* aims to conceal the real identity of each node from the potential adversaries, such as its neighbors and external observers [109]. To this end, pseudonyms, instead of real identities, are used in VANET communications [5]. A pseudonym is an temporary identifier without any obvious connection to the real identity, usually consisting of a node's public key certificate, IP address and MAC address [113]. However, by observing the location history and service accessing history of one node with the same pseudonym, an adversary may derive personal information to deduce its real identity. Thus, pseudonym change is commonly adopted [45], [62], [109], [113], [117], [119], [122], [124], [125], [127] to break down the location history and service accessing history of each node by making this node, after a pseudonym change, a totally new node. To this end, most privacy protection schemes enable several neighboring nodes to synchronize their pseudonym changes and remain silent for a random period afterward. This way, after resuming normal communications, these nodes become indistinguishable to the adversary with the location information and pseudonyms contained in their communications. Furthermore, when reputation is considered, it is also necessary to prevent the manifested reputation from uniquely identifying any node among its neighborhood, in order to make pseudonym change effective.

In VANETs, reputation management evaluates how honest/complying one node is regarding one specific application protocol with *behavior evaluation*, *reputation aggregation* and *reputation manifestation*. Specifically, the protocol-specific behaviors of each node will be evaluated by its neighbors. For instance, [76], [90], [143] allow the neighbors of each node to evaluate its periodical beacons and [78]-[80], [115], [155] allow the evaluation of the routing and data relaying behaviors. Generally, each neighbor will form its own opinion about this node's behaviors, called a *reputation segment* here.

Reputation aggregation refers to forming an overall reputation based on all reputation segments and the reputation history of one node. Existing reputation schemes [93], [95], [97], [98], [104], [105], [107], [196] propose reputation metrics and algorithms to

evaluate the reputation of each node for specific application protocols. For VANETs, one critical question is how reputation aggregation should be performed. In general mobile ad hoc networks, reputation aggregation can be performed in a centralized manner where a central authority aggregates the reputation segments for all nodes. Or it can be performed in a peer-to-peer manner where each node keeps the reputation segments for all other nodes and aggregates the reputation segments by querying the network. However, the centralized approach is unsuitable to VANETs, since in VANETs each node may only have a sporadic access to the central authority. The peer-to-peer approach will incur tremendous communication and storage overhead for each node, due to the high node mobility and numerous nodes of VANETs. Thus, the only feasible reputation aggregation approach for VANETs is for each node and its 1-hop neighbors to locally aggregate its reputation.

Reputation manifestation makes the reputation of each node visible and verifiable to its interacting parties. To make the reputation of each node trustworthy, it should be vouched for by a trustworthy entity, for example a central authority or a set of nodes.

Thus, by breaking down the pseudonym history of each node, privacy protection makes it even more challenging to precisely evaluate the behavior history of each node. Similarly, it becomes difficult to aggregate the reputation segments for any node with changing pseudonyms. Reputation manifestation also becomes difficult, since each node can simply evade its reputation by changing its pseudonym. On the other hand, the reputation manifested by each node becomes an additional property for this node, which could be exploited to profile this node and harm its privacy. To support both privacy protection and reputation management in VANETs, such conflicting requirements and VANETs' unique characteristics need to be thoroughly investigated.

Up to now, only [108] proposes a probabilistic reputation scheme to jointly consider privacy and reputation in VANETs. In [108], each node aggregates its own reputation in its Tamper-Proof Device (TPD) [11], [197], based on the reputation segments of its neighbors. However, a special TPD for reputation management cannot support various application protocols in VANETs, while adding various TPDs to support different application protocols may not be acceptable due to the incurred cost. Besides, [108] ignores the common attacks to reputation aggregation, e.g., blocking negative reputation

segments. More importantly, by directly manifesting the reputation value of each node, the privacy of each node may be harmed. Thus, JPRA is proposed as a novel and comprehensive solution to such challenging issues.

4.3 Background and Overview

4.3.1 Network Model and Assumptions

VANETs consist of the *ad hoc domain* and the *infrastructure domain* [5]. The ad hoc domain is formed by vehicles with Dedicated Short Range Communication (DSRC) [9] transceivers. Each node has multiple pseudonyms certified by the VANET (certificate) Authority and can change pseudonyms at will. A standard tamper-proof device (TPD) [11], [197] in each node keeps its cryptographic elements confidential and allows the usage of only one pseudonym at any time. Thus, the Sybil attack [63] is difficult in VANETs. To support traffic safety applications, each node periodically (with a period between 100 ms and 500 ms) broadcasts beacons containing its driving states, such as location, speed and driving direction [10]. It is assumed that the majority of nodes in VANETs are honest and complying regarding various application protocols.

In the infrastructure domain, RSUs serve to interface vehicular nodes and the VANET Authority, which is in charge of all major management and security functions in VANETs. Due to cost considerations, RSUs are sparsely deployed in VANETs, usually in road intersections. It is assumed that RSUs and Authority are always trustworthy.

4.3.2 JPRA Overview

JPRA adopts a localized reputation management model. As shown in Figure 4.1, in JPRA, the complete reputation information of each node (say node A) consists of a reputation label (RL_A) to indicate its long-term reputation and short-term reputation segments generated by its neighbors. Certified by K (K>0) neighbors, RL_A serves to honestly reflect A's long-term reputation history. Thus, to facilitate reputation manifestation and behavior evaluation, each neighbor of A should learn RL_A in time (Condition 1). To facilitate local reputation aggregation, at any time the 1-hop neighbors of A should keep all the reputation segments for A (Condition 2). Within this localized reputation management model, three novel algorithms are proposed to efficiently support both reputation management and privacy protection.

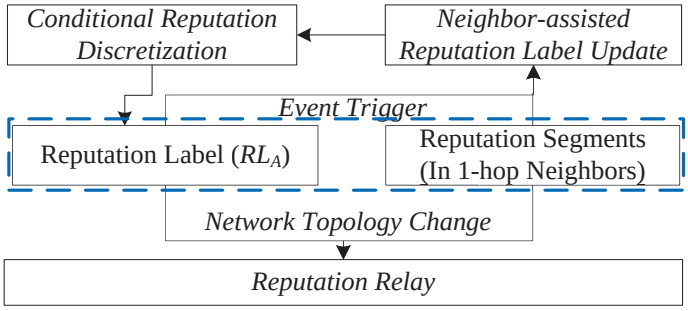

Figure 4.1 The system overview of JPRA

First, a novel *reputation relay* algorithm is proposed to meet both Condition 1 and Condition 2 in face of frequent network topology changes caused by high node mobility and pseudonym changes. Secure and efficient procedures are designed for *A*'s new neighbor to learn RL_A in time, and for *A*'s leaving neighbor to delegate its reputation segment to *A*'s staying neighbors. In this way, *A*'s complete reputation information is always maintained by itself and its neighbors, which makes reputation history maintenance and reputation aggregation efficient in VANETs.

Secondly, a *neighbor-assisted reputation label update* algorithm securely and efficiently updates RL_A in case of the expiration of RL_A, *A* leaving the current network cluster or *A*'s imminent pseudonym change. This way, at any time *A* will carry a valid and up-to-date reputation label. Especially, partially blind signature [195] based procedure is proposed to ensure that *A*'s new reputation label will be certified by *K* neighbors without revealing its new pseudonym in case of *A*'s pseudonym change.

Thirdly, to make reputation manifestation both precise and privacy-preserving, a *conditional reputation discretization* algorithm is proposed to enable the honest/complying nodes to manifest a same reputation label. As such, the reputation label cannot be exploited to harm the privacy of such honest/complying nodes.

With these novel algorithms, JPRA reconciles the challenging conflicts of reputation management and privacy protection, efficiently and synergistically supporting both.

4.3.3 Adversary Model

In JPRA, the most powerful adversary to the location privacy of vehicular nodes, namely the Global Passive Adversary (GPA) [117], [119], will be considered. A GPA can monitor all VANET communications to reconstruct the location history and application

accessing history of each node. When one node changes its pseudonym, GPA may attempt to link the old and new pseudonyms based on various information items, such as the movement trajectories, the application accessing, and the reputation values of the involved pseudonyms. Thus, if the manifested reputation of one node remains constant and unique within its neighborhood during the pseudonym change, its pseudonym change becomes futile. Given that the privacy protection schemes [45], [62], [109], [113], [117], [119], [122], [124], [125], [127] have already considered other information items, JPRA only needs to prevent the reputation manifestation from harming the pseudonym changes.

Regarding reputation management, the misbehaving nodes may selectively block the negative reputation segments from its neighbors and only accept the positive ones in reputation update. The misbehaving nodes may change their pseudonyms in order to get rid of their low reputation values. The misbehaving nodes may also launch a bad-mouthing attack by intentionally giving wrong reputation segments for its neighbors. Similarly, given that the bad-mouthing attack has been considered in the reputation aggregation algorithm, JPRA will be focused on the other two attacks.

Besides, in VANETs, one node may refuse to or fail to comply with the required communications due to misbehaviors or MAC layer collisions. JPRA will ensure reliable and efficient communications in face of these misbehaviors and malfunctions.

4.4 Localized Reputation Management

As previously discussed, JPRA locally manages the reputation of each node so that reputation aggregation can be resilient to the frequent network topology changes in VANETs. To this end, both reputation relay and reputation label update need to be securely and efficiently supported.

A network topology change may be incurred by the relative movement of nodes, as shown in Figure 4.2. When node *A* enters node *B*'s communication range, *A* needs to learn *B*'s reputation label RL_B and *B* needs to learn RL_A. To this end, a *reputation label notification* procedure is proposed. Hereafter, due to the symmetry of procedures, we will describe the procedures in JPRA in the light of one single node arbitrarily selected out of two neighboring nodes. While in *B*'s communication range, *A* will monitor *B*'s behaviors and form a reputation segment RS_{AB} for *B*.

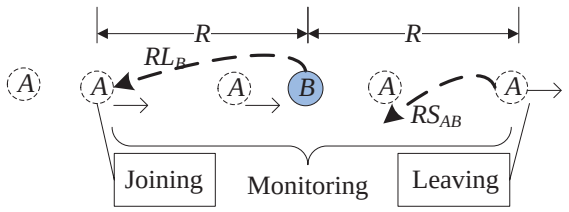

Figure 4.2 The message flows and interactions of an exemplary reputation relay

Before leaving *B*'s communication range, *A* needs to delegate RS_{AB} to one staying neighbor of *B*, so that RS_{AB} will be aggregated in *B*'s future reputation label update. To this end, a reputation segment delegation procedure is proposed. Thus, reputation relay includes both *reputation label notification* and *reputation segment delegation*.

Similarly, a pseudonym change will also result in the network topology change as shown in Figure 4.2. Specifically, the case where *A* changes its pseudonym to *A*' is similar to, regarding network topology, the case where node *A* leaves *B* and node *A*' comes to *B*'s communication range.

On the other hand, to make its reputation label up-to-date and trustworthy, each node needs to update its reputation label from time to time assisted by its neighbors. It is critical to ensure that each node will honestly update its reputation label based on the reputation segments of its neighbors, without harming its own privacy.

For clarity, the notations commonly used in the following subsections will be listed here. PR_X and PU_X indicate the private key and the public key of node *X*, respectively. $PU_X\{Msg\}$ is the message *Msg* encrypted with PU_X. $\{Msg\}PR_X$ is the digital signature of *Msg* generated with PR_X. $H(Msg)$ is the hash value of *Msg* generated by a standard hash function, for instance SHA-2 [168].

4.4.1 Reputation Label Notification

There exist three scenarios for reputation label notification: *a*) two nodes meeting each other, *b*) one node joining a new network cluster, and *c*) one node resuming its communications after a random silent period following a pseudonym change. To ensure efficient and reliable reputation label notification in face of node misbehaviors and communication issues, it is necessary to enable the neighboring nodes to collaboratively notify two newly meeting neighbors of each other's reputation label in all these scenarios.

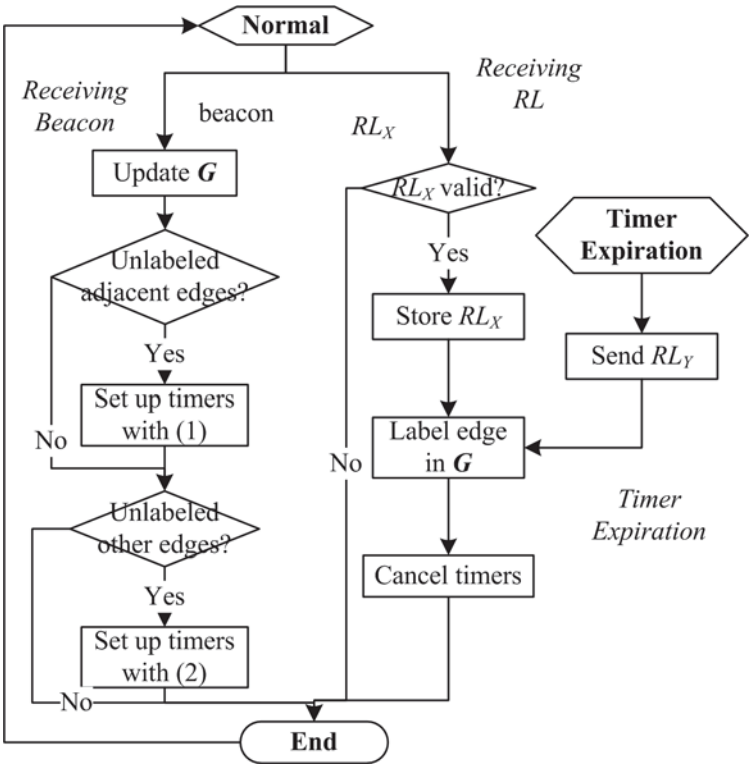

Figure 4.3 The detailed procedure of reputation label notification

In VANETs, with received beacons each node A can learn the locations of its neighbors ($Nei(A)$) and maintain a directed graph $\boldsymbol{G} = <\boldsymbol{V}, \boldsymbol{E}>$ to model its neighborhood. Here, the vertex set $\boldsymbol{V}$ contains both A and $Nei(A)$. The edge set $\boldsymbol{E}$ contains two directed edges (XY and YX) for two nodes X and Y, if $X, Y \in \boldsymbol{V}$ and their distance is no larger than R. Here, R is the common communication range of vehicular nodes. Based on $\boldsymbol{G}$, node A uses a binary value $Labeled(XY)$ to indicate whether node X has learnt node Y's reputation label or not. As shown in Figure 4.3, A will continuously check $\boldsymbol{G}$ and try to make each edge in $\boldsymbol{G}$ labeled, that is, to make all nodes in $\boldsymbol{V}$ learn one another's reputation label. Specifically, the detailed algorithm consists of the following major procedures.

Beacon Triggered Timer Setting: As shown in the left branch of Figure 4.3, upon overhearing a beacon, A will update $\boldsymbol{G}$ based on the location information in this beacon. Afterward, A will check the edges adjacent to A in $\boldsymbol{G}$ (XA, $X \in Nei(A)$) for the unlabeled edges, each of which indicates one node in need of RL_A. For each such unlabeled edge, A will set up a timer T_{XA} for sending (*via uni-cast*) RL_A to node X with the duration

$$t_{xa} = I(|Mid(A,X)|)T_0 \times d_{AX}/R. \quad (4.1)$$

Here, $Mid(A,X)$ is the set of nodes geographically between A and X. $I()$ is an indicator function which outputs 1 for non-zero inputs and outputs 0 for the input of zero. T_0 is the unit duration for such timers, which could be configured based on network parameters of VANETs. d_{AX} is the distance between A and X. Thus, (4.1) ensures that A will immediately send RL_A to X if there is no neighbor between A and X. However, A will first wait for the intermediate neighbors to send RL_A so that more neighbors of node X can also overhear RL_A to increase the effective coverage of RL_A.

Then, A will check the edges without A in $\boldsymbol{G}(XY, X, Y \in Nei(A))$ for the unlabeled edges such that A is geographically between the two nodes adjacent to each edge. For each such edge, say XY, if A knows RL_Y A will set up a timer T_{XY} with the duration as

$$t_{xy} = T_0 d_{AX}/R. \tag{4.2}$$

Equation (4.2) ensures that the node nearest to X will be the first to forward Y's reputation label (RL_Y) to X, so that most of X's 1-hop neighbors can overhear RL_Y as well.

Reputation Label Overhearing: Upon overhearing a reputation label RL_X, as shown in the middle branch of Figure 4.3, A will first store RL_X. Based on the position of the sender of RL_X, A can figure out its neighbors which can also overhear RL_X. Then, the associated unlabeled edges in $\boldsymbol{G}$ will be labeled and the associated timers will be canceled.

Timer Expiration: When a timer T_{XY} expires as shown in the right branch of Figure 4.3, A will send the required reputation label RL_Y to the desired receiver X via uni-cast. Afterward, A will also mark the associated edges in $\boldsymbol{G}$ as labeled by checking the nodes in $Nei(A)$ which can also overhear RL_Y.

The above procedures are based on uni-cast communications, so MAC layer collision is reduced. Thus, with this algorithm, the neighboring nodes can cooperatively perform efficient and reliable reputation relay when two nodes becomes new neighbors in any scenarios. Even if some neighbors may refuse to relay reputation labels, these two new neighbors can learn each other's reputation label as long as they have one cooperative neighbor in common or both nodes are honest.

The above procedure is suitable to the cases where two nodes meet each other due to relative mobility or node A joins a network cluster. However, when node A resumes its communications after its pseudonym change, none of its neighbors has any idea of its

reputation label RL_A. Thus, A should first broadcast RL_A as soon as it resumes communications. On the other hand, A's neighbors will follow the above procedures to notify it of the reputation labels of its neighbors.

4.4.2 Reputation Segment Delegation

In JPRA, when two neighbors leave each other's communication range, each node needs to delegate its reputation segment for the other to one staying neighbor of that node. In this way, all the reputation segments of any node will be locally available for future reputation update.

Within the same network cluster, two nodes (A and B) may leave each other's communication range due to their relative movement. In this case, A and B will find the best neighbors to keep their reputation segments for each other based on the *expected remaining connected time* (CT). For instance, B will estimate the CT of each node X in $Nei(A) \cap Nei(B)$ regarding A, as

$$CT_{XA} = \begin{cases} (d_{XA} + R)/(v_X - v_A), v_X > v_A \\ (R - d_{XA})/(v_A - v_X), v_A > v_X \\ +\infty, \quad , v_A = v_X \end{cases}. \tag{4.3}$$

In (4.3), v_A and v_X are the current speed of A and X, respectively. d_{XA} is the distance between X and A. Thus, bigger value of CT_{XA} indicates that X may remain as A's neighbor for a longer time, which enables X to better aggregate the reputation segment for A. Similarly, the best neighbor could be also selected based on other metrics, for instance, the reputations of the neighbors.

Suppose node D has the largest CT_{DA}, B will send (via uni-cast) its reputation segment for A (RS_{BA}) to D. Upon receiving RS_{BA}, D is expected to aggregate RS_{BA} with its own reputation segment for A, RS_{DA}. Similarly, A will also send RS_{AB} to the node with the largest CT value regarding B.

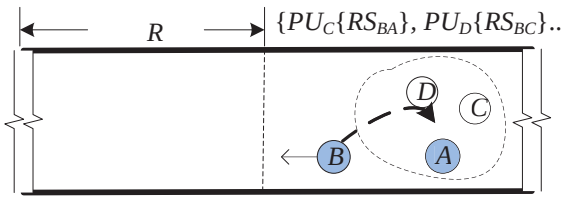

Figure 4.4 The example of node B leaving a network cluster

Node *B* may leave the current network cluster and entering a road segment without any 1-hop neighbors (called *network void*), as shown in Figure 4.4. In this case, the reputation label update procedure will be triggered, as discussed in subsection 4.4.3. Additionally, *B* needs to delegate its reputation segments for all its 1-hop neighbors. To be efficient, *B* will broadcast a message containing all reputation segments to be delegated. Each reputation segment is encrypted with the public key of the intended receiver, as

$RS\_Delegation = \{Payload=\{Type, TSP, Y, PU_Y\{rs_{BX}\}, X, PU_X\{rs_{BZ}\} \ldots\}, \{H(Payload)\}PR_B\}$.

Here, *Type* indicates the type of this message, and *TSP* is the timestamp generated by *B*. The certificate of node *B* is not contained in *RS_Delegation*, due to its presence in *B*'s beacons. Thus, upon overhearing this message, each node can find the reputation segment intended for itself. To ensure that each neighbor will receive this reputation segment, node *B* may broadcast this message for n_t times, where n_t is determined by the probability that *B* can receive the beacons from its neighbors, as discussed in subsection 4.4.3.

In case that *B* decides to change its pseudonym, it also needs to delegate its reputation segments for its neighbors similarly to the scenario of leaving the current network cluster.

4.4.3 Neighbor-Assisted Reputation Label Update

To keep its reputation label up-to-date and trustworthy, each node *A* needs to update its reputation label (RL_A) with the aid of its neighbors, if 1) (***Event* 1**) the remaining valid time of RL_A is smaller than a preset threshold t_m; 2) (***Event* 2)** *A* is leaving the current network cluster or 3) (***Event* 3)** *A* will change its pseudonym. Overall, to update *A*'s reputation label involves two challenging procedures: *a*) to aggregate the reputation segments generated by *A*'s neighbors, and *b*) to get the new reputation label of *A* certified by *K* neighbors. Here, *K* is a *security threshold* to trade off the trustworthiness of the reputation label and the communication overhead, the configuration of which will be discussed in detail in subsection 4.6.3.

Here, it is challenging to ensure that *A* updates RL_A honestly and has only one valid RL_A at any time. It is critical to conceal the connection between *A*'s pseudonyms during reputation label update. To address these challenges, a secure and privacy-preserving neighbor-assisted reputation label update algorithm is proposed with three phases.

4.4.3.1 Phase 1: Reputation Segments Aggregation

To update its reputation label, node *A* will first broadcast an *RS_Query* message to notify its neighbors of its intention to collect the reputation segments, as shown in Figure 4.5. Upon receiving *RS_Query*, each of *A*'s neighbors, say node *X*, will check whether it has a reputation segment for *A* or not. If not, *RS_Query* will be ignored. Otherwise, *X* will broadcast its reputation segment for *A* (RS_{XA}) with a period T_P for n_{rx} times, as shown in Figure 4.5. Here, n_{rx} is

$$n_{rx} = \lceil 1/\, p_{ax} \rceil . \tag{4.4}$$

In (4.4), p_{ax} is the probability that each beacon from *A* is successfully received by node *X*, which can be estimated by *X* based on the timing information in *A*'s beacons. Thus, (4.4) ensures that with a high probability at least one copy of RS_{XA} will be successfully received by *A*. By setting T_P to 100 ms, within one second *A* can receive all reputation segments from its neighbors. Then, *A* will broadcast the aggregated reputation segments so that *A*'s neighbors can also learn all reputation segments for *A*.

To ensure data integrity and authenticity, secure message formats are designed for both *RS_Query* and RS_{XA}, as follows.

$RS\_Query=\{Payload=\{Type=Query, Event, TSP_A\}, \{H(Payload)\}PR_A\}$.

$RS_{XA}=\{Payload=\{Type=RS, Target=A, rs_{xa}, TSP_X\}, \{H(Payload)\}PR_X\}$.

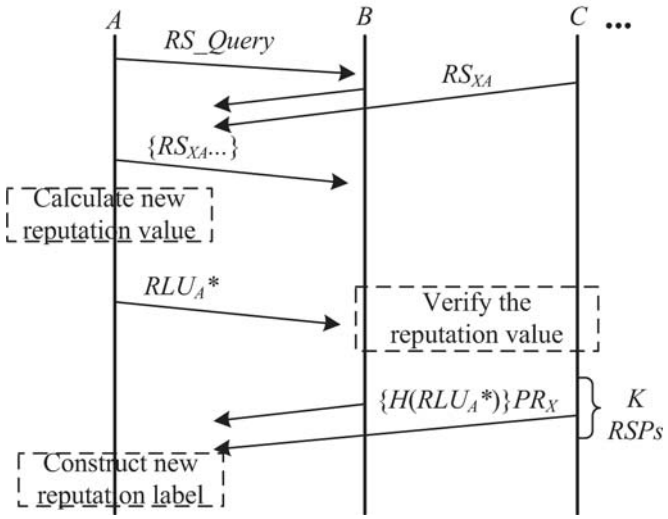

Figure 4.5 The detailed message flows of reputation label update

Here, *Type* indicates the message type and *Event* specifies the event trigger. TSP_A is the current timestamp generated by *A*. *Target* indicates the target of the reputation segment and rs_{xa} is the reputation value generated by *X* for *A*. Similarly, for efficiency the sender's certificate is not present in these messages.

4.4.3.2 Phase 2: Reputation Label Update

After collecting the reputation segments, *A* will calculate its new reputation label as

$$rl_a^* = Update(rl_a, \{rs_{xa}\ldots\}). \quad (4.5)$$

Besides, each neighbor of *A*, say *Y*, will also calculate its version of $rl^{(y)}_a$, as

$$rl^{(y)}_a = Update(rl_a, \{rs_{xa}\ldots\}). \quad (4.6)$$

Here, the function *Update*() can be adopted from the existing reputation aggregation schemes [93], [95], [97], [98], [104], [105], [107], [196]. For instance, a simple *Update*() function will be introduced in our simulation in section 4.7. As previously discussed, in Phase 1 *A* and its neighbors have received the same set of reputation segments ($\{rs_{xa}\ldots\}$) for *A*, so they will form the same reputation label for *A* in (4.5) and (4.6).

Based on rl_a^*, *A* will construct its reputation label update request RLU_A^*, and broadcast it as shown in Figure 4.5. Upon overhearing RLU_A^*, each node is able to verify RLU_A^* according to the following rules. First, rl_a^* should be consistent to the reputation label calculated by itself. Secondly, the starting time and ending time in this message should be correct. Once a node *X* accepts RLU_A^* as being valid, it will set up a timer T_{RX} based on its distance to *A*, with the duration

$$t_{rx} = uni(d_{XA}/R)\times T_P. \quad (4.7)$$

In (4.7), *uni*(*x*) is a function to randomly select a value in the range [0, *x*], following the uniform distribution. If T_{RX} expires, *X* will send its signature on RLU_A^* in RSP_X to *A* (via unicast) as shown in Figure 4.5. Each node will keep track of the RSPs already sent to *A*. Once *K* RSPs are overheard, each node with a running timer will cancel its timer.

To ensure message integrity, authenticity, and privacy protection, secure message formats are designed for these messages.

$RLU_A^* = \{Payload=\{Type, TSP, T_S, T_E, A, rl_a^*\}, \{H(Payload)\}PR_A\}$.

Here, T_S and T_E indicate the starting and ending time for this reputation label. Generally, T_S should be the current time and T_E should be set to T_S+T_C, where T_C is a

preset period for reputation label update as discussed in subsection 4.6.4. If A plans to change its pseudonym (Event 3), it will apply a function *blind*() on its new pseudonym (AN) in RLU_A*, so that RLU_A* becomes

$RLU_{blind(AN)}$*= {*Payload*={*Type*, *TSP*, T_S, T_E, *blind*(*AN*), rl_a*}, {*H*(*Payload*)}PR_{AN}}.

The *blind*() function can be found in any common partially blind signature scheme [195]. With partially blind signature, another node can sign RLU_A* without any clue of AN. After obtaining a signature on $RLU_{blind(AN)}$*, A can reverse the *blind*() function in the signature to get a correct signature for its intended message:

RLU_{AN}* = {*Payload*={*Type*, *TSP*, T_S, T_E, *AN*, RL_A*}, {*H*(*Payload*)}PR_{AN}}.

Thus, with partially blind signature [195], A can get a correct signature of RLU_{AN}* containing, without revealing its new pseudonym AN to the signers. Besides, as discussed in subsection 4.6.1, A is forced to generate a valid $RLU_{blind(AN)}$* with its valid pseudonym AN, to make its new reputation label acceptable to its future neighbors.

The message format of RSP_X is RSP_X={*H*(RLU_A*)}PR_X. After receiving K RSPs, A can construct a complete reputation label packet as RL_A*={RLU_A*, {RSP_X…}, {$CERT_X$…}}, where $CERT_X$ is the certificate of node X. Thus, with valid signatures from K nodes, RL_A* will be accepted as being valid by A's future neighbors.

4.4.3.3 Phase 3: RL Revocation Notification (RRN) Broadcast

In case of Event 2 and Event 3, if the remaining valid time (t_r) of RL_A is larger than the threshold t_m, RL_A needs to be revoked to ensure that at any time each node (A) only has one valid reputation label. In this way, even if the new RL_A* is worse than RL_A, A is forced to use RL_A* in its future communications.

To this end, each neighbor X, in sending out RSP_X as discussed above, will also send out a revocation for the current reputation label RL_A as REV_X={*H*(RL_A)}PR_X. The reputation label revocation notification (RRN) is constructed as RRN_A = {A, {REV_X…}, {$CERT_X$…}}. After collecting K RSP messages and K REV messages, node A is expected to construct and send out RRN_A. To ensure reliability, each neighbor (X) of A will start a timer T_{NX} with the duration as

$$t_{nx} = uni(d_{XA}/R)\times T_P. \quad (4.8)$$

If T_{NX} expires, X will send out RRN_A. Upon overhearing a valid RRN_A, each node with a running timer will cancel its timer.

To notify all relevant nodes of this revoked RL_A, RRN_A will be broadcasted to all nodes which may become the neighbors of A within the duration of t_r. To this end, RPB-MD [166] or any controlled flooding scheme can be adopted to broadcast RRN_A to all the nodes within a certain relative distance (L) from A.

In highway scenarios, it suffices to make A's future neighbors for the next t_r learn RRN_A. Thus, based on the feasible speed difference Δv, the relative distance L can be estimated as

$$L = t_r \times \Delta v. \tag{4.9}$$

Then, from (4.9) RRN_A needs to be sent to all nodes within distance L from A. The communication overhead is L/R in idealistic broadcast scenarios.

In downtown areas, A and its neighbors may make a turn at any road intersection. Thus, RRN_A should be disseminated to any neighbor of A no matter how A turns at the road intersections. Here, to be efficient and reliable, we propose that in each road intersection one neighbor of A broadcasts RRN_A to the vehicles in the future road segment A is about to turn to. In this case, the distance travelled by A within time t_r is

$$L = t_r \times v_M. \tag{4.10}$$

In (4.10), v_M is the speed limit in the concerned downtown area. Thus, the communication overhead becomes L/R revocation message relaying.

4.5 Reputation Considerations

To avoid reinventing the wheel, here the details of the reputation management schemes are omitted and only relevant considerations specific to JPRA will be discussed.

4.5.1 Reputation Label Verification

Considering the possibility of one misbehaving node evading its bad reputation label with pseudonym change, here several rules for reputation label verification are presented. Specifically, the reputation label RL_A of a node A is regarded as valid, if all following conditions are met: *a*) the pseudonym in RL_A is the same as the pseudonym currently used by node A; *b*) the T_E parameter in RL_A is still larger than the current system time; *c*) RL_A contains K valid signatures and *d*) RL_A is not revoked with a RL revocation notification

(RRN). On the other hand, a node without a valid reputation label will be treated by its neighbors as a node with the lowest possible reputation value in JPRA. If this node wants to get a valid reputation label again, its neighbors will only certify a reputation label with the lowest reputation value for it. Specially, when a node A joins a network cluster with RL_A just expiring less than $T_C/2$ ago, its neighbors will still update A's reputation label based on RL_A. This is to allow for the possibility that A unfortunately runs into an abnormally large network void.

The above rules, together with reputation relay and reputation label update, allow each node to timely update its reputation label. Besides, any node trying to evading its bad reputation will be punished with the lowest reputation value, so that each node is encouraged to timely update its reputation label in VANETs.

4.5.2 Conditional Reputation Discretization

The reputation of each node may uniquely identify this node within its neighborhood, so its pseudonym change can be easily traced by the GPA. Here, we first model the tradeoff between privacy and reputation. Suppose a synchronized pseudonym change involves n nodes. Without loss of generality, suppose the reputation's range is [0, 1], with 0 being the smallest value. Let Δr be the definition (accuracy) of the manifested reputation, so that the each node's reputation can only be one value out of $\Phi(\Delta r) = \{0, \Delta r, 2\Delta r, \ldots, 1\}$. For brevity, we assume that each node's reputation at the time of the pseudonym change is a uniform distribution over $\Phi(\Delta r)$. Considering any node with a certain reputation, the probability that its reputation is unique among these n nodes is

$$P_{uni}(n) = \left(\frac{|\Phi(\Delta r)| - 1}{|\Phi(\Delta r)|} \right)^{n-1}. \tag{4.11}$$

In (4.11), $|\Phi(\Delta r)| = 1/\Delta r + 1$. So, from (4.11) we have

$$P_{uni}(n) = \left[1/(1+\Delta r) \right]^{n-1}. \tag{4.12}$$

For $n \geq 2$, $P_{uni}(n) \rightarrow 1$ as $\Delta r \rightarrow 0$; $P_{uni}(n)$ decreases as Δr increases. Thus, (4.12) formally shows the intrinsic tradeoff between reputation manifestation and privacy protection.

On the other hand, the manifested reputation cannot be too ambiguous either. Otherwise, the design goals of reputation management may be contradicted. To achieve a

proper tradeoff between the precision and ambiguity of the manifested reputation, here a *conditional reputation discretization algorithm* is proposed to differentiate the honest nodes and the misbehaving nodes. This algorithm forces each node to manifest its reputation as

$$rl = \begin{cases} r_t, rv \in [r_t, 1.00] \\ rv, rv \in [0.00, r_t) \end{cases}. \tag{4.13}$$

Here, rv is the exact reputation value as calculated by A and its 1-hop neighbors based on rl_a and the aggregated reputation segments in (4.5) and (4.6). The value r_t is a system level reputation threshold, which is the reputation value of one typical honest node with only random errors. Thus, r_t can be easily determined based on the nature of the concerned application and the reliability of common vehicle nodes. r_t usually should be a value quite close to 1.0, e.g., 0.95.

The discretization in (4.13) ensures that any node with a reputation value bigger than r_t will manifest a common reputation value r_t. Thus, the reputation manifestation will not harm the privacy of such nodes. Comparatively, the other nodes with a reputation value smaller than r_t will have to display their own exact reputation value, which may harm its privacy. Thus, each node is encouraged to comply with the application protocols by not only reputation considerations but also privacy considerations.

Formally, let $p_m \in [0, 1]$ be the ratio of misbehaving nodes in VANETs. Then, among the n nodes in a synchronized pseudonym change, the probability of one honest node manifesting a unique reputation label is the probability that the other $n-1$ nodes are all misbehaving. So,

$$\Pr\{Unique|Honest\} = (p_m)^{n-1}. \tag{4.14}$$

In (4.14), p_m commonly is close to 0, so $\Pr\{Unique|Honest\}$ is also close to 0. Comparatively, each misbehaving node has $\Delta r \rightarrow 0$, so its manifested reputation will be most likely to be unique.

Besides being novel, this algorithm is also feasible in VANETs. First of all, (4.13) necessarily trades off the precision of the reputation value for the support of privacy protection. As previously discussed, by manifesting the exact reputation value each node may display a unique property in communications, which may make its pseudonym

changes futile. Thus, to make reputation manifestation compatible with privacy protection, the only option is to discretize the exact reputation value, as in (4.13). Secondly, one common philosophy adopted in many reputation aggregation algorithms [93], [95], [97], [98], [196] is that the reputation will be decreased sharply when one node with a high reputation misbehaves. Another common philosophy is to adopt a forgetting factor to put more weight on the current behaviors of each node in reputation aggregation. Thus, in JPRA any node deviating from the application protocol will find its reputation quickly decreasing to a value smaller than r_t. Thus, our algorithm still serves to encourage the complying behaviors in VANETs.

4.5.3 Feasibility of JPRA

Generally, the common reputation schemes [93], [95], [97], [98], [104], [105], [107], [196] can be supported by JPRA, since they all assume a certain entity to aggregate reputation for each node. In JPRA, each node will serve as such an entity to aggregate its own reputation, assisted and monitored by its neighbors. In this sense, JPRA can support reputation schemes for VANETs.

On the other hand, though JPRA assumes a partially blind signature in VANETs, JPRA can still work with a certificate scheme based normal public key cryptography algorithms. In this case, in neighbor-assisted reputation label update each node (*A*) can establish a session secret key with each of its 1-hop neighbors while broadcasting *RS_Query*, which can serve as the *blind*() function. Here, though *A*'s new pseudonym is known to its 1-hop neighbors, it will be still concealed from GPA, the most powerful privacy adversary. Due to high node mobility, *A*'s 1-hop neighbors keep changing, so *A*'s privacy can still be protected during its reputation label updates.

However, the trust schemes based on the chain of recommendation or authentication [100], [102] cannot be supported in JPRA. Such trust schemes involve not only the close relation between reputation and pseudonym, but also the long latency between evaluating one node and reevaluating the same node. Thus, the neighbor monitoring approach in JPRA is not suitable for such trust schemes. The coexistence of such trust schemes and privacy protection will be investigated in our future work.

4.6 Property and Performance

4.6.1 Security Properties

JPRA is resilient to various attacks to privacy and reputation. First, no node can block the negative evaluations (reputation segments) from its neighbors, since its reputation aggregation is monitored by its neighbors. Thus, any node can only get a valid reputation label certified by its neighbors. Secondly, JPRA ensures that at any time each node can either manifest a valid reputation label or be treated as a node with the lowest reputation label. Thirdly, in case of pseudonym change, neighbor-assisted reputation label update ensures honest reputation label update, so no node can evade its reputation by pseudonym change. Lastly, with conditional reputation discretization, by observing the reputation labels no one can gain any additional information about one honest node.

With the partially blind signature-based procedure in JPRA, one malicious node *A* may attempt to create a reputation label, with the correct rl_a and the pseudonym of another node *B*. *A*'s neighbors cannot detect this discrepancy in the pseudonyms. However, such an attack cannot work unless *A* and *B* are colluding, since it's impossible for *A* to guess the next pseudonym of *B*. If *A* and *B* are colluding, which is very rare in VANETs due to high node mobility, by doing so *A* and *B* as a whole do not gain anything in light of reputation value. Thus, such an attack has no practical significance. Besides, each node *A* is forced to generate $RLU_{blind(AN)}$* with valid digital signature, even though at the time of reputation label update its neighbors cannot verify the digital signature. Otherwise, after its pseudonym change, its new reputation label will be rejected by its neighbors due to the invalid digital signature in $RLU_{blind(AN)}$*.

Besides, in JPRA the conditional discretization of reputation value can further punish the misbehaving nodes by assigning to them unique reputation labels. Thus, the privacy concerns will drive the common nodes to comply with the specific application protocols to keep their reputation higher than the threshold.

4.6.2 The High Efficiency of JPRA

In light of communication overhead, JPRA is more efficient than any possible approach to implement reputation schemes for VANETs. The common reputation schemes imply two design principles: 1) to ensure reliability, all nodes able to monitor

one node should generate reputation segments for this node; 2) all reputation segments for one node should be aggregated to form an authentic reputation for this node. With these principles, the aggregation of the reputation segments from each node's (A) 1-hop neighbors, the dominating part of communication overhead, will be necessary in any possible implementation approach. For instance, one approach is to aggregate A's reputation segments in a centralized entity in VANETs, which may incur higher communication overhead due to multi-hop communications necessary for any node to access this centralized entity. Another approach is to aggregate A's reputation segments into A itself, as adopted in [108] and JPRA, which only incurs 1-hop communications. Indeed, in JPRA the aggregation of reputation segments only occurs when made necessary by node mobility or pseudonym changes, as discussed in subsection 4.4.3. Each neighbor of A will locally aggregate its reputation segments for A first, and relay the aggregated reputation segment to A only when required by A. Thus, in principle JPRA is more efficient than any other approach to implement reputation schemes in VANETs.

4.6.3 Communication Overhead & Latency Analysis

Here, the communication overhead and communication latency incurred by each of the algorithms of JPRA are theoretically estimated.

4.6.3.1 Reputation Label Notification

As discussed in subsection 4.4.1, when two nodes (say A and B) enter each other's communication range, two reputation label messages need to be sent to notify them of each other's reputation label. Thus, the communication overhead here is constant and independent of the network conditions, for example the presence of misbehaving nodes.

Regarding communication latency, the timer duration depends on the distance (d) between B and its nearest neighbor, or B and A if there is no neighbor in between. Thus, assuming the nodes between B and A are uniformly distributed for simplicity, we have

$$d = \begin{cases} 1/\rho, & Neighbors \\ R, & NoNeighbor \end{cases}. \tag{4.15}$$

Here, ρ is the node density, with unit of node/meter. Following the norm of traffic modeling, we assume that the node distribution follows the Geographic Poisson

Distribution [198] in VANETs. Thus, the probability that there is no neighbor (Pr{*NoNeighbor*}) or there are multiple neighbors (Pr{*Neighbors*}) between *A* and *B* can be estimated as

$$\Pr\{Neighbors\} = \sum_{i=2}^{\infty} \Pr\{k = i \mid i > 0\} = \frac{1 - e^{-\rho R} - \rho R e^{-\rho R}}{1 - e^{-\rho R}}. \tag{4.16}$$

$$\Pr\{NoNeighbor\} = \Pr\{k = 1 \mid i > 0\} = \frac{\rho R e^{-\rho R}}{1 - e^{-\rho R}}. \tag{4.17}$$

Thus, without considering the misbehaving nodes, the communication latency for one reputation label message can be derived from (4.15)-(4.17) as

$$\begin{aligned} \tau &= \frac{d}{R} T_0 \times \Pr\{Neighobrs\} + 0 \times \Pr\{NoNeighbor\} + \tau_0 \\ &= \frac{(1 - e^{-\rho R} - \rho R e^{-\rho R}) T_0}{(1 - e^{-\rho R}) \rho R} + \tau_0 \end{aligned}. \tag{4.18}$$

Here, τ_0 is the average latency for a successful MAC access in VANETs. Thus, (4.18) shows that the expected latency is smaller than (τ_0+T_0). Even considering the probability that any intermediate node may refuse to relay RL_A, the largest possible latency is still bounded by (τ_0+T_0) when *A* needs to send RL_A to *B* by itself.

Besides, if a node *B* just joins a new network cluster or resumes communication after a pseudonym change, suppose there totally are n_a nodes within *B*'s communication range. The reputation label exchange will incur exactly n_a reputation label messages, including 1 message from *B* and (n_a−1) messages from *B*'s neighbors. Besides, regardless of the misbehaving nodes, the total latency is

$$\tau = n_a \tau_0 + T_0. \tag{4.19}$$

Equation (4.19) holds, since the maximal timer duration is T_0, and each reputation label message will incur τ_0 due to the uni-cast communications. Thus, the latency of reputation label notification in this case mainly depends on the node density around each node.

4.6.3.2 Reputation Segment Delegation

As discussed in subsection 4.4.2, when two neighbors leave each other, the total communication overhead is at most 2 reputation segments. Similarly, due to the lack of timers in this process, the communication latency is at most $2\tau_0$.

If a node B leaves a network cluster or stops communication for pseudonym change, let n_t indicate the number of rebroadcasts of node B for reliable reception of the reputation segment message. Thus, the total communication overhead is n_t reputation segment messages, and the latency is $n_t \times T_P$, where T_P is the period for rebroadcasts.

4.6.3.3 Reputation Label Update

Assume that there are n_a nodes within the neighborhood. According to the procedures in subsection 4.4.3, the overhead and latency incurred by each message in reputation label update are shown in Table 4.1.

Table 4.1
Overhead and latency analysis of reputation label update

	RS Query	***RS***	***Update Request***	***Certificate***
Com. Overhead	1	$n_{rx}(n_a-1)+ n_{rx}$	n_{rx}	K
Com. Latency	0	$n_{rx}T_P+ n_{rx}T_P$	$n_{rx}\, T_P$	$T_P+K\tau_0$

Thus, the communication overhead and latency for reputation label update are:

$$C_O = n_{rx}(n_a+1)+1+K. \tag{4.20}$$

$$T_L = (3n_{rx}+1)T_P+K\tau_0. \tag{4.21}$$

Due to the presence of n_a in C_O and K in T_L, C_O and T_L are the dominating part of communication overhead and latency of JPRA. Thus, the selection of K has obvious impact on the system performance of JPRA, which will be discussed in detail next.

4.6.4 Configuration of System Parameters

In JPRA the system parameters, such as the security threshold K, the reputation update period T_C and the remaining valid time threshold t_m, need to be properly configured. Here the parameter configurations are discussed based on the regional traffic conditions and parameters, so that JPRA will work smoothly in any geographic region. We reasonably assume that each region has somewhat uniform traffic parameters such as node density and average speed, and the RSUs in this region can timely notify the vehicles of the system parameters of JPRA. In highway scenarios, the concerned region can be a segment of highway; in downtown scenarios, the concerned region can be a city area.

With previous discussions, following considerations about T_C and t_m can be derived.

Time Sufficiency: T_C must allow sufficient time for the neighboring nodes to update their reputation labels one by one. Given K, the latency incurred by one reputation label

update is T_L, as shown in (4.21). In a specific region, on average each node has $n_a=2\rho R$ 1-hop neighbors, where ρ is the average node density. Due to the high node mobility, the remaining valid time of the reputation labels of these vehicles may follow a uniform distribution between 0 and T_C. Thus, we have

$$T_C \geq n_a T_L. \tag{4.22}$$

Besides, t_m should be larger than the typical latency of a reputation label update (T_L).

Network Void Crossing: T_C should be large enough so that a node leaving a network cluster should be able to reach the next network cluster with a still valid reputation label. Specifically, in highway scenarios, we model the road as a 1-D line segment, with the nodes following the Geographic Poisson Distribution (GPD) [198]. Then within a road of length d, the probability that there are i ($i\geq 0$) nodes is

$$\Pr\{X = i\} = (\rho d)^i e^{-\rho d} / i!. \tag{4.23}$$

In (4.23), X is the random variable indicating the number of vehicles. Thus, regarding a road segment of length d, the probability that there is no vehicle is

$$\Pr\{X = 0\} = e^{-\rho d}. \tag{4.24}$$

Given the condition that there is a network void (NV) before a certain node, the expected length of a network void is

$$E[d \mid NV] = R + \int_0^{+\infty} x e^{-\rho x} dx = R + 1/\rho. \tag{4.25}$$

Suppose that a node normally leaves the current network cluster with a minimal speed difference Δv_m. Then,

$$T_C \geq E[d]/\Delta v_m = R/\Delta v_m + 1/(\rho \Delta v_m). \tag{4.26}$$

In downtown areas, the presence of network void mainly is caused by the traffic lights. Thus, we only need to consider the speed limit (v_M) and length (d_M) of the longest road segment in the concerned area. That is,

$$T_C \geq d_M/v_M. \tag{4.27}$$

Thus, given realistic traffic parameters, another lower bound of T_C can be estimated based on either (4.26) or (4.27).

Remaining Valid Time t_r: One misbehaving node may intentionally change its pseudonym right after it receives a reputation label to increase the communication

overhead of its neighbors. In this case, $t_r = T_C$. Generally, the overhead caused by the dissemination of the reputation label revocation notification (RRN) should be smaller than that of a reputation label update. Thus, in highway scenarios, the overhead of a revocation broadcast is

$$O_H = t_r \times \Delta v_m / R = T_C \times \Delta v_m / R. \tag{4.28}$$

Thus, combining (4.28) and (4.20) we have

$$O_H \le C_O \rightarrow T_C \le R[n_{rx}(n_a+1)+1+K]/\Delta v_m. \tag{4.29}$$

Similarly, for downtown areas by combining (4.10) and (4.20) we have

$$O_D \le C_O \rightarrow T_C \le R[n_{rx}(n_a+1)+1+K]/v_M. \tag{4.30}$$

Thus, one upper bound of T_C can be estimated with (4.29) or (4.30).

Reputation Management Requirement: T_C should be smaller than the reputation update period as required by the specific reputation management scheme.

On the other hand, based on regional traffic parameters and application requirements, the upper bounds and lower bounds of K can also be determined, as discussed below.

Sufficient Neighbors: In reality, we need to ensure that at any time the probability that one node has more than K neighbors is larger than a preset value p_0, as set by VANET administrators. In highway scenarios, the probability of any node has more than K neighbors is

$$\begin{aligned} p_K &= \Pr\{k \ge K+1 \mid \lambda = 2\rho R\} = \sum_{i=K+1}^{\infty} \frac{(2\rho R)^i e^{-2\rho R}}{i!} \\ &= 1 - \sum_{i=0}^{K} \frac{(2\rho R)^i e^{-2\rho R}}{i!} \end{aligned}. \tag{4.31}$$

Letting $p_K \ge p_0$, we can derive one upper bound of K in highway scenarios with (4.31).

In downtown areas, we regard one road segment as being good as long as its network density can support K+1 nodes within 2R distance. Thus, we can numerically figure out the proper value of K, so that the proportion of the good road segments is no less than p_0.

Misbehaving Nodes: K should be large enough so that the probability that there are more than K+1 misbehaving nodes among n_a nodes is smaller than a preset value p_1.

$$\Pr\{n_m \ge K+1\} = \sum_{i=K+1}^{n_a} C(n_a, i)\, p^i (1-p)^{n_a - i}. \tag{4.32}$$

In (4.32), n_m is the number of misbehaving nodes in the concerned neighborhood. Let this probability derived by (4.32) be smaller than p_1, we can get one lower bound of K.

Thus, based on regional traffic conditions the feasible ranges of the system parameters of JPRA can be determined. The configuration of these parameters will be performed by the traffic engineering staff and is out of the scope of this chapter.

4.7 Simulation Results

To showcase the application of JPRA in VANETs, here JPRA is adopted to support a simple reputation scheme in the context of privacy protection, where each node changes its pseudonyms with a period of 100 seconds. The reputation scheme is based on *beacon evaluation*, where each node verifies and evaluates the content of the beacons from its neighbors. With existing beacon verification schemes [76], [90], [143], we focus on reputation aggregation to reflect each node's beaconing behaviors. For simplicity, we design the following reputation aggregation algorithm.

Reputation segment: Suppose during the last period node *A* receives *n* beacons from node *B*. A period starts when *A* and *B* become neighbors, or when *A* updates its reputation label for the last time. Let n_b indicate the number of invalid beacons. Then, the reputation segment for node *B* is

$$rs_{AB} = \begin{cases} 1, n_b = 0 \\ -n_b / n, n_b > 0 \end{cases}. \tag{4.33}$$

Reputation aggregation: Based on the reputation segments and its current *rv* value, the reputation of node *B* can be updated. First, the average reputation segment *rs* is calculated. Then, the reputation change Δrv is calculated as

$$\Delta rv = \begin{cases} (1-rv) \times rs, rs \in (0,1] \\ rv \times rs \qquad , rs \in [-1,0] \end{cases}. \tag{4.34}$$

The reputation is updated as $rv = rv + \Delta rv$, which implements the *Update*() function in subsection 4.4.3. Equation (4.34) ensures that the reputation of any node will be changed a lot when the reputation segments is inconsistent with its current reputation, which is a common practice in the existing reputation schemes.

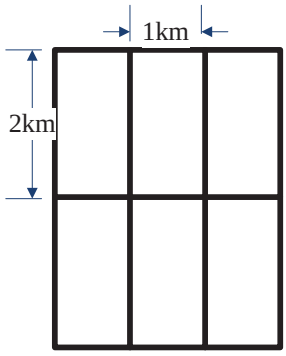

Figure 4.6 The road layout used in the simulation of JPRA

For brevity, only downtown scenarios are simulated as shown in Figure 4.6. Each road segment consists of two lanes in each direction. 250 nodes drive around with an average speed of 20m/s. Each node periodically sends out beacons. To simulate random errors, each honest node will send out invalid beacons with a probability of 0.5%. Each misbehaving nodes, by contrast, will send out invalid beacons with a higher preset probability α. The number of misbehaving node, N_B, is also configured in this simulation.

IEEE 802.11a is adopted in NS2 [169] to simulate DSRC communication, due to its similarity to DSRC. Vehicle mobility trace is generated by MOVE [170]. The simulation parameters are listed in **Table 4.2**.

For comparison, we simulate JPRA (K=1, 2, 3, 4) as well as a baseline scheme and the probabilistic reputation scheme [108]. The baseline scheme, representing reputation schemes without considering privacy protection, enables the neighbors of each node to keep its reputation segments based on its behaviors. To form a reputation for one node, all its neighbors need to be queried for reputation segments. In face of pseudonym change, the reputation segments of any node will be lost and this node can assume a new reputation value. In the probabilistic reputation scheme [108], blocking negative reputation segments is easy and reputation values are manifested in its real value.

Table 4.2
Simulation parameters of JPRA

Parameter	***Value***	***Parameter***	***Value***
# of vehicles	250	Bit-rate	6 Mbps
Road length	25 km	Beacon Period	200 ms
R	300m	Simulation Time	700 s
MAC	802.11*a*	T_P (T_0)	100 ms
T_C	100 s	t_m	1 s

4.7.1 Reputation Values

To evaluate each scheme's capability of calculating the authentic reputation values in face of misbehaving nodes, the average reputation values of honest nodes and dishonest nodes are evaluated. Here, each misbehaving node generates invalid beacons with a probability α, which changes from 0.1 to 0.5 with a step size of 0.05. Each misbehaving node may try to block 100% or 50% of the negative reputation segments, if possible. For brevity, we only show the simulation results for N_B = 20 and K=2 for JPRA.

The average reputation values of the misbehaving nodes in each scheme are shown in Figure 4.7. In the following figures, we use ***PR*** to indicate the probabilistic reputation scheme and use ***BS*** to indicate the baseline scheme. Figure 4.7 shows that, in the probabilistic reputation scheme, the reputation will always be 1.0 if each misbehaving node can block all negative reputation segments. Even if each misbehaving node can only block 50% of the negative reputation segments, its reputations will still be much higher than those estimated by JPRA.

With the baseline scheme, though the misbehaving nodes cannot block the negative reputation segments, they can surely discard their previous low reputations by changing pseudonyms. We can safely predict that the misbehaving nodes will have even higher reputations if they can change their pseudonyms with a smaller period.

By comparison, JPRA prevents any misbehaving nodes from blocking the negative reputation segments and from evading the low reputations by changing their pseudonyms. Thus, JPRA calculates the lowest reputations for the misbehaving nodes, which correctly reflect their misbehaviors.

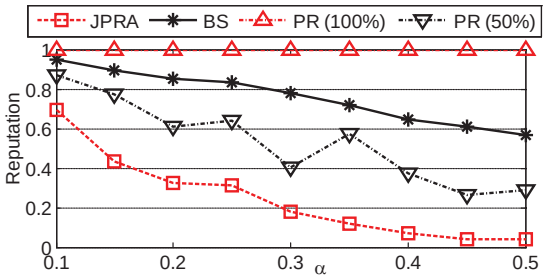

Figure 4.7 Reputation values of misbehaving nodes estimated by various schemes

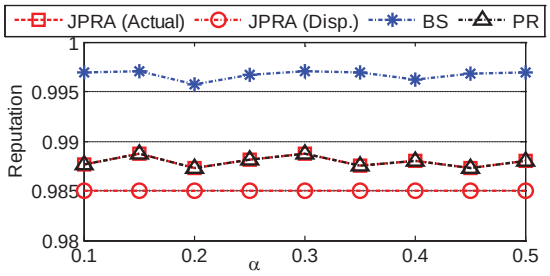

Figure 4.8 Reputation values of honest nodes estimated by various schemes

Besides, the reputations of the honest nodes in cases of JPRA, BS and PR are almost the same, as shown in Figure 4.8. However, even for the honest nodes, the reputation estimated by BS is a little bit higher than those of JPRA and PR, due to the fact that by changing its pseudonyms each node can assume a reputation of 1.0. By setting the reputation threshold r_t to 0.985, the manifested reputation of each honest node, JPRA(Actual), is the same, which is very close to its actual reputation (JPRA (Disp)).

4.7.2 Futile Pseudonym Change Ratio

For any node, its pseudonym change becomes futile if its manifested reputation is unique among its neighborhood. Here, the *futile pseudonym change ratio* is defined as the number of futile pseudonym changes over the total number of pseudonym changes. Since the baseline scheme is based on reputation query, it is not evaluated here.

In Figure 4.9, the futile pseudonym change ratio of the honest nodes and misbehaving nodes of JPRA are labeled “JPRA Good” and “JPRA Bad”, respectively. Similarly, the futile pseudonym change ratio of honest and misbehaving nodes of the probabilistic scheme are “PR Good” and “PR Bad”, respectively. As shown in Figure 4.9, the probabilistic scheme makes most pseudonym changes futile for any node, since the exact reputation value tends to be unique. By comparison, in JPRA, with conditional reputation discretization the honest nodes can well preserve its privacy through pseudonym change, while the misbehaving nodes’ pseudonym changes are mostly futile. Thus, JPRA protects the privacy of honest nodes and punishes the misbehaving nodes in both privacy and reputation schemes.

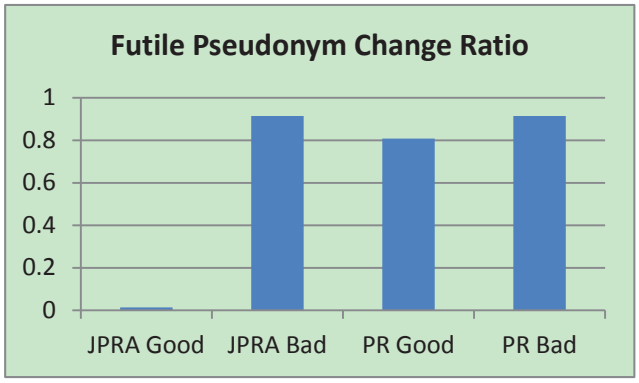

Figure 4.9 The privacy violation ratios of JPRA and PR

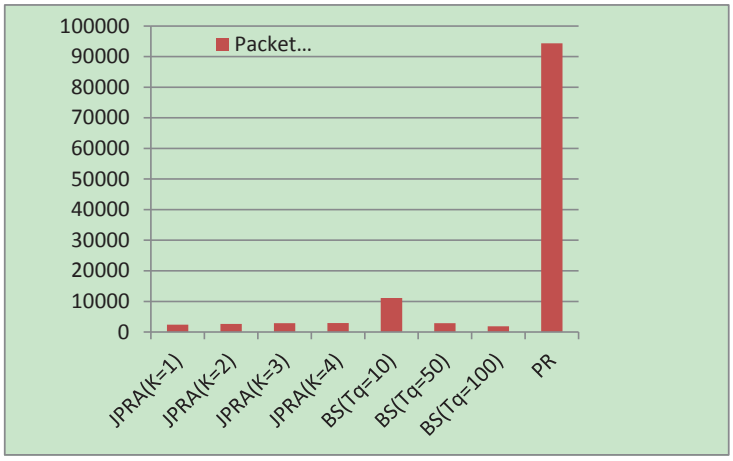

Figure 4.10 The communication overheads of JPRA, BS and PR

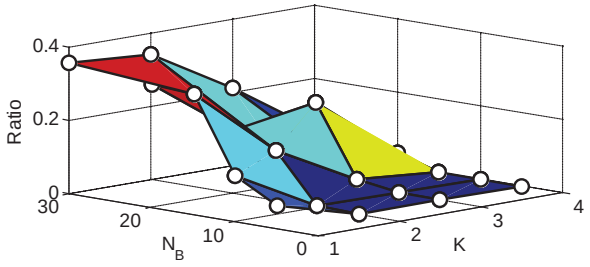

Figure 4.11 The successful collusion ratio of misbehaving nodes in JPRA

4.7.3 Overhead and Successful Collusion Ratio

To compare the communication overhead, here the total communication packets of these schemes are shown in Figure 4.10. In the probabilistic reputation scheme, each beacon will trigger a reputation segment, as discussed in [108], so its communication overhead is much higher than other schemes. In the baseline scheme, to know the current

reputations of its neighbors, each node needs to query the reputation of each of its neighbors for a period T_q. Here, we assume that T_q = 10s, 50s or 100s, respectively.

As shown in Figure 4.10, the communication overhead of JPRA with any K is comparable to the baseline scheme with T_q=50s and T_q =100s. In JPRA, with the reputation label update period (T_C) set to 100s, the actual reputation label update interval is about 50s, considering the additional reputation label updates triggered by Event 2 and Event 3. Thus, the communication overhead of JPRA is smaller than that of the baseline scheme given the same reputation update period. Additionally, the probabilistic reputation scheme has the highest communication overhead.

For different K values, the *successful collusion ratios* for any misbehaving nodes in JPRA are investigated. To allow for the most stringent scenarios, we assume that there is a successful collusion in reputation label update if there are currently (K+1) misbehaving nodes in the neighborhood. Figure 4.11 shows that the successful collusion ratio is generally smaller than 10% for $K \geq 2$ and $N_B \leq 20$. Please note that there are totally 250 nodes in the simulation, so N_B = 20 indicates that 8% nodes are misbehaving nodes, which is untypically high for a realistic VANET. On the other hand, considering that many misbehaving nodes may not collude, the actual successful collusion ratio will be much lower than those shown in Figure 4.11. Thus, we can assume that for a realistic VANET, any K value no less than 2 will be proper for JPRA.

In summary, simulation results show that JPRA can synergistically support both reputation management and privacy protection in VANETs, outperforming the existing schemes in terms of both reputation management and privacy protection. Besides, the communication overhead of JPRA is lower than the existing schemes.

4.8 Summaries

JPRA jointly supports privacy protection schemes and reputation management schemes by reconciling their conflicting requirements, so that both can be synergistically implemented in VANETs. Furthermore, JPRA enables them to enhance each other with additional support. Specifically, JPRA further encourages the common nodes to cooperate in VANETs by decreasing the privacy achieved by the misbehaving nodes. Additionally, the reputation label update for reputation management will not harm the

privacy protection schemes. Thus, considering the significance of reputation management and privacy protection, JPRA is essential to VANETs. Even better, JPRA incurs the lowest communication overhead in supporting both privacy schemes and reputation schemes, as discussed in subsection 4.6.2 and subsection 4.7.3. Thus, JPRA is a practical and novel solution for jointing supporting privacy and reputation in VANETs.

In the future, we will continue to consider the conflicting requirements of trust schemes and privacy protection, and jointly support both types of schemes in VANETs.

Chapter 5 Short-Time Certificates-Based Privacy Protection[5]

The short-time certificate schemes bring new constraints and implications to privacy protection in VANETs, especially the possible power abuse of RSUs and VANET authority. This chapter investigates such issues, based on which a short-time certificate-based privacy protection (STCP2) scheme [147] is proposed. STCP2 adopts a privacy-aware RSU deployment algorithm to optimize the deployment of RSUs with realistic cost and privacy constraints, properly handling the power abuse of RSUs and VANET authority. Furthermore, a secure and privacy-preserving pseudonym update algorithm allows each node to enhance its privacy by pseudonym changes at one RSU, against various privacy adversaries. Theoretical analysis and simulations show that STCP2 ensures proper privacy protection in VANETs with short-time certificates.

5.1 Introduction

To fully realize the application potentials of VANETs it is necessary to address the challenging security requirements of VANETs [5]. Central to any security scheme is a certificate scheme for each vehicular node to securely prove its identity with a certificate issued by the authority of VANETs. Recently, two approaches to manage certificates in VANETs, long-time and short-time certificates, are commonly followed. The long-time schemes follow the certificate management for general networks, where the certificate revocation list (CRL) is necessary to revoke the certificates of the misbehaving nodes. Thus, such schemes usually incur heavy communication overhead by CRL distribution. By contrast, short-time certificate schemes assign to each node a certificate with a short lifetime, so that each node has to update its certificate frequently. Here, CRL distribution is unnecessary, since the authority can simply refuse to update the certificate to evict a misbehaving node. Thus, free of CRL distribution, short-time certificates are appealing to VANETs.

---

[5] The material contained in this chapter was submitted to *IEEE Transactions on Vehicular Technology*. © 2012 IEEE. See Appendix C for a copy of the copyright permission.

Currently, most privacy protection schemes assume a long-time certificate management scheme, where each node is equipped with multiple certificates to form its pseudonyms and can change its pseudonyms at will. Frequent pseudonym change [113], [117]-[119], [121], [124], [127] is critical to the protection of nodes' privacy, as discussed in section 5.2. However, with short-time certificates, each node has only one pseudonym at any time. To change its pseudonym, each node needs to get access to the authority via an RSU for certificate update. Thus, privacy protection faces different assumptions and constraints with short-time certificates. Specifically, since each RSU can monitor the pseudonym changes of all passing-by nodes, the possible power abuse of RSUs and the authority needs to be considered in privacy protection. Besides, it is necessary to make the certificate update procedures at each RSU both secure and confidential, since this is the only feasible pseudonym change opportunity for any node.

To thoroughly address these issues, a Short-Time Certificates-based Privacy Protection scheme, STCP2, is proposed in this chapter. STCP2 identifies and investigates the critical privacy implications of short-time certificates. The deployment of RSUs in VANETs under the constraints of deployment cost and privacy protection is optimized with a novel privacy-aware RSU deployment algorithm. With this algorithm, the vehicular nodes will still get a minimal privacy assurance in case of the power abuse of RSUs and the authority. A secure and privacy-preserving pseudonym update algorithm enables each node to confidentially change its pseudonym with the help of the RSUs. Thus, with STCP2, privacy protection in VANETs becomes both cost-effective and feasible with short-term certificates, as shown by extensive theoretical analysis and simulations.

5.2 Related Work

To support traffic safety applications each node needs to broadcast beacons to announce its driving states such as location, speed and heading direction, with a period varying from 100ms to 500ms [10]. Thus, by monitoring beacons from one node, an adversary can obtain the exact movement trajectory of this node and breach its privacy. To protect the privacy of vehicular nodes, pseudonym change [113], [117]-[119], [121], [124], [127] is commonly adopted in VANETs to break down the movement trajectory (location history) and application accessing history of each node. A pseudonym is a

temporary communication ID which has no obvious connection to the real identity of one node, and a pseudonym usually is the combination of a certificate, an IP address and a MAC address [113]. Though several privacy protection schemes, for instance [134], [199], only consider the certificate in pseudonym changes, such schemes will not be effective without the synchronized IP and MAC address change.

Most existing privacy protection schemes [113], [117]-[119], [121], [124], [127] for VANETs assume long-time certificates, so that CRL distribution is necessary to revoke the certificates of misbehaving nodes. In VANETs, with numerous nodes and multiple pseudonyms per node, the size of CRL tends to be huge. Besides, VANETs' dynamic nature makes CRL distribution both challenging and bandwidth demanding [200]. Though several schemes [50], [54]-[56] have been proposed for efficient CRL distribution, they generally involve complicated control procedures for VANETs.

Thus, short-time certificate schemes [57]-[60] for VANETs have been proposed to avoid CRL distribution. In such schemes, the certificate for each node has a short lifetime, so that to evict a misbehaving node the authority only needs to refuse to update the short-time certificate of this node. Thus, being CRL-free, the short-time certificate schemes tend to be efficient and easy to manage. Indeed, WAVE [201] has listed short-time certificate schemes as a suitable alternative certificate management approach.

With short-time certificates each node can only change its pseudonym assisted and monitored by an RSU, which brings forth new privacy implications. So far, such constraints have not been thoroughly investigated yet, which is one major task of STCP2. Specifically, with short-time certificates the possible power abuse of the RSUs and VANET authority needs to be considered, which has not been considered in existing RSU deployment schemes. For instance, [202] considers the optimization of RSU deployment in light of driving delay time and overhead time, without considering the possible privacy risks of the deployed RSUs. Besides, though [202] considers the incremental deployment of RSUs, it is unclear whether the additional RSUs can be optimally deployed or not. [128] proposes a flow-based privacy model to estimate the privacy strength of each intersection, and optimize the placement of mix zones in a given region. However, [128] relies on precise traffic flow statistics for any road intersection and ignores the possible

privacy risks of the RSUs. More importantly, [128] fails to consider RSU deployment in a progressive manner, which will be necessary in realistic VANET deployment.

Besides, the certificate update procedure at each RSU should be both secure and confidential, to enhance the location privacy of the vehicular nodes. However, existing short-time certificate schemes [57]-[60] are mainly focused on the update of cryptographic materials, without considering the privacy adversary. In [129], a scheme to set up mix zone [131] for VANETs is proposed to enable vehicular nodes to change their pseudonyms without being monitored by the external adversaries. However, the IP and MAC addresses of each node are not considered in pseudonym change, and the more powerful internal privacy adversaries (as discussed in section 5.3.3) are not properly handled. Besides, [129] ignores the impact of encrypted beacons on traffic safety applications. By comparison, STCP2 will consider both internal and external adversaries to location privacy.

5.3 Background and System Model

In this section, the network model and underlying assumptions of STCP2 are presented, based on which the problem statement of STCP2 will be given.

5.3.1 Network Model and Assumptions

VANETs consist of an ad hoc domain and an infrastructure domain [4], [36], [37]. The ad hoc domain is comprised of smart vehicles equipped with DSRC [8] transceivers and GPS receivers. For traffic safety, each node will broadcast beacons every 100ms to 500ms [10]. To securely participate in VANET communications, each node needs a valid short-time certificate issued by the Trust Authority (TA). Each node has a standard tamper-proof device (TPD) [11] to protect the cryptographic materials associated with its short-time certificate, especially its private key. With TPD, it is difficult for any unauthorized entity to access the private key of any node, and it is difficult for any vehicular node to intentionally reveal its own private key.

The infrastructure domain consists of RSUs and the management entities, for instance Trust Authority (***TA***). TA is in charge of all management functions and security functions of VANETs, including identity management of RSUs and vehicular nodes. Equipped with DSRC transceivers, RSUs serve as vehicular nodes' access points to TA. RSUs

usually are deployed at road intersections, probably working together with the traditional traffic lights. The communications between RSUs and TA are assumed to be error-free and instantaneous. It is assumed here that TA and RSUs are difficult to compromise.

5.3.2 Privacy Implications and Problem Statement

With short-time certificates, each node uses a short-time certificate issued by TA and its IP/MAC addresses as its pseudonym in communications. Each node needs to update its certificate whenever it runs into the communication range of an RSU, as shown in Figure 5.1. To be both secure and efficient, certificate update relies on only 1-hop communications. Thus, with short-time certificates each node needs to change its pseudonym assisted and monitored by an RSU. Thus, critical assumptions of privacy protection with short-time certificates can be identified and justified below.

- The real identity of each node should be kept secret to any entities except for TA, as commonly assumed in the existing privacy protection schemes.
- The pseudonym changes of any node should not be traced by any entities except for RSU and TA. Due to the nature of 1-hop communications, it is evitable that an RSU can monitor the pseudonym change of any passing-by vehicles.
- *Minimal Privacy Assurance*: The exact movement trajectory of any node should not be figured out by any entity, including TA and RSUs. This represents the lowest privacy any node can achieve if, in any case, both TA and RSUs are compromised. Even if TA and RSUs are not compromised, the concerns about power abuses of TA and RSU may deter the privacy-sensitive users from participating in VANETs. Thus, based on common senses and the current research on privacy concerns in VANETs [203], such a minimal privacy assurance is desirable for VANETs.

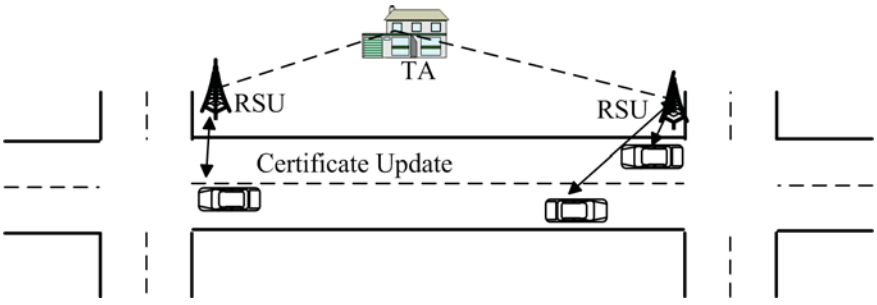

Figure 5.1 The network model of VANETs with short-time certificates

- *Regional Considerations*: We consider VANETs in a specific geographic region. In reality most privacy protection decisions are relevant to specific locations, such as a downtown area, one resident neighborhood and a hospital neighborhood [204]. Besides, in the initial stage of VANET deployment, RSUs may be deployed in certain regions by the local transportation authorities. Thus, it is more likely that each local area will have its own VANET deployment plan and policies. As discussed later, the algorithms proposed in STCP2 can be easily extended to a huge VANET, for instance, a network formed by all vehicles in the USA.

Based on the realistic assumptions presented above, STCP2 addresses two critical problems. First, RSU deployment in VANETs should be optimized in lights of privacy protection, cost and application support. Secondly, the pseudonym update procedure of each node needs to be both secure and privacy-preserving.

5.3.3 Adversary Model

Similar to [113], [117]-[119], [121], [124], [127], three powerful adversaries are considered in STCP2, including the Global Passive Adversary (GPA), the Local Passive Adversary (LPA) and the Local Active Adversary (LAA). Among them, the GPA can overhear all communications within the whole VANETs; the LPA can only overhear the communications within certain local regions. The LAA, besides overhearing the communications within certain local regions, can also actively communicate with other nodes and RSUs. Thus, the LAA is able to get the cryptographic materials present in VANETs, as the normal vehicular nodes do. Realistically, the GPA and the LPA are *external observers* which intend to gain economic interests or to harm the common VANET nodes by breaching the location privacy. The LAA is the compromised nodes (*internal observers*) of VANETs.

TA and RSUs generally are constrained by privacy related policies and legislations, so that they generally will not breach the location privacy of vehicular nodes. However, to be safe, in STCP2 the extreme cases of power abuse and compromise of TA and RSUs are also considered, as discussed in subsection 5.3.2.

5.4 Privacy-Aware RSU Deployment

RSUs have significant impacts on the security, privacy, application, as well as the cost of VANETs. Specifically, many security schemes, such as reputation management and certificate update, benefit from the presence of RSUs as trust anchors. RSUs are also desirable to various traffic safety, traffic management and commercial applications, serving as access points to the infrastructure entities. Thus, to better support security and applications, RSUs should be deployed as densely as possible in VANETs. On the other hand, one RSU, once compromised or in case of power abuse, may also serve as a sampling point for one node's movement trajectory. Besides, each RSU incurs a certain deployment and maintenance cost, which will limit the number of RSUs to be deployed.

Here, RSU deployment will be investigated to achieve the desirable tradeoff among privacy requirements, safety requirements and cost constraints.

5.4.1 Minimal Privacy Condition

As discussed in subsection 5.3.2, it is necessary to provide the minimal privacy assurance to the vehicular nodes in VANETs. Thus, in any region $\mathcal{R}$=<V, E> the RSUs need to satisfy the minimal privacy assurance. Here, V is the vertex set, containing all the intersections and points of interests in this region. E contains the road segments. A sufficient and necessary condition of the minimal privacy assurance is stated as follows.

Weak Minimal Privacy Condition **(WMPC)**: Between any adjacent vertex of one RSU and any adjacent vertex of another RSU, there exist at least two RSU-free paths.

Proof: Suppose the deployed RSUs in VANETs satisfy WMPC. In a typical road topology as shown in Figure 5.2, consider two RSUs (R_1 and R_2). Each RSU can figure out the driving direction of any passing-by node up to its adjacent vertices. When a node moves from R_1 to R_2, R_1 and R_2 cannot figure out the exact movement trajectory of this node. In terms of topology, this node could have followed the path R_1-A-R_2, or R_1-A-B-C-D-E-F-G-H-A-R_2. Thus, WMPC is a sufficient condition of the minimal privacy assurance. On the other hand, suppose that between an adjacent vertex of R_1, say A, and an adjacent vertex of R_2, say B, there is only one or no RSU-free path. Then, from above discussions, the path R_2-B-A-R_1 can be completely monitored by $R_1$and R_2. Thus, this path violates the minimal privacy assurance. Thus, WMPC is also a necessary condition.

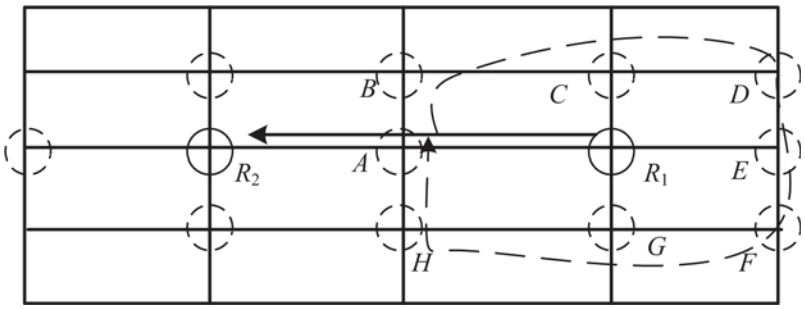

Figure 5.2 The alternative travel paths between two RSUs

WMPC is *weak* in the sense that only the topology information is considered in the above discussions. If R_1 and R_2 have sufficient information about the average vehicle speed and the traffic light status of the nearby road intersections, they probably could differentiate a node following the path R_1-*A*-R_2 from a node following the path R_1-*A*-*B*-*C*-*D*-*E*-*F*-*G*-*H*-*A*-R_2. However, WMPC is still meaningful, considering the uncertainties in the vehicles' movement in reality. For instance, one vehicle may stop beside a shop or an office building for a period, instead of moving continuously. Besides, we can extend WMPC to the Strong Minimal Privacy Condition (SMPC).

***Strong Minimal Privacy Condition* (SMPC)**: The RSUs satisfy WMPC. Besides, for any RSU-free path ($Path_1$), there must exist at least another RSU-free path ($Path_2$) such that $|TravelTime(Path_1) - TravelTime(Path_2)| \leq \tau$.

Here, *TravelTime*() estimates the average travel time of a route. τ is a parameter set by the VANET administrator, with which these two RSU-free paths cannot be differentiated based on the travel time of one vehicle. Similarly, it can be proven that that SMPC is both sufficient and necessary for the minimal privacy assurance. Without realistic traffic statistics, it is difficult to adopt SMPC in the deployment of RSUs. Thus, next we use WMPC for privacy-aware RSU deployment.

Indeed, WMPC provides an upper bound (N_M) on the number of RSUs in a given region $\mathcal{R}$=<*V*, *E*>. Let $V_I \subset V$ be the set of vertices selected for RSU deployment. Then N_M can be obtained by solving the following optimization problem.

$$\begin{aligned} &\max \quad |V_I| \\ &st. |Path_{/V_I}(a_i, a_j)| \geq 2, \forall v_i, v_j \in V_I, a_i \in Nei(v_i), a_j \in Nei(v_j). \\ &\quad V_I \subset V \end{aligned} \tag{5.1}$$

In (5.1), $Nei(v_i)$ is the set of adjacent vertices of node v_i. $Path_{/V_I}(a_i, a_j)$ is the set of paths between vertex a_i and a_j without any vertices in V_I. If $\mathcal{R}$ is a perfect grid with $N \times N$ vertices as shown in Figure 5.2, the range of N_M can be estimated as follows

$$(N^2 - 4N)/4 \le N_M \le N^2/4. \tag{5.2}$$

Formula (5.2) can be derived by counting the RSUs in any two consequential rows or columns in this perfect grid. In these two rows, one row must be RSU-free, and the other row can have at most 1 RSU for every two consequential vertices. Thus, considering the edges in this perfect grid, (5.2) follows.

A region of an arbitrary shape can be divided into smaller squares, each of which can be approximated with a perfect grid. For each square, (5.2) can be used to estimate its maximal number of RSUs. Eventually, the N_M for the whole region can be estimated. To provide minimal privacy assurance, WMPC should be satisfied in RSU deployment, which has not been considered in [128], [202].

5.4.2 Progressive RSU Deployment Algorithm

In reality, a cost budget may mandate that only N_B RSUs can be deployed in the concerned region $\mathcal{R}$. These N_B RSUs need to be deployed to maximize the support to security and applications, while still meeting WMPC. Besides, in the future additional RSUs should be deployed in a consistent and progressive way. Specifically, given that N_B RSUs have been optimally deployed, the deployment of additional n RSUs can result in the optimal deployment of (N_B+n) RSUs. To this end, a progressive RSU deployment algorithm (***PRDA***) is proposed to minimize the ***longest RSU-free shortest path*** (L_R) in $\mathcal{R}$. Here, L_R is the length of the longest pair-wise shortest paths in $\mathcal{R}$ which have no RSU. Obviously, the smaller L_R is, the smaller will be the travel time for any vehicle at any position in $\mathcal{R}$ to reach the next RSU. In this sense, by minimizing L_R, PRDA can maximize the support to security and applications. Thus, PRDA needs to solve the following optimization problem

$$\begin{aligned} &\min L_R = |P_R| \\ &st. |P_R| \ge |P_X|, \forall P_X \in SPath/V_I \\ &\quad V_I \subset V \,\&\, |V_I| \le N_B \,\&\, WMPC \end{aligned} \quad . \tag{5.3}$$

In (5.3), P_R is the longest shortest path in $\mathcal{R}$, and $SPath/V_I$ is the set of all-pair shortest paths in $\mathcal{R}$ excluding these paths containing a vertex in V_I. To solve problem (5.3), PRDA is designed as shown in Figure 5.3.

In PRDA, WMPC is checked for any candidate vertex for RSU deployment, so the resulted V_I will surely meet this condition. Besides, in selecting any vertex, L_R is minimized, so the resulted V_I will be optimal in minimizing L_R. Specifically, two salient properties hold for PRDA. PRDA is ***progressive*** in its nature, so it is especially suitable for the realistic RSU deployment. In the initial stage only a few RSUs can be deployed and more will be further deployed when the budget permits in the future. Besides, the ***optimality*** of PRDA in minimizing L_R is obvious from Figure 5.3.

Thus, PRDA is a progressive and optimal method of deploying RSUs with privacy considerations. By making sure that most vehicles traveling longer than L_R within this region will run into at least one RSU, the safety experience of each vehicle is ensured. Besides, TA is able to estimate the lifetime of the short-time certificates to ensure that any normally travelling node will be able to run into another RSU before its certificate expires. In the future, PRDA can incorporate the speed limit and average traffic volume of each road segment to make the RSU deployment more comprehensive. We leave this extension work to the traffic engineers with sufficient domain knowledge in assessing realistic traffic statistics.

Inputs: $\mathcal{R}$, V, E, N_B
Outputs: V_I, max(*Path*)
Initialization: $V_I=\varnothing$, $Path=\varnothing$
Algorithm:
    P=Floyd($\mathcal{R}$, V, E); //all-pair shortest paths
    Path=QuickSort(P); //quick sort;
    for i=1, 2, …, N_B
        p_{m1}=max(*Path*); //current longest path
        p_{m2}= next_max (*Path*); //second longest path
        while(($v=p_{m1}\cap p_{m2}$)== 0 || $V_I\cup\{v\}$ does not meet ***WMPC***)
            p_{m2} = next_max(*Path*);
        end-of-while
        $v = p_{m1} \cap p_{m2}$;
        $V_I=V_I\cup\{v\}$;
        Path = *Path*/<v>; //remove all paths containing v
    End-of-for
    Return V_I and max(*Path*);

Figure 5.3 The detailed algorithm of PRDA

5.4.3 Analysis and Simulation of PRDA

5.4.3.1 Theoretical Analysis

First, the computation complexity of PRDA is reasonable. For a region $\mathcal{R}$ with N vertices, there will be $N(N-1)/2 \approx N^2/2$ pair-wise shortest paths. Thus, the quick sort algorithm [205] adopted in Figure 5.3 will incur a computation complexity of $O(N^2 \lg N)$. Additionally, Floyd's all-pair shortest path algorithm [206] in Figure 5.3 has computation complexity $O(N^3)$. Thus, PRDA has an overall computation complexity of $O(N^3)$, which allows its application to large regions with thousands of vertices.

Secondly, we would like to show the necessity of checking WMPC in PRDA by estimating the road segments which are completely monitored by randomly deployed RSUs. Here, for brevity we model a region $\mathcal{R}$ with an $n \times n$ perfect grid, where all road segments have the same length d. Thus, the total road segment length (L_T) in $\mathcal{R}$ is $2n(n-1)d$. We model the RSU deployment in $\mathcal{R}$ without considering WMPC as randomly deploying the n_b RSUs. For ease of estimation, we only consider the road segments which are adjacent to two RSUs at the same time.

Suppose one vertex v has one RSU. Then, v has 4 adjacent edges. Let p_0 indicate the probability that one adjacent vertex of v will be selected in RSU deployment. Then,

$$p_0 = (n_b - 1) / (N^2 - 1). \tag{5.4}$$

Equation (5.4) holds, since there are still (N^2-1) vacant vertices and (n_b-1) RSUs left. Thus, the length of the covered edges which are adjacent to v, l_1, can be approximated as

$$l_1 = {p_0}^4 \times 4d + \binom{3}{4} {p_0}^3 \times 3d + \binom{2}{4} {p_0}^2 \times 2d + \binom{1}{4} {p_0}^1 \times d. \tag{5.5}$$

Thus, the total length of covered edges can be roughly estimated as

$$l_T = n_b l_1 / 2. \tag{5.6}$$

The ratio of covered edges is

$$r_T = l_T / L_T. \tag{5.7}$$

From (5.5), (5.6) and (5.7), r_T is always non-zero, which means that certain road segments will violate the WMPC condition. Thus, it is necessary to consider WMPC in RSU deployment, to prevent any road segment from being completely monitored.

5.4.3.2 Simulation of RSU Deployment

To show the effectiveness of PRDA, we simulate RSU deployment in downtown Marquette, MI, which has 519 vertices. In this simulation, we change the number of available RSUs (N_B) from 1 RSU to 100 RSUs.

For comparison, we also randomly select N_B vertices for RSU deployment, and evaluate its L_R. For each given N_B, the L_R values of the random RSU deployment and PRDA are shown in Figure 5.4. Given one N_B, PRDA can achieve much lower L_R than the random RSU deployment. Besides, with any given N_B, L_R of PRDA is significantly reduced from the original value (about 16000 meters) without any RSU.

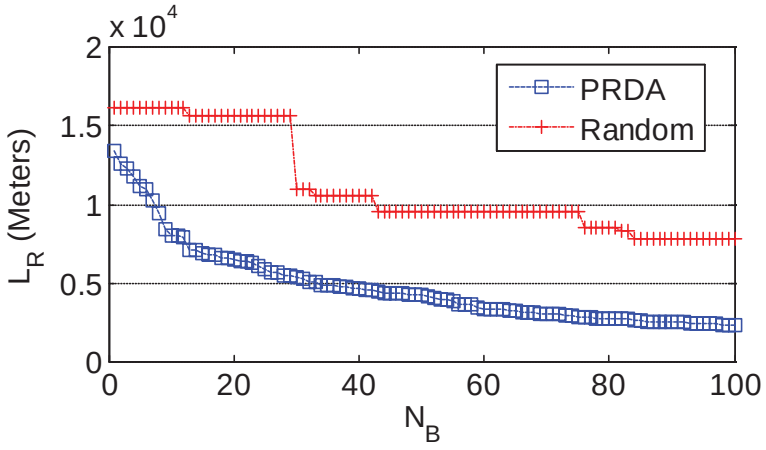

Figure 5.4 The L_R statistics of PRDA and random RSU deployment

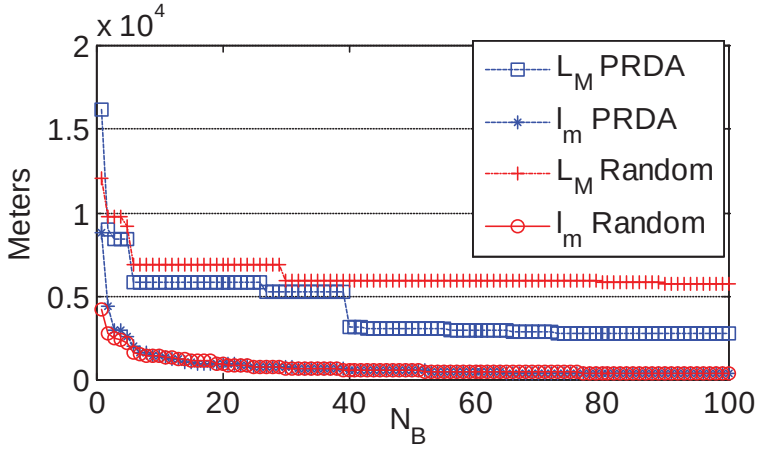

Figure 5.5 The l_m and L_M statistics of PRDA and random RSU deployment

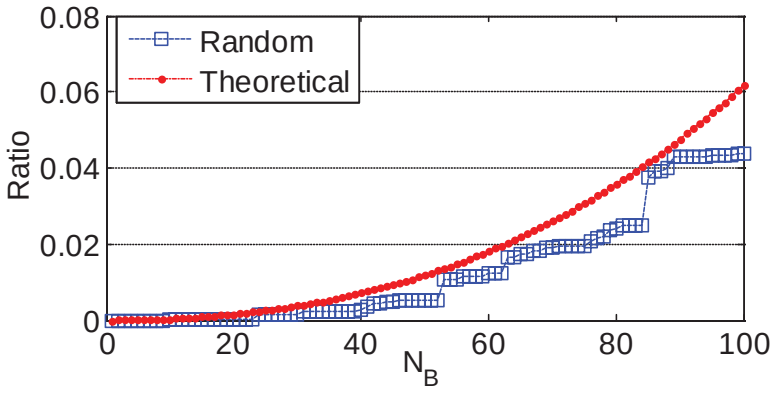

Figure 5.6 The ratio of covered road segments of random RSU deployment

Besides, with N_B RSUs deployed, the distance (l_i) of each vertex to its nearest RSU is investigated. Specifically, L_M is the maximal l_i of all vertices, and l_m is the average l_i of all vertices. Figure 5.5 shows the L_M and l_m of both PRDA and random RSU deployment. It shows that PRDA will result in smaller L_M than random RSU deployment, so that with PRDA each vehicular node can go to the nearest RSU sooner.

The ratio of monitored road segments, in case of the random RSU deployment, is shown in Figure 5.6. In Figure 5.6, the theoretical ratio is estimated based on (5.7). The curve labeled with Random is the ratio of covered road segments with RSUs randomly deployed. Figure 5.6 shows that by randomly deploying RSUs, some road segments will surely be completely monitored by the RSUs. Vehicular nodes traveling on such road segments will not meet the minimal privacy assurance.

In summary, PRDA optimizes the RSU deployment in VANETs with realistic budget constraints, ensuring the minimal privacy assurance to nodes and maximizing the support to security and applications. Being progressive, PRDA is especially appealing to the future massive deployment of VANETs. With RSUs deployed, it is necessary to investigate the pseudonym update procedures at each RSU, as discussed next.

5.5 Secure and Privacy-Preserving Pseudonym Update

As previously discussed, with short-time certificates each node can only update its pseudonym with the help of an RSU. Thus, it is critical to make the pseudonym change of each node secure and privacy-preserving against both external and internal observers. To this end, here a secure and privacy-preserving pseudonym update algorithm is proposed

with three procedures: *location cloaking*, *synchronized pseudonym update* and *random mobility trace auditing*. Among them, location cloaking conceals the mobility trace of vehicular nodes nearby an RSU from the external observers, namely the GPA and the LPA. Synchronized pseudonym update enables each node to change its pseudonym with the aid of an RSU and become a totally new node to any external observer. Besides, random mobility trace auditing can detect LAAs in STCP2. This way, the privacy of vehicular nodes can be properly protected against GPA, LAA and LPA.

For clarity, the notations commonly used in the following subsections will be listed here. PR_X and PU_X indicate the private key and the public key of node X, respectively. $PU_X\{Msg\}$ is the message Msg encrypted with PU_X. $\{Msg\}PR_X$ is the digital signature of Msg generated with PR_X. $H(Msg)$ is the hash value of Msg generated by a standard hash function, for instance SHA-2 [168]. $\Rightarrow$ indicates broadcast and $\rightarrow$ indicates uni-cast. * indicates multiple entities.

5.5.1 Location Cloaking

To conceal the mobility trace of each node nearby one RSU, the RSU configures a location Cloaking Region (CR) with a length D (D>0) in each direction, as shown in Figure 5.7. In CR each node encrypts its beacons with a shared secret key SK_i. To avoid negative impacts on traffic safety, the RSU also configures a Buffering Region (BR) with length R outside CR, as shown in Figure 5.7. R is the communication range of vehicular nodes, and each node in BR will send out plaintext beacons while decrypting the received encrypted beacons with SK_i. Thus, properly configuring D as discussed in subsection 5.5.4, the movement trajectories of nodes in CR will be concealed from GPA and LPA.

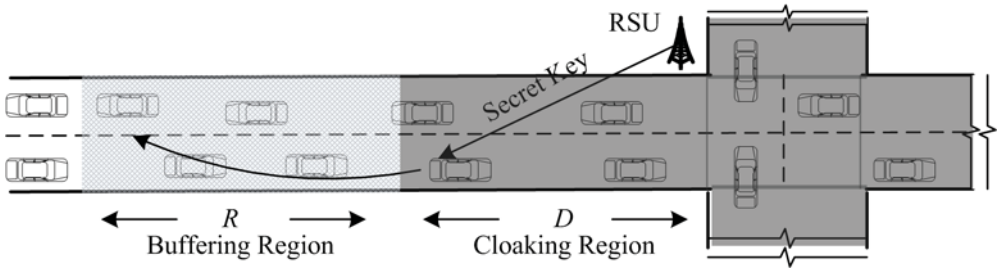

Figure 5.7 One exemplary set-up of location cloaking around an RSU

5.5.1.1 BR and CR Management

The management of BR and CR can be illustrated by one node (*A*) running across this RSU, which will first enter BR, then enter CR and eventually leave CR.

Entering BR: Upon entering BR, *A* will overhear encrypted beacons from the nodes in CR, and it will broadcast a *SK_REQ* message to its neighbors to query the current SK_i used in CR. One of its neighbors in BR, say *B*, will send SK_i to *A* in *SK_RSP*, as follows.

$A \Rightarrow *$: $SK\_REQ = \{Data=\{Type=Key\_REQ, TSP_A\}, \{Hash(Data)\}PR_A\}$.

$B \rightarrow A$: $SK\_RSP = \{Data=\{Type=Key\_RSP, PU_A\{SK\_Package\}, TSP_B\}, \{Hash(Data)\}PR_B\}$.

Here, TSP_A and TSP_B are the timestamps of node *A* and *B*, respectively. With certificates in beacons, in both *SK_REQ* and *SK_RSP* the senders' certificates are not included. *SK_Package* contains the current SK_i, *D* as well as their activation time. In *SK_RSP*, the *SK_Package* is encrypted with PU_A, so it is only accessible to *A*.

In this process, the nodes in BR may follow a contention based approach, e.g., RPB-MD [166] or LEAPER [142], to ensure reliable and trustworthy transmission of *SK_RSP*.

Entering CR: Based on *D* and the position of the RSU, *A* can figure out the boundary of CR. Upon entering CR, *A* will encrypt its beacons as follows.

$A \Rightarrow *$: $Encrypted\_Beacon = SK_i\{Plaintext\_Beacon\}$.

Here, *Plaintext_Beacon* is a standard beacon containing the sender's driving states [10]. Thus, only the vehicular nodes in CR and BR, as well as the RSU, can get access to the beacons of *A*, so *A*'s movement trajectory in CR is concealed from any external observers.

Leaving CR: When *A* leaves CR, it will broadcast plaintext beacons again. However, as long as it overhears encrypted beacons, it will still use SK_i to decrypt them.

With each node following the above procedures, BR and CR around the RSU can be automatically maintained. In CR, if *A* changes its pseudonym, the external adversaries can only rely on the time points of *A* entering CR and existing CR to connect its pseudonyms. Thus, location cloaking serves as the random silent period for pseudonym changes, which is widely adopted in privacy protection [113], [117]-[119], [121], [124], [127]. Unlike random silent period, location cloaking does not stop any node from beaconing, so it imposes no negative impact on traffic safety applications.

5.5.1.2 Update of the Secret Key

It is necessary for the RSU to keep SK_i both fresh and secure, so that the SK_i obtained by any passing-by LAA will not be useful for long. To this end, the RSU may choose to update the secret key SK_i with a new key SK_{i+1} at a randomly selected time point by broadcasting a *SK_Update* message.

RSU⇒*: *SK_Update* = {*Data*={*Type* = *Key_Update*, TSP_{RSU}, SK_T{*SK_Package_New*}, {PU_X, PU_X {SK_T}} … }, {*Hash*(*Data*)}PR_{RSU}}.

Here, *SK_Package_New* contains the new SK_{i+1}, *D* and their activation time. SK_T is a temporary secret key to encrypt *SK_Package_New*. The RSU will, for each of its 1-hop neighbor *X*, encrypt SK_T with the public key of *X* (PU_X). Thus, only the nodes regarded by RSU as its 1-hop neighbors can access *SK_Update* sent by the RSU. For instance, in Figure 5.8, the RSU will encrypt SK_T with PU_A and PU_B.

Upon receiving a *SK_Update* message from the RSU or another node, each node within BR or CR will similarly construct a *SK_Update* message for its neighbors in BR or CR which are farther away from the RSU. For instance, in Figure 5.8, the *SK_Update* message sent out by node *B* will be encrypted in such a way that only node *C* and node *E* can access it. This way, the nodes out of the communication range of the RSU can also receive multiple *SK_Update* messages from different nodes, which can be verified against each other to ensure the authenticity of *SK_Package_New*. Within a limited latency as discussed in subsection 5.5.4, all nodes within BR and CR will receive *SK_Package_New*. At the defined activation time, SK_{i+1} and the new *D* will take effect.

In the above procedures, for clarity we assume that all nodes will be honest and cooperative in sending out the *SK_Update* message. Actually, many existing schemes, e.g., LEAPER [142], can be adopted to detect the dishonest nodes tampering with *SK_Update*, and reputation schemes [93]-[95] can be adopted to punish such nodes.

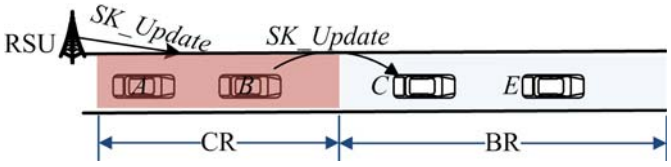

Figure 5.8 One exemplary secret key update procedure

Thus, by changing the secret key from time to time, the RSU can effectively reduce the potential harm of the LAAs. Actually, one LAA needs to go back to this RSU frequently to get the current SK_i. As discussed in subsection 5.5.3, this adds much difficulty to any LAA in continuously monitoring the nodes nearby one RSU.

5.5.2 Synchronized Pseudonym Change

To confuse the external observers, the pseudonym change of any node should be confidential. To this end, the RSU will help the nodes update the short-time certificate and change IP/MAC addresses in their pseudonyms. For brevity, here the technical details of short-time certificate schemes are ignored, and we focus on the secure message exchanges to support any given short-time certificate scheme, for example ECPP [207].

When a node *A* enters the cloaking region (CR), it will request a certificate update from the RSU as follows.

RSU←*A*: $CER\_REQ=\{\{Data=\{Type, IP\_OPT, TSP_A\}, \{Hash(Data)\}PR_A\}\}$.

RSU→*A*: $CER\_RSP = \{Data=\{Type, PU_A\{New\_Cert\}, TSP_{RSU}\}, \{Hash(Data)\}PR_{RSU}\}$.

Here, *IP_OPT* indicates whether *A* is willing to change its IP/MAC address or not. *New_Cert* contains the necessary parameters for short-time certificate update. With *CER_RSP* formatted as above, *New_Cert* is only accessible to *A*. Upon receiving *CER_RSP*, *A* will store the new private/public key pair and new short-time certificate, and use them in its communications after the following IP/MAC exchange.

Let S_W indicate the set of nodes willing to exchange their IP/MAC addresses. The RSU will select the nearby nodes in S_W, and randomly shuffle their IP/MAC addresses. Two nodes are regarded as nearby if they may be mistaken as each other after the pseudonym change, as discussed in subsection 5.5.4. Then, the RSU will broadcast an *IP_SW* message as follows.

RSU⇒*: $IP\_SW = \{Data=SK_i\{Type, TSP_{RSU}, \{A, IP\_MAC_A,\} \{B, IP\_MAC_B\}, \ldots, \{Dummy\ Assignment\}\}, \{Hash(Data)\}PR_{RSU}\}$.

Here, a valid IP address and MAC address will be assigned to any node in S_W. For each node unwilling to change its IP/MAC addresses, the RSU will put a dummy assignment in the *IP_SW* message. After receiving *IP_SW*, the nodes in S_W will assume the new

IP/MAC addresses. Besides, all nodes will start to use their new short-time certificate. To improve the effectiveness of IP/MAC exchange, the following complementary procedures are also proposed.

- Each node, if it keeps its IP/MAC intact, will add a random latency *t* to its next communication activity after receiving *IP_SW*. This *t* is obtained based on the statistics of latency caused by resetting IP/MAC addresses [113]. Thus, by monitoring the communication timing of each node, the external adversaries cannot figure out whether any node has changed its IP/MAC addresses or not.
- Each node will keep record of *IP_SW* messages for future dispute resolution. If any node arbitrarily usurps the IP/MAC of another node, such disputes can be resolved based on the *IP_SW* traces of the involved nodes.

Thus, the IP/MAC exchange maximizes the anonymity set of each node (*A*) while still allowing for each node's application considerations. Here the anonymity set of *A* consists of the nodes which seems to the adversaries likely to be node *A* with a new pseudonym. Due to the presence of the dummy assignments, an external adversary cannot differentiate the nodes changing IP/MAC addresses from those keeping their IP/MAC addresses. To an external adversary, each node entering CR becomes a totally different node upon exiting CR, and the adversary can only rely on the timing information to connect the pseudonyms of one same node, as discussed in subsection 5.5.4.

5.5.3 Random Mobility Trace Auditing

It is necessary to detect and evict the LAAs from VANETs, since each LAA imposes great harms to the privacy of vehicles. Specifically, entering BR or CR, one LAA can obtain the up-to-date secret key SK_i issued by the RSU, and monitor the pseudonym changes of its neighbors. Thus, one single LAA can make the CR futile. Furthermore, one LAA may collude with the GPA in decrypting all communications nearby one RSU. With the help of sufficient LAAs, the GPA could decrypt the beacons sent by the nodes in all CRs within VANETs.

Thus, here we identify the most cost-effective and harmful attack strategies of LAA and GPA. Depending on the number of LAAs required to obtain the up-to-date secret keys from all RSUs in VANETs, the feasible attack strategies are shown below.

- ***Fixing one LAA to one RSU***: Each LAA may continuously monitor the communications of one RSU by remaining static or circling around this RSU.
- ***Continuous Usage of LAAs***: The GPA may organize a number of LAAs to continuously run from one RSU to another. At any moment, it will be ensured that at least one LAA is within the communication range of one RSU.
- ***Advanced Usage of LAAs***: To further blend the mobility pattern of LAAs with that of the normal nodes, the LAAs will only be active in VANETs for a given duration T_0 within a period T.

To detect the LAAs adopting the above strategies, here a *random mobility trace auditing* algorithm is proposed. Specifically, the RSUs in VANETs can collectively obtain the mobility trace of each node, including the time points, positions and directions of this node running into and leaving each RSU. Each day, a period T will be randomly selected from 24 hours, in which all the node mobility traces will be analyzed. An alarm will be raised if one of the following conditions is met: 1) one node stays unreasonably long in one intersection or repeatedly returns to one RSU; 2) one node traverses all RSUs or a subset of RSUs repeatedly with continuous movement; 3) one node traverses a subset of RSUs over a period T_0. Obviously, these three alarms correspond to the above attacking strategies.

If one alarm is raised, the suspicious node will be marked and its future mobility traces will be further monitored and analyzed. If after several periods (T) one suspicious node still behaves in the similar way, this issue will be reported to the TA for further investigations on the background of this node. Once one node is confirmed as a LAA, it will be evicted from VANETs, and its owner may be further punished. In the future, concrete parameters, such as T_0, T and the alarm trigger, can be selected based on the traffic statistics of the concerned region, which is out of the scope of this chapter. Here, we will evaluate the effect of this algorithm in a theoretical setting.

In a region $\mathcal{R}$, suppose that there are N_R RSUs. Also suppose that the minimal spanning tree *Tree* of all RSUs in $\mathcal{R}$ is as shown in Figure 5.9. Then, one adversary adopting the first strategy as discussed above will only need $N_{m1} = N_R$ LAAs to continuously monitor all RSUs in $\mathcal{R}$.

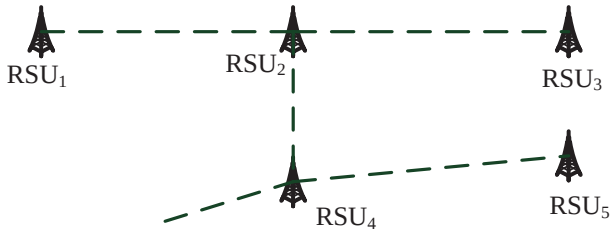

Figure 5.9 The minimal spanning tree of RSUs in VANETs

If the adversary adopts the second strategy, the minimal number of LAAs (N_{m2}) required to continuously monitor all RSUs can be estimated. Since to get the shortest traversal route of all RSUs is a NP-hard travel salesmen problem, here we use the length (*Length*) of the minimal spanning tree (*Tree*) to approximate the shortest traversal route. Then, $N_{m2} \geq 2Length/R$, even when all LAAs can be uniformly spaced in *Tree* and moving from one RSU to another without any overlapping. *Length* is on the order of N_R, and as long as the average edge is *Tree* is longer than R, N_{m2} is much larger than N_R.

If the adversary adopts the third strategy, the minimal number of LAAs (N_{m3}) required to monitor all RSUs will be further increased, as

$$N_{m3} \geq N_{m2} \times T/T_0. \tag{5.8}$$

Formula (5.8) holds, since to avoid being detected each LAA can only continuously run no longer than T_0 out of T.

Thus, with this algorithm, the negative impacts of LAAs can be significantly reduced. To continuously monitor all RSUs, at least N_{m3}, instead of N_{m1}, LAAs are required. On the other hand, if only k LAAs are available, the number of monitored RSUs will be reduced from k RSUs to kN_R/N_{m3} RSUs. To further increase N_{m3}, TA only needs to increase the ratio of T/T_0, at cost of higher computation complexity. However, each LAA is a compromised node, which incurs much higher cost to the adversary. Thus, this algorithm can make deploying LAAs in VANETs practically infeasible for any adversary.

5.5.4 Performance Analysis

We theoretically analyze the performance of the privacy-preserving pseudonym update procedure, including the communication overhead and the expected privacy of each node.

Communication Overhead: Here, for simplicity, we assume that the RSU will update its *SK* with an average period T_{SK}. Let P_{SK_REQ}, P_{SK_RSP}, P_{SK_UP} and P_{IP_SW} indicate the

packet size of *SK_REQ*, *SK_RSP*, *SK_Update* and *IP_SW* messages, respectively. Then, within T_{SK}, the overall communication overhead consists of three parts: *SK* notification, *SK* update and IP/MAC swap. The certificate update messages will be present even without STCP2, so they are not counted as the communication overhead here.

For clarity, here we consider a typical 4-way road intersection. Let λ_1, λ_2, λ_3, λ_4 indicate the average node arrival rate of each entry point around the RSU. Then, within T_{SK}, the average new nodes are $T_{SK}(\lambda_1+\lambda_2+\lambda_3+\lambda_4)$, each of which requires notification of the current *SK*. Thus,

$$C_{O1} = T_{SK}(\lambda_1+\lambda_2+\lambda_3+\lambda_4)(P_{SK\_REQ}+P_{SK\_RSP}). \quad (5.9)$$

Let ρ indicate the average node density around RSU. Then, each node within $(D+R)$ distance from the RSU will need to send out a *SK_Update* message, so that

$$C_{O2} = 4\rho(D+R)P_{SK\_UP}. \quad (5.10)$$

Due to the presence of the dummy IP/MAC entries, the RSU can arbitrarily configure its period T_{IP} for broadcasting *IP_SW* messages. Thus, IP/MAC exchange causes

$$C_{O3} = P_{IP\_SW}T_{SK}/T_{IP}. \quad (5.11)$$

Thus, based on (5.9), (5.10) and (5.11), the average communication overhead for every T_{SK} is

$$c_o = (C_{O1} + C_{O2} + C_{O3}). \quad (5.12)$$

Once the practical traffic parameters are plugged in, the communication overhead of STCP2 can be estimated. This overhead can be controlled to an acceptable level by changing T_{SK} and T_{IP}. Besides, in (5.12) the overhead incurred by *SK* update depends on the node density and *D*, so c_o can be controlled by changing *D*.

***Average Privacy*:** Given *D*, the path length of a node *A* in CR is 2*D*. Suppose that the minimal and maximal average speeds of *A* in CR are v_{min} and v_{max}. Thus, the minimal and maximal time *A* spends in CR are $\Delta t_{min} = 2D/v_{max}$ and $\Delta t_{max} = 2D/v_{min}$. Let t_a be the time point of *A*'s entry, then $[t_a+\Delta t_{min}, t_a+\Delta t_{max}]$ define the possible time range of *A*'s exit from CR. Thus, the nodes existing from CR within the time range $[t_a+\Delta t_{min}, t_a+\Delta t_{max}]$ may be mistaken as *A* by GPA and LPA. Let S_A be the set of nodes can be mistaken as *A*. Then,

$$| S_A | = (\Delta t_{max} - \Delta t_{min})(e_1+e_2+e_3+e_4). \quad (5.13)$$

In (5.13), e_i is the departing rate of each exit point. Assuming that this intersection has no parking lot, then $(e_1+e_2+e_3+e_4) = (\lambda_1+\lambda_2+\lambda_3+\lambda_4)$. So,

$$| S_A | = (\Delta t_{max} - \Delta t_{min}) (\lambda_1+\lambda_2+\lambda_3+\lambda_4). \quad (5.14)$$

Based on (5.14), the privacy of A can be estimated as

$$P_A = \log|S_A|. \quad (5.15)$$

Equation (5.15) is based on the common entropy-based privacy definitions as in [117], [119]. Thus, from (5.13) to (5.15), the average privacy of each node can be controlled by the RSU by configuring D. Besides, the RSUs with higher traffic volumes will ensure higher privacy for any node. Thus, the privacy-aware RSU deployment algorithm should consider the traffic volume of each road intersection, which will be our future work.

Especially, D has direct impact on both communication overhead c_o and privacy P_A for any nodes. As shown in (5.12), bigger D results in higher c_o, while smaller D results in lower P_A. Thus, it is up to the VANET administrators to configure a proper D for each RSU, trading off the desired P_A and the acceptable c_o based on the traffic conditions around this RSU. For example, D should at least be bigger enough to make P_A larger than 0, so that by passing by one RSU each node will generally increase its location privacy.

5.6 Property and Simulations

Here, the salient properties and potential applications of STCP2 are identified with detailed discussions. Besides, simulation results will be presented to corroborate the theoretical analysis of STCP2.

5.6.1 Privacy Protection Significance

As previously discussed, the short-time certificate schemes are appealing to the future VANETs. Thus, by thoroughly investigating the privacy impacts of short-time certificate schemes and proposing novel algorithms to ensure privacy protection, STCP2 paves the way of adopting short-term certificates in VANETs.

Specifically, the progressive RSU deployment algorithm ensures the minimal privacy assurance for the common vehicular nodes even against the TA and RSUs. Thus, this minimal privacy assurance removes the common doubts about the short-time certificate schemes and makes them acceptable to the real-world users of VANETs. This algorithm

also considers the average travel distance between the deployed RSUs, maximizing the support to the traffic management, traffic safety applications of a given number of RSUs.

The privacy-preserving pseudonym update algorithm protects the location privacy of any nodes against the GPA, the LPA and the LAA. The secure message exchanges proposed in subsection 5.5.2 make certificate update confidential and secure. The IP/MAC exchange also ensures that the complete pseudonym of each node is changed nearby the RSU, so that to the GPA and the LPA this node will become a totally new node. The random mobility trace auditing will significantly increase the cost of LAA attacking to any given concerned regions. In summary, this privacy-preserving pseudonym update algorithm comprehensively considers the critical privacy challenges nearby the RSUs and ensures location privacy of vehicular nodes with novel procedures. With STCP2, each RSU can serve as a mix-zone [131], which is the foundation of many privacy protection schemes for VANETs.

5.6.2 Application Significance

With STCP2 implemented in VANETs, each RSU provides not only security and safety assurance, but also privacy enhancement to each node. Thus, the privacy strength of each travel route can be considered when a node selects its travel routes. Conventionally, travel time and travel distance are generally considered in route selection, as applied in GPS devices and digital map website. With STCP2, the privacy strength of each alternative route can be estimated based on the number of RSUs and the privacy strength of each RSU in each route. Then, the trade-off between privacy strength and travel cost can be achieved based on the preference of drivers. This potential privacy-aware route selection further exemplifies the application significance of STCP2.

5.6.3 Simulations

Here we run numerical simulations to verify the salient properties of STCP2 in light of privacy protection. First, to show the reduction in LAAs' negative impacts with the implementation of STCP2, the numbers (N_{m1}, N_{m2} and N_{m3}) of required LAAs to monitor all RSUs following three different attacking strategies discussed in subsection 5.5.3 are investigated. Based on simulated RSU deployment in Downtown Marquette, MI as discussed in subsection 5.4.3, N_{m1}, N_{m2} and N_{m3} are shown in Figure 5.10.

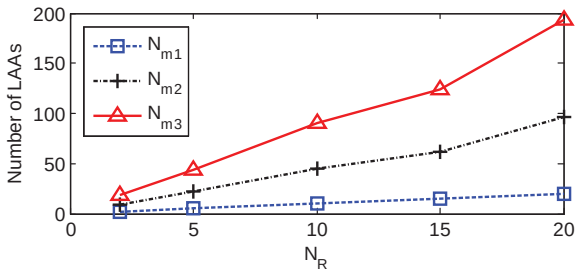

Figure 5.10 The required numbers of LAAs of different attacking strategies

As shown in Figure 5.10, for a given number of RSUs (N_R), N_{m2} is about 5 times of N_{m1}. Let T/T_0 be 2, N_{m3} is twice of N_{m2}. For instance, when there are 20 RSUs in this region (N_R = 20), the cost of deploying LAAs is increased from 20 LAAs to about 200 LAAs. Thus, the cost of deploying LAAs to continuously monitor all RSUs will increase significantly with STCP2. Additionally, STCP2 also significantly decreases the negative impacts of a given number of LAAs. In summary, by effectively detecting LAAs, STCP2 ensures that the nodes in CR only need to consider GPA and LPA.

Next, we investigate the privacy strength and communication overhead of STCP2 against the GPA and the LPA. Due to the lack of accurate traffic data collected in real roads, realistic vehicle mobility trace is simulated with MOVE [170]. Constrained by computation and memory requirements of simulating large VANET, a simplified roadmap with 5 intersections and one RSU, as shown in Figure 5.11, is adopted here.

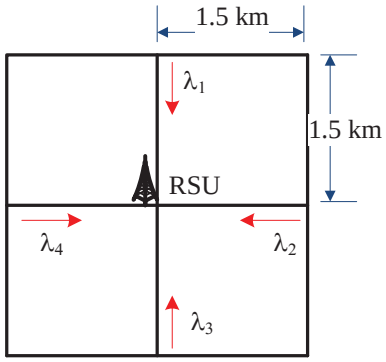

Figure 5.11 The road layout in the simulation of pseudonym changes

In this road layout, there are two road segments to both directions between any two adjacent intersections. The length of each road segment is 1.5 km, so the total road length is 36 km. The vehicles are evenly distributed to 4 flows as show with 4 red arrows, with the average vehicle arrival rate λ_i (i=1, 2, 3, 4). The total number of nodes changes from

100 to 360, with a step size of 20 vehicles. The average speed is 15 m/s, with on average the maximal speed of 30 m/s and the minimal speed of 5 m/s. For brevity, here we only show the simulation results for $D = R = 300$ meters.

The average privacy achieved by each node entering CR, as estimated in (5.15), is shown in Figure 5.12 and Figure 5.13. In Figure 5.12, the average privacy (P_A) achieved by each node entering this CR is shown, together with the minimal P_A and maximal P_A of all nodes. For any given λ_i, the minimal P_A is larger than 2 bits, which means that this node has at least 4 nodes in its anonymity set S_A. On average, each node can achieve a privacy of 4 bits. The occasional drops in minimal P_A and maximal P_A are caused by the randomness in node mobility.

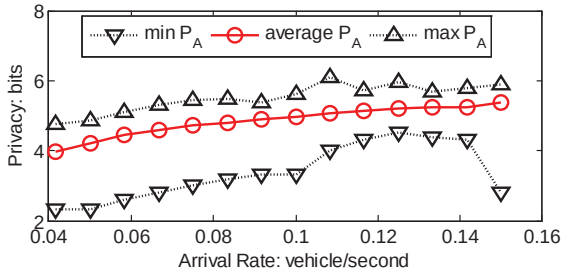

Figure 5.12 The average privacy of each node with minimal and maximal values

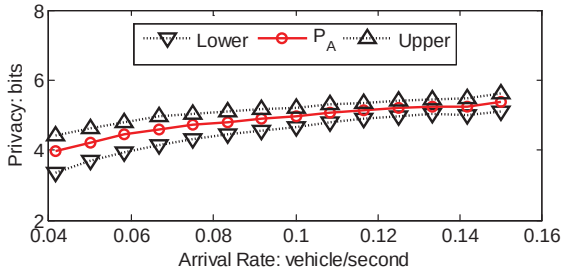

Figure 5.13 The average privacy of each node with 95% confidence level

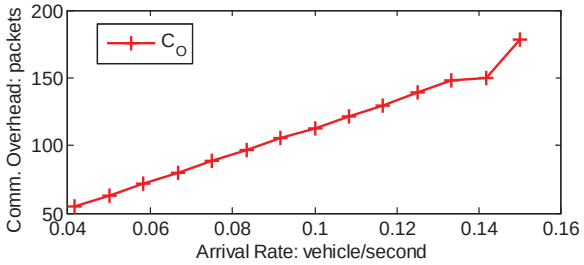

Figure 5.14 The average communication overhead per 100 seconds

In Figure 5.13, the average P_A and its 95% confidence intervals are shown for any given vehicle arrival rates λ_i. The confidence interval is quite small for any given λ_i, indicating that P_A can closely indicate the privacy achieved by each node entering CR.

The average communication overhead c_o as estimated in (5.12) is shown in Figure 5.14 for a given T_{SK} = 100s. As λ_i increases, c_o also increases from about 50 messages per 100s to about 170 messages per 100s. Given that these messages can be constructed with reasonable sizes, the communication overhead of STCP2 is reasonable for VANETs.

In summary, the simulations prove that STCP2 can significantly increase the cost of deploying LAAs in VANETs. Besides, the privacy of each node running by the RSU can be ensured with acceptable communication overhead.

5.7 Summaries

In this chapter, STCP2 is proposed to protect the location privacy of vehicular nodes with short-time certificates. STCP2 identifies the critical privacy implications of short-time certificate schemes, each of which might make short-time certificates unacceptable to VANETs without careful investigation. Then, a progressive RSU deployment algorithm is proposed in STCP2 to optimize the deployment of RSUs given a cost budget. The minimal privacy requirement of vehicular nodes is ensured in this algorithm, and the support to safety and security application is maximized. Eventually, the privacy-preserving pseudonym update algorithm makes the implementation of short-time certificates both secure and privacy-preserving.

Thus, STCP2 makes privacy protection in VANETs with short-time certificates both cost-effective and feasible, paving the way of adopting short-time certificates in VANETs. The potential applications enabled by STCP2, as discussed in subsection 5.6.2, make STCP2 even more appealing to VANETs.

As the future work, more realistic traffic statistics will be considered in STCP2 to make RSU deployment and the configuration of D more adaptive to realistic VANETs. Besides, more concrete cost-effect analysis of the possible attacking strategies of LAAs could be useful to help set the proper parameters in the random mobility trace auditing algorithm based on the realistic traffic statistics in any given region.

Chapter 6 Value-Added Applications

To further realize the application potentials of VANETs, in this chapter three promising value-added applications are identified and supported with novel solutions. Specifically, three novel schemes to support these value-added applications, namely VAAD [150] for VANET-based ad dissemination, GPAS [148], [149] for location-sensitive surveys and VehicleView [151] for vehicle sensor data collection, have been designed by Congyi Liu and me. My focus is on designing the architectural and security (privacy) solutions for these schemes, while Congyi Liu's focus is on ensuring efficient message dissemination and collection in these schemes. Thus, in this chapter, besides the big picture of each scheme, only the novel security and privacy solutions in VAAD [150], GPAS [148], [149] and VehicleView [151] are presented in detail. Our publications [148] [151] and manuscripts [149], [150], [152] provide the complete designs of each scheme.

6.1 Promising Value-Added Applications

With V2V and V2R wireless communications, VANETs provide a handy platform to various value-added applications involving vehicles and drivers/passengers. To such applications, vehicular communications generally incur lower cost than other communication technologies, e.g., cellular communications. Indeed, value-added applications can get a free-ride on vehicular communications, since traffic safety applications more than justify the cost of VANET implementation [208]. Besides, due to the close relation between each vehicle and its location information, value-added applications relying on the vehicle location information may be better supported in VANETs. Thus, VANETs can enable more cost-effective solutions to such applications.

On the other hand, value-added applications may financially benefit VANET users, VANET administrators and service providers. Especially, the revenue from such value-added applications may enable the VANET administrators to further upgrade VANETs. The presence of appealing value-added applications may encourage more drivers (vehicles) to actively participate in VANETs.

To further realize the economic potentials of VANETs, we propose secure and cost-effective solutions to three promising value-added applications. Specifically, a VANET-

based Ambient Ad Dissemination (VAAD) scheme [150] is proposed as a secure solution to VANET-based ad dissemination with practical cost and effect control. A General-Purpose Automatic Survey (GPAS) scheme [148], [149] is proposed as a secure and cost-effective solution to the location-sensitive surveys in VANETs. VehicleView [151], [152] is a secure and cost-effective solution to the large-scale and long-term collection of vehicular sensor data in VANETs. Actually, each of these schemes provides the first comprehensive solution to the corresponding application.

Besides their distinct novelties, these schemes share two salient features. First, a practical application model with an incentive-centered architecture is proposed for each application, so that the conflicting requirements of the involved entities are properly traded off. Secondly, proper security and security assurance is provided to each scheme, so that it can be readily implemented in realistic VANETs with various adversaries, including misbehaving vehicular nodes and rogue service providers.

6.2 Scheme Overview

Here, the overview of each proposed scheme is presented, based on which the common performance, security and privacy challenges are identified and discussed.

6.2.1 VANET-based Ambient Ad Dissemination (VAAD)

Considering numerous commercial service providers (SPs) and vehicles available in VANETs, VANET-based ad dissemination shows great market potential. However, without potent cost and effect control, arbitrary ad disseminations from various SPs may cause unnecessary distractions to the drivers and message storms to VANETs. Furthermore, the conflicting requirements of the involved parties remain to be carefully addressed. Specifically, each SP, to achieve the best advertising effect, wants to broadcast its ads to as many vehicles as possible, while the drivers generally only want to be notified of the local services. To VANETs as a whole, ad dissemination should be scalable to avoid message storms in face of increasingly more ads. Yet, the security and privacy issues of ad dissemination also call for thorough investigation.

As discussed in detail in [150], the existing schemes for ad dissemination in VANETs only, at best, partially tackle the above-mentioned challenges. Thus, VAAD [150] is proposed to ensure secure ad dissemination with pragmatic cost and effect control.

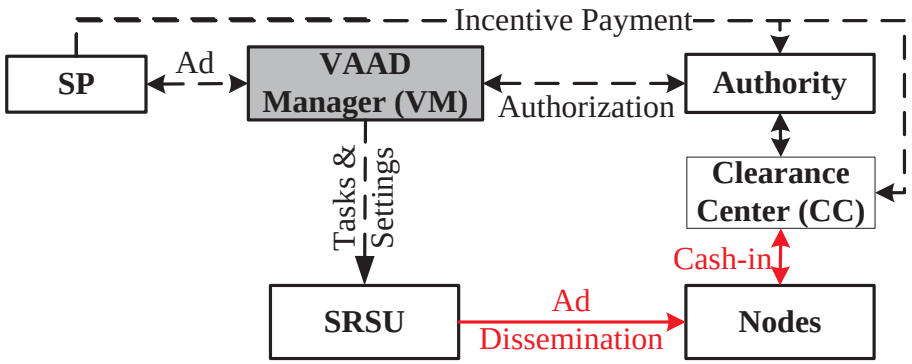

Figure 6.1 The system overview of VAAD

To balance the conflicting requirements of the involved parties, an incentive-centered architecture is proposed for VAAD, as shown in Figure 6.1, where the SP needs to pay other entities for their services in ad dissemination. Constrained by the incurred cost, the SP will set a realistic advertising effect requirement in terms of the number of ad receivers and the ad rebroadcast frequency. The VAAD Manager (VM) is introduced to interface and coordinate the involving parties in VAAD. Upon receiving a dissemination request from SP with cost and effect specifications, VM will obtain proper authorization from the VANET Authority for this ad. With the authorization, VM can request one RSU, usually the RSU nearest to the SP, to act as the source RSU (SRSU) to disseminate the ad.

With this incentive-centered system architecture, two novel algorithms are proposed to support pragmatic cost and effect control for ad dissemination in VAAD.

Distance-based Gradient Ad Dissemination: Inspired by the ad posting pattern in the physical world, a distance-based gradient ad dissemination algorithm is proposed in VAAD to maximize the ad effects given a cost budget. With this algorithm, the ads will be disseminated in such a way that the ad messages form a virtual ad post in VANETs. The key idea is to attenuate the density of a particular ad with a *gradient* $p \in [0,1)$ as the distance increases by a unit road segment (L) from the source RSU (SRSU), as shown in Figure 6.2. When vehicles drive around, they will receive ad packets about local services as if they were driving by real ad posts in the physical world. That is, the closer one vehicle is to a SP, the more frequently it will receive the ads from this SP. As such, the location relevance of ads is exploited to increase the actual advertising effect given a realistic cost budget.

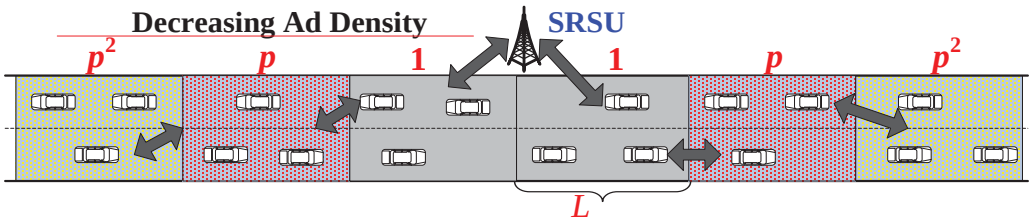

Figure 6.2 The ad density gradient in highway scenarios

Cash-in: To encourage vehicular nodes to strictly follow the ad dissemination requirements as defined by VM and the source RSU, certain incentive will be rewarded to each honest ad forwarder. A novel cash-in algorithm is designed to ensure that each ad forwarder can securely and indisputably prove its ad forwarding services, and obtain its deserved incentive from CC in a privacy-preserving way.

6.2.2 GPAS: a General-Purpose Automatic Survey System

The framework of a general-purpose automatic survey system (GPAS) was proposed by us in [148] to support the *location-sensitive* surveys based on VANETs. Here a location-sensitive survey is often interested in the traffic, transportation, traveling and commercial information of one specific area, such as the driving experience in a downtown area and the possible placement of a new fast food shop nearby a road intersection. For a location-sensitive survey, only the survey respondents related to the concerned geographic location will be able to provide useful information. Thus, the common survey methods [209] by telephone, mail, website or email, will not be efficient in locating the relevant survey respondents for such surveys. Besides, such conventional methods generally are costly, mainly relying on human efforts in information gathering and processing. Comparatively, the relevance between each vehicular node and its location makes VANETs a handy platform for the *location-sensitive* surveys.

The architecture of GPAS [148] is shown in Figure 6.3. GPAS requests each survey customer to pay incentives to the eligible survey respondents and the relevant entities for their services. Thus, constrained by the incurred cost, each survey customer will judiciously initiate its surveys and set reasonable quality requirements for each survey, which will make GPAS scalable in the face of numerous potential surveys. On the other hand, incited by incentives, the eligible vehicular nodes will become more willing to respond to the survey requests.

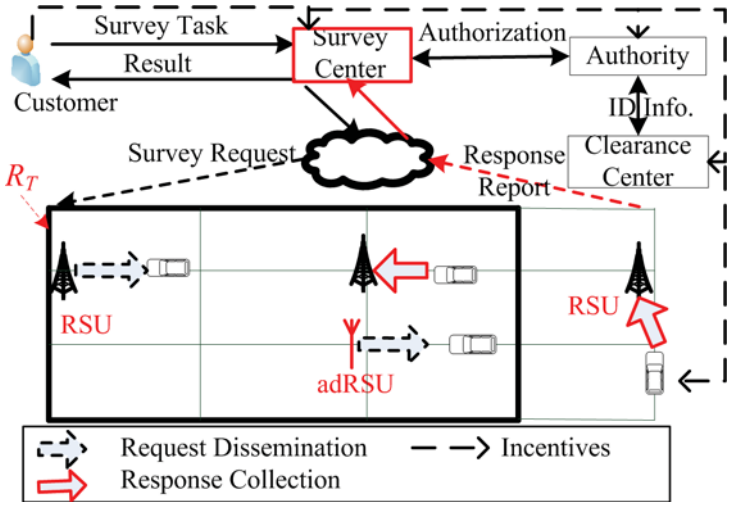

Figure 6.3 The system overview of GPAS

A survey center (SC) is proposed in GPAS to facilitate the interactions among the involved entities. A survey customer will send its survey request to SC, which will get a proper authorization from Authority for it. To efficiently disseminate the survey request to the eligible vehicles within the target survey region (R_T), SC will request the RSUs in R_T to disseminate the survey request. If necessary, adRSUs may also be deployed in R_T to facilitate survey request dissemination. Here, adRSUs are lightweight reusable devices with DSRC transceivers and can be temporarily deployed by SC to support the concerned survey. To allow the eligible nodes to efficiently and securely prove their eligibility, only 1-hop communication is adopted in survey request dissemination.

After receiving one survey request, the eligible nodes may decide whether to respond to this survey based on the incentive for this survey and the efforts required. The nodes agreeing to respond will construct their survey responses properly, and submit their survey responses to SC, via the help of (ad)RSUs both inside R_T and outside R_T. SC will verify the collected survey responses and forward the valid ones to the customer.

The major procedures of GPAS and their respective challenges are presented below.

Survey Request Initiation & Authorization: To initiate a survey, one customer needs to, based on its application requirements, minimize the expected cost while ensuring the desirable quality requirements of its survey. Then, the survey request needs to be specified as an accountable and undeniable service contract between the customer and SC.

To ensure security, SC needs to register the survey task at the Authority and obtain proper authorization for it.

Survey Request Dissemination: With the help of (ad)RSUs, the survey request will be disseminated to the nodes within R_T. The eligibility of any node regarding this survey should be securely proven and survey request dissemination should be accountable, so that future incentive payment can be properly supported.

Survey Response Collection: The survey responses generated by the eligible nodes will be collected by (ad)RSUs and forwarded to SC. While submitting the survey responses, the privacy of survey respondents should not be compromised. To meet the quality specifications of the customer, SC will verify the survey responses to remove the duplicate ones, which may be difficult due to the presence of pseudonyms in VANETs.

Cash-in: After completing a survey, the customer needs to pay incentives to CC, Authority, SC and each honest survey respondent for their services, in a secure and privacy-preserving way.

Thus, GPAS is designed to provide customized location-sensitive survey services in a cost-effective, secure and privacy-preserving way. The key functional, security and privacy challenges are identified and carefully addressed in GPAS [148], [149].

6.2.3 VehicleView

Exemplified by large-scale vehicle field testing, after-sale vehicle performance monitoring, remote vehicle diagnostics, fuel consumption analysis, fleet management, driver behavior analytics, etc., the vehicle performance monitoring and analysis (VPMA) applications show great economic potentials. In general, the VPMA applications rely on the large-scale and long-term collection of vehicular sensor data. For instance, to optimize the future vehicle designs, one vehicle manufacturer may need to collect the engine states of a particular vehicle model in practical uses over (say) 5 years. Besides, with numerous sensors installed in each vehicle, large-scale and long-term vehicular data collection becomes more necessary and challenging, as indicated by the existing commercial vehicular telematics solutions such as OnStar [210] and Ford SYNC [211]. However, these commercial solutions are proprietary systems with applications constrained to specific car manufacturers. Besides, relying on cellular communications

such solutions incur service fees from the application users and require special communication devices in vehicles. Last, with free access to all location and speed states of each vehicle, such solutions impose severe privacy risks to the vehicle drivers [212].

Thus, VehicleView [151], [152] is proposed as a secure and cost-effective solution to large-scale and long-term vehicular data collection based on VANETs. Exploiting V2V and V2R communications, VehicleView is especially cost-effective without any special hardware requirements to vehicles. Moreover, the relevant security and privacy issues are thoroughly addressed in VehicleView with novel solutions. To our best knowledge, VehicleView is the first scheme to support secure and cost-effective vehicular sensor data collection based on VANETs.

In general, to support a specific vehicular sensor data collection application the application customer, say a car manufacturer, firstly will determine its information requirements, for instance, the data to show the engine performance degradation curve of a new vehicle model. Then, the customer may select a subset of vehicles as the data sources (*target vehicles*). The data requirements and incentive information, in form of a *task request*, will be sent to the target vehicles, among which some will agree to participate in this task as the *participants*. The participants will later generate data reports and send them to the customer through V2V and V2R communications. Eventually, the customer will process the collected data in an application specific way.

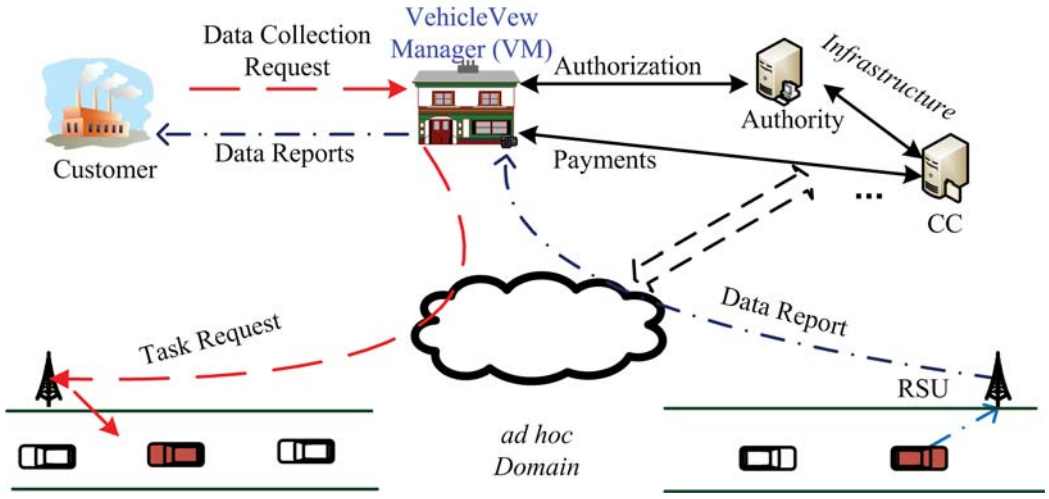

Figure 6.4 The VehicleView overview (© 2011 IEEE. Reprinted with permission)

The above functions, except for the application-specific information requirement determination and data processing, will be supported by VehicleView as proposed in Figure 6.4 [151]. In VehicleView, Authority, Clearance Center (CC), RSUs and vehicular nodes are pre-existing entities in VANETs. The VehicleView Manager (VM) is designed as an interface between the customer and VANETs. To encourage and reward the cooperation of relevant parties, the customer needs to pay certain incentives to Authority, CC, VM and each vehicular participant for their services. Thus, such entities are economically encouraged to participate in VehicleView, and the customer is forced to judiciously initiate data collection tasks in VANETs.

Specifically, VehicleView includes the following major functional components.

Pricing: The customer needs to determine proper incentives for its data collection task, to meet its information requirement with a minimal cost.

Task Registration: Once receiving a task from a customer, VM needs to register it in Authority for proper authorization, which is essential to ensure undeniable and trustworthy interactions among the relevant parties.

Task Dissemination: The task request needs to be securely and efficiently disseminated to the target vehicles, which may be challenging, since the locations of target vehicles may be unknown due to privacy protection.

Data Reporting: The data reports from each participant will be sent to the customer via V2R and V2V communications. Here, the challenge is to protect the location privacy of participants and ensure efficient report submission at the same time.

Therefore, incurring only limited software updates to the existing VANET entities, VehicleView is especially cost-effective. With novel algorithms to address the security, privacy and economy challenges, VehicleView shows great application significance and economic potentials for VANETs.

6.3 Critical Challenges

These proposed schemes face critical performance, security and privacy challenges in VANETs, as listed in Table 6.1. In Table 6.1, the challenges imposed by these schemes fall into two categories, namely common challenges and unique challenges. Both types of challenges will be discussed in detail here.

Table 6.1
Critical challenges imposed by VAAD, GPAS and VehicleView

	VAAD	GPAS	VehicleView
Common Challenges	Practical Application Model		
	Efficient and Privacy-preserving Incentive Distribution		
	Authorization		
	NA	Privacy-preserving Data Collection	
Unique Challenges	Efficient & Reliable Ad Forwarding	Surveys Quality Model	Efficient Task Request Dissemination
	Forming Virtual Ad Post	Scalable Collection of Survey Request Receipts	Sensor Data Access Control

As shown in Table 6.1, to design a practical application model is challenging in VANETs, since it is difficult to comprehensively consider the conflicting requirements of the involved entities. Besides, to distribute incentives to each vehicle is challenging due to privacy protection in VANETs, which makes the real identity and location of each node unknown. Furthermore, it is critical to enable the customer of each application to securely and accountably interact with VANET entities, which requires a secure authorization procedure. Last, GPAS and VehicleView involve data collection from vehicular nodes, which may impose risks to the location privacy of vehicular nodes. These common challenges will be discussed in detail in the following sections.

Besides, each application imposes unique challenges. Next, these unique challenges and the corresponding solutions will be briefly discussed. The corresponding details are presented in our publications [148], [151] and manuscripts [149], [150], [152].

Efficient & Reliable Ad Forwarding: In VAAD, it is critical to ensure that each ad forwarder will reliably forward the ad packet. Besides, the number of ad forwarders required to forward the ad to the requested distance should be reduced, since each ad forwarder requires a certain incentive from the customer. To ensure both efficient and reliable ad forwarding in VAAD, two novel algorithms are proposed as discussed next.

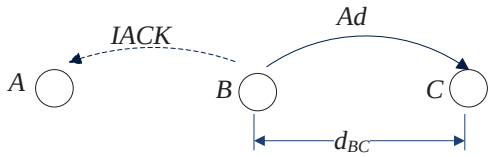

Figure 6.5 The exemplary ad forwarding procedure in one hop

As shown in Figure 6.5, the current ad forwarder *B* is forwarding the ad packet to its downstream ad forwarder *C*. Here, one novel algorithm is proposed for *B* to select the

best downstream ad forwarder based on the distance between *B* and its neighbors, as well as the average successful reception ratio of its neighbors. Thus, the downstream ad forwarder will result in best efficiency for this hop. Besides, an ARQ (Automatic Repeat reQuest) [213] based algorithm is proposed to ensure reliable ad forwarding in each hop. For instance, by overhearing the ad forwarded by *B*, *A* will regard this overheard ad as the implicit acknowledgement (*IACK*) to the ad sent by itself to *B*. If no *IACK* is overheard, *A* may retransmit the ad until it overhears an *IACK* or an explicit acknowledgement from *B*. This way, each forwarder will make sure of the behaviors of its downstream forwarder.

Forming Virtual Ad Post: In VAAD, to form the virtual ad post as shown in Figure 6.2, the source RSU will randomly select the requested ad dissemination distance D_i for each rebroadcast of this ad according to a proper probability distribution as discussed in [150]. Once D_i is selected, only the ad forwarders within distance D_i from the source RSU will be rewarded with incentives. As such, the vehicular nodes are encouraged to forward the ad in such a way that a virtual ad post will be formed.

Quality Model of Surveys: In GPAS, a novel quality model is proposed as a 3-tuple (N, i, ε) to model the quality requirements of the survey customers. Here, N is the total required number of survey responses, and i is the maximal number of misbehaving survey respondents, each of which produces at least two survey responses. ε is the uncertainty level of satisfying this quality requirement. Altogether, (N, i, ε) means that totally N survey responses are required, and the probability of more than $2i$ duplicate survey responses is at most ε. Thus, this quality model allows the customer to control the bias of opinions in the collected survey responses.

One major advantage of this quality model is that it enables the scalable verification of survey responses. Briefly speaking, based on a given quality requirement (N, i, ε), only k ($0<k<N$) survey responses need to be verified in order to meet this quality requirement, where k can be theoretically selected based on (N, i, ε) [148], [149]. This way, survey verification becomes scalable, which is most important to GPAS in face of increasingly more survey tasks.

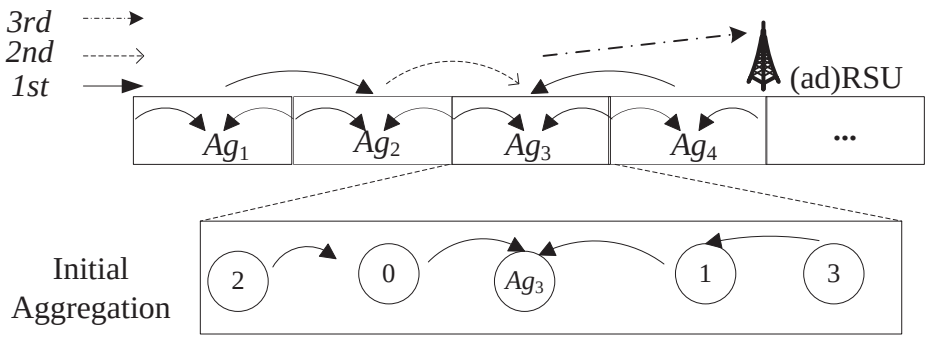

Figure 6.6 The message flows of bipartite receipt collection with b=3

Scalable Collection of Survey Request Receipts: In GPAS, after broadcasting a survey request, the RSU needs to collect a receipt from each receiver of the survey request. However, due to node mobility each node can only directly communicate with the RSU for a limited duration. On the other hand, the transmission of one receipt from a node to the RSU may take up to seconds, depending on the network conditions. To ensure scalable collection of survey request receipts, a bipartite receipt collection algorithm (BRCA) is proposed in GPAS, as shown in Figure 6.6.

The main idea of BRCA is to divide the 1-hop neighbors of the RSU into 2^b clusters. Within each cluster, each node reduces its transmission power to cover only $R/2^b$ distance, and sends its receipt to an aggregator. In this way, the aggregation within each cluster can be performed in parallel. Then, the aggregated receipt in each cluster is further aggregated to an upper-layer aggregator, until all receipts are aggregated at the RSU. In this process, novel algorithms are designed to ensure reliable aggregation and to configure a proper aggregation level b based on the current network conditions.

Efficient Task Request Dissemination: In VehicleView, the data collection task needs to be sent to each eligible vehicle selected by the VehicleView customers. However, in VANETs, the real identity and location history of any vehicular node are unknown to the customers, so task request dissemination becomes challenging. To flood the whole VANET with task requests will incur heavy communication overhead. Thus, in VehicleView a regional query-based request dissemination algorithm is proposed for efficient and reliable task dissemination.

Sensor Data Access Control: In VehicleView, the vehicle sensor data should not be accessed by any entity without the consent of the vehicle owner. In VehicleView, several

practical guidelines are proposed to ensure secure and privacy-preserving access control to vehicle sensor data.

6.4 Incentive and Incentive Distributions

In any value-added application two critical questions arise: 1) how to create a practical application model, and 2) how to direct the distribution of economic value. To answer these two questions, an incentive-centered architecture is proposed for VAAD, GPAS, and VehicleView by following two design guidelines.

6.4.1 Design Guidelines

The first guideline is that the VANET-based value-added application should follow the application model of the general value-added applications. The value-added applications, for instance, ad dissemination, survey or vehicular sensor data collection, have been present before the concept of VANETs was proposed. Thus, the existing application models are mature and reasonable, comprehensively considering the conflicting requirements of the involved entities. So, it is natural for VANET-based solutions to follow these application models.

The second guideline is to use economic incentive to trade off the conflicting requirements of the involved entities. For any application, the entities benefit from this application need to pay incentives for the services obtained from this application. On the other hand, the entities providing services, for instance, data forwarding, to this application should be rewarded with incentives. In this way, the conflicting requirements of the involved parties are properly reconciled, and the involved parties are financially encouraged to participate in each application.

For instance, in VAAD, the service provider (SP) who intends to broadcast its ads should pay incentives to the VANET Authority, Clearance Center, VAAD Manager and each honest ad forwarder for their services. The vehicular nodes are financially encouraged to forward ads for the SP to facilitate ad dissemination. On the other hand, the ad receivers should not be rewarded, since they will overhear the ads anyway due to the nature of wireless communications. Thus, the ad receivers do not provide any service to VAAD. Thus, the incentive model of VAAD is more practical than that adopted in [15], where the ad receivers will also be rewarded with incentives.

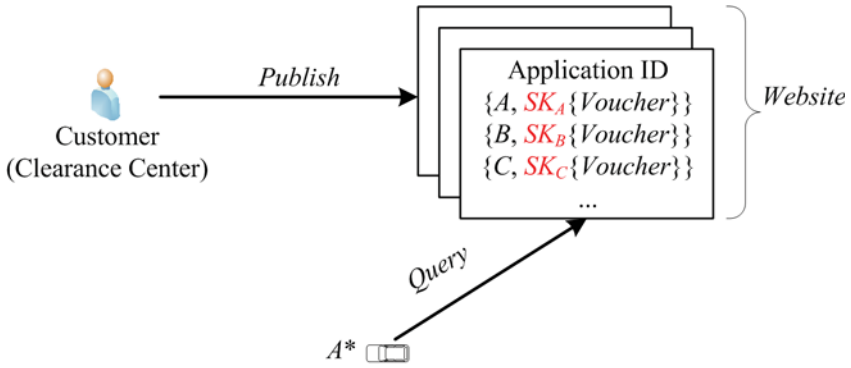

Figure 6.7 The pull model-based incentive distribution

6.4.2 Efficient and Privacy-Preserving Incentive Distribution

In VAAD, GPAS, and VehicleView, the customer or the Clearance Center needs to distribute incentives to each honest vehicular participant. However, in VANETs each node uses its pseudonym in communications for privacy protection [5]. The real identity and location history of any node should be kept secret from all entities except for the VANET Authority. Besides, suppose a node (N_i) uses a pseudonym A in participating in the application. Its pseudonym may have changed to A^* when the incentive is distributed. For privacy protection, the connection between A and A^* should not be known to the customer or the Clearance Center. Constrained by these privacy concerns, one incentive distribution approach is to flood VANETs with the incentive for N_i, which will incur unacceptable communication overhead considering the huge number of incentives.

Thus, a pull model-based incentive distribution approach is proposed for these applications, as shown in Figure 6.7. Here, it is assumed that an E-cash scheme [214] is adopted in VANETs, so that incentives are represented with E-cash vouchers. The advantage of E-cash is that the voucher can be securely verified without revealing the identity of the voucher user, which is beneficial to privacy protection in VANETs.

Besides, in these applications, each honest node N_i with a pseudonym A has already securely established a secret key SK_A with the customer. In distributing the incentives, the customer will encrypt the E-cash voucher for node N_i with SK_A. All encrypted vouchers for a certain application will be published in a public website, as shown in Figure 6.7. The original pseudonym of each node, such as A, B and C, will be used to indicate the owner of each encrypted voucher. Afterward, node N_i, with a new pseudonym A^*, can

query the website to obtain the E-cash voucher intended for itself. In this process, the connection between *A* and *A** will not be known to the customer. Besides, the E-cash voucher for each node is only accessible to this node alone. Furthermore, this pull model-based approach is more efficient than to flood VANETs with incentives.

6.5 Authorization of Customers

In any application, the customer's application contract, for example a survey request in GPAS, specifies the quality requirements and payment information of this customer. Thus, the application contract cannot be denied by the customer. Besides, the application Manager, for instance, the VAAD Manager for VAAD, needs to request RSUs in VANETs to disseminate application-specific messages. To this end, the Manager needs a proper authorization from the VANET Authority to convince the RSUs and the vehicular nodes of the authenticity of the messages it sends out.

To meet these critical security requirements, a common authorization procedure as shown in Figure 6.8 is proposed for GPAS and VehicleView, which can also be adopted in VAAD. Here, it is reasonably assumed that both the customer and the Manager have obtained public/private key pairs and certificates from the VANET Authority. The generic formats of these messages are presented next, and the concrete message formats can be found in [149]-[151].

Customer → Manager: $Contract = \{Payload_{Cust} = \{ID_{Cust}, TSP_{Cust}, K_{Cust-MN}\{Specs=\{QoS, Payment\}, Info\}, PU_{MN}\{K_{Cust-MN}\}\}, \{H(Payload_{Cust})\}PR_{Cust}, Cert_{Cust}\}$.

Here, ID_{Cust} is the ID of the customer, and TSP_{Cust} is the timestamp. *Specs* contain the parameters of quality and cost requirements, as well as application-specific content (*Info*). $K_{Cust-MN}$ is a session secret key established between the customer and the Manager by the customer, which is further encrypted by PU_{MN}, the public key of the Manager.

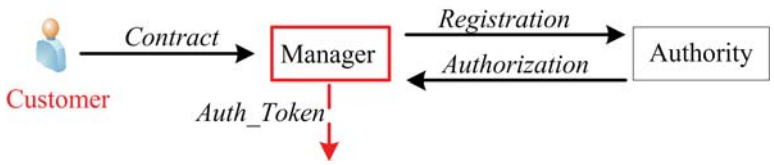

Figure 6.8 The registration and authorization of an application request

$H()$ is a standard hash function, such as SHA-512 [168]. Thus, $\{H(Payload_{Cust})\}PR_{\text{Cust}}$ is the digital signature for this message, signed by the private key of the customer (PR_{Cust}). $Cert_{Cust}$ is the certificate of the customer issued by Authority.

Thus, only the customer and the Manager can figure out $K_{Cust–MN}$, so the sensitive contents in *Contract* are confidential. Besides, with digital signature the customer explicitly specifies its application contract the manager accountably and undeniably.

Upon receiving *Contract*, the Manager will assign an ID to this application contract, and obtain a proper authorization from Authority with the following message exchanges.

Manager → Authority: $Registration = \{Payload_{MN}=\{ID_{MN}, ID_{App}, Contract, TSP_{MN}\}, K_{MN\text{-}Auth}\{K_{Cust\text{-}MN}\}, PU_{Auth}\{K_{MN\text{-}Auth}\}, \{H(Payload_{MN})\}PR_{MN}, Cert_{MN}\}$.

SC ← Authority: $Authorization = \{Payload_{Auth} = \{TSP_{Auth}, K_{MN\text{-}Auth}\{Auth\_Token\}, \{H(Payload_{Auth})\}PR_{Auth}\}$.

$Auth\_Token = \{Token=\{ID_{App}, ID_{MN}, TSP_{Auth}, Specs2, Info\}, \{H(Token)\}PR_{Auth}\}$.

Here, ID_{MN} is the ID of the Manager, and ID_{App} is the ID of this application request as assigned by the Manager. *Specs*2 contains the application parameters which are relevant to the vehicular participants. *Auth_Token* is an authorization token generated by Authority, which allows the Manager to request the RSUs to broadcast application-specific messages for the Manager.

Thus, the survey request from the customer is accountably and undeniably registered at the Manager and Authority, and the Manager obtains a proper authorization from Authority. With this authorization, the Manager is able to request the RSUs to perform specific communications for this application. The above generic message exchanges specify the common authorization procedure in VAAD, GPAS, and VehicleView, and can be instantiated based on the specific application requirements.

6.6 Privacy-Preserving Data Collection

As discussed in section 6.4, one node may assume different pseudonyms while participating in each application. Especially, in both GPAS and VehicleView, one node may assume a pseudonym *A* while receiving the task request, and assume another pseudonym *A** while generating survey response or data report. Thus, it is necessary to prevent the RSUs and the customers from learning the connection between two

pseudonyms adopted by one vehicular node, which is the underlying requirement for privacy protection in VANETs. To this end, a privacy-preserving data collection algorithm is proposed for GPAS [148], [149] and VehicleView [151], [152], with two novel mechanisms: *randomized submission distance* and *per-hop re-signing*.

Randomized submission distance: To submit its data, a node $Node_i$ will select a submission distance d_s with a uniform distribution over (0, D_S). Here, $D_S > R$ is a configured threshold of d_s, the configuration of which has been discussed in detail in [149], [151]. When $Node_i$ is d_s away from the next RSU, it will send its data to the RSU.

Per-hop re-signing: Initially, $Node_i$ signs its data ($Data(A)$) with the private key associated to the original pseudonym (say A). In GPAS, $Data(A)$ is the survey response generated by this node; in VehicleView, $Data(A)$ is the data report generated by this node. In each hop from $Node_i$ to the RSU, $Data(A)$ will be treated as a payload, and each forwarder will digitally sign it with its own private key, as shown in Figure 6.9. Thus, once the RSU receives the payload with a digital signature, it cannot figure out the originator node of this payload, so the relation between A and A^* is concealed.

In this process, $Data(A)$ will be directly sent to the RSU by $Node_i$, if $d_s < R$. Otherwise, the data packet will be relayed by several intermediate forwarders. If one forwarder runs into a network partition, it will keep the survey response and send it to the RSU when runs into the communication range of the RSU. To ensure that each forwarder will reliably forward the authentic survey response, LEAPER [142] can be adopted.

As discussed in [149], [151], this algorithm can effectively prevent the RSUs and the customer from connecting the different pseudonyms used by one same application participant. Thus, secure and privacy-preserving data collection can be ensured in both GPAS and VehicleView.

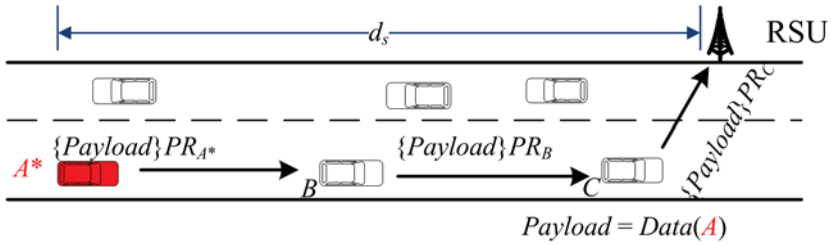

Figure 6.9 The privacy-preserving survey responses collection

6.7 Summaries

In this chapter, VAAD, GPAS and VehicleView are presented as cost-effective solutions to various VANET-based value-added applications. Besides their distinct theoretical novelties, these schemes all feature a practical application model, as well as proper security and privacy assurance. To our best knowledge, these schemes are the first comprehensive solutions to the corresponding applications, showing great application potentials to VANETs.

Chapter 7 Future Work and Conclusions

In this chapter the major contributions of this dissertation will be summarized, and discussions will be provided to facilitate the implementation of the proposed schemes. Then, detailed discussions of the promising future work will be presented. In the end, high-level conclusions will be given to conclude this dissertation.

7.1 Major Contributions

This dissertation addresses several critical security and privacy issues of VANETs, and provides novel solutions to further enhance the security and privacy of VANETs. Besides, novel solutions to three promising value-added applications are also provided to further realize the application potentials of VANETs. Besides being theoretically novel, each proposed scheme also considers the unique properties of VANETs. Thus, these schemes can be readily implemented in VANETs. By addressing the critical security, privacy and application issues of VANETs, this dissertation facilitates the realistic implementation of VANETs in the near future.

Next, the salient properties and implementation considerations of each proposed scheme will be provided. Afterward, the contribution of this dissertation to the traffic engineering community and the VANET community will be discussed.

7.1.1 LEAPER

As discussed in **Chapter 2**, LEAPER [142] ensures reliable and trustworthy multi-hop communications by properly handling the malfunctions and misbehaviors in data packet relaying. A novel adaptive role playing (ARP) strategy is proposed in LEAPER to enhance the cooperation of the neighboring nodes in each hop. This strategy prevents the malfunctions and misbehaviors of individual nodes from harming the trustworthy data packet relaying in any hop. In this sense, LEAPER shows great advantage over the existing schemes which usually suffer from such malfunctions and misbehaviors. Besides, by properly configuring the tradeoff between security strength and communication overhead, LEAPER can achieve higher performance in terms of successful packet delivery. Thus, LEAPER can be implemented in VANETs to better support the applications which rely on multi-hop communications.

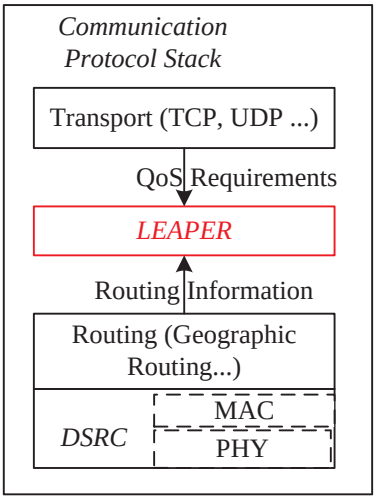

Figure 7.1 An exemplary communication protocol stack for vehicular nodes

LEAPER can be easily implemented in each node as a protocol component to support various VANET applications. LEAPER is a protocol between the transport layer and the routing (network) layer in the communication protocol stack, as shown in Figure 7.1. Taking the QoS requirements from the transport layer, the security parameter of LEAPER can be configured as discussed in Chapter 2. Then, LEAPER ensures reliable and trustworthy packet relaying in each hop, determining the next hop based on the routing information from the routing layer. Our publication [142] provides sufficient information to design the protocol procedures of LEAPER, as well as useful guidelines to configure the security parameter of LEAPER. Besides, to further reduce the computation overhead of LEAPER, RAMV can be adopted in each trust group to allow the group members to adaptively share the computation load of packet verification.

7.1.2 RAMV

In **Chapter 3** RAMV ([143], [144]) addresses the scalability issues imposed by the computation-extensive verification of messages, especially beacons in VANETs. RAMV differentiates the received messages based on their application relevance, and allows each node to verify the messages of high application relevance with a high probability as allowed by its resource budget. By piggybacking the verification results, the neighboring nodes can efficiently exchange their message verification results, so that each node will learn the authenticity status of all its received messages. Thus, RAMV enables the neighboring nodes to share the computation load of message verification. With RAMV,

in any network scenario each node can verify the received messages in a resource-aware, application-friendly and secure way. Thus, RAMV can be adopted for each node to efficiently verify the received messages in the single-hop communication scenarios. In this sense, RAMV enables many important traffic safety, traffic management, and commercial applications which rely on authentic messages exchanges.

RAMV [143], [144] is a security scheme residing in the application domain of each vehicular node. It can be implemented as a scheduler for the concrete message verification algorithms, as shown in Figure 7.2. Given a concrete VANET application (for example, collision avoidance) and a concrete message verification algorithm in the Message Verifier (for example, ECDSA [181]), RAMV can be implemented by following the algorithms described in Chapter 3.

Specifically, RAMV needs to support the user's configuration of the resource budget for message verification. Based on the resource budget and the number of received messages, RAMV will estimate the filtering probability (p) for the Message Verifier to probabilistically decide whether to verify each received message based on its relevance rank. Besides, the Message Receiver needs to route the received piggybacked notification to RAMV, and the Message Transmitter needs to send out the notifications generated by RAMV in a piggybacked manner. The concerned applications should be able to accept the indirect message verification results which are learned by RAMV from the neighboring nodes directly verifying such messages.

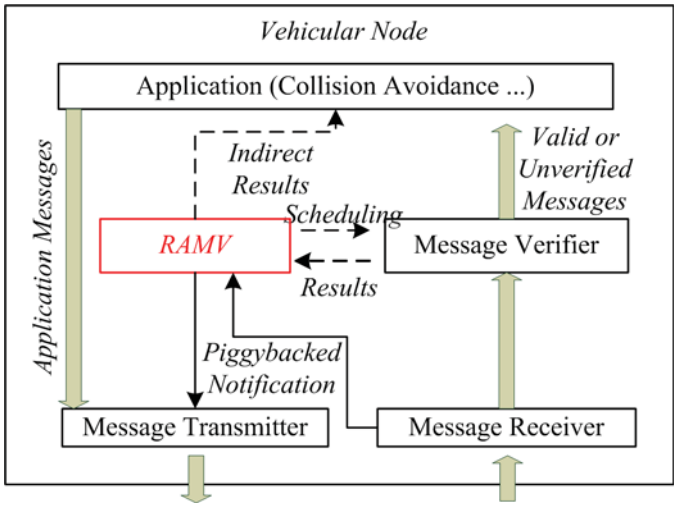

Figure 7.2 One feasible implementation framework of RAMV

7.1.3 JPRA

Chapter 4 introduces JPRA [146], a joint privacy and reputation assurance scheme to reconcile the inherent conflicting requirements of privacy protection and reputation management. JPRA adopts a localized reputation management model to support efficient reputation management in face of frequent network topology changes incurred by node mobility and pseudonym changes. Besides, novel algorithms are proposed to prevent reputation update and reputation manifestation from helping the adversary trace the pseudonym changes of each node. Thus, JPRA efficiently and synergistically supports both privacy protection and reputation management in VANETs, so JPRA is critical to the future implementation of VANETs.

The implementation of JPRA involves modifications to both the privacy protection and the reputation management schemes, as shown in Figure 7.3. While implementing JPRA, the specific privacy protection scheme, reputation aggregation algorithm, and behavior monitoring algorithm are the given conditions.

Specifically, the privacy protection scheme needs to notify JPRA of its pseudonym change in advance to give JPRA sufficient time to update the reputation label of the concerned node. Chapter 4 already estimates the time required for the update of reputation label in JPRA. Besides, the privacy protection scheme needs to consider the reputation label as a component in the pseudonym. If one node has a unique reputation label among its neighbors, the privacy protection scheme should refrain from any pseudonym change, since a pseudonym change would be futile. On the other hand, given a specific node behavior monitoring algorithm and a reputation aggregation algorithm, JPRA accomplishes the necessary functions of reputation management.

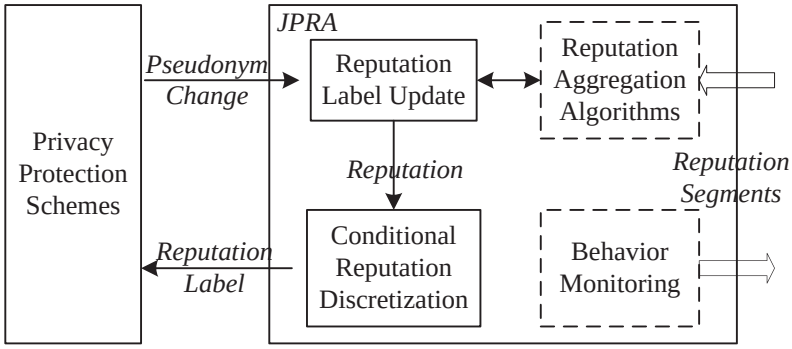

Figure 7.3 One feasible implementation framework of JPRA

7.1.4 STCP2

Chapter 5 identifies and thoroughly investigates the privacy protection issues imposed by short-time certificates to VAENTs. STCP2 [147] optimizes RSU deployment in terms of privacy protection and security provisioning given a deployment cost, properly handling the power abuse of RSUs and VANET Authority. With the RSUs deployed, secure and privacy-preserving pseudonym update procedures are designed for each node to update its certificate and change its pseudonyms at each RSU. Thus, running by an RSU, each node will enhance its location privacy with confidential pseudonym changes against all possible adversaries. Due to the application potentials of short-time certificates, STCP2 is essential to privacy protection in VANETs.

If short-time certificates are to be adopted in VANETs, the RSUs need to be deployed following the progressive RSU deployment algorithm in STCP2, so that a minimal privacy assurance will be provided to the vehicular nodes in face of the power abuse of VANET authorities and RSUs. Besides, the secure pseudonym update procedures need to be implemented in each vehicular node and each RSU. With STCP2 implemented in VANETs, each RSU can periodically report the average privacy achieved by the passing-by vehicles. Such information could be used in GPS devices and digital map websites to provide privacy-aware travel route recommendations to the real-world users, as discussed in Chapter 5.

7.1.5 Value-added Applications

Chapter 6 introduces three promising value-added application solutions for VANETs, namely VAAD [150], GPAS [148], [149], and VehicleView [151], [152].

Table 7.1
Implementation requirements of VAAD, GPAS and VehicleView

Entities	**Requirements**
Vehicular Node	To install an APP software for this application
RSU	To install an APP software for this application
Managing Entity	To be operated by a third party
VANET Authority	To support the authorization of new entities and new messages incurred by new applications
Clearance Center	To support the financial operations of new applications
Customer	To be able to communicate with the managing entity of each value-added application

VAAD provides a secure and privacy-preserving solution to ad dissemination in VANETs with practical cost and effect control. GPAS is a cost-effective solution for supporting location-sensitive surveys in VANETs, including commercial surveys and traffic surveys. VehicleView enables the large-scale and long-term collection of vehicular sensor data to support various vehicle performance monitoring applications. An incentive-centered architecture is proposed in each solution to trade off the conflicting requirements of the involved entities. Besides, the critical application-specific security and privacy issues are identified and solved with novel algorithms. To our best knowledge, our solutions are the first comprehensive ones to these promising applications.

To implement each solution in VANETs, the involved entities need to be created or modified, as summarized in Table 7.1. From Table 7.1, the technical efforts for supporting such value-added applications are reasonable, with only software updates for vehicular nodes, RSUs, the VANET Authority, and the Clearance Center. The corresponding managing entity, VAAD Manager (VM) for VAAD, Survey Center (SC) for GPAS, and VehicleView Manager (VM) for VehicleView, can be created and operated by either the administrators of VANETs or by the profit-seeking companies. Furthermore, these applications require a business-friendly environment which is still to be created by the policy-makers and stakeholders of VANETs. Thus, these applications can serve as a proper use case for the policy-making processes in VANETs. Hopefully, the application potentials of these value-added applications can facilitate the set-up of a business-friendly environment for VANETs.

7.1.6 Supports to Traffic Engineering

In general, the schemes proposed in this dissertation provide valuable supports to traffic engineering and traffic management, which are identified and justified as follows.

Real-time traffic statistics: With VANETs deployed, the vehicle-oriented surveys as supported by GPAS [148] can collect real-time traffic statistics of any given region as the valuable inputs to traffic engineering and traffic management.

Cost-effective traffic surveys: GPAS [148], [149] can support cost-effective traffic surveys about a certain region. The traffic survey results will be very helpful to the decision-makings in traffic engineering and traffic management.

Traffic information reporting and broadcast: By ensuring reliable and trustworthy multi-hop communications, LEAPER [142] provides reliable end-to-end connections between the local traffic authority and the nearby vehicles. Thus, LEAPER can be used by each vehicle to report important traffic incidents to the local traffic authority. Similarly, LEAPER can be used by the local traffic authority to disseminate traffic conditions, route recommendations, or weather information to the nearby vehicles.

Privacy-aware RSU deployment: In STCP2 [147] a privacy-aware RSU deployment algorithm is proposed to optimize the deployment of RSUs in VANETs, which can be adopted in traffic engineering. Besides, the privacy strength of each RSU can be estimated, which can be used to recommend travel routes to the drivers.

Traffic safety improvement: With RAMV [143], [144], the verification of beacons becomes scalable in VANETs, which makes traffic safety applications feasible.

On the other hand, several of our proposed schemes require precise traffic statistics of specific regions, which can only be provided by the traffic engineering staff. For instance, JPRA [146] and LEAPER [142] may benefit from the precise traffic statistics, such as vehicle's average speed and average vehicle density, to configure the system parameters. Thus, these information requirements can also help the traffic engineering staff improve traffic statistics collection.

7.1.7 A Baseline VANET Model

Overall, our proposed schemes complement the existing security and privacy schemes in literature to form a baseline VANET model as shown in Figure 7.4. This baseline VANET model represents the state-of-art of VANET research and development.

In this model DSRC [8] provides the necessary physical layer and MAC layer functionalities for wireless vehicular communications. WAVE [9] provides the necessary management and security functionalities. For brevity, in Figure 7.4 only the major security and privacy functionalities are depicted. Within WAVE, our security and privacy schemes provide the most comprehensive solutions to the corresponding functionalities.

Specifically, the baseline VANET model supports various traffic safety applications with scalable verification of beacons, as enabled by RAMV [143], [144]. With reliable and trustworthy multi-hop communications as enabled by LEAPER [142], this baseline

VANET model can support various traffic management applications and value-added applications such as traffic incident reporting, traffic condition broadcast, internet accessing, and so on. JPRA [146] protects the privacy of vehicular nodes when the PKI-like certificates are adopted in VANETs, while STCP2 [147] protects the privacy of vehicular nodes with short-time certificates. Besides, VAAD [150], GPAS [148], [149], and VehicleView [151], [152] all add to the set of promising value-added applications.

With the traffic safety applications satisfyingly supported with RAMV, this model is ready to be implemented, since the major motivation of VANETs is to enhance traffic safety. Meanwhile, the other applications may demand more support from the infrastructure domain of VANETs, which will be investigated in the future work. Thus, this baseline VANET model also provides a solid starting point for the future research work on VANETs.

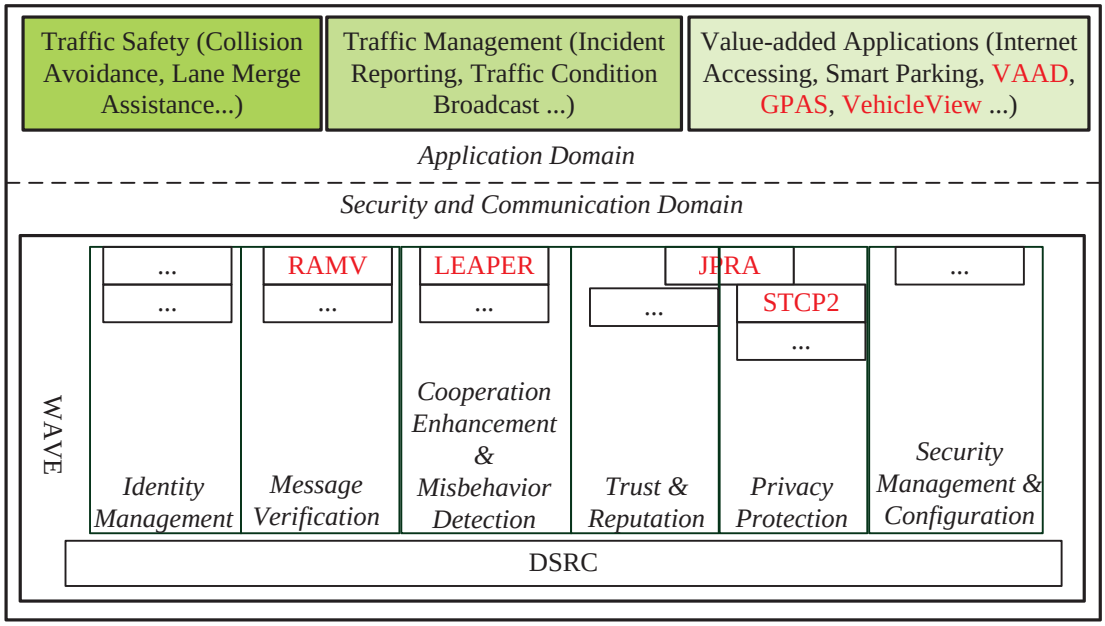

Figure 7.4 The baseline VANET model completed by our dissertation

7.2 Future Work

Using the baseline VANET model as a starting point, we identify several challenging research and development topics which are critical to ensure the secure and cost-effective implementation of intelligent VANETs. Based on our previous research work, the promising future work topics are identified to 1) enable the cost-effective implementation

of VANETs (see subsections 7.2.1 and 7.2.2), 2) realize the critical technical assumptions in the baseline VANET model (see subsections 7.2.3, 7.2.4, and 7.2.5), and 3) design more intelligent and advanced applications based on VANETs (see subsections 7.2.6, 7.2.7, and 7.2.8). With these topics thoroughly investigated in the future, the implementation of a secure, cost-effective and intelligent VANET will naturally follow.

Next, the motivations and challenges of each topic will be discussed in detail, and initial considerations on the possible solutions will also be provided.

7.2.1 Cost-Benefit Analysis of Security Provisioning

As discussed in our book chapter [5], any security scheme will incur a certain cost in terms of communication overhead, computation overhead, and so on. Thus, a thorough cost-benefit analysis of security provisioning is critical to cost-effectively implement VANETs. Such a cost-benefit analysis needs to answer several critical questions. What are the essential security requirements in any certain application scenario? What is the most cost-effective scheme to meet a given security requirement in a given application scenario? What is the best security implementation plan for VANETs?

However, considering the numerous applications and security schemes of VANETs, it is challenging to answer these questions. Up to now, no concrete cost-benefit analysis for VANET security provisioning has been presented in either industry or academia. The security architectures provided by the representative research projects, including Connected Vehicle [215], eSecurity Work Group [216], C2C Communication Consortium [217] and SeVeCom [20], only include all possible security requirements for VANETs without any consideration on these questions.

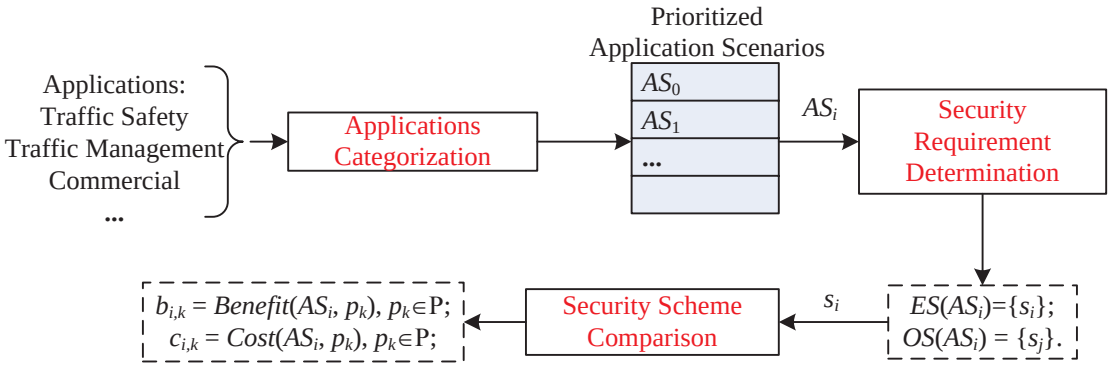

Figure 7.5 Steps for the cost-benefit analysis of security provisioning

Indeed, the Mobile Ad Hoc Network (MANET) community also lack a concrete cost-benefit analysis of security provisioning, though individual efforts on comparing different security schemes [218], modeling the possible attacks to intrusion detection systems [219], and modeling the cost and benefit of node cooperation [220], do exist. Besides, the cost and benefit of any security scheme in VANETs have different emphasis than those in MANETs. For instance, in VANETs network bandwidth and communication latency may be more relevant, while in MANETs the power consumption and computation overhead may be more relevant. Thus, the cost-benefit analysis of security provisioning in VANETs is a unique research topic which deserves systematic investigation.

To investigate this topic, a thorough understanding of the applications, security schemes, and their interactions in VANETs is needed. Besides, a methodology to categorize or partition the huge problem domain into manageable parts is also needed, which may be identified based on the inherent logical relations among the applications, security schemes and network components in VANETs. As a starting point, a feasible approach consisting of the necessary steps of *application categorization*, *security requirement determination*, and *security schemes comparison*, is shown in Figure 7.5.

Application Categorization and Prioritization: The available (or envisioned) VANET applications should be categorized according to their communication requirements, application significance, and economic potentials. The representative application scenarios, each of which may contain several applications, need to be identified and prioritized with different priorities. In Figure 7.5, AS_i, i=0, 1, …, indicates different application scenarios. Here, we assume that the priority of AS_i is higher than or equal to AS_{i+1}. In this process, collaboration between industry and academia is necessary to identify the applications and their distinguishing properties. The utility theory in economics may be a useful tool to evaluate the priority of each representative application scenario.

Security Requirement Determination: Given an application scenario AS_i, its relevant security requirements should be identified. To this end, a solid adversary model should be created for AS_i by considering the potential adversaries and their possible attacks. Game theory may be applied to model the interactions between the adversaries and the involved entities in AS_i, as in [219], [221]. The security requirements of AS_i could be divided into

two subsets: the essential security requirements ($ES(AS_i)$) and the optional security requirements ($OS(AS_i)$). $ES(AS_i)$ includes the security requirements which are critical to AS_i and will be probably breached by the possible attacks. $OS(AS_i)$ contains the security requirements which are either unimportant to AS_i or unlikely to be breached due to the incurred attacking cost. Here, we use s_i or s_j to indicate each concrete security requirement, for instance, message integrity.

Security Schemes Comparison: For each security requirement s_i, the available security schemes ($p_k \in \boldsymbol{P}$) should be compared in terms of cost and effect. Here, $\boldsymbol{P}$ is the set of all available security schemes in literature, and p_k is a concrete security scheme. Generally, the cost and benefit of p_k rely on the specific application scenario AS_i. Thus, a cost matrix $[c_{i,k}]$ and a benefit matrix $[b_{i,k}]$ can be derived for each security scheme p_k in each application scenario AS_i. In this process, the utility theory may also be used to combine various factors in the cost of p_k, including communication overhead and computation overhead, into a single metric. Similarly, a single benefit metric can also be created.

Eventually, based on the cost matrix $[c_{i,k}]$ and the benefit matrix $[b_{i,k}]$, combinatorial optimization may be performed to get the optimal security implementation plan in the form of $IMP = <imp_0, imp_1, \ldots>$. Here, imp_k indicates whether the security scheme p_k should be implemented in VANETs or not. During the optimization, the priority of the representative application scenarios could be treated as either absolute or relative. If the priority is regarded as absolute, *IMP* should optimize AS_0 in terms of cost and effect. With that, *IMP* can go on to optimize AS_1, AS_2, and so on. If the priority is relative, utility theory may also be applied to combine the cost and benefit of all application scenarios into a single utility metric, based on which *IMP* can be selected.

By performing a thorough cost-benefit analysis, an optimal security implementation plan *IMP* can be created. As a side product, various VANET applications will be categorized and prioritized based on practical considerations, which may be helpful to the application implementation. Besides, useful guidelines for the system design and security policy-making may also be derived. For instance, for each application scenario, the essential security requirements and optional security requirements should be differentiated in security scheme implementation. A security scheme for an essential

security requirement should be implemented and activated all the time. Comparatively, a security scheme for an optional security requirement may be implemented, but only activated when necessary, in order to be cost-effective.

In summary, a thorough cost-benefit analysis is meaningful for VANETs and should be performed in the future. Specifically, this research topic is relevant to various current research activities in the RITA project of Connected Vehicles [215], including the Vehicle to Vehicle Communications Systems Engineering direction and the Policy and Institutional Issues direction.

7.2.2 RSU-Assisted Secure and Scalable Communications

As discussed in Chapter 6 and GPAS [149], the wireless communications nearby each RSU could be crowded as shown in Figure 7.6. Within the communication range of one RSU, the nodes may periodically *broadcast* beacons and other application-specific messages. Each node may communicate with its neighbors via uni-cast, resulting in *V2V uni-cast communications*. Besides, each vehicle may communicate with the RSU to update its certificate, report events, or access the infrastructure, resulting in *V2R uni-cast communications*. In the current WAVE operation model, each vehicular node may be equipped with a single-channel radio or a multiple-channel radio [222]. With a single-channel radio, each node can only transmit and/or receive data on a single RF channel at any time. Even with a multiple-channel radio, each node can only transmit data on a single RF channel while receiving on at least one RF channel at the same time. Thus, no matter how the broadcasted messages and the uni-cast messages are divided into different channels, they will contend for the radio resource of the individual nodes. When the traffic density and the message exchanges increase, the network nearby the RSU may become saturated [223], which makes the RSU a bottleneck in VANETs.

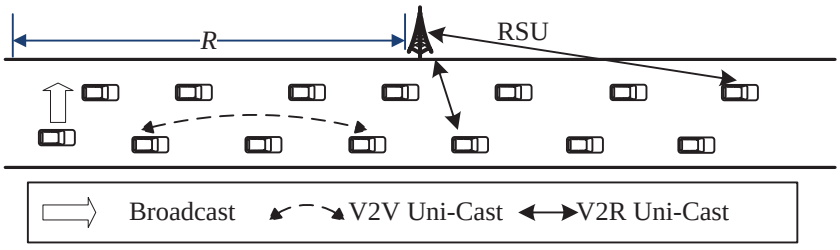

Figure 7.6 All possible wireless communications nearby an RSU

Thus, it is necessary to make the wireless communications nearby the RSU both secure and scalable. To this end, the available control channels (CCH) and service channels (SCH) of WAVE should be properly assigned to different messages from different nodes and the RSU. The nodes and the RSU should transmit or receive on the correct channel at the correct time. Thus, a challenging scheduling problem naturally arises. In this problem, the RSU may serve as a centralized scheduler for all the nodes within its communication range. Besides, each node has a limited communication time with the RSU due to its mobility, which is one important constraint on this problem. To ensure RSU-assisted secure and scalable communications, the above scheduling problem may be tackled with the following steps.

Communication Scheduling: With the broadcasted WAVE Service Announcements (WSAs) from the vehicular nodes, the RSU may obtain a full picture of the communication capability and requirement of each node, in terms of the pending messages, the message sizes, the deadline of each message, the destination of each message, the transceiver capability, and so on. Together with its own communication requirements, the RSU can schedule the communications of itself and the vehicular nodes for the next scheduling interval (T). In this process, the RSU needs to maximize the overall network throughput or the average throughput of all involved entities. The constraints to be considered may include the remaining communication time of each node, the communication capability of each node, and the possible interferences among the communications. The output will be an optimal radio resource accessing plan satisfying all constraints, or an indication of failure to find such a plan. Eventually, the plan can be broadcast to all vehicular nodes in the WSA of the RSU, or a dedicated control message for this end.

To formally model this scheduling problem, the above parameters need to be identified and the constraints need to be enriched based on the realistic VANET scenarios. Besides, the maximal network throughput of the VANETs nearby the RSU needs to be theoretically estimated based on the current node density and communication requirements of the nodes. If the overall communication requirements exceed the maximal network throughput, the RSU will refrain from scheduling the communications as discussed above, and try to perform a clustering of its neighbors instead.

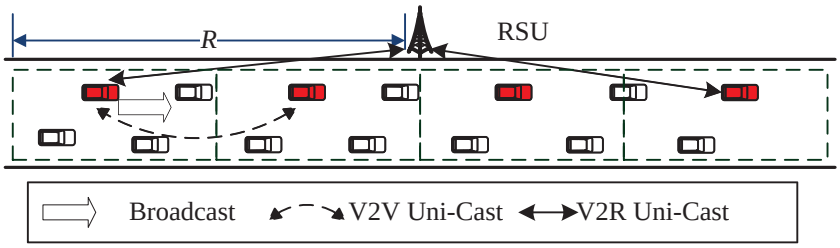

Figure 7.7 The clustering of vehicular nodes around an RSU

Adaptive Clustering: To further improve network throughput, one promising approach may be the clustering of the vehicular nodes as shown in Figure 7.7. As an example, four clusters with the shaded vehicles as the cluster heads are shown in Figure 7.7. The nodes within each cluster (cluster members) will reduce its transmission power to cover only this cluster, and each cluster head keeps its normal transmission range. Broadcasted messages of the cluster members will be aggregated at the cluster head, which will further broadcast the aggregated messages with its full transmission power to support traffic safety applications. Additionally, both V2V and V2R uni-cast communications will also be aggregated by the cluster head, which will further route the aggregated messages to the RSU or other cluster heads.

Based on current network conditions, the RSU needs to select the best clustering strategy in terms of reduced communication overhead and latency. The possible clustering strategies may include 1) forming clusters with a uniform road length, and 2) forming clusters with an equal number of nodes. The impacts of these clustering strategies need to be theoretically modeled and compared. In this process, existing transmission power control schemes [224]-[226] and clustering schemes [227]-[229] may provide useful hints.

Within each cluster, the cluster head needs to forward the broadcast and uni-cast messages of each cluster member. The timing of the forwarding actions of the cluster head needs to increase the efficiency of message aggregation, while still meeting the specific latency requirement of each message. Besides, the communications within each cluster still need to be synchronized to reduce the interference among the cluster members, which may follow a scheduling approach similar to the RSU-assisted scheduling problem, with the cluster head as the scheduler.

Eventually, the aggregation and forwarding actions of each cluster head need to be monitored by its cluster members. Proper countermeasures must be designed to handle the misbehaviors of either the cluster head or cluster members. Besides, data privacy needs to be ensured when the cluster head forwards sensitive messages for its members.

In summary, the RSU-assisted secure and scalable communication is a promising and challenging research topic which is meaningful to the implementation of VANETs.

7.2.3 Finance Infrastructure for VANETs

In VAAD [150], GPAS [148], [149], and VehicleView [151], [152], the financial transactions among the vehicular nodes and the infrastructure of VANETs need to be supported. For instance, in any value-added (commercial) applications the service consumers (say vehicular nodes) need to pay the service providers. Even in security provisioning, the vehicular nodes may need to pay the certificate authority to obtain new pseudonyms [127]. Thus, the financial transactions are prevalent in VANETs and should be supported with a finance infrastructure.

So far, the financial transactions in VANETs are supported in an ad-hoc manner. For instance, we propose a Clearance Center (CC) to function as a virtual bank for VAAD [150], GPAS [148], [149], and VehicleView [151], [152]. Many value-added applications simply assume the presence of a perfect finance infrastructure which could support all necessary financial transactions. Even the currency is represented in different ways in VANETs, including E-cash vouchers in VAAD [150], GPAS [148], [149], and VehicleView [151], [152], Nuglet in [82], and credits in [84]. Thus, to consistently and securely support the financial transactions in various VANET applications, a financial infrastructure will be desirable for VANETs.

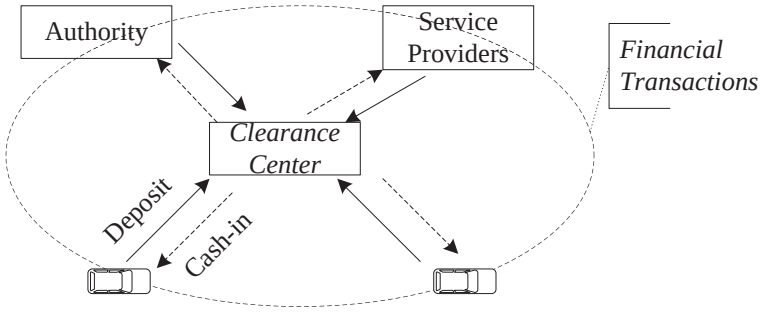

Figure 7.8 The overview of a finance infrastructure for VANETs

We propose a preliminary finance infrastructure for VANETs, as shown in Figure 7.8. The Clearance Center (CC) functions as the bank in VANETs, which will issue E-cash vouchers and support the clearance (cash-in) of E-cash vouchers. All entities in VANETs, including the Authority, the service providers, and vehicular nodes, can get E-cash vouchers by depositing a certain amount of money in CC. On the other hand, each entity can also get back its money by cashing in its E-cash vouchers. Basically, the financial transactions among these entities will be in the form of E-cash voucher exchanges. The advantage of an E-cash scheme [214] is that the voucher can be securely verified without revealing the identity of the voucher user, which is beneficial to the privacy protection in VANETs. In this finance infrastructure, several issues deserve further investigation.

Adopting an E-cash scheme: It is critical to adopt a proper E-cash scheme to VANETs based on the relevant considerations such as the E-cash voucher size, the computation overhead of voucher verification, the feasibility of divisible E-cash voucher, and so on. With an E-cash scheme adopted, it is necessary to allow each entity to securely deposit, store, exchange, and cash in E-cash vouchers, which may lead to many interesting questions. For instance, when should one node go to CC to change its E-cash vouchers with small amount to a whole E-cash voucher with a larger amount? How can each node minimize the division of its E-cash vouchers by scheduling the usage of its E-cash vouchers with different amounts? All these questions need to be answered in VANETs.

Policy making: Necessary policy should be made regarding the owner and operator of CC, which will involve the close coordination among traffic management authorities, car manufactures and drivers. Besides, a business model needs to be designed to differentiate the services to be charged and the free services. For instance, the road condition update service should be free to all VANET users to enhance road safety, while the commercial services should be provided to the vehicular nodes at a proper price. This business model will have a huge impact on the ecosystem of VANETs and should be carefully designed. Eventually, a pricing model should be designed to guide each service provider in charging its services, to reflect the communication and computation overhead. The administrators of VANETs may also adjust the pricing model to steer various applications (services) to properly share the network resource in VANETs.

Finance analytics: With this finance infrastructure, the financial statistics of each entity in VANETs may be analyzed to determine the economic potential of each application in VANETs, as well as to guide the design of new applications.

7.2.4 TPD for VANETs

In VANETs, a Tamper-Proof Device (TPD) is a critical component to many security and privacy schemes. A TPD is a secure hardware module which usually cannot be tampered or harmed by the external attacks. Seemingly, a TPD is a feasible approach to ensure trustworthy computing in each vehicular node. Thus, the TPD has been adopted in each vehicular node to securely store confidential private keys [230], [231], to trustworthily calculate the reputation of this node [82], [108], to perform digital signature generation and verification [35], [36], [231], or to manage the certificate [90], [91]. However, each scheme adopting a TPD usually only assumes a set of desirable functions for the TPD as suit itself. Indeed, if all such schemes have their ways, each vehicular node will be filled with tens of application-specific TPDs, which is not practical due to the cost and design implications incurred by so many TPDs.

Thus, due to the severe cost and application implications of TPDs, it is meaningful to systematically investigate the feasible application of TPDs to VANETs. In this regard, the following issues deserve further investigation.

A standard interface design for a certificate management TPD: As discussed in [35], [36], [231], one major motivation of adopting TPDs in vehicular nodes is to securely manage the certificates and associated private keys issued by the Authority. As various applications and security schemes have different requirements on certificate management, it is necessary to design a standard interface for the TPD in charge of certificate management in each node. Such an interface should meet the requirements of critical VANET applications on certificate management. For instance, it is commonly held that TPD should keep the privacy keys and secret keys intact and secret from all parties except for the VANET Authority. However, for privacy protection each node needs to change its pseudonym from time to time, and a pseudonym usually contains a specific certificate. In this case, it is challenging to define the proper level of control one node may exert over TPD. For instance, should each node be allowed to determine which

pseudonym to be used and when to be used? On one hand, each node may want to change its pseudonyms at will so that it can access multiple value-added applications with different pseudonyms. On the other hand, to prevent the Sybil attack it may be desirable to allow each node to use one pseudonym within a certain time period. Thus, it is critical to identify the important requirements of various applications on certificate management in VANETs, based on which a standard TPD for certificate management can be designed.

As an example, a preliminary interface design for TPD is given in Figure 7.9. This TPD consists of three major interfaces: *signature verification*, *signature generation* and *certificate management*. The Signature Verifier module will verify the digital signatures of the received packets, and return the verification results to the concerned applications. For any out-going data packet generated by this node, the Signature Generator module will attach its own timestamp (TSP) and generate a digital signature based on the current certificate in use. The novelty of this TPD lies in the Data Classifier module and the Certificate Manager module. The Data Classifier module will determine the application type of the out-going data packets, for instance, the beacons and other data packets. The Certificate Manager module will allow the node to explicitly select which pseudonym to be used at any time. However, the Certificate Manager will ensure that the certificate for beacons should not be changed with a frequency higher than a preset threshold, which can be configured by the VANET Authority to prevent Sybil attacks. In this way, both requirements from the general applications and beaconing can be supported by the TPD.

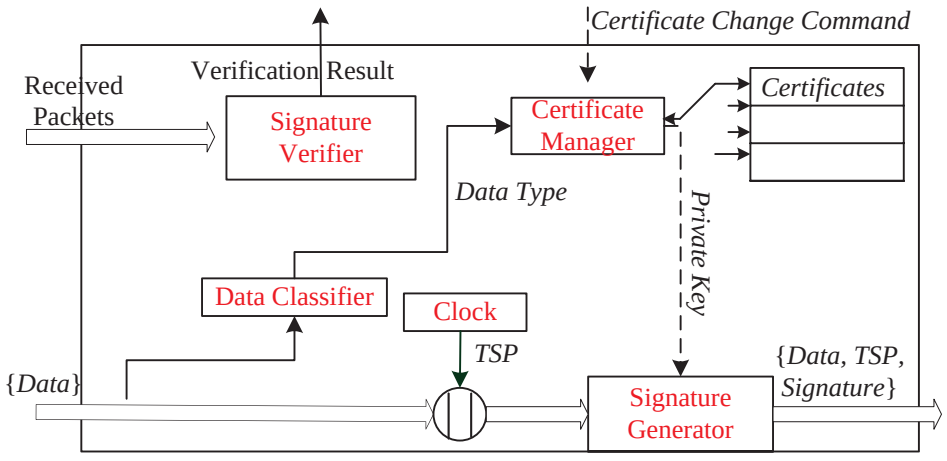

Figure 7.9 A preliminary functional interface of TPD in VANETs

An extensible TPD design for various applications: Besides certificate management, many applications, for instance, reputation management and event data recording, may also rely on a TPD to protect the specific algorithms. However, such schemes are application-specific and may require the TPD to protect different algorithms in various application scenarios. For instance, when a TPD is used to protect the reputation update of each node, many reputation update algorithms with different parameters may need to be implemented to support the aggregation of the reputation for different applications. Thus, for these security schemes relying on application-specific algorithms, multiple TPDs may be needed for different scenarios. However, it will not be cost-effective to replace the current TPD or to add a new TPD for any new application scenario.

Thus, it is meaningful to design an extensible TPD which can be cost-effectively updated for various application scenarios. On preliminary considerations, one possible approach could be to design a set of cryptographic primitives around a given hardware TPD to form an overall extensible TPD module. The wrapping cryptographic primitives will be implemented in software, which will be continuously audited by the hardware TPD to ensure that these primitives are not tampered with. Whenever a new application scenario is to be supported, the VANET Authority will instruct the TPD to register the authentication code of a new software module or update the authentication code of an existing software module.

The cost-benefit analysis of TPD: The application of a TPD will incur a certain cost to the vehicular node. Thus, it is necessary to perform a thorough cost-benefit analysis of the existing trust computing technologies [232] and identify the most cost-effective one for VANETs. With the cost of TPD determined as such, the newly proposed schemes will only make reasonable assumptions regarding the application of TPD to VANETs.

By investigating the above open issues, the usage of TPD in VANETs will become economically feasible. Besides, a set of critical requirements of TPD can be identified by the researchers in VANETs, which may serve as valuable inputs to the trust computing community for designing new TPD platforms. On the other hand, the VANET researchers will be encouraged to make reasonable assumptions of TPD in designing new applications and security schemes.

7.2.5 Ad Hoc RSU (adRSU) Design

In both GPAS [148], [149] and VehicleView [151], [152], ad hoc RSUs (adRSUs) are proposed as additional access points to such applications. An adRSU is a lightweight reprogrammable device which can be temporarily deployed to serve as an RSU. Especially in the initial stage of VANET deployment, adRSUs may be a valuable addition to the sparsely deployed RSUs to better support VANET applications.

Thus, it is meaningful to propose a secure and cost-effective design for adRSUs. Besides better supporting VANET applications, such a design of adRSUs will provide a reference to the design of RSUs. To this end, the following issues need to be addressed.

Requirement analysis: Besides GPAS and VehicleView, other value-added applications and traffic management applications may also benefit from adRSUs. For instance, an adRSU can be deployed at a road intersection to collect the real-time traffic volume data with V2R communications. Thus, it is necessary to identify the specific requirements of such applications, as necessary inputs to the design of adRSUs.

System design: Due to its nature and targeted applications, the adRSU must be secure, extensible and lightweight by design. An exemplary high-level adRSU design is shown in Figure 7.10. This adRSU supports two communication technologies, namely DSRC and cellular. The adRSU can communicate with vehicular nodes via DSRC, and it can communicate with the infrastructure entities via the cellular technology, for instance, 3G or 4G. The Communication Adaption Layer (CAL) provides efficient and reliable data transfer services to the upper layers by shielding the details of the communication technologies. CAL may schedule the data transfer activities of both DSRC and cellular interfaces to reduce the power consumption and bandwidth requirements of the adRSU.

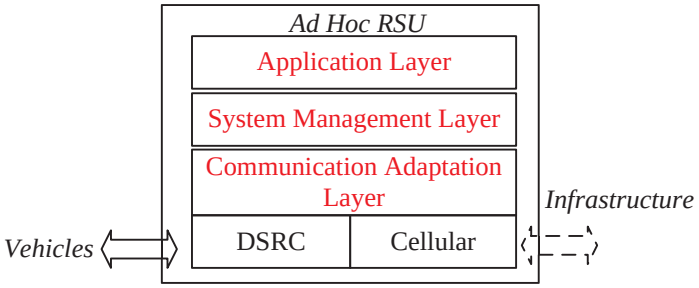

Figure 7.10 A feasible system design for an ad hoc RSU in VANETs

The System Management Layer (SML) maintains the security policies and security credentials of this adRSU. For instance, it may store the authorization from the VANET authority, with which to securely communicate with vehicular nodes. SML may continuously monitor the state of this adRSU, including its location, supported applications and so on, to detect any tampering and intrusion.

Above all, the Application Layer (AL) supports various value-added applications and traffic management applications. AL will be implemented as an open framework where applications can be flexibly added, deleted, activated or deactivated in runtime.

The above preliminary considerations serve as a starting point for the concrete design of adRSUs. More factors need to be considered in reality, especially with inputs from the requirement analysis. For instance, should solar panel, battery or power line be used to power the adRSU? If the power line is available in most road intersections, is it possible to use power line communication as the interface between the adRSU and the infrastructure of VANETs? All these questions need to be answered in the future.

Business model: The cost and benefit of adRSUs in VANETs need to be analyzed to determine the proper business model of adRSUs. It will be meaningful to determine how adRSUs will be deployed and maintained in VANETs, by the individual service providers or by the VANET Authority. To answer this question, the cost and benefit of adRSUs for each application, as well as the frequency of adRSU usage of each application, needs to be estimated.

The design of adRSUs will be relevant to the car manufacturers (e.g., GM, Ford and Chrysler), the network device manufacturers and the government transportation agencies (e.g., RITA [19] and NHTSA [233]). Especially, the design of adRSUs may incite and help the design of RSUs in VANETs. Thus, the design of adRSU needs to be performed with the cooperation from the above parties.

7.2.6 Data (Information) Management

In VANETs, each vehicular node is equipped with numerous sensors which can generate data about its environment. Besides, numerous applications in VANETs also provide each node with bountiful information. Thus, the numerous data (information) overwhelming each node call for the proper data (information) management in VANETs.

The design goals of data management in VANETs are two-fold: 1) to enable each node to timely and precisely present new knowledge of its environment to the drivers, probably through data mining, message aggregation, and knowledge representation; 2) to allow each node to efficiently and timely disseminate data to help other nodes in 1). Currently, research on data management in VANETs is still in its initial stage, as evidenced by the numerous call-for-papers posted each year.

To our best understanding, the data management in each vehicular node consists of a *context model*, a *message aggregator*, a *knowledge presente*r and a *message disseminator*, as shown in Figure 7.11. Here, the context model represents the context of this vehicle based on the sensor data generated by the on-board sensors and the received messages from its neighbors. The message aggregator evaluates the received messages based on the current context model, and aggregates them into a consistent input to the context model. The knowledge presenter will display the new knowledge to the user (driver or passenger) based on the current context of this node and the preferences of the user. The message disseminator will generate and send out messages to share knowledge with its neighbors.

Context Model: The *context* of a vehicular node may consist of its current driving state, its current geographic location, its environment and potentially the intentions of its driver. A comprehensive context model is critical for each node to perform context-aware actions. For instance, if a node is nearby a highway exit and it decelerates obviously, the context model may identify the driver's intention to take the exit and request the knowledge presenter to display the points of interests in the area this exit leads to.

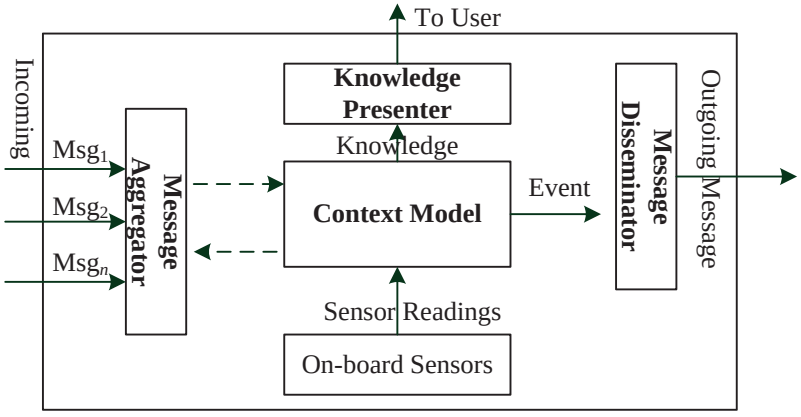

Figure 7.11 Critical components of data management in each vehicle

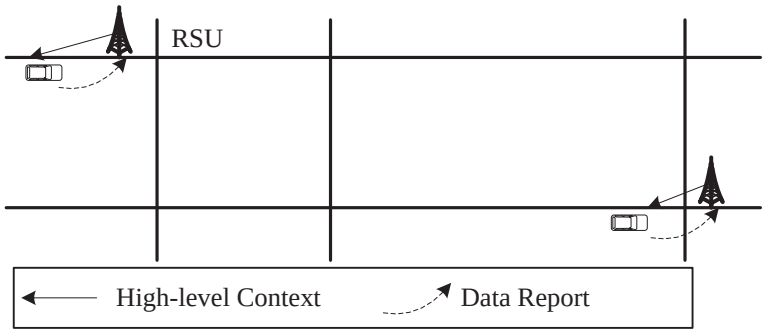

Figure 7.12 RSU-assisted high-level context update

The context model should consist of several sub-models for various applications and knowledge. Each sub-model may rely on data clustering, expert system, Bayesian networks or Markov chain to represent the knowledge of different types. The context model should also be able to figure out the typical actions (intentions) of the driver with pattern recognition techniques.

Besides, to enable each node to timely learn of the high-level knowledge of its neighborhood, an *RSU-assisted high-level context update* approach may be adopted in VANETs. As shown in Figure 7.12, each RSU will collect data reports from the passing-by nodes and form a high-level context about the concerned region. In areas without any RSU, the vehicles in a parking lot or a road intersection may cooperate to work as a hot spot for message aggregation [234]. This high-level context may contain the long-term statistics about the facilities within this region, which may not be accumulated by the passing-by vehicles. The RSU may periodically broadcast the high-level context to the nearby nodes, so that each node may complete its own context model with the received high-level context information. In this process, the collection of data reports, the format of the high-level context, and the dissemination of the high-level context all need to be further investigated.

Knowledge Presenter: The knowledge presenter needs to allow the user to configure his/her preference of the knowledge to be displayed. Besides, the information presented should not intrude on the user's attention or actions in driving. To design a proper knowledge presenter, the principles of user interface (UI) design may be considered.

Message Aggregator: The message aggregator may take as inputs not only the received messages but also the knowledge from the context model. Thus, a

comprehensive model is needed here to evaluate the trust of the received message against the context model, based on the message content, the physical model of VANETs, and potentially the trust of the data sources. Afterwards, the aggregated message could be used to update the context model. To this end, new metrics of knowledge quality and reliability may be proposed to guide the update of the context model.

Message Disseminator: The message disseminator needs to make intelligent and context-aware decision on when and what to disseminate. For instance, if one neighbor has already disseminated a message regarding an event, this node may not need to disseminate its own message regarding the same event to avoid duplicate messages. However, it is also critical to ensure the nodes in the zone-of-relevance (ZoR) of the concerned event will receive the message. To this end, a *context-aware mobility-assisted message dissemination algorithm* is proposed.

In this algorithm, the context-aware property lies in the message aggregation and separation actions of each node. Suppose one node *A* receives one message Msg1 regarding event 1 and one message Msg2 regarding event 2. Further suppose *A* is in the ZoR of both event 1 and event 2. Then, to be efficient, *A* may aggregate Msg1 and Msg2 into a single message Msg3 regarding both events. On the other hand, if another node *B* on the boundary of ZoR of event 1 receives Msg3, it may choose to separate Msg2 from Msg3 and only disseminate Msg2. Thus, by message aggregation and separation as required by the context, this algorithm can ensure efficient message dissemination. However, special security measures may be necessary to ensure trustworthy message aggregation and separation in this process.

To ensure that the message (Msg1) will cover the whole ZoR for all the valid duration T_V of the concerned event, each node with Msg1 may decide when to disseminate Msg1 based on the actions of its neighbors as well as the node mobility in the ZoR. Suppose that the node average speed in the ZoR is v, and node *A* has a distance d from the boundary of the ZoR. Let Δt indicate the lapsed time since *A* disseminates Msg1 or overhears Msg1 from its neighbors for the last time. Then, *A* will disseminate Msg1 when $\Delta t \times v \geq d$. That is, one node may have already approached *A* from outside the ZoR since the last dissemination of Msg1. If all nodes in the ZoR follow this approach, the message

dissemination in ZoR will be minimized while still ensuring that all nodes entering the ZoR will receive Msg1 in time.

7.2.7 Interactions with Emerging Technologies

To further exploit the application potentials of VANETs, it may be helpful to investigate VANETs in the context of several emerging technologies, such as cloud computing [235] and cyber-physical systems (CPS) [236]. New concepts in such technologies could help identify new features and potentials of VANETs, while the unique characteristics of VANETs may find their place in these new technologies.

7.2.7.1 VANETs and Cloud Computing

It will be rewarding to introduce the concept of cloud computing to VANETs. For instance, by implementing the infrastructure of VANETs with clouds, the cost of VANET deployment may be greatly reduced. Besides, as discussed in [237], in emergency scenarios, a public safety vehicle could use its neighbors in VANETs as its cloud, to perform certain computation extensive functions. Interesting research issues will arise in the interactions between VANETs and cloud, as discussed below.

Implementing the VANET infrastructure with a cloud (or clouds): Due to the popularity of cloud computing, in the future the infrastructure of VANETs may be implemented with a cloud or several clouds, as show in Figure 7.13. In this case, each RSU will serve as a gateway to several clouds, which may imply severe constraints on the design of the RSUs. Thus, it is meaningful to model and investigate the impact of clouds on the RSUs and the vehicular nodes. A novel design will be desirable to shield the implementation details of VANET infrastructure from the RSUs and the vehicular nodes. On the other hand, the critical security requirements of VANETs will also impact the design of the clouds in the VANET infrastructure.

Besides, to enable each vehicular node to access the services provided by the infrastructure clouds, it is necessary to enable each node to discover the nearest (or best) gateway and maintain a reliable communication connection with it. To this end, [238] proposes a gateway discovery protocol for each vehicular node to find the nearest gateway (RSU) in VANET cloud. However, in [238] the mobility of vehicular nodes or

the location information of the gateways is not considered. Indeed, a soft hand-over mechanism, similar to that in cellular communications, between two gateways may be proposed based on the mobility of each node as shown in Figure 7.13, so that each node may maintain an unbroken connection with the cloud. In this process, the potential network partitions in VANETs should be considered, and reliable multi-hop communications must be supported.

Implementing make-shift clouds with vehicular nodes: In emergency scenarios, the access to the VANET infrastructure may be lost. In this case, a public safety vehicle may benefit from a make-shift cloud formed by its nearby nodes. Similarly, in a parking lot the vehicular nodes may form a make-shift cloud by sparing their computation capabilities, which may be exploited by the vehicle in demand of high computation capabilities. Thus, in VANETs it is both necessary and feasible to allow the nearby nodes to form clouds providing valuable services. To this end, it is critical to identify the services or tasks which can be divided into smaller subtasks for each individual node. The security and trust issues must be resolved to ensure that each node will honestly perform its subtasks. Besides, the geographic boundary of such a cloud must be properly determined, in order to minimize the impact of the node mobility on the overall performance of the cloud. Eventually, a pricing and payment algorithm is necessary to reward the vehicles participating in the cloud according to their share of computation.

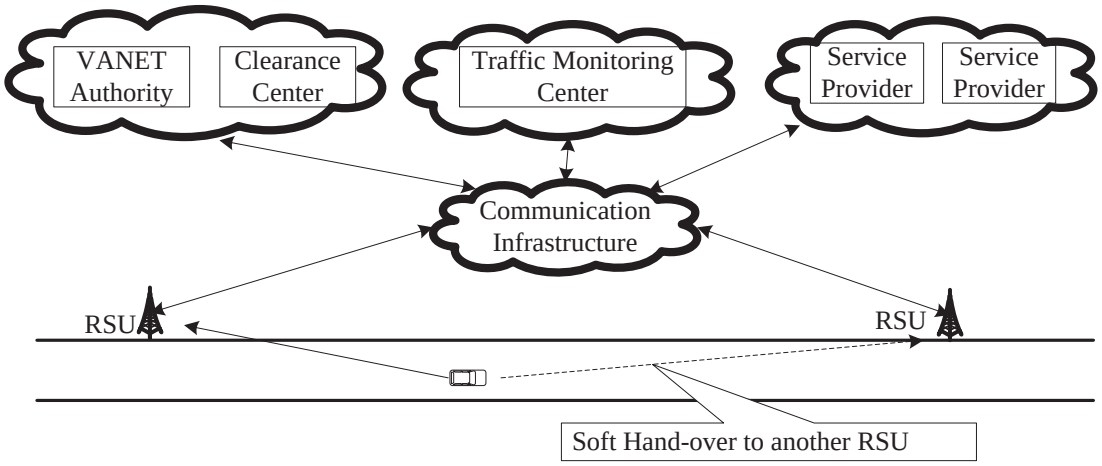

Figure 7.13 VANET infrastructure with clouds

7.2.7.2 VANETs and Cyber-Physical Systems

According to one program solicitation of the National Science Foundation (NSF), the term cyber-physical systems (CPS) [236] "refers to the tight conjoining of and coordination between computational and physical resources". Thus, with the close relation among the physical environment, the on-board sensors, the on-board computation unit, and the human driver, VANETs are a typical cyber-physical system. Thus, it will be beneficial to both the VANET research and the CPS research by investigating VANETs in the perspective of CPS. Specifically, the following directions may be followed.

To model and evaluate the coupling of computational and physical resources in VANETs: In VANETs, computational resources available to each node, such as network bandwidth and services, depend on the physical environment of this node. Specifically, network bandwidth available to one node depends on node density and node mobility of its neighborhood, as well as the network bandwidth requirements of its neighbors. The availability of services, especially the location-based services, obviously depends on the geographic location of this node, and the node density of its neighborhood. By modeling and evaluating the close coupling of the computational and physical resources, better estimation of one resource may be performed indirectly by estimating another type of resource which is easier to be estimated. In this way, adaptive service provisioning may become feasible based on the current available network resources or physical resources.

To consider the human factor in VANET research: So far, the focus of VANET research is usually on the computation part of vehicular nodes, and the human factor is usually omitted. However, the human driver (passenger) is the central entity in any decision-making or monitoring directly related to the physical world. Currently, researchers begin to investigate data fusion [236] and service scheduling [239] with considerations on the human factor. Besides, a specification logic for vehicular cyber-physical systems is also proposed in [240]. More serious research efforts should be put into this direction. For instance, Human-Machine Interface (HMI) design for on-board units should ensure effective information display to the human drivers (passengers), without causing distractions. Another potential research thrust may be to evaluate the feasibility of VANET applications based on their demands on human interactions.

To model and evaluate the impacts of VANETs on traffic safety and traffic management: So far, numerous traffic safety applications and traffic management applications have been proposed for VANETs. It will be meaningful to investigate the impacts of the cyber world on the physical world in VANETs, for instance, the impacts of security provisioning on traffic safety. In this process, the human decision making process needs to be modeled, in order to estimate the human reactions to various events reported by the on-board units. New theoretical tools and simulation tools may need to be designed to this end, which will serve to evaluate the effects of the proposed VANET applications and guide the future application implementation.

7.2.8 Applying VANETs to Traffic Engineering

As discussed throughout this dissertation, V2V and V2R communications in VANETs provide a cost-effective approach to collect real-time traffic data and to disseminate traffic control commands. Thus, it is meaningful to upgrade existing traffic engineering applications or design new ones based on VANETs. Specifically, the following traffic engineering applications may benefit from VANETs.

Traffic-adaptive green waves: In traffic engineering, a green wave refers to the coordinated control of consequential traffic lights in such a way that any vehicle with a normal speed will always run into green lights. Traditionally, the green waves are formed based on the traffic statistics accumulated over a long period, say 1 hour, so the green waves cannot adapt to the real-time traffic conditions in a timely manner. With VANETs, real-time traffic volumes and speeds in each direction of each road intersection can be obtained, which can be used to construct traffic-adaptive green waves in the neighborhood. Not only the green waves can be reconfigured with a higher frequency according to the traffic conditions, but also a green wave can be configured over a more complicated route than a long road segment, as shown in Figure 7.14.

In this process, the emerging dominant traffic flows within the neighborhood needs to be identified based on the real-time data statistics, which need to be collected with reliable V2V and V2R communications. Besides, various green waves need to be coordinated to achieve the best over-all traffic throughput in the concerned region. To tackle these issues, expertise from both VANETs and traffic engineering are needed.

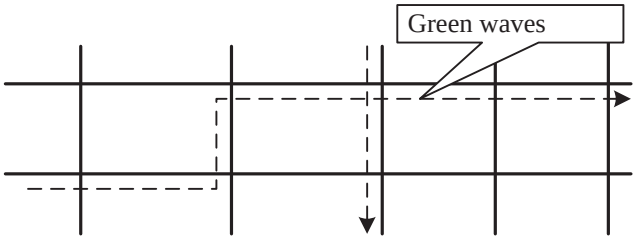

Figure 7.14 Exemplary green waves in a region

Localized traffic light control based on VANETs: As discussed in [13], [14], the localized traffic light control based on the traffic condition of each road intersection alone may be as effective as the traffic control based on global traffic information. With VANETs, it will be easy to implement the localized traffic light control algorithms based on the traffic conditions collected via V2R communications. The realistic performance of [13], [14] can be evaluated and compared to the traditional traffic control algorithms. Depending on the outcome of the realistic experiments, a totally new traffic control strategy may become applicable in traffic engineering. In general, this issue can be considered together with the research issues discussed in subsection 7.2.7.2.

Privacy and security-aware travel route selection: As discussed in Chapter 5, the presence of an RSU indicates an opportunity for any vehicular node to further enhance its privacy and security. Thus, with the deployed RSUs in a region, it is meaningful to enable each node to select its travel route based on not only the traditional metrics, for instance travel time and travel distance, but also the privacy and security strength provided by each alternative route. To this end, the security and privacy strength of each RSU should be quantitatively measured. An approach to equivalently compare the security and privacy strength to the traditional travel metrics should also be designed. In the end, an efficient algorithm is needed to select the best travel route out of numerous alternative ones. On the other hand, the study on privacy and security-aware route selection may provide useful guidelines on the deployment of RSUs in VANETs. For instance, if the RSUs can be deployed on the road intersections crossed by the most frequented travel routes in this region, the privacy and security strength of each travel route will be more likely to correspond to the traditional travel costs.

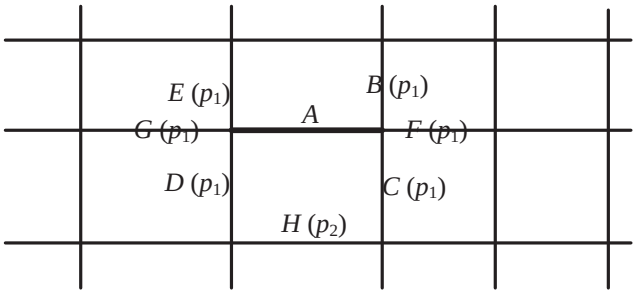

Figure 7.15 The interaction probabilities among road segments

Real-time traffic information dissemination: The real-time traffic information about one region needs to be timely disseminated to the vehicular nodes in this region, so that such nodes may make mobility decisions accordingly. However, it will be both redundant and unnecessary to disseminate the traffic information about any road segment to all the nodes within this region. As shown in Figure 7.15, the nodes in road segment *A* will be more interested in the traffic conditions of the road segments directly adjacent to *A*, namely, *B*, *C*, *D*, *E*, *F* and *G*. Comparatively, these nodes may only be interested in the less detailed traffic information on the road segment *H*, which is farther away from *A*.

To capture the different relations among different road segments, we could define an interaction probability p for any two road segments X and Y. This probability p will indicate the probability that one vehicle on X will go to Y following the shortest path, which indirectly indicates the impact of the traffic information of Y on the nodes on X. For simplicity, in Figure 7.15 a uniform p_1 indicates the interaction probability between two directly adjacent road segments, and a uniform p_2 indicates the interaction probability between two road segments which are connected by another road segment.

Once properly modeled and estimated, the interaction probability can be used to realize efficient traffic information dissemination and encoding in VANETs. Specifically, if the traffic information of each road segment will be independently disseminated, the dissemination probability of the traffic information can be reduced as the interaction probabilities decreases, forming a message gradient similar to that in VAAD [150]. In the case that the overall traffic information of all road segments will be encoded together and disseminated by the RSUs in this region, each RSU may encode the information differently based on its location regarding the road segments in this region. Following this line, more interesting results may be derived.

7.3 High-level Conclusions

As previously discussed, the application potential to improve traffic safety alone is more than enough to justify the cost incurred by the research, development and deployment of VANETs [208]. Thus, both traffic management applications and value-added applications can be regarded as *free-riders* of VANETs. Such applications can be more cost-effectively supported by VANETs with V2V and V2R communications. Thus, VANETs show great application and economic potentials.

This dissertation aims to fill the gap between the theoretic research and the practical implementation of VANETs, pushing VANETs nearer to the stage of massive deployment. Important security and privacy issues, each of which has great impacts on VANET applications, are identified and thoroughly addressed with novel schemes. Additionally, the value-added applications proposed for VANETs further enhance the application potentials of VANETs, making the future massive deployment of VANETs even more appealing. Thus, this dissertation makes the future implementation of VANETs feasible by supporting a baseline VANET model as discussed in section 7.1.7.

Besides, this dissertation also serves as a solid foundation for the future research and development of VANETs. The important open research and development topics discussed in section 7.2 indicate the promising research thrusts for VANETs. The initial considerations on these open issues will incite more novel and concrete solutions in the future research and development efforts.

References

[1] FARS. (2011, August 22). *Fatality Analysis Reporting System Data Table*. Available: http://www-fars.nhtsa.dot.gov/Main/index.aspx

[2] FHWA. (2011, Augest 22). *Focus on Congestion Relief*. Available: http://www.fhwa.dot.gov/congestion/

[3] RITA. (2011, August 22). *Intelligent Transportation Systems*. Available: http://www.its.dot.gov/

[4] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, pp. 49-55, May-Jun 2004.

[5] Z. Li, Z. Wang, and C. Chigan, "Security of vehicular ad hoc networks in intelligent transportation systems," in *Wireless Technologies in Intelligent Transportation Systems*, Y. Z. Ming-Tuo Zhou, Laurence T. Yang, Ed., ed: Nova Publishers, 2011, pp. 133-174.

[6] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, Virginia, USA, 2005.

[7] M. Gerla, B. Zhou, Y.-Z. Lee, F. Soldo, U. Lee, and G. Marfia, "Vehicular grid communications: the role of the internet infrastructure," in *2nd Annual International Workshop on Wireless Internet (WICON 2006)*, 2006, pp. 112-120.

[8] ETSI. (2011, August 22). *DSRC Introduction*. Available: http://www.etsi.org/WebSite/technologies/DSRC.aspx

[9] RITA. (2011, August 22). *ITS Standard Fact Sheets*. Available: http://www.standards.its.dot.gov/fact_sheet.asp?f=80

[10] C. V. S. C. Consortium, "Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by DSRC," National Highway Traffic Safety Administration, U.S. Department of Transportation DOT HS 809 859, March 2005.

[11] E. Shi, A. Perrig, and L. Van Doorn, "BIND: a fine-grained attestation service for secure distributed systems," in *Proc. 2005 IEEE Symposium on Security and Privacy* 2005, pp. 154-168.

[12] D. F. Llorca, M. A. Sotelo, S. Sanchez, M. Ocana, J. M. Rodriguez-Ascariz, and M. A. Garcia-Garrido, "Traffic data collection for floating car data enhancement in V2I networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, 2010.

[13] S. Lämmer and D. Helbing, "Self-control of traffic lights and vehicle flows in urban road networks," *Journal of Statistical mechanics: Theory and Experiment*, pp. 289--298, 2008.

[14] D. Helbing and A. Mazloumian, "Operation regimes and slower-is-faster effect in the controlof traffic intersections," *The European Physical Journal B - Condensed Matter and Complex Systems*, vol. 70, pp. 257-274, 2009.

[15] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. the 8th ACM international symposium on Mobile ad hoc networking and computing*, Montreal, Quebec, Canada, 2007, pp. 150-159.

[16] M. Boban and O. K. Tonguz, "Multiplayer games over vehicular ad hoc networks: A new application," *Ad Hoc Networks*, vol. 8, pp. 531-543, Jul 2010.

[17] FCC. (2004, January 9). *About DSRC*. Available: http://wireless.fcc.gov/services/index.htm?job=about&id=dedicated_src

[18] N. V. Coalition. (2011, August 22). *What is VII?* Available: http://www.vehicle-infrastructure.org/WhatsVII.htm

[19] RITA. (2011, August 22). *Connectivity-The Evolving Paradigm for IntelliDrive*. Available: Connectivity-The Evolving Paradigm for IntelliDrive

[20] SeVeCom. (2011, August 22). *Secure Vehicular Communication*. Available: http://www.sevecom.org/index.html

[21] CVIS. (2011, August 22). *Cooperative Vehicle Infrastructure System*. Available: http://www.cvisproject.org/

[22] AIDE. (2011, August 22). *Adaptive Integrated Driver-vehicle InterfacE*. Available: http://www.aide-eu.org/

[23] EVITA. (2011, August 22). *E-safety Vehicle Intrusion Protected Applications*. Available: http://www.evita-project.org/

[24] COOPERs. (2011, August 22). *Co-operative systems for intelligent road safety*. Available: Co-operative systems for intelligent road safety

[25] CALM. (2011, August 22). *Continuous Air Interface for Long and Medium Inteface* Available: http://calm.its-standards.info/

[26] J. ITS. (2008, August 22). *Cutting-edge ITS Tools & Information from Japan*. Available: http://www.hido.or.jp/itsos/

[27] C.-C. Hung, H. Chan, and E. H. K. Wu, "Mobility pattern aware routing for heterogeneous vehicular networks," in *Proc. IEEE Wireless Communications and Networking Conference*, 2008, pp. 2200-2205.

[28] J. Blum and A. Eskabdaruab, "The threat of intelligent collisions," *IT Professional*, vol. 6, pp. 24-29, Jan-Feb 2004.

[29] J. J. Blum, A. Eskandarian, and L. J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, pp. 347-351, Dec 2004.

[30] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Proc. European Wireless 2002 Conference*, 2002.

[31] L. B. T. Leinmueller, JP Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, E. Schoch, "SEVECOM - secure vehicle communication," in *Proc. 15th IST Mobile and Wireless Communication Summit*, Mykonos, Greece, 2006.

[32] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on Hot Topics in Networks (HOTNETS-IV)*, 2005.

[33] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proc. the First International Conference on Availability, Reliability and Security* 2006, p. 8 pp.

[34] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications Magazine*, vol. 16, pp. 16-22, 2009.

[35] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T. Ta-Vinh, G. Calandriello, A. Held, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, pp. 110-118, 2008.

[36] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, pp. 100-109, 2008.

[37] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Networks*, vol. 15, pp. 39-68, 2007.

[38] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications Magazine* vol. 13, pp. 8-15, 2006.

[39] P. Papadimitratos, ""On the Road"- Reflections on the security of Vehicular communication systems," in *Proc. IEEE International Conference on Vehicular Electronics and Safety* 2008, pp. 359-363.

[40] D. Chaum and E. V. Heyst, "Group signatures," in *Proc. 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, Brighton, UK, 1991, pp. 257-265.

[41] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2001)*, 2001.

[42] F. Li, M. Shirase, and T. Takagi, "Identity-based hybrid signcryption," in *Proc. International Conference on Availability, Reliability and Security*, 2009, pp. 534-539.

[43] R. Li, J. Yu, G. Li, and D. Li, "A new identity-based blind signature scheme with batch verifications," in *Proc. International Conference on Multimedia and Ubiquitous Engineering*, 2007, pp. 1051-1056.

[44] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *2007 Mobile Networking for Vehicular Environments*, 2007, pp. 103-108.

[45] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. The fourth ACM international workshop on Vehicular ad hoc networks*, Montreal, Quebec, Canada, 2007, pp. 19-28.

[46] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *The 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, Montreal, Quebec, Canada, 2005, pp. 79-87.

[47] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed-certificate-service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology* vol. 59, pp. 533-549, 2010.

[48] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology* vol. 58, pp. 5214-5224, 2009.

[49] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications* vol. 8, pp. 1974-1983, 2009.

[50] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *The fifth ACM international workshop on VehiculAr Inter-NETworking*, San Francisco, California, USA, 2008, pp. 86-87.

[51] W. Ren, K. Ren, W. Lou, and Y. Zhang, "Efficient user revocation for privacy-aware PKI," in *Proc. The 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, Hong Kong, 2008, pp. 1-7.

[52] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *The sixth ACM international workshop on VehiculAr InterNETworking*, Beijing, China, 2009, pp. 89-98.

[53] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "A secure and efficient revocation scheme for anonymous vehicular communications," in *Proc. 2010 IEEE International Conference on Communications (ICC)*, 2010, pp. 1-6.

[54] Y. Sun, R. Lu, X. Lin, J. Su, and X. Shen, "NEHCM: A novel and efficient hash-chain based certificate management scheme for vehicular communications," in *Proc. 5th International ICST Conference on Communications and Networking in China (CHINACOM)*, 2010, pp. 1-5.

[55] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Efficient certificate management in VANET," in *Proc. 2nd International Conference on Future Computer and Communication (ICFCC)* 2010, pp. V3-750-V3-754.

[56] J. J. Haas, H. Yih-Chun, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 595-604, 2011.

[57] B. Aslam and C. Zou, "Distributed certificate and application architecture for VANETs," in *Proc. The 28th IEEE conference on Military communications*, Boston, Massachusetts, USA, 2009, pp. 30-36.

[58] A. Wasef, Y. Jiang, and X. Shen, "ECMV: Efficient certificate management dcheme for behicular networks," in *Proc. IEEE Global Telecommunications Conference* 2008, pp. 1-5.

[59] L. Xiaodong, L. Rongxing, Z. Chenxi, Z. Haojin, H. Pin-Han, and S. Xuemin, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, pp. 88-95, 2008.

[60] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework For VANETs," in *the 3rd international workshop on Vehicular ad hoc networks*, Los Angeles, CA, USA, 2006, pp. 94-95.

[61] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proc. First International Conference on Communications and Networking in China*, 2006, pp. 1-8.

[62] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. Eighth International Symposium on Autonomous Decentralized Systems*, 2007, pp. 344-351.

[63] J. R. Douceur, "The sybil attack," in *The First International Workshop on Peer-to-Peer Systems*, 2002, pp. 251-260.

[64] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proc. the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, Los Angeles, CA, USA, 2006, pp. 1-8.

[65] W. Wang and A. Lu, "Visualization assisted detection of sybil attacks in wireless networks," in *Proc. The 3rd International Workshop on Visualization for Computer Security*, Alexandria, Virginia, USA, 2006, pp. 51-60.

[66] G. Y. Yan, G. Choudhary, M. C. Weigle, and S. Olariu, "Providing VANET security through active position detection," in *Proc. the fourth ACM international workshop on Vehicular ad hoc networks*, Montreal, Quebec, Canada, 2007, pp. 73-74.

[67] T. Leinmuller, C. Maihofer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," in *The 3rd international workshop on Vehicular ad hoc networks*, Los Angeles, CA, USA, 2006, pp. 57-66.

[68] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *The 1st ACM international workshop on Vehicular ad hoc networks*, Philadelphia, PA, USA, 2004, pp. 29-37.

[69] X. Lin, R. Lu, and X. Shen, "MDPA: multidimensional privacy-preserving aggregation scheme for wireless sensor networks," *Wireless Communications & Mobile Computing*, vol. 10, pp. 843-856, 2010.

[70] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications* vol. 7, pp. 4987-4998, 2008.

[71] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmuller, "Secure and efficient beaconing for vehicular networks," in *The fifth ACM international workshop on VehiculAr Inter-NETworking*, San Francisco, California, USA, 2008, pp. 82-83.

[72] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE International Conference on Communications* 2008, pp. 1451-1457.

[73] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3357-3368, 2008.

[74] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Leboudec, "Adaptive message authentication for vehicular networks," in *Proc. the sixth ACM international workshop on VehiculAr InterNETworking*, Beijing, China, 2009, pp. 121-122.

[75] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *The 3rd International Workshop on Vehicular Ad Hoc Networks*, Los Angeles, CA, USA, 2006, pp. 67-75.

[76] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proc. 4th Workshop on Vehicle to Vehicle Communications*, 2008.

[77] Z. Wang and C. Chigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs," in *Proc. IEEE International Conference on Communications*, 2007, pp. 3959-3964.

[78] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. The 6th Annual International Conference on Mobile Computing and Networking*, Boston, Massachusetts, United States, 2000, pp. 255-265.

[79] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. The 3rd ACM international symposium on Mobile ad hoc networking & computing*, Lausanne, Switzerland, 2002, pp. 226-236.

[80] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, 2002, pp. 107-121.

[81] V. Oberoi and C. Chigan, "A generic packet-dropping detection mechanism augmented with efficient power saving in ad hoc networks," in *Proc. SPIE Symposium on Defense and Security*, 2006.

[82] L.Buttyan and J. P. Hubaux, "Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Swiss Federal Institute of Technology DSC/2001/001, 2001.

[83] K. Chen and K. Nahrstedt, "iPass: an incentive compatible auction scheme to enable packet forwarding service in MANET," in *Proc. 24th International Conference on Distributed Computing Systems* 2004, pp. 534-542.

[84] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. IEEE INFOCOM*, 2003, pp. 1987-1997 vol.3.

[85] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford University arXiv:cs/0307012v2, May 2003.

[86] F. Dotzer, L. Fischer, and P. Magiera, "VARS: a vehicle ad-hoc network reputation system," in *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 2005, pp. 454-456.

[87] S. Moloney and P. Ginzboorg, "Security for interactions in pervasive networks: applicability of recommendation systems," in *Security in Ad-hoc and Sensor Networks*. vol. 3313, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, Eds., ed: Springer Berlin / Heidelberg, 2005, pp. 95-106.

[88] S. Fahnrich and P. Obreiter, "The buddy system - a distributed reputation system based on social structure," Universit¨at Karlsruhe, Faculty of Informatics Technical Report 2004-1, 2004.

[89] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in *Proc. the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, Tenerife, Canary Islands, Spain, 2009, pp. 106-115.

[90] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications* vol. 25, pp. 1557-1568, 2007.

[91] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J. P. Hubaux, "Fast exclusion of errant devices from vehicular networks," in *Proc. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2008, pp. 135-143.

[92] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The role of trust management in distributed systems security," in *Secure Internet programming*, V. Jan and D. J. Christian, Eds., ed: Springer-Verlag, 1999, pp. 185-210.

[93] 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 *Proc. IEEE INFOCOM*, 2006, pp. 1-13.

[94] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "Attacks on trust evaluation in distributed networks," in *Proc. 40th Annual Conference on Information Sciences and Systems*, 2006, pp. 1461-1466.

[95] Y. L. Sun, Y. Wei, H. Zhu, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications* vol. 24, pp. 305-317, 2006.

[96] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. the 3rd ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, USA, 2005, pp. 1-10.

[97] C. T. Nguyen, O. Camp, and S. Loiseau, "A Bayesian network based trust model for improving collaboration in mobile ad hoc networks," in *Proc. 2007 IEEE International Conference on Research, Innovation and Vision for the Future*, 2007, pp. 144-151.

[98] R. Li, J. Li, P. Liu, and H.-H. Chen, "An objective trust management framework for mobile ad hoc networks," in *Proc. IEEE 65th Vehicular Technology Conference*, 2007, pp. 56-60.

[99] S. Yan, Y. Wei, H. Zhu, and K. J. R. Liu, "Trust modeling and evaluation in ad hoc networks," in *Proc. IEEE Global Telecommunications Conference*, 2005, p. 6 pp.

[100] H. Zhu, F. Bao, and R. H. Deng, "Computing of trust in wireless networks," in *Proc. IEEE 60th Vehicular Technology Conference*, 2004, pp. 2621-2624 Vol. 4.

[101] H. Zhu and F. Bao, "Quantifying trust metrics of recommendation systems in ad-hoc networks," in *Proc. IEEE Wireless Communications and Networking Conference*, 2007, pp. 2904-2908.

[102] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 318-328, 2006.

[103] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *Acm Computing Surveys*, vol. 42, Dec 2009.

[104] E. Staab and T. Engel, "Tuning evidence-based trust models," in *Proc. International Conference on Computational Science and Engineering*, 2009, pp. 92-99.

[105] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, 2006, pp. 1-8.

[106] M. Gerlach, "Trust for vehicular applications," in *Proc. Eighth International Symposium on Autonomous Decentralized Systems*, 2007, pp. 295-304.

[107] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, 2008, pp. 1238-1246.

[108] B. Liu, Y. Zhong, and S. Zhang, "Probabilistic isolation of malicious vehicles in pseudonym changing VANETs," in *Proc. 7th IEEE International Conference on Computer and Information Technology*, 2007, pp. 967-972.

[109] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Proc. the 2009 International Conference on Computational Science and Engineering* 2009, pp. 139-145.

[110] J. Chen and J. Wu, "Cooperative anonymity authentication in Vehicular Networks," in *Proc. IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, 2009, pp. 1018-1023.

[111] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology* vol. 56, pp. 3442-3456, 2007.

[112] F. D¨otzer, "Privacy issues in vehicular ad hoc networks," in *Workshop on Privacy Enhancing Technologies*, Cavtat, Croatia, 2005.

[113] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice," in *Proc. IEEE Wireless Communications and Networking Conference*, 2007, pp. 3400-3405.

[114] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems," in *Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[115] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," in *Proc. 2007 ITG-GI Conference on Communication in Distributed Systems (KiVS)* 2007, pp. 1-12.

[116] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. 2005 IEEE Wireless Communications and Networking Conference*, 2005, pp. 1187-1192 Vol. 2.

[117] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in *The 5th ACM workshop on Privacy in Electronic Society*, Alexandria, Virginia, USA, 2006, pp. 19-28.

[118] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in *Proc. IEEE 65th Vehicular Technology Conference*, 2007, pp. 2521-2525.

[119] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 1569-1589, 2007.

[120] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. 2011 IEEE International Conference on Communications (ICC)* 2011, pp. 1-5.

[121] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in *Proc. 2009 IEEE Vehicular Networking Conference (VNC)* 2009, pp. 1-8.

[122] B. K. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in VANETS," in *Proc. IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1633-1637.

[123] R. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: providing location privacy for VANET," in *Proc. 3rd workshop on Embedded Security in Cars (ESCAR)*, Cologne, Germany, 2005.

[124] A. Wasef and X. Shen, "REP: Location privacy for VANETs using random encryption periods," *Mobile Networks and Applications*, vol. 15, pp. 172-185, 2010.

[125] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *2007 IEEE Intelligent Vehicles Symposium* 2007, pp. 541-546.

[126] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *Proc. The16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2009, pp. 324-337.

[127] J. Freudiger, M. Manshaei, J. Y. L. Boudec, and J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in *Proc. IEEE Infocom*, 2010.

[128] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones," in *The 9th International Symposium on Privacy Enhancing Technologies*, Seattle, WA, 2009, pp. 216-234.

[129] J. Freudiger, Raya, M., Felegyhazi, M., Papadimitratos, P., Hubaux, J.-P., "Mix zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007.

[130] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, pp. 46-55, 2003.

[131] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004, p. 127.

[132] Q. Yang, A. Lim, X. Ruan, and X. Qin, "Location privacy protection in contention based forwarding for VANETs," in *Proc. 2010 IEEE Global Telecommunications Conference* 2010, pp. 1-5.

[133] Y.-C. Wei, Y.-M. Chen, and H.-L. Shan, "RSSI-based user centric anonymization for location privacy in vehicular networks," in *Security in Emerging Wireless Communication and Networking Systems*. vol. 42, Q. Gu, W. Zang, and M. Yu, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 39-51.

[134] R. Hussain, S. Kim, and H. Oh, "Towards privacy aware pseudonymless strategy for avoiding profile generation in VANET," in *Information Security Applications*, Y. Heung Youl and Y. Moti, Eds., ed: Springer-Verlag, 2009, pp. 268-280.

[135] P. Papadimitratos, G. Calandriello, J. P. Hubaux, and A. Lioy, "Impact of vehicular communications security on transportation safety," in *IEEE INFOCOM Workshops*, 2008, pp. 1-6.

[136] A. Festag, P. Papadimitratos, and T. Tielert, "Design and performance of secure geocast for vehicular communication," *IEEE Transactions on Vehicular Technology* vol. 59, pp. 2456-2471, 2010.

[137] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE Transactions on Dependable and Secure Computing* vol. 8, p. 15, 2010.

[138] B. McKeever and P. Pisano, "Clarus: A clear picture," *Thinking Highways (North American Edition)*, vol. 4, Nov/Dec 2009.

[139] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. IEEE INFOCOM*, 2009, pp. 1413-1421.

[140] S. Olariu, "Peer-to-peer multimedia content provisioning for vehicular ad hoc networks," in *The 3rd ACM workshop on Wireless multimedia networking and performance modeling*, Chania, Crete Island, Greece, 2007, pp. 1-1.

[141] R. C. Hsu, H.-E. Lin, and A. Wang, "Mmb:: a mobile music blogger system for inter-vehicle entertainment," in *The 3rd ACM workshop on Wireless multimedia networking and performance modeling*, Chania, Crete Island, Greece, 2007, pp. 35-38.

[142] Z. Li and C. Chigan, "LEAPER: A lightweight reliable and faithful data packet relaying framework for VANETs," *Ad Hoc Networks,* vol. 9, pp. 418-429, 2011.

[143] Z. Li and C. Chigan, "On resource-aware message verification in VANETs," in *Proc. 2010 IEEE International Conference on Communications (ICC)* 2010, pp. 1-6.

[144] Z. Li and C. Chigan, "RAMV: ensuring resource-aware message verification in VANETs," *Security and Communication Networks,* vol. 4, pp. 771-784, Jul 2011.

[145] Z. Li and C. Chigan, "Joint Privacy and Reputation Assurance for VANETs," in *Proc. IEEE International Conference on Communications (ICC),* Ottawa, Canada, 2012.

[146] Z. Li and C. Chigan, "On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc Networks ", Submitted to IEEE Transactions on Mobile Computing, 2012.

[147] Z. Li and C. Chigan, "On Privacy Protection with Short-Time Certificates in Vehicular Ad Hoc Networks," Submitted to IEEE Transactions on Vehicular Technology, 2012.

[148] Z. Li, C. Liu, and C. Chigan, "GPAS: A general-purpose automatic survey system based on vehicular ad hoc networks," *IEEE Wireless Communication Magazine,* vol. 18, August 2011.

[149] Z. Li, C. Liu, and C. Chigan, "GPAS: a secure and cost-effective solution to location-sensitive surveys in VANETs," Submitted to IEEE Journal of Selected Areas in Communications, 2012.

[150] Z. Li, C. Liu, and C. Chigan, "On secure VANET-based ad dissemination with pragmatic cost and effect control," Submitted to IEEE Transactions on Intelligent Transportation Systems, 2011.

[151] Z. Li, C. Liu, and C. Chigan, "VehicleView: A Universal System for Vehicle Performance Monitoring and Analysis based on VANETs," *IEEE Wireless Communications,* 2012.

[152] C. Liu, Z. Li, and C. Chigan, "On secure and cost-effective vehicular data collection based on VANETs," Submitted to IEEE Journal of Selected Areas in Communications, 2012.

[153] R. Kroh, A. Kung, and F. Kargl, "VANETS security requirements final version," Sevecom D1.1, November 21 2006.

[154] C. E. Perkins, E. M. Royer, and S. R. Das. (2001, September 06, 2011). IP flooding in ad hoc mobile networks. [IETF Draft]. Available: http://www.cs.ucsb.edu/~ebelding/txt/bc.txt

[155] Z. Li, C. Chigan, and D. Wong, "AWF-NA: A complete solution for tampered packet detection in VANETs," in *Proc. IEEE Global Communications Conference*, 2008, pp. 1-6.

[156] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. The 6th Annual International Conference on Mobile Computing and Networking*, Boston, Massachusetts, United States, 2000, pp. 243-254.

[157] G. G. Finn, "Routing and addressing problems in large metropolitan-scale internetworks," University of Southern California Tech. Rep. ISI/RR-87-180, 1987.

[158] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," IETF IETF RFC 4728, 2007.

[159] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *The Second IEEE Workshop on Mobile Computer Systems and Applications*, 1999, p. 90.

[160] H. Füßler, H. Hartenstein, J. Widmer, M. Mauve, and W. Effelsberg, "Contention-based forwarding for mobile ad-hoc networks," *Ad Hoc Networks*, vol. 1, 2003.

[161] H. Füßler, H. Hartenstein, J. Widmer, M. Mauve, and W. Effelsberg, "Contention-based forwarding for street scenarios," in *1st International Workshop on Intelligent Transportation*, 2004.

[162] M. Abuelela, S. Olariu, and I. Stojmenovic, "OPERA: Opportunistic packet relaying in disconnected vehicular ad hoc networks," in *Proc. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2008, pp. 285-294.

[163] H. Jiang, H. Guo, and L. Chen, "Reliable and efficient alarm message routing in VANET," in *Proc. 28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 186-191.

[164] C. Chigan, V. Oberoi, and J. Li, "RPB-MACn: A relative position based collision-free MAC nucleus for vehicular ad hoc networks," in *Proc. IEEE Global Telecommunications Conference*, 2006, pp. 1-6.

[165] A. Shamir, "Identity-based cryptosystems and signature schemes," presented at the Proc. CRYPTO 84 on Advances in Cryptology, Santa Barbara, California, United States, 1985.

[166] C. Liu and C. Chigan, "RPB-MD: A novel robust message dissemination method for VANETs," in *Proc. IEEE GLOBECOM*, 2008, pp. 1-6.

[167] N. Yang, R. Sankar, and J. Lee, "Improving ad hoc network performance using cross-layer information," in *Proc. 2005 IEEE International Conference on Communications*, 2005, pp. 2764-2768 Vol. 4.

[168] NIST, "Secure hash standard (SHS)," FIPS PUB 180-3, October 2008.

[169] ISI. (2011, September 02). *The Network Simulator - ns-2*. Available: http://www.isi.edu/nsnam/ns/index.html

[170] K. Lan. (2007, Feb. 13). *Rapid generation of realistic simulation for VANET*. Available: http://lens1.csie.ncku.edu.tw/MOVE/index.htm

[171] Cryptopp. (2011, September). *Crypto++ 5.6.0 Benchmarks*. Available: http://www.cryptopp.com/benchmarks.html

[172] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. the Conference on Communications Architectures, Protocols and Applications*, London, United Kingdom, 1994, pp. 234-244.

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

[174] M. Grossglauser and M. Vetterli, "Locating nodes with EASE: last encounter routing in ad hoc networks through mobility diffusion," in *Proc. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, pp. 1954-1964 vol.3.

[175] K. Jeffay and S. Goddard, "Rate-based resource allocation models for embedded systems," in *the First International Workshop on Embedded Software*, 2001, pp. 204-222.

[176] M. B. Jones, D. Rosu, and M.-C. Rosu, "CPU reservations and time constraints: efficient, predictable scheduling of independent activities," in *Proc. the 16th ACM Symposium on Operating Systems Principles*, Saint Malo, France, 1997, pp. 198-211.

[177] C. L. Liu and J. W. Layland, "Scheduling algorithms for multiprogramming in a hard-real-time environment," *Journal of the ACM*, vol. 20, pp. 46-61, 1973.

[178] J. A. Stankovic and R. Rajkumar, "Real-time operating systems," *Real-Time Systems*, vol. 28, pp. 237-253, 2004.

[179] EASIS, "Requirements specification WP1 software architecture," EASIS Deliverable D1.1 v3.01 2006, 2006.

[180] AUTOSAR, "General requirements on basic software modules," AUTOSAR Deliverables v2.2.2 R3.1, 2008.

[181] ANSI, "Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm," ANSI X9.62-1998, 1999.

[182] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[183] MAXIM, "Using the elliptic curve digital signature algorithm (ECDSA) with the MAXQ1103's Modular Arithmetic Accelerator (MAA)," MAXIM Application Note 4016, 2009.

[184] V. Gupta, S. Gupta, S. Chang, and D. Stebila, "Performance analysis of elliptic curve cryptography for SSL," in *The 1st ACM workshop on Wireless security*, Atlanta, GA, USA, 2002, pp. 87-94.

[185] K. Komathy and P. Narayanasamy, "Strengthening ECDSA verification algorithm to be more suitable to mobile networks," in *Proc. International Multi-Conference on Computing in the Global Information Technology*, 2006, pp. 61-61.

[186] W.-b. Rao and Q. Gan, "The performance analysis of two digital signature schemes based on secure charging protocol," in *Proc. 2005 International Conference on Wireless Communications, Networking and Mobile Computing*, 2005, pp. 1180-1182.

[187] B. Bellur and A. Varghese. (2008, TESLA authentication and digital signatures for v2x messages. Available: www.ip.com

[188] K. Labertaux and Y. Hu, "Strong VANET security on a budget," in *Proc. ESCAR 2006*, Berlin, 2006.

[189] H. Krishnan. (2008, Verify-on-demand – a practical and scalable approach for broadcast authentication in vehicle safety communication. Available: www.ip.com

[190] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An dfficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. the 27th IEEE Conference on Computer Communications*, 2008, pp. 246-250.

[191] Y. Jiang, M. Shi, X. Shen, and C. Lin, "A tree-based signature scheme for VANETs," in *Proc. IEEE Global Telecommunications Conference*, 2008, pp. 1-5.

[192] T. Kosch, C. J. Adler, S. Eichler, C. Schroth, and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *IEEE Wireless Communications Magazine* vol. 13, pp. 22-28, 2006.

[193] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, pp. 422-426, 1970.

[194] S. Andrews and M. Cops, "Final report: vehicle infrastructure integration proof of concept results and findings summary – vehicle," FHWA-JPO-09-043, May 2009.

[195] M. Abe and E. Fujisaki, "How to date blind signatures," in *Proc. The International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*, 1996, pp. 244-251.

[196] F. Li and J. Wu, "Mobility reduces uncertainty in MANETs," in *Proc. 26th IEEE International Conference on Computer Communications.*, 2007, pp. 1946-1954.

[197] A. Lee-Thorp, "Attestation in trusted computing: Challenges and potential solutions," RHUL-MA-2010-09, March 2010.

[198] A. M. Mathai, *An introduction to geometrical probability : distributional aspects with applications*, 1st ed. Amsterdam: CRC Press, 1999.

[199] Y. Xi, W. Shi, and L. Schwiebert, "Mobile anonymity of dynamic groups in vehicular networks," *Security and Communication Networks*, vol. 1, p. 13, 2008.

[200] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," in *Proc. 2010 IEEE Global Telecommunications Conference*, 2010, pp. 1-5.

[201] IEEE, "IEEE 1609.2: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," ed: IEEE, 2006.

[202] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short-time certificate updating in VANETs," in *Proc. 2010 IEEE International Conference on Communications (ICC)*, 2010, pp. 1-5.

[203] L. Jacobson, "VII privacy policies framework, version 1.0.2," NATIONAL VII COALITIONFEBRUARY 16 2007.

[204] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in *Proc. the 16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2009, pp. 348-357.

[205] C. A. R. Hoare, "Quicksort," *The Computer Journal*, vol. 5, pp. 10-16, January 1, 1962 1962.

[206] R. W. Floyd, "Algorithm 97: Shortest path," *Communications of the ACM*, vol. 5, 1962.

[207] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM 2008* 2008, pp. 1229-1237.

[208] S. Peirce and R. Mauri, "Vehicle-Infrastructure Integration (VII) initiative benefit-cost analysis: Pre-testing estimates," Washington, DC US DoT Draft Report, 2007.

[209] M. Schonlau, R. D. Fricker, and M. N. Elliott, *Conducting research surveys via e-mail and the web*. Santa Monica, CA: Rand Publishing, 2001.

[210] GM. (2011). *OnStar*. Available: http://www.onstar.com/web/portal/home

[211] Ford. (2011, October). *Ford Sync*. Available: http://www.ford.com/technology/sync/

[212] J. Baugh and J. Guo, "Location privacy in mobile computing environments," in *Ubiquitous Intelligence and Computing*. vol. 4159, J. Ma, H. Jin, L. Yang, and J. Tsai, Eds., ed: Springer Berlin / Heidelberg, 2006, pp. 936-945.

[213] G. Fairhurst and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)," IETF RFC 3366, 2002.

[214] D. Chaum, "Blind signatures for untraceable payments," in *Proc. International Crytology Conference*, 1982, pp. 199-203.

[215] RITA. (2011, November 9). *Connected Vehicle Research*. Available: http://www.its.dot.gov/connected_vehicle/connected_vehicle_policy.htm

[216] eSafetySupport. (2011, November). *eSecurity Work Group*. Available: http://www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity.htm

[217] C2C-CC. (2011, November 9). *Car to Car Communication Consortium*. Available: http://www.car-to-car.org/

[218] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electronic Notes in Theoretical Computer Science (ENTCS)*, vol. 197, pp. 131-140, 2008.

[219] E. A. Panaousis and C. Politis, "Non-cooperative games between legitimate nodes and malicious coalitions in MANETs," in *Proc. the Future Network and Mobile Summit*, Warsaw, Poland, 2011.

[220] G. Brahim, A. Al-Fuqaha, M. Guizani, and B. Khan, "A model for cooperative mobility and budgeted QoS in MANETs with heterogenous autonomy requirements," in *Proc. 2008 IEEE Global Telecommunications Conference*, 2008.

[221] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Transactions on Information and System Security,* vol. 8, pp. 78-118, 2005.

[222] Y. L. Morgan, "Managing DSRC and WAVE Standards Operations in a V2V Scenario," *International Journal of Vehicular Technology,* vol. 2010, 2010.

[223] J. Li and C. Chigan, "Delay-aware transmission range control for VANETs," in *Proc. IEEE GLOBECOM 2010*, 2010, pp. 1-6.

[224] C. Chunxiao and L. Jialiang, "A delay-bounded dynamic interactive power control algorithm for VANETs," in *Proc. IEEE International Conference on Communications, 2007.*, 2007, pp. 5849-5855.

[225] C. Lin and R. Shakya, "VANET adaptive power control from realistic propagation and traffic modeling," in *2010 IEEE Radio and Wireless Symposium (RWS)* 2010, pp. 665-668.

[226] J. Mittag, F. Schmidt-Eisenlohr, M. Killat, J. Harri, and H. Hartenstein, "Analysis and design of effective and low-overhead transmission power control for VANETs," in *The fifth ACM international workshop on VehiculAr Inter-NETworking*, San Francisco, California, USA, 2008, pp. 39-48.

[227] C. Shea, B. Hassanabadi, and S. Valaee, "Mobility-based clustering in VANETs using affinity propagation," in *Proc. IEEE Global Telecommunications Conference*, 2009, pp. 1-6.

[228] P. Fan, J. Haran, J. Dillenburg, and P. Nelson, "Cluster-based framework in vehicular ad-hoc networks," in *Ad-Hoc, Mobile, and Wireless Networks*. vol. 3738, V. Syrotiuk and E. Chávez, Eds., ed: Springer Berlin / Heidelberg, 2005, pp. 32-42.

[229] Z. Y. Rawshdeh and S. M. Mahmud, "Toward strongly connected clustering structure in vehicular ad hoc networks," in *Proc. 2009 IEEE 70th Vehicular Technology Conference Fall (VTC 2009-Fall)* 2009, pp. 1-5.

[230] B. H. Kim, K. Y. Choi, J. H. Lee, and D. H. Lee, "Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks," in *Proc. International Conference on Convergence Information Technology*, 2007, pp. 681-686.

[231] I. A. Sumra, H. B. Hasbullah, and J.-l. b. A. Manan, "Comparative study of security hardware modules (EDR, TPD and TPM) in VANET," in *Proc. 3rd National Information Technology Symposium (NITS2011)*, 2011.

[232] NIST. (2011, November 16). *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules*.

[233] NHTSA. (2011). *National Highway Traffic Safety Administration* Available: http://www.nhtsa.gov/

[234] S. Chellappan, "Information management in emergent vehicular ad hoc networks," in *2nd Workshop on Research Directions in Situational-aware Self-managed Proactive Computing in Wireless Adhoc Networks*, 2010.

[235] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud computing research and development trend," in *Proc. Second International Conference on Future Networks*, 2010, pp. 93-97.

[236] A. Wagh, X. Li, J. Wan, C. Qiao, and C. Wu, "Human centric data fusion in Vehicular Cyber-Physical Systems," in *Proc. 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* 2011, pp. 684-689.

[237] S. Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *International Journal of Pervasive Computing and Communications*, vol. 7, p. 15, 2011.

[238] Y.-W. Lin, J.-M. Shen, and H.-C. Weng, "Gateway discovery in VANET cloud," in *Proc. 2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC)* 2011, pp. 951-954.

[239] X. Li, X. Yu, A. Wagh, and C. Qiao, "Human factors-aware service scheduling in Vehicular Cyber-Physical systems," in *Proc. IEEE INFOCOM*, 2011, pp. 2174-2182.

[240] M. C. Bujorianu, M. L. Bujorianu, and H. Barringer, "A unifying specification logic for cyber-physical systems," in *Proc. 17th Mediterranean Conference on Control and Automation*, 2009, pp. 1166-1171.

Appendices

Appendix A Copyright Permission for Chapter 2

ELSEVIER LICENSE
TERMS AND CONDITIONS

Jan 09, 2012

This is a License Agreement between Zhengming Li ("You") and Elsevier ("Elsevier") provided by Copyright Clearance Center ("CCC"). The license consists of your order details, the terms and conditions provided by Elsevier, and the payment terms and conditions.

All payments must be made in full to CCC. For payment instructions, please see information listed at the bottom of this form.

Supplier	Elsevier Limited The Boulevard,Langford Lane Kidlington,Oxford,OX5 1GB,UK
Registered Company Number	1982084
Customer name	Zhengming Li
Customer address	1902B Woodmar Dr Houghton, MI 49931
License number	2824810371738
License date	Jan 09, 2012
Licensed content publisher	Elsevier
Licensed content publication	Ad Hoc Networks
Licensed content title	LEAPER: A lightweight reliable and faithful data packet relaying framework for VANETs
Licensed content author	Zhengming Li,Chunxiao Chigan
Licensed content date	May 2011
Licensed content volume number	9
Licensed content issue number	3
Number of pages	12
Start Page	418
End Page	429
Type of Use	reuse in a thesis/dissertation
Portion	full article
Format	both print and electronic
Are you the author of this Elsevier article?	Yes
Will you be translating?	No
Order reference number	
Title of your thesis/dissertation	Securit, Privacy and Applications in Vehicular Ad Hoc Networks
Expected completion date	Mar 2012

Estimated size (number of pages)	200
Elsevier VAT number	GB 494 6272 12
Permissions price	0.00 USD
VAT/Local Sales Tax	0.0 USD / 0.0 GBP
Total	0.00 USD
Terms and Conditions	

INTRODUCTION

1. The publisher for this copyrighted material is Elsevier. By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the Billing and Payment terms and conditions established by Copyright Clearance Center, Inc. ("CCC"), at the time that you opened your Rightslink account and that are available at any time at http://myaccount.copyright.com).

GENERAL TERMS

2. Elsevier hereby grants you permission to reproduce the aforementioned material subject to the terms and conditions indicated.

3. Acknowledgement: If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source, permission must also be sought from that source. If such permission is not obtained then that material may not be included in your publication/copies. Suitable acknowledgement to the source must be made, either as a footnote or in a reference list at the end of your publication, as follows:

"Reprinted from Publication title, Vol /edition number, Author(s), Title of article / title of chapter, Pages No., Copyright (Year), with permission from Elsevier [OR APPLICABLE SOCIETY COPYRIGHT OWNER]." Also Lancet special credit - "Reprinted from The Lancet, Vol. number, Author(s), Title of article, Pages No., Copyright (Year), with permission from Elsevier."

4. Reproduction of this material is confined to the purpose and/or media for which permission is hereby given.

5. Altering/Modifying Material: Not Permitted. However figures and illustrations may be altered/adapted minimally to serve your work. Any other abbreviations, additions, deletions and/or any other alterations shall be made only with prior written authorization of Elsevier Ltd. (Please contact Elsevier at permissions@elsevier.com)

6. If the permission fee for the requested use of our material is waived in this instance, please be advised that your future requests for Elsevier materials may attract a fee.

7. Reservation of Rights: Publisher reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.

8. License Contingent Upon Payment: While you may exercise the rights licensed

immediately upon issuance of the license at the end of the licensing process for the transaction, provided that you have disclosed complete and accurate details of your proposed use, no license is finally effective unless and until full payment is received from you (either by publisher or by CCC) as provided in CCC's Billing and Payment terms and conditions. If full payment is not received on a timely basis, then any license preliminarily granted shall be deemed automatically revoked and shall be void as if never granted. Further, in the event that you breach any of these terms and conditions or any of CCC's Billing and Payment terms and conditions, the license is automatically revoked and shall be void as if never granted. Use of materials as described in a revoked license, as well as any use of the materials beyond the scope of an unrevoked license, may constitute copyright infringement and publisher reserves the right to take any and all action to protect its copyright in the materials.

9. Warranties: Publisher makes no representations or warranties with respect to the licensed material.

10. Indemnity: You hereby indemnify and agree to hold harmless publisher and CCC, and their respective officers, directors, employees and agents, from and against any and all claims arising out of your use of the licensed material other than as specifically authorized pursuant to this license.

11. No Transfer of License: This license is personal to you and may not be sublicensed, assigned, or transferred by you to any other person without publisher's written permission.

12. No Amendment Except in Writing: This license may not be amended except in a writing signed by both parties (or, in the case of publisher, by CCC on publisher's behalf).

13. Objection to Contrary Terms: Publisher hereby objects to any terms contained in any purchase order, acknowledgment, check endorsement or other writing prepared by you, which terms are inconsistent with these terms and conditions or CCC's Billing and Payment terms and conditions. These terms and conditions, together with CCC's Billing and Payment terms and conditions (which are incorporated herein), comprise the entire agreement between you and publisher (and CCC) concerning this licensing transaction. In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall control.

14. Revocation: Elsevier or Copyright Clearance Center may deny the permissions described in this License at their sole discretion, for any reason or no reason, with a full refund payable to you. Notice of such denial will be made using the contact information provided by you. Failure to receive such notice will not alter or invalidate the denial. In no event will Elsevier or Copyright Clearance Center be responsible or liable for any costs, expenses or damage incurred by you as a result of a denial of your permission request, other than a refund of the amount(s) paid by you to Elsevier and/or Copyright Clearance Center for denied permissions.

LIMITED LICENSE

The following terms and conditions apply only to specific license types:

15. **Translation**: This permission is granted for non-exclusive world **English** rights only unless your license was granted for translation rights. If you licensed translation rights you

may only translate this content into the languages you requested. A professional translator must perform all translations and reproduce the content word for word preserving the integrity of the article. If this license is to re-use 1 or 2 figures then permission is granted for non-exclusive world rights in all languages.

16. **Website**: The following terms and conditions apply to electronic reserve and author websites:
Electronic reserve: If licensed material is to be posted to website, the web site is to be password-protected and made available only to bona fide students registered on a relevant course if:
This license was made in connection with a course,
This permission is granted for 1 year only. You may obtain a license for future website posting,
All content posted to the web site must maintain the copyright information line on the bottom of each image,
A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx or the Elsevier homepage for books at http://www.elsevier.com , and
Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

17. **Author website** for journals with the following additional clauses:

All content posted to the web site must maintain the copyright information line on the bottom of each image, and
he permission granted is limited to the personal version of your paper. You are not allowed to download and post the published electronic version of your article (whether PDF or HTML, proof or final version), nor may you scan the printed edition to create an electronic version,
A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx , As part of our normal production process, you will receive an e-mail notice when your article appears on Elsevier's online service ScienceDirect (www.sciencedirect.com). That e-mail will include the article's Digital Object Identifier (DOI). This number provides the electronic link to the published article and should be included in the posting of your personal version. We ask that you wait until you receive this e-mail and have the DOI to do any posting.
Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

18. **Author website** for books with the following additional clauses:
Authors are permitted to place a brief summary of their work online only.
A hyper-text must be included to the Elsevier homepage at http://www.elsevier.com

All content posted to the web site must maintain the copyright information line on the bottom of each image
You are not allowed to download and post the published electronic version of your chapter, nor may you scan the printed edition to create an electronic version.
Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

19. **Website** (regular and for author): A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx. or for books to the Elsevier homepage at http://www.elsevier.com

20. **Thesis/Dissertation**: If your license is for use in a thesis/dissertation your thesis may be submitted to your institution in either print or electronic form. Should your thesis be published commercially, please reapply for permission. These requirements include permission for the Library and Archives of Canada to supply single copies, on demand, of the complete thesis and include permission for UMI to supply single copies, on demand, of the complete thesis. Should your thesis be published commercially, please reapply for permission.

21. **Other Conditions**:

v1.6

If you would like to pay for this license now, please remit this license along with your payment made payable to "COPYRIGHT CLEARANCE CENTER" otherwise you will be invoiced within 48 hours of the license date. Payment should be in the form of a check or money order referencing your account number and this invoice number RLNK500695222.
Once you receive your invoice for this order, you may pay your invoice by credit card. Please follow instructions provided at that time.

Make Payment To:
Copyright Clearance Center
Dept 001
P.O. Box 843006
Boston, MA 02284-3006

For suggestions or comments regarding this order, contact RightsLink Customer Support: customercare@copyright.com or +1-877-622-5543 (toll free in the US) or +1-978-646-2777.

Gratis licenses (referencing $0 in the Total field) are free. Please retain this printable license for your reference. No payment is required.

Appendix B Copyright Permission for Chapter 3

COPYRIGHT TRANSFER AGREEMENT

WILEY-BLACKWELL

Date: 09/03/10 Contributor name: ZHENGMING LI, CHUNXIAO CHIGAN

Contributor address: 1400 Townsend Dr, Houghton, MI 49931

Manuscript number (Editorial office only): _____

Re: Manuscript entitled RAMV: Ensuring Resource-Aware Message Verification in VANETs (the "Contribution")

for publication in Security and Communication Networks (the "Journal")

published by Wiley-Blackwell ("Wiley-Blackwell").

Dear Contributor(s):

Thank you for submitting your Contribution for publication. In order to expedite the editing and publishing process and enable Wiley-Blackwell to disseminate your Contribution to the fullest extent, we need to have this Copyright Transfer Agreement signed and returned as directed in the Journal's instructions for authors as soon as possible. If the Contribution is not accepted for publication, or if the Contribution is subsequently rejected, this Agreement shall be null and void. **Publication cannot proceed without a signed copy of this Agreement.**

A. COPYRIGHT

1. The Contributor assigns to Wiley-Blackwell, during the full term of copyright and any extensions or renewals, all copyright in and to the Contribution, and all rights therein, including but not limited to the right to publish, republish, transmit, sell, distribute and otherwise use the Contribution in whole or in part in electronic and print editions of the Journal and in derivative works throughout the world, in all languages and in all media of expression now known or later developed, and to license or permit others to do so.

2. Reproduction, posting, transmission or other distribution or use of the final Contribution in whole or in part in any medium by the Contributor as permitted by this Agreement requires a citation to the Journal and an appropriate credit to Wiley-Blackwell as Publisher, and/or the Society if applicable, suitable in form and content as follows: (Title of Article, Author, Journal Title and Volume/Issue, Copyright © [year], copyright owner as specified in the Journal). Links to the final article on Wiley-Blackwell's website are encouraged where appropriate.

B. RETAINED RIGHTS

Notwithstanding the above, the Contributor or, if applicable, the Contributor's Employer, retains all proprietary rights other than copyright, such as patent rights, in any process, procedure or article of manufacture described in the Contribution.

C. PERMITTED USES BY CONTRIBUTOR

1. Submitted Version. Wiley-Blackwell licenses back the following rights to the Contributor in the version of the Contribution as originally submitted for publication:

a. After publication of the final article, the right to self-archive on the Contributor's personal intranet page or in the Contributor's institution's/employer's institutional intranet repository or archive. The Contributor may not update the submission version or replace it with the published Contribution. The version posted must contain a legend as follows: This is the pre-peer reviewed version of the following article: FULL CITE, which has been published in final form at [Link to final article].

b. The right to transmit, print and share copies with colleagues.

2. Accepted Version. Reuse of the accepted and peer-reviewed (but not final) version of the Contribution shall be by separate agreement with Wiley-Blackwell. Wiley-Blackwell has agreements with certain funding agencies governing reuse of this version. The details of those relationships, and other offerings allowing open web use are set forth at the following website: http://www.wiley.com/go/funderstatement. NIH grantees should check the box at the bottom of this document.

3. Final Published Version. Wiley-Blackwell hereby licenses back to the Contributor the following rights with respect to the final published version of the Contribution:

a. Copies for colleagues. The personal right of the Contributor only to send or transmit individual copies of the final published version to colleagues upon their specific request provided no fee is charged, and further-provided that there is no systematic distribution of the Contribution, e.g. posting on a listserve, website or automated delivery. For those Contributors who wish to send high-quality e-prints, purchase reprints, or who wish to distribute copies more broadly than allowed hereunder (e.g. to groups of colleagues or mailing lists), please contact the publishing office.

b. Re-use in other publications. The right to re-use the final Contribution or parts thereof for any publication authored or edited by the Contributor (excluding journal articles) where such re-used material constitutes less than half of the total material in such publication. In such case, any modifications should be accurately noted.

c. Teaching duties. The right to include the Contribution in teaching or training duties at the Contributor's institution/place of employment including in course packs, e-reserves, presentation at professional conferences, in-house training, or distance learning. The Contribution may not be used in seminars outside of normal teaching obligations (e.g. commercial seminars). Electronic posting of the final published version in connection with teaching/training at the Contributor's institution/place of employment is permitted subject to the implementation of reasonable access control mechanisms, such as user name and password. Posting the final published version on the open Internet is not permitted.

d. Oral presentations. The right to make oral presentations based on the Contribution.

4. Article Abstracts, Figures, Tables, Data Sets, Artwork and Selected Text (up to 250 words).

a. Contributors may re-use unmodified abstracts for any non-commercial purpose. For on-line uses of the abstracts, Wiley-Blackwell encourages but does not require linking back to the final published versions.

b. Contributors may re-use figures, tables, data sets, artwork, and selected text up to 250 words from their Contributions, provided the following conditions are met:

(i) Full and accurate credit must be given to the Contribution.
(ii) Modifications to the figures, tables and data must be noted. Otherwise, no changes may be made.
(iii) The reuse may not be made for direct commercial purposes, or for financial consideration to the Contributor.
(iv) Nothing herein shall permit dual publication in violation of journal ethical practices.

CTA-PS

D. CONTRIBUTIONS OWNED BY EMPLOYER

1. If the Contribution was written by the Contributor in the course of the Contributor's employment (as a "work-made-for-hire" in the course of employment), the Contribution is owned by the company/employer which must sign this Agreement (in addition to the Contributor's signature) in the space provided below. In such case, the company/employer hereby assigns to Wiley-Blackwell, during the full term of copyright, all copyright in and to the Contribution for the full term of copyright throughout the world as specified in paragraph A above.

2. In addition to the rights specified as retained in paragraph B above and the rights granted back to the Contributor pursuant to paragraph C above, Wiley-Blackwell hereby grants back, without charge, to such company/employer, its subsidiaries and divisions, the right to make copies of and distribute the final published Contribution internally in print format or electronically on the Company's internal network. Copies so used may not be resold or distributed externally. However the company/employer may include information and text from the Contribution as part of an information package included with software or other products offered for sale or license or included in patent applications. Posting of the final published Contribution by the institution on a public access website may only be done with Wiley-Blackwell's written permission, and payment of any applicable fee(s). Also, upon payment of Wiley-Blackwell's reprint fee, the institution may distribute print copies of the published Contribution externally.

E. GOVERNMENT CONTRACTS

In the case of a Contribution prepared under U.S. Government contract or grant, the U.S. Government may reproduce, without charge, all or portions of the Contribution and may authorize others to do so, for official U.S. Government purposes only, if the U.S. Government contract or grant so requires. (U.S. Government, U.K. Government, and other government employees: see notes at end.)

F. COPYRIGHT NOTICE

The Contributor and the company/employer agree that any and all copies of the final published version of the Contribution or any part thereof distributed or posted by them in print or electronic format as permitted herein will include the notice of copyright as stipulated in the Journal and a full citation to the Journal as published by Wiley-Blackwell.

G. CONTRIBUTOR'S REPRESENTATIONS

The Contributor represents that the Contribution is the Contributor's original work, all individuals identified as Contributors actually contributed to the Contribution, and all individuals who contributed are included. If the Contribution was prepared jointly, the Contributor agrees to inform the co-Contributors of the terms of this Agreement and to obtain their signature to this Agreement or their written permission to sign on their behalf. The Contribution is submitted only to this Journal and has not been published before. (If excerpts from copyrighted works owned by third parties are included, the Contributor will obtain written permission from the copyright owners for all uses as set forth in Wiley-Blackwell's permissions form or in the Journal's Instructions for Contributors, and show credit to the sources in the Contribution.) The Contributor also warrants that the Contribution contains no libelous or unlawful statements, does not infringe upon the rights (including without limitation the copyright, patent or trademark rights) or the privacy of others, or contain material or instructions that might cause harm or injury.

CHECK ONE BOX:

☒ Contributor-owned work

ATTACH ADDITIONAL SIGNATURE PAGES AS NECESSARY

Contributor's signature [redacted] Date 09/03/10

Type or print name and title Mr. ZHENGMING LI

Co-contributor's signature [redacted] Date 9/3/10

Type or print name and title CHUNXIAO CHIGAN

☐ Company/Institution-owned work (made-for-hire in the course of employment)

Company or Institution (Employer-for-Hire) Date

Authorized signature of Employer Date

☐ U.S. Government work

Note to U.S. Government Employees
A contribution prepared by a U.S. federal government employee as part of the employee's official duties, or which is an official U.S. Government publication, is called a "U.S. Government work," and is in the public domain in the United States. In such case, the employee may cross out Paragraph A.1 but must sign (in the Contributor's signature line) and return this Agreement. If the Contribution was not prepared as part of the employee's duties or is not an official U.S. Government publication, it is not a U.S. Government work.

☐ U.K. Government work (Crown Copyright)

Note to U.K. Government Employees
The rights in a Contribution prepared by an employee of a U.K. government department, agency or other Crown body as part of his/her official duties, or which is an official government publication, belong to the Crown. U.K. government authors should submit a signed declaration form together with this Agreement. The form can be obtained via http://www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/publication-of-articles-written-by-ministers-and-civil-servants.htm

☐ Other Government work

Note to Non-U.S., Non-U.K. Government Employees
If your status as a government employee legally prevents you from signing this Agreement, please contact the editorial office.

☐ NIH Grantees

Note to NIH Grantees
Pursuant to NIH mandate, Wiley-Blackwell will post the accepted version of Contributions authored by NIH grant-holders to PubMed Central upon acceptance. This accepted version will be made publicly available 12 months after publication. For further information, see www.wiley.com/go/nihmandate.

CTA-PS

Appendix C Copyright Permission from IEEE

Comments/Response to Case ID: 005538F3

ReplyTo: Copyrights@ieee.org

From:	Jacqueline Hansson	**Date:**	03/01/2012
Subject:	Re: Regarding reusing the submitted manuscripts in my PhD dissertation	**Send To:**	Zhengming Li <zli1@mtu.edu>
		cc:	

Dear Zhengming Li :

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ©© [year of original publication] IEEE.

2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table

3) If you expect to use a substantial portion of the original paper, and if you are not the senior author, please obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]

2) The pubished version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.

3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of Michigan Tech's products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library may supply single copies of the dissertation.

In regards to future requests for IEEE copyrighted material, the IEEE has recently implemented a policy that provides an automated means for handling reuse permission of IEEE content through the Copyright Clearance Center RightsLink permission service. You can facilitate this process by taking the steps provided below. If you require answers to specific questions, please contact IEEE Senior Program Manager, Nancy A. Blair-DeLeon. She is responsible for managing this service, and can assist you further. Her contact information is n.blair-deleon@ieee.org

1. Go to http://ieeexplore.ieee.org/Xplore/guesthome.jsp
2. Type the title of the IEEE copyrighted paper into the IEEE Xplore Search Bar and click on the word "Search" .
3. Click on the underlined IEEE copyrighted paper's title that's in orange and blue print.
4. The title will appear again in orange print under the orange Browse tab.
5. Next, click on the orange “Request Permissions” link, which can be found under the IEEE paper title.
6. Continue the process to obtain permission for any material desired from each additional IEEE copyrighted paper.

Jacqueline Hansson, Coordinator
IEEE Intellectual Property Rights Office
445 Hoes Lane
Piscataway, NJ 08855-1331 USA
+1 732 562 3828 (phone)
+1 732 562 1746(fax)
e-mail: j.hansson@ieee.org
IEEE Fostering technological innovation
and excellence for the benefit of humanity.

©©©©©©©©©©©©©©©©©©©©©©©©©©©©©©©©©

Dear Sir/Madam,

Currently I have submitted two manuscripts to two IEEE journals. Based on the Copyright Agreements I can reuse these submitted manuscripts in my PhD dissertation, which will not be commercially published. In this case, what do I need to do in order to reuse these two manuscripts? I will properly cite these two submissions, and attach the IEEE copyright notice to my dissertation. Will these procedures be sufficient for me? If not, please kindly tell me what I need to do. Specifically, my two submissions are listed below.

If it is possible, please kindly respond within 1 week, since I am finalizing my dissertation right now. Thank you so much for your help!

1) On Privacy Protection with Short-Time Certificates in Vehicular Ad Hoc Networks Li, Zhengming; Chigan, Chunxiao
Submitted to IEEE Transactions on Vehicular Technology on Feb. 28, 2012.

2) On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc

Networks Li, Zhengming; Chigan, Chunxiao
Submitted to IEEE Transactions on Mobile Computing on Feb. 27, 2012.

--

Best Regards,

Zhengming Li

Acknowledgement

This dissertation work has been supported by the National Science Foundation CAREER award under grant CNS-0644056.