2016

# Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-Based Architecture for Vehicular Cloud

Kiho Lim
*University of Kentucky*, kiho.lim@uky.edu
Digital Object Identifier: http://dx.doi.org/10.13023/ETD.2016.314

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Kiho Lim, Student

Dr. Dakshnamoorthy Manivannan, Major Professor

Dr. Miroslaw Truszczynski, Director of Graduate Studies

Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-based Architecture for Vehicular Cloud

---

DISSERTATION

---

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the College of Engineering at the University of Kentucky

By

Kiho Lim

Lexington, Kentucky

Director: Dr. D. Manivannan, Associate Professor of Computer Science

Lexington, Kentucky

2016

ABSTRACT OF DISSERTATION

Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-based Architecture for Vehicular Cloud

Vehicular ad hoc Networks (VANETs) allow vehicles to form a self-organized network. VANETs are likely to be widely deployed in the future, given the interest shown by industry in self-driving cars and satisfying their customers various interests. Problems related to Mobile ad hoc Networks (MANETs) such as routing, security, etc. have been extensively studied. Even though VANETs are special type of MANETs, solutions proposed for MANETs cannot be directly applied to VANETs because all problems related to MANETs have been studied for small networks. Moreover, in MANETs, nodes can move randomly. On the other hand, movement of nodes in VANETs are constrained to roads and the number of nodes in VANETs is large and covers typically large area. The following are the contributions of the thesis.

**Secure, authenticated, privacy preserving message dissemination in VANETs:** When vehicles in VANET observe phenomena such as accidents, icy road condition, etc., they need to disseminate this information to vehicles in appropriate areas so the drivers of those vehicles can take appropriate action. When such messages are disseminated, the authenticity of the vehicles disseminating such messages should be verified while at the same time the anonymity of the vehicles should be preserved.

Moreover, to punish the vehicles spreading malicious messages, authorities should be able to trace such messages to their senders when necessary. For this, we present an efficient protocol for the dissemination of authenticated messages.

**Incentive-based architecture for vehicular cloud:** Due to the advantages such as flexibility and availability, interest in cloud computing has gained lot of attention in recent years. Allowing vehicles in VANETs to store the collected information in the cloud would facilitate other vehicles to retrieve this information when they need. In this thesis, we present a secure incentive-based architecture for vehicular cloud. Our architecture allows vehicles to collect and store information in the cloud; it also provides a mechanism for rewarding vehicles that contributing to the cloud.

**Privacy preserving message dissemination in VANETs:** Sometimes, it is sufficient to ensure the anonymity of the vehicles disseminating messages in VANETs. We present a privacy preserving message dissemination protocol for VANETs.

**KEYWORDS**: Vehicular Ad Hoc Networks, Vehicular Cloud, Security and Privacy in Vehicular Networks.

Kiho Lim

June 29, 2016

Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-based Architecture for Vehicular Cloud

By

Kiho Lim

Dakshnamoorthy Manivannan, Ph.D.

---

Director of Dissertation

Miroslaw Truszczynski, Ph.D.

---

Director of Graduate Studies

June 29, 2016

---

Date

ACKNOWLEDGMENTS

Upon finishing my dissertation, I would like to express my gratitude to people who encouraged, assisted, inspired, and cared about me during my Ph.D. journey at the University of Kentucky. Without the guidance of my committee members, help from friends, and support from my family, I would never have been able to finish my dissertation.

First and foremost, I would like to express my deepest gratitude to my advisor, Dr. D. Manivannan, for his guidance, patience, caring, and leading me to do research in Vehicular ad hoc Networks. Dr. Manivannan has been a great mentor on every account, and his broad knowledge and constructive suggestions to this dissertation are sincerely appreciated.

Beside, I would like to thank other faculty members of my Advisory Committee Dr. Mukesh Singhal, Dr. Zongming Fei, and Dr. Sherali Zeadally for their insightful and valuable comments on my dissertation.

Also, I would like to thank Dr. D. Manivannan, Dr. Zongming Fei, Dr. Debby Keen, and Dr. Yi Pike for their kind assistance with writing me recommendation letters and helping me in my job search.

Finally, I would like to express my special thanks to my family and HY. I thank my beloved parents for their continuous support, encouragement and endless love. I am also very grateful to my sister for her support and caring.

Table of Contents

## List of Tables

## List of Figures

## Chapter 1

## Introduction

Vehicular Ad Hoc Networks (VANETs) provide ubiquitous connectivity to mobile users on the road and efficient vehicle-to-vehicle communication that can help in implementing Intelligent Transportation Systems (ITS). ITS can provide support for various types of applications such as collision prevention, traffic monitoring, traffic flow control, providing information about nearby services. [35] Another important application of VANETs is that since vehicles are connected to the Internet, the users could enjoy the services, the infotainment, and the entertainments, supported on the Internet while they are moving.

VANETs are special type of MANETs (Mobile Ad hoc Networks). The main difference between the two is that nodes in VANETs are vehicles on the roadway and their movement is constrained to roads whereas nodes in MANETs move randomly. One of the primary goals of VANETs is to increase road safety. In order to achieve this goal, vehicles monitor phenomena on the roads and inform other vehicles about abnormal and dangerous traffic condition such as icy roads, heavy congestion, or car accidents. Adversaries could exploit this by injecting malicious messages for their own benefit or to deliberately disrupt the users. Thus, securing VANETs from such adversaries is important.

In VANETs, each vehicle is equipped with a communication device to communicate with other vehicles and designated roadside infrastructure, called road side units, to exchange safety related information. These vehicle nodes and roadside infrastruc-

ture together form a self-organized network, called a Vehicular Adhoc Network. In VANETs, various type of techniques are required such as beaconing, forwarding, broadcasting, and routing to deliver messages to the destination through appropriate nodes. Due to the high mobility of vehicle nodes, the network topology changes frequently. Our main aim is to address the security and routing issues in VANETs. Next, we present the necessary background, motivation for our research, and the problems addressed in this dissertation.

## 1.1 Background

In this section, we introduce the security architecture, trust issues, key and certificate management, and attacks in VANETs and existing solutions, which our research is based on.

### 1.1.1 Security Architecture

#### Requirements of Security Services

Security mechanisms in MANETs have been extensively studied; however, they are not suitable for VANETs due to the unique characteristics of VANETs, so they can't be directly applied to VANETs. Despite a broad range of challenges facing securing vehicular communication, the security issues must be addressed and solved for the successful deployment of VANETs. Since the drivers and the vehicles in VANETs rely on shared information to make decisions, they would be vulnerable to malicious and misbehaving nodes; so proper mechanisms need to be implemented for detecting and thwarting attacks from such malicious nodes. The security services of VANETs typically need to meet the following requirements [60], [80], [68]:

1. *Integrity:* The integrity service is to deal with the accuracy, consistency, and the completeness of messages during transmission. In order to prevent attackers

from altering or injecting messages, integrity of messages should be ensured. Also, a reliable time source for accurate time synchronization and a reliable positioning system for precise location information could be used to protect communication against attacks such as replay-attack or position spoofing attack.

2. *Availability:* In VANETs, time critical messages such as emergency traffic information must be handled at any given time. If one channel is not available due to failure or attack, there must be alternative means to maintain vehicular network availability all the time.

3. *Authentication:* Every message exchanged must be authenticated to identify the sender of the message. Vehicles should react only to information or events generated by legitimate senders.

4. *Non-repudiation:* This service is designed to identify misbehaving nodes or attackers and prevent them from denying messages transmitted by them. Any vehicle related information for communication, such as location, speed, and time, will be stored in a tamper-proof On-Board Unit. It also could be used by authorities for investigation to reproduce the scene of an accident with the same sequence and content of the messages communicated before the accident.

5. *Real-time constraints:* Vehicles move with high velocity. In some situations like time-sensitive communication, a real-time response is essential, so time constraints should be respected.

6. *Privacy:* All driver information such as identity, location and speed, should be protected against unauthorized observers. Also, an observer should not be able to trace the routes of the vehicles.

### Network Model

Two types of communicating entities are presented in the currently explored architectures of VANETs. The first type is a vehicle node which forms the majority of all VANET nodes.The second type is the roadside base stations, usually called RSUs (Road Side Units). The radio used for communication is Dedicated Short-Range Communications (DSRC), which has been allocated as a new band in 1999 by the Federal Communications Commission; the band allocated was 75MHz at 5.9GHz frequency for Intelligent Transport System(ITS) applications in North America. Also, the IEEE 802.11p standard supports the communication channel and technology. Communication in VANETs could be either direct communication between vehicles or through multiple wireless link hops. Vehicles operate as both endpoints and routers. Vehicular networking will enable vehicle-to-vehicle communication, vehicle-to-RSU communication, and vehicle-to-existing infrastructure networks communication [80].

High velocity of vehicle is a real-time constraint in VANETs. For example, if two vehicles are moving in opposite direction on highways, they would only have a very short connection time between them. Also, unlike MANETs in which nodes move randomly, vehicles move along the roads, hence their mobility is constrained. Vehicles in VANET are equipped with a wireless communication device and computation resources to perform security tasks. Also, additional devices such as a Global Positioning System (GPS) and an Event Data Recorder (EDR) could be present to provide the location of vehicles. Vehicles also have a tamper-proof storage for private information such as private/public keys and electronic license plate information [80].

### Message Categories

Many applications are waiting for deployment in VANETs. These applications can be divided into two major categories, namely safety related applications and non safety related applications [65, 80].

1. Safety-related applications

For example, collision avoidance warning messages, emergency brake warning messages, traffic light warning messages, or lane merging warning messages could be sent to warn drivers. Since the messages sent by this type of application help drivers make critical decisions, ensuring the security and reliability of such messages is essential.

- *Traffic information messages:* Messages contain information such as road condition and accidents. Messages are sent to all vehicles within specific area for safety and typically they are not time-critical messages.

- *General safety-related messages:* This type of messages are used for general safety applications such as cooperative driving. Due to the high mobility of vehicle nodes, message contents are time sensitive, hence they should arrive within the preset time window.

- *Liability-related messages:* This type of messages are used for liability-related applications, which share traffic information and drivers are responsible for the traffic information. For example, if the message originator need be traced back to investigate an accident by the law enforcement authorities, the authorities should be able to trace the message to its sender.

2. Non-safety-related Application

There are non safety related applications, such as traffic optimization, automatic payment services, location-related services, and driver infotainment services. This type of applications do not have time-critical messages, but securing messages for such services (e.g., payment services) and protecting user privacy (e.g., location service) are still very important for such applications.

### 1.1.2 Trust Issues

Establishing trust between communicating vehicles is still one of the major challenging problems. Especially in safety applications, trust is a key element as receiving nodes make decisions with the critical information from the safety application while moving at high speed. Therefore, VANETs should ensure authenticity and trustability of every message before using it [65].

In VANETs, each node needs to be equipped with a trust system that can make trust decisions. There are two approaches to establish trust. The first approach is the infrastructure-based trust establishment, which relies on trusted and global central authority. Another approach is the self-organizing trust establishment, where the system is built up and adapted dynamically for the environment [83]. The details of these approaches are discussed next.

#### Infrastructure-based Trust Establishment

There are many approaches for infrastructure based trust establishment. In this type of trust establishment, trust relies on a static security infrastructure and certificates are used in most cases. Here, we review some such approaches.

- *Classical Certificate-based Systems:* This is the traditional trust system with certificates. At the initial stage, certificates are issued by a central authority and later they are used for trust verification. One of the example is the simple Public Key Infrastructure, where trust is based on the public keys of nodes [23].

- *Kerberos:* Kerberos system is designed to improve security and prevent replay attacks. In Kerberos system, a central Key Distribution Center (KDC) authenticates users to issue a valid trust token. The trust token contains a session key, a validity period, and the requesting node's identity encrypted with the server's secret key [32], [54].

- *Pseudonyms:* The above mentioned approaches disclose the identities of nodes to interact with other nodes (user ID, public key, attributes). In a VANET, user privacy is indispensable feature and revealing user information should be minimized. One of the solutions to address privacy issues is the use of pseudonyms [83]. The trusted central authority issues and manages pseudonyms and can verify the original identities associated with user's pseudonyms.

- *Blind Signature:* Blind signature [16] is used for a signer to electronically sign a message without knowing the content of the message, so the certificates remain anonymously within the trust systems. Blind signature is a flexible mechanism and it can be used in conjunction with other approaches including above mentioned certificate based approaches.

- *Zero Knowledge / Non-interactive zero knowledge:* With Zero-knowledge approach [28], a node can prove its certified message using knowledge of secret information without disclosing the content. This is a fundamental cryptographic mechanism and has been used in many applications, however, it's not suitable for VANETs due to the limited computation and communication capabilities of nodes, which require heavy interaction between prover and verifier. In order to prevent heavy interaction, Non-interactive zero knowledge proofs can be used with a mono-directional interaction [7]. The proofs allow the prover and verifier to share a common, short, and random string. This lightweight interaction for trust establishment is a key factor for high mobility nodes in VANETs, so Non-interactive zero knowledge approach could be used as one of possible solutions for trust mechanism.

- *Digital Credentials:* With Digital Credentials approach [9], nodes having certificates can selectively disclose the properties of the data fields in the certificates without revealing any other information. This approach could address secu-

rity and privacy issues. So the property values are a component of node's secret/public keys and a verifier can access all properties except the prover's properties without holding all of the prover's secret key.

- *Group Signatures:* In a group signature approach [17], a single public key matches with a large number of private keys. A private key is assigned to every member of the group and the group members use it to generate their signatures that can be verified with the corresponding public key. The major feature of this approach is that non-group members still can verify a signature generated by a group member, but they cannot find which member actually signed it. This provides some extent of anonymity as the signer remains anonymous to outsiders. However, the central authority has an ability to trace the signer with respective private key when necessary.

- *Threshold Cryptography:* This approach was first introduced in [71]. Unlike above mentioned physically centralized trust systems, threshold cryptography based trust system only uses the centralized entity for initialization. With (k,n) threshold scheme, a secret is shared between k parties and any n parties can rearrange the secret to prevent security attacks. This scheme was used to share secret keys in Adhoc Networks [91], but a critical drawback exists; if the available nodes are less than n, then the trust system does not work properly. So, this approach is not suitable for VANETs as the network topology changes frequently with moving vehicles.

All of the above trust systems are not suitable for VANETs because of the dynamic environment of VANETs. Nodes in VANETs are moving vehicles with the limited resources for computation and storing security related data.

### Self-organizing Trust Establishment

VANETs require a modified form of trust establishment due to the highly dynamic nodes. Connection to the security infrastructure for verification may not be available all the time. Also, nodes may need to make a decision quickly based on unverified information, which is sent by unidentified nodes. Hence, for self-organizing trust establishment 1) no trusted third party is involved. (e.g., online infrastructure) and 2) no global knowledge is shared between the nodes.

Trust relationships in VANETs change dynamically with the duration of connection with neighboring nodes. The more time a node remains connected with its neighbors, the higher will be the trust established with them. Therefore, mechanisms for trust establishment are categorized as follows.

- *direct establishment:* Trust is established through direct communication between nodes.
- *indirect establishment:* Trust relationships are transferable as nodes share the information about their trust relationship with other nodes.
- *hybrid establishment:* Trust is established by combining both direct and indirect mechanisms.

### Related Works on Trust Issues

Many approaches have been studied to address trust issues in VANETs. In this section, we introduce some of the recently proposed approaches.

*Proxy Signature-based RSU Message Broadcasting*

Biswas et al. [6] proposed proxy signature based message broadcasting to ensure message integrity, authentication of broadcasted messages, and authentication of the RSU to the OBUs. In this network model, Road Side Controllers (RSC) are involved

for communication in addition to the traditional entities in a VANET including Certificate Authority (CA), Road Side Units (RSU), On-Board Unit (OBU). A RSC manages a group of RSUs which are securely connected.

Two major aspects of this proxy signature based scheme are 1) Authentication of RSU as a valid group member of a RSC group to the OBUs, 2) delivery of messages signed by the RSU for the RSC. In this approach, an RSU advertises the certificate including the identity of the RSC, the public key of the RSC, the identity of the RSU, the MAC address of the RSU, and the location information. And the initial beacon message has a hash value in addition to the message contents. When an OBU receives a message, it uses the public key of the RSC, the MAC address of the RSU, and the location of the designated RSU for verification. In the approach, the signature guarantees the integrity of the message and confirms that the RSU is one of the member of the RSU group managed by the RSC. Once the received RSU's MAC address is verified, the OBU can join the RSU group. Also, the location information attached to message is compared to the actual location of the RSU.

*Anonymous Authentication (PAAVE)*

The protocol for anonymous authentication in Vehicular Networks using Smart Cards [56] has been proposed to address the privacy preservation issue with traceability by authority. This scheme is based on smart cards to generate instant anonymous keys between vehicles and roadside units and provides anonymous authentication and location privacy with a vehicle storing one cryptographic key.

A smart card used in this scheme includes an embedded integrated circuit chip, which is a secure micro-controller with internal memory. The smart cards can store large volume of data, perform functions like encryption/decryption, and connect to a smart card reader. With the benefits of the smart card including physical security and many security techniques, the user privacy is protected. Vehicular Security Module

(VSM) is a module on a smart card that securely stores identity information such as the identity of the driver and cryptographic keys for secure communication. So all messages for communication need to pass through the VSM for encryption. Also, all received messages are decrypted by the VSM as the VSM has all the cryptographic information.

This scheme consists of the following three components: authentication, session key establishment and message verification. The first component is Authentication Process. An OBU needs to authenticate itself to the nearby RSU before joining the network for communication. If the target RSU is located within the communication range of the vehicle, then it sends a message to the RSU to be verified. If there is no RSU within the transmission range of the vehicle, then it simply broadcasts a message in plain text to ask its neighbors for the nearest RSU's public key. After obtaining the pubic key of the nearest RSU, the vehicle now can communicate with the RSU. The second component is obtaining session keys for communication. Every RSU issues a new session key to an OBU for each session after any OBU is authenticated by the RSU. The session key is securely stored in the VSM and is not accessible to any OBU. The third component is communication and message verification. Since messages need to be encrypted by the VSM before transmission, upon receiving messages, the VSM also decrypt the messages.

### 1.1.3 Attacks on VANETs

**Attacks on VANETs**

In VANETs, it is important to account for non-cooperating entities because malicious nodes can deliberately mislead other vehicles by disseminating false traffic information and degrade the network performance. In this section, possible attacks in VANETs are discussed [75], [68], [59].

- *Denial of Service Attack*: In this type of attack, the attackers attempt to make

the communication channels unavailable or take control of vehicle's resources. It can degrade the network's performance and also affect driver's safety, especially when safety-related application is affected. For example, if the attacker creates a massive network traffic on the road, when accident occurs, the approaching vehicles are prevented from receiving warning messages due to the denial of service attack.

- *Message Suppression Attack*: In this type of attack, an attacker selectively drops messages from the network. The dropped message could be safety related messages or critical information for the receiver. Also, the attacker may attempt to replay the dropped message later and mislead the drivers.

- *Fabrication Attack*: In this type of attack, an attacker attempts to transmit fabricated messages into the network. The messages sent by the attacker could contain false traffic information or fake identity information. It can also contain false warning messages and certificates.

- *Alteration Attack*: In this type of attack, an attacker attempts to alter existing messages. The attacker can change the content of the message or delay the message transmission.

- *Replay Attack*: In this type of attack, an attacker attempts to send an earlier message again to take advantage of the situation at the time of sending. Since a message is replayed, this is called replay attack.

- *Sybil Attack:* If fake information is reported by a single malicious vehicle, it is not sufficient to be convinced and trusted. Some applications require several vehicles for the same information to be accepted as true. In this type of attack, a single malicious vehicle acts as multiple vehicles by creating a large number of pseudonyms. Since the vehicles trust the fake information and make decisions

based on the fake information, preventing this type of sybil attacks is crucial in VANET.

- *Privacy Attack:* If vehicles are required to have a unique identity in the messages transmitted, sybil attack may be prevented. However, if such unique identity is used, an observer may be able to identify the vehicle by tracking the messages it transmits. Hence, privacy issues also need to be addressed while protecting sybil attacks.

As seen above, such attacks prevent the enjoyable environment of VANETs. Hence, it's important to address the security issues while the solutions do not affect the performance of the network.

### 1.1.4 Secure Routing and Data Dissemination in VANETs

Security aspect of VANET infrastructure is a very important and has not been dealt with the attention it deserves. Because of the impact on the safety and security of passengers in the vehicles, designing protocols for delivering messages securely is important.

In addition to the communication device, many authors assume that each vehicle is equipped with a reliable positioning device (e.g., a Global Positioning System), so it can obtain accurate location and time information. To ensure that all security constraints are carefully handled, we assume a scenario where the adversaries can intercept any message in the VANET.

Because of their potential impact on the safety and security of human being in the vehicles, designing protocols for exchanging messages securely is important. The security objectives are authentication, non repudiation of signaling packets, protecting conditional user privacy, detecting and correcting malicious data, and excluding misbehaving nodes from route discovery while messages are transmitted efficiently.

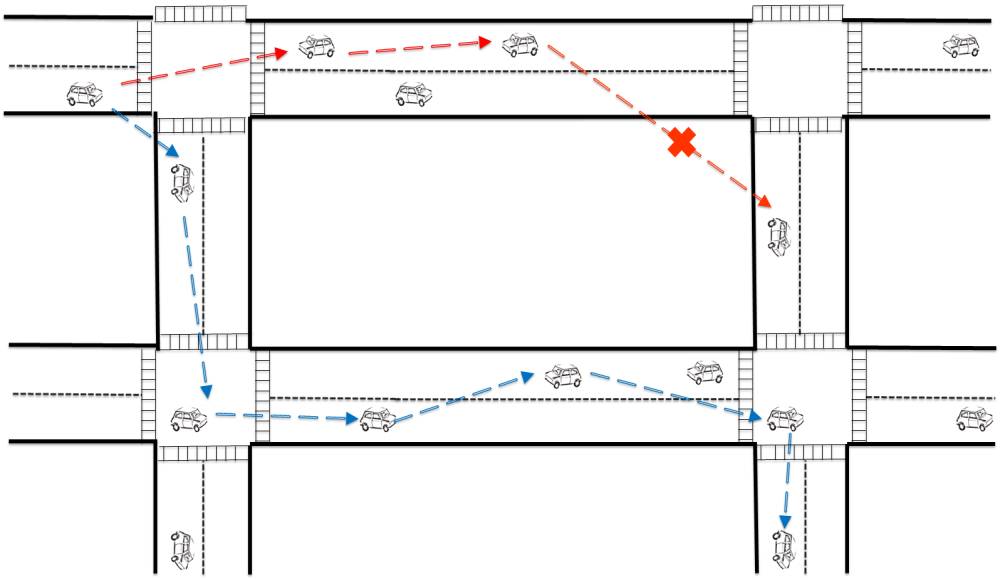

Figure 1.1: VANET Routing

Next, we review some of existing solutions for security and their problems.

### SAODV

Secure Ad-hoc On Demand distance Vector routing [88] is based AODV [58] routing protocol and aims at providing integrity, authentication and non-repudiation routing information. Also, with the help of digital signatures, it authenticates the non mutable fields of messages and hash chains to secure the mutable information fields such as Hop count information. A random number (seed) is generated by the node every time it sends a route request (RREQ) or route reply (RREP) message. The random number uses the time to live field in the IP header to set the max hop count and also sets the hash field and the identifier field of the hash function. The receiver calculates the hash value using the random number and compares if the top hash values are the same to verify the hop count. This function is repeated every time a RREQ or RREP is sent out.

### SPAAR

Secure Position Aided Ad hoc Routing (SPAAR) [15] makes use of precise positional information about nodes. This position information helps in improving efficiency by reducing unnecessary routing messages and securing MANETs. SPAAR uses asymmetric cryptography, certificate authorities and timestamps to prevent attacks from malicious nodes. The necessary entities in this approach are a public/private key pair for every node, a certificate server for binding the identity of nodes to their public keys. The public key of the certificate server is known to each node in the network. The certificate server offers authentication, confidentiality, non repudiation and integrity. Each node also maintains a public and private key pair with its neighbors. These key pairs are generated from the global key pair on detection of new neighbors. Multi-hop messages need to be signed with the private key of the sending node and be encrypted with the public key of the receiver. This enables neighbors to verify the presence and identity of its neighbor. The destination has to verify the identity of the sender. Nodes maintain tables to record information about one hop neighbors and recent destinations. The destination table also contains the speed of nodes so that their subsequent positions can be calculated. Table update messages are piggybacked on every routing message which enables periodic position information exchange. This reduces the load on one hop table to store recent position information. Topology changes are very frequent in VANETs and have to be detected and recorded instantaneously with the help of periodic hello messages. If a node does not know the position of any other node in the network, it sends out location_request messages. Location_request message is propagated in the network and if any intermediate node possesses information about the coordinates of the requested node, it sends a location_reply message back to the requesting node. This approach using asymmetric cryptography requires a lot more processing time for end-to-end and hop-by-hop communication because of the sheer size of the VANET, hence this

approach is not scalable to be applied in VANETs.

### GSIS

A Secure and Privacy Preserving Protocol (GSIS) proposed by X Lin et al. [44] utilizes group based keys and ID based keys to help identify vehicles in various traffic scenarios. This method focuses on helping traffic authorities and telecommunication systems at providing conditional privacy while ensuring the safety of the drivers. The safety of vehicle-to-vehicle as well as vehicle-to-roadside unit communication is discussed. Group signatures are used to secure the communication between vehicles and ID based signatures are used to secure the communication with roadside units. The protocol attempted to achieve data origin authenticity, data integrity, vehicle anonymity, RSU ID exposure, prevention of RSU replication, and vehicle ID traceability. Bilinear pairing [8] (which helps reduce the length of keys) and the various problems associated with Diffie Hellman key exchange [21] form the basis of the proposed Group based and ID based signatures.

The membership managers and traffic managers are the primary entities in the GSIS system. The membership managers provide security and system parameters to the mobile and roadside units and also send out private and group keys to these units. The traffic managers are responsible for collecting information when identities of vehicles need to be revealed. Certificate revocation lists are maintained to maintain a list of compromised vehicles and their certificates. Once a vehicle is determined as compromised, new group and private keys are generated for the remaining safe nodes and are sent out.

**Securing Vehicular Ad hoc NETworks**

Raya and Habaux [63] aim at maintaining the message legitimacy to protect VANETs from outsider attacks. The concept of safety messages is an integral part of this scheme. Since they consider only safety related applications, confidentiality is neglected. As a result of that, encryption is not needed and authentication suffices. Session key based authentication schemes are used to serve safety related applications. This scheme assumes that every vehicle is loaded with a private/public key pair and is familiar with other entities in its own group thereby desiring the content of communication to be kept secret and not disclosed outside of the group. This model classifies the attack models into:

1. Insider vs Outsider attack model
2. Malicious vs Rational attack model
3. Active vs Passive attack model
4. Local vs Extended attack model

This model also considers more sophisticated attack models such as the Hidden vehicle attack, the tunnel attack, Wormhole and Bush telegraph attacks. They assume the physical devices are equipped with tamper proof devices for the transmission of the messages. Since each safety message is attached with both a digital signature and a certificate, an attempt is made to reduce the additional overhead with the use of symmetric keys. Session keys are better for nodes maintaining contact for an extended period of time. The use of pair-wise keys and group keys are used depending on the trust level of vehicles.

As it is considered unwise to preload vehicles with shared pair-wise keys, the pair-wise key establishment is a dynamic process. The communicating entities exchange public keys and certificates, and the pair-wise session keys. The keys produced are used as the hash keys for the HMAC scheme which is then used for authenticating messages. However, congestion due to heavy traffic load makes this approach not

very desirable. To help deal with the heavy overhead due to pair-wise keys, group based signature schemes were proposed. Group joining and leaving is another factor that was separately considered. Group joining is not a big issue because loading the joining vehicle with the group key wasn't very complicated. However, a leaving node caused problems as a new key has to be computed for the entire group. Hence the concept of creating secure groups was introduced, that does not require the computation of a new group key every time a node left the group. This scheme would protect the group from outsider attacks but not insider attacks.

**Secure Position Based Routing**

Harsch et al. [30] aim at providing a comprehensive solution to protect network operations by securing geographic routing operations. The main focus is to secure operations such as beaconing, exchange of node co-ordinates, geo-location discovery, multihop (geographic unicast, topologically scoped broadcast, geographically scoped broadcast and geographically scoped anycast) communication, precision of the location service and forwarding. Their approach is a position based routing specific security solution. Location information received by nodes should correspond to legitimate physical node positions. Since location information is stored in location tables, plausibility of location information is preferred over the preciseness of node locations at that instant of time. Nodes must be made responsible for authentically reporting their location information without being threatened by impersonation attacks. Authentication, integrity and non repudiation of packets, freshness of location information, authorization and reliability of location tables are features of this approach.

A certificate authority loads each vehicle with public/private key pairs and certificates which contain the CA lifetime, the CA identifier and an attribute list. The packet's time and location fields are used as inputs to conduct a series of plausibility

checks. The packet is discarded if it fails any one of these plausibility checks. Two types of signatures are applied to every packet with a source signing the immutable fields and each hop signing the mutable field of the packet. Each hop checks the validity of the source and sender signatures and replaces the mutable information and sends it after resigning it. The plausibility checks are performed to check the validity of the packet lifetime, the allowable range of transmission of the forwarding node that sends it and the allowable velocity with which it is allowed to forward it. If any of these fail, the packet is dropped.

**Time and Location Critical Emergency Message Dissemination**

Zhuang et al. [92] focus mainly on emergency message (EM) dissemination. The focus on the time and location criticality (TLC) aspect has led to the simplification of the radio transceiver design and the contention based MAC protocol for VANETs operating on a single channel. Existing protocols achieved message dissemination to different nodes via different channels but the proposed protocol tried to achieve it using a single channel. The EMs are sent from the Point of Interest (POI) to vehicles closer receiving a more detailed message and vehicles receiving messages with less detail. The POI is generally an accident site and the messages have varying degrees of detail so as to notify as many vehicles as possible and avoid pileups by suggesting different routes or a vehicle to slow down. Vehicles that are closer have a higher Signal to Interference and Noise Ratio (SINR) and hence get a more detailed message so they can maneuver quicker and the degree of detail decreases with distance.

This EM dissemination is achieved with the help of the Scalable Modulation & Coding (SMC) scheme. SMC does bit to symbol mapping in the modulation mapping which determines the level of detail for the messages. The Road Side Units collect vehicle cluster information by observing forward and reverse traffic patterns

and provide this cluster information to the TLC framework.

This proposes an effective way for EM dissemination while reducing cost and connection complexity by using a single channel. However, the need to deal with handover delays has to be dealt with to further refine this scheme.

### Global Public Key Algorithm for Secure Location Service

The geographic routing protocol proposed by Pradeep et al. [61] based on the bilinear pair based cryptography. A global key is used which reduces the overhead caused by digital signatures and path verification of certificates. The use of global keys has no negative effect on the location service while retaining authenticity by reducing signature size. Location information of every node is maintained in a location server and is provided to a source vehicle on request. The importance of the tamper proof device on an OBU is highlighted as the privacy, decrypted location info, ID and cryptographic credentials are protected from illegal external access. The steps involved in the algorithm are simple with the message being signed first and encrypted with the public key parameters generated by the bilinear mapping. A signed message has its authenticity protected. A timestamp is included to identify the freshness of a packet. The final steps of the protocol are the decryption and signature verification. This ensures hop by hop authentication and end to end protection.

### Delay-efficient Geodynamic Group Based Authentication

Riley et al. [66] proposed a geodynamic authentication protocol with geodynamic groups of vehicles formed with distinct group boundaries. A trusted leader is selected for the whole group and vehicles can change group membership based on their geographic location. The authentication scheme utilizes a public key cryptography

system called the Group Based Hybrid Authentication Protocol to create dynamic groups. Symmetric key cryptography provides secure communication with group keys being distributed by trusted group leaders. This scheme ensures privacy, non repudiation and authentication of senders with groups being maintained with small sets of control messages. The electronic license plate information which maps all relevant information about the car, driver and a pseudonym is stored in the form of a unique identifier. A Transportation Authority (TA) maintains identifier to pseudonym. Every vehicle is loaded with a subset of certificates which are periodically replaced with new ones from the pool of certificates maintained by the TA. Key exchange between nodes is achieved with the application of the Diffie Hellman Key agreement protocol [21]. Geodynamic groups are created with the help of distribution algorithms with nodes assuming any one of the following roles: 1. Group leader: The selected group leader periodically sends its group leader to all the members of the group and also periodically distributes a fresh group key to all group members. Messages within the group, to another group and to the TA go through the group leader.

2. Group member: A node can be a member of more than one group but can never be a group leader if it's a member of more than one group. A group member can create and send safety messages to members of a group.

3. Non member: A non member encrypts a search message with the public key of the law agency and broadcasts it to all the nodes in the region. A random number is also included in the search message. If the random number is smaller than that of one of the other members, it becomes a member else it becomes the leader of the group. Privacy of individuals is maintained while non repudiation is provided by the law agency when needed.

**A Novel Message Fabrication Detection (MEFAD) for Beaconless Routing**

The goal of the MEFAD scheme [19] is to prevent malicious in-transit packets or messages creating havoc in beaconless contention based routing (CBR). Vehicles in the same geographic region collaborate with each other to elect a trustworthy vehicle to forward packets to a destination. Every vehicle in the region participates in this contention based approach to elect a trustworthy forwarder. Malicious nodes can create falsified messages in order to intercept packets and this leads to lost or delayed packets. In the MEFAD scheme, when the source node broadcasts a packet to be forwarded to the destination, every neighboring node receiving this packet competes for obtaining the right to forward the packet. The vehicles set a timer which depends on their distance from the destination. The vehicle whose timer expires faster than that of every other vehicle gets the privilege to forward the packet. Every other vehicle has to drop that packet after a forwarder has been selected. This process is repeated till all the packets are successfully sent to the destination. Malicious nodes may take advantage of the use of timers to create fabricated time information in order to obtain forwarding rights.

The IREQ packets sent by the source have a source ID, source and destination position info and the Velocity of the source. The neighbors respond with a IREP packet containing their ID, sending time of the response packet, their position and their velocity (these can be exploited and modified by a malicious node). Once the right to forward is obtained, the packet is forwarded with a packet ID, timestamp and the packet data. In order to detect malicious nodes in the MEFAD scheme, each node assumes the role of decider, claimer or verifier. The decider is usually the source making the final forwarding decision. The claimer claims forwarding rights by sending the response packet to all the neighbors and the third role is that of the Verifier who has to be in the transmission range of the sender and claimer in order to verify the authenticity of the claimer.

### Message Authentication: ECDSA Based Approach

The Elliptic Curve Digital Signature Algorithm (ECDSA) [51] is a variant of the digital signature algorithm. The ECDSA scheme operates on elliptic curve groups with elliptic curve domain parameters mutually selected by source and destination nodes to generate public/private key pairs. The source and destination exchange some public and private information and generate a shared secret key based on the selected domain parameters. This scheme is known as the Elliptic Curve Diffie Hellman scheme. The source vehicle uses private and public (known to every node in the VANET) keys. A cryptographic hash function is used to encrypt the message and sender generates a signature pair using secret key, hashed message and domain parameter. This is encrypted with the source's private key and sent to the destination. The destination uses the source's public key to decrypt this message. The resulting signature is verified using the shared key and receiver's private key.

### TACKing together efficient Authentication

VANETs require an efficient On Board Unit (OBU) key management scheme that maintains sender validity, message integrity, short term linkability and long term unlinkability, traceability and revocability. Studer et al. [74] suggest the Temporary Anonymous Certified Keys (TACK) scheme which prevents mischievous nodes from linking vehicles different keys. Timely revocation of nodes and eavesdroppers is guaranteed while reducing overhead of vehicle to vehicle communication. An OBU ensures message integrity and short term linkability by signing a broadcast message using a short lived private/public key pair. The trusted central authority provides a short lived Certificate (a TACK) which identifies the owner of the key pair as a valid OBU.

The OBU uses a group key provided by the regional authority (RA) to produce a group signature which proves validity without revealing any OBU identifying information. A TACK is valid only till an OBU is within range of the issuing RSU. If it moves into the region of another RSU, it must prove its validity and request for a new TACK. Once a malicious node is detected the central authority creates a revocation token and sends it to all the RSUs. These tokens are generated with the help of the private/public key pair of the malicious node. All TACKs are short lived so that revoked OBUs can be removed in a timely fashion. RSU includes expiration time when signing a certificate. RSUs check revocation lists for the validity of an OBU when it receives a TACK request. It then uses the group signature and group public key to provide a new TACK to a valid OBU. This technique is efficient against Sybill attacks to spot mischievous nodes sending multiple TACK requests within a single acceptable time slot. The random number used for group signature time generation can be used to track back to OBUs sending multiple TACK requests. Additional bandwidth is required for TACK requests and updates. The most expensive operation was found to be the OBU-RSU short term key updates.

**S3P: A Secure and Privacy Protecting Protocol**

In S3P [3], the Public Key Infrastructure is used to provide anonymous and secure communications by identifying VANET nodes. Multiple Certificate Authorities (CAs) are used to manage identities and credentials with each node registered with only one local CA. The local CA issues a certificate with a unique ID, period of validity and a Public/Private Key pair. Compromised certificates have to be revoked by the CAs. Each vehicle maintains two key sets with the first one being used to sign safety messages and the other one being the emergency key set which is used in emergency situations. Digital signatures are replaced with Keyed hash mechanisms to balance

computational overhead. Each key pair is used once and key pair sets have to be refreshed after they have been exhausted. When a malicious node is detected, the CA sends a notification message to every node except the malicious one. When the nodes receive this notification message, they switch to the emergency key set. The ID of the malicious node is encrypted with its own public key and sent to all the nodes. The CA then generates new key sets and sends it to the notified nodes. The wait time for the new key set is minimal. The safety messages are usually encrypted with their long term private keys in order to prevent any node from denying sending a message. Safety messages contain timestamps which it signs with the help of its updated internal clock. All the nodes in the network maintain anonymity and achieve non repudiation with the help of this protocol.

The following table is a summary and comparison of the approaches reviewed in this section.

Table 1.1: Comparison of techniques

| **Approach** | **Security Mechanism** | **Objectives** | **Overhead** | **Scalability** |
|---|---|---|---|---|
| SOADV | Digital Signatures and Hash Chains | Authentication of signaling packets | Average | Average |
| SPAAR | Certificate Authority and timestamps | Authentication, integrity, non repudiation and confidentiality | Average | Good |
| GSIS | Group and ID based signatures | Conditional privacy, authentication | Average | Good |

| | | | | |
|---|---|---|---|---|
| Raya et al. scheme | Pairwise and Group based keys | Confidentiality | Low | Average |
| Harsch et al. scheme | Pairwise, group and session keys, rate limit mechanisms | Position based routing | High | High |
| Time and Location critical Emergency Message dissemination | Scalable modulation and coding | Emergency Message dissemination | Low | Average |
| Efficient Certificate Management in VANETs | Special certificates like valid and adversary certificates | Privacy, non repudiation and anonymity | Low | High |
| Proxy based signature based RSU message broadcasting | Proxy signatures | Privacy through unforgeable proxies | Average | Average |
| Global Public Key algorithm for secure location service | Bilinear pair based cryptography using group keys | Hop by hop authentication and end to end protection | Average | Good |

| | | | | |
|---|---|---|---|---|
| Delay efficient Geodynamic group based authentication | Group based Hybrid Authentication Protocol | Privacy of sender, authentication | High | Average |
| Protocol for anonymous authentication using smart cards | Smart cards on VSM with various symmetric encryption techniques, session keys | Non Repudiation and integrity of messages | Average | high |
| A novel message fabrication detection for beaconless routing | Contention based routing | Message Fabrication detection | High | Good |
| Message authentication: ECDSA based approach | Elliptic Curve Digital Signature Algorithm | Message Origin Authentication | Average | Good |
| TACKing together efficient authentication, revocation and privacy | Temporary Anonymous certified keys | Sender validation, short term linkability, long term unlinkability, traceability, revocability | Average | Low |

| | | | | |
|---|---|---|---|---|
| S3P: A Secure and Privacy protecting protocol for VANETs | Multiple certificate authorities and keyed hash mechanisms | Malicious node detection | Low | Average |

## 1.2 Motivation and Problem Addressed and Solved in the Dissertation

Vehicular ad hoc Networks (VANETs) allow vehicles to form a self-organized network. With benefits such as enhancing road safety, and user convenience, VANETs are likely to be widely deployed in the future, given the interest shown by industry in self-driving cars and satisfying their customers various interests. Vehicles could collect information such as road condition, accidents, available parking space in parking garages, etc. and those information could be used by other drivers for various purpose such as avoiding congested roads, finding vacant parking spaces, etc.

Problems related to Mobile ad hoc Networks (MANETs) have been extensively studied. Issues related to routing, security, etc. have been extensively studied for MANETs. Even though VANETs are special type of MANETs, solutions proposed for MANETs cannot be directly applied to VANETs because all problems related to MANETs have been studied for small networks; moreover, in MANETs, nodes can move randomly. On the other hand, movement of nodes in VANETs are constrained to roads and the numbers of nodes in VANETs is large and covers typically large area. Hence, it is very important to design security mechanisms to authenticate and verify transmitted messages while protecting user privacy and preventing malicious activities/attacks. Also, it's necessary to address selfish nodes problems in the hybrid VANET environments.

In this dissertation, we address and solve the following problems.

**Secure, authenticated, privacy preserving message dissemination in VANETs:** When vehicles discover incidents or observe phenomena such as accidents, congestion, icy road condition, etc., they need to disseminate this information to vehicles in appropriate areas so the drivers of those vehicles can take appropriate action. When such messages are disseminated, the authenticity of the vehicles disseminating such messages should be verified and the integrity of the messages should be guaranteed while at the same time the anonymity of the vehicles (drivers) should be preserved. In addition, legal authorities should be able to trace the messages to their senders when necessary. (e.g. reconstructing accidents, spreading malicious messages, etc.) In this dissertation, we present an efficient protocol for the dissemination of authenticated messages [41] which utilized the RSUs that have higher computation power. Our scheme preserves the anonymity of the vehicles while at the same time allows legal authorities trace the messages to the message sender when necessary.

**Incentive-based architecture for vehicular cloud:** Cloud computing has gained lots of attention in recent years because it provides advantages such as flexibility and availability. Allowing vehicles in VANETs to store the collected information in the cloud would facilitate other vehicles retrieve this information when they need; moreover, the cloud owner can delete obsolete information and use the information for various purposes such as traffic management, parking management. etc. Also, underutilized resources of vehicles such as communication, computation, storage, could be used by Vehicular Cloud. For this, we present a secure incentive-based architecture for vehicular cloud [39]. Our architecture allows vehicles to collect and store information in the cloud; it also provides a mechanism for rewarding vehicles that contributing to the cloud.

**Privacy preserving message dissemination in VANETs:** There are various types of messages in VANETs and sometimes, it is sufficient to ensure the anonymity of the vehicles disseminating messages and encryption of messages is not necessary. In order to protect user location privacy, we present a privacy preserving message dissemination protocol for VANETs without using traditional cryptography [42].

## 1.3 Organization of the Dissertation

The remainder of this dissertation is organized as follows.

- In Chapter 2, we present an efficient protocol for propagating the phenomena observed by vehicles in VANETs to vehicles in appropriate regions so they can use them to make informed decision. Our protocol utilizes RSUs that have higher computation power than OBUs to authenticate and disseminate the messages about the phenomena observed by vehicles within an RSU's transmission range.

- In Chapter 3, we present an architecture for vehicular cloud and an incentive based solution, called secure token reward system, to entice vehicular nodes to participate in the network.

- In Chapter 4, we present a scheme to preserve user location privacy for vehicular communication using non-negative matrix factorization. This scheme does not require traditional cryptography to protect privacy while it can still calculate the location of the event occurred.

- Chapter 5 summarizes the results and discusses the future research directions.

## Chapter 2

## An Efficient Protocol for Authenticated and Secure Message Delivery in Vehicular Ad Hoc Networks

In Vehicular Ad Hoc Networks (VANETs), anonymity of the nodes sending messages should be preserved, while at the same time the law enforcement agencies should be able to trace the messages to the senders when necessary. It is also necessary that the messages sent are authenticated and delivered to the vehicles in the relevant areas quickly. In this chapter, we present an efficient protocol for fast dissemination of authenticated messages in VANETs. It ensures the anonymity of the senders and also provides mechanism for law enforcement agencies to trace the messages to their senders, when necessary.

### 2.1 Background and Related Works

In the past, several researchers addressed the security issues in VANETs. Raya et al. [63] proposed a protocol in which each vehicle needs to be preloaded with a large number of private keys, as well as their corresponding anonymous certificates. However, with limited storage space of On-Boars-Units (OBUs) of the vehicles and the nature of highly dynamic network, this is not suitable for VANETs. In [44], a security protocol based on group signature and identity-based signature scheme was proposed to meet the unique requirements of vehicular communication networks. This protocol addressed privacy issues with traceability, so real identity of vehicles are traceable for

resolving a dispute. However, the verification of each group signature may cause high computation overhead when the density of the traffic increases. In [86], a spontaneous privacy-preserving protocol based on revocable ring signature with a feature for authenticating the safety messages locally; but this scheme is not scalable because every vehicle, with limited computation power, needs to participate in message verification process. In [48], an ID-based authentication framework with adaptive privacy preservation for VANETs is proposed using adaptive self-generated pseudonyms as identifiers. Hao et al. [29] proposed a cooperative message authentication protocol for VANETs to alleviate vehicles' computation burden by allowing vehicles to share verification tasks. Hsiao et al. [81] proposed an efficient broadcast authentication scheme to reduce communication and computation overhead using fast authentication and selective authentication.

In a more recent work [43], Lin et al. proposed a cooperative authentication scheme for VANETs using an evidence-token approach to distribute the authentication workload, without direct involvement of a trusted authority (TA). The vehicles obtain an evidence token as they make contribution to the network and benefits are given to nodes based on the tokens. Wang et al. [31] proposed an accelerated secure in-network aggregation strategy to accelerate message verification and reduce computational overhead using the aggregation structure and TESLA scheme.

Although the studies mentioned above solved the security and privacy issues to different extent, scalability issue has not been addressed well. Also, authenticated messages are not disseminated efficiently under the above algorithms. RAISE [89], also tried to address these issues with the help of RSUs, but under their approach, RSUs must notify all other vehicles whether a message from a particular vehicle is valid or not which results in message overhead. Wu et al. [85] proposed a message authentication scheme for intra and inter RSU range using RID key table with all RSUs' ID and session keys. Priya et al. [62] proposed a group authentication protocol to

address group authentication and conditional privacy. These schemes reduced communication overhead significantly with the aid of the RSU, but efficient dissemination of messages still remains as issues. We propose an efficient message authentication protocol which overcomes these problems. In our protocol, RSUs not only authenticate messages sent by vehicles fast, but also disseminate messages through the other RSUs to the vehicles in the appropriate areas quickly. Also, in order to efficiently secure messages when forwarded, our approach uses the basic idea behind the onion routing scheme [27] for signing and forwarding messages to the nearby RSUs.

The rest of the chapter is organized as follows. Section 2.2 introduces the system model, assumptions, problem statement and solution objectives. Section 2.3 presents our proposed protocol in detail. In Section 2.4 we present an analysis of our protocol. Finally, we summarize the results in Section 2.5.

## 2.2 System Model

In this section, we introduce the system model, assumptions, problem statement and solution objectives.

### 2.2.1 System Model

We assume that the following three types of entities exist in the network: a Trusted Authority (TA), Road Side Units (RSUs), and On Board Units (OBUs).

- **Trusted Authority (TA):** The TA issues certificates for vehicles. It also manages all private information about vehicles including certificates and shares them securely with RSUs upon request. The TA and the RSUs are able to communicate with each other securely via wired or wireless network, so the RSUs can verify vehicles' certificate with the TA and also can obtain identities of vehicles from the TA when investigations are required by legal authorities.

- **Road Side Units (RSUs):** The RSUs are located along the roads and play an important role in verifying the authenticity and integrity of messages sent by vehicles and forwarding them to other RSUs as well as vehicles within its transmission range. Each RSU also stores private information about vehicles such as identity (ID), pseudo ID, public key, shared key and timestamp in a tamper proof device. In addition, each RSU creates a group key and shares it with all vehicles within its transmission range, so the RSU can encrypt messages using the group key and broadcast them to the vehicles within its transmission range. The group key is updated periodically. All the RSUs in the system are assumed to be connected by a network so an RSU can disseminate a message to vehicles in any region quickly. For simplicity, we assume that all RSUs have same transmission range.

- **On Board Units (OBUs):** An OBU, installed on the vehicles, is assumed to have significantly shorter communication range and less computation power than RSUs.

### 2.2.2 Assumptions

We assume that any vehicle that is within a target RSU's transmission range is capable of sending/forwarding messages to the RSU through other vehicles using a routing protocol suitable for VANETs [4, 47, 70, 77]. RSUs have larger storage space and computation power than OBUs. Also, RSUs are connected to each other through wired or wireless network. Hence, our protocol utilizes RSUs not only to verify the authenticity and integrity of the messages received from vehicles, but also to disseminate those messages to the vehicles in appropriate regions through other RSUs, when necessary. A scenario of how a message is forwarded to an RSU by a vehicle for authentication and further dissemination is illustrated in Figure 2.1. Figure 2.2 illustrates how an RSU disseminates an authenticated message to vehicles

in appropriate regions through other RSUs.

We also make the following assumptions.

1. The TA and RSUs are totally trusted and are assumed to be not compromised.

2. When a vehicle is registered, the locations of RSUs and their public keys are stored in the OBUs installed in the vehicles and they are updated during renewal of vehicle registration. So, at any given time, an OBU knows the nearest RSU.

### 2.2.3 Problem Statement and Solution Objectives

When a vehicle senses an incident such as accident, bad road condition due to weather, traffic jam, etc., it needs to send that information to vehicles in appropriate regions so their drivers (or vehicles themselves, if they are self driving) can take appropriate action. When such messages are sent, the integrity and authenticity of the messages sent by the vehicles should be verified while at the same time the anonymity of the senders of these messages should be preserved. i.e, the identities of the vehicles (or drivers) should not be revealed to any other vehicle (driver). The proposed method should be scalable. The protocol should take into consideration the limited computation power of the OBUs. Also, retaining satisfactory security is essential as attacks to the network can be very dangerous and life-threatening to drivers due to the nature of messages in VANET, so the protocol should prevent possible attacks, which will be discussed in section 2.4. If a RSU is not within the transmission range of vehicles sending messages, the original messages are forwarded to the RSU through other vehicles, hence the protocol should be robust against malicious nodes in the network. In this chapter, we present a protocol which addresses and solves all of the above problems.

To preserve the anonymity of the vehicles, our protocol uses pseudo IDs of the vehicles for message transmission. Since RSUs have more computation power, authentication of messages and dissemination of messages are carried out by the RSUs.

Since message dissemination is carried out by RSUs, the protocol is scalable and messages are not unnecessarily broadcasted to vehicles in regions that do not require the message.

Our goal is to design a protocol which achieves the following objectives.

- **Privacy preservation:** During the transmission of a message, identities of the vehicles transmitting the message should be protected. However, when the authorities need to obtain user information for legal investigation, they should be able to do so.
- **Message integrity:** Integrity of messages should be ensured during the transmission of messages. No one in the middle should be able to modify the messages transmitted.
- **Source authentication:** The source of messages should be efficiently authenticated to prevent impersonation attack.
- **Low storage space usage:** OBUs have limited storage space, so its usage requirement should be low for the transmission and the verification of messages.
- **Low communication overhead:** All communication should be done with low overhead.
- **Fast verification and efficient dissemination:** Messages should be verified within a short time and disseminated quickly and efficiently to appropriate users, even to users in another RSU's area.

Next, we describe our protocol in detail.

## 2.3 Proposed Protocol

In this section, we first present the basic idea behind our protocol and then describe the protocol in detail. The notations used in this chapter are listed in Table 2.1.

### 2.3.1 Basic Idea Behind our Protocol

The proposed protocol has the following phases:

- **Phase 1: Group Key and Symmetric key Establishment.** When a vehicle leaves the area covered by an RSU and enters an area covered by another RSU, it initiates communication with the new RSU and establishes a shared symmetric key with the new RSU so it can send encrypted messages using the symmetric key to the nearby RSU. It also gets its pseudo ID and the group key from the RSU. The group key is used by the RSU to encrypt messages and send them to the vehicles in the area covered by the RSU. A vehicle uses its pseudo ID in all communications. Here, by the area covered by an RSU, we mean the area that lies within the transmission range of the RSU.

- **Phase 2: Vehicles Sending Messages to RSU for Dissemination:** After completing Phase 1, a vehicle can send messages to the RSU. It uses the shared symmetric key established in Phase 1 to encrypt the message as well as compute the digest of the messages it sends. This message digest helps the RSU in verifying the authenticity and the integrity of the messages. Note that the RSU to which the message is sent may not be within the transmission range of the vehicle sending a message and hence a routing algorithm is used for routing the messages to the RSU through intermediate nodes.

- **Phase 3: Verification and Dissemination of Messages by RSUs:**. When an RSU receives the messages sent by the vehicles, it verifies the authenticity and integrity of the messages and forwards the messages to the vehicles in appropriate regions either directly (to vehicles within its transmission range) or through other RSUs.

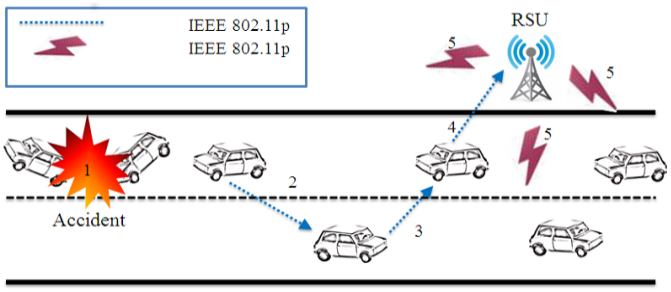


Figure 2.1: Message Forwarding

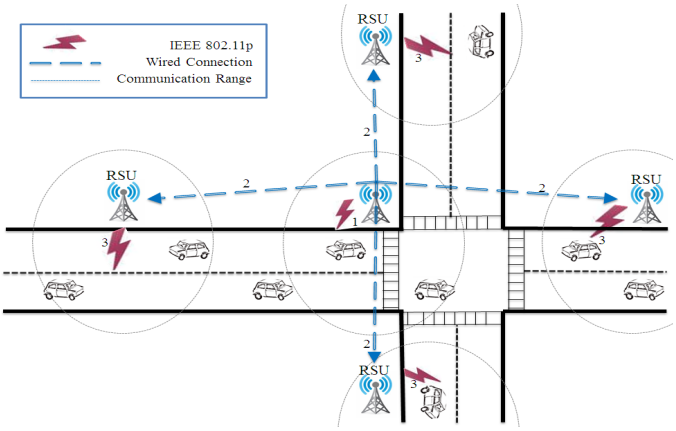


Figure 2.2: Disseminating Messages Through Neighboring RSUs

### 2.3.2 Group key and Symmetric key Establishment

When a vehicle $V_i$ leaves the region covered by an RSU and enters a region covered by a different RSU, say $R_j$, it initiates the key establishment process (illustrated in Figure 2.3). The key establishment process is based on the Diffie-Hellman key agreement protocol [21]. $V_i$ initiates mutual authentication and key establishment by sending the message $g, p, A$, $\{g, p, A\}SK_{V_i}, C_{V_i}$. In this message, $\{A, B, g, p\ \}$ are elements of the Diffie-Hellman key agreement protocol: $p$ is a prime number, $g$ is primitive root $mod\ p$, $A = g^a\ mod\ p$, $a$ is the secret integer kept by $V_i$, $C_{V_i}$ is the certificate of $V_i$, $g, p, A$ is encrypted with the private key $SK_{V_i}$ of $V_i$ so that the RSU can authenticate $V_i$ by decrypting it using the public key $PK_{V_i}$ of $V_i$. Upon receiving this message, the RSU $R_j$ concatenates the pseudo ID $PID_{V_i}$ of $V_i$, the number $B = g^b \mod p$ ($b$ kept secret by $R_j$), the group ID $GID_j$ and the group key $K_{G_j}$ and encrypts all this with the public key $PK_{V_i}$ of $V_i$ and sends it to $V_i$ along with its certificate $C_{R_j}$. Note that $A \| B \| T_s$ are encrypted using RSU's private key, which means that only authentic RSU can generate this message, hence a fake RSU attack is prevented. Finally, $V_i$ sends an acknowledgment for having received $B$. Thereafter $g^{ab}$ serves as the secret key $K_{V_i\_R_j}$ between $V_i$ and $R_j$ and $K_{G_j}$ is the group key used by $R_j$ for encrypting and sending messages to all vehicles in its region. This completes the mutual authentication and key establishment phase and $R_j$ updates its group table which contains pseudo IDs, original IDs, certificates, shared secret keys. Note that we assume that a routing algorithm is used for forwarding messages from $V_i$ to $R_j$ because $R_j$ may not be within the transmission range of $V_i$. Note that timestamp $T_s$ is attached to every message to prevent the replay attack.

### 2.3.3 Vehicles Sending Messages to RSU for Dissemination

After the key establishment phase between a vehicle $V_i$ and an RSU $R_j$, $V_i$ can send messages to $R_j$ securely and without revealing its identity as follows. When $V_i$ wants

$$V_i \rightarrow R_j : g, p, A, \{g, p, A \| T_s\} SK_{V_i}, C_{V_i}$$

$$R_j \rightarrow V_i : \{PID_{V_i} \| B \| GID_j \| K_{G_j}\} PK_{V_i},$$
$$\{A \| B \| T_s\} SK_{R_j}, C_{R_j}$$

$$V_i \rightarrow R_j : \{B \| T_s\} SK_{V_i}$$

Figure 2.3: Key Establishment Process

to send a message $M$ about a sensed event, it computes $M_i$ from $M$ as follows and sends it to $R_j$.

$$M_i = ID_{R_j}, PID_{V_i}, \{M, T_s, S_q\} K_{V_i\_R_j}$$

To compute $M_i$, the secret key $K_{V_i\_R_j}$, established between $V_i$ and $R_j$ is used to encrypt the message $M$, the sequence number of the message $S_q$ and the timestamp $T_s$; the pseudo ID $PID_{V_i}$ of $V_i$ is also appended. Note that when $R_j$ receives the message, it will be able to verify the authenticity of the sender and the integrity of the message based on the pseudo ID and the secret key used for encryption. However, since $R_j$ may not be within the transmission range of $V_i$, the message may have to be routed through other intermediate nodes using the available routing algorithm. We must make sure that the destination RSU $R_j$ is able to authenticate all the intermediate nodes forwarding this message. For that purpose, we adopt the onion signature scheme [64]. With onion signature, every vehicle forwarding message simply appends a signature of received message and forwards it towards the destination RSU. When an intermediate vehicle $V_j$ receives the message $M_i$ FROM $V_i$, it computes $M_j$, by attaching its signature as follows and forwards it to the next hop on the route.

$$M_j = ID_{RSU}, PID_{V_j}, M_i, dgt_j$$

where the digital signature $dgt_j = E\Big(H(M_i), K_{V_j\_RSU}\Big)$ is obtained by computing the hash of the received message $M_i$ and encrypting it using the shared key of $V_j$ and the

destination RSU. This process is repeated until the message reaches the destination RSU.

### 2.3.4 Verification and Dissemination of Messages by RSUs

When an RSU receives a message sent by a vehicle $V_i$, since it has a shared key with each vehicle which forwarded the message, it can decrypt the signatures attached by all nodes on the route one by one and verify the authenticity of each node and the integrity of the message received. After it verifies the authenticity and integrity of the message, it disseminates the message to the vehicles in appropriate regions. Since the RSUs have higher computation power than the OBUs, RSUs can verify messages more quickly than OBUs. After checking the integrity and authenticity of a message received from a vehicle, the RSU, say $R_i$, determines the areas to which the message needs to be propagated. If it needs to be propagated to only vehicles within its transmission range, then it computes the digest $dgt_i = E\Big(H(M), SK_{R_i}\Big)$ of the message $M$ by encrypting the hash of $M$. Then it encrypts the message, sequence number and the digest using the group key $K_{G_i}$ as

$$M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$$

and broadcasts to all vehicles within its transmission range. If the message needs to be propagated to vehicles that are not within its transmission range, then it computes $M_{type2}$ as

$$\begin{aligned} M_{type2} = ID_{receiver\_RSU}, ID_{sender\_RSU}, \\ \{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU} \\ \text{where } dgt_i = E\Big(H(M), SK_{R_i}\Big) \end{aligned}$$

and sends the message to the respective neighboring RSUs by setting the number of hops $h$ (i.e., the number of RSUs, through which the message needs to propagate)

to the appropriate value. When an RSU receives this message, it decrements the value of $h$ by 1 and forwards it to its neighbors if $h > 1$. Based on the nature of the message, an intermediate RSU can decide whether or not to disseminate the message to the vehicles within its transmission range. The detailed algorithm is given in Figure 2.4.

### 2.3.5 Discussion

Under our algorithm, when a vehicle enters a region covered by an RSU (i.e., the area that lies within the transmission range of the RSU), it initiates key establishment with the RSU and establishes a symmetric key with the RSU so that it can encrypt all the messages it needs to send to the RSU while in its region. It also obtains a pseudo ID and the group ID and group key. The vehicle uses only its pseudo ID in all communications and hence the anonymity of the vehicle is preserved. The RSU uses the group key to encrypt messages it sends to the vehicles in its region. So all messages are encrypted and no intruder can decrypt the messages. Vehicles do not broadcast messages for disseminating observed phenomena to other vehicles; instead, they use nearby RSU to disseminate the messages on their behalf. When a vehicle senses an event and wants to disseminate it to other vehicles in specific regions, it simply sends it to the nearby RSU (through the intermediate vehicles using available routing algorithm, if the RSU is not within the vehicle's transmission range). The nearby RSU authenticates the vehicle sending the message, checks the integrity of the message and then disseminates the message to the vehicles in the relevant regions through other RSUs. When a message sent by a vehicle needs to be traced to the vehicles sending the message, it can be done with the help of the RSUs because the RSUs maintain the table binding the pseudo IDs of the vehicles to their real IDs.

A vehicle never broadcasts any message to other vehicles. Dissemination of messages to other vehicles is the responsibility of the RSUs and hence this approach is scalable. Messages exchanged are generally small so OBUs can use symmetric key for

When a vehicle $V_i$ wants to send a message $M$ to the nearby RSU,
*Let* $M_i = ID_{RSU}, PID_{V_i}, \{M, T_s, S_q\}K_{V_i\_RSU}$
Send $M_i$ to the next hop towards the RSU

When a vehicle $V_j$ receives the message $M_i$ from $V_i$,
*Let* $M_j = ID_{RSU}, PID_{V_j}, M_i, dgt_j$,
    where $dgt_j = E(H(M_i), K_{V_j\_RSU})$
Send $M_j$ to the next hop towards the RSU

When an RSU with id $ID_{RSU_i}$ receives a message $M_k$ from vehicle $V_k$,
It peels of the onion $M_k$, and retrieves the message $M$
Sets $h$ based on nature of message
*Let* $M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$,
    where $dgt_i = E(H(M), SK_{R_i})$
Disseminate $M_{type1}$ to all vehicles in the table if needed
**if** $h > 0$ **then**
    $h = h - 1$
    *Let* $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_i}$,
    $\{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU}$,
        where $dgt_i = E(H(M), SK_{RSU_i})$
    Forward $M_{type2}$ to relevant neighboring RSUs
**end if**

When an RSU with id $ID_{RSU_j}$ receives a message $M_{type2}$ from a neighboring RSU with ID $ID_{RSU_i}$,
Decrypt $M_{type2}$ and retrieve $M$
*Let* $M_{type1} = GID_j, \{M, Ts, Sq, dgt_j\}K_{G_j}$,
    where $dgt_j = E(H(M), SK_{RSU_j})$
Disseminate $M_{type1}$ to all vehicles in the table
**if** $h > 0$ **then**
    $h = h - 1$
    *Let* $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_j}$,
    $\{M, Ts, Sq, h, dgt_j\}PK_{receiver\_RSU}$,
        where $dgt_j = E(H(M), SK_{R_j})$
    Forward $M_{type2}$ to relevant RSUs
**end if**

When a vehicle $V$ receives a message $M_{type1}$ from an $RSU$,
Decrypts the message $M_{type1}$ using group key
and consumes it

Figure 2.4: The Algorithm

encryption without incurring much computation overhead and RSUs can use the public key of receiving RSUs for encrypting and sending messages to them; however, the algorithm can be easily modified so that the RSUs use symmetric key for encryption after establishing a shared symmetric key with the receiving RSUs.

## 2.4 Comparison with Related Work and Security Analysis

### 2.4.1 Comparison with Existing Related Works

In this section, we compare our protocol with some existing related works. The protocol proposed in [63] ensures secure communication of messages. But, it is not scalable because each vehicle needs to be preloaded with private keys of all other vehicles and their corresponding anonymous certificates. As the number of vehicles grows in the network, not only maintaining those security data is difficult, but also storage issues may occur due to the large number of private keys and certificates that need to be stored in the limited storage space available in OBUs. In contrast, in our protocol, vehicles do not need to store other vehicles' private keys and their certificates to authenticate messages since RSUs authenticate messages on behalf of vehicles, thus the storage requirements is very low compared to aforementioned protocol.

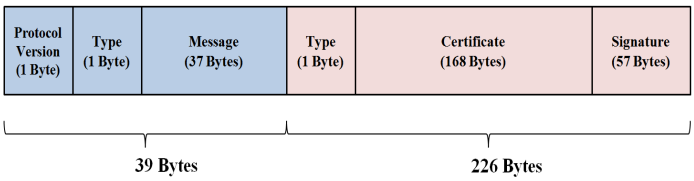


Figure 2.5: The Format of a Signed Message in IEEE Standard

When a vehicle sends a message, a certificate and a signature is attached to the message in order to authenticate the message and ensure the integrity of the message. Figure 2.5 shows the format of a signed message derived from IEEE 1609.2 Standard [73]; the size of a message is 265 bytes including 39-Bytes of unsigned message field, 169-Bytes of a certificate, and 57-Bytes of signature.

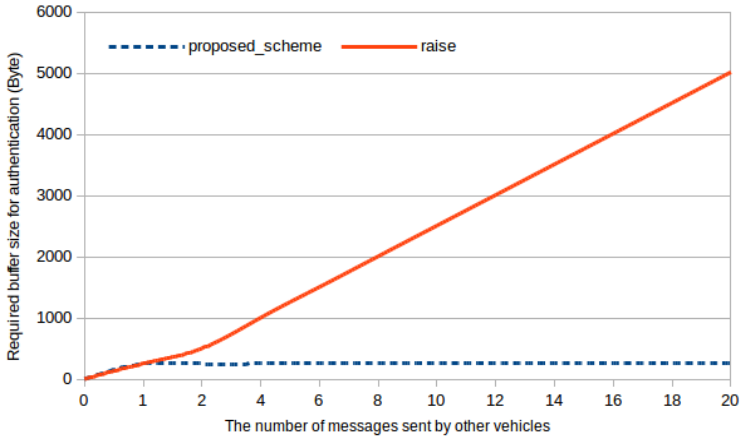


Figure 2.6: Storage Usage vs. Traffic Load

Figure 2.6 shows the relationship between the storage usage and traffic load. The storage usage represents the buffer size required on OBUs for messages waiting to be authenticated and the traffic load represents the number of messages sent by other vehicles. Since each signed message is 265 Bytes long, the necessary buffer size for storing the unauthenticated messages increases under RAISE [89] as the traffic load increases whereas under our protocol the required buffer size for storing the received message is constant. RAISE performs better than the PKI based protocol [73] and group signature protocol [44] in terms of packet loss, packet delay, and communication overhead because the vehicles can simply authenticate messages once validation messages are received from the RSU; however, each vehicle has to buffer all messages received from other vehicles until validation messages arrive. Thus, the vehicles require more buffer space as message traffic increases. Hence, the required buffer space is proportional to traffic load. On the other hand, our protocol does not keep messages in the buffer of OBUs until they are authenticated as RSUs directly send authenticated messages to vehicles. Thus, under our protocol, buffer required for storing messages at OBUs does not increase as the traffic load increases.

Under our protocol, messages sent by vehicles do not need to be authenticated and verified by other vehicles; authentication of messages is done by RSUs which

have higher computation power as well as lager storage than OBUs in vehicles. Figures [2.7,2.8,2.9] compare RAISE [89] and our protocol with respect to the number of retransmissions and the number of original messages sent as the number of vehicles participating varies from 10 to 30 in the network. The number of message transmissions under our protocol is obtained using the following equation:

$$T_n^1 = (V_n * M_n) * 1B + (M_n + 1U), \tag{2.1}$$

where $T_n^1$ is the number of messages sent, $V_n$ is the number of vehicles in the network, $1B$ is 1 broadcast and $1U$ is 1 unicast. And the number of message transmissions for RAISE is obtained using the following equation:

$$T_n^2 = (V_n * M_n) * 2B, \tag{2.2}$$

where $T_n^2$ is the number of message communication, $V_n$ is the number of vehicles in the network, and $2B$ is 2 broadcasts. Under RAISE, every message is stored in each vehicle until a validation message from the RSU arrives, so vehicles sending a message broadcast it once and the RSU broadcasts it again after verifying the message. *However, under our protocol, in order to minimize the communication overhead, vehicles sending a message just unicasts it to the RSU and only the RSU broadcasts the verified message to the vehicles in relevant areas (through other RSUs, if necessary). So, under our protocol, the number of message retransmissions is minimized and this reduction clearly becomes prominent as the number of vehicles sending messages increases.*

There are other approaches [31, 62, 81, 85] to address communication and computational overhead. Hsiao [31], proposed a scheme that addressed excessive signature verification requests by exploiting sender's ability to predict its own future beacons and quickly spreading bogus signatures. Using fast authentication and selective au-

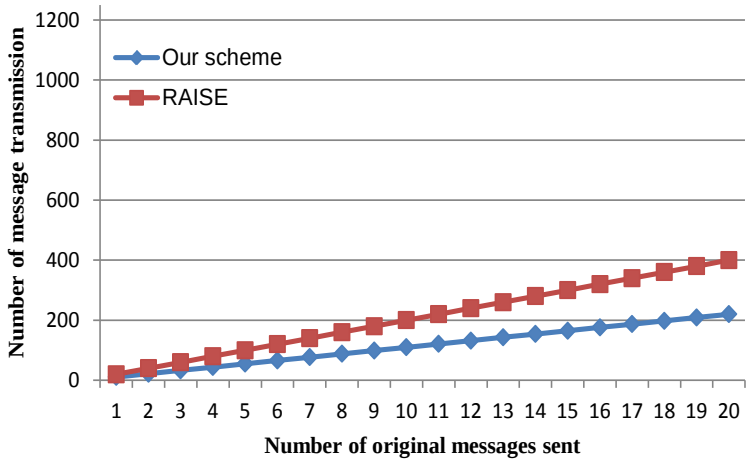


Figure 2.7: Number of Message Transmissions with 10 Vehicles

thentication, their scheme significantly reduced the consumption of the computational resources. However, receivers still need to verify messages received from other vehicles with their limited computation resource. In our scheme, vehicles do not need to verify all messages received. messages are first verified by a RSU, and then disseminated to the network, hence communication overhead is much less because vehicles only need to verify messages received from RSU, not from other vehicles. In [81], an accelerated secure in-network aggregation strategy is proposed to expedite message verification and reduce communication overhead. The scheme uses the aggregation structure to detect potential misbehavior and TESLA-based broadcast authentication scheme to avoid expensive cryptography. However, the TESLA is not suitable for dynamic and time critical environment of VANET as delay in verification process is unavoidable with it. So, receivers need to wait until it receives the key to read the received message earlier even if it's very time sensitive message. The situation may get worse if the sender vehicle and the receiver vehicle are traveling in opposite direction because it might cause delay of the message delivery or even message lost. In our scheme, when RSUs send messages to vehicles, they use group key, therefore, once a vehicle obtains a group key RSU, computation overhead for verification is significantly reduced.

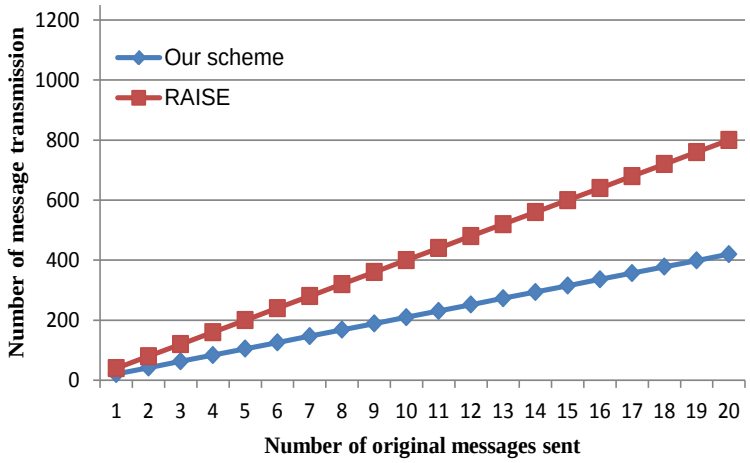


Figure 2.8: Number of Message transmissions with 20 Vehicles

Wu et al. [85] proposed a message authentication scheme with the aid of RSU; however, it is assumed that all vehicles maintain a RSU key table where all RSUs' IDs and session keys are stored, which makes this scheme not scalable. It is also assumed that all vehicles are reachable to RSU in one-hop communication, but it would require dense deployment of RSUs which is unlikely to happen in the near future. In addition, if a receiver is not within the transmission range of the same RSU, then the receiver needs to send another message for corresponding RSU's information to the sender and then needs to verify the message with a RSU in its region. This causes 4-way communication and it's not suitable for high mobility of VANET because the receiver must stay within its RSU's region until it receives a requested message from the sender to verify the message with the RSU. In our scheme, verified messages are quickly disseminated through neighboring RSUs and vehicles within the transmission range of other RSUs do not directly send a request to the sender and verify with another RSU within its transmission range. The message is verified by the first RSU once and if it's verified, then the message is immediately disseminated to appropriate regions. Priay et al. [62] proposed a group authentication protocol to address verifying a large number of messages and improving message loss ratio. However, this scheme

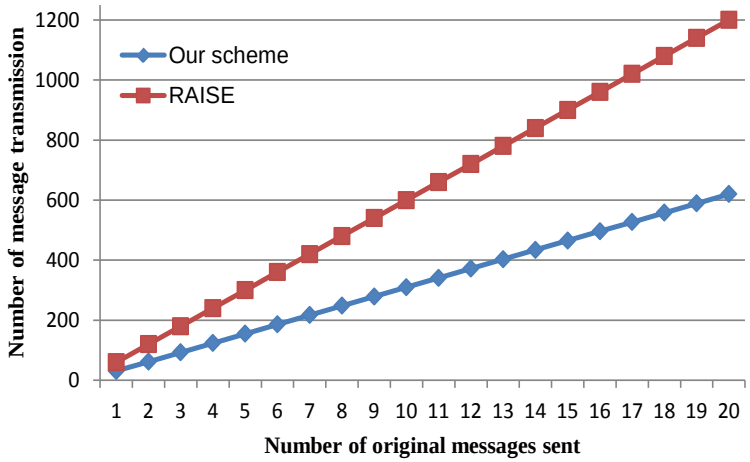


Figure 2.9: Number of Message Transmissions with 30 Vehicles

also does not address the situation when messages need to be forwarded to reach a destination RSU. Also, vehicles outside of transmission range of sender's RSU and in another RSUs are not addressed, hence this scheme is not scalable unlike our scheme.

### 2.4.2 Preventing Propagation of Redundant Messages

In existing algorithms, when a vehicle observes a phenomena, it disseminates the observed phenomena to all the vehicles in relevant regions. This approach can result in the propagation of redundant messages; this is because several vehicles may observe the same phenomena and propagate the same message. *However, under our protocol, observed phenomena are only sent to the RSU for further dissemination. So, RSUs can determine the redundant messages and suppress the propagation of redundant messages through other RSUs, if necessary. Moreover, this approach is more efficient because the RSUs can help in propagating the messages to vehicles far away faster.*

### 2.4.3 Message Integrity

When a node senses an event, it sends a message to the nearby RSU about the event so that the RSU can forward the message to the respective regions. The message is en-

crypted with the shared key between the vehicle and the RSU. When an intermediate vehicle receives the message, it computes the digest of the received message, encrypts the digest using its shared key with the RSU and forwards it to the next hop towards the RSU. This allows the RSU receiving the message to verify the authenticity of each vehicle through which the message traveled as well as the integrity of the message; the RSU then forwards the message to the vehicles in its region and/or other regions through other RSUs, as is necessary. Messages broadcasted by the RSUs to vehicles in their regions are encrypted using the group key. So, the integrity of the messages as well as the privacy of the vehicles are preserved.

### 2.4.4 Source Authentication and Privacy

Every vehicle is assigned a pseudo ID and symmetric key by the nearby RSU. Also, an RSU maintains a table that contains pseudo IDs, original IDs, certificates, shared secret keys and timestamps of all vehicles within its transmission range. If a message sent from a pseudo ID can be decrypted by the RSU that receives the message using the corresponding shared secret key, then the RSU can find the ID associated with the pseudo ID from its table and authenticate the source. A vehicle never uses its real ID in any communication and hence the anonymity of the vehicle is preserved. Also, a new pseudo ID is issued when a a vehicle enters another RSU's region and the issued pseudo ID is re-issued frequently if a vehicle stays in a RSU's region for a long time to prevent tracking of the vehicle associated with the pseudo ID.

### 2.4.5 Computation Overhead

Vehicles simply forward messages to an RSU by attaching its signature for verification and only the RSU verifies authenticity of the messages. When vehicles receive messages from an RSU encrypted using the group key, they simply decrypt the message and consume the message; this reduces the computation overhead on the OBUs

because there is no authentication Using public key cryptography involved, unlike RAISE [89].

### 2.4.6 Fast Verification and Efficient Dissemination

In our protocol, the authenticity and integrity of the messages are verified by RSUs that have higher computation power than OBUs. Also, they can communicate with neighboring RSUs securely via wired or wireless connection. Thus, messages can be verified and disseminated quickly through other RSUs to vehicles in appropriate regions. Therefore, fast verification and efficient dissemination are achieved. Moreover, RSUs can suppress duplicate messages sent by vehicles in the same region (i.e., messages about the observation of the same event by different vehicles in the same region).

### 2.4.7 Man in the Middle Attack

The symmetric key establishment process in our protocol uses the Diffie-Hellman key agreement protocol. Even though Diffie-Hellman key agreement protocol is vulnerable to man-in-the-middle attack [67], our protocol does not suffer from this weakness because of the following reasons: When a vehicle $V_i$ enters the region covered by an RSU, it encrypts $g, p, A$ and the timestamp $T_s$ using its private key $PK_{V_i}$. An intermediate vehicle can carry out the man-in-the-middle attack only if it is also an authentic vehicle which has a (public, private) key pair already established by the TA, in which case the RSU can trace the messages to the intruder.

### 2.4.8 Other Attacks

VANETs are prone to other types of attacks [53] and their consequences may be detrimental to the users. In this section, we discuss how our protocol prevents such attacks.

1. **Sybil attack:** This is a type of security threat that exists when a malicious node can present multiple identities at once. In our protocol, each vehicle is assigned a pseudo ID by an RSU after its certificate is verified and vehicles encrypt outgoing messages using symmetric key established with the RSU. Hence, a malicious node cannot use multiple identities at once.

2. **Replay attack:** In this attack, an attacker keeps a message that was sent earlier and tries to use the same message later by rebroadcasting it. In order to prevent the replay attack, every message in our protocol uses a timestamp to guarantee the freshness of the message. This requires loose synchronization of the clocks. Given the widespread use of GPS devices, they can be used for synchronizing clocks.

3. **Message fabrication/alteration attack:** In this attack, an attacker tries to modify, delete, or alter existing messages. In our protocol, when a vehicle sends a message, it attaches its digital signature that is obtained by computing the hash of the original message and encrypting it with its private key. Since only the sender can create its signature, an RSU (receiver) can verify the integrity of the message received using the signature. Hence, fabrication/alteration attack is prevented. However, if a vehicle is not willing to forward a message sent by another vehicle, it can deleted the message. Handling nodes that do not cooperate has been extensively studied in the context of ad hoc networks. Similar mechanisms can be used for handling such attacks.

4. **Malicious relay nodes:** In our protocol, every vehicle forwarding a message simply appends its signature to the received message and forwards it toward the destination RSU, vehicles on the route are not able to read or modify received message. So, malicious nodes cannot modify the message.

5. **Fake RSU attack:** An adversary may pretend to be a real RSU in this type of attack. In our protocol, however, a fake RSU attack is infeasible because a RSU appends its signature using its private key during symmetric key establishment process so the receiver knows who actually sent the signed message by decrypting it using the RSU's public key. Hence the fake RSU attack is prevented.

## 2.5 Summary

In this chapter, we presented an efficient protocol for propagating the phenomena (such as accidents, road conditions, etc) observed by vehicles in VANETs to vehicles in appropriate regions so they can use them to make informed decision. Our protocol utilizes RSUs that have higher computation power than OBUs to disseminate authenticated messages sent by vehicles within the RSU's transmission range. Since multiple vehicles within the transmission range of an RSU can observe the same phenomenon and inform the RSU about it, the RSU can suppress these messages about the observation of the same phenomenon from disseminating further. Moreover, in our approach, the RSUs have the ability to verify the authenticity of the sender and the integrity of the message before disseminating it to the other vehicles. Our approach preserves the anonymity of the senders while at the same time helps to trace a message to its sender, when required by the law enforcement agencies.

Table 2.1: Notations

| Notation | Description |
|---|---|
| $R_i$ | an RSU |
| $V_i$ | a vehicle |
| $M_i$ | a message sent by $V_i$ |
| $Ts$ | timestamp |
| $Sq$ | Sequence number of a message |
| $h$ | number of hops the message to be forwarded |
| $C_{p_i}$ | $p_i$'s certificate, where $p_i$ is a vehicle or an RSU |
| $ID_{p_i}$ | $p_i$'s identity |
| $PID_{p_i}$ | $p_i$'s pseudo identity |
| $SK_{p_i}$ | $p_i$'s private key |
| $PK_{p_i}$ | $p_i$'s public key |
| $K_{G_i}$ | group key assigned by RSU $R_i$ to vehicles within its transmission range |
| $GID_i$ | group identity of the vehicles within the transmission range of $R_i$ |
| $K_{A\_B}$ | shared key between A and B |
| $H()$ | cryptographic one-way hash function |
| $dgt_i$ | a message digest obtained by $V_i$ using $H()$ |

## Chapter 3

## Secure Incentive-Based Architecture for Vehicular Cloud

Cloud computing has emerged as a viable technology for supporting utility computing. In the future, vehicles are likely to be equipped with devices that have large computation and communication power as well as large storage. Such computation power and storage are often underutilized. People in several areas such as traffic management, parking management, etc. can benefit from utilizing the unused computation, communication and storage capabilities of the vehicles on the road as well as from the traffic information collected by the vehicles. In this chapter, we propose a secure architecture for the vehicular cloud to support the above-mentioned services. The architecture encourages vehicles to contribute their underutilized resources to the cloud by issuing tokens which can be used by the vehicles to get services from the cloud.

### 3.1 Introduction

In the last few years, automobile manufacturers have been incorporating technologies in their vehicles that provide safety and entertainment services to their drivers. Such technologies include on board units (OBUs), global positioning systems (GPSs), computational devices, storage devices, communications devices etc. [37]. In the future, these devices would facilitate the vehicles collect information about various phenomena such as, road condition, traffic congestion, delays due to accidents, etc. and share

them with other drivers. Moreover, they would allow the vehicles to perform complex operations like context management, and data filtering [20, 40]. Vehicles in VANETs could help in collecting such information and sharing them other drivers. For example, accident avoidance warnings could quickly notify drivers of conditions that could cause a collision. Also, in the case of an accident, the scene can be re-constructed by law-enforcement agencies using the velocity information recorded by each vehicle [4].

In the last decade, cloud computing emerged as an economical solution for customers to rent IT infrastructures, platforms or software, instead of investing money to own and maintain such services. The service providers lend such elastic services to customers exactly when they need them, and then they charge them based on their usage. Services provided by the cloud can be broadly divided into three categories: IasS (Infrastructure as a Service), PasS (Platform as a Service), and SaaS (Software as a Service). Although the primary features of the cloud are cost saving, on-demand service, resource pooling, scalability and ease of resources accessing, security and privacy concerns are the major barriers for customers to use the cloud [2, 14].

In order to fully utilize the resources of vehicles in VANETs, Olariu et al. [55] proposed the concept of a vehicular cloud, which combines VANET and cloud. A vehicular cloud is a group of largely autonomous vehicles in VANET that contribute their computing, sensing, communication, and physical resources to the cloud. Vehicles' resources and the information exchanged from the vehicles with the cloud can be used by other vehicles in decision making. Vehicular cloud can facilitate providing services such as parking management, traffic congestion, avoiding accidents, reducing environmental pollution etc. to customers in real time at low cost [24].

A vehicular cloud could help in reducing/eliminating propagation of redundant information in VANETs and use its resources more efficiently. In current studies on VANETs, multiple vehicles which observe the same phenomena propagate it to other vehicles which can result in propagation of redundant messages. This results

in vehicles wasting their resources analyzing the redundant data to find relevant information. A vehicular cloud allows vehicles to exchange their collected data with the cloud, where it can be analyzed, verified, organized, stored, and discarded if it is redundant or irrelevant. Cloud then can send only upto date information to the drivers upon request. Various other applications can benefit from using a vehicular cloud. Following a list of sample applications for vehicular cloud:

- **Intelligent Parking Management :** Millions of vehicles are parked in garages for hours every day. While they are parked, the underutilized resources of the vehicles such as computational and storage facilities could be used to perform tasks coming from the parking management server. Parking management could encourage the drivers of the vehicles to rent the resources of their vehicles and compensate them for that. Compensation could take the shape of free parking, shopping coupons or virtual credits that could be used somewhere else to get a service. Parking lots found in airports, malls, and large companies are examples of where we can use this application [1]. A vehicular cloud could also be used to help finding available parking spots. Drivers and parking management could cooperate in exchanging information about empty parking spots and update it to vehicular cloud, so drivers looking for an empty spot could reserve the space through the vehicular cloud [87].

- **Road safety and traffic Management :** Vehicles could collect data about road conditions, traffic, weather etc. and store this data in the cloud. Then, vehicles can periodically receive information from the cloud regarding road conditions such as, ice on the road, accidents, construction, etc. [26]. Based on this information, drivers may alter their routes.

- **Intelligent Transportation System using Traffic Monitoring:** Current transportation systems use traffic monitoring devices, such as inductive loop

detectors (ILDs), videos cameras, radars and others, to measure and monitor the road traffic. A costly ILD (worth around $8,200) is embedded under the road to measure the road traffic by recording a signal every time a vehicle passes over it [55]. The failure rate of these ILDs are very high and the maintenance costs are continuously growing. Hence, a vehicular cloud could be an alternative and more economical solution to the transportation department for monitoring the traffic using vehicles participating in the VANET.

- **Planned evacuation :** Vehicular cloud can also help expedite evacuation during disasters like earthquakes, hurricanes and others. Data about disaster could be collected using vehicles inside that disaster area and transferred to the cloud, where it could be analyzed, organized and sent back as useful information to the affected people and the evacuation organizations. Examples of such information are locations of open grocery stores, gas stations, shelters and medical centers [24].

Drivers contribute their vehicles' resources to the vehicular cloud, and in return, they are compensated in the form of incentives for participation. It is expected that vehicles cooperate with the cloud by contributing their resources. However, some vehicles may choose not to contribute to the cloud. Vehicles can be enticed to contribute their resources to the cloud by rewarding them with incentives. Several incentive schemes have been proposed in the context of MANETs and VANETs, but none, to our knowledge, in the context of vehicular cloud. In this chapter, we propose an architecture for vehicular cloud that uses incentive based scheme to encourage vehicles to contribute their resources, as well as, the information they collect to the cloud. The vehicles in return, receive incentives (tokens) for their contribution. The architecture not only helps in benefiting the drivers of the vehicles, but also the other users who need this information. Our solution ensures the security of the entities, operations and messages required to maintain the rewarded incentives. Figure 3.1 illustrates the

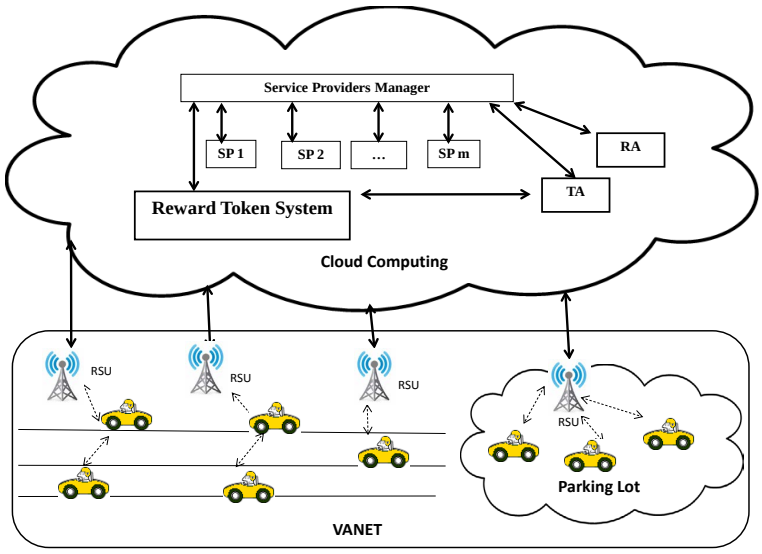


Figure 3.1: Incentive-based Architecture for Vehicular Cloud

architecture proposed in this chapter for vehicular cloud. It mainly consists of two integrated parts: A VANET part where a group of stationary or moving vehicles form a cloud and communicate with the conventional cloud through the road side units (RSUs), the other part is the conventional cloud, which contains many entities that are needed in this architecture. These entities include the service provider manager, Token Reward System, Trust Authority, and Revocation Authority. The detailed functionalities of these entities are explained in the system model in Section 3.3.

The rest of the chapter is organized as follows. Section 3.2 surveys the related works. Section 3.3 introduces the system model, assumptions, problem statement and solution objectives. Section 3.4 presents the proposed architecture in detail and a secure incentive-based scheme for enticing vehicles to participate in the cloud. In Section 3.5, we present an analysis of our scheme. Finally, we conclude in Section 3.6.

## 3.2 Related Works

Vehicular cloud has received a lot of attention in the last few years [24,55,72]. Vehicles could be organized into a cloud where they utilize their unused resources on-demand

to perform tasks. Drivers contribute the information collected by their vehicles and resources to the cloud, and they receive incentives in return. Some vehicles may be non-cooperative by utilizing their resources only for their own purposes. These are called selfish vehicles (nodes).

Selfish nodes problem has been studied extensively in the context of routing in MANETs and VANETs. Various incentive mechanisms were proposed in [10, 11, 13, 18, 34, 36, 38, 46, 52, 69, 90] to stimulate contribution of nodes and make them more cooperative with the others. Butty et al. [11, 13] introduced incentive schemes based on using a tamper proof hardware inside each node. This hardware is responsible to maintain and secure virtual credit gained by the node when it participated in forwarding messages. The sender estimates the rewards based on the number of intermediate nodes.

The authors of [10,46,52] proposed reputation based schemes where nodes observe their neighbors' traffic, record their contribution to the network and isolate nodes which have poor reputation. The high mobility of nodes makes it unfeasible to observe neighboring vehicles or even build a distributed reputation system based on this. Li et al. [36] presented a receipt counting reward scheme which focused on incentive distribution. Their approach requires every source node to obtain permission from an authority for every message they forward before they reward the intermediate nodes. Authors in [18,90] presented a game theory based scheme for manipulating parameters such as the amount earned, designation of charging subject, etc. to analyze and build the incentive scheme. While all of these schemes seem beneficial for MANETs and VANETs, they are not suitable for vehicular cloud because they were designed to entice nodes to participate in routing messages.

Cloud computing promises to provide reliable and elastic services to customers. In order to sustain such objectives, it needs a pool of resources and underutilized resources of vehicles participating in vehicular cloud can be a pool of resources. This

chapter proposes an incentive-based architecture to encourage the vehicles to participate and contribute their resources to the cloud.

## 3.3 System Model

In this section, we introduce the system model, assumptions, problem statement and design objectives.

### 3.3.1 System Model

The vehicular cloud architecture proposed in this chapter, shown in 3.1, consists of the following entities.

- **Service Provider Manager (SPM):** The SPM manages all service providers in the cloud and serves as the representative of service providers so it is responsible for advertising services, making contracts for services, validating proofs of works done by vehicles, and issuing tokens as incentive for their participation in the cloud.

- **Reward Token System (RTS):** The RTS serves as the token bank in the cloud. It creates an account for each vehicle when the vehicle is registered and the account is tied to vehicle's pseudo ID. It assigns tokens to the vehicles when they contribute their resources.

- **Revocation Authority (RA):** The RA maintains the revocation list for the misbehaving vehicles. It also Keeps the records of vehicles whose contribution was poor.

- **Trusted Authority (TA):** The TA in the cloud is able to communicate with RA, RTS and SPM securely. When a vehicle is registered or renewed, it issues a certificate for the vehicle. And it also manages all private information about

vehicles including the certificate, which ties vehicle to the its public key, and (public, private) key pairs. It also helps the SPM in verifying vehicles when needed. The real identity is not given to the SPM, however, when law enforcement agencies need the real IDs of the vehicles for investigation purposes, it can reveal the real IDs of the vehicles to them.

- **Road Side Units (RSUs):** The RSUs are located along the roads and connected by a network so they serve as gateway to the cloud from the VANET.
- **On Board Units (OBUs):** An OBU is a tamper proof device installed on the vehicles. And it has computation, communication capabilities and storage. Also, it is able to check the token balance with the RTS in the cloud.

### 3.3.2 Assumptions

We assume that the RA maintains the certificate revocation list of misbehaving vehicles and the certificate of misbehaving vehicles are revoked using some revocation protocols such as the ones discussed in [74, 78, 79].

We also make the following assumptions.

1. The RTS, TA, and RA are totally trusted and are assumed to be not compromised.
2. When a vehicle is registered, its public/private key pair is assigned and the public keys of the RTS and the SPM are stored in the OBU installed in the vehicles.
3. Vehicles can communicate with the cloud through the RSUs and any vehicle within the transmission range of an RSU can send/receive messages to the RSU, through other intermediate nodes using some available routing protocol.
4. OBUs on vehicles can check their token balance with the RTS.

### 3.3.3 Problem Statement and Solution Objectives

Vehicles are equipped with computational resources and storage facilities, but they are often underutilized. There are many people and application managers interested in renting such resources as well as obtaining the information collected by the vehicles. Since the contribution of the vehicles are optional, some drivers may choose not to do it. Drivers can be enticed to contribute the resources of their vehicles by offering incentives. Several incentive schemes have been proposed to entice selfish nodes in MANETs and VANETs, but they are not suitable for vehicular cloud because they were designed only for handling selfish nodes in routing. Hence, there is a need of an incentive-based architecture to reward the drivers of the vehicles for sharing their resources as well as to help the people who are interested in resources of the vehicles and information collected by the vehicles.

The proposed scheme addresses the following issues: First, the management issue where the rules of every entity involved in the system is determined and the flow of the incentive process is designed, maintained and audited carefully. Second, the scheme should be flexible to deal the dynamicity of vehicles joining or leaving the network, which also include the ability to handle the heterogeneity of the entities and the networks involved, in addition to handling the unpredictable demands of customers. Third, security is one of the most important issues that needs to be addressed. This requires maintaining the incentives operations performed inside the scheme, validating the integrity and authenticity of the messages exchanged between the entities, and preserving the privacy of the entities participating in the cloud.

In this chapter, we introduce an incentive-based architecture for vehicular cloud and propose a secure token reward system as an incentive scheme for enticing vehicles to participate in the cloud by contributing their resources. Our scheme is to achieve the following objectives. First, Integrity and authenticity of the messages exchanged between entities in the cloud should be ensured. Second, privacy of vehicles should

be protected while contributing their resources to the cloud, obtaining services from the cloud and using the resources in the cloud. Third, Token transaction between the cloud and the vehicles should be secure and robust against attacks.

## 3.4 Secure Token Reward System

In this section, we first present the basic idea behind our scheme and then describe our secure token reward system for vehicular clouds in detail.

### 3.4.1 Basic Idea Behind Our Scheme

The proposed scheme has the following phases:

- **Phase 1: Searching Resources:** When a cloud service provider looks for vehicles for resources, the cloud service provider manager (SPM) broadcasts a message through the cloud on behalf of the service provider. When an interested vehicle receives the message and decides to contribute its own resource to the cloud for the service, it sends a request message for the work to the SPM in the cloud through the road side units (RSUs). Then, the SPM authenticates the vehicle (or driver) with the help of the trusted authority (TA) and checks the previous records stored by the revocation authority (RA) (if there's any). If there are more vehicles interested in contributing their resources than what the service provider needs, the SPM picks vehicles based on their reputation in the past. Once the vehicle is authenticated, the SPM signs a contract for the work between the service provider and the vehicle and sends it to the vehicle, so the vehicle can start the work based on the contract. Here, the vehicles use their pseudo ID in all communications to protect their privacy.

- **Phase 2: Requesting Reward Tokens:** After completing an assigned work, a vehicle sends a message with the proof of the work done to the SPM. This

message helps the SPM in verifying the completion of the work. After the completion of the work is verified, the SPM sends a reward token request to the reward token system (RTS) so it can send tokens to the vehicle as compensation for the work done. When the reward token request is processed by the RTS, a transaction number is generated and sent to the SPM and the vehicle as a confirmation.

- **Phase 3: Using Tokens for Cloud Service:** In a vehicular cloud, there are various types of services available through cloud service providers. The cloud services generally can be purchased with pay-as-you-go, but the reward token earned by contributing resources into the cloud can also be used as a method of payment for the could services received. Since vehicles are able to check their token balance with the on board units (OBUs), they can simply use the cloud services with tokens for using the services.

Next, we describe our scheme in detail. The notations used in this scheme are listed in Table 3.1.

### 3.4.2 Searching Resources

In our scheme, we use hash-based digital signature along with public key encryption to ensure the integrity and the authenticity of messages. When a message is sent, the sender attaches the digital signature to the message. The digital signature is made by encrypting the hash of the message using sender's private key. Since only the sender can generate the digital signature, the authenticity of the message is guaranteed. For integrity, the hash in the digital signature should match with the hash of the message calculated by the receiver. If they match, the receiver is able to verify the authenticity and integrity of the message.

When a cloud service provider needs to use the resources of vehicles, the SPM broadcasts an advertising message $M_1$ (Figure 3.2) through the cloud on behalf of

Table 3.1: Notations

| Notation | Description |
|---|---|
| $SPM$ | Service Provider Manager |
| $RTS$ | Reward Token System |
| $R$ | an RSU |
| $V$ | a vehicle |
| $M$ | a message |
| $ts$ | timestamp |
| $Sq$ | sequence number of a message |
| $C$ | certificate |
| $sv$ | cloud service information |
| $sv\#$ | cloud service number |
| $tr\#$ | transaction number for token reward |
| $proof$ | proof of work done |
| $ID_A$ | identity of entity A |
| $PID_A$ | pseudo identity of entity A |
| $SK_A$ | private key of entity A |
| $PK_A$ | public key of entity A |
| $H()$ | cryptographic one-way hash function |
| $SIG_A(M)$ | signature of message M signed by A's private key. |
| $E(M, K)$ | encrypting message $M$ with key $K$ |

the service provider, where

$$M_1 = ID_{SPM}, sv\#, sv, ts, SIG_{SPM}(m_1)$$

$$where\ SIG_{SPM}(m_1)=E(H(sv\#,sv,ts),SK_{SPM}) \quad (3.1)$$

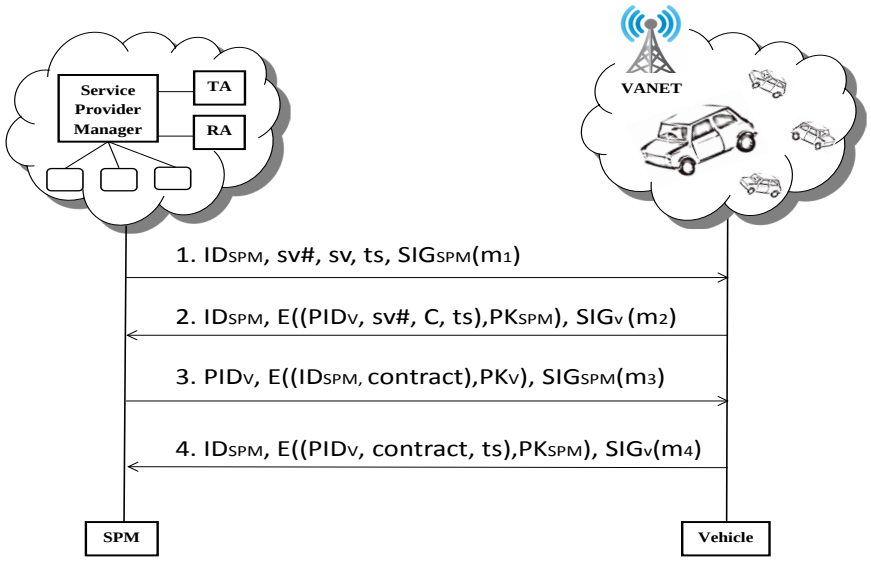


Figure 3.2: Contract Establishment Process

The advertising message $M_1$ includes the service number $sv\#$ and cloud service information $sv$ that contains the ID of the cloud service provider, work type, work requirement, and reward amount. Also, the SPM attaches its digital signature that is obtained by computing the hash of the message and encrypting it with its private key. When an interested vehicle $V$ receives the message $M_1$ and wants to contribute its resource to the cloud, it computes a work request message $M_2$, where $M_2$ is given below, by encrypting the service number, certificate and timestamp with the public key of the SPM. Then it sends the message to the SPM in the cloud through a nearby RSU after attaching its digital signature. Here, the contract is an agreement between a vehicle and the service provider for the service and it includes all the details about the work such as work requirement and payment.

$$M_2 = ID_{SPM}, E((PID_V, sv\#, C, ts), PK_{SPM}), SIG_V(m_2)$$

$$where\ SIG_V(m_2)=E(H(PID_V,sv\#,C,ts),SK_V) \quad (3.2)$$

Upon receiving $M_2$, the SPM is able to verify the authenticity of the messages by checking its certificate $C$ and pseudo ID $PID_V$ received from the TA and decrypt the

message. Also, the SPM checks if the vehicle has been blacklisted. Here, a pseudo ID is used for the vehicle to protect its privacy and the TA does not reveal the original identity of the vehicle to the SPM, however, it can be revealed when necessary such as a when a dispute for a transaction arises.

After the vehicle is authenticated, the SPM generates message $M_3$ by attaching the contract for the work and its signature obtained by computing the hash of the message as follows.

$$M_3 = PID_V, E((ID_{SPM}, contract, ts), PK_V), SIG_{SPM}(m_3)$$
$$where\ SIG_{SPM}(m_3)=E(H(ID_{SPM},contract,ts),SK_{SPM}) \quad (3.3)$$

Once the message $M_3$ is delivered to the vehicle, it first sends an acknowledge $M_4$ to the SPM and then can start the work for the service based on the requirement in the contract.

$$M_4 = ID_{SPM}, E((PID_V, contract, ts), PK_{SPM}), SIG_V(m_4)$$
$$where\ SIG_V(m_4)=E(H(PID_V,contract,ts),SK_V) \quad (3.4)$$

### 3.4.3 Requesting Reward Tokens

After a vehicle finishes an accepted work, it notifies the SPM by sending the message $M_5$(Figure 3.3) with the proof of work done. Where,

$$M_5 = ID_{SPM}, E((PID_V, sv\#, proof, ts), PK_{SPM}), SIG_V(m_5)$$
$$where\ SIG_V(m)=E(H(PID_V,sv\#,proof,ts),SK_V) \quad (3.5)$$

Here, the *proof* of the work done varies depending on the type of work done and it must be verifiable by the SPM. The SPM is able to verify the completion of the

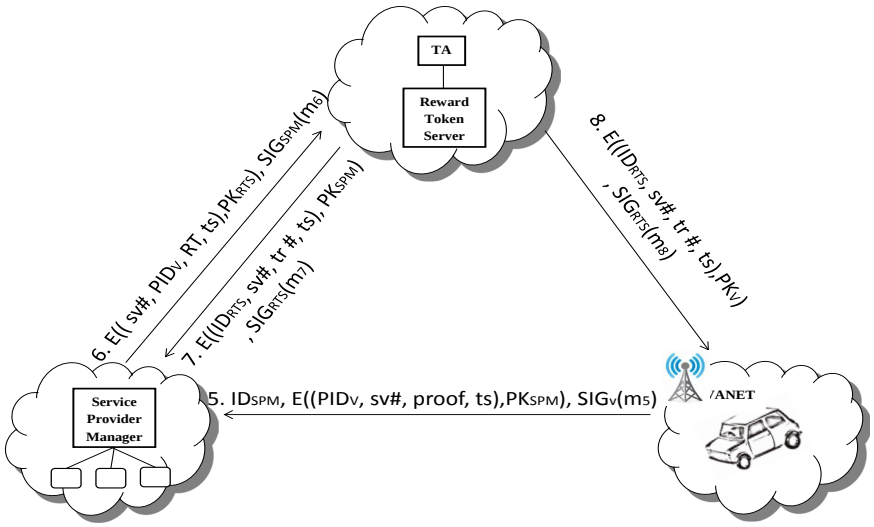


Figure 3.3: Token Reward Process

work by checking the service number and the *proof*. Once the work done is verified, the SPM generates a reward token request message $M_6$, attached with the digital signature to it, and sends it to the $RTS$, so the reward tokens can be sent to the vehicle as a compensation for the work done, where

$$M_6 = ID_{RTS}, E((sv\#, PID_V, RT, ts), PK_{RTS}), SIG_{SPM}(m_6)$$

$$where\ SIG_{SPM}(m_6){=}E(H(sv\#,PID_V,RT,ts),SK_V) \quad (3.6)$$

After the $RTS$ processes the reward token request, it computes the confirmation message $M_7$ and $M_8$ with a transaction number for the SPM and the vehicle respectively as follows

$$M_7 = ID_{SPM}, E((ID_{RTS}, sv\#, tr\#, ts), PK_{SPM}), SIG_{RTS}(m_7)$$

$$where\ SIG_{RTS}(m_7){=}E(H(ID_{RTS},sv\#,tr\#,ts),SK_{RTS}) \quad (3.7)$$

$$M_8 = PID_V, E((ID_{RTS}, sv\#, tr\#, ts), PK_V), SIG_{RTS}(m_8)$$

$$where\ SIG_{RTS}(m_8)=E(H(ID_{RTS},sv\#,tr\#,ts),SK_{RTS}) \quad (3.8)$$

and sends them to the SPM and the vehicle respectively. Note that the service providers are connected to the SPM so all messages related to a particular service provider are eventually delivered to it accordingly.

### 3.4.4 Using Tokens for Cloud Service

In a vehicular cloud, several types of services can be provided by service providers. For example, Parking lot data managers can provide to vehicles information about available parking spaces, Transportation system can use the cloud collect traffic information and divert traffic based on the traffic information as well as optimize traffic signals, dynamic traffic signals, etc. [84]. Vehicular cloud can help make services readily available for vehicles on roads and at the parking lots and can be purchased with pay-as-you-go plan. With our token reward system, the tokens obtained in exchange for sharing their own resources also can be used for the cloud services as a method of the payment. Since a feature of the balance check is available on the OBU, a vehicle simply can use the could services with the tokens by sending a message $M_9$ to the SPM as follows.

$$M_9 = ID_{SPM}, E((PID_V, sv\#, RT, ts), PK_{SPM}), SIG_V(m_9)$$

$$where\ SIG_V(m_9)=E(H(PID_V,sv\#,RT,ts),SK_V) \quad (3.9)$$

Once the SPM receives the message from the vehicle, it authenticates the message and sends a token deduction request to the $RTS$ in the same way as requesting for rewarding tokens. If the authenticity of the vehicle is verified and a confirmation for the token deduction is given to the SPM, then it notifies the service provider that

now the vehicle can use the cloud service.

## 3.5 Security Analysis

In this section, we evaluate the performance of our proposed scheme in terms of security and usability and analyze the token reward system.

To entice the vehicles to contribute their resources, an incentive-based scheme is necessary. Also, dealing with the selfish nodes (i.e., nodes that do not want to contribute their resources but would want to access the services provided by the cloud) is a challenge. We proposed a secure incentive-based architecture for vehicular cloud and a secure incentive-based reward scheme for enticing vehicles to participate and contribute their resources to the cloud. If a driver agrees to share his/her vehicle's resources with the cloud service, then reward tokens are given in return after the completion of the work based on the contract.

### 3.5.1 Message Integrity

Messages are sent with a digital signature generated by the sender using cryptographic one-way hash function. Since the message is discarded upon arrival if the hash of the message does not match, the message integrity is guaranteed. Hence, integrity of token information in the message is guaranteed as well.

### 3.5.2 Source Authentication

The SPM is connected to the TA in the cloud. When a request for authentication is received, the TA helps the SPM in authenticating the sender.

### 3.5.3 Privacy Preservation

Every vehicle is assigned a unique pseudo ID by the TA. With the pseudo IDs, all private information and real identities of vehicles are protected. However, when a

malicious node is detected, the real ID of the malicious vehicle is revealed by the TA to the authorities for legal investigation.

### 3.5.4 Usability

Vehicles earn reward tokens for contributing their resources to the cloud. They can check the token balance with the OBU and use the earned tokens for a cloud service later.

### 3.5.5 Encryption

Since the messages exchanged are generally small, we use public key cryptography for encrypting messages. Messages are also signed. The scheme can be easily changed to use symmetric key encryption by using Public key cryptography during the initial phase of the communication for authentication and exchanging symmetric key.

## 3.6 Summary

In this chapter, we proposed an architecture for vehicular cloud and presented an incentive based solution, called secure token reward system, to entice vehicular nodes for participating and contributing to the cloud. Our scheme is based on the idea that tokens are given as incentive to the vehicles that contribute their resources for cloud services. The token reward system located in the cloud ensures secure management of tokens. Also, the service provider manager is responsible for advertising services, making contracts, validating proofs of work done, and issuing reward tokens on behalf of service providers. Therefore, integrity and authenticity of incentive-related messages are guaranteed and the privacy of vehicles are protected. In addition, tokens received for sharing their resources can be used for obtaining services from the vehicular cloud in the future.

## Chapter 4

## Nonnegative Matrix Factorization based Privacy Preservation in Vehicular Communication

When a vehicle in VANET discovers any events such as car accident, traffic congestion, hazardous road condition, etc., it shares such information with other vehicles. However, drivers may not be comfortable sending their location information with their messages because their privacy can be compromised. In this chapter, we present a Nonnegative Matrix Factorization (NMF) based privacy preservation scheme to perturb the source location data without using cryptography while it can still calculate the location of the event occurred. The proposed scheme utilizes the intrinsic property of NMF to distort the data for protecting driver's location privacy. It then clusters the drivers in accordance with their locations, the relative distances and directions, as well as the timestamps. By doing so, events' location can be identified based on the clusters while driver's private information is preserved.

### 4.1 Introduction and Problem Description

Vehicular Ad hoc Networks (VANETs) are likely to be promising technology of the future because it improves traffic safety and driving comfort. In VANETs, vehicles on the roads form a self-organized network and they exchange information collected from the roads about various things such as road condition, traffic congestion, delays, etc. For example, accident avoidance warnings could quickly notify drivers of conditions

that could cause a collision. Also, drivers may choose an alternate driving route if they are notified that there's traffic congestion or delays ahead. Since such information is collected and reported by vehicles that sense the scene or events, the vehicles' current location and speed should be included in order to provide the accurate and specific information.

Since communications between vehicle to vehicle or vehicle to road side unit (RSU) are via wireless radio, it may be possible that malicious entities could track individuals' location information, gather information and subsequently misuse the gathered information. Consequently, drivers may not want to share their collected data if their location privacy is not protected.

There has been studies to address the privacy issues in VANETs. In SLOW [12], vehicles do not transmit heartbeat messages when their speed is below a pre-defined threshold, and change pseudonym during each silent period to ensure user location privacy. In [25], Freudiger et al. proposed a quantitative framework for choosing the parameters of a pseudonym based privacy system. Liu et al. [45] introduced Traffic-Aware Multiple Mix Zone Placement for Protecting Location Privacy to quantify the system's resilience to privacy attack using multiple mix zones. PCS [49] also addressed location privacy using pseudonym changing at social spots strategy. PCS first identifies the social spots where multiple nodes clustered and then develops two anonymity set analytic models to achieve the location privacy. Lim et al. [40] proposed a scheme using pseudo ID and cryptography to protect user privacy, however, every vehicle needs to obtain a pseudo ID and update it frequently. The traditional public key infrastructure based scheme also addressed the user privacy issue [73]. However, every vehicle needs to load all public keys of other vehicles in the network and it is not practical in real world scenario. In this chapter, we introduce a NMF based privacy preservation scheme that does not use pseudo ID or cryptography to solve the source location privacy problem.

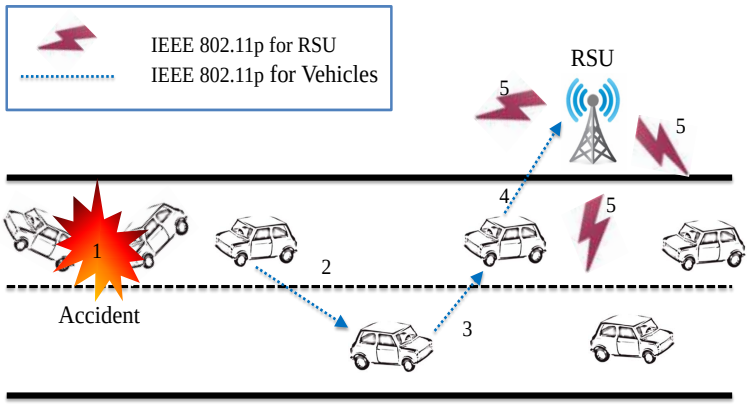


Figure 4.1: An Example of Real-world Scenario

## 4.2 Preliminaries

Non-negative Matrix Factorization has been studied and known as a useful for decomposition multivariate data. When the data to be analyzed in nonnegative, finding reduced rank nonnegative factors for appoximating a given nonnegative data matrix is a viable option as classical tools cannot guarantee to control the nonnegativity. The nonnegative matrix factorization problem (NMF) in the generic form is following: [5]

**NMF Problem:** Given a nonnegative matrix $A \in \mathbb{R}^{m \times n}$ and a positive integer $k < min(m, n)$, find nonnegative matrices $W \in \mathbb{R}^{m \times k}$ and $H \in \mathbb{R}^{k \times n}$ to minimize the functional

$$f(W, H) = 1/2\|A - WH\|_F^2 \tag{4.1}$$

Here, the product $WH$ is called a NMF of A. Note that A is not necessarily equal to the product $WH$.

## 4.3 Ensuring Location Privacy using Nonnegative Matrix Factorization

In most cases, when vehicles report accidents to the RSUs, the drivers may not be willing to expose their private information, such as their identities, and their loca-

tions. To report the accident, the witness vehicle only needs to send the message including the estimated location and the time of the accident. Study shows that matrix factorization techniques are ideal choices for data privacy preservation by their nature. Amongst them, nonnegative matrix factorization (NMF) [33] is a typical and popular representative. NMF is a widely used dimension reduction method in many applications such as clustering [22], text mining [57], data distortion based privacy preservation [76], privacy preserving recommender systems [82] etc. Thus, we adopt nonnegative matrix factorization to preserve the user location privacy in vehicular communications. One example of real world scenarios is described in Figure 4.1. When an accident or event is sensed by a vehicle, it sends a message including distorted location information to nearby RSU. Note that if a vehicle is outside of the RSU's communication range, the message can be delivered to the RSU through intermediate vehicles. Once the message is received by the RSU, the RSU still can verify the message and use it while ensuring location privacy. The details of our scheme is explained below.

A conventional NMF is defined as follows [33],

$$R_{m\times n} \approx U_{m\times k} \cdot V^T_{n\times k} \tag{4.2}$$

The goal is to find a pair of orthogonal nonnegative matrices $U$ and $V$ (i.e., $U^TU = I, V^TV = I$) that minimizes the Frobenius norm (or Euclidean norm) $\|A - UV^T\|_F$. The corresponding objective function is

$$min_{U\geq 0, V\geq 0} f(A, U, V) = \|A - UV^T\|^2_F. \tag{4.3}$$

In real world scenarios, the drivers' location data, which is considered as their private information, can be stored in a numerical matrix, denoted by $A$. Before a vehicle sends the message, it has to perturb its location to avoid privacy leakage.

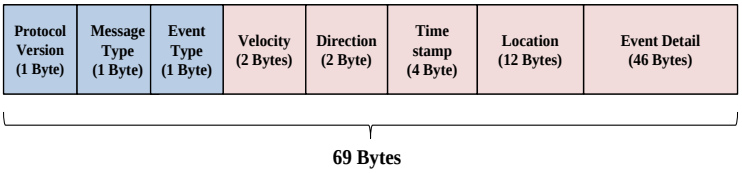


Figure 4.2: Message Format

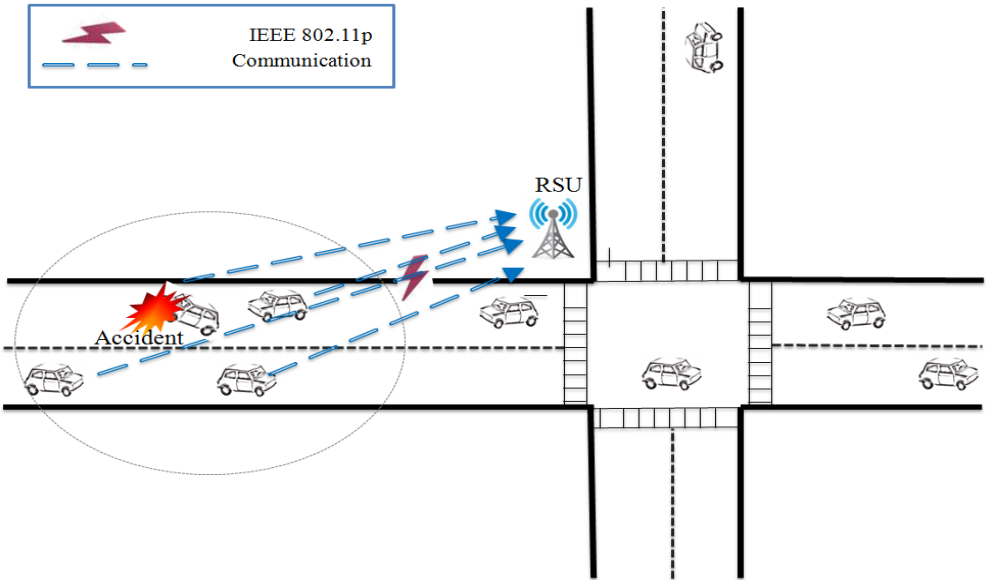


Figure 4.3: Accident Observed by Multiple Vehicles

Hence, we use NMF to factorize the location matrix and approximate it by taking the product of the factor matrices, i.e., $U$ and $V$. Since the update process of NMF produces errors in each round, the approximated matrix, denoted by $\tilde{A}$, is different from $A$. However, by carefully selecting the number of iterations and the dimensions of the factor matrices, $\tilde{A}$ can hold close data utility to $A$, meaning that the perturbed location data still contain reasonable information while the exact values are changed. In the figure 4.3, an accident is observed by multiple vehicles on the road and it is reported to the nearby RSU. Here, the vehicles send the perturbed location data, but they are still reasonable information to locate the approximate area of the accident.

Once a driver's location data has been perturbed, the on board unit(OBU) would assemble it with other meta data, such as protocol version, message type, event type, velocity, direction, timestamp, and event detail, shown in Figure 4.2, to build

a message and send it to RSUs. To identify the events, RSUs need to cluster events according to the messages. In this case, events are objects, while event type, direction, timestamp, as well as the perturbed location, are treated as the attributes of the objects. We suggest using K-Means [50] as the fundamental technique to do this task. K-Means is a popular and well studied approach that is easy to implement and is widely used in many domains. As the name of the algorithm indicates, K-Means needs the definition of "mean" prior to clustering. It minimizes a cost function by calculating the means of clusters. Though the basic idea of K-Means is simple, it can effectively and efficiently cluster objects with numerical attributes.

As mentioned above, the messages that are sent to the RSUs contain perturbed location data. The goal is to obtain accurate event clusters from K-Means and differed $\tilde{A}$ from $A$.

## 4.4 Summary

In this chapter, we presented a scheme to preserve user location privacy for vehicular communication using nonnegative matrix factorization. Our scheme does not require traditional cryptography to protect privacy.

# Chapter 5

# Conclusion and Future Work

VANETs are likely to be deployed in the near future due to the various features they are likely to enhance the driving comfort of drivers as well as passengers traveling in the vehicles. Moreover, due to the widespread adoption of cloud computing, vehicles participating in VANETs are likely to utilize clouds to store information as well as retrieve information. In this dissertation, we addressed some of the issues related message dissemination in VANETs; we also presented an architecture for Vehicular cloud. Next, we summarize the results presented in this dissertation and also discuss our future work.

## 5.1 Dissertation Summary

First, we presented an efficient protocol for propagating messages about observed phenomena to other vehicles in relevant areas. Many of the existing protocols broadcast such messages to other vehicles through other vehicles. This approach doesn't scale well. We presented a protocol which has the following features: (i) messages sent are encrypted and they are sent to nearby RSU, and not broadcasted to other vehicles; (ii) messages sent are authenticated by the RSUs; (iii) RSUs also help in suppressing duplicate messages; so redundant propagation of messages about the same phenomena observed by different vehicles is prevented; (iv) since RSUs (and not vehicles themselves) propagate the messages to vehicles in relevant regions, it is more scalable; (v)

anonymity of the vehicles sending messages is preserved; (vi) it facilitates authorities to trace the messages to their senders when necessary (i.e., such as a malicious node sending malicious messages); (vii) since RSUs which have more computation and communication power authenticate and propagate the messages, vehicles' OBUs incur less overhead.

Second, we presented an architecture for vehicular cloud and presented an incentive based solution, called secure token reward system, to entice vehicular nodes for participating in the network. Unlike traditional vehicular networks, nodes' participation is crucial in vehicular cloud. Our scheme is based on the idea that an incentive is given to the drivers/vehicles who contribute their resources for cloud services. The token reward system is located in the cloud and it ensures the integrity of token transaction and efficient management of tokens. In addition, the service provider manager advertises services on behalf of the service providers, makes contracts with vehicles, and validates work proofs after vehicles finish the work. In this scheme, message integrity and authenticity of incentive-related messages are guaranteed and the privacy of vehicles are also protected. This architecture allows vehicles earn tokens for sharing resources as well as use earned tokens for obtaining services from the vehicular cloud.

Third, for applications which require the location of the vehicles disseminating observed phenomena, we presented a efficient scheme to preserve user location privacy using nonnegative matrix factorization. This scheme does not require traditional cryptography to protect privacy, so it can save computation involved in encrypting messages. Instead of encrypting user location information, our scheme can calculate the location of the event while preserving user privacy. Our scheme utilizes the intrinsic property of nonnegative matrix to distort the data, hence the driver's location privacy is protected during communication.

## 5.2 Future Work

In the future, we will continue our research in the following directions. First, although our approach achieved an efficient way of secure message delivery, it still requires that every vehicle needs to obtain a shared key and group key whenever it enters the transmission area of an RSU. In order to reduce its communication overhead for key change, we will focus on establishing secret keys for multiple RSUs. Second, vehicular clouds are one of the examples of the hybrid vehicular networks. We will work on securing communications for such inter-networking environments and finding efficient routing protocols. Third, as shown in Chapter 4, nonnegative matrix factorization could be used for protecting user privacy without using traditional cryptographic methods. Hence, we will analyze and compare its performance in real vehicular communication in terms of accuracy and computation power requirement. Lastly, we will work on finding efficient schemes for establishing dependable routes in VANETs. When a vehicle sends a message to a destination node in VANETs, a VANET routing protocol should be able to determine the most reliable route in order to deliver the message without loss. The existing schemes such as least weight path routing based on the reliability ratings of the road edges [4] find the route whose weight from the source node to the destination is the lowest. However, the route of lowest weights is not necessarily the most reliable route. Hence, we will develop an efficient routing protocol for establishing dependable routes by determining which street edges are most likely to remain reliable.

## Bibliography


[1] Samiur Arif, Stephan Olariu, Jin Wang, Gongjun Yan, Weiming Yang, and Ismail Khalil. Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. *IEEE Transactions on Parallel and Distributed Systems*, 23(11):2067–2080, 2012.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[3] Ali Osman Bayrak and Tankut Acarman. S3p: A secure and privacy protecting protocol for vanet. In *Proceedings of 2010 6th International Conference on Wireless and Mobile Communications (ICWMC)*, pages 441–447. IEEE, 2010.

[4] James Bernsen and D Manivannan. RIVER: A reliable inter-vehicular routing protocol for vehicular ad hoc networks. *Computer Networks*, 56(17):3795–3807, 2012.

[5] Michael W. Berry, Murray Browne, Amy N Langville, V Paul Pauca, and Robert J Plemmons. Algorithms and applications for approximate nonnegative matrix factorization. *Computational Statistics & Data Analysis*, 52(1):155–173, 2007.

[6] Subir Biswas and Jelena Mišic. Proxy signature-based rsu message broadcasting in vanets. In *Proceedings of 25th Biennial Symposium on Communications (QBSC)*, pages 5–9. IEEE, 2010.

[7] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 103–112. ACM, 1988.

[8] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual International Cryptology Conference*, pages 213–229. Springer, 2001.

[9] Stefan Brands. A technical overview of digital credentials. *Available Online: citeseer.ist.psu.edu/brands02technical.html*, 20:145–8, 2002.

[10] Sonja Buchegger and J-Y Le Boudec. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In *Proceedings of 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, 2002.*, pages 403–410. IEEE, 2002.

[11] Levente Butty and Jean-Pierre Hubaux. Enforcing service availability in mobile ad-hoc wans. In *Proceedings of the 1st ACM International Symposium on Mobile ad hoc Networking & Computing*, pages 87–96. IEEE Press, 2000.

[12] Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte. Slow: A practical pseudonym changing scheme for location privacy in vanets. In *Proceedings of IEEE Vehicular Networking Conference (VNC) 2009*, pages 1–8. IEEE, 2009.

[13] Levente Buttyán and Jean-Pierre Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8(5):579–592, 2003.

[14] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, 2009.

[15] Stephen Carter and Alec Yasinsac. Secure position aided ad hoc routing. In *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, 2002.

[16] David Chaum. Blind signature system. In *Advances in cryptology*, pages 153–153. Springer, 1984.

[17] David Chaum and Eugène Van Heyst. Group signatures. In *Proceedings of Eurocrypt 1991*, pages 257–265. Springer, 1991.

[18] Tingting Chen, Liehuang Zhu, Fan Wu, and Sheng Zhong. Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach. *IEEE Transactions on Vehicular Technology*, 60(2):566–579, 2011.

[19] Sam Ang Chhoeun, Kannikar Siriwong Na Ayutaya, Chalermpol Charnsripinyo, Kosin Chamnongthai, and Pinit Kumhom. A novel message fabrication detection for beaconless routing in vanets (mefad). In *Proceedings of the International Conference on Communication Software and Networks, 2009. ICCSN'09.*, pages 453–457. IEEE, 2009.

[20] Paolo Costa, Daniela Gavidia, Boris Koldehofe, Hugo Miranda, Mirco Musolesi, and Oriana Riva. When cars start gossiping. In *Proceedings of the 6th Workshop on Middleware for Network Eccentric and Mobile Applications*, pages 1–4. ACM, 2008.

[21] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[22] Chris Ding, Tao Li, Wei Peng, and Haesun Park. Orthogonal nonnegative matrix tri-factorizations for clustering. In *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 126–135. ACM, 2006.

[23] Carl Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas, and Tatu Ylonen. SPKI certificate theory. Technical report, RFC 2693, 1999.

[24] Mohamed Eltoweissy, Stephan Olariu, and Mohamed Younis. Towards autonomous vehicular clouds. In *Proceedings of International Conference on Ad Hoc Networks*, pages 1–16. Springer, 2010.

[25] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. On the age of pseudonyms in mobile ad hoc networks. In *Proceedings of IEEE INFOCOM 2010*, pages 1–9. IEEE, 2010.

[26] Mario Gerla. Vehicular cloud computing. In *Proceedings of the 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pages 152–155. IEEE, 2012.

[27] David Goldschlag, Michael Reed, and Paul Syverson. Onion routing for anonymous and private internet connections. *Communications of the ACM*, 42(2):39–41, 1999.

[28] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[29] Yong Hao, Tingting Han, and Yu Cheng. A cooperative message authentication protocol in vanets. In *Proceedings of Global Communications Conference (GLOBECOM), IEEE*, pages 5562–5566, Anaheim, CA, December 2012.

[30] Charles Harsch, Andreas Festag, and Panos Papadimitratos. Secure position-based routing for vanets. In *Proceedings of the IEEE Vehicular Technology Conference, VTC Fall.*, pages 26–30. IEEE, 2007.

[31] Hsu-Chun Hsiao, Ahren Studer, Chen Chen, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer. Flooding-resilient broadcast authentication for vanets. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, pages 193–204. ACM, 2011.

[32] John Kohl and Clifford Neuman. The kerberos network authentication service (v5). Technical report, RFC 1510, September, 1993.

[33] Daniel D. Lee and H. Sebastian Seung. Algorithms for non-negative matrix factorization. *Advances in Neural Information Processing Systems*, 13:556–562, 2001.

[34] Suk-Bok Lee, Joon-Sang Park, Mario Gerla, and Songwu Lu. Secure incentives for commercial ad dissemination in vehicular networks. *IEEE Transactions on Vehicular Technology*, 61(6):2715–2728, 2012.

[35] Fan Li and Yu Wang. Routing in vehicular ad hoc networks: A survey. *Vehicular Technology Magazine, IEEE*, 2(2):12–22, 2007.

[36] Feng Li and Jie Wu. Frame: An innovative incentive scheme in vehicular networks. In *Proceedings of IEEE International Conference on Communications, 2009. (ICC'09)*, pages 1–6. IEEE, 2009.

[37] Fei-Yue Wang Li Li, Jingyan Song and Nanning Zheng. Ivs 05: New developments and research trends for intelligent vehicles. *IEEE Intelligent Systems*, 20(4):10–14, 2005.

[38] Kiho Lim and Ismail M. Abumuhfouz. STORS: Secure token reward system for vehicular clouds. In *Proceedings of the IEEE Southeastcon, 2015*. IEEE, 2015.

[39] Kiho Lim, Ismail M Abumuhfouz, and D Manivannan. Secure incentive-based architecture for vehicular cloud. In *Proceedings of IEEE International Conference on Ad-Hoc Networks and Wireless*, pages 361–374. Springer, 2015.

[40] Kiho Lim and D. Manivannan. An efficient scheme for authenticated and secure message delivery in vehicular ad hoc networks. In *Proceedings of the 12th IEEE Consumer Communications and Networking Conference 2015.* IEEE, 2015.

[41] Kiho Lim and D Manivannan. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Vehicular Communications*, 4:30–37, 2016.

[42] Kiho Lim and Xiwei Wang. Nonnegative matrix factorization based privacy preservation in vehicular communication. In *Proceedings of IEEE SoutheastCon 2015*. IEEE, 2015.

[43] Xiaodong Lin and Su Li. Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 62(7):3339–3348, 2013.

[44] Xiaodong Lin, Xiaoting Sun, Pin Han Ho, and Xuemin Shen. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6):3442–3456, 2007.

[45] Xinxin Liu, Han Zhao, Miao Pan, Hao Yue, Xiaolin Li, and Yuguang Fang. Traffic-aware multiple mix zone placement for protecting location privacy. In *Proceedings of IEEE INFOCOM 2012*, pages 972–980. IEEE, 2012.

[46] Yanbin Liu and Yang Richard Yang. Reputation propagation and agreement in mobile ad-hoc networks. In *Proceedings of Wireless Communications and Networking, 2003.*, volume 3, pages 1510–1515. IEEE, 2003.

[47] Christian Lochert, Hannes Hartenstein, Jing Tian, Holger Füßler, Dagmar Hermann, and Martin Mauve. A Routing Strategy for Vehicular Ad Hoc Networks in City Environments. In *Proceedings of the IEEE Intelligent Vehicles Symposium*, pages 156–161, Jun 2003.

[48] Huang Lu, Jie Li, and M. Guizani. A novel id-based authentication framework with adaptive privacy preservation for vanets. In *Proceedings of Computing, Communications and Applications Conference (ComComAp), 2012*, pages 345 – 350, Hong Kong, January 2012.

[49] Rongxing Lu, Xiaodong Li, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology*, 61(1):86–96, 2012.

[50] J. B. MacQueen. Some Methods for Classification and Analysis of Multivariate Observations. In *Proceedings of 5-th Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 281–297, 1967.

[51] SS Manvi, MS Kakkasageri, and DG Adiga. Message authentication in vehicular ad hoc networks: Ecdsa based approach. In *Proceedings of International Conference on Future Computer and Communication, 2009. ICFCC 2009.*, pages 16–20. IEEE, 2009.

[52] Sergio Marti, Thomas J Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pages 255–265. ACM, 2000.

[53] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 2014.

[54] Steven P Miller, B Clifford Neuman, Jeffrey I Schiller, and Jermoe H Saltzer. Kerberos authentication and authorization system. In *Project Athena Technical Plan*. Citeseer, 1988.

[55] Stephan Olariu, Ismail Khalil, and Mahmoud Abuelela. Taking VANET to the clouds. *International Journal of Pervasive Computing and Communications*, 7(1):7–21, 2011.

[56] Vamsi Paruchuri and Arjan Durresi. Paave: protocol for anonymous authentication in vehicular networks using smart cards. In *Proceedings of IEEE Global Telecommunications Conference, 2010. (GLOBECOM 2010)*, pages 1–5. IEEE, 2010.

[57] V Paul Pauca, Farial Shahnaz, Michael W Berry, and Robert J Plemmons. Text mining using nonnegative matrix factorizations. In *Proceedings of 2004 SIAM Interational Conference on Data Mining*, volume 54 of *SDM '09*, pages 452–456. SIAM, 2004.

[58] Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. Technical report, 2003.

[59] Chris Piro, Clay Shields, and Brian Neil Levine. Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006*, pages 1–11. IEEE, 2006.

[60] Klaus Plossl, Thomas Nowey, and Christian Mletzko. Towards a security architecture for vehicular ad hoc networks. In *Proceedings of The First International Conference on Availability, Reliability and Security, 2006.* IEEE, 2006.

[61] B Pradeep, MMM Pai, M Boussedjra, and J Mouzna. Global public key algorithm for secure location service in vanet. In *Proceedings of 9th International Conference on Intelligent Transport Systems Telecommunications (ITST)*, pages 653–657. IEEE, 2009.

[62] K Priya and Komathy Karuppanan. Secure privacy and distributed group authentication for vanet. In *Proceedings of 2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, pages 301–306. IEEE, 2011.

[63] M Raya and JP Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[64] Maxim Raya, Adel Aziz, and Jean-Pierre Hubaux. Efficient secure aggregation in vanets. In *Proceedings of the 3rd International Workshop on Vehicular ad hoc Networks. VANET '06*, pages 67–75, September 2006.

[65] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[66] Marshall Riley, Kemal Akkaya, and Kenny Fong. Delay-efficient geodynamic group-based authentication in vanets. In *Proceedings of IEEE 35th Conference on Local Computer Networks (LCN)*, pages 280–283. IEEE, 2010.

[67] Ronald L Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393–394, 1984.

[68] Ghassan Samara, Wafaa AH Al-Salihy, and R Sures. Security analysis of vehicular ad hoc nerworks (VANET). In *Proceedings of 2010 Second International Conference on Network Applications Protocols and Services (NETAPPS)*, pages 55–60. IEEE, 2010.

[69] Fragkiskos Sardis, Glenford E Mapp, Jonathan Loo, Mahdi Aiash, and Alexey Vinel. On the investigation of cloud-based mobile media environments with service-populating and qos-aware mechanisms. *IEEE Transactions on Multimedia*, 15(4):769–777, 2013.

[70] Boon-Chong Seet, Genping Liu, Bu-Sung Lee, Chuan-Heng Foh, Kai-Juan Wong, and Keok-Kee Lee. A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications. In *Proceedings of International Conference on Research in Networking*, pages 989–999. Springer, 2004.

[71] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[72] Junggab Son, Hasoo Eun, Heekuck Oh, Sangjin Kim, and Rasheed Hussain. Rethinking vehicular communications: merging vanet with cloud computing. In *Proceedings of the 4th International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 606–609. IEEE Computer Society, 2012.

[73] IEEE Standard 1609.2. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - security services for applications and management messages. *IEEE Standard*, July 2006.

[74] Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. TACKing together efficient authentication, revocation, and privacy in VANETs. In *Proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. SECON'09.*, pages 1–9. IEEE, 2009.

[75] P Ning T Zhou, RR Choudhury. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In *Proceedings of the fourth Annual International Conference on Mobile and Ubiquitous Systems*, pages 1–8. IEEE, 2007.

[76] Nirmal Thapa, Lian Liu, Pengpeng Lin, Jie Wang, and Jun Zhang. Constrained nonnegative matrix factorization for data privacy. In *Proceedings of the 7th International Conference on Data Mining (DMIN '11)*, pages 88–93, 2011.

[77] Jing Tian, Lu Han, Kurt Rothermel, and Christian Cseh. Spatially Aware Packet Routing for Mobile Ad Hoc Inter-Vehicle Radio Networks. In *Proceedings of the IEEE Intelligent Transportation Systems, 2003.* , pages 1546–1551. IEEE, 2003.

[78] Boyang Wang, Baochun Li, and Hui Li. Public auditing for shared data with efficient user revocation in the cloud. In *Proceedings of IEEE INFOCOM, 2013*, pages 2904–2912. IEEE, 2013.

[79] Guojun Wang, Qin Liu, Jie Wu, and Minyi Guo. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. *Computers & Security*, 30(5):320–331, 2011.

[80] Neng-Wen Wang, Yueh-Min Huang, and Wei-Ming Chen. A novel secure communication scheme in vehicular ad hoc networks. *Computer Communications*, 31(12):2827–2837, 2008.

[81] Xiao Wang and Patrick Tague. Asia: Accelerated secure in-network aggregation in vehicular sensing networks. In *Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 514–522. IEEE, 2013.

[82] Xiwei Wang, Jun Zhang, Pengpeng Lin, Nirmal Thapa, Yin Wang, and Jie Wang. Incorporating auxiliary information in collaborative filtering data update with privacy preservation. *International Journal of Advanced Computer Science and Applications*, 5(4):224–235, May 2014.

[83] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller, and Luca Delgrossi. Trust issues for vehicular ad hoc networks. In *Proceedings of Vehicular Technology Conference, Spring 2008*, pages 2800–2804. IEEE, 2008.

[84] Md Whaiduzzamana, Mehdi Sookhaka, Abdullah Gania, and Rajkumar Buyyab. A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, 40:325–344, 2014.

[85] Hsin-Te Wu, Wei-Shuo Li, Tung-Shih Su, and Wen-Shyong Hsieh. A novel rsu-based message authentication scheme for vanet. In *Proceedings of the fifth International Conference on Systems and Networks Communications (ICSNC)*, pages 111–116. IEEE, 2010.

[86] Hu Xiong, K. Beznosov, Zhiguang Qin, and M. Ripeanu. Efficient and spontaneous privacy-preserving protocol for secure vehicular communication. In *Proceedings of IEEE International Conference on Communications (ICC)*, pages 1–6, May 2010.

[87] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C Weigle. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, 14(1):284–294, 2013.

[88] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106–107, 2002.

[89] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin Han Ho. RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks. In *Proceedings of IEEE International Conference Communications. ICC '08.*, pages 1451 – 1457, Beijing, May 2008.

[90] Sheng Zhong, Li Erran Li, Yanbin Grace Liu, and Yang Richard Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks. *Wireless Networks*, 13(6):799–816, 2007.

[91] Lidong Zhou and Zygmunt J Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[92] Yanyan Zhuang, Jianping Pan, Yuanqian Luo, and Lin Cai. Time and location-critical emergency message dissemination for vehicular ad-hoc networks. *IEEE Jounal on Selected Areas in Communications*, 29(1):187–196, 2011.

# Vita

## Personal Data:

Name: Kiho Lim

## Educational Background:

- Master of Science in Computer Science, University of Kentucky, 2012.
- Bachelor of Engineering in Computer Engineering, Chosun University, South Korea, 2007.

## Professional Experience:

- Teaching Assistant, 08/2008 - 12/2015.
  Department of Computer Science, University of Kentucky, Lexington, KY, USA.
- Research Assistant, 05/2013 - 8/2013.
  Department of Library Science, University of Kentucky, Lexington, KY, USA.
- Research Assistant, 11/2010 - 02/2011.
  Department of Library Science, University of Kentucky, Lexington, KY, USA.

## Awards:

- Outstanding Presentation Award, 2015 KSEA-KY Winter Conference, University of Kentucky, Dec 2015
- Travel Funding Award for Scientists and Engineers Early-Career Development Workshop, Dec 2015
- Kentucky Opportunity Fellowship, University of Kentucky, 2015

- Travel Funding Award for ADHOC-NOW conference, 2015
- International Student Scholarship, University of Kentucky, 2015
- International Student Scholarship, University of Kentucky, 2014
- Travel Funding Award for CCNC conference, 2014
- Kentucky Graduate Scholarship, University of Kentucky, 2008
- Academic Excellence Scholarship, Chosun University, 2005-2007

## Publications:

- Kiho Lim and D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, Vehicular Communications, 4, 2016, Elsevier.
- Kiho Lim, Ismail M. Abumuhfouz, and D. Manivannan, Secure Incentive-Based Architecture for Vehicular Cloud, Ad-hoc, Mobile, and Wireless Networks (ADHOC-NOW 2015), LNCS 9143, Springer.
- Ismail M. Abumuhfouz and Kiho Lim, "Protecting Vehicular Cloud against Malicious Nodes Using Zone Authorities", in Proceedings of IEEE SoutheastCon 2015. Ft. Lauderdale, FL, Apr 2015.
- Kiho Lim, "Enticing Selish Nodes with Secure Token for Vehicular Cloud, 28th Annual Symposium in Mathematical, Statistical and Computer Sciences, Eastern Kentucky University. Apr 2015.
- Kiho Lim and Xiwei Wang, "NMF-Based Privacy Preservation in Vehicular Communication, in Proceedings of IEEE SoutheastCon 2015. Ft. Lauderdale, FL, Apr 2015.

- Kiho Lim and Ismail M. Abumuhfouz, "STORS: Secure Token Reward System for Vehicular Clouds", in Proceedings of IEEE SoutheastCon 2015. Ft. Lauderdale, FL, Apr 2015.

- Kiho Lim and D. Manivannan, "An efficient scheme for authenticated and secure message delivery in vehicular ad hoc networks, in Proceedings of the 12th IEEE Consumer Communications and Networking Conference (IEEE CCNC 2015). Las Vegas, Nevada, Jan 2015.

## Professional Service:

- Reviewer for Vehicular Communications Journal, 2016
- Reviewer for IEEE SoutheastCon Conference, 2016
- Reviewer for IEEE SoutheastCon Conference, 2015

## Career Development Activities:

- Scientists and Engineers Early-Career Development (SEED) Workshop, Vienna, VA, (Dec 2015)
- Grant Writing: Progressing from an Idea to Funding, University of Kentucky (Apr 2014)
- Effective Research Presentations, University of Kentucky (Apr 2012)
- Writing the Faculty Job Application Letter, Teaching Philosophy Statement, and
- Research Statement, University of Kentucky (Mar 2012)
- Piecing the Puzzle: Using Manageable Writing Tasks to Finish the Thesis or Dissertation, University of Kentucky (Nov 2011)

- Creating Grading Rubrics to Evaluate Student Work and Provide Useful Feedback, University of Kentucky (Oct 2011)
- Working with Undergraduate Students in Social Networking Environments, University of Kentucky (Mar 2011)
- Developing Effective Teaching Philosophy Statements, University of Kentucky (Apr 2010)
- Working with Undergraduate Students in Social Networking Environments, University of Kentucky (Mar 2010)
- Strategies for Effective Research Presentations, University of Kentucky (Oct 2009)