Establishing Security and Privacy in WAVE-enabled Vehicular Ad hoc Networks

by

Subir Biswas

A thesis submitted to
The Faculty of Graduate Studies of
The University of Manitoba
in partial fulfillment of the requirements
of the degree of

Doctor of Philosophy

Department of Computer Science
The University of Manitoba
Winnipeg, Manitoba, Canada
December 2012

Thesis advisors Author

Dr. Jelena Mišić and Dr. Rasit Eskicioglu **Subir Biswas**

Establishing Security and Privacy in WAVE-enabled Vehicular Ad hoc Networks

Abstract

Security and privacy are among the growing concerns of a Vehicular Ad hoc Network (VANET) which requires a high degree of liability from its participants. In this dissertation, We address security, anonymity and privacy challenges of VANETs in the light of the IEEE standards for vehicular communications.

VANET provides a variety of road-safety and other applications through wireless devices installed in vehicles and roadside infrastructure. A roadside infrastructure in VANET is generally public, and is prone to several different malicious attacks including node compromise, impersonation, and false message delivery attacks. Therefore, a user of a VANET must verify the integrity of a message that is delivered from a roadside infrastructure. On the other hand, a vehicle-originated message should be anonymous in order to ensure user-privacy in a VANET. However, a vehicle must not be able to take advantage of its anonymity for any misbehavior like sending false messages or malicious updates to other vehicles or a roadside infrastructure. We use proxy signature, identity-based signature, and elliptic curve cryptosystems to provide authentication for infrastructure generated messages, and anonymous authentication for vehicle originated messages.

Authentication in a dense traffic condition is a challenge for a receiving entity as it incurs a processing delay at the receiving end. We address this issue with a dynamic approach that selectively verifies received messages based on a message's MAC-layer priority and a sender's information relevance. This approach makes a trade-off between priority and fairness in vehicular message authentication.

We develop a network simulator to measure the impact of our authentication schemes over a WAVE protocol stack. Also, we investigate how some of the MAC-layer weaknesses may impair the security of a VANET. Our solutions are lightweight, bandwidth friendly and compatible to the current standards of vehicular communications.

Contents

List of Figures

List of Tables

Acknowledgments

Completion of my Ph.D. would have been impossible without the kind cooperation of my supervisors, advisory committee members, colleagues, and friends.

I would like to express my heartfelt gratitude to my Ph.D. supervisor, Professor Jelena Mišić for her warm encouragements and thoughtful supervision. With her extraordinary talent and academic skills, she has not only guided me to develop my research ability, but also inspired me to strive for excellence.

I would also like to thank my co-supervisor, Dr. Rasit Eskicioglu for his sincere support and cordial guidance for my Ph.D. dissertation.

My honest appreciation to the external member of the advisory committee, Dr. Soumaya Cherkaoui for patiently reviewing my dissertation, and giving her valuable comments. I would extend my gratitude to the internal members of the advisory committee: Dr. Ekram Hossain, and Dr. John van Rees for making their time and effort for reading my thesis, and giving their motivational remarks.

My special thanks to Dr. Vojislav Mišić who has always helped me with his ideas and useful insights on academic writings and publications.

Thanks to the administrative assistants and technical staff of the Dept. of Computer Science for their kind cooperation and sincere help.

I am grateful to Canada's AUTO'21 program for the research grant which I have received during my study at the University of Manitoba. My sincere thanks to the Dept. of Computer Science, Faculty of Science, Faculty of Graduate Studies, and the Province of Manitoba for awarding me numerous fellowships and grants.

Finally, special thanks to all my colleagues, friends and family members who have always been inspirational for me along the way.

Dedicated to the memory of my late beloved mother, Kamala Biswas.

List of Abbreviations

AC Access Category

AIFS Arbitration Inter-Frame Space

CA Certificate Authority/Central Authority

CCH Control Channel

CW Contention Window

DDoS Distributed Denial of Service

DoS Denial of Service

DOT Department of Transportation

DSRC Dedicated Short Range Communications

ECC Elliptic Curve Cryptography/Cryptosystems

ECDSA Elliptic Curve Digital Signature Algorithm

ECIES Elliptic Curve Integrated Encryption Scheme

EDCA Enhanced Distributed Channel Access

GPS Global Positioning System

HALL High Availability Low Latency

NIST National Institute of Standards and Technology

OBU On-board Unit

PKI Public Key Infrastructure

PRJ Parking Rejection

PTN Parking Token

PRQ Parking Reservation Request

PSC Parking Site Controller

RSC Roadside Controller

RSU Roadside Unit

SCH Service Channel

SIFS Short Inter-frame Space

UTC Universal Coordinated Time

WAVE Wireless Access in Vehicular Environment

WBSS WAVE Basic Service Set

WSA WAVE Service Announcement

WSIE WAVE Service Information Element

WSMP Wireless Short Message Protocol

Chapter 1

Introduction

1.1 Background

Road-traffic accidents claim thousands of lives every year in North America and all over the world [2, 3]. Statistics have shown that over 60% of all these mishaps take place in suburban areas, while probable causes include speeding vehicles, fewer traffic signals, no or less number of speed breakers, and lack of traffic surveillance or monitoring.

A Vehicular Ad hoc Network (VANET) is a significant innovation toward avoiding such deadly traffic mishaps with the assistance of a variety of state-of-the-art safety applications. A VANET is a self organized, multi purpose, service oriented communication network enabling vehicle-to-vehicle and vehicle-to-roadside infrastructure communication for the purpose of exchanging messages to ensure an efficient and comfortable traffic system on roads. It is commonly anticipated that this network would play an effective role for active safety in roads and highways

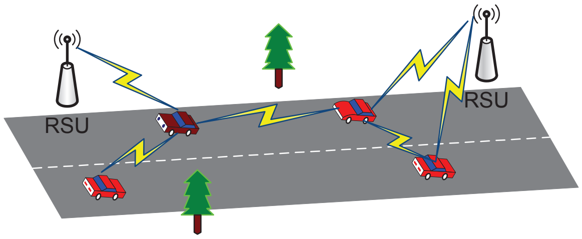


Figure 1.1: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication in VANET.

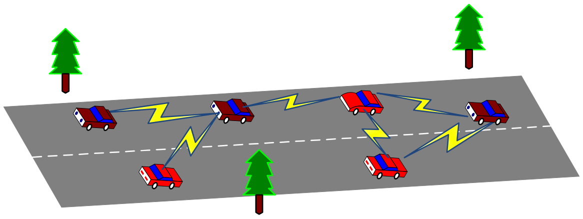


Figure 1.2: Vehicle-to-Vehicle (V2V) Communication in absence of the roadside infrastructure.

by introducing several different lifesaving applications for traffic management, driver's safety, and driver's assistance.

Research on VANETs has drawn a substantial interest among researchers, entrepreneurs, and car manufacturers around the world. Different aspects of VANET research have been discussed and analyzed with the goal of developing new, improved systems for safe traffic environment. Most of these applications are reliant on IEEE's vehicular communication standards: Dedicated Short Range Communications (DSRC [4]) and Wireless Access in Vehicular Environment (WAVE [1, 5, 6]).

In order to enable the effective ad hoc networks on road, each vehicle is equipped with a wireless communication device called an on-board unit (OBU), while roadside units (RSUs) are installed at the roadside locations as access points for OBUs. An OBU may broadcast information regarding vehicle's location, speed, acceleration, direction, and road condition; while an RSU may deliver road-safety application messages, traffic warnings, and changed road condition information.

According to the DSRC and WAVE standards (detailed in Section 1.3), an OBU or an RSU can exchange data over a single hop communication. Depending on the speed of the individual vehicles on road, the one-hop communication range is roughly equal to the distance over which a vehicle travels in 10 seconds (that is, between 15 to 300 meters). In a typical VANET scenario, RSUs are installed at the roadside locations so that each OBU can independently communicate with an RSU to exchange some safety or road condition information as indicated in Figure 1.1. Should there be no roadside infrastructure, vehicles would still be able to exchange traffic-safety or other application messages with each other as shown in Figure 1.2.

1.1.1 Scope of Vehicular Telematics

The area of vehicular telematics can be categorized according to the communication range and the impact of the communication type. There could be local area communications, wide area communications, and intra-vehicle communications.

Local Area Communications

Local area communications for VANET are those, where the impact of the communication is limited to the vehicles and/or roadside units in the vicinity of a target vehicle. For instance, a vehicle disseminates information regarding the speed, acceleration, braking information, GPS data, and road condition information periodically to the neighboring vehicles and RSUs. These periodic messages are collectively known as heartbeats. These heartbeats are to enable a safe and comfortable driving environment among the users of VANET on the street. A driver can also interact with other drivers in the OBU's communication range while driving.

Wide Area Communications

This category of telematics often results in a large scale dissemination of messages as required by most emergency and safety applications of VANETs. This type of communication can be initiated either by a vehicle or by the roadside infrastructure on a particular road condition or traffic situation. For example, vehicles approaching an accident site on a highway should be notified on time so that they can take detours and avoid the probable traffic hazards. A driver could also report about a certain road condition like a road-traffic congestion to other VANET entities (OBUs and RSUs) which can later broadcast the specific safety messages to the vehicles operating in a distant location in order to avoid a potential traffic hazard.

Intra-vehicle Communications

These are short range communications among wireless sensors within different parts of a vehicle. Modern day vehicles are equipped with some built-in sensors for monitoring brake efficiency, carbon emission, engine's heat/temperature, tire pressure, and road-traffic collision. These would reduce the risk of mechanical failure of a vehicle while in operation. An auto generated failure warning could alert a driver about on time maintenance of the specific part of the vehicle.

1.2 VANET Applications

The main motivation for an effective VANET is to have not only intelligent vehicles on roads, but also smart roads to provide safer driving environment. As mentioned earlier, VANETs have been considered for several different potential applications including road-safety, efficient driving, vehicle-to-vehicle communications, car maintenance, and multimedia applications. Generally, all these anticipated applications fall into following categories.

1.2.1 Road-safety Applications

More than 90% of the fatal road accidents take place due to drivers' error [7]. Hence, road-safety Applications are to assist a driver to have a better perspective about the surroundings of a vehicle in order to avoid potential dangers. These can be further divided into following subcategories of applications.

General Safety

General safety applications include several different automated warning systems to alert the driver about the traffic. These warnings are mostly pre-determined ones and usually unchanged for a given location. Such applications include traffic signal violation warning, stop sign violation warning, intersection ahead warning, pedestrian crossing alert, blind spot warning, rail crossing warning, milestone notifications, and wrong way driving warning.

Traffic Scenario Based Safety

These are the traffic safety applications that use dynamic safety alerts which may change according to the traffic situation on a specific road. Emergency vehicle approaching alert, pre-crash warning, road maintenance in progress alert, and changed road condition alert (e.g., slippery/wet road warning, and snow alert) are some of the possible applications in this category. These applications would improve driving safety, as well as provide enhanced driving comfort.

Post-incident Safety

Should there be an abnormal situation on the road, an approaching vehicle has to be notified so that drivers of such vehicles would be able to avoid the probable hazard at that specific location. For instance, a collision in the middle of a highway may cause a heavy traffic congestion which can possibly be avoided if oncoming vehicles are notified about the mishap before they enter the highway. Similar applications can be developed for slow traffic, or traffic congestions on certain roads and highways.

1.2.2 Traffic Assistance

Applications are emerging to assist drivers to enable efficient road and highway usage. Likewise, there can be cooperative platooning of vehicles or adaptive platoon management for a highway, fleet management applications, highway merge assistance, highway access control applications, and electronic toll collection for providing an intelligent traffic flow on roads. Also, different electronic surveillance systems can be developed and deployed as part of the law enforcement on roads.

1.2.3 Commercial Applications

VANET services that are provided to the user for revenue belong to the category of commercial applications. Depending on the target area and policy, there can be one or multiple VANET service providers. Potential applications include various download operations including maps, multimedia contents, and software updates. Instant messaging between vehicles may assist drivers on their driving safety and comfort. Commercial applications may also involve other parties than just vehicles and drivers. For example, there could be event specific commercial advertisements of the nearest shopping mall, a nearby restaurant, or any other point of interest to the vehicles on a particular road. Interested business organizations in a given location may tie up with the VANET service provider(s) to disseminate their commercial information to the users of the VANET on a timely basis. As a matter of fact, these potential applications are generally anticipated to be the major source of profit for the investors, and entrepreneurs of the whole VANET system, and thus, success of VANETs would highly depend on this particular type of applications.

1.3 DSRC and WAVE Overview

In December 2003, The Federal Communications Commission (FCC)— an independent US government agency responsible for licensing and regulations of frequency for the US and North America, adopted a 75 MHz spectrum from 5.850 to

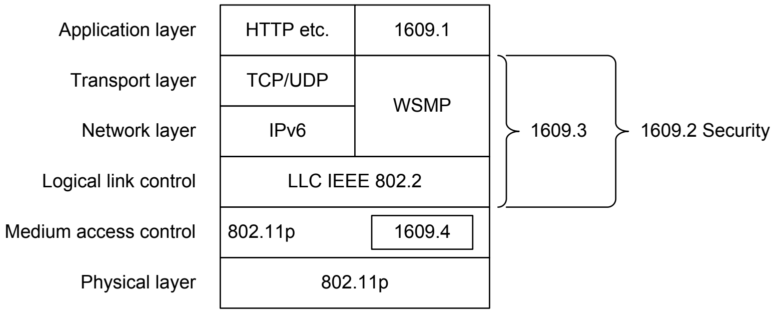


Figure 1.3: 1609.x and IEEE 802.11p DSRC Layers for a WAVE-based VANET.

5.925 GHz band known as the Dedicated Short Range Communications (DSRC) for the Intelligent Transportation System (ITS). The DSRC spectrum enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications for both public safety and commercial applications. DSRC applications are to be built over OBUs and RSUs.

The IEEE Std 802.11p, and the protocol stack 1609.x [1, 5, 6] together define the foundation for the wireless communications among different entities (OBUs and RSUs) of VANETs. The IEEE protocol suite of 1609.x is also termed as Wireless Access in Vehicular Environment (WAVE). As indicated in Figure 1.3, WAVE provides security applications (1609.2), networking services (1609.3), and multi-channel operations (1609.4), while DSRC characterizes the IEEE 802.11p PHY-layer that has been modified from IEEE 802.11a [8] by incorporating the Orthogonal Frequency Division Multiplexing (OFDM). Nevertheless, both DSRC and WAVE are used interchangeably in the context of vehicular communications.

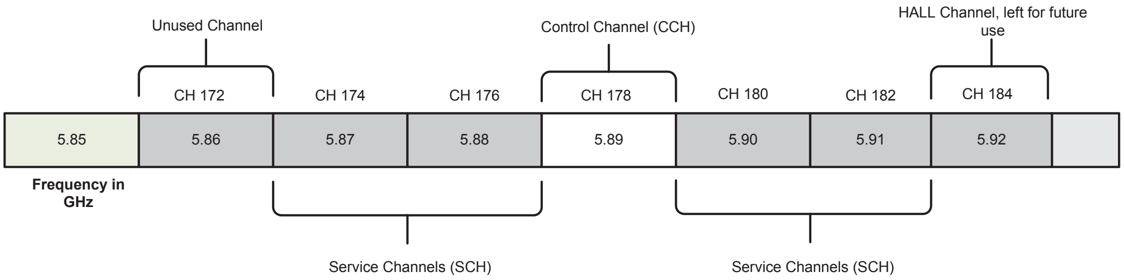


Figure 1.4: DSRC 5.9 GHz band spectrum.

1.3.1 IEEE 802.11p Radio

As indicated in Figure 1.4, the DSRC standard provides seven channels with each having 10 MHz of bandwidth. Within the 5.9 GHz spectrum, channel 172 is an unused channel as of the most recent prototypes, while channel 184 is the High Availability Low Latency (HALL) channel kept for future use. Channels 174, 176, 180, and 182 are defined as service channels (SCH), whereas channel 178 is specified as the the control channel (CCH) for the WAVE communications.

Two consecutive DSRC channels can be combined to one when additional bandwidth is required by a VANET. A 10 MHz channel offers the data rate up to 27 Mbps, where 3, 6, and 12 Mbps data rates are mandatory. A 20 MHz combined channel would offer a maximum of 54 Mbps with mandatory data rates of 6, 12, 24 Mbps.

However, data transmission rates in WAVE communication also depend on different speed levels of vehicles. A vehicle speeding 0-60 Km/hour can achieve VANET data rates 9, 12, 18, 24, and 27 Mbps, whereas, for 60-120 Km/hour vehicle speed, date rates 3, 4.5, 6, 9, and 12 Mbps are achievable.

The communication range of an IEEE 802.11p device using the 5.9 GHz radio is limited to 1 Km at the most, which varies based on the different transmission power of the WAVE transceiver. Vehicles (OBUs) join and exchange information with their nearest RSU's WAVE Basic Service Set (WBSS) [1]. A vehicle's dwell time may be as short as 3.6 sec [9]. This short dwell time of an OBU in a WBSS allows VANET applications only with low processing time and latency.

By default, WAVE devices operate on the control channel (CCH). This channel is reserved for short, high-priority application and system control messages. WAVE announcement frames are only allowed to be transmitted over the CCH, while other management frames may use the SCH. Both CCH and SCH can be utilized for regular data transfer.

1.3.2 WAVE Multi-channel Operation

A single-channel WAVE device can not transmit or receive using more than one channel at a time. In order to enable various WAVE applications to operate on a single-channel device, A WAVE device (OBU or RSU) switches between the CCH and at least one SCH. It is mandatory for a WAVE device to monitor the CCH on a regular interval. Since WAVE devices are single channel devices, in order to enable them to transfer data over SCH while monitoring the CCH, time synchronization of WAVE devices is obvious.

IEEE 802.11p requires time synchronization of WAVE devices. This is accomplished by using Coordinated Universal Time (UTC) with reasonable accuracy—commonly provided by Global Positioning System (GPS). Figure 1.5 shows the sync interval, guard interval, CCH interval, and SCH interval for the synchronized WAVE communications. CCH interval begins with the start of each UTC second,

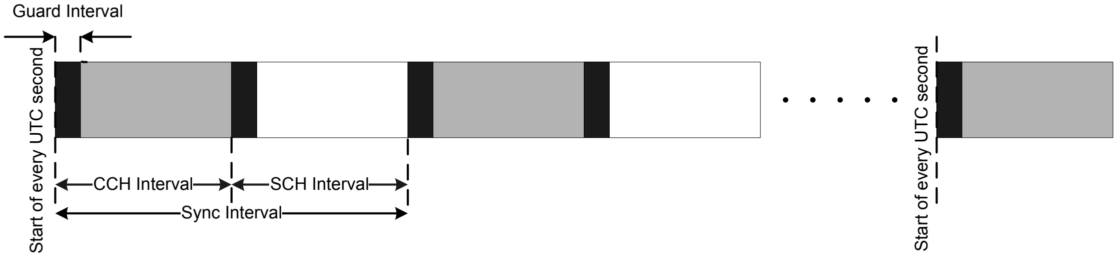


Figure 1.5: Time synchronization for WAVE devices.

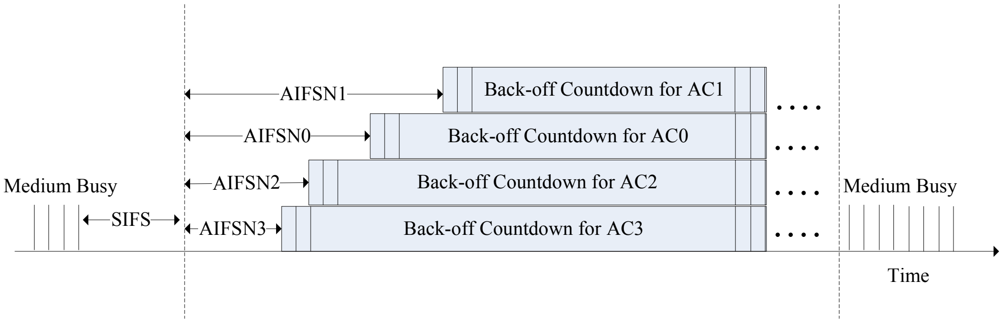

AIFSN1
Back-off Countdown for AC1
AIFSN0
Back-off Countdown for AC0
Medium Busy
AIFSN2
Back-off Countdown for AC2
Medium Busy
SIFS
AIFSN3
Back-off Countdown for AC3
Time

Figure 1.6: IEEE 802.11p EDCA mechanism.

and a guard interval is at the beginning of both SCH and CCH to comply with the possible time synchronization inaccuracies among different devices. Duration of CCH and SCH intervals may vary, resulting in different tradeoffs in channel performance [10]. Recent evaluations of IEEE 802.11p [11] consider each of SCH and CCH intervals as 50 ms, while the Sync interval is 100 ms. Besides time synchronization, IEEE 802.11p incorporates Enhanced Distributed Channel Access (EDCA) mechanism to enable prioritized transmissions in DSRC channels.

WAVE Multi-channel Operation [1] allows different access priorities among traffic classes. The access priorities of traffic classes let WAVE applications contend for the medium using EDCA mechanism. The concept of user priority in DSRC has been borrowed from the IEEE 802.11e EDCA mechanism [12] to induce the prioritized access for data transmission on each DSRC channel. Access over each channel is contended by four access categories: AC0, AC1, AC2, and AC3. Two channel access parameters, namely the Arbitration Inter-Frame Space (AIFS) and Contention Window (CW), along with a fixed value Transmit Opportunity (TXOP= 0) jointly define the four EDCA access categories for independent channel access function. Figure 1.6 illustrates IEEE 802.11p EDCA mechanism.

A VANET entity wishing to transmit a data frame of a specific access class (AC_k, where $k = 0..3$) would first listen to the medium for $AIFS_k = SIFS + AIFSN_k \times Slot\ Time$ period to check the availability of the medium. If the medium is busy during the $AIFS_k$ time, sender node cancels the timer, and waits a complete $AIFS_k$ period once the medium is idle again. The sender node then performs a back-off countdown whose length is determined by a random number between 0 and the minimum contention window (CW_{min_k}).

If the medium becomes busy during the back-off count, sender node freezes the timer until the medium is idle. The sender node resumes its frozen back-off timer following a fresh $AIFS_k$ waiting period. When the back-off count reaches to 0, the data frame is transmitted. However, if retransmission of a data frame is needed (due to frame loss, or a lost ACK), the size of the CW is doubled in each retransmission attempt until maximum limit (CW_{max_k}) is reached.

1.3.3 WAVE Networking Services

The IEEE 1609.3 standard defines protocols for networking services in VANETs. This standard specifies the logical link control (LLC), network, and transport layer functions. A provider of VANET services disseminates WAVE Service Announcements (WSA) for announcing the availability of a WAVE Basic Service Set (WBSS). This WSA is transmitted in a special message template called WAVE Service Information Element (WSIE) which may contain secured WSA in it. A secured WSA includes a signed message, but the application data is the original unsigned WSA payload. This secured WSA also comes with a short lifetime of no more than 5 seconds.

The IEEE Std 1609.3 [6] provides WAVE communication services by accommodating WAVE Short Message Protocol (WSMP) and IPv6. WSMP may initiate a WBSS to make a particular SCH available. Otherwise, CCH can also be used for data transfer. Two different types of operations have been suggested by the standard: operations with WBSS, and operations without WBSS. For the first case, the service is announced over CCH, and data packets are sent over SCH. For the latter kind, WSMP is sent on CCH only which is broadcast using the broadcast MAC address of the sending device. Note that each WAVE device is assigned with a unicast MAC address, in addition to which a broadcast MAC address is also supported. These addresses are changeable by application layer protocols.

WAVE supports two distinguished categories of WBSS: persistent and non-persistent. A persistent WBSS is announced periodically during CCH interval. It may offer an on-going service to a newly joined vehicle. A non-persistent WBSS is announced only on WBSS initiation, which can be used for providing limited duration on-demand services.

WAVE BSS (WBSS)

DSRC introduces a new type of Basic Service Set called WAVE BSS or WBSS which is initiated when a WAVE device transmits an on-demand beacon to advertise the WBSS. The on-demand beacon contains all needed information for the offered services, as well as necessary configuration parameters for a node joining to the WBSS. The receiving node can decide whether to join or ignore the WBSS advertisement based on the information provided in the beacon. This mechanism avoids multiple handshaking for the network association among WAVE devices.

WAVE Mode

The IEEE 802.11 MAC operations are substantially time consuming for DSRC operations due to its rapidly varying environment. Therefore, IEEE 802.11p introduces an amendment over IEEE 802.11 called WAVE mode. In this mode, a WAVE device can send and receive messages using a wildcard ID without needing any prior association with any BSS. This mechanism allows any two vehicles in the communication range to communicate with each other right away without any additional handshaking.

1.3.4 WAVE Security Services

Security issues in DSRC/WAVE communications are addressed in the IEEE Std 1609.2 [5] which defines essential security primitives like public key encryption and non-anonymous authentication protocols. The standard also specifies WAVE management and application message security mechanisms. Elliptic Curve Digital

Signature Algorithm (ECDSA) over two standard NIST curves: P-224 and P-256 has been specified for WAVE message signing operations. While the standard suggests Elliptic Curve Integrated Encryption Scheme (ECIES) as the sole asymmetric encryption algorithm, provision for customized application layer and network layer algorithms makes VANET security functions flexible and adaptable.

1.4 Motivation for Research

Security is an integral part of any communication system. The large network span, high degree of mobility, and transient nature of the vehicle association pose some unique challenges that make the common mechanisms of ad hoc networks inappropriate for VANETs. The ad hoc nature of the network with its self-organized operations, as well as the service-oriented scopes make a VANET prone to a number of anti-social and criminal activities which eventually could jeopardize the usability of the network.

In order to prevent these, an obvious choice is to have secure authentications between RSUs and OBUs, and among OBUs as indicated in WAVE security services [5]. However, modern day consumers are extremely privacy-concerned who would not like to expose their actual identities in a public domain like VANET. For instance, a driver would not like to be traced and fined for speeding his vehicle. Hence, maintaining driver's privacy is very important for a VANET provider. Nonetheless, a user has to be accountable for his potential misbehavior in a VANET since it would be unacceptable if a vehicle can manage to run away after a harmful and malicious conduct on road.

Therefore, security and privacy issues are among the most crucial challenges for the future of VANET. However, we must consider the cost of security and privacy assurance on essential and user-specific VANET applications. In this work, we focus on VANET security and privacy research, as well as its implications over various communication issues.

1.4.1 VANET Security Challenges

In a service oriented and interactive network like VANET, a potential adversary could be among the consumers or within the service providers. For instance, in order to have a congestion-free drive, a 'greedy driver' may attempt to take advantage by disseminating false traffic congestion warning for the road s/he is approaching. Some insider adversaries working for the service provider may illegally track a driver's daily route, identity, and other sensitive information with an intention to use them in future. Also, a malicious attacker may compromise a legitimate OBU or an RSU to impair the traffic safety and warning system.

Potential adversaries, as well as several different anticipated attacks on vehicular networks have been classified by Parno et al. [13] and Raya et al. [14]. We divide the most commonly anticipated misbehavior and attacks on VANETs according to the involved communication layers in a VANET.

Attacks on Application Layer

These are the attacks launched by malicious entities on the Application layer of a WAVE-based VANET.

- **False Message Attack:** An adversary may abandon a VANET by deliberately broadcasting false information into the network regarding an emergency road condition, a safety warning, or a collision report. The situation would be even worse if an attacker can successfully convince a user to install a malware (malicious software) update in the OBU. Also, a malicious user may use a fake identity or a false location information in order to become un-traceable for an investigation after committing a crime. Similarly, an adversary may take over a roadside infrastructure to make it deliver false data or unnecessary warnings to degrade the effectiveness of the network. If an attacker can manage to compromise an electronic toll collection system, the whole transportation network will suffer from fatal consequences. Therefore, the originator of a message must be authenticated, as well as the message integrity should be verified by the receiving node upon reception.

- **Attack on Message Integrity:** An intermediate node in a vehicular communication may modify the actual packet content to deceive the receiving node [13]. Hence, this attack is a different approach of false message attack discussed above. In a similar kind of attack, an adversary selectively drops the relaying packets to destabilize a VANET.

- **Trust-based Attacks:** *Exculpability* and *Repudiation* are attempted by an adversary to launch trust-based attacks in a network. The former refers to an attack where the adversary tries to replicate another valid node's signature on its own message, so that the signature appears to be given by a legitimate node. The latter takes place if a malicious node signs a message, but later on denies its involvement in signing it. Another undesirable situation for a vehicle using VANET is *signature linking*— meaning that an adversary (most likely an insider at the provider end) may store all or some of the anonymous signatures delivered from a vehicle over a period of time, and can successfully link them to determine the vehicle's identity, route, and other activities. Thus, signatures given from a vehicle must be unlinkable for anonymous user authentication in VANETs.

Attacks on Network Layer

Attacks of this category capitalize on the Network layer weaknesses of entities in a VANET.

- **Impersonation Attack:** In an impersonation attack, an adversary masquerades as another entity to commit a malicious act. This attack has several different aspects. For example, an adversary may pretend to be an emergency vehicle to speed up and mislead the other vehicles on road. Again, an attacker may use another legitimate node's identity, location information to abuse the reputation of a legitimate node, and to harm regular traffic activities.

- **Sybil Attack:** This is an attack on network routing protocols, where a node maliciously advertises several different fake identities and pretends as multiple nodes with an intention to misguide the other entities (i.e. RSUs and OBUs) [15]. When RSUs and OBUs prepare their routing tables, they consider those fake identities as the legitimate ones, and eventually the message transmission fails.

- **Traffic Analysis Attack:** This category of attacks in VANETs allows a malicious node to illegitimately build a communication profile of a VANET entity. This is a threat on user-privacy in VANETs, where an adversary obtains users' information like communication patterns, periodicity of transmissions by simply following a victim node's incoming and outgoing traffic.

Attacks on MAC and PHY Layers

These attacks in VANETs involve WAVE's MAC and PHY layers.

- **Denial of Service Attacks:** In this category of attacks, an adversary deliberately occupies network resources to prevent the regular activities of the network. In most cases, an attacker floods the network with false and useless data, or attempts to repeatedly generate unnecessary requests to a provider. Denial of Service (DoS) also means to interfere the transmission channel of the network in order to disrupt the actual communication. This attack can easily thwart a VANET system as it doesn't require any cryptographic effort. An attacker would simply need a low-power transmitter from a roadside location for launching a denial of service attack.

- **OBU Tampering Attack:** This is a form of physical attack in which a malicious entity may tamper an OBU to steal the secret credentials for signature generation and authentication. Adversaries may also collude to temper their own OBUs and broadcast false vehicle information like speed, location, acceleration for denying their liabilities in a traffic dispute [14].

Legal Issues

A VANET would involve a large community of consumers, a number of industrial partners, insurance providers, and the traffic administrations (e.g., licensing authority, department of transportation, and police) of countries, states, or provinces. Hence, it would be essential to have a thorough review of existing legislations, as well as the introduction of new laws for an appropriate coordination among involved parties.

The law must protect a user's right of privacy, anonymity, and other relevant issues while using a vehicular network. It should also provide a guideline to the user for maintaining the safe driving environment on roads and highways.

1.5 Research Contributions

The main goal of this thesis is to develop a suitable security and privacy platform that can support large scale VANETs by ensuring message integrity, anonymous authentication, user accountability, data confidentiality for user applications, and resource availability. The major contributions of this research are:

- We introduced a proxy signature based authentication scheme for VANET, which allows an RSU to sign an emergency or other application message on behalf of the corresponding service provider. An OBU can distinctively verify the signature as a proxy signature which confirms the message integrity, source authentication, and accountability of a signing RSU. Also, an OBU can deliver its own messages with anonymous and conditional signature. Multiple sets of OBU credentials provide the user-anonymity in the authentication scheme.The actual identity of an OBU can be revealed only by the third-party trusted authority.

- Two forms of identity-based authentication have been developed using elliptic curve cryptography for VANET safety messages. RSU messages can be authenticated to ensure the user trust and message integrity. It also provides conditional privacy-preserving authentication to OBU messages. In each case, the location information is used as the identity of the sender. This approach waives the necessity of a trusted third-party certificate for the verification, which saves on the network bandwidth and memory space.

- A high density road-traffic condition poses a challenge for authentication of vehicular messages since required verification time is often much longer than the average inter-arrival time. We have designed an adaptive verification strategy that exploits cross-layer communication features of WAVE-based VANETs and information relevance for verifying the received safety messages. Messages of each traffic class are verified following the corresponding verification probability which depends on VANETs MAC-layer priorities and the intensity of messages in each access category.

- We proposed a secure, privacy-preserving parking assistance application using priority-based vehicular communications. The proposed scheme utilizes two modified Elliptic Curve algorithms for vehicular message authentication between client vehicles and corresponding infrastructure. We addressed the major challenges associated with VANET security and user privacy. The standard Wireless Access in Vehicular Environment (WAVE) protocol suite has been used to construct our signature mechanism, application data secrecy, and message integrity.

- A VANET that uses IEEE 802.11p EDCA mechanism is susceptible to a synchronization-based DDoS attack due to periodicity of transmissions and small contention window sizes. Neither the sender nor receivers of periodic broadcasts would be aware of the attack since broadcast communications in VANET do not have acknowledgements. We analyzed the prospect of such attacks, and proposed various mitigation techniques to avoid them in VANETs.

- We designed a WAVE-based network simulation model with NS-2.34 [16] to evaluate our security schemes running on the WAVE protocol stack. DSRC MAC-layer defined in IEEE Std 1609.4 [1], has been implemented in our simulation along with the sync interval structure and EDCA mechanism for four access classes over CCH. Our simulation model also includes an implementation of Wireless Short Message (WSM) protocol following IEEE Std 1609.3 [6], while messages have been formatted and transmitted according to IEEE Std 1609.2 [5].

1.6 Thesis Outline

The rest of the thesis is organized as follows. A literature review of current research on security and privacy issues in VANETs has been given in Chapter 2. Chapter 3 introduces a proxy signature approach to mitigate VANET safety message authentication with trust and user-privacy. Chapter 4 illustrates a new identity-based authentication scheme for RSU safety messages, where the location information of a VANET entity is used for signature generation and verification. A conditional privacy-preserving message authentication scheme is illustrated in Chapter 5 which also includes a dynamic message verification mechanism based on the message priority and relevance. Chapter 6 describes a secure and privacy-preserving parking assistance application that uses identity-based authentication schemes for RSU and OBU messages. Chapter 7 presents a potential DDoS attack on VANETs based on periodic message synchronization. Chapter 8 contains the concluding remarks and direction of future research.

Chapter 2

Related Work

It should come as no surprise that a number of research papers have proposed and analyzed various security, privacy and anonymity schemes in recent years. In this chapter, we survey the existing work on VANET security and privacy based on their cryptographic techniques, implementation methodologies, functionality, and other important characteristics. We identify the pertinent characteristics of different approaches and highlight their comparative advantages and disadvantages.

Figure 2.1 summarizes distinguished types of the recent VANET security and privacy approaches.

VANET applications that require communications among OBUs or between an RSU and OBUs, should be authenticated to establish adequate trust on the data source. While authenticity and data integrity are important, a secure VANET may expose the identity of a user in public or to a malicious individual. Therefore, as long as user-privacy is concerned, a good privacy-preserving secure communication scheme is a crucial prerequisite. Again, in a critical situation or in a traffic

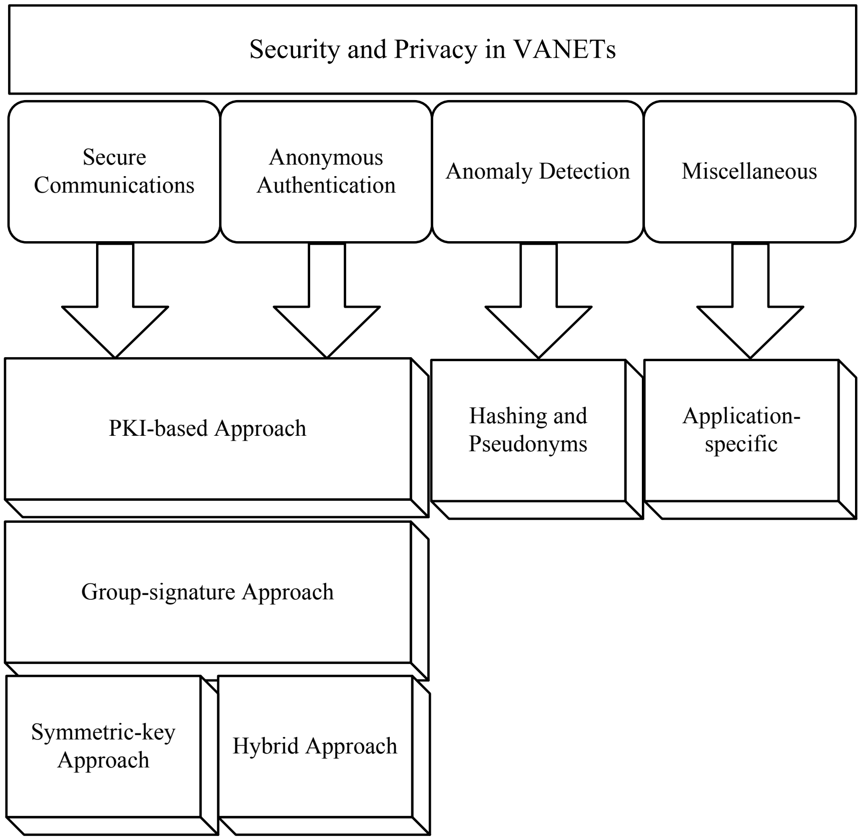


Figure 2.1: A taxonomy of existing security and privacy approaches for VANETs.

dispute when a user is needed to be identified, the appropriate authority should be able to retrieve the user's actual identity.

Most of the existing privacy-preserving vehicular communication schemes use either an ordinary public key infrastructure (PKI)-based approach, a group signature based approach, or a 'hybrid' approach.

2.1 Public Key Infrastructure (PKI)-based Approaches

Raya et al. [17] described authentication and privacy issues as fundamental security features in VANETs. In their PKI-based approach, each message from an

OBU is signed using its private key while a certificate from a trusted authority is attached with the message. The receiver OBU or an RSU then checks the certificate for the authentic public key of the sender, which is used for verifying the signed message. To keep the overhead low, Elliptic Curve Cryptography (ECC) has been suggested, while it is also recommended that only critical messages should be signed by an OBU.

Certificates of a malicious node must be revoked to prevent future intrusions and attacks on the network. Three different techniques have been suggested for the compromised certificate revocation in a VANET, namely Revocation Protocol of the Temper Proof Device (RTPD), Revocation Protocol using Compressed Certificate Revocation Lists (RCCRL), and Distributed Revocation Protocol (DRP). In RTPD, the certificate authority (CA) encrypts a revocation message by OBU's public key and send it to the corresponding OBU which then deletes all the keys and returns an ACK to the CA. This communication can be accomplished through the base station. The RCCRL approach uses Bloom filters to test the membership of any given certificate in a set of revoked certificates. In RCCRL, the size of the list of revoked certificates is fairly short and neighboring vehicles are also aware of the revocation list. Unlike RTPD and RCCL, DRP runs on each vehicle, while neighbors can revoke the certificate of a vehicle when any misbehavior from the malicious vehicle is detected.

To enforce the privacy, Raya et al. [17] suggested the use of a number of short lived anonymous keys which would expire once they are used. These keys are certified by the CA and are preloaded in every OBU. In each session, a vehicle will be using a separate key for authentication so that no one can track the actual identity of the vehicle. In case of a dispute, the actual identity of the vehicle (which is an electronic license plate) can be traced back by the CA. The details of this framework is yet left as an open issue for research.

Sun et al. [18] addressed the revocation of anonymous certificates in VANETs. A bilinear pairing based technique [19], as well as a one-way hash functions keep the size of the revocation list linear with the number of revoked OBUs in VANET. In this approach, an OBU updates the trusted third-party certificates by re-signing them with corresponding RSU-keys. However, this scheme requires RSUs at regular intervals of VANET-enabled roads and highways. Secondly, since RSUs are installed at the roadside locations without due surveillance and physical protection, they are vulnerable to compromise attack. Therefore, implementation of such scheme would be expensive and yet prone to malicious attacks.

Lu et al. [20] presented a solution that resolves the issue of RSU compromise attack, while it requires multiple handshaking between an OBU and an RSU for vehicular authentication. Like Sun et al. scheme, this approach also requires an uninterrupted coverage of RSUs in the VANET.

2.2 Group-signature Approaches

A group-signature based approach has been proposed by Chaum et al. [21] for providing privacy-preserving security in VANETs, where user-anonymity is ensured as each group member signs messages using the indistinctive group signature. In a group-signature approach (e.g., [21, 22]), a member of a group can sign a message on behalf of the entire group where the identity of the signing member remains anonymous within the group. No one inside or outside the group would know the actual identity of the sender, while it is possible to find the group the sender of the message belongs to. A group manager in each group can essentially open any signature signed by a member of a particular group using its group manager secret key (*gmsk*). In case of any dispute when it is crucial to track the signing member, corresponding group manager is intervened. Note that it is computationally infeasible to determine the actual identity of a group member just from its signature without having the *gmsk*. Apart from anonymity, this scheme provides some other desirable features like unlinkability (meaning that no identifiable link may be found between two signatures even if they have been used by the same source), exculpability (no member can fake a signature of another member and can not masquerade a message as delivered by a different source), unforgeability (message should not be forged by an outsider so that it appears to be sent by a member of another group), and coalition-resistance property which makes it impossible for a subset of the group to collude and fake another group member's signature.

In this group-signature based communication framework, six following fundamental components have been suggested for security and privacy control:

- *capability check* to defeat malicious message sender,
- *signature generation* for data authentication,
- *firewall* to block unsigned messages as viruses, worms, and DoS attacks;
- *signature verification* using the particular group public key to determine the

group of the sender,

- *authorization check* determines if the sender group has the privilege to send the message, and
- *anomaly detection* confirms the consistency of the received message.

To increase the efficiency of the scheme, authors suggested a probabilistic verification of signatures by vehicles. That is, instead of verifying each and every signature, a vehicle will randomly check a few received messages. A theoretical analysis by Guo et al. [23] showed that for up to $n = 1000$ nodes in a VANET, 95% of broadcast messages are authenticated if each OBU randomly verifies just 3 messages per n messages received. To ensure scalability of the network, access rights would be assigned to groups instead of individual vehicles. RSUs can be grouped mainly based on their given role, while OBUs can be grouped on the basis of geographical locations. A group manager is responsible for the accountability of each group member. However, it has been suggested that the role of a group manager can be divided into several authorities by escrowing [24] a group manager secret key (*gmsk*) among them.

Lin et al. [25] proposed a secure and privacy-preserving protocol for vehicular communications using group signature and ID-based signature schemes for Vehicle-to-Vehicle and infrastructure-to-vehicle communications respectively. For vehicle-to-vehicle communication, the suggested network design includes a membership manager (MM), a tracing manager (TM), and OBUs of communicating vehicles. All vehicles in the network are essentially registered with the MM and preloaded with group public key as well as individual private keys. Vehicles on road may broadcast time synchronized traffic safety messages containing traffic information like speed, geographical positions, acceleration, and deceleration. An implementation of short group signature scheme [22] is used in each OBU for signing the broadcast messages. As mentioned earlier, a group signature allows any member in a group to anonymously sign a message on behalf of the group, while the signing individual is still traceable upon any dispute or on a critical circumstances with TM and MM being consulted. Before the actual signature verification, a receiving OBU would first check for the time information of the message to make sure that the message has been received during the allowable time window, otherwise the message is discarded immediately.

Upon detecting a compromised OBU or a stolen Vehicle/OBU, the compromised entity must be revoked from the network. The proposed protocol uses a hybrid method of node revocation, in which if the number of revoked nodes is below a predetermined threshold, a verifier-local revocation (VLR) [26, 27, 28] scheme is used. VLR is efficient only for a small number of compromised entities. In case if the number of compromised node is higher than the threshold, the group public key and the individual private keys are updated on each legitimate member OBU leaving all compromised nodes unable to update the keying materials.

On the other hand, RSU-to-OBU communications use an ID-based signature scheme [29] in which the location information of the RSU is used as the public key for the message signature. Each message sent from an RSU contains its physical location information so that when a message is received at an OBU, it can be verified by comparing the actual location of the RSU and the location information in the message. This is how the proposed protocol prevents the RSU-to-OBU communications from a probable replication attack since messages from an RSU will be discarded if the RSU is relocated by an adversary.

However, this approach doesn't address a probable node compromise scenario where an RSU can be taken over by an adversary to deliver false and harmful messages. Moreover, privacy and security challenges of OBU-to-RSU communication were left unattended. The revocation schemes suggested are also not scalable and they are less effective for a large administrative area of transportation networks.

An OBU and an RSU should be mutually authenticated without directly using vehicle's real identity. Nonetheless, authentication in a vehicular environment is somewhat different from the traditional authentication approaches. Most vehicular network authentication schemes rely on either a trusted authentication server or a roadside unit (RSU). Taking into account the inherent vulnerabilities of wireless broadcast communications, there are a number of approaches addressing VANET authentication based on a numerous customized network services, as well as available cryptographic protocols. However, not all these authentication approaches essentially prioritize privacy and anonymity issues over other fundamental VANET requirements.

A group-based adaptive privacy-preserving authentication scheme has been suggested by Sha et al. [30] where a user can choose his degree of privacy according to the network resources an OBU can afford. High privacy requirement will incur a huge communication, computation, and memory overhead; while a low privacy level costs resources in small amount. In this scheme, each OBU is pre-loaded with an ordered list of all public keys for the whole group. An OBU then constructs a binary tree where public keys are at the leaves and each of the subtree root is expressed by a binary number. All RSUs have the current version of this tree and the authentication process uses the tree for the shared secret verification.

The process is essentially initiated by an RSU which broadcasts its certificate signed by a certificate authority (CA). An OBU seeking for authentication would verify the identity of the RSU using CA's public key before an OBU send out the authentication request. The authentication request includes a session key, a timestamp, and most importantly, the index of a subtree root that indicates the level of privacy sought by the user; while the subtree must contain the OBU's public key. The RSU then prepares a challenge string using all the public keys of the binary tree and sends to the OBU. An OBU partially decrypts the challenge by its own private key to get the answer of the challenge and then encrypts the challenge message by all other public keys in the subtree to check the validity of the RSU. Once the RSU is verified by the OBU, it sends back the challenge using the session key and a timestamp for message freshness. This adaptive scheme provides an opportunity for mutual authentication between an OBU and an RSU since both of them share the same tree of public keys. The level of required privacy can be preset by a user.

This protocol has scalability problem, and it can hardly be considered for a practical application. This is because, each OBU requires to keep the public key of every other vehicle in the group. The group size might change quite frequently. Therefore, OBUs must be updated every now and then which would be very inefficient for a realtime system like a vehicular network.

Wu et al. [31] proposed a message linkable group signature (or MLGS) for anonymous authentication in VANETs. Sybil attacks in VANETs can be thwarted with this approach as the actual identity of the sender is detected if it signs a message more than once. This scheme relies on bilinear-pairing groups, and a cryptographic primitive called threshold cryptography [32], where an adaptive algorithm enables a receiver to trust a message only if the message is endorsed by at least a predefined number of anonymous vehicles.

Parno et al. [13] suggested a privacy primitive called *anonymization service* for VANET authentication where a specialized third-party trusted entity is responsible for delivering a temporary certificate to substitute the permanent identity of a VANET user. Authors argued that a vehicle does not need to authenticate the exact identity of another vehicle, rather, it is good enough to authenticate the link between the received information and the sender vehicle. Thus, a vehicle can use the temporary certificate to authenticate itself to other vehicles on road. This certificate is irreversible by an adversary, though an authorized entity can trace back the original identity from a temporary certificate. This mechanism prevents identity spoof, and preserves the privacy of a driver. A simple extension of the idea recommends the use of re-anonymizers that would provide fresh temporary certificates to vehicles upon receiving their old temporary certificates. A vehicle would renew its certificates as soon as another re-anonymizer is available in its vicinity since a certificate comes with an expiry time. It is extremely hard for an adversary to identify a driver's actual identity even if he collects a number of temporary certificates.

In this scheme, a vehicle would be unable to authenticate itself once the temporary certificate is expired in a location with no anonymizer around. Again, if the vehicle achieves multiple valid certificates, it may launch a Sybil attack as there is no provision for certificate revocation with this approach. Also, planning the right spots for re-anonymizers in a transportation network would be a challenge.

2.2.1 Symmetric-key Approach

Xi et al. [33] proposed a more effective and scalable privacy-preserving authentication scheme using symmetric random key set in VANETs. A set of random keys are chosen for each vehicle from a large central key pool without any replacement. Each random key in a given set is shared by multiple vehicles making it almost impossible for any RSU to uniquely identify the vehicle since the same key can be shared among several other vehicles. The authentication process is conducted in the following manner:

i. In the beginning of the connection setup, the RSU advertises its services along with its public key certified by central server.

ii. If an OBU is interested to accept the service, it will send back a reply with a set of keys randomly chosen from the key ring it possesses and a timestamp as an indication of message freshness. This message is encrypted by a session encryption key which is sent to the RSU using the RSU's public key.

iii. The RSU generates a random challenge and encrypts it with keys sent by the

OBU in a Cypher-Block-Chaining(CBC) fashion.

iv. In reply, the OBU simply decrypts the challenge message, re-encrypts it using the session key and sends to the RSU.

A set of keys are used for the authentication process to ensure that in a critical situation, a particular vehicle is still traceable with a higher probability than that of just using one single random key which might be common in a large number of vehicles. If an OBU uses any invalid or revoked keys for the authentication, the authentication will fail and the RSU will be broadcasting the revocation list to update the OBU's key ring for future use. Authors of this paper proposed a pre-defined authentication period for each key set that would be chosen from the key ring to defeat a potential correlation attack from RSU. Upon choosing the number of keys required for each authentication and the proportion of vehicles sharing a set of keys carefully, it is possible to track the identity of a vehicle with the involvement of the key distribution center. It has been shown that the impact of a key ring revocation is very negligible given that the size of the key ring and the central key pool is chosen carefully.

However, a potential RSU compromise attack has not been discussed by Xi et al. [33]. The memory of a tamper-proof OBU might be hard to copy, but not absolutely impossible for an adversary. A malicious OBU can be detected based on the number of invalid keys it uses in its authentication request. This detection may involve a technique called threshold cryptography [32] during an authentication request.

2.2.2 Hybrid Approach for Anonymous Authentication

Calandriello et al. [34] proposed a hybrid approach that allows a VANET group member to sign its self-generated pseudonyms which are delivered along with signed messages. Each OBU is pre-loaded with a unique group signing key and a common group public key. Self-generated pseudonyms are certified using its group signing key, while the message is signed by the corresponding private key for the used pseudonym. When received, a self-certificate is verified using the group public key, while the signed message is verified by the authenticated sender public key.

Apparently, a message verification in this approach consumes additional network bandwidth since each transmission from a sender contains a signature on the message as well as on a pseudonym.

Studer et al. proposed VANET Authentication using Signatures and TESLA++ mechanism (VAST) [35]. A combination of elliptic curve digital signature algorithm (ECDSA [36]) and a modified TESLA protocol [37] has been used for carrying out VANET message authentications. Upon receiving a message from a VANET entity, the receiver would perform a TESLA++ verification which could be followed by an ECDSA verification when non-repudiation is required. To prevent the major computational and memory-based DoS attacks, the received payload is verified using TESLA++ before the ECDSA verification is performed. If the initial TESLA++ verification fails for some reasons, then CPU utilization, as well as the size of the message queue are taken into consideration before switching to ECDSA mode of authentication.

Nonetheless, RSUs are still assumed to be trusted and the approach doesn't explicitly address the issue of replay attack and false message injection attack by a supposedly legitimate RSU. There is no clear indication on how a VANET should react upon detection of a node compromise. Moreover, Haas et al. in [38] remarked that ECDSA performs better than a TESLA implementation at longer communication distances since TESLA requires a second packet delivery for the message verification purpose.

Wen et al. [39] exploit the spatial and temporal properties of physical layer channel responses for securing each communication pair in VANETs. The basic idea is to distinguish one sending transmitter from another using the physical layer measurements for a series of messages. The sending entity attaches the authenticating signals which is a unique channel response along with the information payload transmission. A receiving entity can verify the legitimate transmission by comparing the authenticator signal with the estimated channel response.

This approach is efficient and scalable for a physical layer approach, but again, comes with some limitations. For instance, each vehicle has to be preloaded with public keys of other vehicles to be able to access the network. This will obviously require a massive task of updating and maintaining a huge number of keys as the size of the VANET grows. Authors also haven't addressed the node compromise attack which can have a deadly consequence in the form of false message broadcast, or replaying expired safety messages as mentioned in the previous section.

Among other recent work, ASIC scheme [40] introduces a faster and efficient way of aggregated verification of signatures and certificates for VANETs using Bilinear pairing technique. This approach can verify a large number of signatures and certificates to ensure a reliable and optimized operation of VANETs, nevertheless, establishment of trust on VANET safety messages has not been covered by this mechanism.

2.3 Anomaly Detection

Several among VANET security schemes are based on the assumption that the total number of compromised and malicious OBUs is smaller than that of non-compromised and legitimate OBUs for any traffic scenario. Security measures like authentication of a vehicle, verification of a *changed traffic/road condition* alert from a vehicle, reporting a malicious act on road, or even establishment of trust among vehicles may require voting from the vehicles coexisting on road. This may tempt an adversary for launching a Sybil attack in a VANET in which several false identities can be created by a single malicious node for pretending as multiple vehicles in order to mislead the RSU or other legitimate vehicles about some false events. Zhou et al. [41] proposed a set of mechanisms to effectively detect Sybil attacks on VANETs, while maintaining the privacy of a user. The transportation authority provides each vehicle with a set of pseudonyms which is used by the vehicle to hide the original identity of the OBU. Vehicles may abuse the pool of pseudonyms by launching a Sybil attack to convince the RSU and other OBUs on some fake event. One way to resolve this is to generate a huge set of random numbers which will be allocated to multiple unique 'fine-grained groups' as the hash of each random number from a group gives the same unique value. Upon receiving the contemporary event messages from vehicles, an RSU can check if the same vehicle has reported of an event using multiple pseudonyms. This technique allows an RSU to protect a VANET from Sybil attacks. However, because a particular pseudonym set would produce the same hash value each time, an attacker will be able to partially discover the identity of a vehicle if he/she can manage to compromise an RSU which contains the hash key in its memory. To address this, an RSU would be using keys with short life time from a predetermined key set for the purpose of coarse-grained hashing. To deal with the privacy and anonymity issues, the proposed methodology suggests multiple 'fine-grained subgroups' of pseudonyms under each initial 'coarse-grained' group where each of the pseudonyms is hashed again with a different key(fine-grained key) to give another unique hash value. A 'fine-grained' subgroup is provided to a vehicle's OBU to be used as the pool of pseudonyms, while the fine-grained key is always kept with the administrative entities, so that only the trusted authority can verify the identity of a vehicle.

A legitimate vehicle has a secret license number consisting of the coarse-grained hash value as well as the fine-grained hash value. When an event is reported by a vehicle to the RSU, the RSU can only verify the coarse-grained hash value of the vehicle. If the RSU finds multiple reports on the same event with the same coarse-grained hash value, it reports the event to the controlling authority with the coarse-grained hash value and the pseudonyms of the reported OBUs. The controller is trusted and will calculate both the coarse-grain hash value as well as the fine-grain hash value of the individual suspects. If for a particular event, the coarse-grained hash values and the fine-grained hash values both match for two or more pseudonyms, the Sybil attack attempt is detected. The combination of these two hash values forms the secret license number of the particular vehicle which is detected as an attacker. A false alarm can be issued upon detection of a sybil attack, whereas an RSU may simply raise a suspicion only when it receives a contradictory event report from a vehicle.

For further improvement of Zhou et al. [41] scheme, a threshold based approach (e.g., [32]) can be useful which can detect a collusion among nodes less than the chosen threshold value for the Sybil attack. An RSU forwards the event, pseudonyms, coarse-grained hash values, and signatures to the trusted controller which verifies the fine-grain hash values for the detection of colluded Sybil attack. The biggest challenge in this scheme is to maintain the appropriate trade-off between the number of coarse-grained hash values and the number of vehicles. A bad combination of these two may increase the false alarm rate considerably, while user-anonymity of VANET would also be affected.

2.4 Application-specific Approaches

Dötzer [42] addressed some application-specific solutions to privacy issues in VANETs. Without describing much technical or cryptographic details, this paper highlighted the practical privacy concerns with a manufacturer's perspective. Cars are termed as 'personal devices' since a driver's personal information/records are somehow kept in a car for a long period of time. Evolution of splendid digital navigation systems (e.g., GPS), electronic toll collection, on-road Internet access facilities, and many other service oriented applications provide a driver with a better grip and safety on driving environment of roads and highways. However, these safety and worthwhile applications might turn out to be extravagant in terms of car owner's privacy.

Probable solutions to the privacy threats in VANETs demand certain capabilities like having a number of pseudonyms to represent the vehicle instead of a real world identity, appropriate mapping mechanism between a pseudonym and a real world identity, and a set of credentials to be bonded cryptographically with pseudonyms for VANET applications. The architecture suggests a third-party trusted authority which is essentially accepted by all participating entities in a VANET. The proposed idea is divided into three distinguished operational phases: the initialization phase, operational phase, and the credential revocation phase.

A tamper-proof smart card is associated with a unique and permanent electronic ID. An ID is delivered to the supreme authority by a user through a secure, pre-established link. The authority cryptographically generates some pseudonyms from the ID and delivers them to the vehicle (user) using the same secure link. These pseudonyms are important for different services provided by a manufacturer. Against each pseudonym, a vehicle is provided with subscription of several services from the service provider (e.g., a manufacturer). The service provider receives a pseudonym from a vehicle, prepares some cryptographic credentials based on the received pseudonym and sends them back to the vehicle with a signature. During the operational phase, a vehicle can use any of its pseudonyms to access the network service. Neighboring vehicles and/or other network entities can verify the vehicle's legitimacy by checking the necessary credentials.

In the credential revocation phase, credentials of a particular vehicle are canceled upon detection of a malicious behavior. Neighboring network-participants would file a report along with appropriate evidence to the service provider if there is any discrepancy in the alleged vehicle's standard function. The service provider gathers the evidence and complains from the network members, and forwards them to the supreme authority. The authority would calculate the actual identity of the alleged vehicle to shutdown its services if the evidence is sufficient to revoke the vehicle.

Dötzer [42] also highlighted on some additional privacy considerations for on-road vehicles. For instance, during the changing of pseudonyms in a vehicle, an eavesdropper may record the entire transmission to distinguish the vehicle by correlating the new pseudonym with the previous one. Two possible solutions have been proposed to address this problem: the first one is to take a considerable amount of time between switching off the previous pseudonym and starting to use the new one. The second approach is to change the pseudonym in a crowded place called 'MIX-zone' where many other vehicles are also changing their pseudonyms at a time.

Both approaches proposed by Dötzer have flaws. For instance, taking too long to change the pseudonym may cause safety and communication problems. Also, there may be no other vehicles in a MIX-zone to hide the pseudonym change of the vehicle. An alternative solution is to use Geo-specific pseudonyms, in which the pseudonyms are selected based on different geographical areas the vehicle travels to. Again, scalability might be an issue with this approach since a vehicle usually roams around a huge geographical area in its lifetime. Obviously, all these ideas and considerations are highly subjected to the law of the specific territory, government policies, and people's preferences of privacy.

A somewhat similar approach by Choi et al. [43] addressed the problem of appropriate balancing between privacy and auditing capability in VANETs, where they investigated the use of symmetric primitives for controlling privacy in a vehicular network. Since the issue of privacy is highly application dependent, a new privacy structure has been suggested that involves a trusted third-party ombudsman along with a database of all users in a given vehicular network. The ombudsman can securely collaborate with base stations (OBUs) when it is necessary to reveal a user's actual identity. The base stations store the long-term pseudonyms from the vehicles. These pseudonyms are used by the ombudsman during the retrieval of a user's original identity from the database. The ombudsman escrows ([24, 44]) the association between an actual identity and pseudonyms, provided that all the legal formalities are already fulfilled.

In this approach, an OBU's anonymity in an OBU-to-OBU communication is achieved by the short-term pseudonyms, while the long-term pseudonyms assure the vehicle's anonymity in OBU-to-RSU communications. Scalability, network overhead, as well as the security overhead issues have not been considered in this paper. Also, authentication of a vehicle in an OBU-to-OBU communication has been left unattended.

Many other different approaches have been introduced to address security and privacy issues of vehicular networks. In this chapter, we discussed some of the major schemes with their cryptographic foundations, applications, and security features. We analyzed the fundamental aspects regarding VANET security and privacy. We also identified some open issues for future research in order to have safer, improved, and stronger mechanisms for VANET security and privacy.

2.4.1 Signature Verification Policies

The problem of authenticating a huge number of signed messages in a given time has been addressed in two major ways: random verification, and aggregated (batch) verification of messages.

Random Verification

In a random verification scheme, received messages are randomly selected for verification by a receiving entity. The idea has been incorporated for VANET by Raya et al. [17] to obtain scalability in signature verification process.

A resource-aware verification scheme for VANET messages has been presented by Li et al. [45] where the physical distance between sender and receiver is considered as the basis of prioritizing received messages. Received messages from the nearest vehicles are to be authenticated immediately, while rest of the messages would be chosen for verification in a random manner within the resource budget. However, in a sparse traffic scenario where the average distance between two vehicles is large, this approach becomes an ordinary random verification scheme.

Batch Verification

A batch verification technique in VANET allows verification of all received messages simultaneously. Most batch-verification schemes proposed for VANETs use a costly bilinear pairing-based verification technique [46, 47]. A fast batch verification mechanism has been presented by Cheon et al. [48] using ECDSA authentication scheme.

A batch verification mechanism is an efficient way of ensuring the trust of multiple messages received in a unit time. Nevertheless, implementation of this approach depends on the underlying mechanism of the signature protocol.

2.5 Novelty in Research

In this thesis, we designed a vehicular communication platform which not only provides secure communications and anonymous authentications for VANET users, but also considers different communication aspects of security and privacy in WAVE-enabled VANETs.

We have addressed the challenges of security and privacy in VANETs using the well-established cryptographic primitives like proxy signature, Identity-based Cryptography, and Elliptic Curve Cryptosystems. We analyzed the cryptographic overhead introduced by our security and privacy schemes, as well as its implications on the communication channel for VANETs.

In order to cope with the challenges of verifying multiple messages in a given time-frame, we introduced a cross-layer verification scheme which can selectively verify messages based on information relevance and lower layer access priorities of vehicular communications.

Our contributions also include a distributed denial of service (DDoS) attack in VANETs utilizing WAVE's EDCA limitations and the periodicity of vehicular transmissions. Mitigating such attacks involves modification of WAVE's EDCA features, as well as the randomization of transmission schedule.

For each individual contribution in this work, we combined the communication aspects of VANETs with our proposed security and privacy framework. To the best of our knowledge, incorporating communication aspects of VANETs with security and privacy schemes is a novel contribution in the area of VANET security and privacy research.

Chapter 3

Deploying Proxy Signature In VANETs

3.1 Introduction

A vehicular ad hoc network (VANET) consists of a number of on-board units (OBUs), roadside units (RSUs), and an infrastructure that connects the VANET to the Internet. Generally, an RSU is responsible for providing information to OBUs about road-safety issues like traffic collision warning, accident notification, traffic rule violation warning, and changed road condition. It can also be used as an advertisement agent for commercial benefits. On the other hand, OBUs can communicate with other vehicles for exchanging information like traffic/road condition, and destinations. Apart from that, an OBU periodically disseminates the vehicle's location, brake, acceleration information to the RSU and other OBUs in its vicinity.

Since the success of such an ad hoc network depends highly on exchanging messages among multiple entities, trust is a vital aspect of a VANET. A user (e.g., a driver) would be comfortable with any VANET application only when he/she can have a lot of confidence on its network components. In other words, a VANET application is useless and not very appealing unless all involved entities are trustworthy. An adversary in the disguise of an RSU or an OBU may deliberately broadcast false traffic-safety messages, or send old and expired notifications to all OBUs. This would impair the transportation safety by misleading the entire traffic in a VANET.

Another prime concern in vehicular communications is the privacy/anonymity of a user. A user would not like to share his actual credentials that might expose his identity. However, the system has to ensure that an anonymous OBU can not take advantage of its anonymity by sending false messages to misguide the traffic. In other words, anonymity in VANET has to be conditional so that in case of a traffic dispute, the original identity of an OBU can be traced by the appropriate law enforcement authority.

Therefore, VANET entities must have the ability to authenticate the message sender, as well as to maintain the integrity of the delivered message. A suitable signature scheme can resolve these issues. However, identity verification in a realtime VANET environment is not an easy task due to high and variable velocity of nodes, varying density, and roads with nonuniform characteristics. The issue of scalability is of high importance as under heavy traffic, a single controller might need to attend hundreds, perhaps even thousands of vehicles in a given segment of the transportation network.

To cope with the above requirements, we design the following two schemes:

- *RSU Message Authentication:* It provides authentication of an RSU as a valid member of the corresponding RSU group to the on-road OBUs. All the messages delivered through the RSU are signed by a roadside controller (RSC) and an RSU. RSUs in a given geographical area are grouped together to work under an RSC where RSUs are connected to the RSC by high bandwidth secure links.

- *OBU Message Authentication:* It provides anonymous authentication of OBU messages to the RSU and other OBUs as a registered entity of the Department of Transportation (DOT).

In order to ensure the message integrity and trust requirements of RSU-to-OBU, OBU-to-RSU, and OBU-to-OBU communications, our authentication schemes would enable a sender (an RSU, or an OBU) to generate a proxy signature on a VANET message. Upon reception, a recipient of the message (an OBU or an RSU) can verify the message integrity and source authenticity.

The term 'proxy signature' refers to a variation of digital signature that designates an entity (called a proxy signer) to sign a message on behalf of the original signer. The concept of proxy signature— proposed by Mambo et al. [49], has been extended by Kim et al. [50] where two additional features were incorporated: proxy signature by partial delegation with warrant, and the threshold delegation based proxy signature. Enhancements of the fundamental proxy signature approach include blind proxy signature schemes by which a proxy signer is made unable to

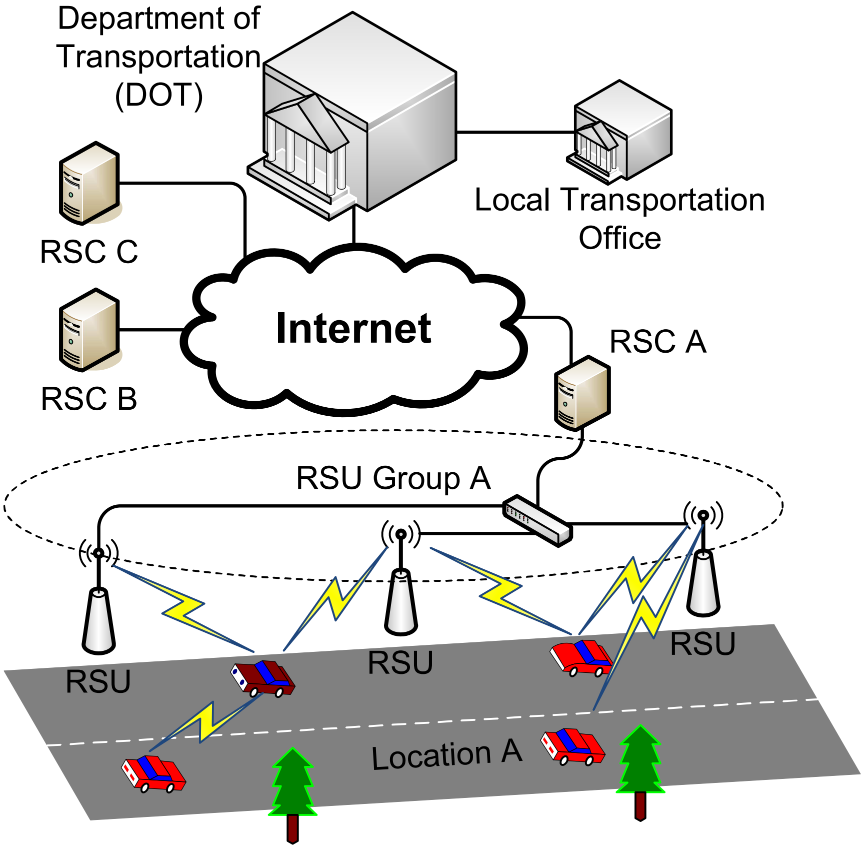


Figure 3.1: The framework for RSU safety message delivery in VANETs.

manipulate the original message contents [51, 52, 53]. However, blind proxy signatures are not practical for VANET applications since they require a new proxy tuple to be generated and securely delivered to the proxy signer for every single new message.

We exploit the features offered by partial delegation based proxy signature [49] for VANET messages. A partial delegation mechanism of a proxy signature produces a new secret key from the original signer's secret, and the new secret is used as the signing key for the proxy signer. We consider Schnorr's scheme [54, 55] for signing of VANET's safety messages.

The rest of the chapter is organized in the following manner. A brief account of the network assumptions is given in Section 3.2. Section 3.3 and Section 3.4 describe our schemes for RSU and OBU message authentications respectively. Security analysis of our scheme is provided in Section 3.5 and Section 3.6 summarizes the chapter.

3.2 Network Assumptions

A number of RSCs are deployed over the VANET, which are connected to the Internet as shown in Figure 3.1. The Department of Transportation (DOT) works as the Certificate Authority (CA) which maintains all necessary information of each RSU under an RSC. For instance, DOT stores the pre-assigned location information, deployment history of individual RSUs along with the public key of the RSC. DOT issues the certificate for each of the RSUs in the VANET.

We assume that the DOT's public key is known to all the members including the vehicles in a VANET. Local transportation authorities may communicate with the DOT through offline or online transmission to negotiate any dispute, including issuing licensing materials for a vehicle and commercial aspects of VANETs.

An RSU advertises the certificate containing ID_{RSC}, the public key (later denoted as v) of the RSC, ID_{RSU}, the MAC address of the RSU, and the RSU's location information, Loc_{RSU}. The initial (beacon) advertisement message has the following certificate:

$$(\mathrm{ID}_{RSC}, \mathrm{ID}_{RSU}, \mathrm{Loc}_{RSU}), H(\mathrm{ID}_{RSC}, \mathrm{ID}_{RSU}, \mathrm{Loc}_{RSU})_{S_{CA}},$$

where $H(.)$ is a one-way hash function and $(.), H(.)_{S_{CA}}$ indicates a signature using CA's secret key.

An OBU finds the public key of the RSC, the original MAC addresses of the RSU, and the designated RSU location from the certificate. The certificate authority's signature confirms the integrity of the message and proves the fact that the RSU belongs to the corresponding RSU group administrated by the particular RSC. Upon receiving the beacon frame [4, 6], the OBU matches the received MAC address with the transmitting RSU's MAC address. Once the RSU's MAC address is verified, the OBU decides to join the RSU group, or, it may wait for another beacon. The OBU also compares the location information of the RSU (from the received packet's *transmission_location* field) with its GPS information to verify that the RSU is at its designated location. The time synchronization among vehicles and RSUs are done using the timing information field of WAVE Service Announcement (WSA) frame [1].

3.3 RSU Message Authentication Scheme

All VANET entities are equipped with two prime numbers: p (512 bits) and q (140 bits), where q is a prime factor of $(p - 1)$. p and q are associated to an administrative area: for instance, p is assigned to a country, and q is for a given large geographical area (a state, or province) in that country. An order q generator g for Z_p^* (i.e. $g^q = 1\, modp$) is associated with a comparatively small area (for example, a city, or a town). We divide the scheme into following steps.

3.3.1 Proxy Pre-processing

For each RSU, RSC generates a random number $s < q$ which is the private key of the original proxy signer (RSC) for reliable message delivery in VANET. The public key is calculated as $v = g^s mod\, p$.

The private key/public key pair is pre-calculated at the RSC prior to the actual operation. Parameters $p, q, g,$ and v are made public for the subordinate RSUs and vehicles. The list of parameters used along with their scopes in this scheme is given in Table 3.1. In addition, RSC generates another random number, $k \in_R Z_{p-1} \backslash \{0\}$;

Table 3.1: List of parameters and their scopes for RSU-to-OBU message delivery in VANETs.

Parameters	Generated by	Scope in VANET
p, q, g, v, K, h_s	RSC	Public
k, s, x, h	RSC	Private (RSC)
σ, r	RSC	Private (RSC, RSU)
y	RSU	Private (RSU, OBU)
x'	OBU	Private (OBU)

where $Z_{p-1} \backslash \{0\}$ denotes a *non-zero finite field of modulo p*. We refer to k as the *revocation parameter* of our scheme. A detailed revocation process is given in Section 3.5.1.

During the initialization phase, RSC computes

$$K = g^k mod\, p. \tag{3.1}$$

Parameter K is dependent on the revocation parameter k as indicated in Equation (3.1), and is used for calculating a proxy secret key σ.

$$\sigma = s + kK mod\, (p - 1). \tag{3.2}$$

The value of σ will be used as the secret identity of an individual RSU, hence it would be stored as a secret in the RSU's volatile memory.

On the other hand, K is defined as the verification parameter since it is used by an RSU and an OBU for the verification of a proxy pair (σ, K) and the delivered message respectively.

An RSU works as a proxy signer of an RSC. The proxy pair (σ, K) is then delivered to an RSU through a secure channel. Henceforth, we refer to the pair (σ, K) as a *proxy*.

Values of σ and K are different for individual RSUs, and normally they are valid for a long time unless a proxy is detected to be used by some unauthorized entity.

Should there be a message for transmission over the VANET, either for a road-safety or some other application (e.g., a commercial advertisement, or, weather update), the RSC must associate the message content m with a message expiry time t_x. It is very important to prevent the RSU from abusing the proxy signature by posting invalid messages, or replaying old messages. The message m is thus jointly signed by the RSC and individual RSUs before it is delivered to the vehicles on road.

The RSU uses the value of σ instead of s as the secret key of the basic signature scheme. We apply Schnorr's scheme as the underlying signature mechanism due to its simplicity and compatibility [49, 50].

3.3.2 RSU Proxy Signature

RSC selects a session parameter $r = H(s, m, t_x) mod\ q$, and computes

$$x = g^r mod\ p. \tag{3.3}$$

This session parameter is generated as soon as there is an event for which a message has to be delivered. RSC subsequently calculates the hash value h of the message m concatenated with x.

$$h = H(m, x, t_x). \tag{3.4}$$

The message m, expiry information t_x, hash value h, and session parameter r are delivered to the RSU through a secure channel. This is done every time when there is a message to be transmitted through RSUs.

The RSU utilizes the received r and h values to calculate y as given in

$$y = (r + \sigma h) mod\, q. \tag{3.5}$$

Proxy signature (h_s, y) is concatenated with the (safety application or other) message, which eventually results in a tuple (m, t_x, h, y, K) to be delivered by the RSU.

3.3.3 Verification

A receiver node (OBU) generates a new public key from the actual public key of the RSC.

$$v' = vK^K mod\, p. \tag{3.6}$$

The new public key is used in the following calculation.

$$x' = g^y v'^{-h} mod\, p. \tag{3.7}$$

The expiry information t_x is immediately matched with the current system time of the OBU. Upon detecting an expired message from an RSU, it may release a replay alert to notify the concerning authority after discarding the message. If not, the message is verified as below:

$$h = H(m, x', t_x). \tag{3.8}$$

If (3.8) holds then the message is accepted. Otherwise, an OBU may generate a false message alarm, or it can simply ignore the message, depending on the system configuration and application requirements.

Note that the RSC must store a copy of each delivered message in its database, along with the corresponding session parameter r, and the generation time of the message. This is done in order to resolve any future dispute that involves the liabilities of an RSU or OBU.

3.3.4 Correctness

Equations (3.4) and (3.8) suggest that x' is equal to x for any legitimate signature. Hence in order to prove the correctness of our signature and verification mechanism, it would be sufficient to prove that $x = g^y v'^{-h} \; mod \; p$. Equation (3.7) is given as: $x' = g^y (v')^{-h} \; (mod \; p)$.

Now, $g^y = g^{r+\sigma\, h+mq} \; (mod \; p)$, [By replacing y with $r + \sigma\, h + mq$, where m is an integer]

$= g^r.g^{\sigma\, h}.g^{mq} \; (mod \; p)$

$= g^r.g^{\sigma\, h}.(g^q)^m \; (mod \; p)$

$= g^r.g^{\sigma\, h} \; (mod \; p)$, [Since $g^q = 1$ according to our definition above]

$= g^r.g^{\{(s+kK)+n(p-1)\}h} \; (mod \; p)$, [By replacing σ with $s + kK + n(p-1)$, where n is an integer]

$= g^r.g^{(s+kK)h}.g^{n(p-1)h} \; (mod \; p)$

$= g^r.g^{(s+kK)h}.(g^{(p-1)})^{nh} \; (mod \; p)$

$= g^r.g^{(s+kK)h}\ (mod\ p)$, [According to Farmet's little theorem, if p is a prime and g is not divisible by p; $g^{(p-1)} = 1\ (mod\ p)$ for $g \neq 0$].

Again, $(v')^{-h} = (vK^K)^{-h}\ (mod\ p)$, [From Equation (3.6)]

$= v^{-h}.K^{-Kh}\ (mod\ p)$

$= g^{-sh}.(g^k)^{-Kh}\ (mod\ p)$, [Since, $v = g^s (mod\ p)$]

$= g^{-(s+kK)h}\ (mod\ p)$.

Therefore, $x' = g^y(v')^{-h}\ (mod\ p) = g^r.g^{(s+kK)h}.g^{-(s+kK)h}\ (mod\ p) = g^r\ (mod\ p) = x$. Hence, our signature scheme is correct.

3.4 OBU Message Authentication Scheme

We use the partial delegation based signature scheme [49] for OBU message authentication. Public parameters p, q, and g are chosen in the same manner as in the RSU message authentication.

In this approach, OBUs are partial delegation based signers which sign messages, while the secret credentials for OBUs would be stored at the trusted authority (e.g., Dept. of Transportation (DOT)). DOT collaborates with the local transportation office which is responsible for delivery of delegation materials to vehicles (OBUs) at the time of registration/renewal of vehicle's license. The intention of this scheme is to enable an OBU to anonymously sign messages which are unforgeable, verifiable, identifiable, and non-repudiable.

3.4.1 Pre-processing

During the pre-processing phase, DOT generates its private key/public key pair (s_D, v_D) following the same procedure as indicated in Section 3.3.1. All the system parameters are chosen so that they can support enough delegation proxies for a large number of vehicles operating in a given geographical area. At the time of registration/license renewal, an OBU_c is pre-loaded with n different delegations $(\sigma_{c,i}, K_{c,i})$, where $i = 1, 2, ..., n$. The size of n is important for the vehicle's anonymity and may vary according to the owner's preference of privacy.

A non-overlapping random value α_c is chosen for each individual OBU_c at the corresponding DOT such that:

$$\begin{aligned} \beta_{c,1} &= \alpha_c \oplus K_{c,1}, \\ \beta_{c,2} &= \alpha_c \oplus K_{c,2}, \\ \beta_{c,3} &= \alpha_c \oplus K_{c,3}, \\ &. \\ &. \\ &. \\ \beta_{c,n} &= \alpha_c \oplus K_{c,n}, \end{aligned} \tag{3.9}$$

where α_c and the set $\{\beta_{c,i}; i = 1..n\}$ are secret credentials of OBU_c, which are stored only in the DOT.

Table 3.2: List of parameters used in OBU message authentication, and their scopes.

Parameters	Generated by	Scope in VANET
$p, q, g, v_D, K_{c,i}$	DOT	Public
$k, s_D, \alpha_c, \{\beta_{c,i}; i = 1..n\}$	DOT	private (DOT)
$\sigma_{c,i}$	DOT	private (sender OBU, DOT)
r_c	sender OBU, RSU	private (sender OBU, RSU)
x_c	sender OBU	private (sender OBU)
x'_c, v_{new}	receiver OBU, RSU	private (receiver OBU, RSU)
y_c, h_c	sender OBU	private (receiver OBU, RSU)

3.4.2 Signature Generation

We assume that every vehicle in a VANET is equipped with a GPS onboard which can determine its current location. The location information of the vehicle is taken from the GPS data to generate a session value $r_c < q$. The GPS data is passed to a function which generates a rounded output r_c which is equal for all devices in the communication range of the OBU. This is done by taking the most significant bits of the GPS data so that in the communication range of an OBU (approximately 300 meters), r_c values come same. To prevent potential replay attack, a message m_c is associated with its expiry time t_{cx}. The following equations are used for signing a message m_c by an OBU.

$$\begin{aligned} x_c &= g^{r_c} mod\, p. \\ h_c &= H(m_c, x_c, t_{cx}). \\ y_c &= (r_c + \sigma_{c,i} h_c) mod\, p. \end{aligned} \tag{3.10}$$

The set $\{m_c, t_{cx}, h_c, y_c, K_{c,i}\}$ is delivered by the OBU to RSUs and/or to other OBUs in the communication range.

As mentioned before, an OBU is pre-loaded with multiple delegations (i.e. the combination $(\sigma_{c,i}, K_{c,i})$). To maintain the anonymity on road while communicating, it uses different delegation every time for signing a safety message.

3.4.3 Signature Verification

The receiving RSU/OBUs compute a new public key $v_{new} = v_D K_{c,i}^{K_{c,i}} mod\, p$. The location information, either collected from the local GPS (in case of an OBU) or the pre-determined one (for an RSU) is used for determining the r_c value. The following relationship is checked.

$$x'_c = g^{y_c} v_{new}^{-h_c} mod\, p = g^{r_c} mod\, p. \tag{3.11}$$

If Equation (3.11) holds, the receiving node verifies the expiry information with the message in the following manner.

$$h_c = H(m_c, x'_c, t_{cx}). \tag{3.12}$$

If the last equation does not hold, the receiving node either ignores the message or sends an alert to the corresponding RSC depending on the system configuration.

3.4.4 Overhead

Table 3.3 gives an account of the signature overhead for our VANET message authentication approach. Assuming that prime numbers p and q are of 512 bits and 140 bits respectively, the total size of the signature overhead in either of authentication schemes would be equal to 106 bytes with MD5 hashing. Replacing MD5 with SHA-1 would extend the signature overhead to 110 bytes.

Table 3.3: Signature Overhead.

Parameter	Size (in Byte)
t_x, t_{cx}	8
h, h_c	20
y, y_c	18
K, $K_{c,i}$	64
Total	110

3.5 Security Analysis

The security of our VANET authentication approach relies mainly on the inherent difficulty of solving discrete logarithm problem. Proxy signature mechanism uses a new secret derived from the actual secret key of the original signer. The intractability of the discrete logarithm problem assumes that an adversary can not reverse the process to generate the actual secret from the knowledge of a proxy key.

In the first part of our security analysis, we focus on the secure RSU-to-OBU message delivery approach of the VANET. In the second part, we analyze the anonymous OBU message delivery.

3.5.1 RSU Message Authentication

False Message Injection

The original signer (i.e. RSC) produces a message to be delivered to the OBUs, while it allows the subordinate RSUs to sign on behalf of the originator. Unlike the conventional warrant based proxy signature approaches where the original signer designates a proxy signature either by signing a declaration or where the original signer signs the message along with a newly derived public key, our approach determines a session parameter r from the message m and the expiry info t_x using the secret key of the original signer: $r = H(s, m, t_x) mod\, q$. Since the key s is secret, only the original signer (RSC) can produce a valid session parameter.

However, the session parameter r is computed through a modulo q operation, and therefore, it is possible for an adversary to guess the session parameter r. The probability of a successful guess on r is $1/(q-1)$ since $r \neq 0$. Using the session parameter r, an adversary can compute h and y from Equations (3.3) and (3.4) respectively.

Again, computing y would require the value of the proxy secret σ [Equation (3.2)]. The probability of successfully guessing the value of σ is $1/(p-2)$ (from Equation (3.2), since $\sigma \neq 0$]). The adversary can successfully launch a false message attack by constructing a message tuple as the other parameters (t_x, K) are known to it.

Hence, the overall probability of an OBU to be misled by accepting a false message is $\frac{1}{(q-1)} \times \frac{1}{(p-2)}$. Therefore, parameters p and q should be large enough in order to avoid such attacks. Choosing p and q of length 512 bits and 140 bits respectively would keep the probability of a successful false/modified message attack significantly low.

Unforgeability

Only a valid proxy-signer RSU can create a given signature on behalf of the RSC. An RSU uses the session parameter r, and the newly derived secret σ from its proxy set (σ, K) to sign a message. Each σ value is distinct and is explicitly assigned to only a single RSU.

For launching an attack by signing and broadcasting invalid messages, an adversary may try to derive a valid combination of proxy (say, (σ', K')) that satisfies Equation (3.2). Since signing also requires a valid h (refer to Equation (3.5)) which is solely generated by the RSC, an adversary can never create a valid proxy signature.

Because σ is derived from a random secret s, computing a new σ or determining the secret s from a given σ of a proxy is commonly believed to be hard due to the complexity of solving discrete logarithm problem.

Non-repudiation and Impersonation

As an RSU is strictly assigned with only one proxy tuple (σ, K), it can not generate any valid signature which would be recognized as a valid proxy signature by a different RSU. The y value of a valid signature for a given session is unique and can only be generated by a particular RSU using Equation (3.5). An adversary cannot generate a valid proxy signature from the public parameters since s and k values are stored only in the RSC. Even if an adversary succeeds in generating a new proxy (σ', K') which satisfies Equation (3.2), launching an impersonation attack is not possible since a malicious RSU cannot provide an appropriate session parameter r with a considerable probability for computing a valid y using Equation (3.5).

Exculpability

The term exculpability refers to a scenario where a malicious signature from an adversary would appear to be signed and delivered by an innocent entity in the network [21]. An RSU is always identifiable from its proxy signature for a given message as no one except the RSC can generate a proxy combination (σ, K) with a high probability. The last two components of a proxy signature: y and K represent the identity information of an RSU. Thus, one has to come up with a valid new combination of (y, K) in order to hide identity information of the RSU. But, the changed values of y and/or K would produce different results in Equations (3.6) and (3.7) which would lead to an unsuccessful verification in the process. Again, since h value is not changeable for a given message, change of y using Equation (3.5) requires change of σ and/or r. Note that the value of r should always remain smaller than q, and finding a valid combination of (σ, K) with a given public key v, requires extreme efforts as s and k values are only known by the RSC.

Revocation

An adversary may successfully compromise an RSU to get the possession of its designated proxy. Upon detection of the compromise, the RSC must revoke the proxy as the adversary may attempt to use the proxy to sign a malicious message. The revocation process starts at the RSC with regenerating the revocation parameter k followed by computing a verification parameter K using Equation (3.1) and so on.

Although, the compromised proxy is still a valid one and can be used by the adversary, it can not harm the system by signing an illegitimate or expired message. This is due to the fact that the session parameter r can only be generated by the RSC using the original message m itself, the expiry information t_x, and the primary secret s. Nevertheless, the misbehaving RSUs must be replaced once identified after conducting an investigation by the VANET administrator.

3.5.2 OBU Message Authentication

We discuss below some of the major security issues concerning the authentication of OBU messages in VANETs.

Anonymity

An OBU is preloaded with n number of proxies, while it randomly picks one of them for signing a new message. Thus, the original identity of the vehicle is not exposed to other parties during vehicular communications. Corresponding $K_{c,i}$ values are unlinkable at the receiving end which provides anonymity and privacy to a VANET user, while the original MAC address of the sender is also undisclosed as indicated by the standards [6]. Thus, the original identity of the vehicle is not exposed to other entities during an OBU message transmission.

Accountability

Under a critical situation when it is necessary and permitted by the appropriate law enforcement authorities, a vehicle's identity can be traced by investigating a sent message. A signed message $(m_c, t_{cx}, h_c, y_c, K_{c,i})$ is taken into consideration. Assuming that the message is a valid one (it could be an expired message though), the value $K_{c,i}$ is checked against the stored messages at the DOT. There is a possibility that multiple vehicle entries may come up for a given $K_{c,i}$. The corresponding $\sigma_{c,i}$

values are considered, and the message is reconstructed at the DOT using each individual proxies assigned to that particular vehicle, as well as parameters m_c, t_{cx} from the signed message, and r_c from the reporting RSU. The proxy for which the reconstructed signature matches the signature of the reported message is detected as the accountable one. The complete identity of the tainted vehicle is retrieved using its secret credentials at the DOT.

False Message Injection

A malicious OBU may try to transmit a false or modified message m_f in a VANET. Since r_c is available from the location data, and h_c can be determined accordingly using Equation (3.10), the only difficulty for an adversary would be to compute a valid y_c for m_f. As y_c is computed through a modulo p operation, the probability that the false (or, modified) message would be accepted at the receiving end is $1/(p-1)$. Therefore, a large (usually, at least 512 bit for a proxy signature) p value would be essential for our proxy signature based VANET message authentication.

Replay Attacks

An adversary may attempt to replay a valid message at the same location where the signed message was originally delivered. However, the expiry information of the message is associated with the main message content which would make the signed message invalid once the validity expires. Given that the validity period is long enough, the adversary may try to replay the same message in a different location (e.g., in a different street with different sets of vehicles on road). Since the receiving node uses its own location information during the message verification phase (refer to Equation (3.11)), the adversary would not be able to get a false message accepted.

Node Compromise and Sybil Attacks

An adversary may launch several useless and misguiding messages to distract a VANET by an OBU compromise. The malicious behavior of a vehicle must be reported to the DOT as soon as identified. The DOT would release a revocation order for the tainted vehicle over the VANET if it has evidences about the malicious act of the reported OBU. The DOT would publish the revocation secret α_j, as well as the secret set $\{\beta_{j,i}; i = 1..n\}$ for the reported OBU_j. Each RSU in the VANET would compute $\alpha_j \oplus K_{j,i}$ upon receiving a message from any OBU. If the computed value matches one of the items in the set $\{\beta_{j,i}; i = 1..n\}$ released from DOT, the RSU generates an alert so that the legitimate OBUs can ignore the messages from the reported OBU. This process would continue till the issue is resolved and the DOT further notifies the VANET about it.

Since an OBU is preloaded with multiple proxies, a malicious vehicle may launch a sybil attack where a vehicle sends out several identities in order to misdirect a VANET. To thwart such an attack, an entity would store the $K_{c,i}$ fields for all the messages received in a short time frame (say, 30 sec. On an average, a vehicle dwells within the communication range of an RSU for this time period). If the stored messages are same or if they trigger the similar course of action, the receiving device can report the incident to the RSC. As the actual identity of a vehicle is traceable based on the contents of its signed messages in VANET, the adversary would not be able to deny the responsibility of the attack.

3.6 Summary

In this chapter, we presented two authentication schemes for RSU and OBU messages in vehicular networks. Proposed techniques have been derived from the modifications of discrete logarithm based proxy signature mechanism to comply with VANETs' integrity and privacy requirements. Security analysis shows that our approach has strong resistance against potential forgery and attacks launched by adversaries. Our schemes have low communication overhead which essentially saves on communication bandwidth.

The following chapters provide extensions of our VANET authentication approach with lightweight cryptographic primitives, as well as the experimental evaluation of the schemes with IEEE Std 802.11p [4] and 1609.2 [5] frameworks.

Chapter 4

An Identity-based Authentication Scheme for RSU Messages in WAVE-enabled VANETs

4.1 Introduction

Due to the ad hoc nature of the network, and high speed mobility of vehicles, VANET entities like RSUs and OBUs can not be pre-authenticated while operating on road. This poses a high degree of vulnerability to the network in terms of security, privacy and trust. Adversaries either from the provider or among the consumers may take advantage of unauthenticated communications in VANETs for several anti-social or criminal activities. For instance, an unauthorized entity could transmit a malicious software update for the users of a VANET. Installation of such malware in the system might result in a massive failure of vehicles in terms of irregular behavior, security malfunctioning, and/or user privacy. An adversary may mislead the traffic system by broadcasting false traffic-safety or changed road-condition messages on a certain road.

Also, a malicious entity may repeat an expired traffic-safety notification to handicap the road-traffic system in the coverage area of a VANET. Replaying of an expired message that contains some commercial contents (e.g., an electronic flyer of a nearby shopping mall) might jeopardize the prospect of value added services in VANETs. Thus, VANETs' safety or other application messages must be authenticated by the receiving OBUs.

However, with the existing solution from the current standards, a sender of safety messages enjoys full freedom of creation, distribution, and re-distribution of a safety or other application messages. Since an RSU is installed at the roadside location without having much physical protection or surveillance, trusting the received content from an RSU might be harmful. This is because, an adversary could take over an RSU, and transmit malicious safety messages to deceive on-road vehicles using the compromised RSU credentials.

In reality, it is obvious that a road-safety message, an emergency traffic notification, or a software update is issued by the trusted third-party (e.g., the department of transportation) rather than an ordinary roadside unit (RSU) or a vehicle (OBU). However, depending on application's coverage area, a delivered message may need to be forwarded by RSUs and OBUs at a multi-hop distance. Hence, multiple entities are to be involved in a VANET application message generation and distribution process.

A number of papers have addressed the issue of VANET message authentication (e.g., [17, 23, 30, 33, 34]), where researchers mainly focused on authenticating OBU messages to RSUs and to other OBUs in the light of vehicular anonymity and other VANET requirements. However, safety messages from RSUs are trusted by default.

Lin et al. [25] and Sun et al. [56] suggested ID-based signature schemes [29] using bilinear pairings, where the location of RSU can be used as public key for the message signature. Each message sent from the RSU contains the physical location information so that once the message is received by an OBU, it can be verified based on the location information.

A bilinear pairing based approach is expensive in terms of time and computation complexity, as well as, the pairing assumptions are difficult to incorporate as discussed in Section 4.6.

In this chapter, we design an ID-based authentication scheme which uses an identity-based proxy signature on Elliptic Curve Digital Signature Algorithm (ECDSA) in order to address the security and authentication for road-safety and other emergency application messages while accommodating the requirements from the existing VANET standards IEEE 802.11p DSRC [4] and WAVE protocol stack 1609.x [1, 5, 6]. We also investigate different combinations of traffic classes (AC0, AC1, AC2, and AC3) for transmission of RSU and OBU safety messages under our authentication scheme.

We organize the rest of the chapter as follows. Section 4.2 contains our motivation for an ID-based proxy signature in VANET communications. We provide some useful fundamental information and definitions for our scheme in Section 4.3.

Section 4.4 illustrates our scheme in details. Security analysis and comparisons are given in Section 4.5 and Section 4.6 respectively, while Section 4.7 provides performance evaluation from network simulation. Section 4.8 concludes the chapter.

4.2 Motivation for ID-based Approach and Proxy Signature in VANETs

An ID-based signature allows a verifier to use a publicly well-known piece of information about the signer for the verification of the digital signature. Depending on the context, this public information could be an actual identity of the signer, signer’s host network address, signer’s email address, or even a combination of any number of such identifications.

ID-based cryptosystem was first proposed by Adi Shamir in 1984 using the difficulty of integer factoring [57]. Cocks [58] proposed a quadratic residuosity based solution, while Boneh et al. [59] and Hess [60] introduced similar schemes using bilinear Diffie-Hellman problem.

An ID-based system is very efficient for a VANET since a verifier entity (e.g., an OBU) does not require to store, fetch, and verify the public key certificates of the emergency/road-safety application message signer from a third-party trusted authority. As a result, a VANET can save on storage, communication bandwidth, and time— making an ID-based system a potential replacement for a conventional PKI-based signature scheme used in vehicular networks.

Delegation of rights to sign messages on behalf of the originator of the message is a much required feature for many of the road-safety/emergency applications in VANETs. In a system where it is impractical for an original signer (e.g., department of transportation) to sign a message destined to an end user or a verifier (e.g., an OBU), the right of signing can be transferred or delegated to an intermediate entity (e.g., an RSU, or an OBU) called a proxy signer.

A proxy-signer RSU signs messages on behalf of the original signer, and when the end user (usually an OBU) verifies the message s/he can distinguish the signed message as signed by the proxy signer RSU rather than the original signer.

Originally introduced by Mambo et al. [49] in 1996, proxy signature mechanism has been improved further by a number of researchers with new security features and added functionalities [50, 51, 52, 53, 61, 62, 63, 64]. In general, a proxy signature offers a system with resilience to message forgery, repudiation, impersonation, and exculpability. In Chapter 3 and in our work [65, 66, 67], we used proxy signature scheme for protecting user-privacy, as well as to thwart replay attacks in vehicular ad hoc networks.

We considered each RSU as a valid member of some RSU group where each member RSU would include its certificate within the periodic beacon or WAVE Service Announcement (WSA) [6] to authenticate itself. We also assumed that an RSU is trusted by the central authority, while an OBU doesn't trust the corresponding RSU without verifying its received messages.

In this chapter, we present a practical VANET security scheme where RSUs are independent of each other for signing and delivering a message on behalf of the central authority (CA). A verifier can verify the message by using its own location information, and without requiring any public-key certificates. We also provide forwarding of signature components to the OBUs that are beyond the communication range of the signing RSU.

4.3 Preliminaries

In this section, we briefly describe the fundamentals of identity-based signature, proxy signature, as well as the elliptic curve digital signature algorithm (ECDSA).

4.3.1 Identity-based Signature

An identity-based signature [60] consists of the following phases.

i. *Setup:* A third-party trusted authority (TA) generates a random secret $t \in \mathbb{Z}_P$, and computes $Q_{TA} = tG$, where G is a generator. Derived Q_{TA} is a public key, and t is the secret key kept within the TA.

ii. *Extract:* A signer uses its identity (ID) to request for the secret key from TA. TA computes the secret key, $S_{ID} = tH(ID)$, and returns it to the signer in a secure way. This step is carried out once for each entity.

iii. *Sign:* A signer uses the secret key (S_{ID}) to generate the identity-based signature using an underlying signature scheme.

iv. *Verify:* A verifier of an identity-based signature uses the signature credentials, the publicly-known ID, as well as the public key Q_{TA} to verify the signature.

4.3.2 Proxy Signature

Definition 1. Proxy signature refers to a variation of digital signature that designates an entity (called a proxy signer) to sign a message on behalf of the original signer.

Definition 2. Partial Delegation: The original signer derives a secondary secret key from a primary secret such that it is computationally infeasible to retrieve the primary secret from the knowledge of the secondary secret key. The primary secret is kept with the original signer, while the derived secret key is delivered to the proxy signer in a secure way.

Proxy Signature Mechanism

A proxy signature scheme involves an original signer, a proxy signer, as well as a verifier in proxy preprocessing, proxy signature, and verification phases. The following steps are generally followed:

i. *Proxy derivation:* An original signer generates a proxy key from the original secret key as required by *partial delegation* based proxy signature.

ii. *Proxy delivery and verification:* Original signer delivers the proxy tuple to the proxy signer. A proxy signer can verify the proxy tuple using a verification equation.

iii. *Signing:* A proxy signer uses any ordinary digital signature scheme to sign a message on behalf of the original signer. It uses the proxy key (derived by the original signer) as the secret key for signing the message.

iv. *Verification of the proxy signature:* Upon reception of a signed payload, an end user derives a new public key from the original signer's public key using the modified verification equation. This new public key is used for verification of proxy signature using the verification method of the corresponding signature scheme.

4.3.3 On ECDSA

The IEEE Std 1609.2 [5] for Wireless Access in Vehicular Environment (WAVE) define the VANET security services, which adopted ECDSA-based [36] message authentication for vehicular communications. ECDSA is a variant of the conventional Digital Signature Algorithm (DSA) which is based on the Elliptic Curve Cryptosystem (ECC). ECC provides the same level of security strength as the other discrete logarithm based systems, while the size of required parameters for ECC is much smaller than that of the discrete logarithm based systems. Therefore, ECDSA is fast, efficient and an effective mechanism for a service oriented, ad hoc, and dynamic network like VANET.

We use an elliptic curve over a finite field for our scheme. Below, we discuss the fundamentals of elliptic curves and ECDSA.

Definition 3. For a prime number q, a finite field $\mathbb{F}_q$ is a finite set of q elements along with addition and multiplication operations on $\mathbb{F}$. The number of elements is denoted as the order of the finite field. There exists a finite field of order q if and only if q is a prime power ($q = p^n$, where p is a prime number, and n is any positive integer), and on the other hand, if q is a prime power, then there exists only one non-isomorphic finite field of order q denoted by $\mathbb{F}_q$.

Definition 4. An Elliptic Curve E over a finite field $\mathbb{F}_p$ is defined in the form of the following equation:

$$y^2 = x^3 + ax + b, \tag{4.1}$$

where prime $p > 3$; $a, b \in F_p$, and $4a^3 + 27b^2 \not\equiv 0(mod\, p)$. The set of elements of the Elliptic Curve $E(\mathbb{F}_p)$ consists of the points (x, y), where $x \in \mathbb{F}_p$ and $y \in \mathbb{F}_p$. A point at infinity O together with the set of points $E(\mathbb{F}_p)$ identifies an elliptic curve.

Note that the point addition, multiplication, and inversion operations on an elliptic curve are different from ordinary binary operations. Please refer to [36] for the detailed description of the above mentioned point operations.

ECDSA Domain Parameters

The domain parameters of Elliptic Curve Digital Signature Algorithm (ECDSA) require an Elliptic Curve E over a finite field of size q, and a base point $G \in (\mathbb{F}_q)$. Value q is chosen as a prime power p^n, where p is a prime number, and n is a positive integer. In our scheme, $n = 1$, thus $p = q$. Also, as indicated in Equation (4.1), two field elements a and b are chosen, where $a, b \in (\mathbb{F}_q)$. All these parameters could be shared by the entities or by some specific user depending upon the ECDSA configuration.

ECDSA Steps

A signer of message m follows the steps:

i. *Key Pair Generation:* Select a random number $d \in_R \mathbb{Z}_q^*$ to compute $Q = dG$, where G is a base point of the elliptic curve $E(\mathbb{F}_p)$.

ii. *Signature Generation:* The signer computes $(x_1, y_1) = kG$, where k is a random number and $1 \leq k \leq q$. The signer then computes $r = x_1 mod\ q$, and $s = k^{-1}(SHA1(m) + dr) mod\ q$; where if $r = 0$ or $s = 0$, the signer aborts the current operation and restarts the procedure. (r, s) represents the signature for message m.

iii. *Verification:* A verifier first checks if r and s are in the interval $[1, q - 1]$. It then does the following computations: $w = s^{-1} mod\ q$.
$u_1 = SHA1(m)w\ mod\ q$.
$u_2 = rw\ mod\ q$.
$(x_1, y_1) = u_1G + u_2Q$.
$\bar{x}_1$ =Integer form of x_1.
If $(x_1, y_1) \neq \mathcal{O}$, and $\bar{x}_1\ mod\ q = r$, the verifier accepts the signature, otherwise rejects.

4.4 Our Scheme

As required by an identity-based system, signatures on VANET application messages in our approach are to be made verifiable using a publicly known identity information associated with the signer. This essentially waives the necessity of a public key certificate from a trusted third-party for the signature verification.

We use the current location information of a signer as its identity in order to sign and verify the proxy signature, while ECDSA is used as the basic signature generation and verification mechanism. Table 4.1 denotes the notations used throughout the illustration of our scheme.

Table 4.1: Notations.

Component	Description
CA	trusted third-party central authority
q	a prime number of size 160 bits
x	system's master secret; $1 < x < q$
G	a base point on the elliptic curve $E(\mathbb{F}_p)$
k_o	a random secret with $1 < k_o < q$ for the original signer
k_i	a random secret with $1 < k_i < q$ for proxy signer i
$H(.)$	a one way hash function (e.g., SHA1)
m	a message to be signed by the proxy signer
t_m	expiry information of message m
a_m	position tolerance for a message m
loc_i	location information of the proxy signer RSU_i
ID_o	given identity of the original signer of m
t	current time, rounded up in seconds, or minutes
$\|\|$	concatenation operation

4.4.1 Application Zone

A VANET application might be valid only within a certain area of VANET. A provider (either a CA, or an RSU) can decide the application zone for individual message, within which a message is issued and valid for. If the application message is delivered outside the zone determined by the message source, it would be discarded immediately by the receiver. A technique is given below for determining the position tolerance of an application message along with the verification procedure using which an OBU can determine if a received message is legitimate for the current location, or not. We neglect the fading and propagation issues of data communications.

Derivation of a_m

A position tolerance value a_m is associated with each message m as CA generates the message. The tolerance value a_m indicates the application zone of the corresponding message m. In Figure 4.1, the solid circle represents the application scope of m, whereas the dashed circle indicates the communication range of an RSU. CA— the actual source of m, determines a region for which m is valid as a safety application message. Let γ be the radius of the application scope for message m. We assume that γ is always a power of 2. That is, for any positive integer δ, $\gamma = 2^{\delta}$. Hence, the tolerance value for message m is computed as $a_m = \delta = \log_2 \gamma$. This a_m will be used by a receiving OBU to determine the validity of m in its current location.

Validation of the Application Zone

Upon receiving a message m, an OBU compares its own location (obtained from GPS data) with the origin of m taking into account the tolerance value a_m specified in the message.

Let the current GPS data include l-bits long x_{OBU} and y_{OBU} for latitude and longitude of an OBU respectively. Validation of application zone of a received message is done at the corresponding receiver OBU in following manner:

i. Take $l - a_m$ most significant bits from both x_{OBU} and y_{OBU} and replace the

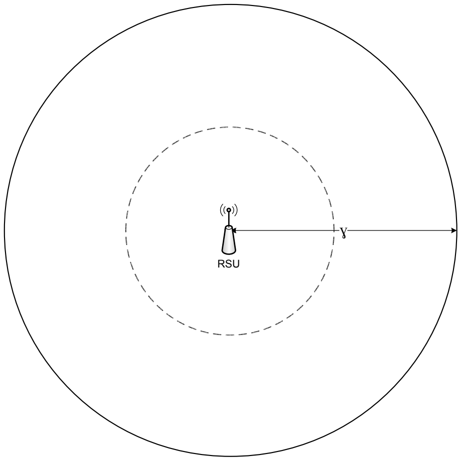


Figure 4.1: Application zone of a message m as shown by the solid circle, and the communication range of an RSU as indicated by dashed circle.

remaining bits with 0s. Use the outcome x'_{OBU} and y'_{OBU} as rounded values for the current position of the OBU.

ii. Check if (x'_{OBU}, y'_{OBU}) matches the RSU's rounded location information (x'_{RSU}, y'_{RSU}) of the received message. If it does, the application zone is valid, otherwise not.

4.4.2 Identity-based Proxy Signature With ECDSA for VANET

An emergency/road-safety application message is issued by a trusted central authority (e.g., department of transportation), while the released message is signed and delivered to the end users (OBUs) by a local RSU on behalf of the originator of the message.

We define the following steps to formulate an identity-based proxy signature with ECDSA for VANET applications.

Key Setup

i. CA generates a system secret x, where $1 < x < q$ and computes

$$Q = xG. \tag{4.2}$$

This Q is a public parameter, and is preloaded to all possible verifiers in the network.

ii. CA then randomly picks k_o, where $1 < k_o < q$ for the original signer to compute

$$R_o = k_o G. \tag{4.3}$$

iii. For each RSU_i, CA assigns a random number k_i, and determines R_i using the following equation.

$$R_i = k_i G. \tag{4.4}$$

Generated Q, R_o, and R_i are securely delivered to the RSU_i.

Proxy-key Extract

i. The identity of the original signer CA, and the location of the proxy signer RSU_i (ID_o, and loc_i respectively) are public, and all verifier OBUs in the vicinity of an RSU are aware of their own locations from their individual GPS devices. CA generates message m along with its expiry information t_m, and the position tolerance a_m. It then computes,

$$h_{i,m} = H(loc_i \| ID_o \| m \| t_m \| a_m). \tag{4.5}$$

ii. The proxy key of RSU_i for a message m is computed at the CA as

$$s_{i,m} = (k_i + h_{i,m}x)k_o^{-1} \; mod \; q. \tag{4.6}$$

iii. $(s_{i,m}||m||t_m||a_m)$ is delivered to the RSU_i in a secure way. The proxy signer verifies the proxy key $s_{i,m}$ by checking if the following equation holds. If it does not, the proxy signer requests for a fresh proxy key from the original signer CA.

$$R_i = (s_{i,m}R_o - h_{i,m}Q) \; mod \; q. \tag{4.7}$$

Proxy Signature

i. RSU_i computes a session parameter k_p from its location (loc_i) and the system time t.

$$\begin{aligned} k_p &= H(loc_i||t). \\ (x_p, y_p) &= k_pR_o. \end{aligned} \tag{4.8}$$

ii. Once the payload is processed, proxy signer RSU_i generates the proxy signature using the following equation.

$$s_{p,i,m} = k_p^{-1}(H(m) + s_{i,m}x_p) \; mod \; q. \tag{4.9}$$

iii. The proxy signature $(s_{p,i,m}||R_o||R_i)$ along with the tuple $(m||t_m||a_m)$ is delivered to the end user (an OBU).

Verification

i. Upon receiving a signed message, a receiver OBU_j computes:

$h_{j,m} = H(loc_j||ID_o||m||t_m||a_m)$, where loc_j denotes the location of OBU_j.

ii. The following verification equation is checked:

$$(x_p, y_p) = (H(m)R_o + x_p(R_i + h_{j,m}Q))s_{p,i,m}^{-1} \ mod \ q. \tag{4.10}$$

If the above equation holds, the signature over message m is valid. Value x_p is independently computed at the verifier end using verifier OBU_j's location loc_j and current system time t in Equation (4.8). We consider that the rounded up location information of RSU_i is same as the rounded up location information of OBU_j within the RSU's communication range. That is, $loc_i = loc_j$ if OBU_j is in the communication range of the RSU_i.

Correctness of the Scheme

We investigate the correctness of our scheme by deriving the following lemmas related to our proxy-key generation and proxy signature verification equations.

Lemma 1. *If the proxy key verification equation holds, the proxy key is valid.*

Proof. The proxy key (Equation (4.6)) is given as:

$s_{i,m} = (k_i + h_{i,m}x)k_o^{-1} \ mod \ q.$

1. Multiplying both sides by k_oG gives:

   $s_{i,m}k_oG \ mod \ q = (k_iG + h_{i,m}xG) \ mod \ q.$

2. Using Equations (4.2), (4.3) and (4.4) yields:

   $s_{i,m}R_o = (R_i + h_{i,m}Q) \ mod \ q$

   or, $R_i = (s_{i,m}R_o - h_{i,m}Q) \ mod \ q.$

This is proxy key verification equation used by proxy signer RSU_i. Hence, if the verification equation holds, the proxy key is valid. □

Lemma 2. *If a proxy signature* $(s_{p,i,m}||R_o||R_i)$ *on a given message content* $(m||t_m||a_m)$ *is generated by a valid proxy signer* RSU_i*, it would be accepted by a verifier* OBU_j*.*

Proof. The proxy signature equation (Equation (4.9)) is given as:

$$s_{p,i,m} = k_p^{-1}(H(m) + s_{i,m}x_p) \ mod \ q$$

or, $s_{p,i,m} = (k_p^{-1}H(m) + s_{i,m}x_pk_p^{-1}) \ mod \ q.$

1. Using Equation (4.6), we get:

$$s_{p,i,m} = (k_p^{-1}H(m) + (k_i + h_{i,m}x)k_o^{-1}x_pk_p^{-1}) \ mod \ q$$

or, $s_{p,i,m} = (k_p^{-1}H(m) + k_ik_o^{-1}k_p^{-1}x_p + h_{i,m}xk_o^{-1}k_p^{-1}x_p) \ mod \ q.$

2. Dividing both sides by $s_{p,i,m}$, we get:

$$1 = (k_p^{-1}H(m)s_{p,i,m}^{-1} + k_ik_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1} + h_{i,m}xk_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1}) \ mod \ q.$$

3. Multiplying by G on both sides, we get:

$$G = (k_p^{-1}H(m)s_{p,i,m}^{-1}G + k_ik_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1}G + h_{i,m}xk_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1}G) \ mod \ q$$

or, $G = (k_p^{-1}H(m)s_{p,i,m}^{-1}G + (k_iG)k_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1} + h_{i,m}(xG)k_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1}) \ mod \ q.$

4. Replacing (xG) and (k_iG) using Equation (4.2) and (4.4) yields:

$$G = (k_p^{-1}H(m)s_{p,i,m}^{-1}G + R_ik_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1} + h_{i,m}Qk_o^{-1}k_p^{-1}x_ps_{p,i,m}^{-1}) \ mod \ q$$

or, $k_pk_oG \ mod \ q = (k_oH(m)s_{p,i,m}^{-1}G + R_ix_ps_{p,i,m}^{-1} + h_{i,m}Qx_ps_{p,i,m}^{-1}) \ mod \ q.$

5. Using Equation (4.3), we get:

$$k_pR_o \ mod \ q = (R_oH(m)s_{p,i,m}^{-1} + R_ix_ps_{p,i,m}^{-1} + h_{i,m}Qx_ps_{p,i,m}^{-1}) \ mod \ q$$

or, $(x_p, y_p) = (R_oH(m)s_{p,i,m}^{-1} + R_ix_ps_{p,i,m}^{-1} + h_{i,m}Qx_ps_{p,i,m}^{-1}) \ mod \ q$

or, $(x_p, y_p) = (R_oH(m) + x_p(R_i + h_{i,m}Q))s^{-1}_{p,i,m}\ mod\ q$.

6. A verifying OBU receives a message within the communication range of the corresponding RSU. Since, OBU_j is in the communication range of RSU_i, we can say $loc_j = loc_i$ which implies $h_{i,m} = h_{j,m}$ from Equation (4.5). Therefore, the above equation yields as: $(x_p, y_p) = (R_oH(m) + x_p(R_i + h_{j,m}Q))s^{-1}_{p,i,m}\ mod\ q$.

We derived the verification equation from the proxy signature equation (Equation (4.9)). Hence, if a proxy signature is generated by a legitimate proxy signer, the signature passes the verification process. □

4.4.3 Forwarding of VANET's Safety Messages

If the application zone of a VANET's safety application does not have a complete network coverage through RSUs (as shown in Figure 4.2), an outbound vehicle's OBU can be used for forwarding authenticated messages to the vehicles operating beyond the RSU's communication range. An OBU outside the communication range of an RSU may receive the broadcast through an intermediate "message-forwarder" OBU. The receiver vehicles verify the signature contents. One easy way to accomplish this is to forward exactly the same signature materials as received from the RSU. The receiving OBU verifies the signature as if it received the message from the corresponding RSU. However, since the message is already received and authenticated by the forwarding OBU, repeating the full verification process in each receiving OBU would be inefficient, specially when the traffic density is high. Also, in case of any traffic dispute, there would be no way to distinguish the message source— whether it was received directly from an RSU, or from an intermediate

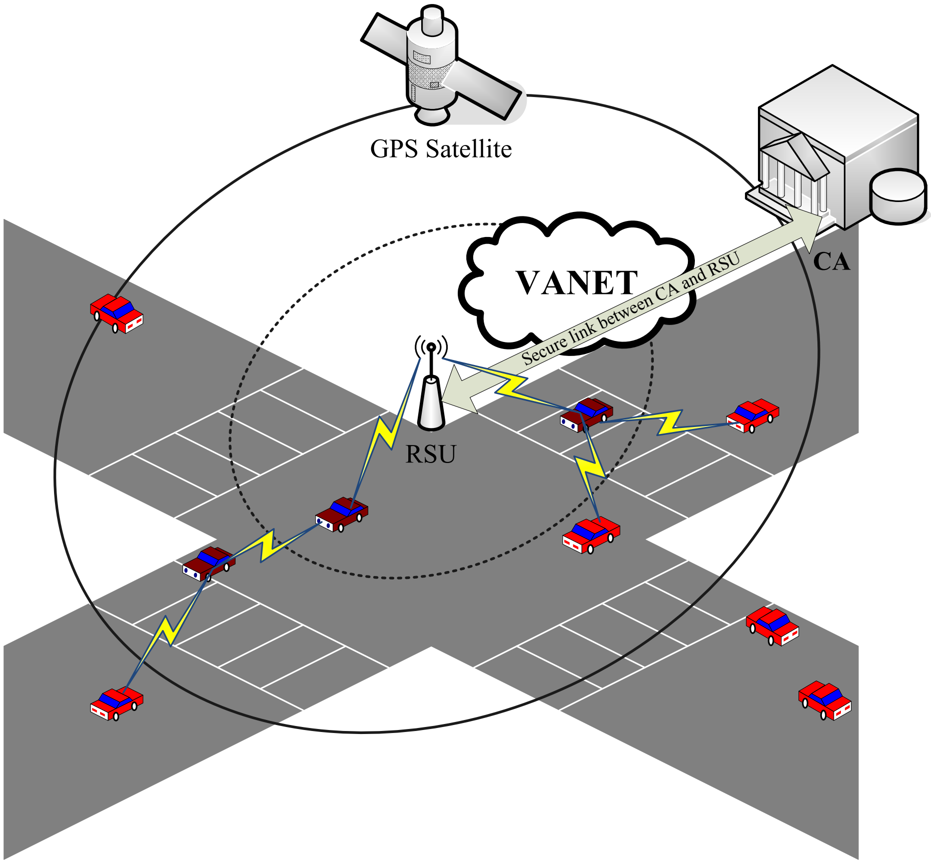


Figure 4.2: Framework of ID-based Safety Message Signature and Forwarding in VANET.

OBU.

We present an efficient and bandwidth friendly way of signature forwarding for RSU messages.

If the proxy signature from RSU_i is verified and accepted by an OBU, the OBU can forward the contents $(s^{-1}_{p,i,m}||u||R_o||m)$ [where $u = (R_i + h_{j,m}Q)$] to vehicles that are in the communication range of the forwarding OBU, but outside the range of RSU_i. Note that $(R_i + h_{j,m}Q)$, and $s^{-1}_{p,i,m}$ are already derived at the forwarding OBU during the signature verification process. R_o was pre-computed at CA during the key setup phase. Assuming that a receiver of forwarded content is identified as loc'_j (=current location of OBU'_j) whose clock is synchronized with the VANET system time, and the vehicle is within the application zone of m, the forwarded signature is verified as follows.

i. Compute $k' = H(loc'_j||t)$.

ii. Compute $(x', y') = k'R_o(mod\ q)$.

iii. Verify $(x', y') = (H(m)R_o + x'u)s^{-1}_{p,i,m}(mod\ q)$.

If the equation holds, the forwarded message is accepted. Otherwise, the received message is rejected.

Note that this verification equation is a variation of Equation (4.10). In Lemma 7, we discuss the security of VANET message forwarding.

4.5 Security Analysis

The security of our scheme depends mainly on the size of the prime q, and the hardness of solving the elliptic curve discrete logarithm problem.

An original signer of a safety message is a trusted entity. We assume that the central authority (CA) is secured against any kind of physical compromise, whereas a proxy signer RSU could be malicious, or compromised by an adversary. Therefore, an RSU would not be trusted by a vehicle without the verification of the generated proxy signature for a particular message.

We consider the following points for attack/misbehaviour scenarios on our scheme:

- A malicious RSU may attempt to sign a false or a modified message.
- An RSU may launch a replay attack by signing an old message.
- Given that there are multiple RSUs under the same central authority, a malicious entity may attempt to falsify an RSU by impersonating it and sending forged signatures over harmful messages. This misconduct is known as *exculpability*.
- A malicious RSU may sign a harmful message, and later deny its involvement in producing such signature. This misbehavior is referred to as *repudiation*.

In the light of the above points, we derive the following lemmas to prove the strength of our scheme.

Lemma 3. *RSU_i **can not generate a valid proxy key** $s_{i,m}$.*

Proof. In order to generate a valid proxy key $s_{i,m}$, a proxy signer RSU_i would require the system secret x, hash value $h_{i,m}$ over the corresponding location and identity (loc_i and ID_o), and two other random numbers k_i, k_o as indicated in Equation (4.6).

The secret x is irreversible from the knowledge of the public key Q, since that involves point multiplications over an elliptic curve $E(\mathbb{F}_p)$.

The corresponding location values indicate the location information of the entities, which are fixed and must not be altered by the proxy signers as they will be used by the verifier OBUs during the verification of the proxy signature.

The other two random numbers: k_i and k_o are selected by the CA. Assuming that both of them are 160 bit random numbers, total probability of a successful guessing of k_i and k_o is $1/(2^{160}-1)^2$.

□

Lemma 4. *RSU_i can not launch a false message attack, or a replay attack.*

Proof. While signing a message m on behalf of CA, a proxy signer RSU_i uses the proxy key $s_{i,m}$ which has been derived by CA. As given in Equation (4.6), CA uses secrets k_i, k_o, x, and the hash value $h_{i,m}$. Derivation of hash $h_{i,m}$ requires the original message content m, and expiry info t_m. Therefore, any change or modification of the message content m, or expiry information t_m would result in a different proxy key $s_{i,m}$ for which the signature in Equation (4.9) would be different. This makes sure that a false message attack or a replay attack with this approach would not be successful.

In addition to that, a malicious RSU can not use a different value for the location information to reproduce the same signature in a different geographical area. This is because the location information of CA and the RSU_i are also associated with the corresponding proxy key as shown in Equations (4.5) and Equation (4.6). □

Lemma 5. *An ID-based ECDSA proxy signature in VANET is non-repudiable and non-exculpable.*

Proof. An adversary may use the identity of a different RSU to launch an impersonation attack. Suppose, RSU_v uses another proxy signer RSU_i's location loc_i instead of loc_v, and calculates $h_{i,m'} = H(loc_i||ID_o||m'||t_{m'}||a'_m)$ to use in Equation (4.6) for deriving RSU_i's proxy key $s_{i,m}$.

Since the location information of CA and the RSU_i are associated with the corresponding proxy key in Equation (4.5) and Equation (4.6), a malicious RSU can not use a different location value to reproduce the signature in a different VANET area. Therefore, assuming that the total number of RSUs would be less than q, one (other than CA) can not reproduce $s_{i,m}$ with an acceptable probability. Hence, a valid proxy signature $s_{p,i,m}$ for a given message can only be created by RSU_i, and thus, it is non-repudiable.

Apart from that, a verifier OBU would use loc_v as the location information of the proxy signer during the verification. Hence, using $s_{i,m'}$ instead of $s_{v,m'}$ for the proxy signature operation would not get the signature through the verification process.

The original signer CA keeps record of all individual proxy keys ($s_{i,m}$) along with corresponding k_i values. If there is any dispute, CA can reproduce the signature using the credentials of the disputed RSU(s). Therefore, a proxy signer RSU_i can not sign a message that would appear as signed by a different entity, which preserves non-exculpability in our scheme. □

Lemma 6. ***ID-based ECDSA proxy signature in VANET is resilient to a proxy-key compromise attack.***

Proof. Suppose, an adversary successfully compromises an RSU_i, and finds the proxy key $s_{i,m}$. The adversary then attempts to launch an impersonation attack by signing a potentially harmful message using the compromised proxy key $s_{i,m}$.

As indicated in Equation (4.9), for launching a modified message m', an adversary would require to generate the corresponding proxy key $s_{i,m'}$. However, as shown in Lemma 3, an adversary cannot produce a proxy key with an acceptable probability. Thus, signing a modified message using the compromised proxy key is not possible in our scheme. □

Lemma 7. ***A forwarding OBU can not forge a signed message.***

Proof. A forwarding OBU may attempt to modify the original contents of a signed message to dismantle the integrity of a VANET. However, any modification in the original message m would demand the forwarding OBU to derive a different $s_{p,i,m}^{-1}$ value. This will essentially require the corresponding proxy key $s_{i,m}$ as indicated in Equations (4.9) and (4.10).

As suggested by Lemma 3, an OBU is highly unlikely to be able to generate all the necessary secrets for deriving a valid proxy key. Hence, an ordinary forwarding OBU can not forge a signed message in our scheme. □

4.6 Discussion

In a certificate-based PKI system, a public key certificate must be verified by a verifier node. As a result, a certificate-based system requires more space, bandwidth, and computation time for storage, delivery, and verification of the certificate. In this section we provide the comparative analysis of related security and cryptographic primitives, as well as the communication overhead of our scheme.

4.6.1 Comparison with Related Security Schemes

Most established ID-based proxy signature approaches utilize the difficulty of solving Computational Diffie-Hellman (CDH) problem from bilinear pairings. The idea of ID-based signature with bilinear pairing by Hess [60] has been used by Zhang et al. [68] for an ID-based proxy signature scheme that uses *partial delegation* *with warrant* [50]. A variation of bilinear pairing based formal proxy signature approach is deduced by Xu et al. [69]. Similarly, Dong et al. [70], Gu et al. [71], Lang et al. [72], Li et al. [73], Wu et al. [74], and Zhang et al. [75] have proposed pairing-based schemes with slight modifications in each to offer different security and privacy features in ID-based proxy signatures.

However, it is often very difficult to generate appropriate combinations of parameters for pairing-based approaches as most typical and frequently made assumptions are not feasible in practice [76].

Besides, a pairing operation is substantially expensive in terms of time and computation complexity compared to a point scalar multiplication as indicated in [76, 77]. Our ID-based ECDSA proxy signature scheme for VANET outclasses all pairing-based approaches where multiple pairing operations are needed in *key setup*, *signature* and *signature verification* phases.

Therefore, we consider few other elliptic curve based proxy signature approaches to compare the computation time complexity. These schemes utilize the intractability of the elliptic curve discrete logarithm problem (ECDLP) to secure the proxy key generation and signature processes.

Tan et al. [78] proposed an ECDLP-based proxy blind signature which is an elliptic curve analogue of the discrete logarithm based proxy signature scheme. Although this proxy signature approach is easily computable, it is not very suitable for fast moving vehicles in a VANET scenario as the scheme requires multiple handshaking among original signer, proxy signer and the requester.

An extension of Tan et al. approach is presented by Qi et al. [79] where the authors incorporated a combination of integer factoring problem and elliptic curve discrete logarithm problem (ECDLP) to improve the security of the proxy blind signature. A similar approach for an elliptic curve based proxy signature scheme has been presented by Sun et al. [61].

A proxy-protected ECDSA signature scheme was presented by Chang et al. [62]. In a proxy-protected signature, an original signer can not forge a proxy signer as the generation of proxy key associates random secrets from both the original signer and the proxy signer. However, in this approach, a proxy signer can modify the contents of the message before signing, which is inappropriate for our intended VANET model.

Table 4.2 compares the proposed scheme with few other ECC-based techniques in terms of required operations for key setup, signature generation and verification stages. The most expensive operation type here is the point multiplication, since it involves multiple ordinary multiplications as well as modular inverse operations. On the other hand, a one-way hash function imposes very negligible computation complexity for processing. We ignore the computation time complexity invovled in key validation for each of the schemes.

Our scheme is efficient in computation time complexity compared to the standard ECDSA signature mechanism specified in the VANET security specifications, as it requires only one extra point multiplication and one additional hash operation during the signature generation, and verification phases for providing ID-based proxy signature capability. Besides, verification procedure for the forwarded messages does not require the modular inverse operation as it has been pre-computed by the forwarding vehicle.

Table 4.2: Comparison of related Elliptic Curve Cryptography (ECC) based schemes in terms of number of different operations used, and offered features. Each modular multiplication operation time is denoted as μ, while the time complexity of a modular inverse operation is expressed by a ξ. Also, the time complexity of a hash function is assumed as ψ.

Item	Key Generation	Signature	Verification	ID-based	Proxy-sign.
ECDSA [36]	μ	$\mu + \xi + \psi$	$2\mu + \xi + \psi$	✗	✗
ID-based ECDSA [80]	2μ	$\mu + \xi + \psi$	$3\mu + \xi + 2\psi$	✓	✗
Chang et al. [62]	4μ	$\mu + \xi + \psi$	$3\mu + \xi + \psi$	✗	✓
Sun et al. [61]	3μ	$3\mu + \xi + \psi$	2μ	✗	✓
Tan et al. [78]	4μ	$7\mu + \psi$	$3\mu + \psi$	✗	✓
Our scheme	$3\mu + \xi + \psi$	$\mu + \xi + 2\psi$	$3\mu + \xi + 2\psi$	✓	✓

4.6.2 Overhead Calculation

We consider WAVE's wireless short message protocol (WSMP) with a NIST P-256 elliptic curve [81] for signature generation and verification. A P-256 curve is generally used for signing certificates from a third-party trusted authority, whereas a P-224 curve is used for signing VANET messages.

The message format of a signed WSMP provided by the WAVE 1609.2 standard (Annex. C.6 of [5]) includes a certificate associated to the sender of a message. The total length of the secure WSM is 254 bytes including a 125 byte certificate from a third-party trusted authority, and 1 byte for the *type* field.

Our identity-based proxy signature has the signature components $(s_{p,i,m}||R_o||R_i)$

along with the message tuple $(m \| t_m \| a_m)$. If a P-256 curve is used, the *signature* payload within the WSM message would be of 64 bytes instead of its default length of 56 bytes in the WSM format. Each of $s_{p,i,m}$, R_o, and R_i would be of 32 bytes, while t_m and a_m are of 8 bytes each. The message payload m would be assigned to the *application data* field as $s_{p,i,m}$ and R_i values are sent within s and r subfields respectively.

Since our authentication mechanism does not require a third-party certificate for signature verification, we can reduce the total length of the WSM by deducting 126 bytes for certificate payload and the *type* field for the signer. However, R_o, t_m and a_m would add additional signature overhead of 48 bytes (32 bytes for R_o, 8 bytes for t_m and a_m each). Therefore, we reduce the total size of a WSM payload to only 184 bytes.

4.7 Simulation

Table 4.3: Simulation Parameters for MAC and PHY.

Parameters	Values
Simulation Area	$500 \times 100\ m^2$
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

We investigate the performance of our authentication scheme, as well as an ordinary proxy signature based scheme (please refer to Chapter 3) using network

Table 4.4: EDCA Parameters for IEEE 802.11p CCH (values taken from [1]).

Priorities	Type	CWMin	CWMax	AIFSN
AC1	Background	15	511	9
AC0	Best effort	7	15	6
AC2	Video	3	7	3
AC3	Voice	3	7	2

simulator (ns-2.34) over DSRC IEEE 802.11p control channel (CCH). The simulator is designed to work with four EDCA classes [4] to provide different access priorities for OBUs and the RSU's periodic safety message broadcasts. Related PHY and MAC parameters are chosen from [10, 82], as summarized in Table 4.3, and Table 4.4. For our scheme, signed WSMP messages with 254 bytes payload have been considered for each OBU's periodic safety messages following the signed WSM format, while RSU safety messages are of 184 bytes as indicated in Section 4.6.2. The payload for RSU and OBU messages in the ordinary proxy signature based scheme is chosen as 308 bytes including 125 bytes for the associated certificate, and the signature overhead of 156 bytes as shown in Chapter 3.

We consider a simple vehicular traffic scenario for a 500 m long bidirectional road with 4 lanes in each direction. We assume that vehicles have constant speed within the coverage of the RSU. Vehicles' positions within the lane are determined from the one dimensional spatial Poisson arrival process with average distance of 10 m. Each OBU, and RSU broadcast a WSM packet every 100 ms. Initial message delivery times for individual OBUs and the RSU have been uniformly distributed over 100 ms. The simulation has been performed for 30 seconds with a warm up period of 10.0 seconds. We averaged the outcome of 10 samples with different random seeds for each experiment.

Successful delivery ratio of OBU and RSU messages for different combination of access categories are summarized in Figure 4.3, 4.4, 4.5, and 4.6 for RSU's broadcasts on access categories AC0, AC1, AC2, and AC3 respectively. In each case, our scheme outperforms the ordinary proxy signature based scheme in terms of higher successful message delivery ratio in the VANET. Please note that AC0 has the higher priority than AC1 as listed in Table 4.4. We summarize our observations based on the following cases:

Case 1: RSU's access categories are higher than OBUs': RSU signed messages have very high success ratio (over 95% for up to 200 OBUs in VANET) under higher ACs when OBUs are assigned with lower ACs as shown in Figure 4.5(a), 4.5(b), 4.6(a), and 4.6(b). This is due to the fact that smaller contention window and AIFSN value of the higher priority RSU compared to lower priority OBUs provide more opportunities for the higher access classes to transmit successfully. However, high back-off delay in transmission and/or collisions of frames due to smaller contention window may limit the success of the periodic broadcasts. Figure 4.3(b) and 4.6(c) have shown that the RSU transmitting the signed messages on higher traffic classes have 95% successful delivery for only 100 OBUs. The first case is mainly due to the longer back-off delay from the RSU and OBU combination of AC0 and AC1, while the latter is from the collision of frames caused by small minimum contention window size of AC3 and AC2.

Case 2: RSU's access categories are lower than OBUs': The successful delivery ratio of RSU-signed messages over lower access classes still remains higher than the OBU-signed messages for scenarios with non-saturation condition. In Figure 4.3(c), 4.3(d), 4.4(c), and 4.4(d), the successful message delivery ratio is over 95% for about 200 OBUs in the communication range of RSU. This is due to the combination of RSU's access categories with large contention window (AC0 and AC1) and OBUs' access categories with short contention window (AC2 and AC3).

Because of the long back-off delay resulted from the large contention windows of AC1 and AC0, VANET gets into saturation as shown in Figure 4.4(a) where 95% RSU-signed messages are delivered successfully for up to 100 OBUs using our authentication scheme. Similar delivery success has been shown by the scenario of RSU access class AC2 and OBU access class AC3 in Figure 4.5(d). This is caused by collisions of signed message frames sent over AC2 to OBUs operating on AC3.

Note that when ordinary proxy signature based scheme is used, the VANET enters into saturation earlier than that of our authentication scheme due to the larger signature overhead of the conventional approach.

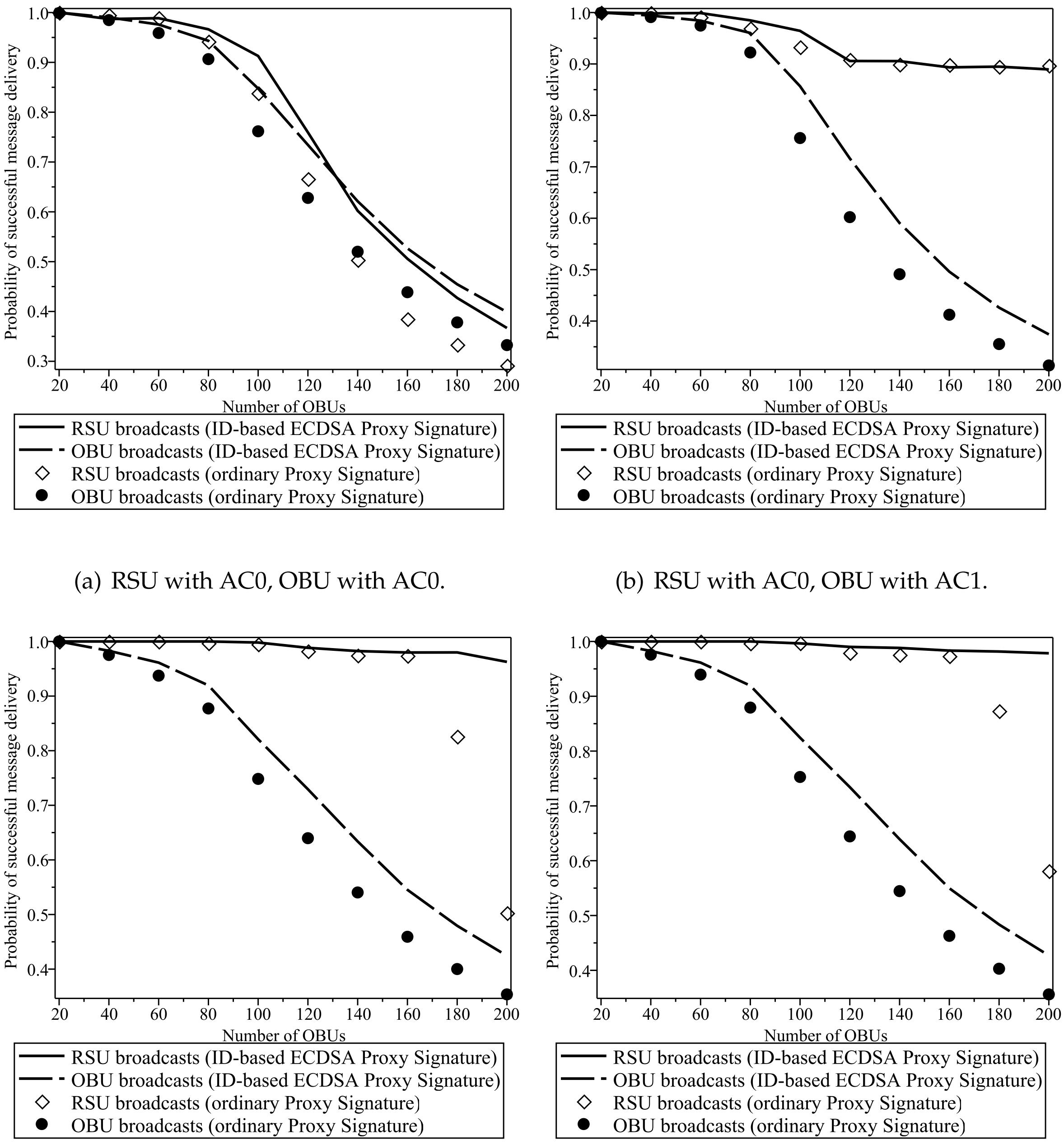
Case 3: RSUs and OBUs have the same access category: Figure 4.3(a), 4.4(b), 4.5(c) and 4.6(d) indicate the delivery ratio of RSU-signed messages and OBU-signed messages with the same access classes. As anticipated, all scenarios of equal access classes for RSU and OBUs perform almost similar to each other.

Because of the smaller contention window size and AIFSN value, OBU-signed messages over a higher access priority (AC2 and AC3) often collide with each other, and delivery of messages fail. Under the saturation condition when other data communications take place in the VANET along with the mandatory periodic safety message broadcasts, RSU-signed messages should always be associated with a higher priority traffic class (AC2 or AC3) when OBU-signed messages are on lower priority access categories. However, in order to achieve the highest successful delivery of RSU-signed messages in a VANET during a non-saturation condition, if the RSU transmits over a high priority traffic class, OBUs should transmit on a low priority access category, and vice-versa.

4.8 Summary

In this chapter, we presented a VANET framework for RSU's safety-message authentication using a new identity-based proxy signature mechanism. Security features of id-based systems along with the proxy signature is incorporated to accomplish the authentication requirements for infrastructure-generated vehicular safety messages. The central authority delivers road-traffic application messages with some signature credentials to corresponding RSUs. An RSU signs the message on behalf of the trusted central authority, and broadcasts to OBUs in its communication range. A receiver can verify the received messages by using its own location information without requiring any third-party certificates. Therefore, it saves on communication bandwidth, as well as the certificate verification processing time. Our scheme is accountable, resilient to all known attacks, and efficient. Security analysis, comparison with VANET standards and other related security primitives justify our authentication scheme. Results from the network simulation experiments allow us to determine the most suitable traffic classes for required communications in our scheme.

Our scheme allows centrally generated safety/emergency messages to be signed and relayed to OBUs by RSUs. Obviously, OBUs on road should also be able to



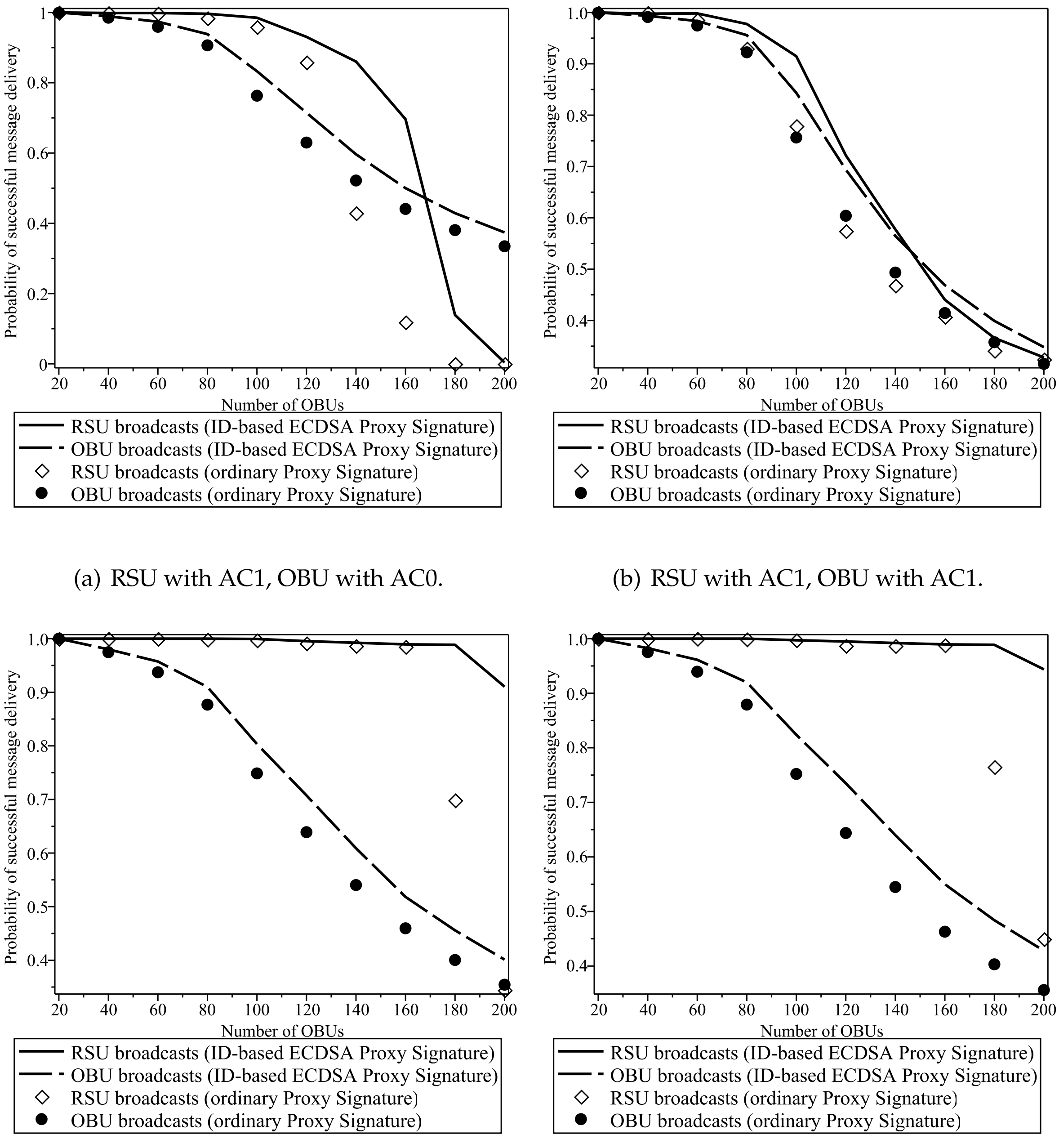
(a) RSU with AC0, OBU with AC0.

(b) RSU with AC0, OBU with AC1.

(c) RSU with AC0, OBU with AC2.

(d) RSU with AC0, OBU with AC3.

Figure 4.3: Successful message delivery ratio (RSU generates traffic with access category AC0): The dashed line is for the OBU messages (254B), while the solid lines indicate the RSU safety messages (184B).



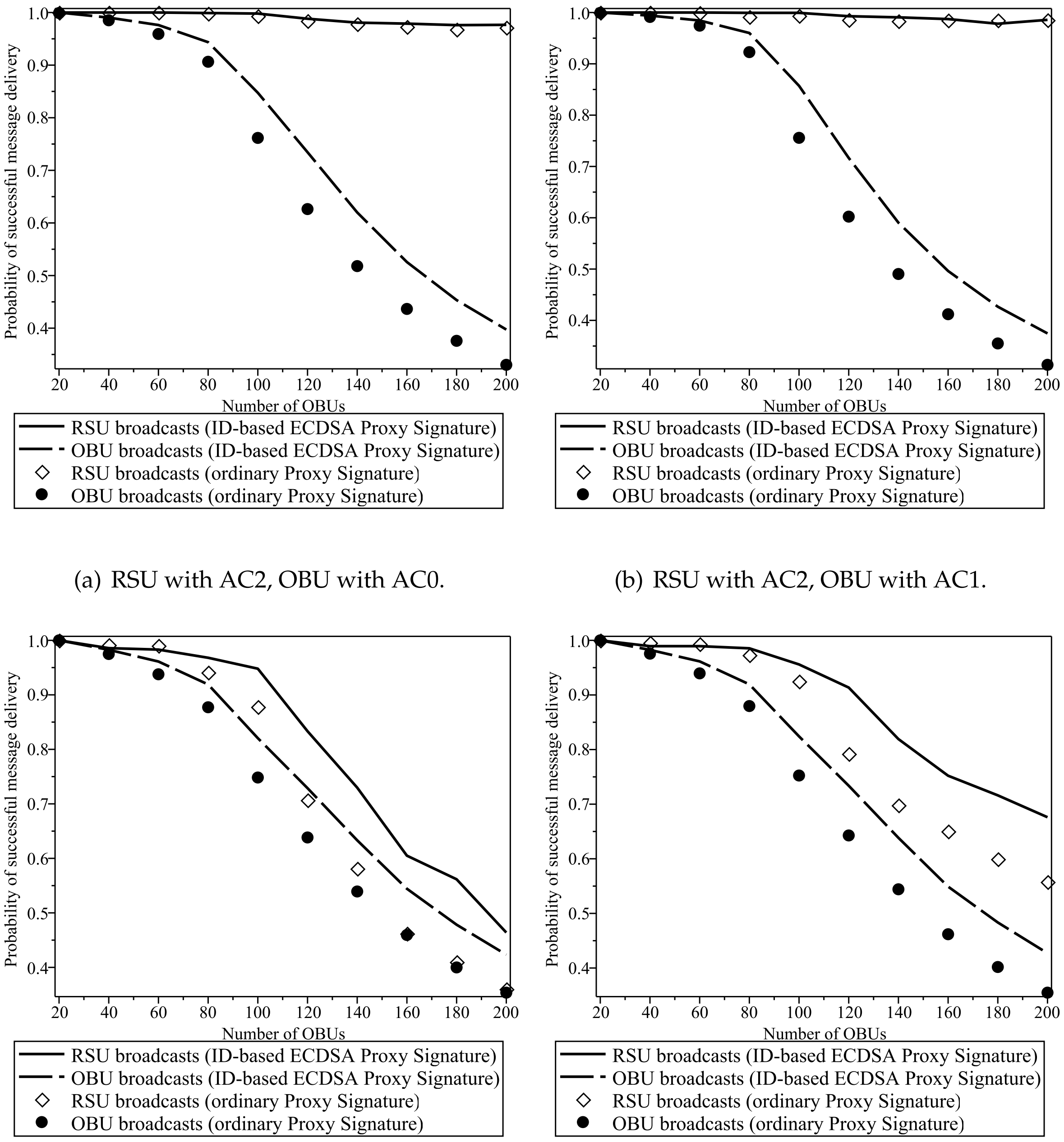
(a) RSU with AC1, OBU with AC0.

(b) RSU with AC1, OBU with AC1.

(c) RSU with AC1, OBU with AC2.

(d) RSU with AC1, OBU with AC3.

Figure 4.4: Successful message delivery ratio (RSU generates traffic with access category AC1): The dashed line is for the OBU messages (254B), while the solid lines indicate the RSU safety messages (184B).



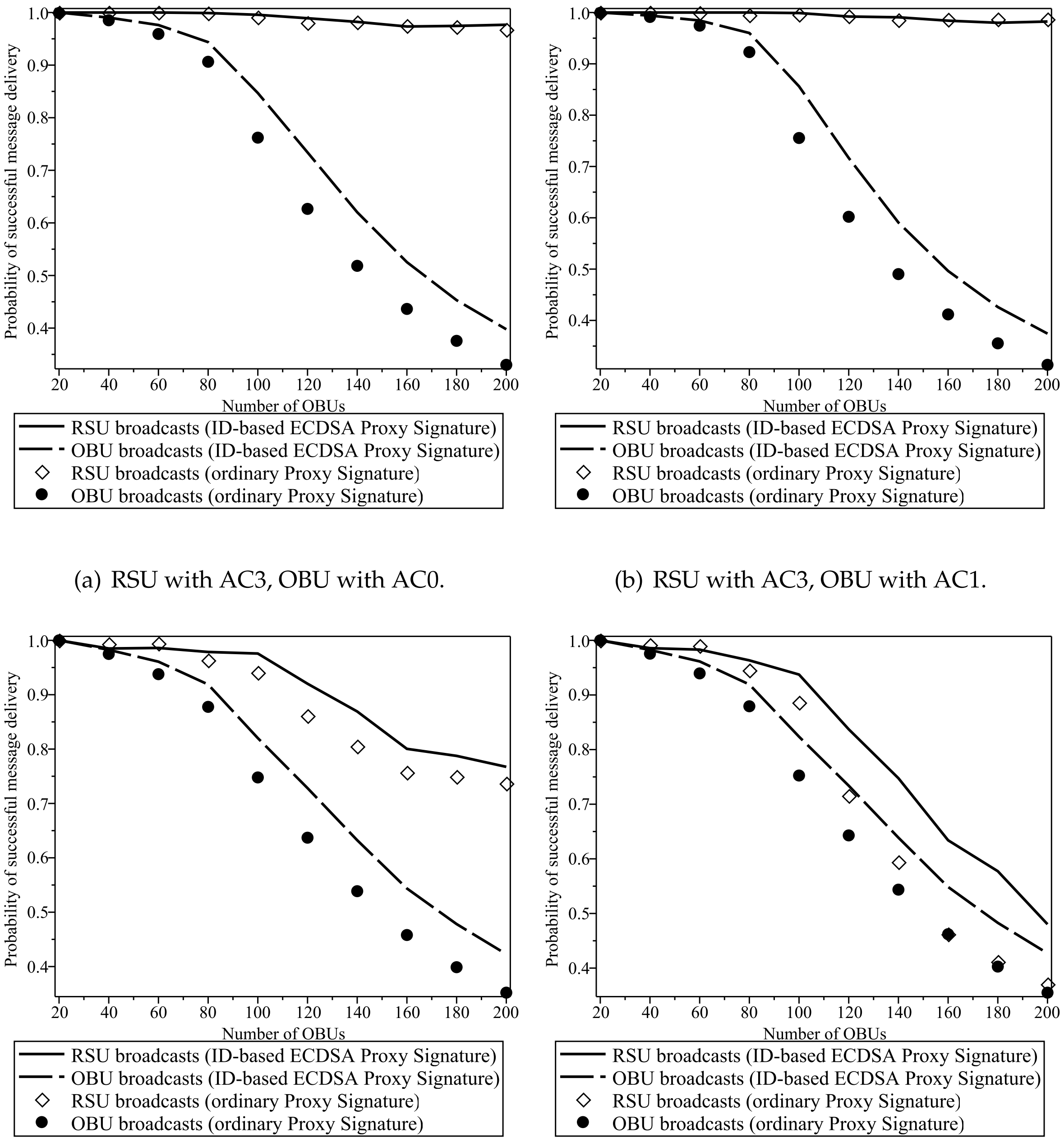
(a) RSU with AC2, OBU with AC0.

(b) RSU with AC2, OBU with AC1.

(c) RSU with AC2, OBU with AC2.

(d) RSU with AC2, OBU with AC3.

Figure 4.5: Successful message delivery ratio (RSU generates traffic with access category AC2): The dashed line is for the OBU messages (254B), while the solid lines indicate the RSU safety messages (184B).



(a) RSU with AC3, OBU with AC0.

(b) RSU with AC3, OBU with AC1.

(c) RSU with AC3, OBU with AC2.

(d) RSU with AC3, OBU with AC3.

Figure 4.6: Successful message delivery ratio (RSU generates traffic with access category AC3): The dashed line is for the OBU messages (254B), while the solid line indicates the RSU safety messages (184B).

produce similar emergency/road-safety messages. However, user-privacy would be an important aspect as a user's identity could be exposed by OBU-generated messages. In the following chapter, we introduce a new cross-layer scheme for privacy-preserving authentication that provides OBUs' safety/emergency message authentication, as well as an efficient way of message verification in VANETs.

Chapter 5

A Cross-layer Approach to Privacy-preserving Authentication in WAVE-enabled VANETs

5.1 Introduction

Authentication of received messages is essential for a reliable vehicular ad hoc network. VANET allows on-board units (OBUs) to deliver safety and/or other application messages to the neighboring vehicles to ensure safe driving, road-safety, and driver's comfort. However, a received traffic message from a VANET entity may contain harmful contents that can jeopardize the integrity of a VANET. Therefore, a VANET message should be authenticated upon reception.

As discussed in previous chapters, VANET trust issues can be addressed using an appropriate signature scheme (e.g., [36, 83]). Yet, an ordinary signature scheme reveals the actual identity of a signer which is undesirable as far as privacy is concerned. Nevertheless, unconditional privacy may impair the prospect of vehicular communications since an anonymous entity could deliberately transmit some false and misleading messages to its neighbors. Therefore, a VANET entity should be accountable to the corresponding authority in case of a critical event or dispute on road (e.g., a collision, or a traffic congestion).

A VANET entity is required to transmit periodic safety messages containing its current coordinates, speed, and acceleration to the neighboring devices. A typical interval for safety message broadcasts ranges from 100 ms to 300 ms. An authentication scheme has to be incorporated in order to provide reliability and trust for the delivered safety information. Received messages are verified by the receiving entity to ensure the message integrity, and authenticity of sender's identity. Unfortunately, signature verification incurs a cryptographic processing delay at the verifier's end. Although the verification delay for ECDSA is in the order of milliseconds [84], with hundreds of vehicles in a dense traffic scenario, an OBU would receive an enormous amount of periodic messages per unit time causing a bottleneck to the authentication process at the receiver end.

If OBUs are configured to broadcast their periodic messages every 100 ms, under a heavy traffic scenario, many of the safety messages would either be discarded due to the constrained buffer size of the receiver, or accepted without any verification. Therefore, in heavy traffic hours, a receiver of vehicular messages would either risk a fatal road-traffic consequence, or it would reject a significant portion of received messages without authenticating when its maximum verification capacity is reached.

The current WAVE standards do not include an efficient anonymous authentication scheme for vehicular messages, or even an intelligent authentication policy which can efficiently verify from a large number of vehicular safety/application messages.

A number of different signature schemes have been suggested to incorporate the anonymous authentication features for vehicular communications. We can roughly categorize them into two different types: *anonymous certificate-based approaches*, and *group signature based approaches*. These approaches are impractical and/or inappropriate for a large scale VANET implementation as they are either inefficient, or established on some infeasible mathematical assumptions.

In this chapter, we present a WAVE-based cross-layer scheme of privacy-preserving and conditional authentication for signing and verifying general purpose vehicular safety application messages. We develop a variant of ECDSA mechanism incorporating ID-based authentication [58, 60] where the current position of the signer vehicle will be used as the corresponding identity parameter for anonymous signature generation and verification. Unlike most other existing ideas of anonymous authentication, this scheme does not need a trusted third-party certificate, or any strong mathematical assumption-based signature procedures.

We assume that application priorities are mapped into the Enhanced Distributed Channel Access (EDCA) traffic classes in a VANET. The probability of successful delivery of message broadcasts depends on the WAVE's EDCA traffic class and the traffic load so that the receiver can scale message verification rates according to

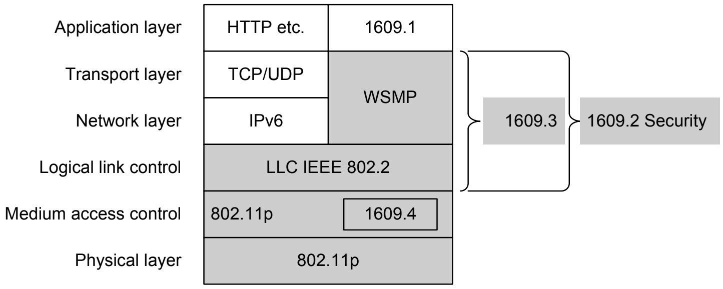


Figure 5.1: The cross-layer aspect of a WAVE-based VANET. Shaded layers are used in our scheme.

MAC priorities and traffic congestion. For message verification in a dense traffic scenario, received messages are chronologically ordered according to their relevance. The verification mechanism considers MAC-layer priorities along with the current traffic intensity to derive an adaptive verification probability for received messages.

Figure 5.1 gives a cross-layer aspect of our authentication scheme. Our scheme involves Security [5], Networking with WSMP [6], IEEE 802.11p MAC and PHY [1, 4] layers to generate the signature, to transmit signed periodic safety messages, and for the verification of received messages. VANET entities use WSMP packets for broadcasting periodic traffic-safety messages, while the message delivery and verification procedures of received messages rely on the EDCA mechanism of IEEE 802.11p MAC.

We organize the rest of the chapter as follows. Sections 5.2, and 5.3 contain anticipated attack/adversary model, and the design goals respectively. The anonymous user-authentication scheme is illustrated and discussed in Section 5.4. The prioritized message verification is described and analyzed in Section 5.5. Performance of the related networking issues have been discussed in Section 5.6 as Section 5.7 concludes the chapter.

5.2 Attack Model and Vulnerabilities

We assume that our communication channel is not secure, and participating OBUs are not trustworthy. Major attacks and malicious behavior of an adversary anticipated on an anonymous authentication scheme in VANET environment are listed below.

5.2.1 Message Forging

An adversary may attempt to forge a message by altering the original contents of a valid message from a legitimate OBU. It may also try to produce a valid signature on the altered message payload. Required secret credentials of the target node are either derived by guessing, or stolen from a legitimate OBU as OBUs are not equipped with tamper-resistant hardware.

5.2.2 OBU Compromise and Repudiation

An adversary may compromise an OBU to obtain its secret credentials which are used for generating valid signatures. Also, a compromised node may deliberately send false and harmful messages, and later deny its involvement in signing any such messages. Denial of responsibility of this kind is termed as repudiation.

5.2.3 Message Replaying and Tunneling

An attacker may collect and store a signed emergency message from a particular traffic area, and attempt to deliver it at a later time when the original message is invalid. Similarly, an attacker may collude with another attacker from a different area. A colluding attacker may tunnel the legitimate emergency messages from a specific traffic area to a different area where the message content is irrelevant for the given traffic. This unnecessary replaying of legitimate emergency or safety messages would create confusion among the VANET users in the new area.

5.2.4 Linking of Signatures

Signature linking refers to a situation when an attacker or an eavesdropper successfully distinguishes an anonymous entity within a group by linking some of its signatures. Back to back periodic messages might contain similar information in the message payload from a particular OBU. An adversary may attempt to use two or more consecutive signed messages from a node to identify the signer based on the received contents.

In a group-signature based approach, each vehicle belongs to a group which allows "group-anonymous" message signature [23] for vehicular authentications. However, if the ratio of the number of OBUs and the number of groups in a specific scenario is not high enough, the user-anonymity of the VANET is compromised.

Suppose, we have n vehicles from a maximum of $\mathscr{R}$ different OBU-groups in a traffic scenario. The probability of having a certain number of OBU-groups in the given scenario follows a multinomial distribution of OBUs over $\mathscr{R}$ groups.

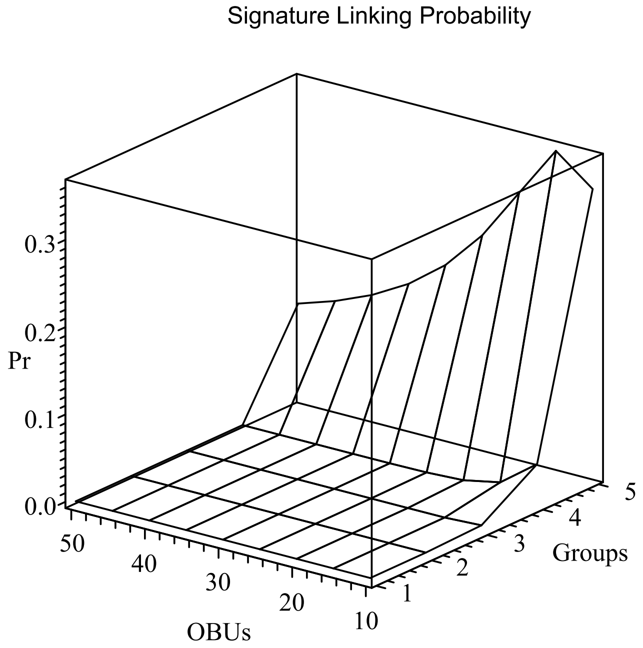


Figure 5.2: Signature linking probability in a group signature based approach.

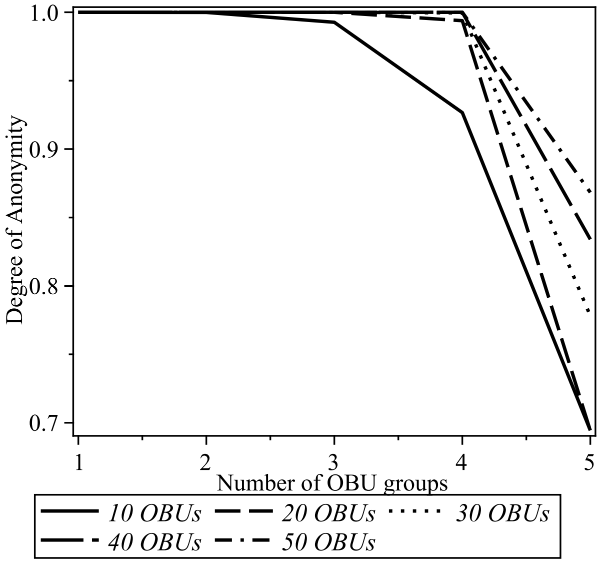


Figure 5.3: Degree of anonymity in a group signature based approach.

Therefore, for n OBUs with maximum r_l possible groups, the probability that a random OBU message from a group of r_1 nodes can be linked by its signature is computed as:

$$P_r(l,n) = \sum_{r_1=1}^{n-l+1} \dots \sum_{r_{l-1}=1}^{n-r_1\dots-r_{l-2}-1} \frac{n!}{r_1 \times r_1!r_2!\dots r_{l-1}!r_l!}\lambda^n, \tag{5.1}$$

where $\lambda = \frac{1}{\mathscr{R}}$, and $r_l = (n - r_1 - r_2\dots - r_{l-1})$.

Figure 5.2 plots the probability distribution for signature linking for the given group-anonymous VANET scenario.

Obtained probability (P_r) is used as the basis of measuring the degree of anonymity of a group signature based VANET. We use the information theoretic concept of entropy model presented by Díaz et al. [85] for analyzing the anonymity of a VANET. Entropy in information theory measures the contained information from a particular distribution of probabilities. The anonymity is measured based on the probability of an entity for being the sender of a transmitted message. In other words, we compute how distinguishable an OBU is among all the OBUs in a specific location. As shown in Figure 5.2 and 5.3, the anonymity of a group-anonymous VANET is under threat if a linking attack is launched using the group id of collocated vehicles belonging to several groups.

5.2.5 Random Verification Attack

This attack is a consequence of the vulnerability induced by a random verification policy. Success of a random verification approach is highly reliant on traffic density or the number of participants in the VANET, and therefore, un-sustaining.

A harmful message may get through the authentication process without verification to jeopardize the safety of the traffic system. In a dense traffic condition, it is quite unlikely that all received messages would be authenticated. Knowing that a verifier would randomly verify received messages, an adversary may take advantage of this situation by injecting a large number of harmful messages in each authentication cycle. This attack may bring fatal traffic consequences for a VANET-based traffic system. We define this attack as *random verification attack* in VANETs.

Hence, a realtime system like VANET must not risk an abuse by deploying the ordinary random verification approach which might allow a harmful message from a malicious VANET entity.

5.2.6 False Signature Attack on Batch Verifications

Signatures can be aggregated in batches for batch verifications. However, the whole batch would be dropped or rejected even if there is just one false signature in the batch.

An improved mechanism of batch verification [46] can isolate all false signatures in a batch. Upon detection of false signature in a batch, the verification algorithm divides the batch recursively, and follows a binary authentication tree (BAT) down to its leaves where individual signatures are associated. Nonetheless, this approach is effective only under normal situations when there are few false signatures in a batch.

A collusion of multiple attackers could make this approach unscalable in a high density traffic scenario since a verifier would require longer time to isolate individual malicious messages than the message inter-arrival time. This may eventually turn up as a denial of service (DoS) attack if all receivers in a VANET fail to process subsequent batches of signatures due to resource unavailability.

5.3 Design Goals

In order to mitigate the anticipated attacks and vulnerabilities in VANETs, we introduce the following design goals based on our attack model and anticipated vulnerabilities on an anonymous authentication scheme for VANET.

5.3.1 A Third-party Trusted Authority

We suggest a third-party trusted authority called central authority (CA) which would be responsible for generating and storing secrets, and signature credentials of OBUs and RSUs. It should be able to resolve any identity dispute on traffic incidents upon request from an appropriate authority (e.g., Police, Court, and Dept. of Transportation). The CA is secured and protected against all sorts of physical attacks and adversarial compromises.

5.3.2 Privacy-preserving ID of OBUs

In order to provide anonymous authentication through signed messages in a VANET, it is essential to have multiple entities (i.e. OBUs) in the network with an identical name so that individual nodes may not be recognizable from the sender information of the delivered messages. Therefore, for privacy-preserving authentication in a VANET, each participating OBU in a given area must have a common identifier. Assuming that each OBU is equipped with a GPS device, the common geographical area of participating OBUs can be used as the privacy-preserving identifier for individual OBUs. Identity information of an OBU is determined from the most significant bits of GPS coordinates so that all OBUs within the communication range of each other can have the same identity information.

5.3.3 Privacy-preserving Authentication for VANETs

- An adversary should not be able to associate a unique identifier with an OBU in a particular VANET. However, the third-party trusted authority or CA must be able to distinguish an OBU based on a unique credential used by the OBU. Retrieving the actual identity of an OBU might be required for resolving a traffic dispute that involves VANET communications. Therefore, a unique primary secret has to be associated with an individual node in a VANET.

- An OBU must have the proof of its association with the third-party CA, as well as the specific vehicle type, and the OBU itself. Hence, a secondary delegation key for each entity in VANET should be generated at the CA involving the third-party system, vehicle type identifier, and the OBU's primary unique secret.

- An adversary may obtain the secondary unique key (delegation key) by compromising an OBU from a stolen vehicle. This may encourage an adversary to launch false or harmful message delivery attacks using the compromised key. In that case, the responsibility of such malicious act would go to the original user of the compromised OBU of the stolen vehicle. Thus, the activation of signature generation process should be protected by a user-password at the OBU.

- An adversary should not be able to tunnel a signed message from a valid OBU to deliver it in a different area within the same time frame or at a different time. Therefore, a signing OBU must associate its current area (GPS location) information, as well as the current timestamp of the message during the signature generation process. A verifying node should also utilize its own area identifier and current time frame during the verification of a received message.

5.3.4 Limitations of Bilinear Pairing

Most existing anonymous authentication approaches (e.g., [18, 20, 25, 31]) and signature verification schemes for VANET use bilinear pairing as the foundation of their cryptographic primitives for VANET authentication and verification. When computation time and complexity are concerned, bilinear pairing operations are expensive compared to other alternative primitives in cryptography. Bilinear pairing-based approaches of cryptographic primitives have been criticized in [76] since most typical and frequently made pairing assumptions are impractical and not feasible to comply with.

5.3.5 Priority-based Verification of VANET Safety Messages

Efficient authentication of periodic safety messages is a challenge in VANETs with dense traffic conditions. Verifying all individual signatures in such conditions would create a bottleneck at each of the receivers.

Although we can not completely avoid a random verification attack (as indicated in Section 5.2.5), we can effectively reduce the impact of such misbehavior by introducing verification priorities among received messages. High priority messages would be more frequently verified than the low priority ones. Also, high-priority application messages must be less vulnerable to a random verification attack.

Therefore, application priority should be mapped into priority scheme of lower protocol layers (e.g., in Medium Access Control (MAC) traffic classes). This mapping would be beneficial for achieving the quality of service (QoS) differentiation among messages and protection against MAC-layer's denial of service (DoS) attacks [86]. Messages with high MAC priority have smaller delay and lower drop probability which enhance their chances of being verified at the receiving end.

5.4 Anonymous User-authentication in VANETs

In our authentication model, each vehicle is registered at the local transportation department which works as the central authority for providing the security and privacy to VANETs. Privacy credentials are securely preloaded into a vehicle's OBU during the registration or yearly renewal time.

5.4.1 Notations

Table 5.1 contains the list of notations that are used throughout the illustration of our scheme.

Table 5.1: Notations.

Component	Description
CA	Trusted central authority
Q	master public key
q	a large random prime number
x	master secret, $1 < x < q$
G	a base point over $E(\mathbb{F}_p)$
x_p	session parameter
k_i	primary secret associated to user i
$H_1(.), H_2(.)$	hash functions $H_1(.), H_2(.) : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
loc_p	area identifier of a user during session p
k_p	hash outcome of current area identifier and time
m	a message to be signed and delivered
t	a timestamp

5.4.2 Description

We derive following four functional steps of our scheme based on the modification of the original ECDSA mechanism.

Key Initialization Module

i. CA chooses the system secret x, where $1 < x < q$, and computes

$$Q = xG. \tag{5.2}$$

ii. CA associates a random primary secret k_i (where $1 < k_i < q$) with each individual OBU_i of a particular type. And, the vehicle-type identifier R_i is calculated as:

$$R_i = k_i G. \tag{5.3}$$

Suppose, $i, i+1, i+2, ..., i+N-1$ are registered vehicles, CA computes the vehicle-type identifier $R_i = k_i \ (mod\ q)G = k_{i+1} \ (mod\ q)G = k_{i+2} \ (mod\ q)G = ... = k_{i+N-1} \ (mod\ q)G$.

iii. Hash function $H_1(.)$ is used for computing $h_i = H_1(R_i)$.

iv. CA derives a unique partial delegation key (secondary key) for each vehicle i from the the master secret x using the corresponding primary secret k_i, and h_i values as indicated below.

$$s_i = (1 + x h_i k_i^{-1}) mod\ q. \tag{5.4}$$

$$s_{u_i} = s_i \oplus Password. \tag{5.5}$$

Derived user secret s_{u_i} is securely copied to the corresponding OBU_i's disk-space.

Pre-processing

In the beginning of OBU activation, a user enters his password which is then XOR-ed with the saved secret s_{u_i} to reproduce the actual delegation secret s_i.

A deliverable message, whether a periodic safety message, or an emergency event message such as a road-traffic accident notification is associated with the current system time, and the vehicle's position. Session parameters are obtained by the signer and a verifier entity (OBU and/or RSU) using the corresponding area information and current system time. The steps are given as:

i. The signing vehicle determines k_p for the message m.

$$k_p = H_2(loc_p||t). \tag{5.6}$$

The value of loc_p is rounded up by taking only few most significant bits of the GPS coordinates so that OBUs in the communication range of each-other would have the same loc_p.

ii. It then computes the session parameter x_p as

$$(x_p, y_p) = k_p R_i mod\, q. \tag{5.7}$$

Signature Generation

i. Once the session parameter x_p is generated for the message m, OBU signs the message as shown by the following ECDSA formula:

$$s_{p,i} = k_p^{-1}(H_1(m) + s_i x_p) mod\, q. \tag{5.8}$$

ii. The signature payload and the message are combined as $(m||R_i||s_{p,i})$ to be delivered to the neighboring vehicles (OBUs) and RSUs within the communication range of the OBU.

Verification

For a receiver OBU or RSU, it is important to verify the the source identity, as well as the integrity of the received message. The received signature components are used in the verification process as illustrated below.

i. A receiving entity computes k_p from its own area information and the current timestamp using the relationship given in Equation (5.6).

ii. Equation (5.7) is used to obtain (x_p, y_p) values by the verifier.

iii. The verifier entity computes h_i by following the relation $h_i = H_1(R_i)$.

iv. Finally, if the following relationship holds, the signature is verified as a valid one.

$$(x_p, y_p) = (H_1(m)R_i + x_p(R_i + h_iQ))s_{p,i}^{-1} mod\, q. \tag{5.9}$$

5.4.3 Security Analysis

Security of this scheme depends on the anticipated difficulty of solving the elliptic curve discrete logarithm problem. Following malicious behaviors and challenges are among the most anticipated ones in our anonymous authentication scheme:

Signature Forging

Generation of a signature by OBU_i involves the corresponding secret key s_i. As given in Equation (5.4), secret s_i is computed by CA using the system secret x, individual secret k_i, and h_i.

The system public key Q is known to all OBUs in a VANET. However, an adversary can not successfully determine the value of x from the knowledge of Q (= xG) due to the intractability of elliptic curve discrete logarithm problem.

On the other hand, k_i is a secret corresponding to the OBU_i, which is randomly generated and stored only within the CA. The hash value h_i is computed using k_i and G as given in $R_i = k_iG$, and $h_i = H_1(R_i)$. Therefore, an adversary would not be able to derive a valid signature on a message using OBU_i's k_i, h_i, and the system secret x.

Replaying Old/Expired Messages

Assume that an adversary attempts to replay an old and expired message m' in the VANET. The session parameter x'_p has been generated by the original sender using Equation (5.6) and (5.7) as shown in $k'_p = H_2(loc_p \| t')$, and $(x'_p, y'_p) = k'_p R_i mod\, q$, where t' is the timestamp used by the original signer of the message. If t' is an old/expired timestamp, the current session parameter x_p generated by verifying nodes would be different from x'_p which would discard the signed m' as an invalid message. Therefore, repeating an old and expired signature would not pass the verification process at the receiver OBU/RSU.

Message Tunneling

Let, loc_p'' be the area identifier of a verifier. A session parameter would be generated at the verifier's end as $k_p'' = H_2(loc_p'' \| t)$, and $(x_p'', y_p'') = k_p'' R_i mod\, q$. However, if the position of the original sender of the message is outside the communication range of the receiver, $loc_p'' \neq loc_p$ (where loc_p is is the position of the original signer). Therefore, the received session parameter x_p would be different from the receiver's session parameter x_p'', and hence, signature verification of the message would be unsuccessful in a different area than the area of the original signer of the message.

An adversary is unable to forge a signature in this scheme. Also, an old message from an OBU would not pass the verification process. Since the area information is embedded with each signature, the verification process of the received message would be unsuccessful if it is delivered at an area outside the communication range of the original sender.

Non-repudiation

In order to generate a message signature, a signer requires a unique secret key s_i, as well as session parameters k_p and x_p as shown in Equation (5.6) and (5.7) respectively. Nevertheless, a valid signature can not be produced without the unique secret s_i of a node, which is generated by the CA from the master secret key x as given in Equation (5.4). Calculation of the system secret x involves solving an elliptic curve discrete-logarithm problem. Thus, if a signature is successfully verified by a receiver, the message must have been signed only by the sender with the corresponding unique secret s_i. As a result, once a message is signed and delivered, the sender OBU can not deny the signature for the sent message.

OBU Compromise

An attacker may compromise an OBU_i to obtain its unique secret credential s_i using which an adversary may sign false and malicious messages later on. However, an OBU_i does not store the unique secret key s_i in its memory (since it is generated and stored only at the CA). As indicated in Section 5.4.2, the corresponding user-password is XOR-ed with the unique secret key s_i, while the outcome s_{u_i} is stored in the memory of OBU_i. In order to activate the OBU_i, the corresponding user-password is entered which is XOR-ed with the s_{u_i} to reproduce the unique secret s_i for signing messages.

Hence, in order to obtain the original value of s_i, an attacker must know the corresponding user-password. Therefore, a compromise in our scheme would not let an adversary find the unique delegation secret s_i.

Signature Linking

An OBU may sign identical payloads in subsequent time-frames. A timestamp t is used for generation of a session parameter x_p (refer to Equation (5.7)) during the signature preprocessing phase. The timestamp t is valid until 100 ms from the signature generation time. It ensures the change of signature contents in different time frames even if the message resembles to a previously sent expired message. An adversary attempting to link two or more subsequent signatures may not be successful as the signature contents change every time due to the change of the timestamp.

5.4.4 Overhead

For a 160-bit elliptic curve, the size of $s_{p,i}$ is 40 bytes. The current security standards for VANET [5] suggest two different types of NIST [81] curves: P-224 and P-256, which have signature size of 56 bytes, and 64 bytes respectively. While P-224 is used for safety message broadcasts, P-256 is generally used for certificate

Table 5.2: Comparison among VANET authentication schemes.

Authentication Scheme	Signature size (Bytes)
WAVE 1609.2 [5]	182
Lu et al. [20]	189
GSIS. [25]	201
Wu et al. [31]	137
Hybrid [34] (un-optimized)	298
Our scheme (160-bit EC)	40
Our scheme (NIST P-224)	56
Our scheme (NIST P-256)	64

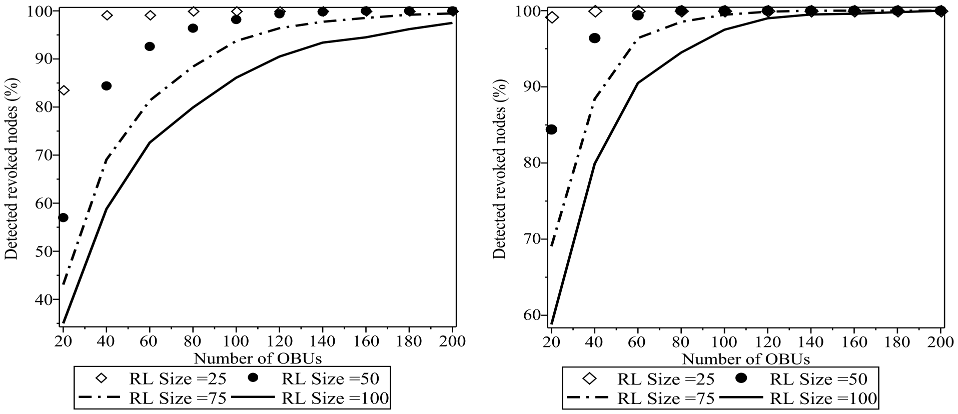
generation and delivery. Note that we do not need any public key certificate in our scheme. Table 5.2 gives a comparison of signature overheads from other VANET message-authentication approaches.

5.4.5 Identity Dispute and Revocation

On an identity dispute, CA may use the tainted vehicle's type-id and generate signatures using each individual secret s_i with the same type-id. If the alleged signature is a valid one, as well as the time and area information are accurate, it would match with one of the generated signatures by CA. Secret credentials of the matched signature are used for identifying the tainted OBU.

When CA revokes an entity (say, OBU_i), it appends the corresponding secret s_i to the revocation list and sends an update to all suspected traffic locations through RSUs. Using the revoked s_i, an OBU can internally derive a new signature on each received message. If a received signature matches the derived one, verifying OBU identifies the sender as a revoked entity, and alerts the neighborhood.

Instead of checking through the complete revocation list, a random checking



(a) $\alpha = 2$

(b) $\alpha = 4$

Figure 5.4: Randomizing the revocation process among OBUs for different RL sizes.

Table 5.3: EDCA Parameters used in CCH (values taken from [1]).

ACI	AC	CWmin	CWmax	AIFSN
3	voice	3	7	2
2	video	3	7	3
0	best effort	7	15	6
1	background	15	511	9

policy would enable an OBU or RSU randomly verify α number of entries from the revocation list. Figure 5.4 indicates the proportion of the detected revoked OBUs for different sizes of revocation lists. Revoked OBUs in a VANET have higher chances of being detected if the revocation list is smaller. Also, a higher α value ensures the detection of revoked entities by comparatively less number of users. Intuitively, the more the neighboring OBUs are, the greater the proportion of revoked nodes spotted in a VANET.

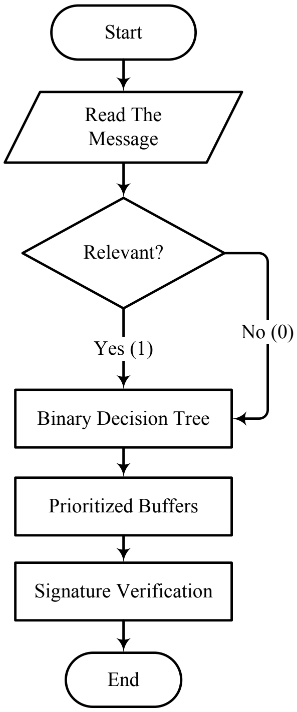


Figure 5.5: Block diagram of our verification scheme.

5.5 Priority-based Verification of VANET Messages

5.5.1 The Framework

Since vehicles in close proximity have similar safety features and attributes in their periodic messages, a portion of all received messages at a particular time would give a fair idea about the contemporary traffic condition in a VANET. In this scheme, an OBU prioritizes all received messages based on the relevance of some important physical attributes of a vehicle along with their EDCA classes.

A general framework of our scheme is given in Figure 5.5. We consider three different pieces of primary safety information: position, acceleration and speed to be extracted from all received messages. Received information is fed into the corresponding Bloom Filters of the receiving entity. Individual Bloom Filters are deployed in each verifier entity in order to keep record of the most recent traffic safety updates. A primary overview of Bloom Filters is illustrated in [87].

An OBU periodically updates its own road-safety attributes (e.g., location, acceleration, and speed) into the corresponding Bloom Filters. Recent entries of road-safety information of the vehicle remain in the Bloom Filter's bit array until the Bloom Filter is reset.

Each Bloom Filter individually checks the corresponding part of the received payload, and compares it against the existing entries within the bit array. A perfect binary decision tree [88] as given in Figure 5.6 assigns each received message with a relevance score. The relevance score is determined based on the received message's similarity to the recent history of periodic safety information of the receiving entity.

Relevance Score from the Binary Tree

The root of the tree represents a received message *m*, while the other subsequent parent nodes indicate the responses from the associated Bloom Filters at each level. Every tree level corresponds to an individual attribute of a safety message.

Up on reception, a periodic safety message's data payload is passed to the designated Bloom Filters where each filter checks for the specific part of the safety information. If a newly received message component *with an acceptable tolerance* [89] matches an existing entry (i.e. any recent entry of the vehicle itself) in the corresponding Bloom Filter, it returns a 1. Otherwise, it returns a 0.

At each level of the binary decision tree, a left child of a parent node represents

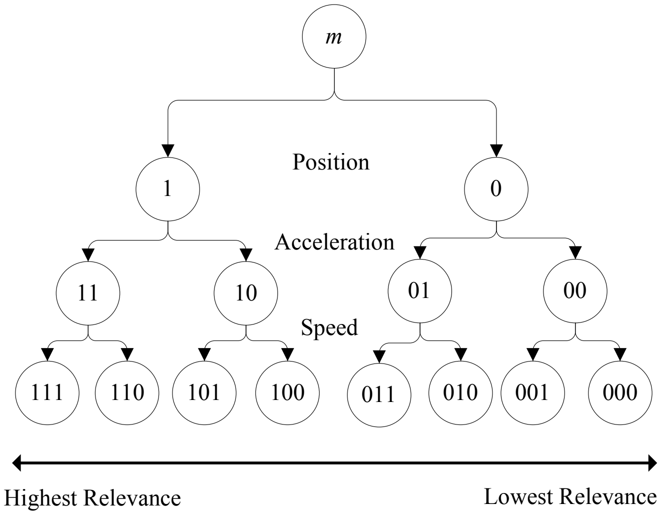


Figure 5.6: Binary decision tree for relevance scores.

the corresponding relevance of safety information, and is given a value 1. On the other hand, a right child of a parent node indicates the non-relevance of an associated safety attribute, and is assigned with a value 0. Assigned binary values from parent nodes are passed to the corresponding child nodes to determine the relevance score by concatenating the bits in order. Each received message in a receiving VANET entity is tagged with a relevance score defined by the leaves of the decision tree.

Messages tagged at the left most leaf are the most relevant ones (with relevance score 7) as the relevance score of the tagged messages tend to get lower as we move along from left to right at the bottom of the tree.

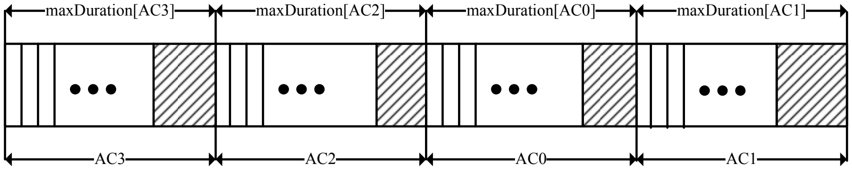


Figure 5.7: Prioritized scheduling of message verification. Shaded area represents unused time-slots in a buffer.

Prioritized Buffering of Messages

As shown in Figure 5.7, an OBU temporarily stores all received messages into four buffers according to their EDCA access categories. Each buffer contains corresponding access category messages arranged in the decreasing order of their relevance scores. The size of a buffer is determined by the maximum number of messages that can be verified within the time frame called $maxDuration[AC_\gamma]$ (for $\gamma = 0..3$). The verification probability (p_{v_γ}), and the time frame $maxDuration[AC_\gamma]$ of a particular access category are proportional to the successful delivery ratio of the corresponding AC_γ messages.

Verifications of buffered messages are done in a round robin fashion over the message buffers in order of their priorities. The length of the round robin cycle should be shorter (say, 100 ms) than the maximum buffering time (say, 300ms) of un-authenticated messages.

If the total number of received safety messages in a round robin cycle exceeds the receiver's verification capacity, highest priority messages from across the prioritized buffers would be verified in each cycle.

5.5.2 Cross-layered Approach to Verification

VANET periodic safety messages use broadcast communications over the IEEE 1609.4 [1] MAC protocol which incorporates EDCA mechanism for prioritizing among the four traffic classes.

Back-off Time and Verification Probability

The WAVE EDCA mechanism ensures that a packet with the higher priority access class gets the preference to a packet from a lower priority access class during the transmission. Thus, lower access category packets in a VANET experience a higher packet drop rate than that of the higher access category packets. Packets drop in VANET communications due to the EDCA priorities of MAC-layer transmissions, and the traffic intensity within the access class.

Apparently, the probability of successful packet delivery on a particular access category could be used as the basis of determining the verification probability of received messages. However, since broadcast messages are not acknowledged in EDCA, neither a sender nor a receiver of a message is aware of the collision leading to a packet drop event in the medium. Therefore, successful packet delivery ratio can not be used by a WAVE device to estimate the verification probability of received messages.

Nevertheless, the required back-off time for transmitting a packet also depends on: a) the MAC priority, and b) congestion within the traffic class just like a packet drop event in VANET. Hence, an alternative measure could be to use the back-off time of a message transmission to determine the verification probability of the prioritized buffers.

The correlation between the drop probability and the back-off time for a single message transmission over a particular access category is given as:

$$Corr(p_{d_\gamma}, BK_\gamma) = \frac{cov(p_{d_\gamma}, BK_\gamma)}{var(p_{d_\gamma}).var(BK_\gamma)}, \tag{5.10}$$

for $\gamma = 0..3$, where the covariance $cov(p_{d_\gamma}, BK_\gamma) = \mathbf{E}(p_{d_\gamma} \times BK_\gamma) - \mathbf{E}(p_{d_\gamma}) \times \mathbf{E}(BK_\gamma)$, and $var(p_{d_\gamma})$, $var(BK_\gamma)$ are the variances of the drop probability p_{d_γ} and average back-off time for a message transmission BK_γ respectively. We further discuss the packet drop probability and back-off time in Section 5.6.

We use the back-off time for a packet transmission in order to derive the verification probability of a particular access class in VANET.

$$p_{v_\gamma} = \left(1 - \frac{BK_\gamma^\omega}{\sum_{z=0}^{3} BK_z^\omega}\right) \times \frac{1}{\delta - 1}, \tag{5.11}$$

where BK_γ is the average back-off time for a message delivery over AC_γ, δ is the number of ACs in use by OBUs in VANET, ω is a scaling factor which provides a weight value to the verification probability of an individual access category.

An OBU can estimate its average back-off delay for all access categories while transmitting different priority data frames. If an OBU does not have any data to transmit from a particular access category, it can still measure the back-off time by transmitting a zero payload probing packet over the specific access class. Authentication primitives for the probing packet are not required as it would be ignored by all nodes upon reception.

Adaptive Scheduling of Message Buffers for Verification

When a buffer for a particular access category messages is fully or partially empty, the verifier application chronologically verifies the buffered messages (if there is any) before switching to the next buffer. Unused verification time from each individual buffer is distributed among all the access classes following the ratio of their successful message delivery. The maxDuration[AC_γ] (where γ = 0..3) values are updated at the end of the verification of each access category buffer. This ensures the fairness in distribution of the unused time among the buffered messages. Algorithm 1 illustrates the procedure of scheduling the message buffers for prioritized verification of received messages.

Bloom Filter Stabilizing

Frequent updates from the neighboring vehicles would contribute to the rapid growth of the number of elements in a Bloom Filter's bit array, affecting the performance of the filter with false positive errors since the size of a Bloom Filter is constant. A large size Bloom Filter may resolve the problem to some extent, but it aggravates the false positive rate for some of the elements in the bit array [90].

A *stable* Bloom Filter [91] stores only the most recent elements in the bit array with the requirement of extra spaces to save the history for each element of the bit array. Since there is no way to separate the most recent elements from the old ones in an ordinary Bloom Filter, we must clear the *aged* Bloom Filter, and re-load it with fresh elements at a regular interval in order to restrict the error probability to a fixed level.

Algorithm 1 Adaptive scheduling of message verification.

```
DEFINE AC {AC3,AC2,AC0,AC1}
while (TRUE) do
  AC ← AC3;
  bufferCount ← 4;
  while (bufferCount>0) do
    bufferCount−−;
    if (buffer[AC]! =null)AND(elapsedTime[AC]<maxDuration[AC]) then
      VERIFY messages from the beginning of buffer[AC];
    else if (buffer[AC]==null) then
      $excessTime[AC] \leftarrow maxDuration[AC] - elapsedTime[AC]$;
      for $index$ = 0 to 3 do
        $maxDuration[AC_{index}] \leftarrow maxDuration[AC_{index}] + \frac{p_{v_{index}} \times excessTime[AC]}{\sum_{z=0}^{3} p_{v_z}}$;
      end for
      AC ← NEXT AC;
    else if (elapsedTime[AC]>=maxDuration[AC]) then
      AC ← NEXT AC;
    end if
  end while
end while
```

In a traffic scenario of N vehicles in the communication range of a verifier entity, let us assume that the refresh interval of a Bloom Filter is I seconds, and the periodic transmission rate is f messages per second. Then, elements inserted into each Bloom Filter before resetting is computed as, $n_{bf} = N \times I \times f$.

The relationship between the total number of elements n_{bf}, and the Bloom Filter size M for an optimal use with a predefined error probability of P_{error} is given as, $n_{bf} \approx M \times \frac{(ln\,2)^2}{|ln\,P_{error}|}$ [90].

Combining these two above relationships, we get:

$$I \approx \frac{M}{N \times f} \times \frac{(ln\,2)^2}{|ln\,P_{error}|}. \tag{5.12}$$

Therefore, the refresh interval of a Bloom Filter depends on the number of total data entries, as well as the error probability of the corresponding Bloom Filter.

5.5.3 Mitigating Vulnerabilities

Our approach allows safety message authentication according to the relevance score of received messages in the individual access category. Received messages from closer OBUs get higher verification opportunity than others and messages from distant OBUs are less likely to be chosen for the verification. Since a message with higher relevance score is relatively close, and hence, more important to the verifier, an attacker would be spotted easily by the verifying entity.

5.6 Performance Evaluation

5.6.1 Network Simulation Setup

We consider a simple urban vehicular traffic scenario in a $1500m \times 100m$ bidirectional road with 2 lanes in each direction. Vehicles' speed vary following a

Gausian distribution with mean of 60 km/hr and standard deviation of 5 km/hr. An RSU is installed at the roadside, while different number of OBUs are mounted with moving vehicles on road. We allow the RSU and OBUs to broadcast a WSMP packet every 100 ms for simulating OBU's basic safety messages and RSU's periodic service announcements, respectively. RSU transmits its periodic messages over the highest access category AC3, while equal number of OBUs broadcast their periodic safety messages over each access category.

Times of the initial message broadcast for individual OBUs and the RSU have been selected from a uniform distribution over 100 ms period. We run each experiment for 90 seconds following a 10 seconds warm up period. Each experiment has been conducted 10 times using different seeds, while individual results are averaged for the final outcome.

We implemented the EDCA mechanism over IEEE Std 802.11p MAC and PHY provided by ns-2.34's IEEE 802.11Ext package given in [82]. EDCA parameters as shown in Table 5.3 have been configured for four access categories. We assume that each VANET entity operates only on the control channel (CCH) with a specific priority class. Other MAC and PHY parameters used in our simulation are listed in Table 5.4. Payloads for the ordinary WSM broadcast is set to 254 Bytes as indicated in the WAVE Standard (see C.6 of [5]). Since our authentication scheme does not require any third-party certificates, the payload size in our scheme is reduced to 128 Bytes.

Table 5.4: Simulation Parameters for MAC and PHY.

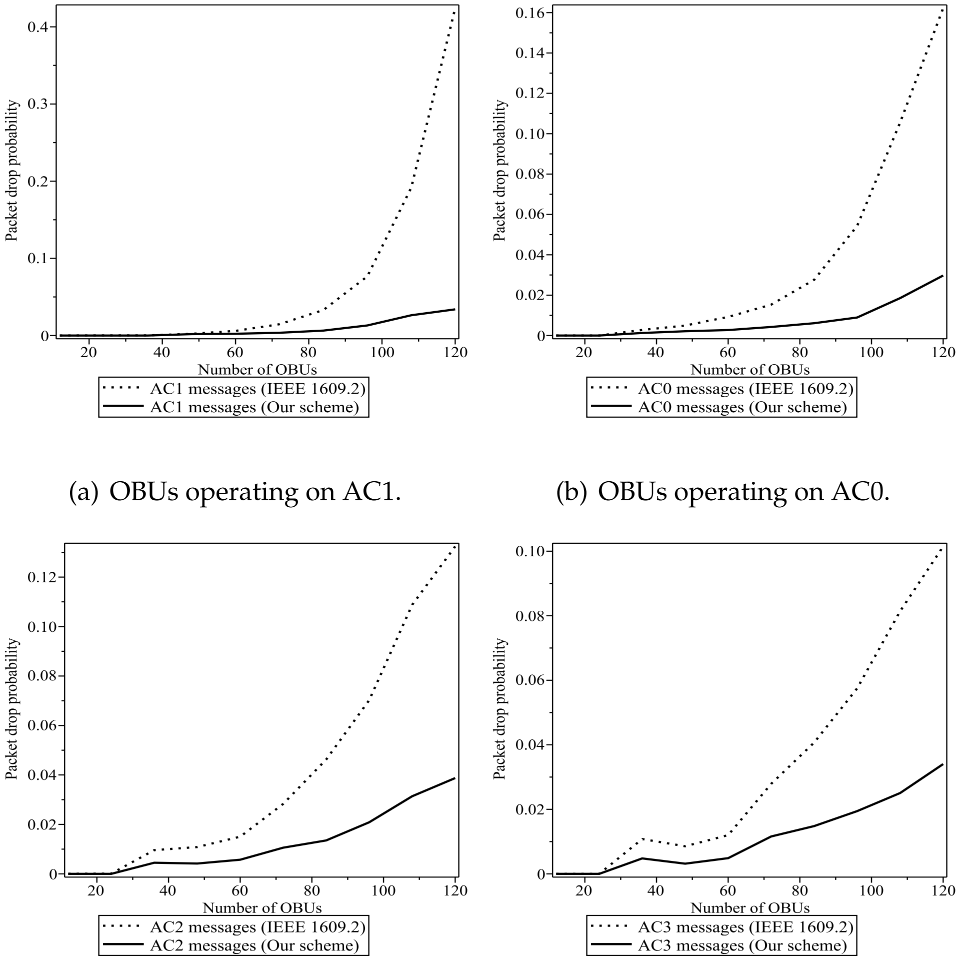
Parameters	Values
Radio Range	500m
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

5.6.2 Packet Drop Probability and Back-off Delay

Packet delivery in a wireless network is impaired due to the excessive offered load, and inherent noise of the medium. Figure 5.8 illustrates the affect of different access categories on OBUs' periodic transmissions in terms of the probability of failed delivery of broadcast messages. The probability of packet drop climbs as the number of OBUs increases. Exclusion of the trusted third-party certificate with each OBU message implies reduced payload size in our authentication scheme, which results in a lower packet drop rate compared to the IEEE Std 1609.2-based authentication in VANETs.

Unlike an OBU's periodic transmission, an RSU includes a trusted third-party certificate with every individual broadcast. However, this inclusion does not significantly affect the vehicular communications as the number of OBU messages is much higher than that of RSU's.

Figure 5.9 presents the average back-off period measured for each individual transmission using IEEE Std 1609.2-based authentication and our approach respectively. The back-off time in EDCA depends on the AIFSN value, as well as the CW size of the corresponding access category. Therefore, higher access class messages have low back-off time, and vice versa. Our authentication scheme is lighter than the conventional ECDSA scheme used in IEEE Std 1609.2, and hence, incurs reduced back-off delay compared to the ECDSA-based approach. This would accelerate the message authentication process in a high-speed road-traffic condition of VANET.



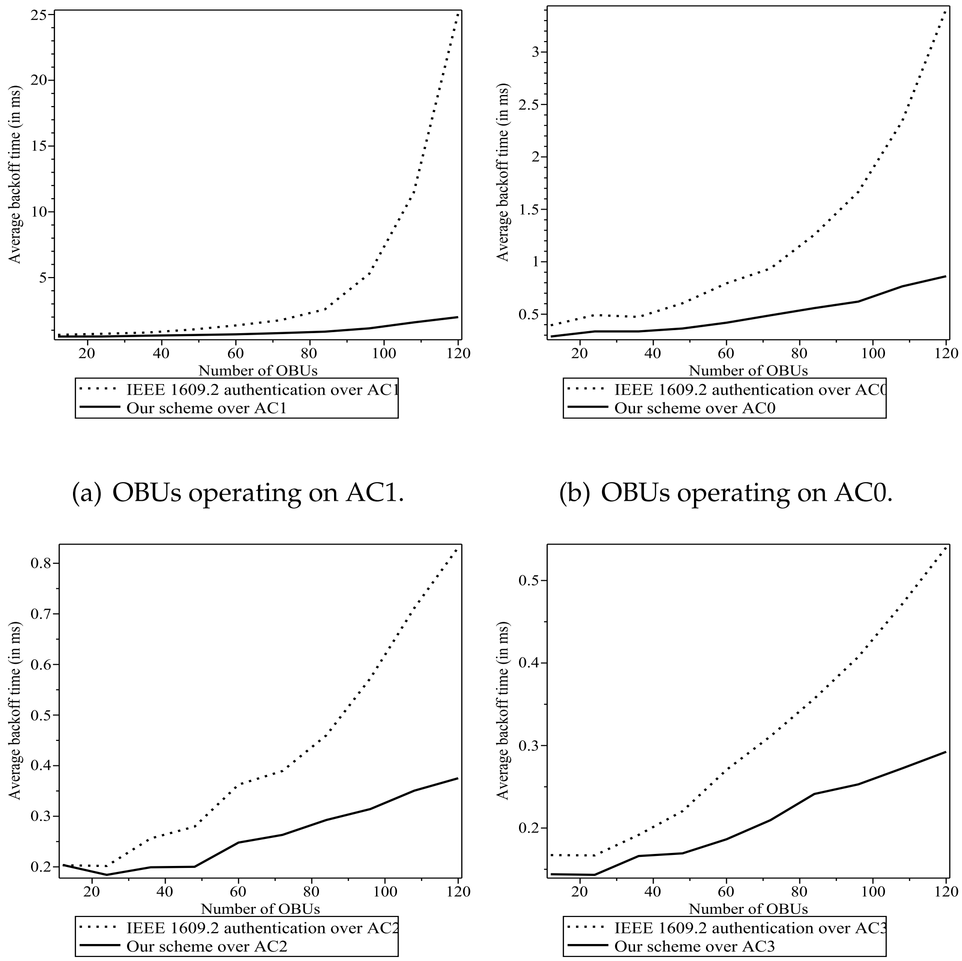
(a) OBUs operating on AC1.

(b) OBUs operating on AC0.

(c) OBUs operating on AC2.

(d) OBUs operating on AC3.

Figure 5.8: Drop probability of periodic safety messages for OBUs over different access categories.



(a) OBUs operating on AC1.

(b) OBUs operating on AC0.

(c) OBUs operating on AC2.

(d) OBUs operating on AC3.

Figure 5.9: Average backoff delay in periodic transmissions for different access categories.

5.6.3 Prioritized Verification Probability

Table 5.5 shows strong correlations (over 95%) between the message drop probability (Figure 5.8) and the average back-off time to transmit a message (Figure 5.9) for each access category with IEEE Std 1609.2- and our authentication scheme. This would allow an OBU to utilize its average back-off time as the basis of determining the verification priority of a particular access class using Equation (5.11). The verification probabilities of received messages for different access categories are presented in Figure 5.10. The verification probability of each access class is determined according to the Equation 5.11. For any number of OBUs in a VANET with different access classes, cumulative message verification probability is always 1.

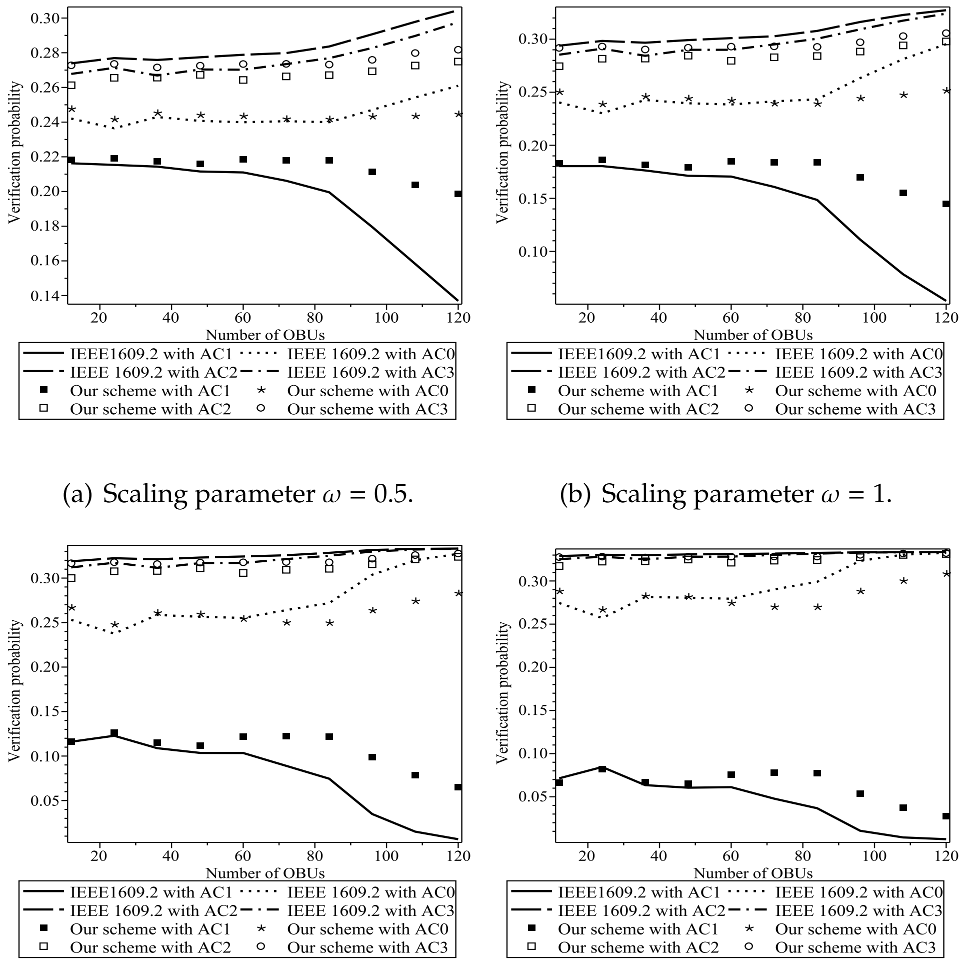
Table 5.5: Correlation between drop probability of OBU messages and the average backoff period for different access categories.

	Access Categories			
Approaches	AC1	AC0	AC2	AC3
IEEE 1609.2	0.9998	0.9918	0.9908	0.9835
Our scheme	0.9961	0.9501	0.9659	0.9767

When traffic load is increasing, verification probabilities for lower priority traffic classes (AC1 and AC0) diverge significantly due to their larger contention windows and AIFSN values compared to the higher priority access classes (AC3 and AC2). This is because back-off times for all access classes are increasing at different rates. For instance, traffic classes with lower priorities have higher increase of back-off time which leads to decrease of their message verification probability as shown in the Equation (5.11). Therefore, under high traffic-load message verification probability of access classes AC3 and AC2 will increase on behalf of access classes AC0 and AC1. Since high offered load takes place in a VANET due to the rush hour traffic or a consequence of an accident, this scheme allows verification of the most important messages in such critical condition.

Our signature scheme allows a user to have shorter traffic-safety messages compared to the conventional IEEE Std 1609.2-based authentication. Shorter messages allow smaller back-off pause times during the transmission and therefore verification probabilities of different access categories are less diverging for our scheme than that of the standard approach.

A larger ω value emphasizes more on high priority ACs, while a smaller value of ω reduces the differences among verification probabilities of the access classes.



(a) Scaling parameter $\omega = 0.5$.

(b) Scaling parameter $\omega = 1$.

(c) Scaling parameter $\omega = 2$.

(d) Scaling parameter $\omega = 3$.

Figure 5.10: Verification probability of individual access category messages with different values of scaling parameter.

5.6.4 Refresh Interval

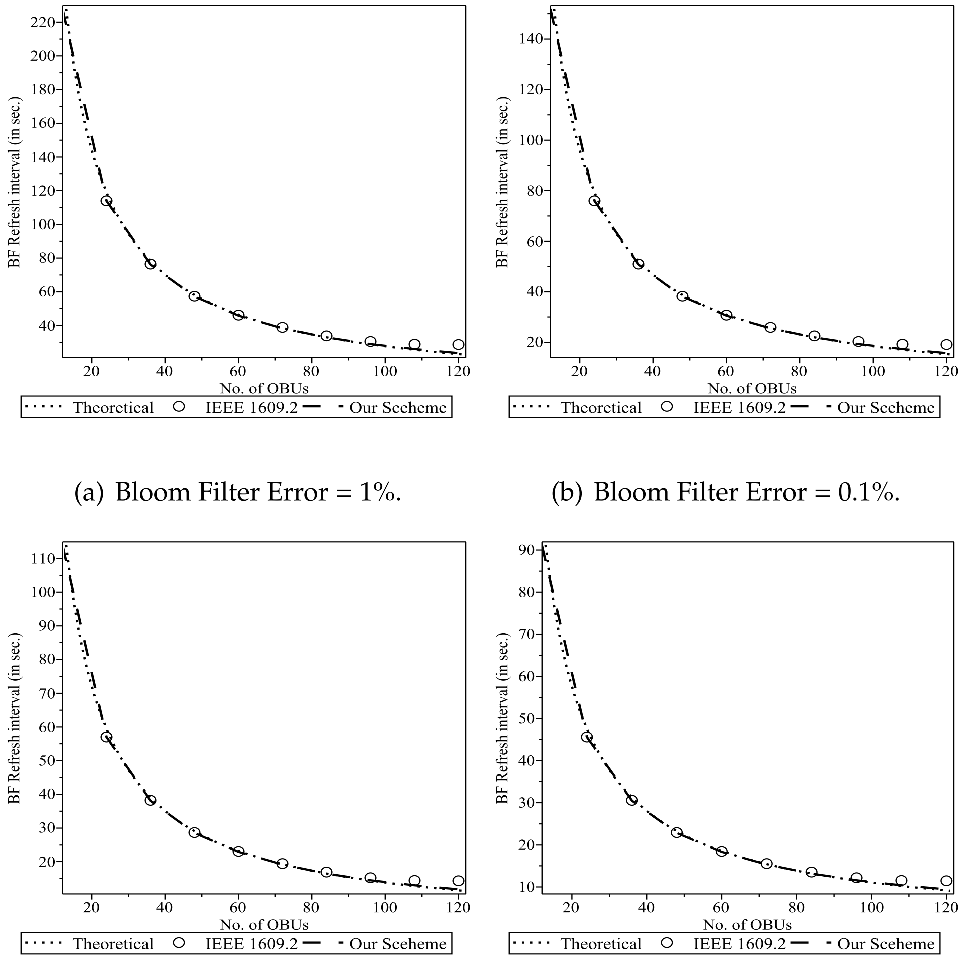
The refresh interval of a Bloom Filter depends on the number of input data elements (received messages in our case), the size of the filter M, and the error probability P_{error} as given in Equation 5.12. We choose $M = 32KB$ for our Bloom Filters with P_{error} = 1%, 0.1%, 0.01%, and 0.001% for each experiment.

Utilizing the total number of successfully transmitted messages from simulations, we determine the refresh interval of the Bloom Filter for OBUs. Figure 5.11 presents the Bloom Filter's refresh interval for different error probabilities. Since a Bloom Filter does not store any message payload, the interval values do not depend on the underlying authentication scheme, but on the chosen error probability of the Bloom Filter.

Since a user can not precisely determine the number of neighboring OBUs during an intense traffic condition (due to potential packet loss in broadcast communications), a Bloom Filter should be pre-configured with a fixed value of its refresh interval. The interval must be less than or equal to the minimum refresh interval for the highest number of neighboring OBUs the Bloom Filter is designed for.

5.7 Summary

We designed an identity-based anonymous user-authentication scheme and a cross-layer verification approach for WAVE-enabled VANET's safety messages. A variation of the conventional ECDSA approach is used with the identity-based



(a) Bloom Filter Error = 1%.

(b) Bloom Filter Error = 0.1%.

(c) Bloom Filter Error = 0.01%.

(d) Bloom Filter Error = 0.001%.

Figure 5.11: Refresh interval of a Bloom Filter for different combination of RSU and OBU access categories.

signature approach where the common geographical area information of signing vehicles is taken as the signer's identity. This exempts a vehicle from the inclusion of a trusted third-party certificate with each broadcast message in a VANET, while a user is still identifiable by the trusted third-party upon an identity dispute. A cross-layer message verification scheme verifies received messages based on their MAC traffic classes and sender information relevance. This ensures that under the rush hour congestion or after a traffic accident, most important messages will not be missed by the verifier. Security analysis and performance evaluation justify our authentication and verification approach for WAVE-enabled vehicular communications.

The following chapter incorporates a potential application scenario which combines our secure and anonymous authentication schemes presented in Chapter 4 and Chapter 5 respectively.

Chapter 6

WAVE-based Parking Assistance with Security and User Anonymity

6.1 Introduction

Wireless Access in Vehicular Environment (WAVE) is turning out to be an intriguing avenue of research and innovation with traffic-safety and other user-friendly applications that assist the driver of a vehicle, providing a better traffic atmosphere for safe and efficient driving. The primary intention of a Vehicular Ad hoc Network (VANET) is to reduce the number of traffic accidents caused due to potential driver errors on roads and highways. However, typical features of vehicular communications can be extended to provide unconventional user-applications like parking assistance for WAVE-enabled vehicles.

According to the WAVE standards, the DSRC (Dedicated Short Range Communications) enables WAVE devices to communicate with each other within the communication range. Also, each entity in a VANET broadcasts a periodic safety message (every 100-300ms) where the information about the vehicle's current location, speed, and road-conditions are disseminated. These two forms of communications in VANET can be used as the basis of an efficient parking system for an automated parking facility.

Authentication of VANET entities demands fast and realtime signature generation and verification schemes, while pre-authorization of users is not feasible due to the following limitations.

i. High-speed vehicles come across a particular OBU or a VANET infrastructure for a very short period of time.

ii. Chance of having a previously seen vehicle in an RSU's communication range is significantly low. A commuter may go by the same RSU everyday, but pre-authentication would expose his identity to the RSU.

Intuitively, a privacy-preserving parking assistance application would require two-way communications between an RSU and a vehicle's on-board unit (OBU). The corresponding RSU must inform the vehicles about the current status of the parking facility, while an OBU should be able to ask for a reservation of a parking spot in the parking facility. Potential risks involved with VANETs have to be addressed with mutual authentication, confidentiality, and confirmation of message integrity. The scheme should protect the network from all known security attacks in order to be trusted by a VANET user. Moreover, the actual identity of a user should be recoverable by a high administrative authority in case of any dispute.

Thus, our WAVE-based parking assistance application should provide conditional user-anonymity to users of the service.

Lu et al. [92] proposed a scheme for intelligent parking of vehicles using the spatiotemporal properties of available parking space and VANET mobility. While the scheme addressed some fundamental security and privacy requirements of a VANET, the approach is basically dependant on bilinear-pairing based signature and verification techniques [59] with some strong assumptions like: i. considering radio-signal strength based measurements to be precise and reliable, and ii. the use of tamper-proof devices in a VANET. Although RSUs are installed at roadside locations without much physical protection and surveillance, they have been assumed non-compromisable in Lu et al.'s work.

A bilinear-pairing approach is expensive in terms of time and computation complexity, and in most cases, it is very difficult to generate the appropriate combination of parameters for pairing-based approaches as the most typical and frequently made assumptions are not feasible in practice [76].

We use our ID-based authentication mechanisms over Elliptic Curve Digital Signature Algorithm (ECDSA [36]) to provide message authentication and user anonymity in a parking facility. As we have seen in previous chapters, our ID-based authentication schemes do not depend on trusted third-party certificates to provide source authentication; instead, they use the current time and geographical position of an entity to validate a received VANET message.

We organize the rest of the chapter in the following fashion. The overview of the proposed system and related assumptions are listed in Section 6.2. Section 6.3

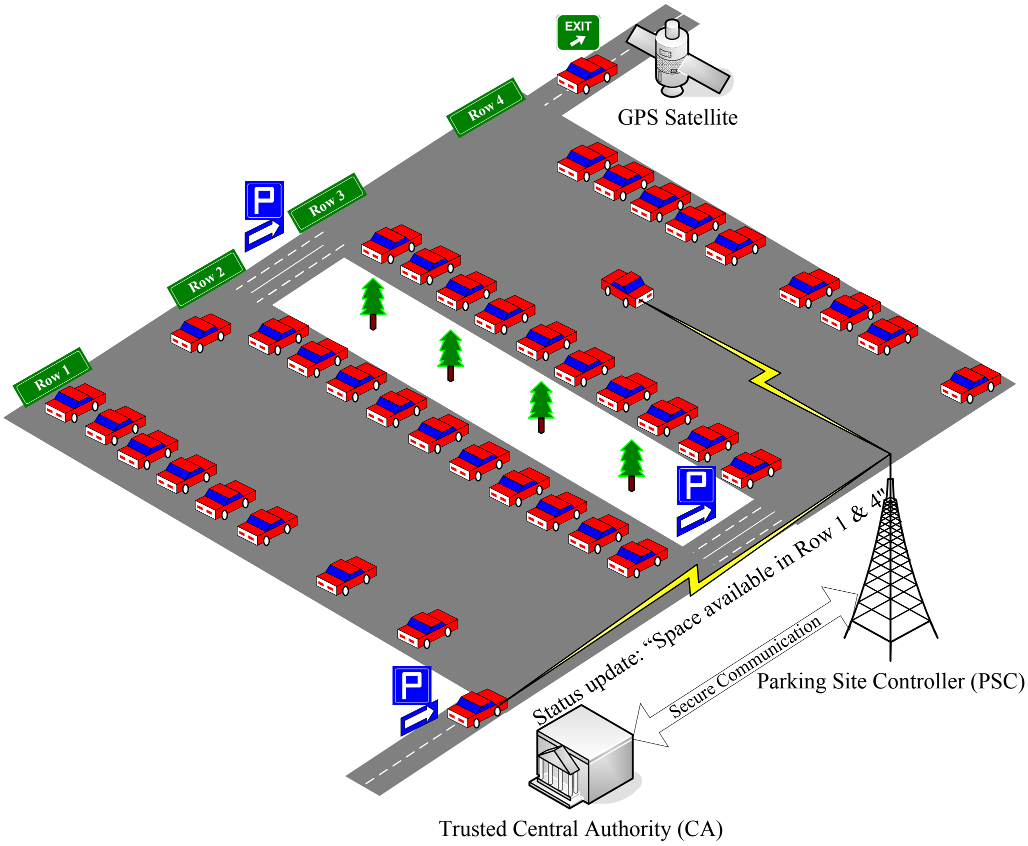

EXIT
GPS Satellite
Row 4
Row 3
Row 2
Row 1
Status update: "Space available in Row 1 & 4"
Secure Communication
Parking Site Controller (PSC)
Trusted Central Authority (CA)

Figure 6.1: System model for our proposed WAVE-enabled parking facility.

illustrates our WAVE-enabled parking assistance scheme in details. Security and anonymity issues are analyzed in Section 6.4, while Section 6.5 describes the performance evaluation of our approach through network simulation. Section 6.6 contains the summary and concluding remarks of our work.

6.2 System Design

We took into account the fundamental security and privacy aspects during the design process of our secure parking assistance scheme which provides user-data

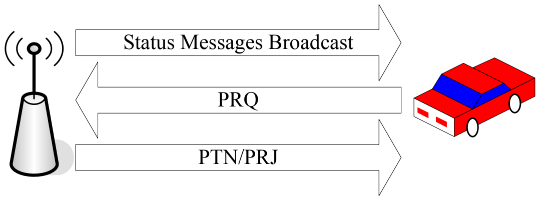


Figure 6.2: System overview of WAVE-enabled parking facility.

confidentiality, message integrity, and message authentication with conditional user-anonymity.

Our system design includes a global trusted central authority (CA), a parking site RSU called *parking site controller* (PSC), and a secure higher layer communication between the CA and the PSC. We assume that all the vehicles are equipped with global positioning systems (GPS) so that their OBUs are aware of their corresponding geographical positions. Figure 6.1 illustrates our proposed model for a WAVE-enabled car parking facility.

When in operation, a PSC disseminates periodic service status messages which include the current status of the corresponding parking facility. A recipient OBU would accept or reject a periodic message following a signature verification process.

In addition to the periodic transmission of safety messages that contain the vehicle's speed, location, and road-safety information, an OBU nearby a parking facility may request for a parking space by sending a *parking reservation request* (PRQ) to the PSC. Upon successful reception of a PRQ, PSC stores a copy of it, and if a parking space is available, it would grant a *parking token* (PTN) to the requesting OBU. A parking token is an approval of the request made by the vehicle, which can be used during the admission and toll collection process in the parking facility with some suitable applications.

A parked vehicle's OBU periodically updates its parking status by sending PRQs to the PSC on a regular interval. PSC acknowledges the OBU's update by sending a fresh PTN each time it receives the periodic update from an OBU.

If there is no parking space available, PSC notifies the requesting vehicle with a *parking rejection* (PRJ) message which may also contain information of the nearest available parking lot, or an estimated waiting time for a probable parking spot allocation. Figure 6.2 outlines the communications needed by the proposed parking assistance scheme.

6.3 Proposed Scheme

We deploy two authentication schemes to sign periodic safety and other application messages for infrastructure-to-vehicle and vehicle-to-infrastructure message authentications. Table 6.1 lists the notations used in the rest of our work.

6.3.1 Geographical Tolerance

Upon receiving a message m, a receiving entity compares its own location (obtained from GPS) with the origin of message m taking into account the tolerance value a_m specified in the message.

Let, the current GPS position data of an OBU includes l-bits long x_{gps} and y_{gps} for latitude and longitude respectively. The validation of geographical scope is done at an RSU/OBU in the following manner:

Table 6.1: Notations.

Component	Description
CA	a trusted central authority
Q	master public key
q	a large random prime number
x	system's master secret, $1 < x < q$
G	base point on the elliptic curve $E(\mathbb{F}_p)$
k_o	random secret associated to the CA
k_p, k_c	session parameters
k_i, k_g	random secrets $< q$
R_o	original signer credential
R_i	credential for RSU_i
R_g	vehicle type identifier
$H(.)$	hash function $H(.) : \{0,1\}^* \to \mathbb{Z}_q^*$
loc_z	GPS position information of entity z
m	a message to be signed and delivered
a_m	geographical tolerance
t	current system time (rounded up)
t_m	message m's expiry information

i. Take $l - a_m$ most significant bits from both x_{gps} and y_{gps}, and represent them as x'_{gps} and y'_{gps}.

ii. Return (x'_{gps}, y'_{gps}) as the new location information.

iii. Verify m if $l - a_m$ most significant bits of the receiver's current position match (x'_{gps}, y'_{gps}).

6.3.2 Parking Assistance With Security and User Anonymity

In our system, periodic status messages from PSC are to disseminate the public information about parking availability, tariff rates for parking, and environmental changes. On the other hand, parking request (PRQ), parking token (PTN), and parking rejection (PRJ) messages are solely associated to a specific user of the

Algorithm 2 Location-based I2V Message Authentication using ECDSA

```
I. Key Initialization Module (at CA): Initialized with public parameters $\{q, G, ID_o, loc_i\}$, and secret parameters $\{x, k_o, k_i\}$. Following computations take place:
    $Q = xG$
    $R_o = k_oG$
    for $i = 1 \rightarrow n$ do
        $R_i = k_iG$
    end for
II. Application Message Generator (at CA):
    Generates status message $m$, expiry time $t_m$, and geographical tolerance $a_m$.
III. Key Generator (at CA):
    $h_{i,m} = H(loc_i, ID_o, m, t_m, a_m)$
    $s_{i,m} = (k_i + h_{i,m}x)k_o^{-1} mod\, q$
    $(s_{i,m}, m, t_m, a_m)$ to $PSC_i$.
IV. Preprocessing (at $PSC_i$ and $OBU_j$):
    $k_p = H(loc_{i,or j}, t)$
    $(x_p, y_p) = k_pR_o\ mod\ q$
V. Signature Generation (at $PSC_i$): $PSC_i$ computes the following signature equation.
    $s_{p,i,m} = k_p^{-1}(H(m) + s_{i,m}x_p) mod\, q$
    Signature $(s_{p,i,m}, R_i)$, and $(m, t_m, a_m)$ are transmitted to the OBUs.
VI. Verification (at $OBU_j$): An $OBU_j$ computes:
    $h_{j,m} = H(loc_j, ID_o, m, t_m, a_m)$
    if $(x_p, y_p) = (H(m)R_o + x_p(R_i + h_{j,m}Q))s_{p,i,m}^{-1} mod\, q$ then
        Accept $m$
    else
        REJECT
    end if
```

Algorithm 3 Location-based Anonymous Authentication Scheme using ECDSA

```
I. Key Initialization Module (at CA): Initialized with public parameters $\{q, G\}$, and secret parameters $\{x, k_g\}$.
    $Q = xG$
    $R_g = k_g G = k_{g+1} G = k_{g+2} G = ...$
    $s_g = (1 + xH(R_g)k_g^{-1}) mod\ q$
    $s_{ug} = s_g \oplus Password$

II. Pre-processing (both at signer and verifier):
    $k_c = H(loc_c, t)$
    $(x_c, y_c) = k_c R_g\ mod\ q$

III. Signature Generation (at signer): A signer $g$ computes the following equations.
    $s_g = s_{ug} \oplus Password$
    $s_{c,g} = k_c^{-1}(H(m) + s_g x_c) mod\ q$
    Signature $(s_{c,g}, R_g)$, and $m$ are delivered.

IV. Verification (at recipient):
    if $(x_c, y_c) = (H(m)R_g + x_c(R_g + H(R_g)Q))s_{c,g}^{-1} mod\ q$ then
        Accept $m$
    else
        REJECT
    end if
```

VANET. This implies that data secrecy in VANET is mandatory in user-specific messages, while message authentication is required in periodic broadcasts.

Signed WAVE Short Message Protocol (WSMP) [6] is used for constructing a parking status message whose payload is generated by the CA before delivered to the PSC. The message is signed and periodically transmitted by the PSC using the mechanism stated in Algorithm 2. Along with the parking availability information, a periodic status message also contains PSC's ephemeral public key v in the WSM's application data field.

We use our identity-based [59] proxy signature [49, 50] technique over ECDSA for the authentication of infrastructure originated messages in VANET [89]. The authentication scheme is summarized in Algorithm 2. The location information of the PSC in a parking facility is used as the location-identity for the signer. CA generates a status message m, produces a delegation proxy key $s_{i,m}$ associated to the message m and PSC_i using the generated message, expiry information (t_m) and the geographical tolerance (a_m). CA then securely delivers the key along with other credentials to the proxy signer PSC_i which would sign and deliver the message on behalf of the CA. The mechanism also allows a recipient OBU to verify the received signature using its own GPS location, and other received credentials. Inclusion of geographical tolerance (a_m) in the message payload allows a PSC to have its control over the scope of the periodic advertisement for parking service within the communication range of the PSC. The detailed description of the signature scheme is illustrated in Chapter 4.

Anonymity in a VANET is vital since a user would not like to be traced by the messages s/he sends and receives over the vehicular communication. Unlike, parking service status messages, a vehicle's periodic broadcasts are anonymous, which are created and signed by the OBU. The anonymous authentication scheme has been described in Chapter 5 and summarized here in Algorithm 3. The signing key (s_g) of an OBU is derived from a random secret (k_g) at the CA (Step I of Algorithm 3). The signature generation (and verification) mechanism uses current time and GPS data of the vehicle to compute the session parameters for a signature as indicated by Step II of Algorithm 3. A receiving entity can verify received messages, but can not identify the sender. However, the CA can identify a signing vehicle by reproducing the signature using the associated random secret and other credentials upon any road-traffic dispute. Therefore, our authentication mechanism provides conditional anonymity in vehicle-to-infrastructure communications.

We do not need to include third-party certificates with signed messages as we are deploying identity-based signature technique in Algorithms 2 and 3. Nonetheless, we must include the message expiry information (t_m), and the geographical tolerance (a_m) to the WSM payload from PSC. The geographical tolerance values of OBU-originated messages are pre-determined and fixed for a given vehicular network. Hence, OBUs in our parking authentication scheme do not need to include an explicit a_m value with their message payloads. Generated signatures using our schemes are unforgeable, verifiable, distinguishable, and undeniable as indicated in Chapter 4 and 5.

In a VANET-enabled parking facility, a user would not like to publicly disclose the contents of application messages that are sent or received by an OBU. Therefore, the payloads of parking messages must be ciphered by random symmetric keys, while the symmetric keys are encrypted with individual recipient's public keys.

A PRQ from a requesting vehicle is designed to contain an encrypted message. The encryption is done using OBU's random symmetric key δ. The key δ is encrypted by PSC's temporary public key v, and included in the PRQ. Note that PSC's periodic status messages contain the current version of its public key (v) within the message payload. An OBU includes a temporary public key β with the PRQ message payload. The private key α of the key-pair is kept within the OBU.

$$OBU \rightarrow PSC : \underbrace{\{E_\delta(message\ payload), E_v(\delta)\}}_{\text{PRQ}}$$

$$PSC \rightarrow OBU : \underbrace{\{E_\gamma(message\ payload), E_\beta(\gamma)\}}_{\text{PTN/PRJ}}$$

A parking token (PTN), or a parking rejection (PRJ) message is produced by the corresponding PSC to notify the requesting OBU about the acceptance or rejection of the request respectively. These messages are encrypted by PSC with a random session key γ. Again, the session key γ is encrypted by recipient OBU's temporary public key β. These notifications are valid for a pre-specified time period. Specially, parking tokens expire and become unusable after the specific time duration.

6.3.3 Signature Overhead

For a 160-bit elliptic curve, the size of an ECDSA signature is 40 bytes. In case of our identity-based periodic message signature (from Algorithm 2), we need to include the expiry time t_m, as well as the geographical tolerance a_m. Assuming 2

Table 6.2: Signature Overheads Of Proposed Scheme.

	Used Elliptic Curve		
Approach	160-bit EC	P-224	P-256
Ordinary ECDSA	166 Bytes	182 Bytes	190 Bytes
Algorithm 2	44 Bytes	60 Bytes	68 Bytes
Algorithm 3	40 Bytes	56 Bytes	64 Bytes

bytes of space requirement for each of them, the total size of the signature overhead for periodic status message yields 44 bytes. The other signatures (from Algorithm 3) do not include t_m and a_m, and hence will have only 40 bytes of signature overhead. Using two different types of NIST [81] curves: P-224 and P-256 as suggested by the current security standard for WAVE [5], would have signature overhead of 56 bytes, and 64 bytes respectively including an additional overhead for the third-party certificate (126 bytes). Table 6.2 summarizes the signature overheads of our proposed secure parking assistance scheme. P-256 is usually chosen for signing third-party certificates, whereas P-224 is commonly used for safety and other application messages.

6.4 Security Analysis

Following malicious behaviors and challenges are among the most anticipated ones in our secure parking assistance scheme.

Signature Forging

For deriving a valid proxy key $s_{i,m}$, the CA requires the system secret x, hash value $h_{i,m}$ over the corresponding identity credentials loc_i, ID_o, and two other random numbers k_i, k_o as indicated in Algorithm 2. The secret x is irreversible from the knowledge of the public key Q as the derivation involves point multiplication operations of an elliptic curve $E(\mathbb{F}_p)$. The corresponding identity credentials assure the time and location based identification of the entities, which must not be changed by the PSC as those credentials would be used by the verifier OBUs during the verification of the proxy signature. Therefore, different values of the signature credentials would result in a message rejection.

Also, generation of a signature by an OBU_g involves the delegation key s_g. As given in Algorithm 3, delegation secret s_i is computed by the CA using the system secret x, and individual secret k_g. Thus, forging a signature would require an attacker to have at least two secrets (x, and k_g) which are stored only in the CA. Again, associated difficulty in solving an elliptic curve discrete logarithm problem would not allow an attacker to retrieve the system secret x from the knowledge of public key Q. Hence, forging a signature in this approach would be extremely hard.

Replaying Old/Expired Messages

Any change or modification on message content m, or expiry information t_m would result in a different proxy key $s_{i,m}$ for which the generated signature in Algorithm 2 would be different. This ensures that a false message or a replay attack with this approach will not be successful.

A signing OBU computes the session parameter x_c from k_c using Algorithm 3. This k_c is derived by hashing the message-originator's position and timestamp which would be same as the receiving node's current position and time assuming that both the signer and the verifier are in close proximity. Therefore, replaying an old and expired signed message would not pass the verification process at the receiver OBU/RSU.

Message Tunneling

In addition to the current timestamp, CA uses the PSC's pre-authorized geographical position in order to derive session parameters of the signatures. This prevents an adversary to bypass the signed message for using in a different location. When a parking status message is delivered in a different location (say, a different parking spot), the verification will fail due to the different location (and time) of the verifier OBU.

Non-repudiation

An adversary in our parking assistance application is unable to forge a signature originated from OBU or PSC. An expired message from an OBU or a PSC would contain different a timestamp (t_m or t) than the timestamp used by the verifier, and hence, the old message would not pass the verification process. Since the location information is embedded with each signature, it would be rejected by a verifier at a different location. As a result, once a message is signed and delivered, the sender OBU can not deny the signature for the sent message.

Node Compromise

An adversary may compromise an OBU to obtain the delegation secret (s_{ug}), and use it later on for signing PRQ messages to the PSC so that the user of the compromised vehicle is charged for parking instead of the attacker. However, the signature generation of OBU requires the corresponding user-password without which the delegated secret s_g can not be obtained (refer to step III of Algorithm 3). Hence, an OBU compromise in our scheme would not let an adversary find either the delegation secret s_g, or the system secret x.

Signature Linking

An OBU may sign identical payloads in subsequent time-frames. A timestamp-based session parameter x_c during the signature preprocessing phase ensures the change of signatures in different time frames even if the message contents resemble to the previously sent messages.

Data Confidentiality

An adversary would not be able to launch a data spoofing, or a man in the middle attack over the communication between an OBU and the PSC. Message payloads for parking requests and PSC responses are encrypted by session keys (i.e. δ and γ respectively), while the session keys are sent in encrypted form using the temporary public key of the recipient. The public key-private key pair of a VANET entity is changed frequently, and kept within the corresponding device's memory. Therefore, an adversary would not be able to read the message contents of a PRQ, or PTN/PRJ message.

6.4.1 Identity Dispute and Revocation

In case of any dispute in the parking facility that requires the actual identity of an OBU, CA may generate all possible signatures using each individual secret s_g with the corresponding R_g value. If the alleged signature is valid with appropriate timestamp and position information, it would resemble to one of the generated signatures. Secret credentials like k_g, s_g of the matched signature will then be used for identifying the disputed user.

When CA revokes an entity (say, OBU_g), it appends the corresponding secret s_g to the revocation list and sends an update to *PSC*. Using the disclosed s_g, PSC can internally derive the PRQ that would be similar to the parking request originated from the revoked OBU. If a received signed message matches the derived one, PSC identifies the sender as a revoked entity.

6.5 Network Simulation

We develop a simulation program to investigate the network performance of our scheme using network simulator ns-2.34 with IEEE 802.11p parameters for MAC and PHY provided by IEEE 802.11Ext package from Chen et al. [82].

A small roadside parking facility of 200 m length and 100 m width has been considered where vehicles unicast periodic parking updates/requests (PRQs) to the PSC, as well as broadcast the regular periodic safety messages. PSC at the parking lot responds to each vehicle's update request with individual response (PTN/PRJ). While an OBU disseminates periodic safety messages every 100 ms (10 messages per sec.), the interval for parking message updates has been set to 300ms.

The simulator is configured for two major types of data traffic: i. periodic broadcasts by OBUs and the PSC for safety messages and parking updates respectively, and ii. parking request/responds messages from OBUs and RSU respectively. Application messages (i.e. PRQ and PTN/PRJ) are associated to a higher priority access class (AC2, or AC3), whereas periodic broadcasts of OBUs and PSC are of less importance, and associated to one of the lower priority traffic classes (either AC0, or AC1) over DSRC control channel (CCH) at IEEE 802.11p MAC. Other MAC and PHY parameters used in our simulation are listed in Table 6.3.

IEEE 802.11p MAC allows four distinguished priority classes for best effort, background, video, and voice data traffic. The latter two categories are given higher priorities over the first two traffic classes as the related EDCA parameters for IEEE 802.11p control channel (CCH) are listed in Table 6.4.

We choose the signed WSMP format (see C.6 of [5]) for the used payload size and signature overhead of broadcast communications, while a *signed and encrypted* message format has been adapted for a unicast operation. The signed original message would be an input to the encryption process, where the *content type* field would be equal to "*signed*". Since the PSC will communicate with every OBU individually for exchanging PRQ and PTN/PRJ messages, the *recipients* field of the encrypted message will have the security credentials for only one entity at a time. Thus, the total length of the signed encrypted message in our scheme would be

213 octets - 73 octets = 140 octets (bytes). Credentials v, c and t in the encrypted message format stand for the temporary public key of the recipient, symmetric encrypted session key, and the authentication tag respectively.

Details of the used message payloads for different broadcast and unicast communications are given in Table 6.5.

Figure 6.3(a)–6.3(d) describe the network performance in terms of successful message delivery for different combination of access categories used in our simulation.

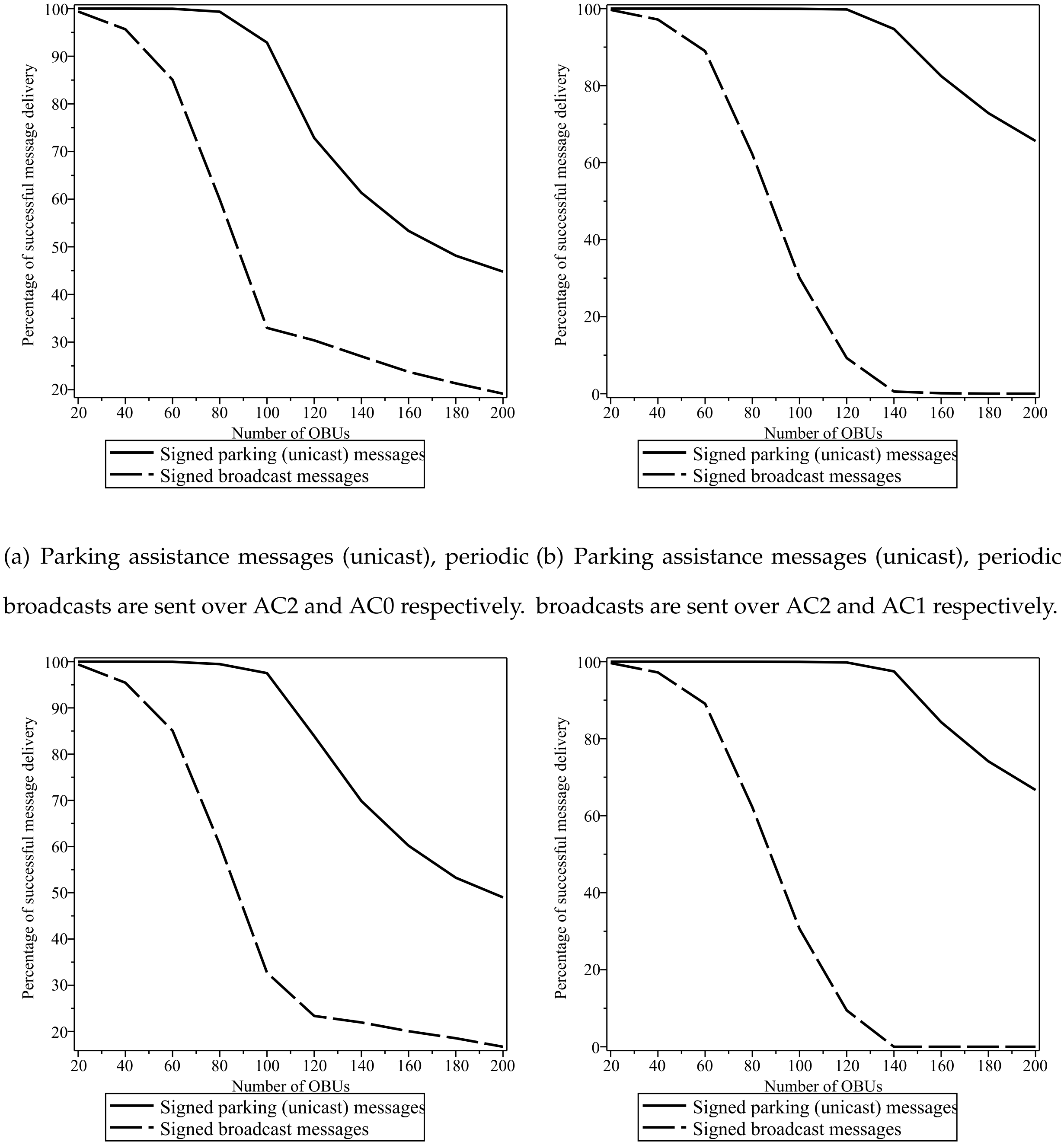
Table 6.3: Simulation Parameters for MAC and PHY.

Parameters	Values
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Short Retry Limit	7
Long Retry Limit	4
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

Table 6.4: EDCA Parameters for IEEE 802.11p CCH (values taken from [1]).

Priorities	Type	CWMin	CWMax	AIFSN
AC1	Background	15	511	9
AC0	Best effort	7	15	6
AC2	Video	3	7	3
AC3	Voice	3	7	2

As shown in Figures 6.3(a)–6.3(d), parking status messages have greater success ratio than that of VANET's periodic safety message broadcasts. The lower offered load, as well as the association with higher priority traffic classes (AC2 or AC3) for the authenticated parking status updates ensured the higher success in delivering



(a) Parking assistance messages (unicast), periodic broadcasts are sent over AC2 and AC0 respectively.

(b) Parking assistance messages (unicast), periodic broadcasts are sent over AC2 and AC1 respectively.

(c) Parking assistance messages (unicast), periodic broadcasts are sent over AC3 and AC0 respectively.

(d) Parking assistance messages (unicast), periodic broadcasts are sent over AC3 and AC1 respectively.

Figure 6.3: Percentage of successful message delivery in a prioritized WAVE-enabled parking facility.

Table 6.5: Used payloads for different communication types.

Communication Type	WAVE Security	Our scheme
PSC Status Updates	254 Bytes	132 Bytes
OBU Safety Messages	254 Bytes	128 Bytes
Parking Request (PRQ)	140 Bytes	140 Bytes
PSC Response (PTN/PRJ)	140 Bytes	140 Bytes

secured unicast parking assistance messages.

Figure 6.3(a) illustrates the scenario where periodic safety messages and parking updates are associated with AC0 and AC2 respectively. Signed parking assistance messages using our ID-based signature scheme allows secure parking message exchange between PSC and OBU with 97% successful message delivery for up to 80 OBUs in the parking facility.

Percentages of successful message delivery in periodic safety message broadcasts over access class AC1 and parking status message updates over AC2 are shown in Figure 6.3(b). The significant difference of the corresponding contention window (CW) sizes, as well as the Arbitration Inter-Frame Space Number (AIFSN [4], refer to the Table 6.4) values between AC1 and AC2 access classes enable the unicast parking updates with higher success in message delivery. Our scheme allows above 99% successful delivery of messages for as many as 120 vehicles in the WAVE-enabled parking facility.

In a scenario where periodic broadcasts are sent over AC0, whereas unicast parking status updates are delivered using AC3, our scheme allows around 97% successful parking status message delivery for up to 100 vehicles in the communication range of the PSC as indicated in Figure 6.3(c).

Due to the significant relative difference of CW and AIFSN values between AC1 and AC3 (refer to the Table 6.4), the parking status messages assigned with AC3 perform with greater success rate compared to the low priority (AC1) periodic safety messages' delivery ratio. As shown in Figure 6.3(d), for up to 140 OBUs in the parking lot, the success ratio of our scheme is about 97%.

Obviously, parking status updates need to be assigned with higher priority traffic classes than that of the VANET's periodic safety messages in order to achieve high degree of successful message delivery in a parking assistance application. In our experiments, we have shown that our scheme can provide over 97% successful message delivery for 140 vehicles in a parking site. Since the saturation condition of the network depends on the offered load as well as the size of the back-off contention window (CW), the successful parking message delivery can be improved for higher number of vehicles in the network by choosing smaller contention window, and/or by selecting smaller AIFSN value for the associated higher traffic class assigned to the parking status messages. However, a small contention window in the back-off process may cause synchronization of periodic messages, and more packet drops as shown in the following chapter.

6.6 Summary

A WAVE-enabled system for secure and privacy-preserving car parking assistance has been presented in this chapter. This work relies on two modified ECDSA authentication mechanisms for infrastructure-to-vehicles and vehicles-to-infrastructure message communications. The development of signature schemes for providing message authentication, integrity, and anonymity is in harmony with the current WAVE security services which makes our approach compatible with the existing VANET standards. We investigated our scheme in the light of all known malicious attacks and scenarios, while it is proved that a successful attack is reasonably hard to launch on our proposed system. Simulation results provide the network performance of the scheme suggesting a high priority access class for infrastructure-to-vehicle, as well as a low priority access class for vehicle-to-infrastructure communications.

So far we have addressed different aspects of vehicular message authentication and user-privacy in VANETs. In the following chapter, we introduce a potential distributed denial of service (DDoS) attack that can be launched by exploiting the underlying weaknesses of WAVE's EDCA mechanism and the periodicity of transmission in VANETs.

Chapter 7

DDoS Attack on WAVE-enabled VANETs Through Synchronization

7.1 Introduction

Authentication and data integrity problems like identity/signature forging, repudiation, exculpability, and Sybil attacks are among the top VANET security issues addressed in recent years [18, 31, 35, 92, 93, 94]. However, denial of service (DoS) attack on vehicular communications has not received much attention, although such attacks have been commonly addressed in other ad hoc networks [95, 96, 97, 98].

VANET providers offer several different applications and services to the users through RSUs which can deliver road-safety information to the on-road vehicles. An RSU in a VANET serves as a gateway to the Internet backbone, several different road-safety applications and other services from the VANET providers. For example, an RSU may transmit periodic status for a parking assistance application [99] or traffic signal violation warning to the OBUs [23]. It can also broadcast traffic safety messages like 'maximum curve turning speed' or 'construction ahead' notifications to the vehicles in its communication range [100].

Presence of a long-term service or application is announced either in the context of a persistent WAVE Basic Service Set (WBSS [1]) using WAVE Service Announcements (WSA) on the control channel (CCH) at a regular interval, or through periodic WAVE Short Messages (WSMs [6]). A high-speed vehicle (OBU) may exchange information with neighboring entities by joining the nearest RSU's WBSS. Also, a PSOBU (Public Safety OBU, installed in an emergency vehicle) may either form a persistent WBSS, or deliver periodic WSMs for transmitting its emergency public safety messages.

In a VANET, malicious entities might launch a denial of service (DoS) attack by overwhelming the communication channel so that crucial messages do not reach their destinations. The intention of such an attack is to disable the whole network by continuously or selectively jamming the important transmissions. Since VANET is a real time communication system, consequences of losing regular transmissions could be fatal.

A straightforward attack of this kind might be launched by a malicious node that would simply synchronize to the corresponding provider's transmission schedule, and broadcast false messages at the exact same time as the service announcement (which are delivered in a periodic fashion). Multiple attackers may focus on the same transmission, with increased chance of success. Simultaneous frames would eventually collide making a legitimate user unaware of the real messages with potentially disastrous consequences. Worse yet, the device that sent the real message would never know that the transmission was lost since a receiver does not admit the reception of a broadcast by sending acknowledgements.

In this chapter, we analyze mathematically and through simulations a synchronization based distributed denial of service (DDoS) attack on a VANET by a small group of attackers. Also, we present different mitigation techniques to thwart the aforementioned DDoS attack in VANETs. Our solutions require modification of MAC-layer's Contention Window (CW) size and/or randomization of the provider's message inter-arrival time for broadcasting the periodic beacons.

We organize the rest of the chapter as follows. DSRC and EDCA mechanism of IEEE 802.11p MAC are explored in Section 7.2. Our attack model is presented in Section 7.3. Configuration of the network simulator has been described in Section 7.4. Prevention methods to the synchronization-based DDoS attack in VANETs have been discussed in Section 7.5, while concluding remarks are posted in Section 7.6.

7.2 Preliminaries

IEEE's Dedicated Short Range Communications or DSRC (IEEE 802.11p) [4] operates on a 75 MHz radio spectrum dedicated to a control channel (CCH), and 6 service channels (SCHs) in the range of 5.8/5.9 GHz.

A WAVE device in a VANET switches between the CCH and at least one of the SCHs as it is mandatory for a device to monitor the CCH on a regular interval. CCH is used for transmitting short, system control, and safety application messages, while the SCH is usually used for conducting ordinary data communications. Since WAVE entities are mostly assumed as single channel devices, they are essentially time synchronized using Coordinated Universal Time (UTC)—commonly provided by Global Positioning System (GPS).

Access over each channel can be controlled using four access categories AC_k, $k = 0..3$ as shown in Table 7.1. Priority of AC_k is regulated with two channel access parameters, namely the Arbitration Inter-Frame Space ($AIFS_k$), and Contention Window (CW_k). Unlike a unicast operation, WAVE broadcast using AC_k uses only $CWmin_k$ value to construct the back-off period.

When the medium is idle, before transmitting a data frame, a station waits for $AIFS_k = SIFS + AIFSN_k \times t_{slot}$, where t_{slot} is the duration of one time slot ($t_{slot} = 16\mu sec.$), and $AIFSN_k$ is determined by the priority class k.

If the medium becomes busy during $AIFS_k$ period, the sender needs to wait for the end of busy period. As soon as the medium becomes idle, the sender restarts the $AIFS_k$ waiting process before being able to perform any action.

When there is a frame to broadcast, the sender selects a random number between 0 and CWmin and counts down after every time slot while medium is idle. If the medium becomes busy, the station has to wait again for $AIFS_k$ before being able to decrement the backoff counter. The sender can broadcast the packet only when the back-off counter reaches the value of 0,

Hence, IEEE 802.11p's EDCA mechanism at the MAC-layer randomizes the time interval between two periodic announcements on a specific channel. WAVE's EDCA mechanism not only prioritizes among the transmitted messages, but also

Table 7.1: EDCA Parameters used in CCH(values taken from [1]).

ACI	AC	CWmin	CWmax	AIFSN
3	voice	3	7	2
2	video	3	7	3
0	best effort	7	15	6
1	background	15	511	9

reduces the chance of an external collision.

Broadcast communication in WAVE has no retransmission feature, meaning that the choice of CW_k values for a particular AC_k is limited. Therefore, due to the small CWmin of WAVE EDCA as shown in Table 7.1, an attacker operating on the same AC_k can successfully synchronize to the RSU's periodic broadcasts with a high probability. The greater the access category of an RSU is, the easier it is for attackers to launch the attack.

7.3 Attack Model

Our attack model consists of varying number of attackers which have the typical features of regular WAVE devices. An RSU broadcasts periodic frames either via Wireless Short Message Protocol (WSMP) on CCH, or transmits WAVE announcements at a regular interval for some service advertisement. The attackers attempt to synchronize to the RSU's periodic transmissions and transmit frames to collide with RSU's frames. In order to launch a successful attack, attackers need to achieve two kinds of synchronization. The first one is called *jitter estimation* with respect to start of back-off slot, and the second one is related to the duration of a back-off period.

Jitter Estimation: In order to synchronize to the RSU's periodic broadcasts, an attacker must first estimate the slot boundary. This can be accomplished by the following function of jitter estimation which takes into account multiple physical parameters of the attackers and the RSU.

$$jitter = f(t_{prop}, v_a, c_p, f_p), \tag{7.1}$$

where t_{prop} is the propagation delay, v_a is the ground speed of an attacker (attackers could be stationary too), c_p is the clock precision indicator of an attacker with the corresponding RSU, and f_p is the fading between an attacker and RSU. An attacker can compute the RSU's subsequent broadcast times by simply adding on the known interval period to the estimated delivery time.

Since several different physical parameters contribute to the jitter between slot boundaries of the RSU and an attacker, the probability of an attacker starting to broadcast within the same slot time as the RSU can be determined by approximating the jitter using normal distribution with zero mean, and standard deviation of half of unit back-off slot time $t_{slot}/2$= 8μsec. i.e.

$$pr = \int_{-t_{slot}/2}^{t_{slot}/2} \frac{1}{\sqrt{2\pi(\frac{t_{slot}}{2})^2}} e^{\frac{-x^2}{2(\frac{t_{slot}}{2})^2}} dx. \tag{7.2}$$

Estimation of Back-off Period: A successful attack would require an attacker to have the same random CW_k size as RSU for a particular access category k.

Let us consider that there are n attackers in a VANET trying to launch a DDoS attack by synchronizing to the RSU's periodic broadcasts. The probability of having

r attackers with the same CW_k as RSU is given as:

$$p_{cw}(r,k) = \binom{n}{r}(\frac{1}{CW_k})^r(1-\frac{1}{CW_k})^{n-r}, \tag{7.3}$$

where CW_k is the size of the random contention window for an access category k.

Similarly, the probability of having l attackers that transmit within the same slot period as the RSU is:

$$p_{slot}(r,l) = \binom{r}{l}(pr)^l(1-pr)^{r-l}, \tag{7.4}$$

where r is the number of attackers having same random CW_k as RSU on class k.

Hence, the probability of a DDoS attack by n attackers is computed as:

$$P_{DDoS_k} = \sum_{r=1}^{n} p_{cw}(r,k) \sum_{l=1}^{r} p_{slot}(r,l). \tag{7.5}$$

From the equations above and the earlier discussions in Section 7.2, we can claim that a successful synchronization to RSU's periodic broadcast mostly depends on the length of the CW_k of the RSU and the attackers when both parties are operating on the same AC_k. Since an RSU and DDoS attackers in a VANET would transmit packets on the same access category AC_k, corresponding $AIFS_k$ value does not affect the P_{DDoS_k}.

7.4 Simulation Setup

We developed a simulation program to investigate the synchronization based DDoS attack in VANET using the network simulator ns-2.34.

We assume a simple urban vehicular traffic scenario in a $900m \times 100m$ bidirectional road with 2 lanes in each direction. Individual vehicle's speed varies following a Gausian distribution with mean = 50 km/hr and standard deviation = 5 km/hr. We allow each OBU and the RSU to broadcast a WSMP packet every 100 ms for simulating OBU's basic safety messages and RSU's periodic service announcements, respectively.

A varying number of malicious attackers in the scenario pretend to be ordinary OBUs participate in a DDoS attack by synchronizing to the RSU's periodic broadcast schedule.

Times of the initial message broadcast for individual OBUs and the RSU have been chosen from a uniform distribution over 100 ms period. However, each attacker chooses the attack delay time to be the sum of the uniformly distributed random back-off period and normally distributed jitter with mean value 0 and standard deviation of half of the unit back-off slot time (i.e. 8μsec).

We run the simulation for 30 seconds following a 10 seconds warmup period. Each experiment is run 10 times using different seeds, and individual results are averaged for the final outcome.

We implement the EDCA mechanism over IEEE Std 802.11p MAC and PHY provided by ns-2.34's IEEE 802.11Ext package from Chen et al. [82]. We configure the EDCA parameters for individual access categories on the DSRC CCH. Other MAC and PHY parameters used in our simulation are listed in Table 7.2.

IEEE 1609.4 and 802.11p MAC access classes AC_k, $k = 0..3$ (with parameters listed in Table I) are mapped into best effort, background, video and voice classes respectively.

We assume that there are 100 OBUs including varying number of DDoS attackers

Table 7.2: Simulation Parameters for MAC and PHY.

Parameters	Values
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

in the VANET. Message payloads for the RSU, OBUs, and attackers are 254 Bytes long following the signed WAVE Short Message (WSM) protocol format (see C.6 of [5]). We plot the drop probability of RSU's periodic frames, using analytical values obtained from Equation (7.5) and simulation results obtained with the same

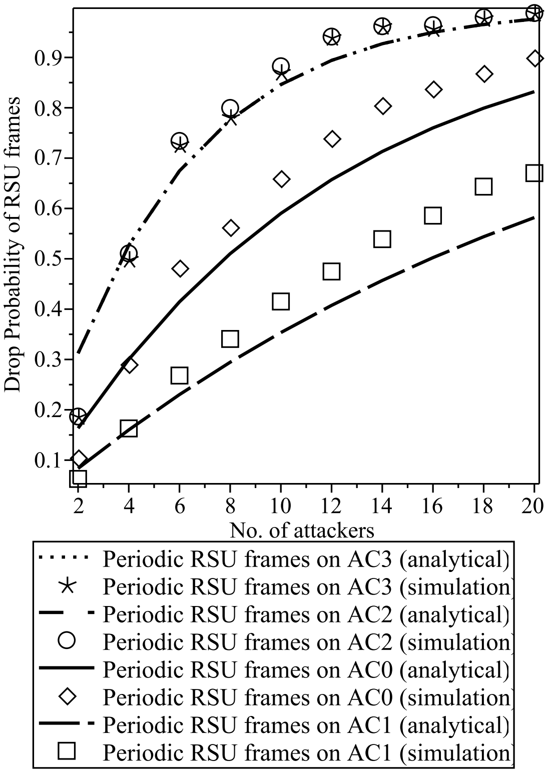


Figure 7.1: Probability of RSU's periodic message drop on a DDoS attack.

access categories and number of attackers. As shown in Figure 7.1, the drop probability of a periodic broadcast from the RSU increases with the number of simultaneous attackers. Since DDoS attackers use the same access category as an RSU, they would have the same AIFS value as RSU too. In general, lower priority access classes are more resilient than the higher priority ones for a synchronization-based DDoS attack due to their larger minimum contention window sizes. As AC3 and AC2 have the same minimum contention window of size 3, the corresponding curves are very close to each other.

7.5 Mitigating the DDoS Attack

We introduce the following techniques to thwart the synchronization-based DDoS attack in VANETs.

7.5.1 Randomizing the RSU Schedule

Since a WSM packet contains the time of its transmission, and periodic broadcasts allow delivery of frames at a regular interval, an attacker may successfully guess the timing of subsequent broadcast attempts from the knowledge of any of the previous delivery times. In order to mitigate this problem, a deliberate randomization of the delivery time can be applied during each cycle of periodic transmission.

An RSU can randomize the schedule of its periodic broadcasts following a normal distribution with original transmission time as the mean, and a predetermined delay as the standard deviation. The intention is to reduce the accuracy of an attacker's jitter estimate, and diminishing its ability to synchronize to an RSU's transmission.

Experiment 1: Using the simulator described in Section 7.4, we run an experiment with a VANET formed by 100 OBUs including varying number of DDoS attackers. RSU and OBUs periodically transmit 10 equal size frames every second, while attackers would be attempting to synchronize to the RSU's transmissions. We choose six different standard deviations for this experiment: unit slot time period (16μsec.), two slot period (32μsec), four slot period (64μsec.), five slot period (80μsec.), ten slot period (160μsec.), and fifteen slot period (240μsec.).

Assuming that all the WAVE devices are working in the same AC_k, we repeat the experiment for four priority classes.

Results of this experiment are shown in Figure 7.2. We also compare the results with the regular periodic broadcast scenario for the corresponding access categories. The changed RSU schedule achieves notable success in reducing the frame loss due to the synchronization-based DDoS attack. From the outcome of the experiment, we can also anticipate that this mitigation technique is effective mostly within the range of 4 to 5 slot times.

7.5.2 Increasing the Contention Window

As given in Equation (7.3), an attacker's estimation of back-off period depends on the CW_k for corresponding access category AC_k. Increasing the value of the CW_{min} would result in a smaller probability ($p_{cw}(r, k)$) of having the same contention window size as attackers.

Experiment 2: We keep the similar set up of Experiment 1, and run the simulation with larger minimum contention window (CW_{min}) for each of the VANET entities. We use the minimum contention window (CW_{min}) size 31 and 63 respectively to make a DDoS attack harder for DDoS attackers. We assign $AIFSN_k = 2$ in either case for our convenience.

Results are plotted in Figure 7.3. The drop probability of RSU's periodic broadcasts has been reduced significantly compared to the similar experiment with AC3 (Figure 7.1). Hence, the larger the contention windows are in a VANET, the more resilient it is against a synchronization-based DDoS attack.

However, incrementing CW size in a VANET would result in a longer back-off period during packet transmissions. We measure the average back-off delay for broadcasting a packet in a VANET with varying number of OBUs and different CW_{min} values. Transmission of a packet with larger CW_{min} incurs higher back-off delay than that of a transmission with smaller CW_{min} as shown in Figure 7.4.

7.5.3 Randomization with Increasing the Contention Window

We apply the techniques of Experiment 1 and 2 simultaneously to prevent the synchronization-based DDoS attack in VANETs.

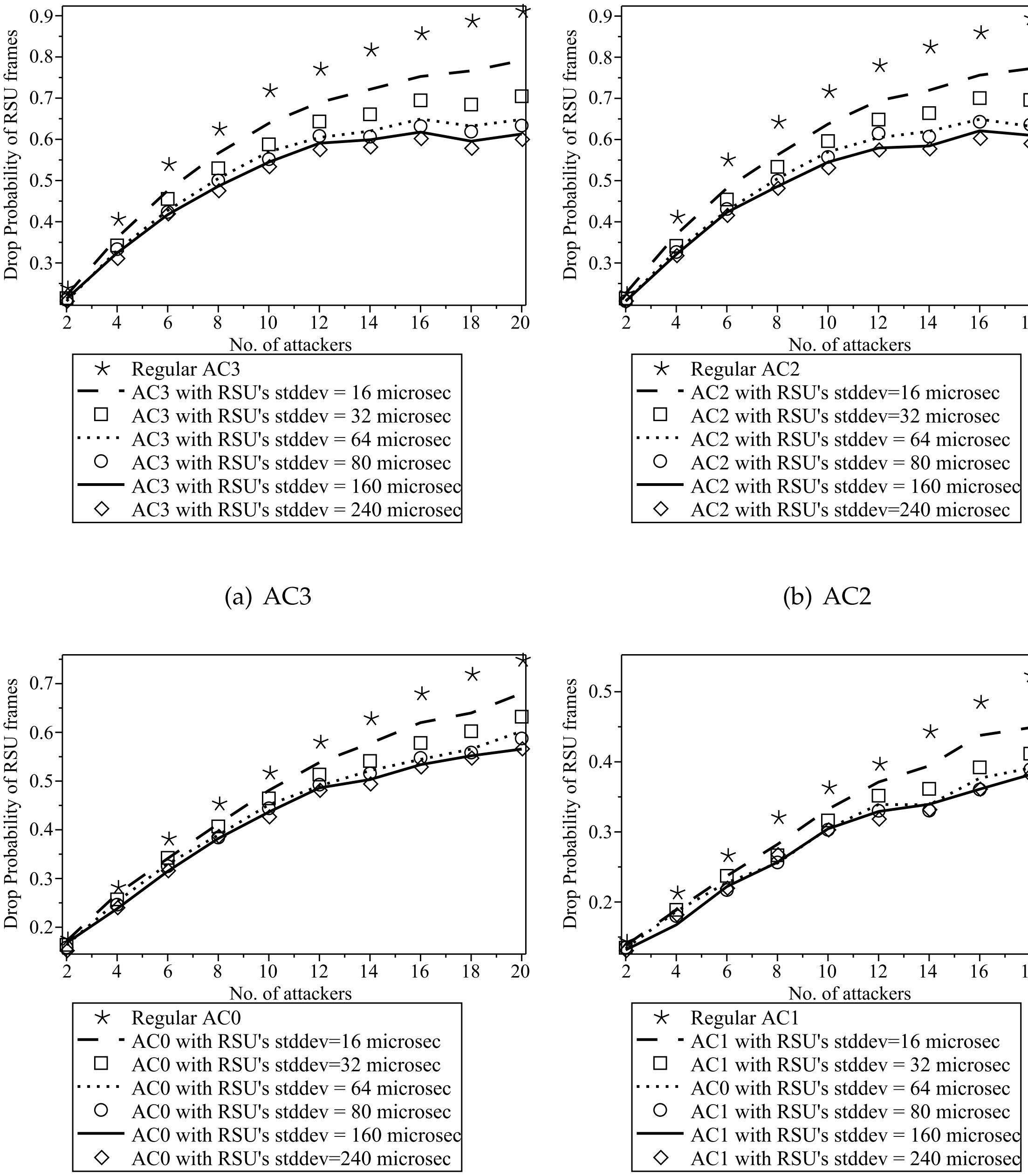
Experiment 3: We increase the contention window size of each VANET entity, and let the RSU randomize its interval for periodic transmissions following the same normal distribution as of Experiment 1 with different values of standard deviation.

Figure 7.5 shows the outcome of the experiment. The drop probability declines further for each combination of increased CW_{min} size and the standard deviation of the RSU's randomization of the periodic transmission.

Therefore, a synchronization-based DDoS attack in VANETs can be prevented by configuring RSUs and OBUs with large contention windows and/or randomizing the periodic events of an RSU.

7.6 Summary

In this chapter, we addressed a security weakness of VANETs where a group of malicious entities can launch a DDoS attack exploiting the IEEE 802.11p's EDCA vulnerabilities based on small contention window, lack of acknowledgements in broadcast communications, and periodicity of service beacons. An intelligent attacker can easily synchronize to any periodic transmission in the network. We analyzed the prospect of launching such an attack, and also suggested different mitigating techniques including larger EDCA parameters for VANET entities. Our attack model and the solutions have been well supported by mathematical analysis, as well as simulation results.



(a) AC3

(b) AC2

(c) AC0

(d) AC1

Figure 7.2: Experiment 1: Periodic message drop probability on a DDoS attack for different access categories and standard deviation values.

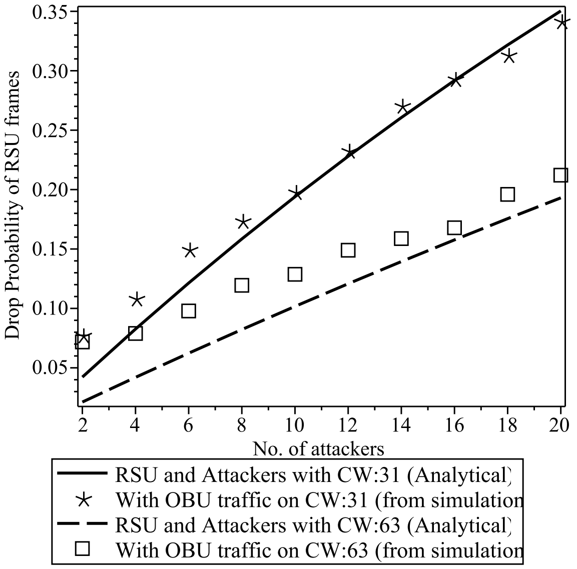


Figure 7.3: Experiment 2: Packet drop probability on DDoS Attack with extended contention window size in AC3.

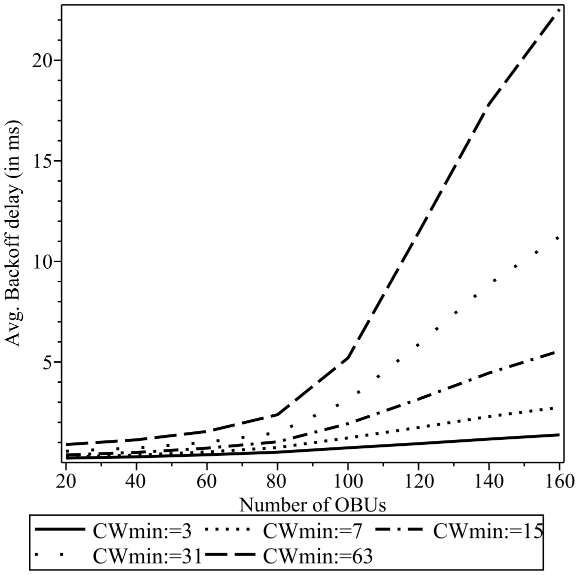
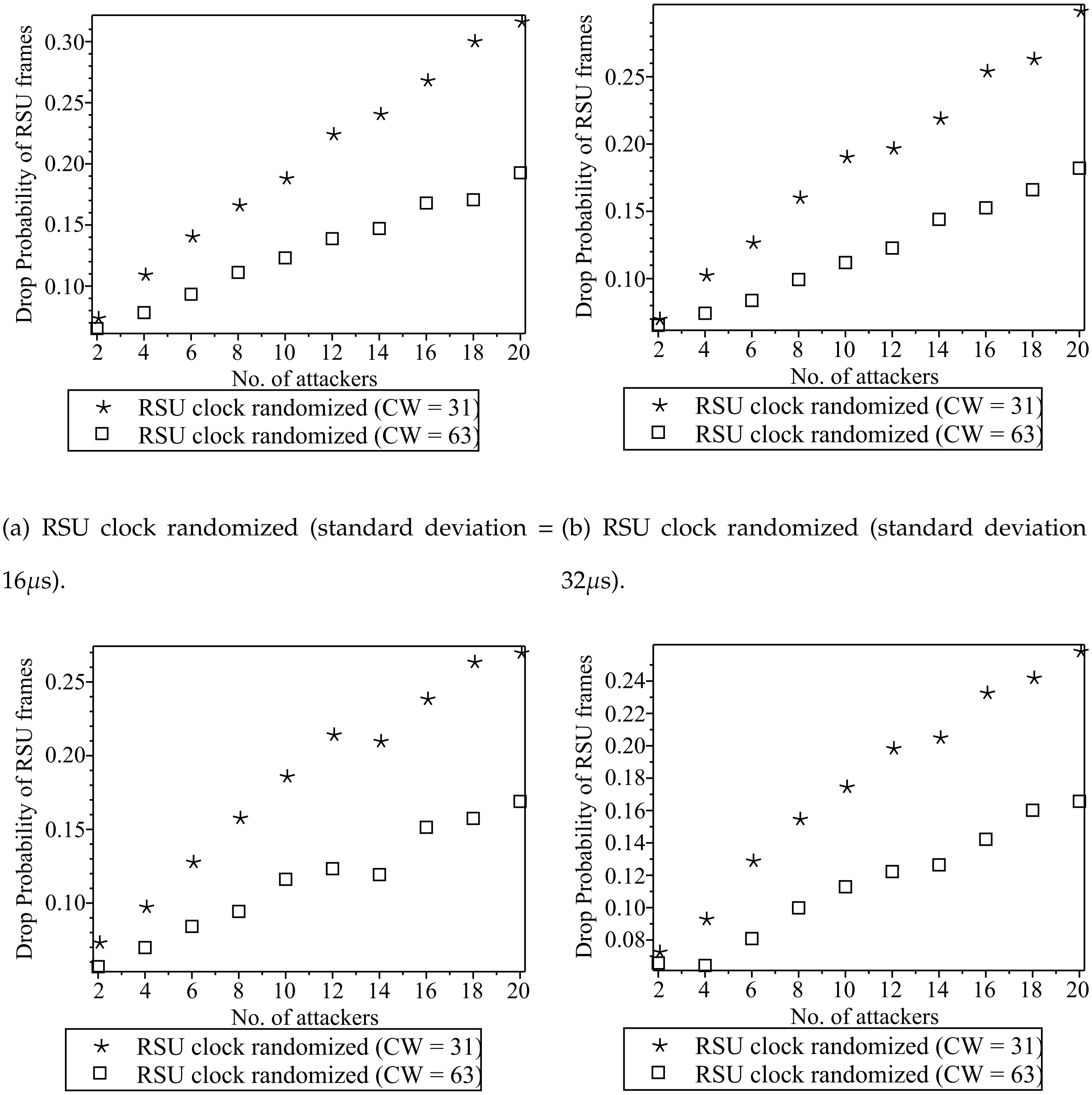


Figure 7.4: Average back-off delay (in ms) for transmitting a periodic message with different minimum contention window (CW_{min}) sizes.



(a) RSU clock randomized (standard deviation = 16μs).

(b) RSU clock randomized (standard deviation = 32μs).

(c) RSU clock randomized (standard deviation = 64μs).

(d) RSU clock randomized (standard deviation = 80μs).

Figure 7.5: Experiment 3: Drop probability of periodic frames by an RSU during a DDoS attack with extended contention window size and RSU time randomized.

Chapter 8

Conclusion and Future Work

This chapter concludes the dissertation with a brief summary of contributions and future direction of our research.

8.1 Contributions

One of the main contributions of this dissertation is providing secure authentication of VANET messages in vehicle-to-vehicle and vehicle-to-infrastructure communications. A vehicle is a personal device, hence in order to ensure user-privacy, authentication of an OBU originated message must be anonymous. On the other hand, a VANET infrastructure (i.e. an RSU) belongs to the public domain for which the anonymity of an RSU is not important. However, accountability is a crucial requirement for both RSU and OBU transmissions since a malicious node in the disguise of an RSU or an OBU may attempt to misuse the VANET features to destroy the traffic integrity and network consistency.

In this dissertation, we presented efficient authentication schemes using cryptographic primitives like proxy signature, identity-based signatures, and elliptic curve digital signature algorithm (ECDSA). A proxy signature based authentication scheme allows an RSU to sign an emergency or other application message on behalf of the corresponding roadside controller. A recipient OBU can distinctively verify the signature for message integrity and validity. Also, an anonymous and conditional authentication scheme for OBU messages has been presented using the modification of the RSU's proxy signature approach. Multiple sets of preloaded credentials provide the anonymity to an OBU in our authentication scheme. Upon a traffic dispute, it is possible to retrieve the actual identity of an OBU using the secret credentials of the third-party trusted authority. We extended our proxy signature based authentication approach by incorporating an identity-based authentication mechanism over ECDSA for authenticating RSU and OBU messages. RSUs and OBUs use their position information and current time to generate signature credentials for each individual signing session. This approach not only provides message integrity and session validation in VANETs, but also waives the requirement of the third-party proxy certificate for signature verification as the necessary signature and verification credentials are computed from the corresponding GPS data and current system time. A practical use of our extended authentication approach has been shown through a user application for parking assistance in VANET.

Verification of a signature incurs a cryptographic delay at the receiver during the message verification. Therefore, a high volume of traffic is always a challenge for authentication of safety messages since the collective verification time of received messages is often much longer than the average inter-arrival time of messages in VANETs.

We designed a verification technique that uses access priorities of traffic classes at the MAC-layer, as well as the sender's relevance to verify selective received messages. For each traffic class, a verification probability is calculated following the message's access priority and the relative traffic intensity of the particular access category.

An attacker in a VANET can synchronize its transmission with important periodic beacons from a service provider or an RSU. This is a form of a denial of service attack on VANET, which may block periodic beacons and legitimate periodic messages. Small contention window size for access classes, and the periodic nature of VANET messages or service advertisements make IEEE 802.11p EDCA mechanism vulnerable to such synchronization-based attacks. It gets even worse when multiple attacker collude to launch a synchronization-based DDoS attack. Broadcast communications in VANET do not have acknowledgements, meaning that neither the sender nor a receiver of periodic broadcasts would be aware of such an attack. We proposed modifications of current EDCA contention window sizes, as well as a periodic broadcast schedule in VANETs to thwart such attacks.

We developed a WAVE-based simulator of a VANET cell using NS-2.34. We simulated road-traffic scenarios with varying number of OBUs, RSUs and attackers in our experiments. Our simulator has been designed to incorporate WAVE protocol family including 802.11p's EDCA mechanism and WSM protocol of 1609.3 on CCH to evaluate WAVE MAC-layer performance for corresponding security and privacy schemes. Using our simulator, we also addressed the MAC-layer weaknesses related to the small contention window size and broadcast periodicity, which may impair the security of a WAVE-based VANET.

8.2 Future Work

For future development, we are looking forward to having some immediate collaboration with some local and international automobile industries, and/or transportation safety organizations for further research and implementation of our proposed schemes.

We plan to continue our research on the following topics:

8.2.1 Privacy-preserving Data Aggregation in VANETs

VANET users share vehicular data with RSUs and other OBUs. A compilation of such information from a VANET is worth using for road-safety measures, traffic planning, transportation research, and statistical or marketing purposes. Therefore, it is important to ensure the trust and reliability of the data collected from VANET entities. On the other hand, a VANET provider must protect user-privacy since it would be unethical from business point of view to disclose original identities of VANET users or their vehicles. Our security schemes can be extended to provide a secure and privacy-preserving data aggregation system for VANETs.

Anticipated challenges in a VANET data aggregation system are: (i) false data injection by OBUs, (ii) Sybil attacks, (iii) impersonation of OBUs, (iv) user-identity theft, and (v) validation of compiled data.

We would like to design a suitable approach which can fulfill the security and privacy requirements of a user and a provider in a VANET-based data aggregation system. Our research methodology would include study, research, and analysis of several cryptographic primitives, as well as finding the security weaknesses within the network infrastructure.

We strongly believe that we can come up with an appropriate solution which would be a good contribution to the research and development of vehicular ad hoc networks.

8.2.2 Secure Cloud Computing

Motivated by the recent progress in research and development of cloud systems, we want to extend our area of research to the secure and privacy-preserving cloud computing. We will use our knowledge of cryptography, network security, and anonymity to identify the security weaknesses of different cloud systems. We would also like to design, develop, and analyze new security and privacy models for cloud computing environments.

For our long-term research, we will continue our study and investigation on cryptographic primitives, security and privacy approaches for various networks and communication systems.

Bibliography

[1] IEEE, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Multi-channel Operation," IEEE, New York, NY, IEEE Std 1609.4, Nov. 2006.

[2] Transport Canada, "Canadian Motor Vehicle Traffic Collision Statistics," http://www.tc.gc.ca/eng/roadsafety/tp-tp3322-2007-1039.htm#t8, 2007.

[3] U.S. Census Bureau, "Transportation: Motor Vehicle Accidents and Fatalities," http://www.census.gov/compendia/statab/cats/transportation/motor_vehicle_accidents_and_fatalities.html, 2012.

[4] IEEE, "Draft Amendment for Wireless Access in Vehicular Environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.

[5] ——, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Security Services for Applications and Management Messages," IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006.

[6] ——, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environ-

ments (WAVE)- Networking Services," IEEE, New York, NY, IEEE Std 1609.3, Apr. 2007.

[7] K. Kowalenko, "Keeping Cars From Crashing," *The Institute, IEEE*, vol. 34, no. 3, pp. 5–5, Sep. 2010.

[8] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band," IEEE Computer Society, New York, NY, IEEE Std, Sep. 1999.

[9] Y. L. Morgan, "Novel Issues in DSRC Vehicular Communication Radios," *IEEE Canadian Review*, vol. Spring 2010, no. 63, pp. 7–10, 2010.

[10] J. Misic, G. Badawy, S. Rashwand, and V. B. Misic, "Tradeoff Issues for CCH/SCH Duty Cycle for IEEE 802.11p Single Channel Devices," in *Proceedings of the IEEE Global Communications Conference, 2010 (GLOBECOM 2010)*, Miami, Florida, USA, Dec. 2010, pp. 1–6.

[11] S. Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard," in *Proceedings of IEEE 66th Vehicular Technology Conference, 2007. VTC-2007 Fall*, Baltimore, MD, USA, Oct. 2007, pp. 2199–2203.

[12] IEEE, "IEEE Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," IEEE Computer Society, New York, NY, IEEE Std 802.11e, Nov. 2005.

[13] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in

Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV), College Park, MD, USA, Nov. 2005, Electronic Proceeding.

[14] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Networks," in *Proceedings of The 25th Conference on Computer Communications, (INFOCOM 2006)*. Bercelona, Spain: IEEE Communications Society, Apr. 2006, Electronic Proceedings.

[15] J. R. Douceur, "The Sybil Attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '02)*. Cambridge, MA, USA: Springer-Verlag, Mar. 2002, pp. 251–260.

[16] NS2, "The Network Simulator- ns-2," http://nsnam.isi.edu/nsnam/index.php/User_Information, 2012.

[17] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications Magazine*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[18] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[19] F. Zhang, R. Safavi-Naini, and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," in *Proceedings of 7th International*

Workshop on Theory and Practice in Public Key Cryptography (PKC 2004), LNCS 2947. Singapore: Springer-Verlag, Mar. 2004, pp. 277–290.

[20] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *Proceedings of he 27th Conference on Computer Communications (INFOCOM 2008)*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.

[21] D. Chaum and E. van Heyst, "Group Signatures," in *Proceedings of Advances in Cryptology, EUROCRYPT '91*, Brighton, UK, Apr. 1991, pp. 257–265.

[22] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in *Proceedings of The 24rd Annual International Cryptology Conference (CRYPTO 04), LNCS series*. Santa Barbara, CA, USA: Springer-Verlag, Aug. 2004, pp. 41–55.

[23] J. Guo, J. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," in *Proceedings of Mobile Networking for Vehicular Environments 2007*, Anchorage, Alaska, USA, May 2007, pp. 103–108.

[24] J. Nechvatal, "A Public-key-based Key Escrow System," *Journal of Systems and Software*, vol. 35, no. 1, pp. 73–83, Oct. 1996.

[25] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[26] G. Ateniese, D. Song, and G. Tsudik, "Quasi-Efficient Revocation of Group

Signatures," in *Proceedings of Sixth International Financial Cryptography Conference*. Southampton, Bermuda: Springer-Verlag, Mar. 2001, pp. 183–197.

[27] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," in *Proceedings of Eurocrypt 2004, volume 3027 of LNCS*. Springer-Verlag, May 2004, pp. 571–589.

[28] S. Zhou and D. Lin, "Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps," in *Proceedings of 5th International Conference on Cryptology and Network Security*, Suzhou, China, Dec. 2006, pp. 126–143.

[29] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," in *Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT '05)*, Chennai, India, Dec. 2005, pp. 515–532.

[30] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive Privacy-Preserving Authentication in Vehicular Networks," in *In Proceedings of the First International Conference on Communications and Networking in China, 2006. ChinaCom '06.*, Beijing, China, Oct. 2006, pp. 1–8.

[31] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[32] Massachusetts Institute of Technology, "CIS: The Threshold Cryptography," http://groups.csail.mit.edu/cis/cis-threshold.html, 2009.

[33] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," in *Proceedings of Eighth International Symposium on Autonomous Decentralized Systems, 2007. ISADS '07*, Sedona, Arizona, USA, Mar. 2007, pp. 344–351.

[34] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad hoc Networks (VANET '07)*, Montreal, Quebec, Canada, Sep. 2007, pp. 19–28.

[35] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, Dec. 2009.

[36] D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Certicom Research, Canada; and Dept. of Combinatorics and Optimization, University of Waterloo, Canada, Tech. Rep., Aug. 1999.

[37] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, vol. 5, no. Summer, pp. 2–13, 2002.

[38] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Real-World VANET Security Protocol Performance." in *Proceedings of IEEE Global Communications Conference (GLOBECOM 2009)*. Honolulu, HI, USA: IEEE, Dec. 2009, pp. 1–7.

[39] H. Wen, P.-H. Ho, and G. Gong, "A Novel Framework for Message Authentication in Vehicular Communication Networks," in *Proceedings of IEEE Global Telecommunications Conference, 2009 (GLOBECOM 2009).*, Honolulu, HI, Nov.–Dec. 2009, pp. 1–6.

[40] A. Wasef and X. Shen, "ASIC: Aggregate Signatures and Certificates Verification Scheme for Vehicular Networks," in *Proceedings of the 28th IEEE Conference on Global Communications (GLOBECOM 2009)*, Honolulu, HI, USA, Dec. 2009, pp. 4489–4494.

[41] T. Zhou, R. Roy Choudhury, P. Ning, and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," in *Proceedings of The 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, Philadelphia, PA, USA, Aug. 2007, pp. 1–8.

[42] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks," in *Proceedings of the 5th international conference on Privacy Enhancing Technologies*. Cavtat, Croatia: Springer Berlin/Heidelberg, May–Jun. 2005, pp. 197–209.

[43] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*. Montreal, Quebec, Canada: ACM, Oct. 2005, pp. 79–87.

[44] A. K. Lenstra, P. Winkler, and Y. Yacobi, "A Key Escrow System with Warrant Bounds," in *CRYPTO '95: Proceedings of the 15th Annual International*

Cryptology Conference on Advances in Cryptology. Santa Barbara, CA, USA: Springer-Verlag, Aug. 1995, pp. 197–207.

[45] Z. Li and C. Chigan, “On Resource-Aware Message Verification in VANETs,” in *Proceedings of IEEE International Conference on Communications*. Cape Town, South Africa: IEEE, May 2010, pp. 1–6.

[46] Y. Jiang, M. Shi, X. Shen, and C. Lin, “BAT: A Robust Signature Scheme For Vehicular Networks Using Binary Authentication Tree,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, Apr. 2009.

[47] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks,” in *Proceedings of The 27th Conference on Computer Communications (INFOCOM 2008).*, Phoenix, AZ, USA, Apr. 2008, pp. 246–250.

[48] J. H. Cheon and J. H. Yi, “Fast Batch Verification of Multiple Signatures,” in *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography - PKC 2007*, Beijing, China, Apr. 2007, pp. 442–457.

[49] M. Mambo, K. Usuda, and E. Okamoto, “Proxy Signatures for Delegating Signing Operation,” in *CCS ’96: Proceedings of the 3rd ACM conference on Computer and communications security*. New Delhi, India: ACM, Oct. 1996, pp. 48–57.

[50] S. Kim, S. Park, and D. Won, “Proxy Signatures, Revisited,” in *Proceedings*

of the First International Conference on Information and Communication Security (ICICS '97). Beijing, China: Springer-Verlag, Nov. 1997, pp. 223–232.

[51] M. Cai, L. Kang, and J. Jia, "A Multiple Grade Blind Proxy Signature Scheme," in *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, vol. 2. Los Alamitos, CA, USA: IEEE Computer Society, Nov. 2007, pp. 130–133.

[52] J.-H. Park, Y.-S. Kim, and J. H. Chang, "A Proxy Blind Signature Scheme with Proxy Revocation." Harbin, China.: IEEE Computer Society, Dec. 2007, pp. 761–764.

[53] L. Wei-min, Y. Zong-kai, and C. Wen-qing, "A New ID-based Proxy Blind Signature Scheme," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 3, pp. 555–558, Jan. 2005.

[54] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," in *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '89*. Santa Barbara, CA, USA: Springer-Verlag, Aug. 1989, pp. 239–252.

[55] ——, "Efficient Signature Generation By Smart Cards," *Journal of Cryptology*, vol. 4, pp. 161–174, Jan. 1991.

[56] X. Sun, X. Lin, and P.-H. Ho, "Secure Vehicular Communications Based on Group Signature and ID-Based Signature Scheme," in *Proceedings of IEEE*

International Conference on Communications, Glasgow, Scotland, Jun. 2007, pp. 1539–1545.

[57] A. Shamir, “Identity-based Cryptosystems and Signature Schemes,” in *Proceedings of CRYPTO 84 on Advances in Cryptology*. Santa Barbara, California, United States: Springer-Verlag New York, Inc., Aug. 1985, pp. 47–53.

[58] C. Cocks, “An Identity Based Encryption Scheme Based on Quadratic Residues,” in *Proceedings of IMA International Conference*. Cirencester, UK: Springer-Verlag, Dec. 2001, pp. 360–363.

[59] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, Mar. 2003.

[60] F. Hess, “Efficient Identity Based Signature Schemes Based on Pairings,” in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Aug. 2003, vol. 2595, pp. 310–324.

[61] X. Sun and M. Xia, “An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography,” in *Proceedings of International Conference on Computer and Communications Security*. Chicago, IL, USA: IEEE Computer Society, Nov. 2009, pp. 88–91.

[62] M.-H. Chang, I.-T. Chen, and M.-T. Chen, “Design of Proxy Signature in ECDSA,” in *Proceedings of the 2008 Eighth International Conference on Intelligent Systems Design and Applications (ISDA '08)*. Washington, DC, USA: IEEE Computer Society, Nov. 2008, pp. 17–22.

[63] Z. Dong, L. Shengli, and C. Kefei, "Cryptanalysis of LKK Proxy Signature," in *Progress on Cryptography*. Springer-Verlag, 2004, vol. 769, pp. 161–164.

[64] Q. Xue, F. Li, Y. Zhou, J. Zhang, Z. Cao, and H. Qian, "An ECDLP-Based Threshold Proxy Signature Scheme Using Self-Certified Public Key System," in *Proceedings of The First International ICST Conference on Security and Privacy in Mobile Information and Communication Systems*, Turin, Italy, Jun. 2009, pp. 58–70.

[65] S. Biswas and J. Misic, "Deploying Proxy Signature in VANETs," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2010)*. IEEE, Dec. 2010, pp. 1–6.

[66] ——, "Establishing Trust on VANET Safety Messages," in *Proceedings of the Second International Conference on Ad Hoc Networks, 2010*. Victoria, BC, Canada: Springer, Aug. 2010, pp. 314–327.

[67] ——, "Proxy Signature-based RSU Message Broadcasting in VANETs," in *Proceedings of the 25th Biennial Symposium on Communications (QBSC), 2010*. Kingston, ON, Canada: IEEE, May 2010, pp. 5–9.

[68] F. Zhang and K. Kim, "Efficient ID-based Blind Signature and Proxy Signature From Bilinear Pairings," in *Proceedings of the 8th Australasian Conference on Information Security and Privacy (ACISP'03)*. Wollongong, Australia: Springer-Verlag, Jul. 2003, pp. 312–323.

[69] J. Xu, Z. Zhang, and D. Feng, "ID-Based Proxy Signature Using Bilinear

Pairings," in *Proceedings of Parallel and Distributed Processing and Applications - ISPA 2005 Workshops*, ser. Lecture Notes in Computer Science. Nanjing, China: Springer Berlin / Heidelberg, Nov. 2005, vol. 3759, pp. 359–367.

[70] Z. Dong, H. Zheng, K. Chen, and W. Kou, "ID-Based Proxy Blind Signature," in *Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA '04)*, vol. 2. Fukuoka, Japan: IEEE Computer Society, Mar. 2004, pp. 380–383.

[71] C. Gu and Y. Zhu, "Information Security and Cryptology." Springer-Verlag, 2008, ch. An Efficient ID-Based Proxy Signature Scheme from Pairings, pp. 40–50.

[72] W. Lang, Y. Tan, Z. Yang, G. Liu, and B. Peng, "A New Efficient ID-based Proxy Blind Signature Scheme," in *Proceedigns of IEEE Symposium on Computers and Communications*, vol. 1. Alexandria, Egypt: IEEE Computer Society, Jun.–Jul. 2004, pp. 407–411.

[73] X. Li and K. Chen, "Identity Based Proxy-Signcryption Scheme from Pairings," in *Proceedings of IEEE International Conference on Services Computing*. Shanghai, China: IEEE Computer Society, Sep. 2004, pp. 494–497.

[74] W. Wu, Y. Mu, W. Susilo, J. Seberry, and X. Huang, "Identity-Based Proxy Signature from Pairings," in *Proceedings of 4th International Conference Autonomic and Trusted Computing, ATC 2007*, ser. Lecture Notes in Computer Science, vol. 4610. Hong Kong, China: Springer, Jul. 2007, pp. 22–31.

[75] J. Zhang and W. Zou, "Another ID-based Proxy Signature Scheme and Its Extension," *Wuhan University Journal of Natural Sciences*, vol. 12, no. 1, pp. 33–36, Jan. 2007.

[76] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for Cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, Sep. 2008.

[77] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based Key Agreement Protocols from Pairings," *International Journal of Information Security*, vol. 6, no. 4, pp. 213–241, Jun. 2007.

[78] Z. Tan, Z. Liu, and C. Tang, "Digital Proxy Blind Signature Schemes Based on DLP and ECDLP," MM Research Preprints, Tech. Rep., Dec. 2002.

[79] C. Qi and Y. Wang, "An Improved Proxy Blind Signature Scheme Based on Factoring and ECDLP," in *Proceedings of International Conference on Computational Intelligence and Software Engineering, 2009 (CiSE 2009).*, Wuhan, China, Dec. 2009, pp. 1–4.

[80] H. Jin, H. Debiao, and C. Jianhua, "An Identity Based Digital Signature from ECDSA," *International Workshop on Education Technology and Computer Science*, vol. 1, pp. 627–630, Mar. 2010.

[81] NIST, "NIST: National Institute of Standards and Technology," http://www.nist.gov/index.html, 2011.

[82] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi,

and H. Hartenstein, “Overhaul of IEEE 802.11 Modeling and Simulation in ns-2,” in *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM ’07)*, Oct. 2007, pp. 159–168.

[83] T. El Gamal, “A Public Key Cryptosystem and A Signature Scheme Based On Discrete Logarithms,” in *Proceedings of CRYPTO 84 on Advances in Cryptology*. Santa Barbara, California, United States: Springer-Verlag New York, Inc., Aug. 1985, pp. 10–18.

[84] J. Petit, “Analysis of ECDSA Authentication Processing in VANETs,” in *Proceedings of the 3rd International Conference on New Technologies, Mobility and Security (NTMS’09)*, Cairo, Egypt, Dec. 2009, pp. 388–392.

[85] C. Díaz, S. Seys, J. Claessens, and B. Preneel, “Towards Measuring Anonymity,” in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*. Springer-Verlag, LNCS 2482, Apr. 2002, pp. 54–68.

[86] S. Biswas, J. Misic, and V. Misic, “DDoS Attack on WAVE-enabled VANET Through Synchronization,” in *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2012)*. IEEE, Dec. 2012, pp. 1–6.

[87] S. Biswas and J. Misic, “Relevance-based Verification of VANET Safety Messages,” in *Proceedings of IEEE International Conference on Communications, ICC 2012*. Ottawa, ON, Canada: IEEE, Jun. 2012, pp. 1–5.

[88] NIST, “NIST: National Institute of Standards and Technology,” http://xlinux.nist.gov/dads/HTML/perfectBinaryTree.html, 2011.

[89] S. Biswas, J. Misic, and V. Misic, "ID-based Safety Message Authentication for Security and Trust in Vehicular Networks," in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*, Minneapolis, MN, USA, Jun. 2011, pp. 323–331.

[90] P. S. Almeida, C. Baquero, N. Preguiça, and D. Hutchison, "Scalable Bloom Filters," *Information Processing Letters*, vol. 101, no. 6, pp. 255–261, Mar. 2007.

[91] F. Deng and D. Rafiei, "Approximately Detecting Duplicates For Streaming Data Using Stable Bloom Filters," in *Proceedings of the 2006 ACM SIGMOD International Conference on Management of Data (SIGMOD '06)*. Chicago, IL, USA: ACM, Jun. 2006, pp. 25–36.

[92] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 2772–2785, Jul. 2010.

[93] S. Biswas and J. Misic, "Location-based Anonymous Authentication for Vehicular Communications," in *Proceedings of the 22nd IEEE Symposium on Personal, Indoor, Mobile and Radio Communications (PIMRC 2011)*. Toronto, ON, Canada: IEEE Communication Society, Sep. 2011, pp. 1–5.

[94] J. Isaac, S. Zeadally, and J. Camara, "Security Attacks and Solutions For Vehicular Ad hoc Networks," *IET Communications*, vol. 4, no. 7, pp. 894–903, Apr. 2010.

[95] P. Ding, "Central Manager: A Solution to Avoid Denial of Service Attacks

for Wireless LANs," *International Journal of Network Security*, vol. 4, no. 1, pp. 35–44, Jan. 2007.

[96] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks At the MAC Layer In Wireless Ad hoc Networks," in *Proceedings of Military Communications Conference (MILCOM 2002).*, vol. 2, Anaheim, CA, USA, Oct. 2002, pp. 1118–1123.

[97] D. J. Thuente, B. Newlin, and M. Acharya, "Jamming Vulnerabilities of IEEE 802.11e," in *Proceedings of Military Communications Conference, 2007 (MILCOM 2007).*, Orlando, FL, USA, Oct. 2007, pp. 1–7.

[98] Y. Zhou, D. Wu, and S. M. Nettles, "On MAC-layer Denial of Service Attacks in IEEE 802.11 Ad hoc Networks: Analysis and Counter Measures," *International Journal of Wireless and Mobile Computing*, vol. 1, no. 3/4, pp. 268–275, Feb. 2006.

[99] S. Biswas and J. Misic, "Prioritized WAVE-based Parking Assistance with Security and User Anonymity," *Journal of Communications: Special Issue on Security and Privacy in Communication Systems and Networks*, vol. 8, no. 7, pp. 577–586, Aug. 2012.

[100] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in Vehicular Ad hoc Networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, Apr. 2008.