석 사 학 위 논 문

Master's Thesis

차량 애드-혹 네트워크에서의 효율적인 익명 인증 기법 연구

A Study on Efficient Anonymous Authentication Scheme in Vehicular Ad-hoc Networks

임 준 현 (任 俊 賢 Yim, Junhyun)

전산학과

Department of Computer Science

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

2011

차량 애드-혹 네트워크에서의 효율적인 익명 인증 기법 연구

A Study on Efficient Anonymous Authentication Scheme in Vehicular Ad-hoc Networks

A Study on Efficient Anonymous Authentication Scheme in Vehicular Ad-hoc Networks

Advisor : Professor Kwangjo Kim

by

Yim, Junhyun
Department of Computer Science
Korea Advanced Institute of Science and Technology

A thesis submitted to the faculty of the Korea Advanced Institute of Science and Technology in partial fulfillment of the requirements for the degree of Master of Engineering in the Department of Computer Science

Daejeon, Korea
2010. 12. 16.
Approved by

Professor Kwangjo Kim
Advisor

차량 애드-혹 네트워크에서의 효율적인 익명 인증 기법 연구

임 준 현

위 논문은 한국과학기술원 석사학위논문으로 학위논문심사 위원회에서 심사 통과하였음.

2010년 12월 16일

심사위원장 김광조 (인)

심사위원 윤현수 (인)

심사위원 이동만 (인)

MCS 20094079 임 준 현. Yim, Junhyun. A Study on Efficient Anonymous Authentication Scheme in Vehicular Ad-hoc Networks. 차량 애드-혹 네트워크에서의 효율적인 익명 인증 기법 연구. Department of Computer Science . 2011. 30p. Advisor Prof. Kwangjo Kim. Text in English.

Abstract

Vehicular Ad-hoc Networks (VANETs) are one of typical application of wireless communication technology, which provide communications among nearby vehicles and between vehicles and roadside units (RSUs) connected the infrastructure. VANETs provide a perfect way to collect dynamic traffic information and sense various physical conditions related to traffic distribution with very low cost and high accuracy, which have a great potential to revolutionize driving environment, and will undoubtedly play an important role in the future transportation system. However, it is clear that security and privacy enhancing mechanisms are necessary, which are in fact a prerequisite for deployment. This has been recently well understood in academia, the industry, and among authorities. And a large number of agreed efforts have been undertaken to design security architectures for VANET systems. Extensive research efforts have been made by both industry and academia to make VANETs secure. In this thesis, we proposed a novel anonymous authentication scheme in VANETs. Our proposed scheme guarantees authentication, anonymity, unlinkability, and traceability simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. We utilize the traceable ring signature scheme with the k-times anonymous authentication scheme to address the contradictory between the unlinkability and the traceability. Our scheme also uses elliptic curve cryptosystem to achieve storage, computation, and communication efficiency. Compared with existing works, we claim that our scheme has better performance in terms of storage, computation, and communication overhead. In addition, our scheme has three advantages compared with other previous works. First, our scheme doesn't have revocation list update process in authentication process. Second, our scheme always provides unlinkability although multiple RSUs are compromised. Finally, our scheme requires only one authentication process for mutual authentication when the vehicle communicates with the same RSU, because our scheme has key agreement functionality that makes secure channel to communicate. These advantages make our scheme efficient in large-scale and busy networks like VANETs.

Contents

List of Tables

List of Figures

1. Introduction

1.1 Overview

Along with the fast improvement and wide deployment of wireless communication technologies, Vehicular Ad-hoc Networks (VANETs) [8] which are one of their typical applications, as a special form of Mobile Ad-hoc Networks (MANETs) [3], provide communications among nearby vehicles and between vehicles and roadside units (RSUs) connected the infrastructure. VANET inherently cannot only provide a perfect way to collect dynamic traffic information, but also sense various physical conditions related to traffic distribution with very low cost and high accuracy, which is considered to be essential for achieving automatic and dynamic information collection and fusion in an Intelligent Transportation System (ITS) [4]. Automatic payment for parking lots and toll collection are other examples of applications inside VANETs. VANETs have a great potential to revolutionize driving environment, and will undoubtedly play an important role in the future transportation system. Recently, the growing demand for optimization of road traffic and improvement of road safety has brought a wide interest on VANETs. Therefore, car manufactures and telecommunication industries prepare to equip each vehicle with wireless devices that enable vehicle-to-vehicle and vehicle-to-RSU communication in order to improve driver's driving experience and safety.

The VANET system mainly consists of vehicles, RSUs and Certificate Authorities (CAs). Vehicles have wireless communication and computation devices, While RSUs connected with infrastructure are deployed in roadside to provide wireless communication to vehicles within their radio coverage. VANETs can be implemented variety of wireless technologies such as Dedicated Short Range Communications (DSRC) [1]. Other candidate wireless technologies are cellular, satellite, and WiMAX. According to the DSRC, each vehicle in a VANETs broadcasts a traffic safety message every 100-300ms, which keeps the vehicle's driving related information, such as location, speed, turning intention, and driving status (*e.g.*, regular driving, waiting for a traffic sign, traffic jam, *etc.*) to other vehicles. With multi-hop forwarding, the messages will be either terminated by a vehicle or dropped when exceeding over their lifetimes. When receiving a message, the vehicle can either react to it if the sending vehicle of the message is nearby with some requests that can be handled locally, or deliver the information to a traffic control center if the message is considered

to contain any useful information. The vehicle can also monitor the traffic situation of its current location and report the summarized information to the traffic control center. The traffic control center can generate an optimized control and management strategy for traffic sign control by analyzing the current traffic load in each intersection, in addition to traffic information collection for traffic flow analysis and control. There are also multimedia and Internet connectivity facilities for passengers, all provided within the wireless coverage of each vehicle. Most of the concerns of interest to MANETs are interested in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interaction with RSUs can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion being constrained to follow a paved highway.

In the VANET, a formidable set of abuses and attacks always happens. We have to consider, for example, an attacker that contaminates the large portions of the vehicular network with false information. A single compromised vehicle can transmit false hazard warnings, which can then be taken up by all vehicles in both traffic streams. A tampered vehicle can forge messages to masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. A different type of attacker can deploy a number of receivers and records messages transmitted by the vehicles. Then, the attacker can infer the private information about its driver and passengers from recorded messages to track the location of the vehicle. It is clear that security and privacy enhancing mechanisms are necessary to thwart such attacks, which are in fact a prerequisite for deployment. Otherwise VANET systems could make anti-social and criminal behavior easier, in a way that would actually jeopardize the benefits of their deployment. This has been recently well understood in academia, the industry, and among authorities. And a large number of agreed efforts have been undertaken to design security architectures for VANET systems.

Extensive research efforts have been made by both industry and academia to solve this problems and make VANETs secure. Some researches [5, 6, 7, 8, 9] described secure network models and threats in VANETs. And there are privacy preservation and conditional tracking issues. But most of existing schemes for secure vehicular networks [12, 13, 14] were simply for authentication with privacy preservation without an effective and efficient conditional tracking mechanism. The conditional tracking mechanism is required to reveal the real identity of vehicles from their pseudo identity and track target vehicles in situation such as traffic accident, illegal activity, and liability investigation. When a malicious node is detected in VANETs, the conditional tracking mechanism could be utilized to manage revocation list [10] efficiently. So some researches [15, 16, 17] proposed an anonymous

authentication protocol which has the conditional tracking mechanism. Their schemes are based on a huge number of anonymous keys and pure group signature technique. They can fall disadvantage in the aspects of requiring a huge storage for anonymous keys and safety message for anonymous authentication. This problem becomes essentially fatal when the size of the revocation list, which keeps all the revoked anonymous keys, is large.

1.2 Our Contribution

In this thesis, we propose a novel anonymous authentication scheme in VANETs. Our scheme guarantees authentication, anonymity, unlinkability, and traceability simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. We utilize the traceable ring signature scheme [18] with the k-times anonymous authentication scheme [19] to address the contradictory requirements. Our scheme also use elliptic curve cryptosystem [20] to achieve storage, computation, and communication efficiency. Compared with existing works, our scheme has better performance in terms of storage, computation, and communication overhead.

1.3 Organization

The remainder of the thesis is organized as follows: A brief survey on the related work and describing background of our work are conducted in Chapter 2. The our scheme and security requirements are presented detail in Chapter 3. Chapter 4 analyzes the security and performance of the proposed scheme. Finally, we summarize and conclude the thesis in Chapter 5.

2. Background and Related Work

2.1 Related Work

2.1.1 DSRC/WAVE

Dedicated Short Range Communications (DSRC)/Wireless Access in a Vehicular Environment (WAVE) [2] standards suite is based on multiple cooperating standards for mobile wireless radio communications mainly developed by the IEEE. DSRC/WAVE is part of Vehicle Infrastructure Integration (VII) initiative by Federal Highway Authority and supports vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications for emerging ITS. DSRC/WAVE systems fill a niche in the wireless infrastructure by facilitating low latency, geographically local, high data rate, and high mobility communications. The following table compares DSRC/WAVE capabilities to other wireless technologies.

	DSRC/WAVE	**Wi-Fi**	**GSM**	**WiMAX**
Transmission Rate	3-27 Mbps	6-54 Mbps	$<$ 2 Mbps	1-32 Mbps
Latency	$<$ 50 ms	Seconds	Seconds	/
Range	$<$ 1 km	$<$ 100 m	$<$ 10 km	$<$ 15 km
Bandwidth	10 MHz	20 MHz	$<$ 3 MHz	$<$ 10 MHz
Operating Band	5.86 $\sim$ 5.92 GHz	2.4 GHz, 5.2 GHz	800 MHz, 1.9 GHz	2.5 GHz
IEEE Standards	802.11p	802.11a	N/A	802.16e

Table 2.1: Comparison of DSRC/WAVE and other wireless systems

WAVE is a term used to describe the suite of IEEE P1609.x standards that are focused on MAC and network layers. WAVE is fairly complex and is built over the IEEE 802.11 standards by amending many tweaks to guarantee fast reliable exchange of safety messages. WAVE is the core part of DSRC. However, either of the two terms is commonly used arbitrarily. In some cases, the term DSRC is used as a more general term compared to WAVE. The history leading to the development of current DSRC goes back almost a decade and a half. In the early 1990s, it became clear that road toll collection

can be simplified by means of RFID transponders. Major industrial suppliers of electronic toll collection quickly discovered that further development on 915?MHz might pave the road for much elegant breed of applications facilitating enhanced road safety and collision avoidance. The group of electronic toll suppliers along with other stake holders formed a consortium focused on DSRC development. Coincidently, multiple studies on vehicular safety and collision avoidance revealed that short-range communication (100?meters) would be sufficient for most safety application. The DSRC community then attempted to standardize the 915?MHz using the ASTM framework but quickly thought of the IEEE 802.11 approach and the 5.9?GHz as a direct way to benefit from its ad-hoc mode. The ad-hoc mode of IEEE 802.11 resembles the situation of vehicle-to-vehicle communications and hence, simplifies the development of DSRC. Almost a decade of DSRC standards development has resulted in the IEEE 802.11p standards along with IEEE 1609.x, both standards represent together proposed DSRC suite of standards.

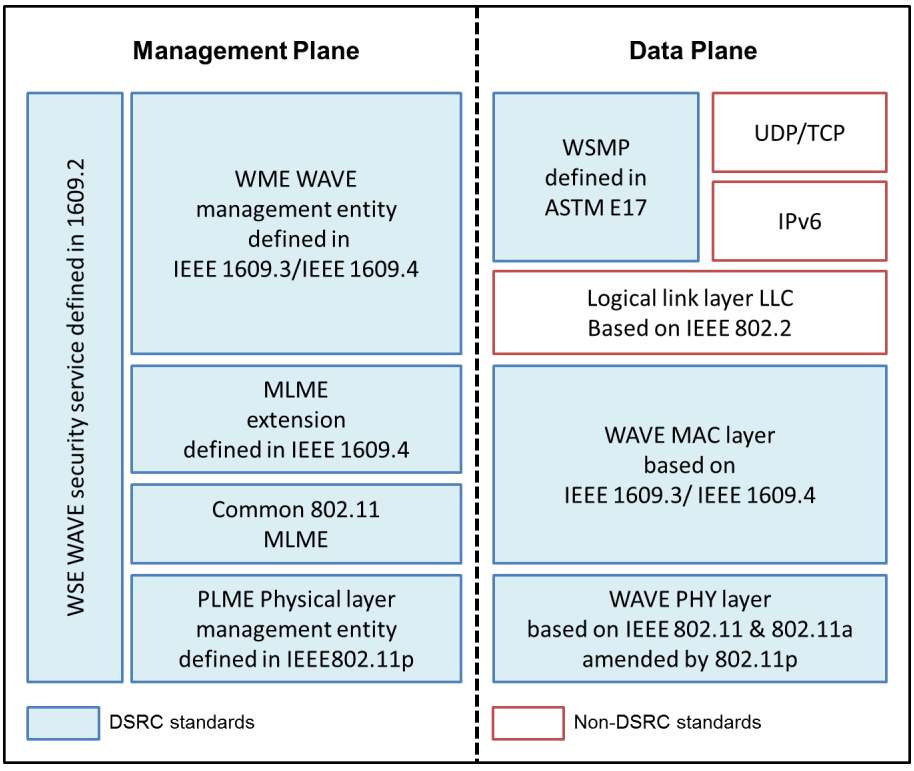

Figure 2.1: DSRC/WAVE communication stack

2.1.2 Anonymous Authentication Schemes for VANETs

M. Raya *et al.* proposed some building blocks for secure vehicular communication [15]. As a straightforward solution in their protocol, each vehicle possesses a set of anonymous keys to sign a message and these keys are periodically changed to avoid being tracked. However, it has some critical disadvantages. Each vehicle requires large storage space to store huge number of anonymous key pairs and anonymous public key certificates. Moreover, it takes long time to update the certificate revocation list due to the large number of public keys. This protocol provides authentication, anonymity, unlinkability and traceability. Although authority can track problematic certificate, it is very time consuming process due to the long revocation list.

X. Lin *et al.* proposed a secure and privacy preserving protocol for vehicular communications called GSIS [16], using a group signature [22] and identity-based signature techniques [23] to resolve the requirement of a large number of public key certificates. They use the group signature for communication between vehicles. And the identity-based signature scheme is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity. The GSIS providesauthentication, anonymity, unlinkability and traceability. In their work, vehicles possess only their own group signing key issued by a trusted group manager, and each vehicle signs a message by using group signature scheme to be authenticated as a legitimate sender of the message. However, although the revocation list is short and easily updated, the time for message verification accompanied with revocation check grows linearly with the number of revoked vehicles in the revocation list. Thus each vehicle has to spend more time on message verification when the scale of revocation list is large. Once the safety message is time-aware, this solution may not be feasible due to the heavy verification process.

R. Lu *et al.* proposed an efficient conditional privacy preservation protocol for secure vehicular communications, called ECPP [17], which issues on-the-fly short-time anonymous certificate to vehicles by using a group signature scheme [24]. Since RSUs can check the validity of the requesting vehicle during the short-time anonymous certificate generation phase, such revocation check by vehicle itself of GSIS is not required. Therefore message verification is more efficient that GSIS. The ECPP provides authentication, anonymity, unlinkability and traceability under the unrealistic assumption that most RSUs will not disclose any inner information without the authorization of the trusted authority. However, due to a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection facilities against malicious attacks. Therefore, it is possible for an attacker to access RSUs and disclose the information in the RSUs. When multiple RSUs are

compromised, an attacker is able to track the movement of a vehicle by using the information stored in the compromised RSUs, because each RSU stores unchanged pseudonyms for OBUs in ECPP. As a result, ECPP does not provide unlinkability when some RSUs are compromised.

2.1.3 Traceable Ring Signature Scheme

A ring signature scheme allows a signer to sign a message while preserving anonymity behind a group, called a ring, which is selected by the signer. A verifier can check the validity of the signature, but cannot know who generated it among all possible ring members. In addition, two signatures generated by the same singer are unlinkable. Namely, it is infeasible for the verifier to determine whether the signatures are generated by the same signer. This notion was first formally introduced by Rivest, Shamir, and Tauman [21], and since then, this topic has been studied extensively. The ring signature provides great flexibility: No group manager, no special setup, and the dynamics of group choice. However the ring signature is vulnerable to malicious or irresponsible signers in some applications, because of its anonymity. A traceable ring scheme is a ring signature except that it can restrict excessive anonymity. The traceable ring signature has a tag that consists of a list of ring members and an issue that refers to, for instance, a social affair or an election. A ring member can make any signed but anonymous opinion regarding the issue, but only once (per tag). If the member submits another signed opinion, possibly pretending to be another person who supports the first opinion, the identity of the member is immediately revealed. If the member submits the same opinion, for instance, voting "yes" regarding the same issue twice, everyone can see that these two are linked. The traceable ring signature can suit to many applications, such as an anonymous voting. It preserves the flexibility of the ring signature: No group manager, no special setup for sharing secrets among members in a group, and the dynamics of group choice. It implies that the identity of a signer is never escrowed by a special person or group. A traceable ring signature has a tag $L = \{issue, PK_N\}$, where PK_N is the set of public keys of the ring members and $issue$ refers to, for instance, an identifier of an election or some social issue. A ring member can sign a message using his own secret key and the verifier can verify the signature on the message with related tag L, but cannot know who generated the signature among all the possible ring members in L.

2.1.4 k-Times Anonymous Authentication Scheme

A k-times anonymous authentication scheme in which users can be authenticated anonymously so long as times that they are authenticated is within an allowable number. It has two features that allow 1) no one, not even an authority, identify users who have been authenticated within the allowable number, and that allow 2) anyone to trace, without help from the authority, dishonest users who have been authenticated beyond the allowable number by using the records of these authentications. Although identity escrow/group signature schemes allow users to be anonymously authenticated, the authorities in these schemes have the unnecessary ability to trace any user. The k-times anonymous authentication scheme can be applied to e-voting, e-cash, electronic coupons, and trial browsing of content. In these applications, unlike the previous one, conceals users' participation from protocols and guarantees that they will remain anonymous to everyone.

Any traceable ring signature scheme can be efficiently transformed into a traceable ring signature scheme with k-times anonymity, where the k-times anonymity means that a signer is allowed to sign messages with respect to the same tag at most k times without being traced. It is simply obtained by regarding $(i, Sig_{sk}((L, i), m))$ as a signature on m, with related tag L, where the verifier checks if $\mathrm{Ver}((L, i), m) = 1$ and $1 \leq i \leq k$ (Here the signer need not publish i in order). It is obvious that the identity of a signer is not revealed if the signer is enough careful not to issue the same index twice on the same tag. However, they remark that this implementation has a weakness in the unlinkability property. Because whether or not the two signatures have been generated by the different signers can be easily determined, if the two signatures have the same tag and index.

2.1.5 Elliptic Curve Cryptosystem (ECC)

The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + a^x + b$, where $4a^3 + 27b^2 \neq 0$. Each value of the a and b gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters a and b, together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA algorithm. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). Let P and Q be two points on an elliptic curve such that $kP = Q$, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k,

if k is sufficiently large. k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is point multiplication.

2.2 Background

2.2.1 System Model

VANETs have three entities such as CA, RSU, and vehicle. In this model, CA is in charge of the registration of immobile RSUs at the road side and vehicles. And RSUs are subordinated by the CA, which have storage units for storing information coming from the CA and vehicles. It works like CA's gateway. Because the secure vehicular communications are mainly served for the public applications, in the most highway scenarios, RSUs are assumed to connect with the CA by wired links or any other links with high bandwidth, low delay and low bit error rates. RSUs also communicate to each other either via the CA or through a secure and reliable peer-to-peer channel. According to DSRC, the medium used for communications among nearby vehicles and between vehicle and RSU is 5.9GHz DSRC identified as IEEE 802.11p.

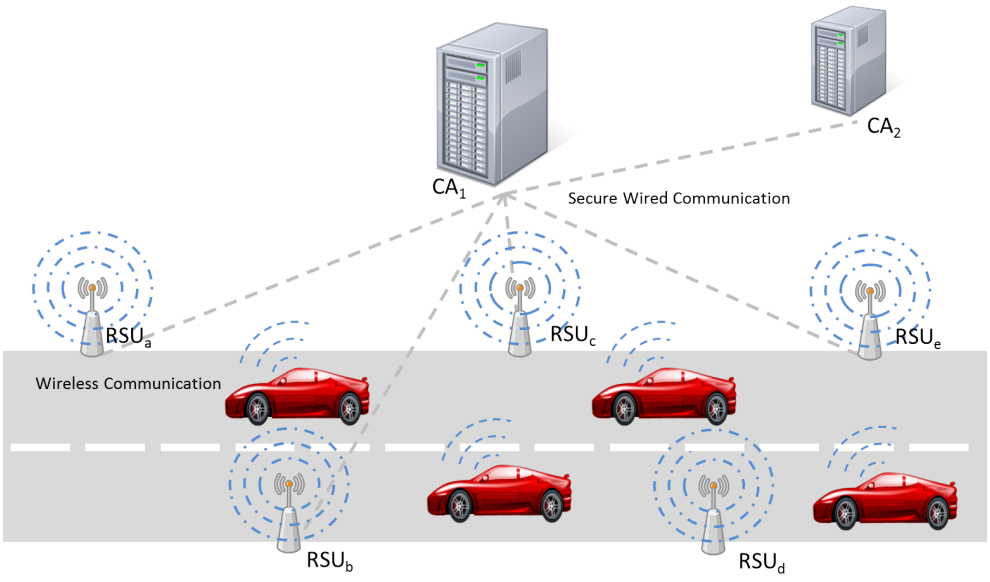

Figure 2.2: System model of VANETs

In this system, some assumptions must be made. First, CAs are fully trusted by all

parties in the system. And they are infeasible for any attacker. Second, RSUs can be captured by an attacker. If an attacker captures the RSU, the attacker can get only stored messages that can be also obtained by eavesdropping. Because of secret information of the RSU is stored in secure storage such as hardware security module, secret information isn't exposed. Even if some RSUs are captured and compromised by an attacker, the attacker cannot obtain secret information such as the key and cryptographic parameters. Third, vehicles move most of time, and could be easily compromised by a malicious attacker. Compared with the RSUs, the population of the vehicles in the system could be up to millions, whereas the number of RSUs is at most tens of thousands based on the national infrastructure construction.

2.2.2 Certificate Authority

Drawing from the analogy with existing administrative processes and automotive authorities (*e.g.*, city or state transit authorities), we assume that a large number of CAs will be instantiated. Each CA is responsible for a region (national territory, district, county, *etc.*) and manages identities and credentials of all nodes registered with it. To enable interactions between nodes from different regions, CAs provide certificates for other CAs (cross-certification) or provide foreigner certificates to vehicles that are registered with another CA when they cross the geographical boundaries of their region.

2.2.3 Node Identification

Each vehicle is registered with only one CA, and has a unique long-term identity and a pair of private and public cryptographic keys, and long-term identity and key pair are equipped with a long-term certificate. A list of vehicle's attributes and a lifetime are included in the certificate issued by the CA. The CA is also responsible for the eviction of vehicles or the withdrawal of compromised cryptographic keys via the revocation of the corresponding certificates. In all cases, the interaction of vehicles with the CA is rare and intermittent, with the roadside infrastructure acting as a gateway to and from the vehicular part of the network, with the use of other infrastructure (*e.g.*, cellular) being also possible. The in-car system and data processing functionality are discussed in [11].

2.2.4 Hardware Security Module (HSM)

A HSM is a type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signing/verifying, and for providing strong au-

thentication to access critical keys for server applications. They are physical devices that traditionally come in the form of a plug-in card or an external TCP/IP security device that can be attached directly to the server or general purpose computer. The goals of an HSM are onboard secure generation, onboard secure storage, use of cryptographic and sensitive data material, and offloading application servers for complete asymmetric and symmetric cryptography. HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. In short, they protect high-value cryptographic keys. The cryptographic materials handled by most HSMs are asymmetric key pairs and certificates used in public-key cryptography. Some HSMs can also handle symmetric keys and other arbitrary data.

Figure 2.3: Examples of HSMs

We envision that both vehicles and RSUs are equipped with HSM whose purpose is to store and physically protect sensitive information and provide a secure time base. This information is primarily private keys for signature generation. If modules were tampered with to extract private keys, the physical protection of the unit would ensure that the sensitive information (private keys) would be erased to prevent the adversary from obtaining them. In addition, the HSM performs all private key cryptographic operations with the stored keys, in order to ensure that sensitive information never leaves the physically secured HSM environment. Essentially, the HSM is the basis of trust. Without HSM, private keys could be compromised and their holders could masquerade as legitimate system nodes.

3. Our Scheme

3.1 Security Requirements

Our scheme, an efficient anonymous authentication scheme in VANETs, should achieve following requirements.

3.1.1 Authentication

The sender of the messages should be authenticated to guard against impersonation attack. And, message authentication should also be provided to protect message forgery and related attacks. Even though an attacker compromises some RSUs or vehicles, the attacker cannot forge a message and signature in a communication range of compromised RSUs or vehicles.

3.1.2 Anonymity

A real identity of vehicles should be hidden from normal message receivers except the CA during authentication process. Moreover, even if an adversary obtains stored information of compromised RSUs, the adversary cannot disclose real identities of vehicles. Anonymity must be achieved in the sense that the user related information has to be protected, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships.

3.1.3 Unlinkability

A moving route of each vehicle should be protected even if the identities are hidden, and received messages from vehicles in the authentication process should be unlinkable. RSUs should not be able to figure out the relationship between safety messages when the authentication is processed. Moreover, even though the adversary compromised RSUs, nobody can link information stored in the RSUs to track vehicles.

3.1.4 Traceability

The authority should be able to trace the sender of messages by revealing the real identity of vehicles from its pseudo identity in situation such as traffic accident, illegal activity, liability investigation, *etc.* In addition, even if multiple RSUs are compromised, the authority should be able to trace real identities of target vehicles from its pseudo identity without assistance of compromised RSUs. When malicious nodes are detected in VANETs, the traceability could be utilized to manage revocation list efficiently.

3.2 Our Scheme

In this section, we propose an efficient anonymous authentication scheme. Our scheme consists of initiation, authentication and key agreement, and conditional tracking mechanism. To design our scheme, we use a traceable ring signature with k-times anonymity as a building block and ECC. The security of ECC depends on the difficulty of ECDLP. Table 3.1 describes the notation used in our scheme, and Figure 3.1 shows our authentication protocol briefly.

Notation	**Description**
H_1, H_2, H_3	distinct hash function modeled as random oracles
G	generator point on elliptic curve E
V_i	vehicle that has index number i in a group N
R_k	RSU with identifier ID_{R_k}
GID_N	group identifier of a group N
sk_{CA}, pk_{CA}	CA's private and corresponding public key
sk_{R_k}, pk_{R_k}	R_k's private and corresponding public key
sk_{V_i}, pk_{V_i}	V_i's private and corresponding public key
PK_N	a list of public keys in a group N
K_{R_k,V_i}	short-term shared key between R_k and V_i
$Cert_{R_k}$	RSU R_k's certificate issued by the CA
Sig_{R_k}	normal signature signed by R_k using pk_{R_k}
$\widehat{Sig}_{V_i}$	traceable ring signature signed on given message by vehicle V_i
$E_K(m)$	symmetric-key encryption function with shared key K and message m

Table 3.1: Notations for our scheme

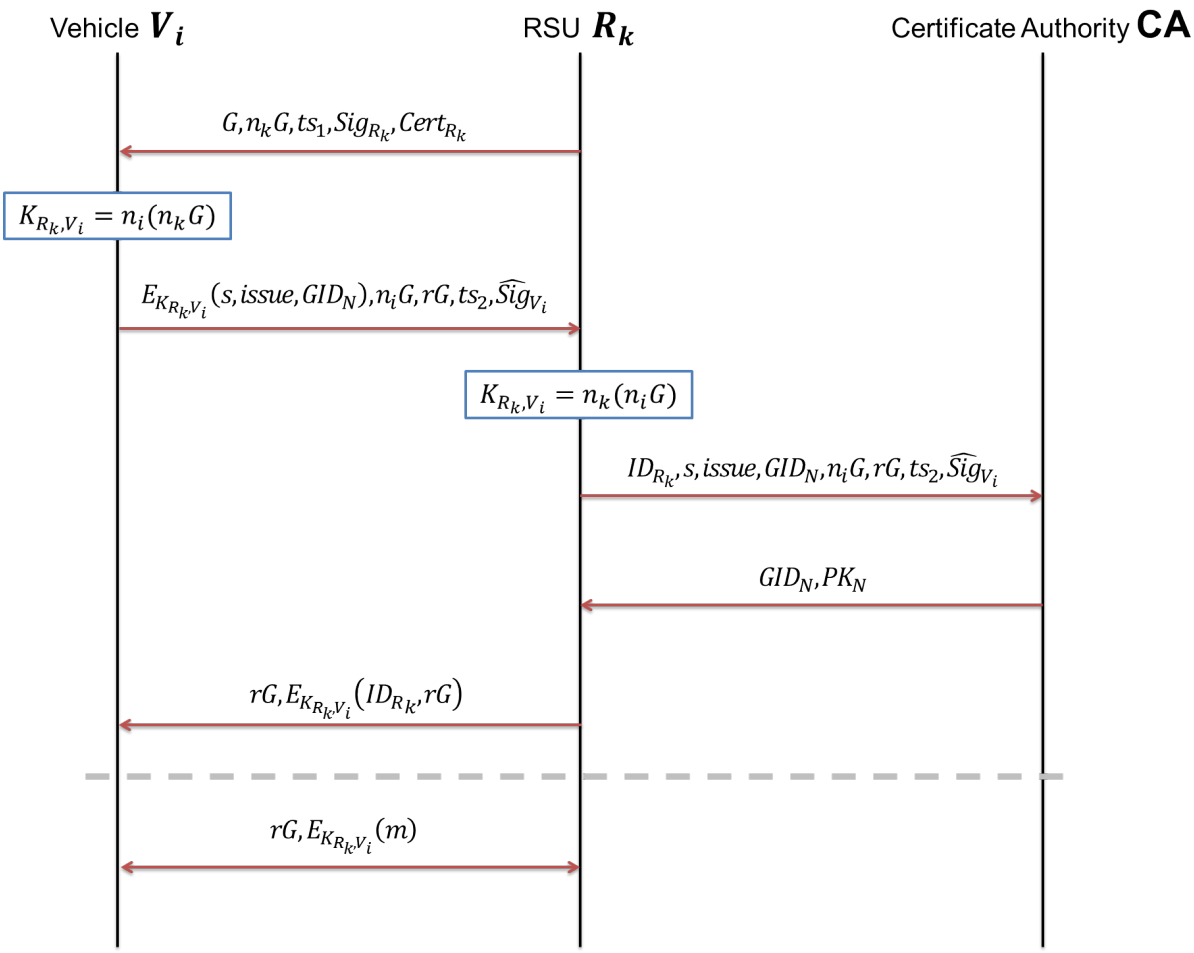

Figure 3.1: Abstract view of our authentication protocol

3.2.1 Initiation

Let E be an elliptic curve over additive group $\mathbb{G}$ of prime order q, and let G be a generator point. Let $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, and $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q$ be distinct hash function modeled as random oracles. Above parameters will be shared by all entities in VANETs.

When a vehicle V_i is registered to CA, a pair of private and public cryptographic keys (sk_{V_i}, pk_{V_i}) are equipped in vehicle's HSM. The key generator picks up random element x_i in $\mathbb{Z}_q$ and computes $y_i = x_i G$. The public key is $pk_{V_i} = y_i$, and the corresponding secret key is $sk_{V_i} = x_i$. Next V_i's public key is registered in CA on off-line. The CA classifies newly legitimate vehicle V_i into several new groups depend on the vehicle's attributes. For example, V_i will be classified into group N as $N = \{\cdots, i, \cdots\}$, and vehicle V_i keep the group identifier GID_N. The CA then makes an ordered public key list for group N as $PK_N = \{\cdots, pk_{V_i}, \cdots\}$. After generating new group and those group key lists, CA store related information of newly registered vehicle such as VIN(Vehicle Identification Number), attributes of vehicle V_i, expiration time, *etc.* In addition, RSU R_k also has its pair of private and public cryptographic keys (sk_{R_k}, pk_{R_k}). Each RSU R_k also has a public key certificate signed by the CA to prove pk_{R_k} valid. The certificate $Cert_{R_k}$ is formed as follows.

$$Cert_{R_k}=\{ID_{R_k},\, pk_{R_k},\, Expiration\ time,\, location,\, Sig_{CA}\}$$

Where Sig_{CA} denotes a signature (*e.g.*, ECDSA-160) signed on a given message using the private key of the CA.

3.2.2 Authentication and Key Agreement

To access VANETs, a vehicle should authenticate himself to a RSU.

1. The RSU R_k picks a random number $n_k \in \mathbb{Z}_q$ and computes $n_k G$ using a generator G. R_k signs on G, $n_k G$ and current timestamp ts_1 using signing algorithm. R_k then broadcasts the following beacon message.

   $$G,\, n_k G,\, ts_1,\, Sig_{R_k},\, Cert_{R_k}$$

   Each RSU will broadcast this beacon message periodically to declare service existence.

2. After receiving this beacon message, a vehicle V_i proceeds as follows.

(a) First V_i check that ts_1 is valid to prevent from the replay attack. Then, V_i verifies Sig_{CA} in $Cert_{R_k}$ using pk_{CA}, and confirm $Cert_{R_k}$ to verify public key pk_{R_k}, certificate expiration time, and location of R_k. V_i then verifies Sig_{R_k} using pk_{R_k}.

(b) V_i picks a random number n_i, computes n_iG and the short-term shared symmetric key with R_k : $K_{R_k,V_i} = n_i(n_kG)$, and encrypt $(s, issue, GID_N)$ using K_{R_k,V_i} where s is the index which is not used and will be exhausted at this time for generating signature and $issue$ can be an arbitrary string in $\{0,1\}^*$. In this system, $issue$ will be concatenation of the service identifier and the service expiration time of V_i. In addition, $issue$ can be changeable depending on the taste of CA.

(c) If all the verifications are positive, V_i believes that R_k is legitimate and executes the following:

i. First V_i picks random number $r \in \mathbb{Z}_q$ and computes rG. Then V_i finds current index s and makes message m as concatenation of n_iG, rG, and current timestamp ts_2. V_i also prepares the tag $L = \{s, issue, PK_N\}$.

ii. V_i computes $Q = H_1(L)$ and $\sigma_i = x_iQ$, using $x_i \in \mathbb{Z}_q$.

iii. V_i sets $A_0 = H_2(L, m)$ and $A_1 = i^{-1}(\sigma_i - A_0)$

iv. For all $j \neq i$ in a group N, V_i computes $\sigma_j = A_0 + jA_1 \in \mathbb{G}$. Note that every $(j, \sigma_j(Q)^{-1})$ are defined by $(0, A_0(Q)^{-1})$ and (i, x_i), where $x_i = \sigma_i(Q)^{-1}$.

v. V_i makes signature (c_N, z_N) on (L, m) depending on a non-interactive zero-knowledge proof of knowledge for the relation derived from language

$$\mathscr{L} \stackrel{\triangle}{=} \{(L, Q, \sigma_N) | \exists i' \in N \text{ such that } y_{i'}(G)^{-1} = \sigma_{i'}(Q)^{-1}\}$$

where $\sigma_N = (\cdots, \sigma_i, \cdots)$, as follows:

A. V_i picks up random $w_i \in \mathbb{Z}_q$ and sets $a_i = w_iG$, $b_i = w_iQ \in \mathbb{G}$.

B. V_i picks up at random z_j, $c_j \in \mathbb{Z}_q$, and sets $a_j = z_jG + c_jy_i$, $b_j = z_jQ + c_j\sigma_j \in \mathbb{G}$ for every $j \neq i$ in a group N.

C. V_i sets $c = H_3(L, A_0, A_1, a_N, b_N)$ where $a_N = (\cdots, a_i, \cdots)$ and $b_N = (\cdots, b_i, \cdots)$.

D. V_i sets $c_i = c - \sum_{j \neq i} c_j \ (mod\ q)$ and $z_i = w_i - c_ix_i \ (mod\ q)$. V_i then generates (c_N, z_N), where $c_N = (\cdots, c_i, \cdots)$ and $z_N = (\cdots, z_i, \cdots)$, as a proof of $\mathscr{L}$.

(d) V_i generates $\widehat{Sig}_{V_i} = (A_1, c_N, z_N)$ as the signature on (L, m).

(e) V_i sends the following back to R_k.

$$E_{K_{R_k,V_i}}(s, issue, GID_N), n_iG, rG, ts_2, \widehat{Sig}_{V_i}$$

Where $E_K(m)$ denotes encrypted message by symmetric-key encryption function (*e.g.*, AES-128) whose parameters are shared key K and message m.

3. After receiving this message from vehicle V_i, R_k carries out the following to authenticate V_i.

   (a) R_k verifies ts_2 and rG to make sure the freshness of this message from V_i.

   (b) R_k computes the short-term shared symmetric key with V_i as $K_{R_k,V_i} = n_k(n_iG)$, and decrypts $E_{K_{R_k,V_i}}(s, issue, GID_N)$.

   (c) R_k sends to CA $(ID_{R_K}, s, issue, GID_N, n_iG, rG, ts_2, \widehat{Sig}_{V_i})$, and receives response (GID_N, PK_N) from CA.

   (d) R_k parses L as $\{s, issue, PK_N\}$ and also checks s by confirming $1 \leq s \leq k$ where k is the maximum index number of V_i.

   (e) R_k verifies that $\widehat{Sig}_{V_i}$ is valid signatures as follows:

      i. R_k checks $G, A_1 \in \mathbb{G}$, $c_i, z_i \in \mathbb{Z}_q$, and $y_i \in \mathbb{G}$ for all $i \in N$. R_k sets $Q = H_1(L)$ and $A_0 = H_2(L, m)$, and compute $\sigma_i = A_0 + iA_1 \in \mathbb{G}$ for all $i \in N$

      ii. R_k computes $a_i = z_iG + c_iy_i$ and $b_i = z_iQ + c_i\sigma_i$ for all $i \in N$.

      iii. R_k verifies that $H_3(L, m, A_0, A_1, a_N, b_N) \equiv \sum_{i \in N} c_i \ (mod\ q)$, where $a_N = (\cdots, a_i, \cdots)$ and $b_N = (\cdots, b_i, \cdots)$.

      iv. If all the verifications are finished successfully, R_k believes V_i is legitimate vehicle and accepts their access to the network, otherwise rejects.

   (f) R_k sends the following back to V_i.

$$rG, E_{K_{R_k,V_i}}(R_k, rG)$$

The above protocol can authenticate explicitly each other between legitimate vehicle and RSU. In addition, it enables anonymous authentication and establish a short-term shared symmetric key K_{R_k,V_i} that will be used for the subsequence communication session. Each session is uniquely defined as (rG).

3.2.3 Conditional Tracking Mechanism

In our scheme, only CA can revoke the anonymity of the vehicle and track the target vehicle. When the CA decides the target vehicle, the CA obtains the public key of the target vehicle and real identity, and link related records as follows:

1. RSUs report the record with $(ID_{R_K}, s, issue, GID_N, n_iG, rG, ts_2, \widehat{Sig}_{V_i})$ to CA in the authentication process.
2. The CA parses L as $\{s, issue, PK_N\}$, and sets message m concatenation of n_iG, rG, and ts_2.
3. The CA sets $Q = H_1(L)$ and $A_0 = H_2(L, m)$, and compute $\sigma_i = A_0 + iA_1 \in \mathbb{G}$ for all $i \in N$. The CA also does the same computation for σ', and retrieve σ'_i for all $i \in N$.
4. For all $i \in N$, if $\sigma_i = \sigma'_i$, store pk_{V_i} in **List**, where **List** is initially an empty list.
5. If public key is the only entry in **List**, the CA can determine an identifier of the target vehicle and obtain its public key.

Since CA has the vehicle's identity, public key pair, and linked authentication records, the CA can revoke the anonymity of the target client, obtain the real identity of vehicle, and track the target vehicle. We utilize a tag-linkability [18] which is property of traceable ring signature to track the target vehicle. The tag-linkability is that every two signature generated by the same signer with the same tag are linked. Our scheme utilize k-time anonymity using index value s to provide unlinkability with traceability. So we use vehicle's real identity and public key to connect related linked records.

4. Security and Performance Analysis

4.1 Security Analysis

Our scheme, an efficient anonymous authentication protocol in VANETs, satisfies following requirements.

4.1.1 Authentication

Our scheme provides authentication of message and sender of message using signature on message, certificate, and corresponding public key. Vehicles authenticate RSUs and messages using RSU's certificate issued by the CA and RSU's signature on message. RSUs authenticate vehicles and messages verifying traceable ring signature on messages. After authentication process, messages are protected using symmetric key encryption with shared key. So, no adversary can try impersonation attack, message forgery, and related attacks. In our scheme, even though an attacker compromises some RSUs or vehicles, the attacker cannot forge a message and signature in a communication range of compromised RSUs or vehicles.

4.1.2 Anonymity

Our scheme utilizes the traceable ring signature to satisfy the anonymity of vehicle's identity. Anonymity is one of the traceable ring signature's properties. As long as a signer does not sign on two different messages with the same tag, the identity of the signer is indistinguishable from any of the possible ring members. In addition, any two signatures generated with two distinct tags are always unlinkable. Namely, it is infeasible for anyone to determine whether they are generated by the same signer. [18] shows the proof of anonymity of traceable ring signature. The used ring signature scheme is anonymous under the decisional Diffie-Hellman assumption in the random oracle model [25]. And it can be extended on ECC. CAs have only negligible advantage to determine which is client among all members in same group compared with the probability of just guessing randomly one among all members in same group.

4.1.3 Unlinkability

An eavesdropper cannot link the safety messages, because our scheme use k-times anonymity on the same tag. Any traceable ring signature scheme can be efficiently transformed into a traceable ring signature scheme with k-times anonymity, where the k-times anonymity means that a singer is allowed to sign messages with the same tag at most k times without being traced. It is simply obtained by regarding $(i, \mathbf{Sig}_{sk}((L, i), m))$ as a signature on m, with the tag L, where the verifier checks if $\mathbf{Ver}((L, i), m) = 1$ and $1 \leq i \leq k$. It is obvious that the identity of signer is not revealed if the signer is enough careful not to issue the same index twice on the same tag. Our scheme utilizes an index value s that is changeable in the tag L to provide unlinkability utilizing k-times anonymity. So, signatures generated by same vehicle with the different tag which is changeable are not linked and received messages from same vehicles in authentication process also have unlinkability. Moreover, even though the adversary compromised RSUs, nobody can link information stored in the RSUs to track vehicles.

4.1.4 Traceability

The authority can trace the sender of messages by revealing the real identity of vehicles from its pseudo identity in situation such as traffic accident, illegal activity, liability investigation, *etc.* Our scheme provides traceability using tag-linkability which is property of traceable ring signature. Anyone who creates two signatures for different message with the same tag can be traced due to tag-linkability. When the CA decides the target vehicle, the CA can revoke the anonymity of the target vehicle and obtain the real identity of vehicle, because CA stores the vehicle's identity and public key pair. CA then traces the target vehicle using tag-linkability property and real identity. In addition, even if multiple RSUs are compromised, the authority can trace real identities of target vehicles from its pseudo identity without assistance of compromised RSUs.

4.2 Performance Analysis

In this section, we evaluate the performance of the scheme. We conducted analysis of our protocol in terms of storage, computation, and communication overhead comparing with previous schemes: M. Raya *et al.*'s model [15], X. Lin *et al.*'s GSIS [16], and R. Lu *et al.*'s ECPP [17]. For the performance analysis, we estimate the required storage units, the required time for computation, and the number of message transmissions.

4.2.1 Storage Overhead

We compared the vehicle storage overhead of the our scheme with previous schemes: M. Raya *et al.*'s model, GSIS, and ECPP. In our scheme, each vehicle stores one unique private key issued by the CA. Let each key (with its certificate) occupy one storage unit. Then, since the vehicle does not need to store the revocation list, the storage overhead of our scheme is only one unit, denoted as $\mathbf{S}_{Ours} = 1$. In M. Raya *et al.*'s model, on the other hand, each vehicle should store not only its own N_{okey} anonymous key pairs, but also all the anonymous public keys and their certificates in the revocation list. Assuming that there are n vehicles being revoked, then the size of revoked anonymous public keys is $n \times N_{okey}$. The storage overhead of M. Raya *et al.*'s model increases linearly, denoted as $\mathbf{S}_{Raya} = (n+1) \times N_{okey}$. By assuming that $N_{okey} = 10^4$ as mentioned in [15], we have $\mathbf{S}_{Raya} = (n+1) \times 10^4$. In GSIS, each vehicle stores one unique private key issued by the CA, and n revoked public keys in the revocation list. So storage overhead of GSIS is denoted as $\mathbf{S}_{GSIS} = n + 1$. In ECPP, each vehicle stores one unique private key issued by the CA and short-time key pair together with its certificate issued by the RSU. Because vehicle does not need to store the revocation list, the storage overhead in ECPP of denoted as $\mathbf{S}_{ECPP} = 2$.

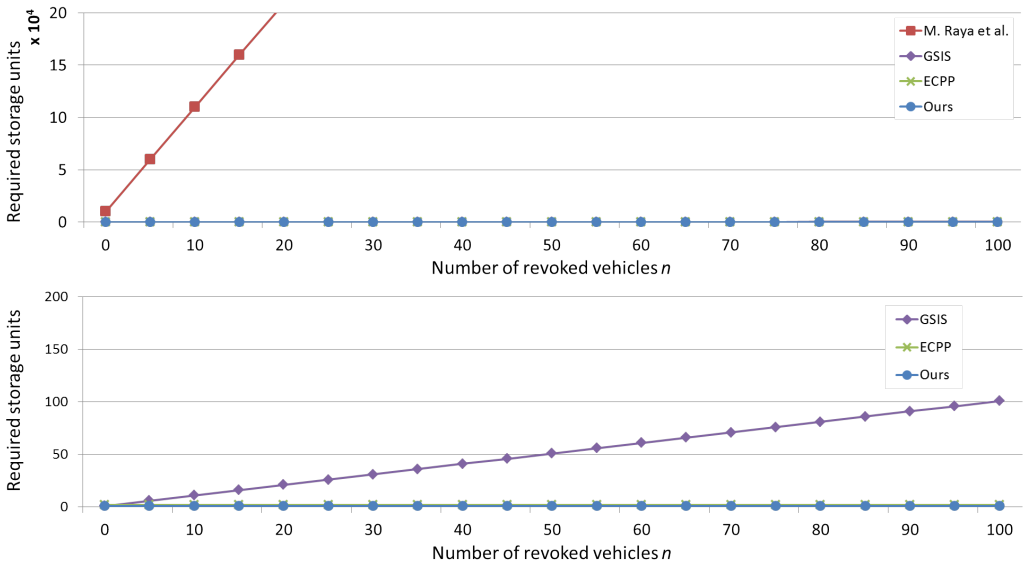

Figure 4.1: Comparison of storage overhead in different n revoked vehicles

Figure 4.1 shows the required storage units in vehicle for our scheme, ECPP, GSIS, and M. Raya *et al.*'s model as n increases, n varying from 0 to 300. We can observe that the storage overheads of M. Raya *et al.*'s model and GSIS increase linearly with the number of revoked vehicles n. Since the storage overhead of M. Raya *et al.*'s model is much larger than the storage overhead of GSIS, the storage overhead of GSIS looks like still small in spite of its linear increase with n. Therefore, it also implies that the vehicles in M. Raya *et al.*'s model and GSIS would take a long time to update their local revocation lists, which is not the case in our scheme and ECPP. The storage overhead of our scheme and ECPP are always only one and two storage units, and does not increase with the number of revoked vehicles n. Our scheme is the most efficient in terms of vehicle storage overhead, though difference is very small. In addition, ECPP does not provide unlinkability when some RSUs were compromised.

4.2.2 Computation Overhead

In this subsection, we compare the computation overhead for mutual authentication in our scheme with previous schemes: GSIS and ECPP. To investigate the performance issue, we calculate the time for computation. Since the point multiplication in $\mathbb{G}$ and pairing computations dominates each party's computation overhead, only these operations are counted in the calculation. For fairness in comparisons, we selected the same security measures of [17]. We assumed an MNT curve [26] of embedding degree $k = 6$ and $|q| = 160$ $bits$. The implementation was executed on an Intel Pentium IV 3.0 GHz machine [27].

	Description	**Execution Time**
$\mathbf{T}_{pmul}$	The time for one point multiplication in $\mathbb{G}$	0.6 ms
$\mathbf{T}_{pair}$	The time for pairing operation	4.5 ms

Table 4.1: Cryptographic operation's execution time

Table 4.1 gives the measures to estimate the computation time. The computation overhead of our scheme is changeable depending on the group size N, and some variables can be pre-computed for the optimization. For the calculation, we set $N = 10$, which can guarantee proper level of anonymity and signature length. In this case, our scheme requires $70\mathbf{T}_{pmul}$ for mutual authentication and verification of message. Let $\mathbf{T}_{Ours}$ be the required time cost in our scheme, then we have:

$$\mathbf{T}_{Ours} = 70\mathbf{T}_{pmul} = 70{\times}0.6 = 42\ ms$$

In ECPP, for mutual authentication, short-time anonymous certificate issuance, and verification of message, it requires $24\mathbf{T}_{pmul} + 9\mathbf{T}_{pair}$. Let $\mathbf{T}_{ECPP}$ be the required time cost in ECPP, then we have:

$$\mathbf{T}_{ECPP} = 24\mathbf{T}_{pmul} + 9\mathbf{T}_{pair} = 24{\times}0.6 + 9{\times}4.5 = 54.9\ ms$$

In GSIS, the time cost of verifying a safety message is related to the number of revoked vehicles in the revocation list. Let $\mathbf{T}_{GSIS}$ be the required time cost in GSIS. Assume that there are n revoked vehicles, then we have:

$$\mathbf{T}_{GSIS} = 6\mathbf{T}_{pmul} + (3+2n)\mathbf{T}_{pair} = 6{\times}0.6 + (3+2n){\times}4.5 = 3.6 + 13.5 + 9n = (17.1 + 9n)\ ms$$

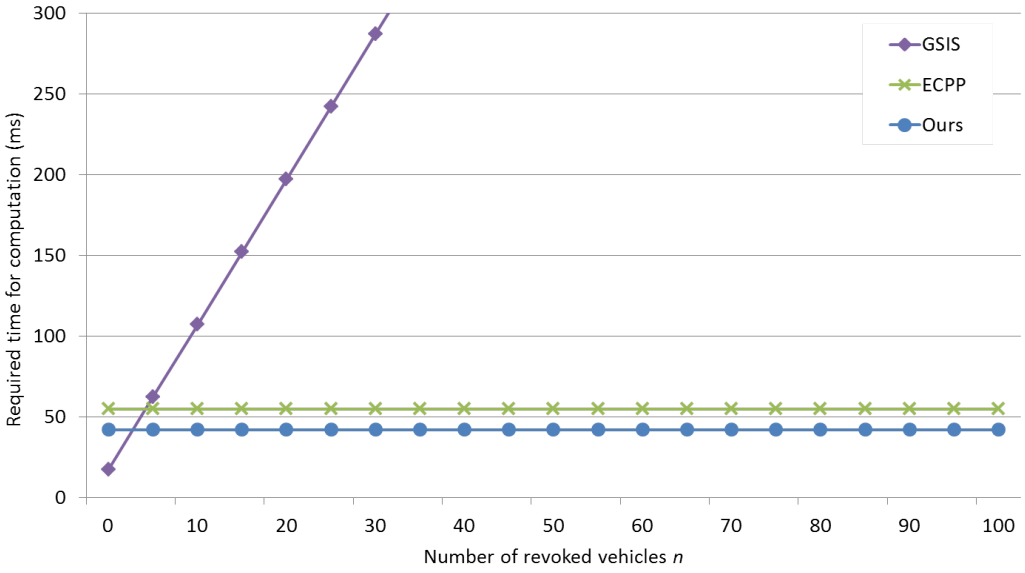

Figure 4.2: Comparison of computation overhead in different n revoked vehicles

Figure 4.2 shows the comparison of computation overhead for authentication and message verification process in our scheme, ECPP, and GSIS as the number of vehicles n increases. We can observe that the computation overhead of GSIS linearly increases with n. On the other hand, computation overheads of our scheme and ECPP are constant. But, our scheme is the most efficient in terms of computation overhead, because ECPP require more time for computation than ours, and has additional exponentiation operations.

4.2.3 Communication Overhead

In the previous subsection, we computed and compared computation overhead for mutual authentication and verification of message in our scheme, ECPP, and GSIS. In this subsection, to analyze communication overhead of our scheme, we estimate the number of message transmissions for mutual authentication and compare the required total number of message transmissions for mutual authentication and message exchanges between the vehicle which was authenticated by the RSU and the RSU which was authenticated by the vehicle in our scheme with other previous schemes: GSIS and ECPP.

	Ours	**GSIS**	**ECPP**
Vehicle	1	1	2
RSU	3	2	3
CA	1	1	1
Total	5	4	6

Table 4.2: Comparison of the number of message transmissions for mutual authentication

Table 4.2 shows the comparison of the required number of message transmissions for mutual authentication in each scheme. Each scheme has one message exchange between RSU and CA to get vehicle's group public key or confirm updated revocation list. GSIS requires only four message transmissions for mutual authentication, but it needs additional message transmissions sometimes to update revocation list. Since GSIS has same authentication process for all messages, GSIS requires $4n$ message transmissions for n times message exchanges between the vehicle which was authenticated by the RSU and the RSU which was authenticated by the vehicle. Let $\mathbf{C}_{GSIS}$ be the communication overhead of GSIS, the communication overhead of GSIS is denoted as $\mathbf{C}_{GSIS} = 4n$. On the other hand, our scheme and ECPP require $2n$ message transmissions to exchange n messages, because they use result of authentication to exchange messages. ECPP uses short-time certificate issued by the RSU and location awareness key to authenticate messages, and our scheme uses short-term shared key to authenticate and protect messages. However, ECPP and GSIS don't have message eavesdropping protection mechanism such as payload encryption. Let $\mathbf{C}_{Ours}$ and $\mathbf{C}_{ECPP}$ be the communication overhead of our scheme and ECPP, the communication overheads in our scheme and ECPP are denoted as $\mathbf{C}_{Ours} = 5 + 2n$ and $\mathbf{C}_{ECPP} = 6 + 2n$.

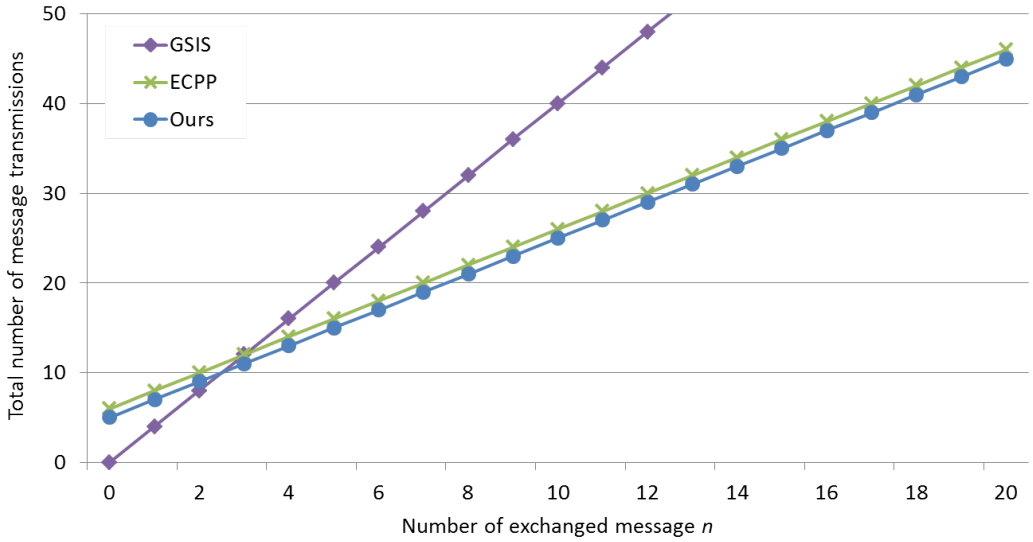

Figure 4.3: Comparison of communication overhead in different n message exchanges

Figure 4.3 shows the total number of message transmissions with growing of the number of exchanged messages n when the vehicle communicate with the same RSU. The Total numbers of message transmissions in each protocol are linearly increase with growing of n. Especially, the total number of message transmissions in GSIS increases in multiples of four, but total numbers of message transmissions in our scheme and ECPP increase in multiples of two. The difference between GSIS and the others grows with increasing of the number of message exchanges. Our scheme is most efficient in terms of communication overhead, although there is slight difference compared with ECPP.

5. Conclusion

VANETs are one of typical application of wireless communication technology, which can provide communications among nearby vehicles and between vehicles and RSUs connected infrastructure. VANETs cannot only provide a perfect way to collect dynamic traffic information, but also sense various physical conditions related to traffic distribution with very low cost and high accuracy, which have a great potential to revolutionize driving environment, and will undoubtedly play an important role in the future transportation system. However, it is clear that security and privacy enhancing mechanisms are necessary, which are in fact a prerequisite for deployment. Otherwise VANET systems could make antisocial and criminal behavior easier, in a way that would actually jeopardize the benefits of their deployment. This has been recently well understood in academia, the industry, and among authorities. And a large number of agreed efforts have been undertaken to design security architectures for VANET systems. Extensive research efforts have been made by both industry and academia to make VANETs secure.

In this thesis, we proposed a novel anonymous authentication scheme in VANETs. Our scheme guarantees authentication, anonymity, unlinkability, and traceability simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. We utilize the traceable ring signature scheme with the k-times anonymous authentication scheme to address the contradictory requirements. Our scheme also uses elliptic curve cryptosystem to achieve storage, computation, and communication efficiency. Compared with existing works, our scheme has better performance in terms of storage, computation, and communication overhead. In addition, our scheme has three advantages compared with other previous works. First, our scheme doesn't have revocation list update process in authentication process. Second, our scheme always provides unlinkability although multiple RSUs are compromised. Finally, our scheme requires only one authentication process for mutual authentication when the vehicle communicate with the same RSU, because our scheme has key agreement functionality that makes secure channel to communicate. These advantages make our scheme efficient in large-scale and busy networks like VANETs.

요 약 문

차량 애드-혹 네트워크에서의 효율적인 익명 인증 기법 연구

차량 애드-혹 네트워크는 무선 통신 기술을 활용한 대표적인 예로 근접한 차량 간의 통신과 차량과 인프라스트럭처에 연결된 RSU 사이의 통신을 지원하는 네트워크이다. 그리고 저비용 고효율로 교통정보와 도로의 물리적인 상태를 수집하고 운전자에게 최적의 경로를 안내함으로써 교통량을 분산시키고 최적의 운행 환경을 제공할 수 있도록 한다. 그렇기 때문에 차량 애드-혹 네트워크는 미래의 교통 시스템에서 큰 역할을 할 것으로 기대되고 있다. 그러나 차량 애드-혹 네트워크가 널리 이용되기 위해서는 공격자의 악의적인 공격을 막고 사용자의 개인 정보를 보호할 수 있는 기술에 대한 연구가 선행되어야 한다. 이 점은 모든 사람들이 공감하고 있으며 최근에는 많은 연구들이 진행되고 있다. 본 학위 논문에서는 차량 애드-혹 네트워크에서의 새로운 익명 인증 기법을 제안한다. 우리가 제안한 기법은 인증, 익명성, 비연결성, 그리고 추적가능성을 동시에 만족한다. 전송된 메시지들로부터 위치 정보 등의 개인정보를 유출되지 않도록 해주는 비연결성과 특정한 상황에서 지정된 기관이 목표가 되는 차량을 추적할 수 있도록 하는 추적가능성은 서로 상반되는 속성들이다. 우리는 상반되는 두 속성을 한꺼번에 만족시키기 위하여 추적 가능한 환 서명 기법과 k-times 익명 인증 기법을 이용하였으며 저장공간, 연산량, 그리고 통신량 측면에서의 효율성을 위해 타원곡선 암호시스템을 이용하였다. 우리가 제안한 기법은 기존 기법들과 비교하여 저장공간, 연산량, 그리고 통신량 측면에서 가장 효율적이며 추가적으로 기존의 기법들과 비교하여 세 가지 장점을 가지고 있다. 첫 번째는 인증과정에서 폐기목록의 업데이트 과정이 없어서 더욱 빠른 인증이 가능하다. 두 번째는 복수의 RSU가 공격자에 의해 탈취되더라도 비연결성을 지원하여 불법적인 위치 추적이 불가능하다. 세 번째는 키 합의 기능을 포함하고 있기 때문에 차량이 같은 RSU와 여러 번의 통신을 필요로 하는 경우에도 안전한 통신을 위해 한 번의 상호 인증과정만을 필요로 한다. 이 세 가지 장점은 우리가 제안한 기법이 차량 애드-혹 네트워크와 같이 빈번한 통신이 발생하는 큰 규모의 네트워크에서 기존 기법들보다 효율적으로 동작하도록 해준다.

References

[1] *"Dedicated Short Range Communications (DSRC)"*, Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] L. Morgan, *"Notes on DSRC and WAVE Standards Suite, Its Architecture, Design, and Characteristics"*, IEEE Communications Surveys & Tutorials, 2010.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, *"Security in Mobile Ad Hoc Networks: Challenges and Solutions"*, IEEE Wireless Communications, Vol. 11, Issue 1, pp. 38-47, 2004.

[4] F.Y. Wang, D. Zeng, and L. Yang, *"Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update"*, IEEE Pervasive Computing, Vol. 5, Issue 4, pp. 68-69, 2006.

[5] M. Raya, *"The Security of Vehicular Ad Hoc Networks"*, in Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 11-21, Alexandria, VA, USA, November 2005.

[6] M. Raya, P. Papadimitratos, and J.P. Hubaux, *"Securing Vehicular Communications"*, IEEE Wireless Communications, Vol. 13, Issue 5, pp. 8-15, 2006.

[7] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, *"Securing Vehicular Communications - Assumptions, Requirements, and Principles"*, in Proc. of ESCAR 2006, pp. 5-14, Berlin, Germany, November 2006.

[8] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho, and X.S. Shen, *"Security in Vehicular Ad Hoc Networks"*, IEEE Communications Magazine, Vol. 46, Issue 4, pp. 88-95, 2008.

[9] P. Papadimitratos, A. Kung, F. Kargl, Z. Ma, M. Raya, J. Freudiger, E. Schoch, T. Holczer, L. Buttyan, and J.P. Hubaux, *"Secure Vehicular Communication Systems: Design and Architecture"*, IEEE Communications Magazine, Vol. 46, Issue 11, pp. 100-109, 2008.

[10] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, *"Certificate Revocation List Distribution in Vehicular Communication Systems (short paper)"*, in Proc. of the 5th ACM International Workshop on VANET, San Francisco, CA, USA, September 2008.

[11] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, *"Secure Vehicular Communications: Implementation, Performance, and Research Challenges"*, IEEE Communications Magazine, Vol. 46, Issue 11, pp. 110-118, 2008.

[12] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, *"Adaptive Privacy-Preserving Authentication in Vehicular Networks"*, in Proc. of IEEE International Workshop on Vehicle Communication and Applications, October 2006.

[13] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, *"Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks"*, in Proc. of the 8th International Symposium on Autonomous Decentralized Systems (ISADS 2007), pp. 344-351, Sedona, AZ, USA, March 2007.

[14] C. Zhang, R. Lu, P.H. Ho, and A. Chen, *"A Location Privacy Preserving Authentication Scheme in Vehicular Networks"*, in Proc. of WCNC 2008, pp. 2543-2548, 2008.

[15] M. Raya and J.P. Hubaux , *"Securing Vehicular Ad Hoc Networks"*, Journal of Computer Security, Vol. 15, Issue 1, pp. 39-68, 2007.

[16] 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, Issue 6, pp. 3442-3456, 2007.

[17] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, *"ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications"*, in Proc. of INFOCOM 2008, pp. 1229-1237, April 2008.

[18] E. Fujisaki and K. Suzuki, *"Traceable Ring Signature"*, PKC 2007, LNCS 4450, pp. 181-200, 2007.

[19] I. Teranishi, J. Furukawa, and K. Sako, *"k-Times Anonymous Authentication"*, Advances in Cryptology - ASIACRYPT 2004, LNCS 3329, pp. 308-322, 2004.

[20] N. Koblitz, *"Elliptic Curve Cryptosystems"*, Mathematics of Computation, Vol. 48, No. 177 pp. 203-209, 1987.

[21] R. Rivest, A. Shamir, and Y. Tauman. *"How to Leak a Secret"*. Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, pp. 552?565, 2001.

[22] D. Chaum and E. van Heijst, *"Group Signatures"*, Advances in Cryptology - EUROCRYPT 1991, LNCS 576, pp. 257-265, 1991.

[23] A. Shamir, *"Identity-Based Cryptosystems and Signature Schemes"*, Advances in Cryptology - CRYPTO 1984, LNCS 196, pp. 47-53, 1984.

[24] D. Boneh and H. Shacham, *"Group Signatures with Verifier-Local Revocation"*, in Proc. of ACM CCS 2004, pp. 168-177, 2004.

[25] M. Bellare and P. Rogaway, *"Random Oracles are Practical: A Paradigm for Designing Efficient Protocols"*, in Proc. of ACM CCS 1993, pp. 62-73, November 1993.

[26] A. Miyaji, M. Nakabayashi, and S. Takano, *"New Explicit Conditions of Elliptic Curve Traces for FR-Reduction"*, IEICE Transactions on Fundamentals, Vol. E84-A, Issue 5, pp. 1234-123, 2001.

[27] M. Scott, *"Efficient Implementation of Cryptographic Pairings"*, Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscottsamos07.pdf

감 사 의 글

이 논문을 완성하기까지 주위의 많은 분들께서 도움을 주셨습니다. 도움을 주신 모든 분들께 감사드립니다. 김광조 교수님께서는 틈틈히 연구 상황을 확인해 주셔서 체계적인 연구방향을 세울 수 있었습니다. 그리고 암호와 정보보호 연구실에서 함께 연구실 생활을 한 선후배님 (현록이형, 규석이형, 진이형, 장성이형, Duc, Divyan, 혜란누나, 혜원이, 승목이형, 임성이형, 명한이형, Made, 도영이, 이재) 들에게 연구실 생활 및 연구 등 많은 부분에서 격려 및 도움을 받았습니다. 바쁘신 와중에 학위논문심사를 위해 참석하셔서 진심어린 조언을 주신 윤현수 교수님과 이동만 교수님께도 감사드립니다. 끝으로 오늘의 제가 있게 해주신 우리 가족, 어머니와 아버지께 감사드립니다. 저의 이 작은 결실이 그 분들께 조금이나마 보답이 되기를 바랍니다.

이 력 서

이 름 : 임 준 현

생 년 월 일 : 1986년 5월 24일

주 소 : 경기도 고양시 덕양구 행신동 785 소만마을 611동 903호

E-mail 주 소 : junhyunv@kaist.ac.kr

학 력

2002. 3. – 2005. 2. 한국디지털미디어고등학교 해킹방어과

2005. 2. – 2009. 2. 연세대학교 컴퓨터과학과 (B.S.)

2009. 2. – 2011. 2. 카이스트 전산학과 (M.S.)

경 력

2007. 12. – 2008. 2. (주)SOVICO 음향기술연구소 인턴연구원

2010. 7. – 2010. 8. LG 유플러스 기술연구원 응용기술연구팀 인턴연구원

연 구 업 적

1. 박혜원, 문혜란, **임준현**, 김광조, "애드 혹 네트워크에서의 복수 그룹을 고려한 ID 기반 그룹키 합의 프로토콜", Proc. of CISC-S'09, pp. 406-410, 2009.6.19, 강원대학교, 삼척.
2. **Junhyun Yim**, Imsung Choi, and Kwangjo Kim, "An Efficient Anonymous Authentication Protocol in Vehicular Ad-hoc Networks", The 10th International Workshop on Information Security Applications (WISA 2009), Aug. 24-26, 2009, Busan, Korea.
3. Sungmok Shin, **Junhyun Yim**, and Kwangjo Kim, "Authenticated and DoS-Resilient Channel Assignment Mechanism for Wireless Mesh Networks", Symposium on Cryptography and Information Security 2010 (SCIS 2010), Jan. 19-22, 2010, Kagawa, Japan.
4. **임준현**, 한규석, 김광조, "ZigBee WPAN에서의 안전한 키 관리기법과 인증 프로토콜", Proc. of CISC-S'10, pp. 249-254, 2010.6.18, POSTECH, 포항.