A Scalable Privacy-preserving Authentication Protocol for Secure Vehicular Communications

Zeen Kim, Jangseong Kim, Doyoung Chung, Kwangjo Kim
Department of Information and Communications Engineering, KAIST, Korea
{zeenkim,jskim.withkals,wordspqr,kkj}@kaist.ac.kr
Taeshik Shon
Division of Information and Computer Engineering,
College of Information Technology, Ajou University,
Suwon 443-749, Korea, Corresponding author
tsshon@ajou.ac.kr

Abstract

In this paper, we provide the first scalable privacy-preserving authentication protocol for VANETs without participation of the nearby RSU. Existing authentication methods for VANETs require the participation of the nearby RSUs. So, bottleneck problem can be occurred as increasing the number of vehicles. Also, the time delay to authenticate the nearby vehicle will increase. In order to minimize the participation of the nearby RSU, we propose a verification of the authenticated vehicle, which only requires two modular exponentiations. Our verification methods uses homomorphic encryption algorithm and keyword searching on encrypted data algorithm as cryptographic tools. Through this verification, the vehicle i can verify whether the nearby vehicle j is authenticated by the nearby RSU. As a result, our solution overcomes the inefficiency and bottleneck problem of previous approaches. Our construction of privacy-preserving authentication for VANETs provides better transmission delay between nearby RSU and vehicle.
Keywords : authentication, privacy-preserving, vehicular communication, VANET

1 Introduction

A Vehicular Ad-hoc NETwork (VANET) is a type of Mobile Ad-hoc NETwork (MANET) that is used to provide communications among the nearby vehicles, and between vehicles and fixed infrastructure on the roadside. VANET allows a driver in the vehicle to collect dynamic traffic information and sense various physical conditions related to traffic distribution with very low cost and high accuracy. Since VANET has a great potential to revolutionize driving environment and will undoubtedly play an important role in the future transportation system [1], we should address security and privacy problems in the VANET.

We can classify the communications in VANET into Vehicle-TO-Vehicle (V2V) and Vehicle-TO-Infrastructure (V2I). V2V indicates the communications between On-Board Units (OBUs) in vehicles while Vehicle-TO-Infrastructure (V2I) denotes the communications between OBUs and Road-Side Units (RSUs), which is fixed equipment on the road. Through V2I communication, the driver in a vehicle can identify the road condition, the road traffic, and the estimated time to the destination. Since the nearby vehicles can propagate the emergency warning message to the driver's vehicle by V2V, 60% roadway collisions can be avoided [9].

Figure 1 shows the typical system architecture consisting of vehicle, RSU, and Certificate Authority (CA). The vehicle A communicates with the CA through the nearby RSU. The RSU gathers the communication messages within its communication range and forwards them to the CA. To support sufficient bandwidth, the RSU should have wireless communication capability such as 3GPP. In addition, the RSU has the permanent power supply in order to satisfy scalability and easy maintenance. Because the battery-powered RSU may not available in case of emergency due to the numerous accesses of the nearby vehicles. Also, frequent battery replacement causes more maintenance cost. That's why the RSU has the permanent power supply. The CA, believed to be trusted third party.

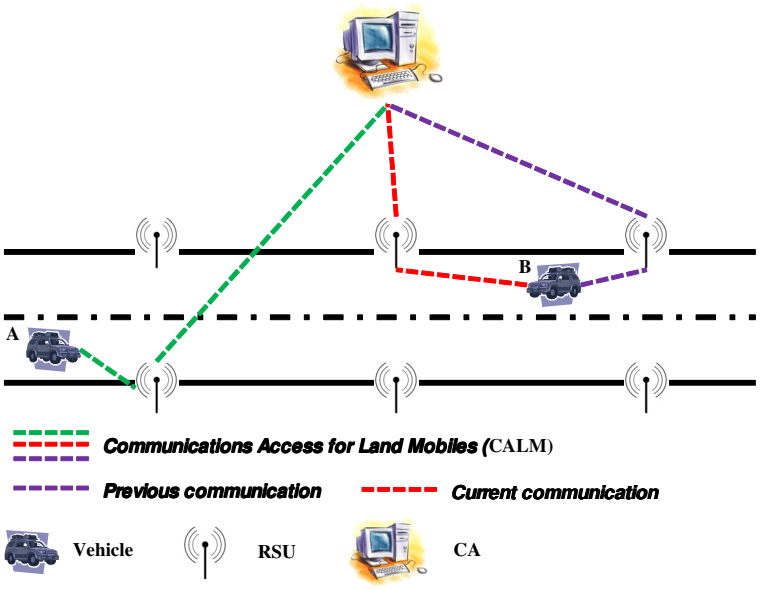

Figure 1: System architecture

To provide the privacy of the drivers in VANET (Vehicular Ad-hoc Network), various anonymous authentication protocols [2, 3, 4] have been proposed. However, these protocols can allow the target vehicle to communicate with the nearby vehicles through the trusted authority. As the number of the vehicles in certain location area increases, these protocol may suffer the bottleneck problem in the nearby RSUs. For instance, during lunar holidays in Asian countries, as

the Asian people visit their hometown using public transportation (*i.e.*, car and train), the traffic on highways is heavy. Due to the number of vehicles in the certain area, the nearby RSUs cannot support the numerous number of authentication requests. Also, the time delay to authenticate the nearby vehicle will increase.

Recently there are several approaches which solve the security weakness in ad-hoc networks and heterogeneous wireless sensor networks [5, 6, 7]. But these results cannot be applied to VANET in direct.

Our contribution

In this paper, we propose a scalable privacy-preserving authentication protocol for secure vehicular communications. Through the verification of the service subscribers, the proposed authentication protocol allows the vehicle A to authenticate itself to the nearby vehicles without any participation of the nearby RSU. If the vehicle A has authenticated with the nearby RSU, the vehicle can obtain the token, authenticating the vehicle to the nearby vehicles, from the CA. The verification of the service subscribers enable the nearby vehicles to verify whether the vehicle A has valid token or not. Therefore, the nearby vehicles can check whether the vehicle A has authenticated with the nearby RSU or not. Compared to the previous approaches [3, 4], the proposed protocol reduces computational overhead in V2V authentication process in order to support better scalability.

Organization

The remainder of this paper is organized as follows: A brief survey on the related work is conducted in Section 2, and our proposed scheme is presented in detail in Section 3. Section 4 analyzes the security and performance of our scheme and gives a comparison with previous work. Finally, we summarize and conclude our paper in Section 5.

2 Related work

In this section, we give some preliminaries of our work. At first, we summarize previous work for authentication in VANETs. We also give a brief introduction of cryptographic tools which are used in our scheme, BGN encryption and a keyword search on encrypted data.

2.1 Privacy-preserving authentication protocols for VANETs

Lin *et al.* [2] proposed a secure and privacy-preserving protocol for vehicular communications, called GSIS which is based on group signature [10] and identity-based signature [11]. While guaranteeing anonymity, confidentiality, and other security primitives, the GSIS can provide traceability of each vehicle. Only if any dispute happens, the identity of the message sender will reveal. In order to provide V2V communication between the vehicle A and nearby vehicles, the GSIS employs the group signature. The identity-based signature scheme is

used to sign each message sent by each RSU for ensuring its authenticity. However, when the adversary compromises many of the RSUs, the adversary can track any movement of the target vehicle.

Lu *et al.* [3] proposed an efficient conditional privacy preservation protocol for secure vehicular communications, called ECPP, which issues on-the-fly short-time anonymous certificate to vehicles by using a group signature scheme. 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 strong assumption that most RSUs will not disclose any internal 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 can trace 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.

In 2009, Yim *et al.* [4] proposed a anonymous authentication scheme in VANETs. The proposed scheme guaranteed authentication, anonymity, unlinkability, and traceability simultaneously. The unlinkability which enables privacy preservation and the traceability which enables conditional tracking are contradictory. Yim *et al.*'s protocol utilize the traceable ring signature scheme with the k-times anonymous authentication scheme to address the contradictory requirements. In addition, the proposed scheme has three advantages compared with other previous works. First, the scheme does not have revocation list update process in authentication process. Second, the scheme always provides unlinkability although multiple RSUs are compromised. Finally, the scheme requires only one authentication process for mutual authentication when the vehicle communicate with the same RSU, because proposed scheme has key agreement functionality that makes secure channel to communicate. These advantages make Yim *et al.*'s scheme efficient in large-scale and busy networks like VANETs.

2.2 BGN encryption

In 2005, Boneh *et al.* proposed a new homomorphic encryption scheme supporting unlimited modular additions and one modular exponentiation on encrypted data. The proposed encryption scheme enables one entity to evaluate the encrypted data without revealing the content of encrypted data. We review the BGN encryption scheme in brief.

In BGN encryption, all operations are done on two cyclic groups G and G_1 with the same order $n = q_1 q_2$, where q_1 and q_2 are two large prime numbers. The public key PK_{BGN} is g and $h = g^{\mu q_2}$ under the group G, where g is random generator and μ is a random integer in the group G. The encryption of m_i, $m_i + m_j$, and $m_i m_j$ can be computed as $g^{m_i} h^{r_i}$, $g^{m_i} h^{r_i} g^{m_j} h^{r_j}$, and $e(g^{m_i} h^{r_i}, g^{m_j} h^{r_j})$ where T is a non-zero random number less than q_2, $m_i \in \mathbb{Z}_T$ be i^{th} message, r_i is i^{th} random number, and e is a bilinear mapping from $G \times G$ to G_1, respectively. The expected decryption time using Pollard's lambda

Table 1: Notations

CA / RSU / V	Certificate Authority / Road-Side Unit / Vehicle
$Credential$ / ID_A / n	A ticket for entity authentication / An identifier of entity A / A user's access frequency
$CertA$ / VSS	A certificate that binds entity A with A's public key / Verification of the service subscriber
MT	A ticket for VSS which indicates subscribers of the target SP
PK_A / SK_A	A public key of entity A / A private key of entity A
PK_{BGN}	A public key under BGN encryption scheme [13] owned by AS
S	A set of selected numbers where $\mid S \mid \geq 2n$
SID	A service type identifier describes a selected subset of the available service pool and includes an polynomial identifier for membership test
SK_{BGN}	A private key under BGN encryption scheme [13], which is owned by AS and distributed to DS for membership test
C^i or C_A^i, $i = 0, 1, \cdots$	A series of authorized credentials by entity A
j^i or j_A^i, $i = 1, 2, \cdots$	A series of a user's number selections by entity A
$K_{A,B}$	Shared secret key between entities A and B
$E\{m, K_A\}$	A message m is encrypted by a symmetric key K_A
$E[m, PK_A]$ or $D[m, SK_A]$	A message m is encrypted by an entity A's public key or signed by an entity A's private key
$E[m, PK_{BGN}, G]$	A message m is encrypted by the public key PK_{BGN} on cyclic group G and the ciphertext is g^m
$H(m)$	A hash value of message m using SHA-1 or other cryptographic strong hash functions
R^i or R_A^i, $i = 1, 2, \cdots$	A series of nonces generated by entity A where $\mid R^i \mid \geq$ 64-bit.

method is $\tilde{O}(\sqrt{\mid T \mid})$ although the authentication server has the private key, $SK_{BGN} = q_1$.

3 Our protocol

In this section, we explain our protocol consisting of vehicle registration, V2I authentication, and V2V authentication in detail. In order to reduce the computational overhead in V2I authentication and V2V authentication, we proposed the verification of the authenticated vehicle. This idea is based on the following fact: When the vehicle A has authenticated itself with the CA, the vehicle and CA can share the secret information. Hence, the nearby vehicles can verify whether the vehicle A has been authenticated with the base station or not.

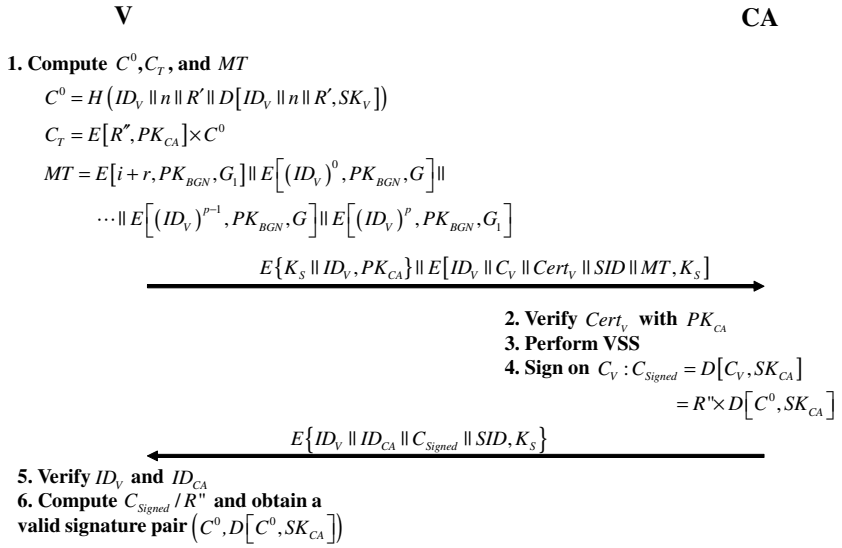

Figure 2: Vehicle registration

Before describing our protocol, we summarize our notations used throughout this paper in Table 1.

We assume that a driver can control the source addresses of the outgoing Medium Access Control (MAC) frames since this assumption is a prerequisite for anonymous communications. A detailed method for this modification is covered by Gruteser *et al.* [15]. The CA issues SID, a polynomial $f(x)$ with degree p, access key ak_i, $E[i + r, PK_{BGN}, G_1]$, and ID_i to a driver i. Using the received information, the driver i can generate his/her MT. The CA stores the coefficients of the given polynomial $f(x)$, (i.e., a_0, $\cdots$, a_p), in its database after encrypting the coefficients using BGN encryption [13]. The administrator in the CA cannot obtain any relationship between the authorized credential and driver A. That's why the CA encrypts the coefficients of the given polynomial $f(x)$. Finally, PK_{CA}, ID_{CA}, PK_{BGN}, and SK_{BGN} are assumed to be known to all entities.

3.1 Verification of the authenticated vehicle

Using the idea used in keyword search on encrypted data, we can preserve the privacy of the driver A while allowing the driver B to authenticate the driver A without any help of the nearby RSUs. Since the driver A should submit the proper trapdoor with the encrypted identifier, the verifier (*i.e.*, RSUs or CA) can compare the computation result with the verification value. If the result is the same as the verification value, the verifier believes that the end-user has proper access permission on the service. Note that anyone can take a role of the verifier in keyword search on the encrypted data if the entity knows the stored vale and PK_{BGN}. Using this novel property, we can allow B can authenticate the other driver A without communicating with the nearby RSUs. However, in the existing approach by Kim *et al.*, the verifier requires $(p + 1)$ pairing

operations where p is the number of the service subscribers. As the number of the nearby vehicle increase, the verification time will be increased.

3.1.1 Authorized token Generation phase

To address the above problem, we employ the following approach. When the nearby RSU receives the authentication request of a driver A, the RSU forwards the request and R_{RSU} to the CA. If the driver is a legitimate entity, having proper access permission on the service, the CA issues the verification value $E[\gamma, PK_{BGN}, G]$ and trapdoor $E[R_{RSU} + \beta, PK_{BGN}, G]$ to the vehicle. Note that $\gamma = \beta + R_{RSU}$. The verification value and trapdoor are encrypted by PK_{BGN} so that only the CA knows the exact value. By sending $E[-R_{RSU} + \beta, PK_{BGN}, G]$, the driver can authenticate himself/herself to the other drivers.

3.1.2 Verification phase

If the other drivers have been authenticated with the nearby RSU, they should have $E[\gamma, PK_{BGN}, G]$. Using the received information, R_{RSU} and β, the other drivers can verify whether the drive A has been authenticated by the nearby RSU.

Then, the nearby vehicles performs the following steps:

1. Set V to $E[-R_{RSU} + \beta, PK_{BGN}, G]$.
2. If $V^{SK_{BGN}} = (E[\gamma, PK_{BGN}, G])^{SK_{BGN}}$, return TRUE.
3. Return FALSE.

According to the property of BGN encryption, V is the same as $g^{-R_{RSU}+\beta}h^{r_1}$ $= g^{-R_{RSU}+\beta+\mu q_2}$. Similarly, $(E[\gamma, PK_{BGN}, G])$ is $g^{\gamma}h^{r_2} = g^{\gamma+\mu q_2}$. Note that μ is a random integer less than n and q_2 is a large prime number where the order n of the given group G is $q_1 q_2$. By computing modular exponentiation $SK_{BGN} = q_1$, $V^{SK_{BGN}} = g^{-R_{RSU}+\beta}$. As a result, the driver B can identify whether the driver A has authenticated with the nearby RSU. This idea will be used to support V2V authentication.

3.2 Vehicle registration

In vehicle registration phase, each vehicle register its credential with the CA. Only if the driver of the vehicle belongs to one of the service subscribers, indicating that the driver has valid certificate issued by the CA and proper access permission on the service, the CA authorizes the received credential. In order to verify proper access control on the service, we employ Verification of the Service Subscribers (VSS), which is proposed by Kim *et al.*. If the driver has his/her identifier and valid access permission, $E[i + r, PK_{BGN}, G]$, VSS returns the index of the driver among the legitimate service subscribers. To illustrate VSS, let assume that $f(x)$ is the polynomial representation of the given legitimate service subscribers. The evaluation result of $f(ID_V)$ will be $-r$ if ID_V is an identifier of the legitimate service subscribers. Using $f(ID_V)$ and $i + r$, the CA can verify that the driver is one of the legitimate service subscribers without identifying the driver.

The driver A of the vehicle computes initial credential C^0 using his/her vehicle registration number ID_V, access frequency n, random number R'. This credential will be used to prove whether the driver A has valid ID_V, Certificate and SK_v. Without knowing SK_v and ID_v, the malicious driver cannot generate the above credential. For VSS, the driver A generate $MT = E[i + r, PK_{BGN}, G_1]||E[(ID_V)^0, PK_{BGN}, G]||\cdots||E[(ID_V)^{p-1}, PK_{BGN}, G]\,||E[(ID_V)^p, PK_{BGN}, G_1]$.

In order to verify whether the driver A is one of the legitimate service subscribers, the CA performs the following steps:

1. Set $z = 1$.
2. Compute $C = \prod_{n=1}^{p-1} e(E[a_n, PK_{BGN}, \mathbb{G}]\ , E[(ID_V)^v, PK_{BGN}, \mathbb{G}])$.
3. Compute $C' = C \cdot E[a_0, PK_{BGN}, \mathbb{G}_1] \cdot E[(ID_V)^t, PK_{BGN}, \mathbb{G}_1]\ \cdot E[i + r, PK_{BGN}, \mathbb{G}_1]$
4. Repeat the following steps until $z \leq p$.
   (a) If $C'^{(SK_{BGN})} = e(g, g)^{(z \cdot SK_{BGN})}$, return z.
   (b) z = z + 1
5. Return 0.

Using $f(x) = a_t \cdot x^t + a_{t-1} \cdot x^{t-1} + \cdots + a_1 \cdot x + a_0$ and the homomorphic properties of the BGN encryption scheme, we can change $\prod_{v=1}^{t-1} e(E[a_v, PK_{BGN}, \mathbb{G}]$, $E[(w_j)^v, PK_{BGN}, \mathbb{G}])$ to C in the above procedure. Assuming that a_t and a_0 are both 1, C' in the above step (3) is the same as $E[i + r, PK_{BGN}, G_1] \cdot E[f(ID_V), PK_{BGN}, G_1] = E[(i + r) + f(ID_V), PK_{BGN}, G_1]$. If the driver is one of the legitimate service subscribers, the above computation $E[(i + r) + f(ID_V), PK_{BGN}, G_1] = E[i, PK_{BGN}, G_1]$. Therefore, the CA can verify that the driver has proper access permission without identifying the driver. Only if the driver has proper access permission, the CA signs on C_V. As applying blind signature technique [16] to C_V, the CA cannot identify C^0. The detailed procedure is illustrated in Figure 2.

To verify whether the driver A has proper certificate $Cert_V$, its corresponding private key SK_V, and MT, the CA can request the driver A to send $D[C_T||K_S, SK_V]$. Because the legitimate driver A, having proper SK_V and performing vehicle registration, only can generate $D[C_T||K_S, SK_V]$. Although this approach can allow the CA to distinguish the received registration request with the eavesdropped registration request, this approach requires additional computation and communication overhead. When the CA receives the frequent vehicle registration from the same driver A, we recommend this approach.

3.3 V2I Authentication

In V2I authentication phase, the vehicle authenticates itself by sending the one-time credential, authorized by the CA, to the nearby RSU. We adopt entity authentication in [14], since the approach supports various security features (*i.e.*, mutual authentication, non-linkability, and enhanced level of security) with less computational overhead and communication cost. Figure 3 depicts this phase.

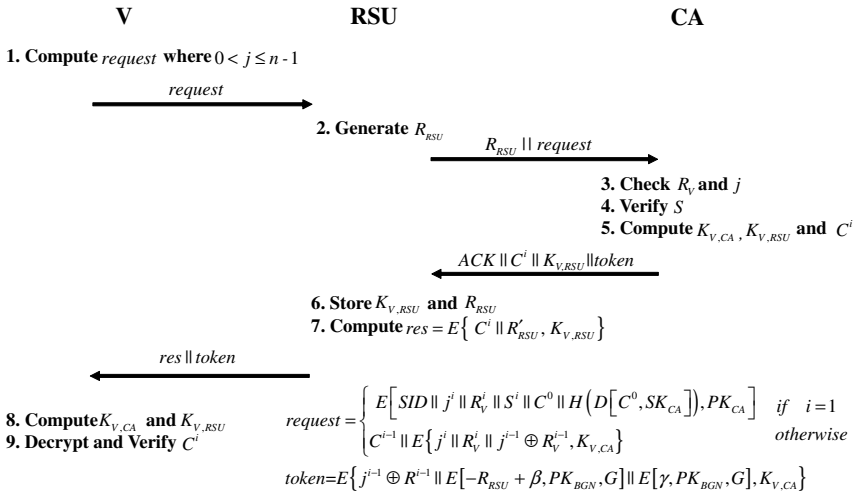

Figure 3: V2I Authentication

In the V2I authentication, each entity establishes $K_{V,AS}$ and $K_{V,RSU} = H(K_{V,CA}||C^i||R_{RSU})$.

$$K_{V,CA} = \begin{cases} H(C^0||PK_{CA}||R^1||j^1||SID) & \text{if } i = 1 \\ H(C^0||C^{i-1}||SID) & \text{otherwise} \end{cases}$$

To provide accountability of the authorized credential, we adopt a set of selected numbers S, which is l-bit array. In the first access request, a vehicle generates the set randomly. Whenever sending an i^{th} authentication request, the vehicle generates a fresh nonce R^i_{Entity} and selects one random number j between 0 to $l-1$ until $j-th$ value of S is 0. Since the set is only known to the vehicle and CA, the adversary without knowing S cannot generate the authentication request. Therefore, we believe that our protocol can enhance security level. Note that $C^i = H(C^0||j^i||R^i)$. For V2I authentication, the CA performs the following verification procedure:

1. 1^{st} request: After decrypting the request message, the CA computes $H(D[C^0, SK_{CA}])$ and compares the result with the received $H(D[C^0, SK_{CA}])$. Only if the result is same, the CA believes that the entity has an authorized credential and computes $C^1 = H(C^0||j^1||R^1)$ and stores SID, S^1, C^0, and C^1 in the database. Otherwise, the CA discards the request.

2. i^{th} request: The CA finds C^0, $S^{(i-1)}$ and SID in the database using the received $C^{(i-1)}$ and decrypts the received message with $K_{V,CA}$. Next, the CA verifies that the entity has the same set of selected numbers and j^i is not in the set. Only if the result is correct, the CA stores the received C^i and S^i. Otherwise, the CA discards it. If the entity is a legal one with proper access permission, C^i and S^i are stored in the database. As a result, the CA can verify whether the entity has an authorized credential using the received $C^{(i-1)}$.

When the vehicle is a legitimate entity, the CA issues trapdoor $E[-R_{RSU} + \beta, PK_{BGN}, G]$ and $E[\gamma, PK_{BGN}, G]$ to the vehicle. Based on the received acknowledge, the nearby RSU receives sends $E\{C^i||R'_{RSU}, K_{V,RSU}\}$ and the proper *token*, to the vehicle. *token* consists of $E\{j^{i-1} \oplus R^{i-1} \ ||E[-R_{RSU} + \beta, PK_{BGN}, G] \ ||E[\gamma, PK_{BGN}, G], K_{V,CA}\}$. Since $E[-R_{RSU} + \beta, PK_{BGN}, G]$ and $E[\gamma, PK_{BGN}, G]$ are encrypted by the shared key with the vehicle $K_{V,CA}$, only the legitimate vehicle can obtain this information. Note that the CA generates β and γ which have the relation as $-R_{RSU} + \beta = \gamma$. In order to support non-linkability, the nearby RSU should generates a random R_{RSU} to each vehicle. Therefore, the CA should generate different β so that the same group has the same γ. This property can allow us to support numerous vehicles in the same group while reducing the computation and communication cost for VSS. From this point, we believe that our protocol can satisfy scalability requirement.

3.4 V2V Authentication

In V2V authentication phase, the vehicle m sends its $TICKET_m$ to the nearby vehicle n. Using $E[-R_{RSU} + \beta, PK_{BGN}, G]$, the vehicle n verifies whether the vehicle m has been authenticated with the CA. Figure 4 illustrates this phase. Through V2I authentication phase, the legitimate vehicle can obtain $E[-R_{RSU} + \beta, PK_{BGN}, G]$, which have the relation as $-R_{RSU} + \beta = \gamma$. In order to share a fresh session key $K_{m,n}$, the vehicle m selects a random point a on cyclic group G and sends g^a with $TICKET_m$.

After verifying $TICKET_m$, the vehicle n generates $TICKET_n$, selects a random point b on cyclic group G, computes $K_{m,n}$, and forwards $TICKET_n$ to the vehicle m. Although our protocol supports non-linkability, we can prevent misbehavior of a vehicle having the authorized credential. In order to execute V2V authentication, each vehicle should prove that it has been authenticated with the CA using $E[-R_{RSU}+\beta, PK_{BGN}, G]$, $H(R^{i-1} \oplus j^{i-1})$, and C^{i-1}. However, the adversary cannot generate the different $E[-R_{RSU} + \beta, PK_{BGN}, G]$ without knowing the actual value of β or γ. Therefore, the adversary should reuse his/her $E[-R_{RSU} + \beta, PK_{BGN}, G]$ to deceive the nearby vehicles.

The above authentication is useful when two-way communication between the vehicle m and n is required. However, when we want to send the emergency warning message, one-way communication from the vehicle m to n is better. Because one-way communication requires only one message transmission which reduces the propagation time of the emergency message. Then, the vehicle m sends its $TICKET'_m = C_m^{i-1}||MSG||E\{MSG||g^a||C_m^{i-1}|| \ H(R_m^{i-1} \oplus j_m^{i-1})||RT_m, K_m\}$.

In addition, for stable operation of our proposed, we suggest combining our proposed scheme and Policing Traffic Management (PTM) [18] algorithm as rate control algorithm.

4 Analysis

4.1 Performance analysis

In this section, we analyze our protocol in detail. Table 2 shows the computational overhead in each phase. Note that $1/n$ indicates that one operation is

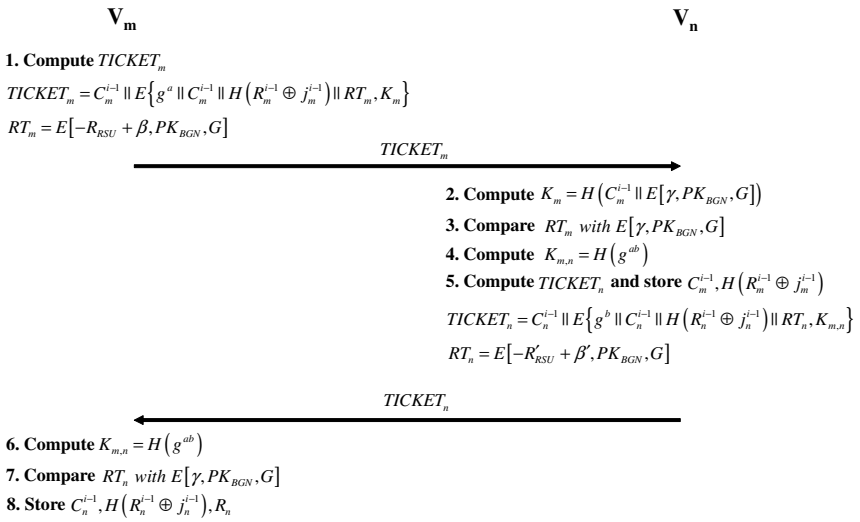

Figure 4: V2V Authentication

required during n sessions and p is the degree of the polynomial $f(x)$ used to enforce proper access permission. In our protocol, a vehicle m only requires two modular exponentiations to share a fresh session key with the nearby vehicle n. In our approach, vehicle registration phase is important to support anonymous communication in V2I and efficient verification of the authenticated vehicle. During vehicle registration, the CA can verify whether the driver has registered as a legitimate subscriber. Only if the driver is one of the legitimate service subscribers, the CA issues the authorized credential to the driver. Using the credential, the driver A can authenticate himself/herself with the nearby RSU. Although the computation overhead for vehicle registration is additional cost, vehicle registration can be done in the driver A's home. Hence, we believe that this phase does not affect the actual performance of our protocol. Also, through the verification of the authenticated vehicle, the vehicle m can authenticate itself to the vehicle n.

To illustrate the efficiency of our protocol, we compare our protocol with the existing approaches [3, 4] in Table 3 and 4. Through verification of the proposed algorithms in the existing approaches [3, 4], we can derive the computation overhead of their algorithms. Also, we refer to the computation overhead of VSS in V2I authentication as shown in [14]. Although our protocol and the approach by Yim *et al.* [4] can support mutual authentication, the protocol proposed by Lu *et al.* [3] only provide one-way authentication. Compared to the previous protocols [3, 4] requiring several pairing operations, our protocol needs 3 hash operations and 3 secret key operations as online computation, and $1/n$ hash operations and $1/n$ public key operation as off-line computation.

In addition, our protocol can support V2V communication using 3 hash operations, 1 secret key operation and 2 modular exponentiations as online computation, and 1 secret key operation as off-line computation. During V2V communication, the vehicle A does not need to communicate with the nearby

RSUs. However, the previous protocols [3, 4] need heavy computation such as several public key operations and pairing operations.

From these points, we believe that our protocol has reduced the processing delay time for vehicle authentication. Through the reduced time, the nearby RSUs can authenticate more vehicles within the fixed time period. Therefore, our protocol can support better scalability than the previous protocols [3, 4].

Table 2: Computational overhead in each phase

	Registration		**V2I Auth.**			**V2V Auth.**	
	V	CA	V	RSU	CA	V_m	V_n
Public key Oper.	$(2)^{\dagger}$ + 1	2	$(1/n)^{\dagger}$	0	2/n	0	0
Hash Oper.	0	0	$(1/n)^{\dagger}$ + 3	0	$(1/n)^{\dagger}$ + 3	3	3
Secret Key Oper.	2	2	3	1	2	$(1)^{\dagger}$ + 1	$(1)^{\dagger}$ + 1
Pairing Oper.	0	p-1	0	0	0	0	0
Modular Exp.	$(2p+3)^{\dagger}$	2	0	0	0	2	2
Modular Addition	$(p+2)^{\dagger}$	p+2	0	0	0	0	0

† : Precomputation Auth.: Authentication
Oper.: Operation Exp.: Exponentiation

Table 3: Computational overhead comparison for V2I authentication

	Ours			**Yim *et al.***			**Lu *et al.***		
	V	RSU	CA	V	RSU	CA	V	RSU	CA
Public key Oper.	$(1/n)^{\dagger}$	0	2/n	2	2	1	0	0	0
Hash Oper.	$(1/n)^{\dagger}$	0	$(1/n)^{\dagger}$	2	1	0	1	1	2
Secret Key Oper.	3	1	2	1	1	0	4	1	1
Pairing Oper.	0	0	0	0	0	0	1	3	0
Modular Exp.	0	0	0	9	6	1	4	2	3
Modular Addition	0	0	0	3	2	0	2	1	0

† : Precomputation
Oper.: Operation Exp.: Exponentiation

Table 4: Computational overhead comparison for V2V authentication

	Ours		**Yim *et al.***		**Lu *et al.***	
	V_m	V_n	V_m	V_n	V_m	V_n
Public key Oper.	0	0	3	3	0	0
Hash Oper.	3	3	3	3	3	3
Secret Key Oper.	$(1)^{\dagger}$ + 1	$(1)^{\dagger}$ + 1	1	1	2	2
Pairing Oper.	0	0	0	0	9	9
Modular Exp.	2	2	12	12	24	24
Modular Addition	0	0	4	4	3	3

† : Precomputation
Oper.: Operation Exp.: Exponentiation

4.2 Security analysis

Our protocol provides the following security-related features.
Mutual authentication: The vehicle authenticates the CA through a public key of the CA and knowledge of the corresponding private key. Also, the CA authenticates the end-user using an authorized credential of the vehicle.
Data confidentiality and integrity: All communications are protected by a shared session key or the receiver's public key. In this point, our protocol supports data confidentiality. Although we do not explain explicitly how to generate a key for integrity check, vehicle, RSU, and CA can derive the key using the shared information such as a fresh session key (or the receiver's public key) and exchanged nonce. By applying HMAC with the derived key, our protocol can support data integrity.
Non-linkability: Non-linkability means that, for insiders (*i.e.*, RSU and nearby vehicle) and outsiders, 1) neither of them can ascribe any session to a particular driver, and 2) neither of them can link two different sessions to the same driver [17]. More precisely, non-linkability needs to prevent insiders and outsiders from obtaining an driver's private information. Our protocol can achieve non-linkability with respect to both insiders and outsiders. First, the information to distinguish each driver is never transmitted in a plaintext form. As a result, outsiders cannot associate a session with a particular driver and ascribe two sessions to the same driver. Second, outsiders and insiders cannot find any relationship between the exposed credentials due to the one-way hash function. Finally, all communications are protected by a fresh session key.
Scalability: Since our protocol reduces the computational overhead compared to the previous approaches [3, 4], our protocol allows one RSU to authenticate the more vehicles within the certain time period. Moreover, our protocol does not require the participation of the nearby RSU in V2V authentication.

5 Conclusion

In this paper, we have presented a scalable privacy-preserving authentication protocol for secure vehicular communications. Compared to the previous approaches [3, 4], our protocol excludes the participation of the nearby RSU so that the nearby vehicle from a vehicle A require less the time delay authenticating the vehicle A. As the nearby vehicles can authenticate the vehicle A without the help of the nearby RSU, we can save the transmission delay for sending authentication request of the vehicle A. In addition, our protocol requires less computational cost in V2I authentication and V2V authentication. From these points, our protocol increases the number of the vehicles which can be authenticated by one RSU.

Acknowledgements

This work was supported by the ETRI (7010-2011-0036), "Research on international cooperation of side channel analysis between Korea and Japan".

References

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

[2] X. Lin, X. Sun, P.H. Ho, and X. Shen, GSIS: A Secure and Privacy-pserving Protocol for Vehicular Communications, IEEE Transactions on Vehicular Technology, 56(2007), 3442-3456.

[3] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, in Proc. of The 27th IEEE Conference on Computer Communications (INFOCOM 2008), (2008), 1229-1237.

[4] J. Yim, I. Choi, and K. Kim, An Efficient Anonymous Authentication Protocol in Vehicular Ad-hoc Networks, in Proc. of The 10th International Workshop on Information Security Applications (WISA 2009), Aug. 24-26, (2009).

[5] M. Imani, M. Taheri, and M. Naderi, Security enhanced routing protocol for ad hoc networks, Journal of Convergence (JoC), 1:1(2011), 43-48.

[6] B. Xie, A. Kumar, D. Zhao, R. Reddy, and B. He, On secure communication in integrated heterogeneous wireless network, International Journal of Information Technology, Communications and Convergence (IJITCC), 1:1(2011), 4-23.

[7] D. Kumar, T. C. Aseri, R.B. Patel, Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor networks, International Journal of Information Technology, Communications and Convergence (IJITCC), 1:1(2011), 130-145.

[8] Jangseong Kim, Joonsang Baek and Taeshik Shon, An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network, IEEE Transactions on Consumer Electronics, Vol 57, Issues 2, May 31, 2011, pp 516-522, ISSN: 0098-3063

[9] C. D. Wang and J. P. Thompson, Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network, 1997. US. Paten No. 5,613,039.

[10] D. Chaum and E. van Heijst, Group signatures, in Proc. Advances in Cryptology - Eurocrypt '91, LNCS, 196(1984), 257-265.

[11] A. Shamir, Identity-based cryptosystems and signature schemes, in Proc. Advances in Cryptology - Crypto '84, LNCS, 8(1984), 47-53.

[12] S. S. Yau and Y. Yin, Controlled Privacy Preserving Keyword Search, Proc. of ACM Symposium on Information, Computer & Communication Security (ASIA-CCS '08), Mar. 2008, 321-324.

[13] D. Boneh, E.-J. Goh and K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in Proc. of Theory of Cryptography (TCC '05), LNCS, 3378(2005), 325-341.

[14] J. Kim, J. Baek, J. Zhou, K. Kim, and T. Shon, An Efficient and Secure Service Discovery Protocol for Ubiquitous Computing Environments, in Proc. of 7th European Workshop on Public Key Services, Applications and Infrastructures (EuroPKI 2010), LNCS, 6711(2010), 45-60.

[15] M. Gruteser and D. Grunwald, Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis, Mobile Networks and Applications, 10:3(2003), 315-325.

[16] D. Chaum, Untraceable Electronic Mail, Return Address, and Digital Pseudonyms, Communications of the ACM, 24:2(1981), 84-88.

[17] S. Xu and M. Yung, K-anonymous Secret Handshakes with Reusable Credentials, in Proc. of the 11th ACM Conf. on Computer and communications security (CCS '08), (2008), 158-167.

[18] S. Prahmkaew, Performance Evaluation of Convergence Ad Hoc Networks, Journal of Convergence (JoC), 1:1(2011), 101-106.

Zeen Kim
He received the B.S. degree in Mathematics from Korea Advanced Institute of Science and Technology (KAIST), Korea, in 2001 and the M.S. degree in the School of Engineering from the Information and Communications University [now merged with KAIST], Daejeon, Korea, in 2004. His research interests include: Secure and privacy-preserving (cryptographic) algorithms and cryptography.

Dr. Jangseong Kim
He received the B.S. degree in Computer Engineering from Kyungpook University, Korea and PhD degree in Korea Advanced Institute of Science and Technology, Korea, respectively 2006 and 2011. He is currently a senior engineer in the Convergence Service Lab, DMC R&D Center of Samsung Electronics Co., Ltd. His interests are in network security, security for smart grid, VANET security, and security for ubiquitous computing environment.

Doyoung Chung
He received the B.S. degree in Computer Science from Korea Advanced Institute of Science and Technology (KAIST), Korea, in 2010. His research interests include: Secure and privacy-preserving (cryptographic) algorithms in ubiquitous computing environment.

Prof. Kwangjo Kim
He received the B.S and M.S. degrees of Electronic Engineering in Yonsei University, Korea in 1881 and 1983, respectively. He has also finished his Ph.D course in Div. of Electrical and Computer Engineering in Yokohama National University, Japan in 1991. He was Section Head in ETRI (1983–1997) and Professor at School of Engineering in ICU (1998–2008). Currently he is Full Professor at Computer Science Department in KAIST, Korea. Prof. Kim has served President of KIISC (2009), Editor of JCN (– 2007) and IJIS (– 2008), and IEICE Special Issue on Information Security and Cryptography (2007). He was elected to serve Board of Director Member of IACR (1999–2004) and Chair of Asiacrypt Steering Committee (2005 – 2008). He is currently Member of IEEE, IACR, and IEICE. He served a Honorable President of KIISC and an editor of JMC.

Prof. Taeshik Shon
He received his Ph.D. degree in Information Security from Korea University, Seoul, Korea and his M.S. and B.S. degree in computer engineering from Ajou University, Suwon, Korea. From Aug. 2005 to Feb. 2011, Dr. Shon had been a senior engineer in the Convergence S/W Lab, DMC R&D Center of Samsung Electronics Co., Ltd. He is currently a professor at the Division of Information and Computer Engineering, College of Information Technology, Ajou University, Suwon, Korea. He is also serving as a guest editor, an editorial staff and review committee of Computers and Electrical Engineering - Elsevier, Mobile Network & Applications, Springer, Security and Communication Networks - Wiley InterScience, Wireless Personal Communications, Springer, Journal of The Korea Institute of Information Security and Cryptology, IAENG International Journal of Computer Science, and other journals. His research interests include Convergence Platform Security, Mobile Cloud Computing Security, Mobile/Wireless Network Security, WPAN/WSN Security, anomaly detection algorithms, and machine learning applications.