International Journal of Control and Automation
Vol. 10, No. 11 (2017), pp.145-156
http//dx.doi.org/10.14257/ijca.2017.10.11.13

Secure Group Key Transmission Scheme for Vehicles Parked Beyond the Communication Range of Roadside Units

Young-Hoon Park

Division of Computer Science, Sookmyung Women's University
yh.park@sookmyung.ac.kr

Abstract

With progressive developments in vehicular technology, it is expected that vehicles in the future will be able to participate in group communication even when they are parked and the ignition has been turned off. However, when the vehicle is parked beyond the communication range of the Roadside Unit (RSU), the vehicle cannot update the group key and will be unable to participate in the group communication.

In this paper, we propose a group key transmission scheme for the vehicles parked beyond the RSU's communication range. For this scheme, we provide a vehicle-to-vehicle group key delivery protocol, which includes procedures for vehicle verification and group key verification. The two procedures do not include any interaction with a third party because the vehicles cannot communicate with the RSUs. Moreover, in the vehicle verification procedure, the encrypted subscription information is transmitted and verified without being decrypted, and thus privacy of the vehicle is guaranteed. We demonstrate that the proposed scheme is secure against potential attack scenarios using mathematical analysis, and show that the privacy of the participant vehicles is secured.

Keywords*: Group Key, VANET, Multicast, Parked Vehicle, V2V communication*

1. Introduction

Owing to the remarkable development of vehicular accessories, vehicle owners have access to information about the status and surroundings of their vehicles, even when they are parked and the owners are not in the vicinity [3]. Furthermore, it is expected that the vehicles are connected to vehicular ad hoc networks (VANET). Thus owners may receive such information through communication devices such as laptops, smartphones, and tablets. Moreover, multicast communication can be used to transmit such information for efficient and secure communication [4]. However, with multicast, if vehicles are parked beyond the communication range of the road side unit (RSU), the vehicle is not able to send the status or information to the owner when the group key is changed.

VANET comprises vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications, where the former is the communication between a vehicle and an RSU, and the latter is the communication between several vehicles. Through V2I communication, the RSU sends traffic information or various keys to the vehicles, and the vehicles transmit their statuses or surrounding information to the RSU. V2V communication provides an additional service whereby the vehicles exchange status or surrounding traffic information and relay messages from the RSU for the receiver vehicle beyond the RSU communication range.

In VANET, multicast applications are widely employed for efficiency and security. With multicast, a message can be sent to a specific group of vehicles simultaneously with a single transmission [4]. A group key, which is shared amongst a specific group only, is used to encrypt or sign the transmitted message. Moreover, the group key is updated when

Received (June 25, 2017), Review Result (August 9, 2017), Accepted (August 28, 2017)

ISSN: 2005-4297 IJCA

the key is compromised or group membership changes. Therefore, if a vehicle does not have the latest group key, it cannot participate in the group communication. The group key is updated for many reasons, such as a change in the group membership, and a compromised or expired group key is compromised.

Initially, when the group key is updated, each vehicle in the group receives the key from the RSU. Therefore, the vehicles, including those parked, can update the group key only when they are in the communication range of the RSU. If a vehicle is parked beyond the RSU's communication range, the group key cannot be updated when the key is changed [5]. From this time, the vehicle is unable to participate in the group communications; thus, it may not send its status or surrounding information to the owner. Furthermore, the parked vehicle can play the role of a substitute RSU, however if the group key is updated, this function must be stopped.

To overcome this problem, we consider a method of vehicle-to-vehicle group key transmission [2]. Let us assume that there is a vehicle parked beyond the communication range of the RSU and the group key is updated. When another vehicle in the same group with the latest group key passes the parked vehicle, the passing vehicle can send the group key to the parked vehicle. Finally, the parked vehicle is able to participate in the group communication. In this process, to deliver the group key to the group member, the passing vehicle should be able to check whether the parked vehicle is a group member. Moreover, the parked vehicle should be able to verify the integrity of the group key to avoid illegal behavior by the passing vehicle.

Therefore, V2V group key transmission requires the passing vehicle to have a procedure to determine if the parked vehicle is a group member, and the parked vehicle to have a procedure to determine if the transmitted group key is a forgery. However, note that the two vehicles are beyond the communication range of the RSU. Thus, the verification procedures should not include interaction with a third party including the RSU, i.e., the vehicles must perform these verification procedures independently.

To solve the aforementioned problem, this paper proposes a V2V group key transmission protocol for vehicles parked beyond the communication range of the RSU. Because the protocol is operated beyond the RSU's range, it does not include interaction with third parties. For this, the protocol is designed based on the Strong Diffie Hellman (SDH) problem [6]. Specially, in terms of verification of the parked vehicle as a group member, the verification protocol is designed using the multi-value Strong Diffie Hellman (MVSDH) problem because there are several values that require verification [2].

This paper focuses on the design of a V2V group key transmission protocol. The problem was first addressed in a short conference paper [1], of which this work is the extended version.

Section 2 lists the previous work related to the proposed scheme, and Section 3 addresses the preliminaries. Section 4 proposes verification schemes for parked vehicles and to check the integrity of the transmitted group key. Section 5 provides a method of employing the proposed schemes in the VANET, and Section 6 discusses security and privacy. Finally, Section 7 concludes this paper and addresses the future work.

2. Related Works

This paper addresses both group key management and authentication. In this section, we illustrate the previous works related to the two research areas.

2.1. Key Management in Vehicular Networks

In most existing schemes with a group key, researchers have considered methods of securely and efficiently revoking and updating the group key. In [7], Wong *et al.* proposed a tree-based logical key hierarchy, thus reducing the rekeying cost from $O(N)$ to $O(\log N)$, where N is the number of subscribers. Following this work, many rekeying schemes attempting to reduce the rekeying cost further have been proposed, *e.g.*, [8] and [9].

In addition, group keys have been employed in vehicular networks. In [10], vehicular communication frameworks based on a group signature are given, where they are based on centralized key management schemes. To reduce the communication and computation overheads, Park *et al*. and Hao *et al*. proposed schemes in [11] and [12], respectively, that delegate the function of the group key management to each RSU. However, there remains the limitation that the vehicles beyond the communication range cannot receive the group key. In [2], a V2V group key transmission for the vehicle out-of-range V2I communication was proposed; however, the authors did not address the case of transmitting the group key to the parked vehicle.

Moreover, instead of changing the group key with each group change, schemes based on a certificate revocation list (CRL) have been proposed, to reduce the number of rekeying processes. According to [13], to revoke a vehicle, the CRL is issued by a certification authority and broadcasted. Furthermore, in [14], the CRL is generated and distributed in a decentralized way; in [15], the rekeying process is also operated by a decentralized method. While the communication and computation overheads are reduced, and the delay in updating the CRL and keys decreased with these schemes, there is no procedure in V2V transmission for checking other party vehicles, and the integrity of the key.

2.2. Authentication in Vehicular Networks

Authentication issues in vehicular networks have been studied by many researchers. Raya *et al*. proposed an authentication scheme based on anonymous certificates, to provide privacy [16]. In addition, a message authentication protocol based on group signatures [17] and one based on both group signature and ID-based signatures [10] have been presented. Moreover, in [18], Zhang *et al*. proposed privacy-preserving protocols, which consider efficient certificate distribution and revocation, avoidance of bottleneck, and reduction in strong dependence on tamper-proof devices. While there are numerous alternative proposed protocols for authentication, they cannot check whether the certificate is out-of-date, without interaction with the RSU.

3. Preliminaries

3.1. System Model

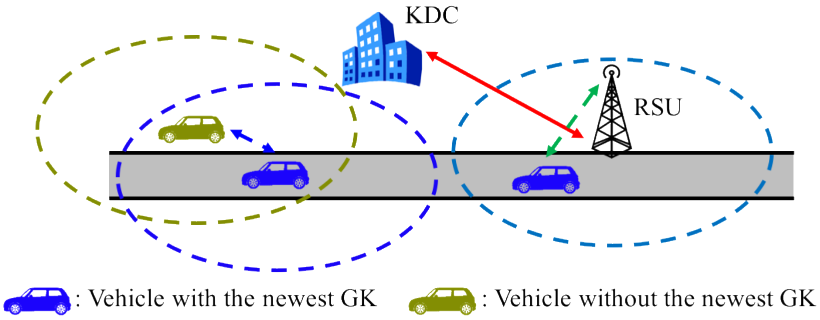


Figure 1. System Model

First, we consider the system model for the proposed scheme. As shown in Figure 1, the system is composed of a key distribution center (KDC), several road side units (RSUs), and vehicles. The role of each item is as follows:

1) KDC: The aims of the KDC is to generate all the values, including keys, and distribute them to the RSUs and vehicles. It is connected to all the RSUs through a wired network. In addition, it is assumed that it has sufficiently powerful computation and storage capacities, and that it is not compromised.

2) RSU: RSUs are widely deployed at fixed positions. The primary role of the RSU is to connect the KDC and the vehicles. RSUs are connected to the KDC via a wired network. In addition, each RSU is connected to vehicles in the communication range of the RSU via wireless network. It is assumed that the RSU has sufficiently powerful computation and storage capacities, and that it is not compromised. Moreover, we assume that there exist some regions that are not covered by the communication range of the RSU; thus, the vehicles in this region are unable to communicate with the RSU.

3) Vehicle: Vehicles can move freely on the roads and can be parked in parking lots or on the roadside. They can communicate with the RSU and other vehicles through the wireless network. We assume that parked vehicles can communicate with the RSU and other vehicles, and there exist malicious vehicles that attempt illegal behaviors.

3.2. System Requirements

The requirements for the proposed scheme are as follows:

1) When the vehicle parked beyond the communication range of the RSU does not have the latest group key, it should be able to receive it as fast as possible. This is to enable the parked vehicle to participate in the group communication.

2) The group key should be delivered to group members only. Thus, in the V2V group key transmission, the passing vehicle should send the group key to the parked vehicle after verification. It is assume that the group key is delivered through a secure channel following verification.

3) For 2), the passing vehicle should be able to verify if the parked vehicle is a group member. As mentioned, because the verification process is conducted outside of the communication range of the RSU, the passing vehicle must verify this independently.

4) The parked vehicle should be able to determine if the received group key is a forgery, As in 3), the parked vehicle should verify this independently.

3.3. Bilinear Mapping

In security- or privacy-enhanced networks, bilinear mapping is receiving considerable attention since it verifies the encrypted value without decryption; an example of this is identity-based cryptography [19]. Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be three multiplicative cyclic groups of prime order$p$, and assume that there exists a computable isomorphism ψ from $\mathbb{G}_2$ to $\mathbb{G}_1$. Let $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ be generators, where $g_1 = \psi(g_2)$. A map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear mapping provided it satisfies the following properties:

1) Bilinearity: $\forall u \in \mathbb{G}_1, v \in \mathbb{G}_2$, and $a, b \in \mathbb{Z}_p^*$, $e(u^a, v^b) = e(u, v)^{ab}$.

2) Nondegeneracy: $e(g_1, g_2) \neq 1$.

3) Computability: $\forall u \in \mathbb{G}_1, v \in \mathbb{G}_2$, there exists an efficient algorithm to compute $e(u, v)$.

4. Protocols for Verification

In this section, we propose two verification protocols. Let a receiver vehicle be a vehicle that tries to receive the latest group key, and let a sender vehicle be a vehicle that is requested to send the group key. Note that both vehicles are members of the same group, and they do not know the other's subscription information. First, we describe a protocol to verify the receiver vehicle for the sender vehicle; then, we propose a method of verifying the integrity of the group key for the receiver vehicle.

4.1. Verification of Receiver Vehicle

When a sender vehicle transmits the new group key, it should check if the receiver vehicle is a group member. For verification, the integrity of the receiver's subscription information, including private key and expiration time, should be confirmed. Note that the private key must be confidential to the sender vehicle, whereas expiration time is public information.

To verify the integrity of hidden information without making it available, a zero-knowledge proof protocol based on the SDH problem is employed. However, for this process, the sender vehicle should verify both hidden (private key) and public (expiration time) information simultaneously. To accomplish this, a zero-knowledge proof based on MVSDH is used [2].

Table 1. Notations for Verification of Receiver Vehicle

Variable	Meaning
p	Large prime
$x \in \mathbb{Z}_p$	Prover's private key
$g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$	Generators
$k \in \mathbb{G}_2$	Prover's public key (g_2^x)
$\mu, \nu, \gamma \in \mathbb{Z}_p$	KDC's secret
$U, V, H \in \mathbb{G}_1, D \in \mathbb{G}_2$	Helper values (g_1^ν, g_1^μ, $g_1^{\mu\nu}$, g_2^γ)
$t \in \mathbb{Z}_p$	Prover's expiration time
$C \in \mathbb{G}_1$	Prover's certificate ($g_1^{\frac{1}{x+\gamma t}}$)

Table 1 introduces variables and their meanings, which are used for the protocol. p is a large prime number, and $\mathbb{Z}_p$ is $\{0,1,2,\cdots,p-1\}$. Let $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ be generators of the multiplicative cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$. In addition, let $x \in \mathbb{Z}_p$, $k \in \mathbb{G}_2$, $t \in \mathbb{Z}_p$ be the receiver vehicle's private key, public key, and expiration time, respectively, where $k = g_2^x$. Moreover, $\mu, \nu, \gamma \in \mathbb{Z}_p$, $U, V, H \in \mathbb{G}_1$, and $D \in \mathbb{G}_2$ are KDC's secret and helper values, which are used to verify x and t. Finally, $C \in \mathbb{G}_1$ is prover's certificate, where $C = g_1^{\frac{1}{x+\gamma t}}$. Here, $\frac{1}{x+\gamma t}$ is a value b that has a remainder of 1 when the product of b and $x + \gamma t$ is divided by p.

The variables listed on Table 1 are generated by the KDC. Among them, p, g_1, g_2, t, U, V, H, and D can be published to all the vehicles; μ, ν, and γ should not be known by anyone other than the KDC, and x is confidential to the receiver vehicle. If privacy is required in the communication, e and C should not be revealed to other vehicles. In this study, we assume that these two values are not revealed to the sender vehicle.

The MVSDH problem is as follows:

Given $(p+3)$-tuple $\left(g_1, g_2, g_2^{\gamma}, g_2^{\gamma^2}, \cdots, g_2^{\gamma^p}, t\right)$ as an input, the pair $\left(g_1^{\frac{1}{x+\gamma t}}, x\right)$ is output, where $\gamma, x, t \in \mathbb{Z}_p$.

It is known that solving the MVSDH problem is computationally infeasible, which means that $g_1^{\frac{1}{x+\gamma t}}$ can be generated only by the KDC; if γ is not known to the vehicle, the pair $\left(g_1^{\frac{1}{x+\gamma t}}, x\right)$ cannot be determined. Conversely, a vehicle with a known $\left(g_1^{\frac{1}{x+\gamma t}}, x, t\right)$ is a legal subscriber.

Now, let us consider the verification method. If there is no problem with the values, the following equation is established:

$$e(C, k \cdot D^t) = e(g_1, g_2) \tag{1}$$

In this study, the protocol maintains the receiver vehicle's privacy and replay attack should not be allowed. Therefore, we employ a challenge-response method as follows. In the following protocol, the sender vehicle is a verifier, and the receiver vehicle is a prover.

1) The prover selects α, β, r_α, r_β, r_x, $r_{\delta1}$, and $r_{\delta2} \in \mathbb{Z}_p$, randomly.

2) The prover calculates the following equations:
$$T_1 \leftarrow U^{\alpha},\ T_2 \leftarrow V^{\beta},\ T_3 \leftarrow CH^{\alpha+\beta}$$
$$R_1 \leftarrow U^{r_\alpha},\ R_2 \leftarrow V^{r_\beta},\ R_3 \leftarrow e(T_3, g_2)^{r_x} e(h, g_2)^{-r_{\delta1}-r_{\delta2}} e(h, D^t)^{-r_\alpha-r_\beta}$$
$$R_4 \leftarrow T_1^{r_x} U^{-r_{\delta1}},\ R_5 \leftarrow T_2^{r_x} V^{-r_{\delta2}} \tag{2}$$

3) The prover sends the following values to the verifier:
$$(T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, t) \tag{3}$$

4) The verifier generates a challenge value c randomly, and sends it to the prover.

5) The prover calculates the following equations:
$$s_\alpha \leftarrow r_\alpha + c\alpha,\ s_\beta \leftarrow r_\beta + c\beta,\ s_x \leftarrow r_x + cx$$
$$s_{\delta1} \leftarrow r_{\delta1} + cx\alpha,\ s_{\delta2} \leftarrow r_{\delta2} + cx\beta \tag{4}$$

6) The prover returns s_α, s_β, s_x, $s_{\delta1}$, and $s_{\delta2}$ to the verifier.

7) The verifier checks the values by checking that the following five equations are valid:
$$U^{s_\alpha} = T_1^c R_1,\ V^{s_\beta} = T_2^c R_2,\ T_1^{s_x} U^{-s_{\delta1}} = R_4,\ T_2^{s_x} V^{-s_{\delta2}} = R_5$$
$$e(T_3, g_2)^{s_x} e(H, g_2)^{-s_{\delta1}-s_{\delta2}} e(H, D^t)^{-s_\alpha-s_\beta} = \left(\frac{e(g_1, g_2)}{e(T_3, D^t)}\right)^c \cdot R_3 \tag{5}$$
If all of the equations hold, the verifier accepts the prover.

4.2. Verification of Group Key

The verification protocol for checking integrity of the received group key is also required for the receiver vehicle, which prevents illegal benefit of the sender vehicle. The process of verification for the group key is based on the MVSDH problem.

Table 2. Notations for Group Key Verification

Variable	Meaning
$\lambda, \varepsilon \in \mathbb{Z}_p$	KDC's secret
$K \in \mathbb{G}_2$	Helper value (g_2^{ε})
$v_{gk} \in \mathbb{Z}_p$	Version of group key
$GK_1 \in \mathbb{G}_1, GK_2 \in \mathbb{G}_2$	Elements of group key
$f: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \{0,1\}^*$	Group key generation function
GK	Group key ($f(GK_1, GK_2)$)

Table 2 indicates the notations used for the group key verification. Note that all of the variables listed in Table 2 are generated by the KDC; λ, ε are secret values and should not be revealed beyond the KDC; GK_1, GK_2, and GK are confidential to the KDC and vehicles in the group; and the remaining variables and function f are available to all vehicles.

Let us consider the elements of the group key, GK_1 and GK_2, which are generated by the KDC as follows:

$$GK_1 \leftarrow g_1^{\frac{1}{\lambda+\varepsilon \cdot v_{gk}}},\ GK_2 \leftarrow g_2^{\lambda} \tag{6}$$

Note that λ changes whenever the group key is updated, whereas ε is fixed. In addition, when the group key is updated, v_{gk} increases by 1. The group key is calculated using the equation $GK \leftarrow f(GK_1, GK_2)$. Because f is a public function, the vehicle can generate the group key when GK_1 and GK_2 are known.

The group key generation process operated by the KDC is as follows:

1) The KDC selects a secret $\lambda \in \mathbb{Z}_p$ randomly.

2) The KDC increases v_{gk} by 1.

3) The KDC calculates $GK_1 \leftarrow g_1^{\frac{1}{\lambda+\varepsilon \cdot v_{gk}}}$ and $GK_2 \leftarrow g_2^{\lambda}$

4) The KDC sends GK_1 and GK_2 to the group members through the RSUs.

Now, let us consider the method of verifying the group key. If there is no problem with the elements of the group key, the following equation must be established:

$$e(GK_1, GK_2 \cdot K^{v_{gk}}) = e(g_1, g_2) \tag{7}$$

Therefore, when the receiver vehicle obtains the elements of the new group key, equation (7) is calculated.

5. Framework of Group Key Transmission for Parked Vehicles

In this section, we propose the framework of group key transmission for vehicles parked beyond the RSU's communication range. First, we describe how to determine and deploy the variables for the verification procedures. Then we provide the group key transmission process. In this section, we use the notations introduced in Section 4.

5.1. Determining Variables for Verification

First, we describe how to determine the variables used for the verification process, and how to allocate them to the vehicles. Here, we provide procedures for system initialization, new vehicle registration, and group key update.

The procedure for system initialization is to determine the variables for verifying the vehicle that tries to receive the new group key. The procedure is as follows:

1) The KDC chooses a large prime p.

2) The KDC determines three multiplicative cyclic groups based on prime p, $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$. Note that $\mathbb{G}_1$ and $\mathbb{G}_2$ can be the same, but $\mathbb{G}_T$ must be different to $\mathbb{G}_1$ and $\mathbb{G}_2$.

3) The KDC determines a bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, an isomorphic function $\psi: \mathbb{G}_2 \rightarrow \mathbb{G}_1$ [19],and group key generation function $f: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \{0,1\}^*$.

4) The KDC chooses $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ randomly, where $g_1 = \psi(g_2)$.

5) The KDC chooses $\mu, \nu, \gamma,$ and $\varepsilon \in \mathbb{Z}_p$ randomly, and calculates $U = g_1^{\gamma}$, $V = g_1^{\mu}$, $H = g_1^{\mu\nu}$, $D = g_2^{\gamma}$, and $K = g_1^{\varepsilon}$.

After these five steps, the system is initialized.

Second, we describe the procedure for a new vehicle registration. In this procedure, the new values for the vehicle are created and several values determined in the previous procedure are delivered to the vehicle.

1) When the new vehicle requests to join the group, the KDC determines the expiration time t, and randomly chooses a private key $x \in \mathbb{Z}_p$ for the vehicle, where x is a non-trivial value.

2) The KDC calculates the vehicle's public key $k = g_2^x$ and certificate $C = g_1^{\frac{1}{x+\gamma t}}$.

3) The KDC sends $p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2,\ U, V, H, D, K, x, k,$ and C to the vehicle via a secure channel.

4) The KDC also sends functions e and f to the vehicle.

Next, we provide a procedure for group key generation.

1) The KDC increases the version of the group key v_{gk} by 1.

2) The KDC chooses $\lambda \in \mathbb{Z}_p$ randomly.

3) The KDC calculates $GK_1 = g_1^{\frac{1}{\lambda+\varepsilon\cdot v_{gk}}}$ and $GK_2 = g_2^{\lambda}$.

4) The KDC sends GK_1 and GK_2 to the vehicles in the group via a secure channel.

5) The vehicles generate the new group key by calculating $f(GK_1, GK_2)$.

Note that the vehicles that can receive the group key are those in the communication range of the RSUs. The group key transmission procedure for vehicles that are beyond the communication range is introduced in 5.2.

5.2. V2V Group Key Transmission Process

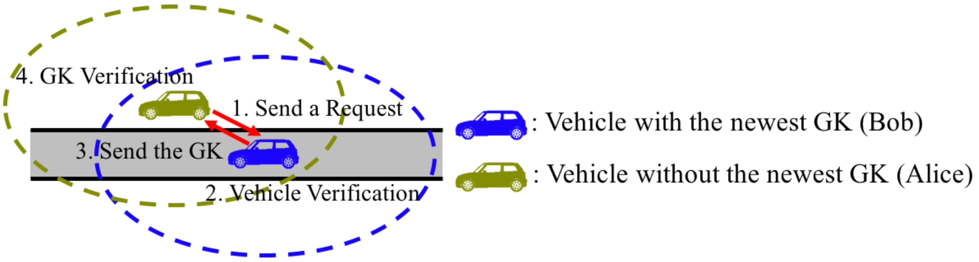

4. GK Verification
1. Send a Request
3. Send the GK
2. Vehicle Verification
: Vehicle with the newest GK (Bob)
: Vehicle without the newest GK (Alice)

Figure 2. Architecture of V2V Group Key Transmission

Now, we describe the vehicle-to-vehicle group key transmission protocol. For convenience, let a vehicle that is parked beyond the RSU's communication range and wants to receive the latest group key be **Alice**, and let the vehicle that is requested to send the group key to Alice be **Bob**. Here, let x, k, C, and t be Alice's private key, public key, certificate, and expiration time, respectively. As in Figure 2, this protocol is composed of four phases: Alice's request, Bob's verification of Alice, transmission of the group key, and Alice's verification of the group key. The procedure is as follows:

1) When Bob passes around Alice, Alice requests Bob to send the newest group key.

2) If Bob accepts, Alice calculates equation (2) and sends (3) to Bob.

3) Bob uses t to check whether Alice's subscription is expired. If it is not expired, Bob sends a challenge value c to Alice.

4) Alice derives responses using equation (4), and returns them to Bob.

5) Bob checks if equations (5) are established. If so, Bob sends GK_1, GK_2, and v_{gk} to Alice via a secure channel.

6) Alice checks if equation (7) is established. If so, Alice derives the latest group key GK using equation $f(GK_1, GK_2)$.

If the verification fails, the process is terminated. In addition, to prevent offender vehicles from trying to attack repeatedly, a certificate revocation list (CRL) may be employed. If a vehicle repeatedly misbehaves, it may be listed on the CRL. Following this, when the vehicle tries to receive the group key illegally, the requested vehicle checks if the requesting vehicle is on the CRL and blocks it.

6. Discussion

6.1. Security Analysis

We assume that there is a malicious vehicle. The goals of the malicious vehicle can be categorized into two objectives: obtaining the group key illegally and sending a fake group key.

Let us consider the case where the malicious vehicle attempts to obtain the group key in an illegal manner. There are two potential methods: modifying subscription information and using other vehicle's subscription information.

The malicious vehicle may modify the subscription information, such as expiration time. Let t' be the modified expiration time. To pass the vehicle verification process, the malicious vehicle should also choose a certificate C' and a private key x, which satisfy the following equation:

$$e\left(C', g_2^{x'} \cdot D^{t'}\right) = e(g_1, g_2) \quad \Leftrightarrow \quad \zeta' \cdot (x' + \gamma t') \equiv 1 (\mathrm{mod}\, p), \tag{8}$$

where $g_1^{\zeta'} = C'$. As mentioned, no vehicle knows γ, and the malicious vehicle should find tuple (ζ', x', t') that satisfies equation (8). The number of possible tuples (ζ', x', t') is p^3, and there is a maximum of p^2 tuples that satisfies equation (8). This is because there exists a maximum of one ζ' for each given pair (x', t'). Therefore, the probability that the malicious vehicle succeeds in obtaining the group key using the method of modifying the subscription information is less than $\frac{1}{p}$. Prime p is a relatively large integer; thus, the probability is sufficiently small.

Let us consider the case where a malicious vehicle tries to be verified by reusing a valid vehicle's subscription information. Let x_1, k_1, C_1, and t_1 be the other vehicle's valid private key, public key, certificate, and expiration time, respectively. Note that the malicious vehicle knows k_1, but not x_1.

In this case, because these values are generated by the KDC, $e(C_1, k_1 \cdot D^{t_1}) = e(g_1, g_2)$ is established. However, the malicious vehicle cannot calculate equation (4) since it does not have x_1. Therefore, the malicious vehicle guesses the responses. There is only one value for the correct private key x_1 among p possibilities of x_1; thus, the probability that the malicious vehicle succeeds in this type of attack is $\frac{1}{p}$.

Finally, we consider the case where the malicious vehicle sends a fake group key to a parked vehicle. Let GK_1' and GK_2' be the elements of the fake group key, and let $g_1^{\chi} = GK_1'$, and $g_2^{\lambda'} = GK_2'$. At the end of the V2V group key transmission process, the parked vehicle verifies the group key by using equation (7). For this, χ and λ' should satisfy $\chi\left(\varepsilon + \lambda' \cdot v_{gk}\right) \equiv 1 (\bmod\, p)$. The malicious vehicle should find an appropriate pair (χ, λ') without knowing ε. Similarly, the probability of success of this type attack is less than $\frac{1}{p}$.

In conclusion, the proposed V2V group key transmission scheme is strong against the aforementioned possible attack scenarios. In other words, it is infeasible that a malicious vehicle obtains the latest group key illegally and sends a fake group key.

6.2. Privacy Analysis

Now, we consider the privacy issues in the proposed scheme. In the vehicle verification procedure, the parked vehicle sends its subscription information to the passing vehicle to prove that the parked vehicle is a group member. Here, the passing vehicle, or a third-party eavesdropper, may see or track the information.

First, let us consider the case where the subscription information of the parked receiver vehicle is revealed to the passing sender vehicle or third-party. The personal data of the parked vehicle are the private key, public key, and certificate. However, these data are not revealed during the verification process. In the verification procedure, the private key is included by s_x, $s_{\delta 1}$, and $s_{\delta 2}$ in equation (4). The value that the passing vehicle generates is only c, and r_x, $r_{\delta 1}$ and $r_{\delta 2}$ are chosen by the parked vehicle. This means the passing vehicle cannot determine x. It is more difficult for the third-party to determine the private key. Similarly, certificate C is in T_3 and R_3; however, it is infeasible for the passing vehicle to determine C because it does not know α nor β.

Now, let us consider the location privacy. The passing vehicle or the third-party may track the parked vehicle by collecting the subscription information. However, this strategy is impossible because the transmitted information is encrypted with random variables, thus it is changed whenever the parked vehicle sends information. In turn, the location privacy is guaranteed.

7. Conclusion and Future Work

In this paper, we propose a group key transmission scheme for vehicles parked beyond the communication range of the RSU. Because the parked vehicle cannot communicate with the RSU, it should receive information from the passing vehicle, which is a member of the same group and has the latest group key. In addition, before sending the group key, the passing vehicle should check the group membership of the parked vehicle. Moreover, after the group key transmission, the parked vehicle should be able to verify that the received group key is not forged. Neither verification contains any interaction with the third party because this vehicle-to-vehicle group key transmission is operated beyond the RSU's range. From the mathematical analysis, we prove that the proposed group key transmission scheme is strong against possible attack scenarios. In addition, we demonstrate that the privacy of the parked vehicle is guaranteed.

Acknowledgments

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. 2017-0-01705, Development of SDN Platforms and Security Schemes for Service Scalable and Trustable IoT Environments) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2017R1C1B5018116).

This paper is a revised and expanded version of a paper entitled "Development of Updating Group Key Method for Vehicles Parked Out-of-V2I Range in VANET" presented at International Conference on Green and Human Information Technology (ICGHIT), Hangzhou, China, February 15-17, 2018.

References

[1] B. Bold, J. E. Park and Y. H. Park, "Development of Updating Group Key Method for Vehicles Parked Out-of-V2I Range in VANET", Proceedings of International Conference on Green and Human Information Technology (ICGHIT), **(2018)**; Hangzhou, China.

[2] Y. H. Park and S. W. Seo, "Fast and Secure Group Key Dissemination Scheme for Out-of-Range V2I Communication", IEEE Transactions on Vehicular Technology, vol. 64, no. 12, **(2016)**, pp. 5642-5652.

[3] N. Liu, M. Liu, G. Chen and J. Cao, "The sharing at roadside: Vehicular Content Distribution using Parked Vehicles", Proceedings IEEE INFOCOM, Orlando, FL, **(2012)**.

[4] Y. Lu, B. Zhou, F. Jia and M. Gerla, "Group-based secure source authentication protocol for VANETs", IEEE Globecom Workshops, Miami, FL, **(2010)**.

[5] H. Zhu, R. Lu, X. Shen and X. Lin, "Security in Service-oriented Vehicular Networks", IEEE Wireless Communications, vol. 16, no. 4, **(2009)**, pp. 16-22.

[6] D. Boneh and X. Boyen, "Short Signatures without Random Oracles", Advances in Cryptology, EUROCRYPT, vol. 3027 of Lecture Notes in Computer Science, **(2004)**, pp. 56-73.

[7] C. Wong, M. Gouda and S. S. Lam, "Secure group communications using key graphs", IEEE/ACM Transactions on Networking, vol. 8, no. 1, **(2000)**, pp. 16-30.

[8] Y. Ji and S. W. Seo, "Optimizing the Batch Mode of Group Rekeying: Lower Bound and New Protocols", Proceedings IEEE INFOCOM, San Diego, CA, **(2010)**.

[9] Y. H. Park, D. H. Je, M. H. Park and S. W. Seo, "Efficient Rekeying Framework for Secure Multicast with Diverse-Subscription-Period Mobile Users", IEEE Transactions on Mobile Computing, vol. 13, no. 4, **(2014)**, pp. 783-796.

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

[11] M. H. Park, G. P. Gwon, S. W. Seo and H. Y. Jeong, "RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications", IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, **(2011)**, pp. 644-658.

[12] Y. Hao, Y. Cheng, C. Zhou and W. Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, **(2011)**, pp. 616-629.

[13] "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages", IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), **(2016)**, pp. 1-240.

[14] K. Laberteaux, J. Haas and Y. Hu, "Security Certificate Revocation List Distribution for Vanet", Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking (VANET), ACM, New York, NY, USA, **(2008)**.

[15] A. Wasef and X. Shen, "EDR: Efficient Decentralized Revocation Protocol for Vehicular *ad hoc* Networks", IEEE Transactions on Vehicular Technology, vol. 58, no. 9, **(2009)**, pp. 5214-5224.

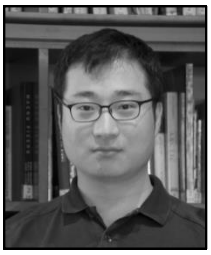
[16] M. Raya and J. Hubaux, "The Security of Vehicular *ad hoc* Networks", Proceedings of the 3rd ACM Workshop on Security of *ad hoc* and Sensor Networks (SASN), ACM, New York, NY, USA, **(2005)**.

[17] B. K. Chaurasia, S. Verma and S. M. Bhasker, “Message Broadcast in VANETs using Group Signature”, Fourth International Conference on Wireless Communication and Sensor Networks, Allahabad, **(2008)**.

[18] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, “A Scalable Robust Authentication Protocol for Secure Vehicular Communications”, IEEE Transactions on Vehicular Technology, vol. 59, no. 4, **(2010)**; pp. 1606-1617.

[19] D. Boneh and M. Franklin, “Identity-based Encryption from the Weil pairing”, SIAM J. Comput., vol. 32, no. 3, **(2003)**, pp. 586–615.

Author



Young-Hoon Park received B.S., M.S., and Ph.D. degrees from Seoul National University, Seoul, South Korea, in 2006, 2008, 2013, respectively. He was a senior engineer with Cloud Computing Lab, Software Center, Samsung Electronics, Suwon, South Korea. He was a Postdoctoral Researcher sponsored by Brain Korea 21 with School of Electronic Engineering, Seoul National University. He is currently an Assistant Professor with Division of Computer Science, Sookmyung Women’s University, Seoul, South Korea. He is also a committee member of the Institute of Electronics and Information Engineers, and International Conference on Green and Human Information Technology (ICGHIT) 2018. His research area includes network security, cryptography, and system optimization.