electronics

MDPI

Article

SSKM: Scalable and Secure Key Management Scheme for Group Signature Based Authentication and CRL in VANET †

Kiho Lim [1], Weihua Liu [1], Xiwei Wang [2] and Jingon Joung [3,*]

[1] Department of Computer Science, William Paterson University of New Jersey, Wayne, NJ 07470, USA; limk2@wpunj.edu (K.L.); liuw3@wpunj.edu (W.L.)
[2] Department of Computer Science, Northeastern Illinois University, Chicago, IL 60625, USA; xwang9@neiu.edu
[3] School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, Korea
* Correspondence: jgjoung@cau.ac.kr; Tel.: +82-2-820-5145

† This paper is an extended version of our paper published in the 8th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference, New York City, NY, USA, 19–21 October 2017.

Received: 1 October 2019; Accepted: 4 November 2019; Published: 11 November 2019

Abstract: The security in vehicular ad hoc networks (VANETs) has become a large consideration in safeguarding growing applications and intelligent transport systems. A group signature, a popular authentication approach for VANETs, can be implemented to protect vehicular communications against malicious users. However, the issue of securely distributing group keys to fast-moving vehicular nodes arises. The growing size of the certificate revocation list (CRL) has provided the corresponding complication in its management and distribution in VANETs. In this paper, an efficient key management protocol for group signature based authentication is proposed. A group is extended to a domain with various roadside units forming a hierarchical topology. Our proposed scheme provides a secure method to deliver group keys to vehicular nodes, ensuring the security requirements. Similarly, through utilizing the two Bloom filters in our hierarchical topology, an efficient and scalable vehicle revocation mechanism can be achieved that can minimize the CRL size. Our experiment results demonstrate a scalable, efficient, and secure key distribution scheme in vehicular networking. Moreover, an effective CRL management mechanism can be accomplished using the hierarchical topology.

Keywords: VANET; group signature; key distribution; CRL

1. Introduction

The vehicular ad-hoc network (VANET) is a special type of mobile ad-hoc network (MANET) with unique features, such as a dynamically changing topology, fast-moving vehicular nodes, and the ephemeral interaction of vehicular nodes. In VANET, vehicles can have a hybrid communication between vehicle-to-vehicle (V2V) communications or vehicle to infrastructure (V2I) communications [1]. The roadside units (RSUs) are located along the road to provide extensive coverage of the services to vehicular nodes in the networks. Vehicular nodes are equipped with an on-board unit (OBU), which is a communication and computation device that stores, computes and transmits the traffic information collected from the roads. Besides providing security services, VANETs also support various applications including traffic management, safety messages, and intelligent infotainment services [2].

Vehicles exchange information related to the weather, roadside emergencies, broadcasting alerts, navigation/maps, and entertainment services through shared wireless communication. Since the network is shared, the privacy of the user and the message integrity of the vital information are required to ensure that the driving environment is safe and sound. Thus, VANETs must provide the following security requirements [3] to protect their systems and applications against threats: (1) attackers should not be able to identify a particular vehicle by analyzing messages to ensure driver's privacy; (2) drivers' private information should not be associated with any type of messages in the message transmission; (3) the desired vehicles can only verify or decrypt intended messages; (4) the authenticity and integrity of messages should be guaranteed during communications.

The group signature [4] is a security approach that forms a group from a set of users, but the users remain anonymous. Boneh et al. [5] then proposed the short group signature where multiple group private keys are assigned to a single group public key. Many approaches employed a short group signature: Hao et al. [6] with a distributed key management (DKM) scheme used the trusted authority to generate and manage the group keys; Chim et al. [7] with the VANET-based secure and privacy-preserving navigation (VSPN) scheme applied the trusted authority to design and classify the users and also to distribute the group keys among the user groups and update them in the revocation procedure; Rongxing et al. [8] with the efficient conditional privacy preservation protocol for secure vehicular communications (ECPP) utilized the trusted authority alone to manage all the short-time anonymous keys for anonymous authentication. The practice of designing a trusted authority to perform such activities (managing and distributing the group keys) [6–8] leads the VANET architecture to be centralized and the trusted authority to bear a high amount of load. As the nodes in VANET interact with the multiple infrastructures while moving, the trusted authority (TA) needs to initiate, distribute, and monitor the group keys of all vehicles, as well as revoke certificates when necessary. However, since the key management is centralized, the network performance can be affected adversely. For example, when the backbone link is temporarily not available or system maintenance is required, the service would not be available until the issue is resolved.

Although the group keys are used for the secure V2V and V2I communications, there is still a challenge in delivering the group keys securely from the key generator to vehicles, and if the transmitted group keys are intercepted by the attacker, then it might impact the networks severely. Thus, this demands an efficient manner to deliver the secret keys to vehicular nodes. Regarding the group keys in VANET, it has only been applied to the set of nodes confined within the coverage of an RSU [6,7]. The RSU issues the keys to the vehicles only within its range, so the vehicle has to perform the key initialization process to get a key with every RSU along with its movement. If the coverage can be widened to a larger space, then the same group key can be utilized in the larger area so that the frequency of the group key initiation can be mitigated.

Vehicles are authenticated by the trusted authority using certificates that have an expiration time. To preserve the privacy and anonymity of the user, the certificates are frequently updated [9]. Upon the detection of malicious nodes, all the certificates that are held by such nodes must be revoked through the certificate revocation list (CRL). The growing size of CRL creates another issue in VANETs. To describe it further, a total of 4.3 million vehicles were stolen from 2011 to 2016 [10]. Even with one certificate (size of 100 bytes approximately) to one vehicle, the total size of the certificates to be revoked would be 431 MB. A larger size of certificates to be revoked creates a larger CRL size. Such a large CRL must be propagated throughout the entire vehicular network, which is a challenging issue in VANETs, as it demands the excessive consumption of resources.

To overcome the above-mentioned issues, in this paper, we propose a hierarchy based topology of VANET that comprises a number of RSUs as a domain with a leader RSU that manages the domain. Our group based signature scheme, an extended version of [11], intends to provide secure, scalable, and efficient key management solutions in VANETs. Besides, before issuing a key to a node, our scheme authenticates the vehicle's credential using the CRL list to allow the legitimate vehicles to communicate within the domain. Further, to deliver secret keys to vehicles in a secure manner, a symmetric key encryption is used between a vehicle and an RSU, which is faster due to its low computation overhead. A symmetric key can be obtained by the Diffie–Hellman key exchange protocol [12].

The utilization of the multiple group private keys and group public keys in the larger space, i.e., domain, improves the efficiency of the short group signature. Further, the group keys are managed by the leader RSU within the domain, which distributes the centralized workload of the trusted authority. Furthermore, with the distribution of the updated CRL in each domain, we aim to minimize the CRL size within VANETs such that vehicular nodes achieve the secure, efficient, and scalable key management mechanism with a small sized revocation lists.

The remainder of this paper is structured as follows. Section 2 discusses the background of our work. Section 3 introduces the system model and presents our proposed scheme in detail. Section 4 discusses the management of certificate revocation lists. In Section 5, we describe the analysis and the evaluation of our protocol. Finally, Section 6 concludes the paper.

2. Related Work

The security and privacy challenges in VANETs have been studied in many research articles. To preserve the privacy of drivers, threats to track the movement of vehicles and to reveal the identity of drivers should be prevented. In [13], a vehicle used a pseudo-identity called a pseudonym instead of its real identity to protect the privacy of the vehicle/driver. To keep the location privacy throughout the vehicle movement, pseudonyms should be dynamically updated, otherwise the location of vehicles can be tracked through the static pseudonyms' update, and driving patterns can be identified by eavesdroppers. This problem can be addressed by using multiple pseudonyms where the vehicle only uses each pseudonym for a certain amount of time. Besides, the new and used pseudonyms should be carefully changed to prevent eavesdroppers from identifying them. To address this issue, a silent period [14] and mix-zone [15] have been proposed to strengthen the security of the pseudonym schemes. A silent period is a transition period between the use of new and old pseudonyms. A mix-zone is the area where the pseudonyms can be replaced. However, finding such conditions requires extra computation, and it overlooks the potential of the attacker. Sampigethaya et al. [16] proposed another approach, called AMOEBA, to address the privacy preservation issue, where a group of vehicles is formed and managed by their group leader so all messages from the group members are forwarded to the group leader. While the privacy of group members is preserved under this approach, if the group leader is compromised, then all privacy information of the group members can be leaked.

Chaum et al. [4] introduced group signatures for anonymous authentication such that a member of a group can anonymously sign the message on behalf of the group. However, the proposed approach was not practical due to the large size of group signatures. Boneh et al. [5] re-constructed and made the size of the group signature under 200 bytes, which is suitable for practical applications. By the use of bilinear mapping, it had multiple group private keys associated with a single group public key. In this approach, a message signed with the group signature can be verified without knowing the sender. A pseudonymous authentication scheme was proposed by Sun et al. [17] for vehicular communication, which utilized the group signature to provide security, traceability, and anonymity. Similarly, a group signature based scheme [6] was proposed for key management and distribution. Under this scheme, an RSU distributes the group keys to its group members within its area for efficient key management and distribution; however, communication overhead caused by frequent key establishments was not considered. For example, if a vehicle enters the area of a new RSU, then it has to initiate the key establishment process over again. Further, how to deliver the group keys securely between the vehicles and the infrastructure was not discussed in this scheme, although it was a crucial component of the system.

Zhang et al. [18] presented an IBV (identity based batch verification), which uses an identity based signature to realize batch verification of signatures that can reduce the verification time of the signature; however, it is possible that a malicious vehicle can forge the signature, and it cannot detect an invalid signature. EPAS (efficient privacy-preserving authentication scheme) [19] is also an IBV based protocol that is modified to reduce the verification time for emergency communication. Ravi et al. [20] proposed an elliptic curve digital signature algorithm (ECDSA)-based message authentication scheme for VANET, and Huang et al. [21] proposed a scheme, called ABAKA (anonymous batch authenticated and key agreement scheme), for batch authentication and key agreement. Both algorithms utilized the ECDSA scheme for message authentication. Although the verification time in both ECDSA and ABAKA was lower compared to other schemes, the usage of the elliptic curve in every message added a large computational overhead. Thus, in this paper, we will compare the performance of our algorithm with the previously mentioned schemes in terms of the computation delay.

An anonymous authentication scheme [3] was proposed to provide the features of authentication, integrity, repudiation, and privacy, which were not present in the pseudonym schemes. In this scheme, each vehicle requires storing large preloaded anonymous public/private key pairs, and the authority has to handle the distributions of key pairs. Pseudonymous authentication schemes [22,23] are a kind of anonymous authentication scheme that uses a pseudonym certificate instead of the real vehicle identity. Certificate revocation lists (CRLs) have to be updated and stored for all the revoked vehicles, which makes this scheme less efficient.

As the number of vehicular node grows in VANET, it is very important that the existence of malicious nodes be considered, and such nodes must be revoked promptly when detected. To distribute such information quickly throughout the network, a CRL can be used. Since the CRL has to be distributed widely and quickly, it is necessary to compress it as much as possible for efficiency. To reduce the size of the CRL in VANET, several approaches have been proposed [24,25]. Besides, to address the false-positives associated with the Bloom filter, another interesting scheme that utilizes two Bloom filters was proposed [26]. Our proposed scheme leverages the two Bloom filters to deal with the false-positive problem, and a CRL can be efficiently distributed in a hierarchical manner.

In this paper, our goal is to design a scalable and secure key management framework such that vehicles can communicate with the same group keys as a group in a larger area covering multiple RSUs instead of the limited boundary of a single RSU. In our scheme, a domain leader, called the leader RSU, manages a domain for issuing group keys to all vehicles within the domain and maintaining all associated records. This alleviates the burden of the key management and distribution process on the trusted authority and provides a more scalable network.

3. Proposed Scheme

First, this section provides our system model and then a general overview of our proposed scheme. Finally, the secure key management scheme is elaborated. Table 1 lists the notations used in this paper.

Table 1. Notations. TA, trusted authority.

Notation	Description
V_i	a vehicle i
R_i	an RSU i
T_s	a time-stamp
$L\text{-}RSU$	a leader RSU
$M\text{-}RSU$	a member RSU
SK_{V_i}	private key of V_i
PK_{V_i}	public key of V_i
gpk	a group public key
$gsk[V_i]$	a group private key of a vehicle V_i
C_{V_i}	certificate of V_i issued by the TA
dgt	digital signature
$K_{V_i\_MR}$	shared secret key between V_i and $M\text{-}RSU$
FPR	false positive rate
N_v, N_r	Number of valid vehicles and revoked vehicles
m_v, m_r	bit vector length of valid and revoked vehicles
H_v, H_r	hash functions of valid and revoked vehicles
LR_{Index}	leader RSU index

3.1. System Model

We describe our system model and the assumptions for the proposed scheme. In the vehicular network, we assume that the following three key components exist: the trusted authority, two types of roadside units, and vehicular nodes. The overview of the system model is illustrated in Figure 1.

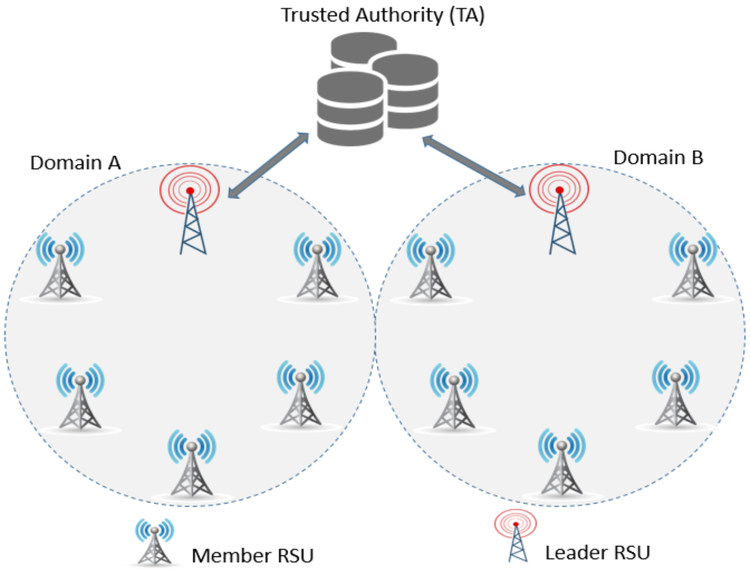

Figure 1. Overview of the system model.

- Trusted authority (TA): When vehicles join the network, they are registered, and their certificates are issued by the trusted authority. The TA and RSUs are securely connected via a wired connection network. An RSU can identify the real identity of vehicles with the help of the TA when an investigation is necessary. The TA manages and distributes the regional CRLs for the specific region. The TA also executes the revocation status query requests from any region. With the high-level security protection, we assume that the TA is trusted and cannot be compromised.
- Domain and roadside units (RSUs): RSUs are the infrastructure located along the roadside that plays an important role in message authentication/verification, key management, and message dissemination in the networks. A group of RSUs forms a domain. The number of RSUs within a domain can be determined based on the infrastructure capacity, geographical location, vehicle demography, and deployment plan. The size of the domain is defined as the desired number of vehicles that can be accommodated by the RSUs within a geographic region, called the domain.
- Leader roadside units (L-RSU): RSUs are classified into leader RSU (L-RSU) and member RSU (M-RSU). An L-RSU coordinates with the TA and generates the group private keys and group public keys for the vehicles within its domain. The L-RSU also manages and maintains the database of the group keys and the regional CRL for its domain. When detecting suspicious behavior, the L-RSU communicates with the TA to reveal the identity of the malicious vehicle or it can also send the query to TA to authenticate the certificate of the vehicle. Since the L-RSUs are the primary component in the key generation and management process, we assume that the L-RSUs are equipped with trusted platform modules and high level security protection, hence it cannot be compromised.
- Member roadside units (M-RSU): M-RSUs are not involved in the key generation and management process nor in the CRL management. Instead, M-RSUs help vehicles obtain the group keys and an up-to-date regional CRL produced by the L-RSU. Therefore, the M-RSUs are semi-trusted with medium level security protection.
- Vehicle nodes: Vehicle nodes are cars with an on-board unit (OBU) installed for communication and computation, a GPS (global positioning system) for location services, and an interface for

interacting with drivers/passengers. Vehicles can communicate with each other or with RSUs through the radio defined under the IEEE Standard 1609.2 [27], which is a standard for wireless access in the vehicular environment (WAVE). The group keys and public/private key pairs are used for vehicular communications to provide authentication and encryption/decryption features. All secret keys are stored in a tamper-proof device [28] for protection. A vehicle node validates received messages by evaluating the sender's certificate with the CRL. We assume that every vehicle obtained the public keys of the RSUs in the networks when registered by the TA, and they are regularly updated.

3.2. *Basic Idea behind Our Scheme*

In this paper, our proposed scheme utilizes a short group signature protocol [6,17] to generate group private keys. In the network, the L-RSU issues group private keys within a domain as a key generator. Here, a domain consists of multiple RSUs including the L-RSU and M-RSUs. In a domain, a group public key is associated with many corresponding group private keys, so any domain member can send a message with the signature of the domain, and any other members can verify the signed message using the group public key. Note that the M-RSUs are not involved in the key generation process, but they help the key establishment process. Compared with other group signature approaches, this offers insignificant overhead, and the group private keys could be retrieved from the signatures using tracing keys. Besides, the same group key can be used with different RSUs within the domain without having to generate another group key. Figure 2 illustrates how vehicles send request messages for a group private key to the L-RSU within a domain.

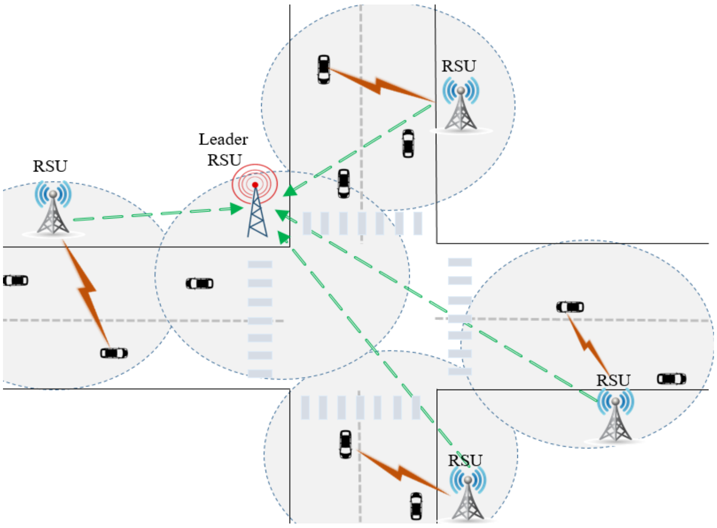

Figure 2. Group key request to the leader RSU.

3.3. *Short Group Signature*

We adopt a short group signature [6,17] in this paper, and the working of the short group signature is as follows.

3.3.1. Key Setup

To form the cryptographic system, the trusted authorities generate two bilinear multiplicative groups G_1 and G_2 with the generators g_1 and g_2 of a prime order p. Let χ be a computable isomorphism from G_2 to G_1 with $\chi(g_2) = g_1$. Now, parameters are selected by the trusted authority $h \xleftarrow{R} G_1 \setminus \{1_{G_1}\}$ and $\xi_1, \xi_2 \xleftarrow{R} Z_p^*$ randomly and set $u, v \in G_1$, such that $u^{\xi_1} = v^{\xi_2} = h$, where Z_p^* is a multiplicative group of order $p - 1$. TA randomly selects $\psi \xleftarrow{R} Z_p^*$ and then sets $w = g_2^{\psi}$. The private key can be derived as $gmsk_t = (\xi_1, \xi_2)$ and $gmsk_m = (\psi)$, respectively. Furthermore, the group public key for the vehicles in the domain can be derived as $gpk = (g_1, g_2, u, v, h, w)$.

3.3.2. Membership Registration

The registration process is initiated as the vehicle moves towards the domain. A tuple (A_i, x_i) for a vehicle i is maintained by the membership manager, which is the group private key of the vehicle $gsk[i]$. For the selection of the private key, a random number λ is chosen such that $A_i \leftarrow g_1^{1/(\lambda+x_i)}$. By using ψ, the authority selects $x_i \leftarrow Z_p^*$

Thus, the trusted authority saves the pair (A_i, ID_i) for future purposes. After the completion of the registration, the assigned private key is transmitted securely to the vehicle, which is covered in Section 3.4.

3.3.3. Signing

After receiving the group public key/private key pair, the vehicle can transmit a message after the signing procedure, which is detailed as follows:

First, it selects the exponents $\alpha, \beta \overset{R}{\leftarrow} Z_p$ and encrypts A_i, and (T_1, T_2, T_3). (T_1, T_2, T_3) are defined as follows: $T_1 \leftarrow u^{\alpha}$, $T_2 \leftarrow v^{\beta}$, $T_3 \leftarrow A_i h^{(\alpha+\beta)}$.

It then calculates $\delta_1 \leftarrow x\alpha, \delta_2 \leftarrow x\beta$ and picks the random numbers r_α, r_β, r_x, r_{δ_1}, $r_{\delta_2} \in Z_p$. It calculates R_1, R_2, R_3, R_4, R_5 as follows:

$$R_1 \leftarrow u^{r_\alpha}, R_2 \leftarrow v^{r_\beta}$$

$$R_3 \leftarrow e(T_3, g_2)^{r_x}.e(h, w)^{-r_\alpha - r_\beta}.e(h, g_2)^{-r_{\delta_1} - r_{\delta_2}}$$

$$R_4 \leftarrow T_1^{r_x}.u^{-r_{\delta_1}}, R_5 \leftarrow T_2^{r_x}.v^{-r_{\delta_2}}$$

Now, the challenge c can be obtained from the values above and the message M
$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p$

It calculates $s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}$ where s_α is defined as $s_\alpha = r_\alpha + c\alpha$,

$$s_\beta = r_\beta + c\beta, s_x = r_x + cx, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2$$

Now, the message is signed in the combination of the parameters:

$$\sigma \leftarrow (T_1, T_2, T_3, c, s_\delta, s_x, s_{\delta_1}, s_{\delta_2})$$

3.3.4. Verification

After receiving the signed message, the receiver first verifies the validity if the packet has arrived within the allowed time window. The receiver now recomputes the parameters to perform the signature verification by rebuilding the challenge c by itself. The following parameters $(R_1, R_2, R_3, R_4, R_5)$ are reconstructed as follows:

$$\tilde{R_1} \leftarrow u^{s_\alpha}/T_1^c, \tilde{R_2} \leftarrow u^{s_\beta}/T_2^c$$

$$\tilde{R_3} \leftarrow e(T_3, g_2)^{s_x}.e(h, w)^{-s_\alpha - s_\beta}.e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}}.(e(T_3, w)/e(g_1, g_2))^c$$

$$\tilde{R_4} \leftarrow {T_1}^{s_x} / u^{s_{\delta_1}}, R_5 \leftarrow T_2^{s_x} / v^{s_{\delta_2}}$$

Now, $\tilde{C}$ is re-computed from:

$$\tilde{C} = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$$

After computing the challenge, now the receiver verifies if the value of $\tilde{C}$ matches the value of c in the signature contained in σ.

3.3.5. Key Retrieval

This process is performed when the real identity of the signer needs to be revealed. The trusted authority checks the validity of the signature and calculates A_i as:

$$A_i \leftarrow T_3 / (T_1^{\xi_1} . T_2^{\xi_2})$$

The authority can now look up its saved database to identify the real identity from the element A_i.

3.3.6. Membership Revocation

If the vehicle is found to be compromised, its keys are identified by the TA. The provided group private key $gsk[i]$ to the vehicle i is associated with A_i through the tuple, and thus, the identity ID_i can be revealed. The identified vehicle is added in the CRL based revocation scheme, and the updated CRL is distributed to all the valid vehicular nodes; hence, the vehicle will be excluded from the system. The CRL based revocation scheme is covered in Section 4.

3.4. Scalable and Secure Key Management Scheme

In this section, we present the detailed protocol to distribute secret keys securely while defending the networks against malicious attackers. It is assumed that the L-RSU is fully trusted and the M-RSUs are semi-trusted with the possibility of being compromised. Under our scheme, vehicles can sign messages with the group name using a group private key. Because a single group public key is associated with many group private keys, receiver vehicles can verify the authenticity of the message by validating the signature with the group public key. Additionally, while the privacy of the message sender is preserved by the group name, the real identity of the sender can be disclosed if a legal investigation requiring the user information is required by the authorities. Figure 3 illustrates the message flow in our protocol and the detailed process of the protocol is shown in Table 2.

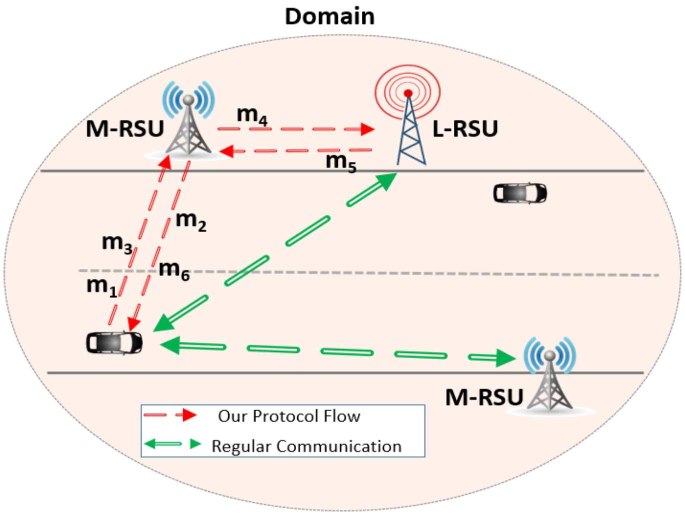

Figure 3. The protocol.

When a vehicle arrives in a region of a domain consisting of the L-RSU and multiple M-RSUs, it initiates a process to securely obtain a group public/private key pair by communicating with any RSU. The proposed secure key management scheme is based on the Diffie-Hellman key exchange protocol [12] for obtaining a symmetric key after mutual authentication. When a vehicle V_i receives beacon messages from a nearby RSU, V_i sends a message m_1 to launch the protocol. In the key establishment process, $\{A, B, g, p\}$ are the base elements of the Diffie-Hellman key exchange protocol, where p is a prime number, T_s is a timestamp, g is primitive root $mod\ p$, a is the secret integer kept by V_i, b is the secret integer kept by the RSU ($M\text{-}RSU$ or $L\text{-}RSU$), and C_{V_i} is the certificate of V_i issued by the TA. Besides, A and B are defined as $A = g^a\ mod\ p$ and $B = g^b\ mod\ p$, respectively. In the message m_1, $\{g, p, A \| T_s\}$ are encrypted with the private key SK_{V_i} of V_i so the vehicle V_i can be authenticated by the RSU after the timestamp is validated and the message is decrypted with the public key PK_{V_i} of V_i. Note that a timestamp T_s is inserted into the message to prevent the message replay attack. When $M\text{-}RSU$ receives the initial message, it sends the message m_2 by encrypting $\{A \| B \| T_s\}$ with the private key SK_{MR} of $M\text{-}RSU$ and encrypting B with the public key PK_{V_i} of V_i, respectively. When receiving the message m_2, V_i sends an acknowledgment message (m_3) for having received B by encrypting it with the private key SK_{V_i} of V_i. Now, g^{ab} serves as the common secret key $K_{V_i\_MR}$ between V_i and $M\text{-}RSU$, and this shared symmetric key is used for further communication. With an acknowledgment, V_i sends a $Request, C_{V_i}$ to $M\text{-}RSU$ to request a group secret key pair. As only $L\text{-}RSU$ can issue the group secret keys, $M\text{-}RSU$ sends the message m_4 on behalf of V_i to $L\text{-}RSU$. Note that only $L\text{-}RSU$ can decrypt and read the content of the messages because they are encrypted using the sender's public key for communications between RSUs. Once the identity of V_i is verified, $L\text{-}RSU$ issues a group public key/group private key $\{gpk, gsk[v_i]\}$ and sends the message (m_5) with a digital signature $dgt_L = E(H(M), SK_{LR})$ and a timestamp T_s to $M\text{-}RSU$, which can forward the key pair to V_i. It is worth pointing out that by attaching the digital signature dgt_L, it is ensured that the L-RSU for the domain generated the group key pair for the vehicle. Lastly, $M\text{-}RSU$ computes a keyed-hash message authentication code (HMAC) with the shared symmetric key $K_{V_i\_MR}$ and sends it with the m_5 received from the $L\text{-}RSU$ to V_i. This completes the secure key establishment and distribution process, and the vehicle V_i now can sign a message with the group public key $gsk[v_i]$ and verify the received messages with the group private key gpk within the region of the domain.

As a vehicular node moves on the road and detects an event such as accidents, traffic jams, bad road conditions, severe weather, and so on, it shares the event information with nearby vehicles or vehicles within the same domain so they can make informed decisions. When a vehicle broadcasts safety messages to the networks, it signs the message using the $gsk[v_i]$ issued by the $L\text{-}RSU$ of the domain. It is worth noting that if the message needs to be propagated beyond the communication range of the vehicle due to the importance of the message content, then the message can be further disseminated through nearby vehicles or other RSUs using a message dissemination scheme such as [29]. When such messages are received by vehicles, then they use the group public key gpk to verify the messages and utilize the information to take an appropriate action. However, it is still possible that the contents of the message could be falsified or malicious even if the message sender is authenticated. For example, a malicious legitimate user could broadcast a false message asserting an accident at a particular location to exploit the traffic on the road such as a traffic detour. If such a malicious message is found, it is reported to $L\text{-}RSU$ or the legal authorities. Since the real ID of the vehicle can be retrieved from the group private key $gsk[v_i]$ by $L\text{-}RSU$, $L\text{-}RSU$ can perform an investigation process using a verification scheme such as [30]. Note that our proposed scheme primarily focuses on addressing secure key distribution and the scalability issue for group signature based authentication; hence, evaluating message contents and alleviating broadcast overhead are beyond the scope of this paper.

Table 2. Key establishment process.

Vehicle ***V***		**Member RSU (*M-RSU*)**		**Leader RSU (*L-RSU*)**
1. Sends message m_1 to *M-RSU* $g, p, A, \{g, p, A \Vert T_s\}_{SK_{V_i}}, C_{V_i}$	→	2. Sends message m_2 to V_i		
		$(B)_{PK_{V_i}}, \{A \Vert B \Vert T_s\}_{SK_{MR}}, C_{MR}$		
3. Sends m_3 (Ack. and Request) to *M-RSU*	←			
$(B \Vert T_s)_{SK_{V_i}}, (Req)_{K_{V_i-MR}}$	→	4. Forwards request to *L-RSU* (m_4)		
		$ID_{LR}, ID_{MR}, \{Req, C_{V_i}, T_s\}_{PK_{LR}}$	→	5. Issues a group key and sends msg m_5
			←	$ID_{LR}, ID_{MR}, \{gpk, gsk[v_i], T_s, dgt_L\}_{PK_{V_i}}$
		6. Sends message m_6 to V_i		
	←	m_5, $HMAC(m_5)$		
7. V_i receives the group key and can use it				

4. CRL Management

In the VANET applications, an attacker can cause harm in many ways, for example a malicious vehicle can spoof the traffic message to make some roads congested and obtain the desired route. Similarly, corrupted vehicles could cause an accident by triggering warning signals in other vehicles, inducing them to apply the brake suddenly. Thus, the integrity of the message is crucial. All the messages received from the malicious vehicle must be detected first, and such nodes have to be isolated from the network. IEEE Std 1609.2, standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages [27], has specified that the vehicle must be authenticated using certificates issued by TA in a PKI format and defines the CRL that contains the identities of the revoked certificates of the vehicle. Such CRLs are managed by the authority and disseminated in the vehicular network securely, quickly, and broadly [31]. Under our scheme, the L-RSU always checks the authenticity of the vehicle before issuing the group keys. The L-RSU sends the certificate information to the TA. If a vehicle is malicious, then it revokes the certificates and distributes the CRL to all the vehicular nodes hierarchically through L-RSU, M-RSU, and the nodes. Thus, upon receiving any messages, vehicles can identify the legitimate sender by verifying the certificate in the CRL published by the TA.

A set of certificates is issued to the vehicles since an attacker can track a specific certificate. The number of certificates issued to a vehicle is determined by considering the amount of time the certificate will be used. Haas et al. in [25] stated that a vehicle will need around 5000 certificates per year considering a single certificate will be used for 10 mintues and, on average, vehicles operate 15 hours/week in the U.S. The vehicle must be able to store approximately 25,000 certificates if there is a requirement to replace the certificates once every five years. Considering that the size of each certificate is approximately 100 bytes, the storage size of the certificates required would be around 2.5 MB. However, if the vehicle is malicious, all the certificates held by the vehicles need to be revoked. Since the CRL should be broadly propagated, such growth in the size of the CRL would result in exorbitant storage requirements, computational overhead, and network bandwidth consumption.

To compress the revocation list, a Bloom filter [32] can be loaded with revoked certificate identifiers. A Bloom filter is a probabilistic data structure that specifies if the given element belongs as a member of the set. However, the query of the member returns either "possibly in the set" or "definitely not in set", i.e., false positive matches are possible in the Bloom filter. The Bloom filter consists of the bit vector with length m bits that is initialized to zero in the beginning. For CRL compression, the certificate serial number SN_i is saved in the bit vector after hashing with the k-hash functions. The element SN_i is stored by setting all the addresses of the bit vector to one, pointed at by the K hash functions of the certificate in the m bit vector. To validate the given SN_i of the certificate in the Bloom filter vector, the SN_i of the certificate is hashed by the k-hash functions, and the location is compared with the location of the provided Bloom filter. If all the bit locations are set (matched), then the given SN_i of the certificate is possibly on the list, otherwise it is not on the list. However, the bit vector is composed of the multiple hashes of the multiple SN_i of the certificates, and the bit can be set to one multiple times as different hashes can point to the same location. This causes a false match, and the false positive rate can be calculated as the following formula $P(\text{False positive Rate}) = (1-(1-1/m)^{KN})^K$ where $1-(1-1/m)^{KN})$ represents the probability that the location B_i is set to one. Thus, there is the probability that the search may result in the data item that does not belong in the filter, which occurs when a non-revoked certificate is treated as a revoked certificate.

To alleviate the effect of a false positive, we adopted the two Bloom filter scheme [26,33]. The concept of the two Bloom filter is illustrated in Figure 4. This scheme consists of the two bit vectors of various sizes $\{B_1, B_2, ...B_{m_r}\}$ and $\{B_1, B_2, ...B_{m_v}\}$ for the revoked certificates and the valid certificates. Then, the certificate serial number SN_i is hashed with two different hash functions $\{H_1(), H_2(), ...H_{K_r}()\}$ and $\{H'_1(), H'_2(), ...H'_{K_v}()\}$ for the Bloom filters of the valid and revoked certificates to store in the filter. It capitalizes on the fact that the Bloom filters are free of false negatives. To verify the status of the certificate, vehicular nodes use the technique as stated in Algorithm 1. The vehicle checks if the given certificate is in the list of revoked certificates by comparing it in the revoked bit vectors. If the search certificate is not on the list, then it is obviously true that the searched certificate is not revoked, and it is certainly valid; similarly, if the certificate is not found in the valid vectors, then it is assuredly revoked. If the given certificate is in both vectors, then this hints that one of them caused a false positive, and in such a case, the nodes have to query the authority for the authenticity of the given certificate. In this scheme, it will definitely find the searched certificate in at least one of the two vectors since the TA adds the certificate in one of the two vectors. Furthermore, if the certificate is found in both vectors, then it is because of the false positive that happened in one or both filters. As stated in the algorithm, when the Bloom filter generates the false positive, the algorithm will find out the SN_i of the certificate, and the TA verifies the authenticity of the certificate that has generated the false positive. Thus, it will minimize the possible error of misidentifying the valid certificate as a revoked certificate.

$$FPR_r = \left(1-\left(1-\frac{1}{m_r}\right)^{K_r N_r}\right)^{K_r} \tag{1}$$

$$FPR_v = \left(1-\left(1-\frac{1}{m_v}\right)^{K_v N_v}\right)^{K_v} \tag{2}$$

$$\begin{aligned} CVFP = P_r\,(\text{certificate is revoked}) \times FPR_v \\ +P_r\,(\text{certificate is valid}) \times FPR_r \end{aligned} \tag{3}$$

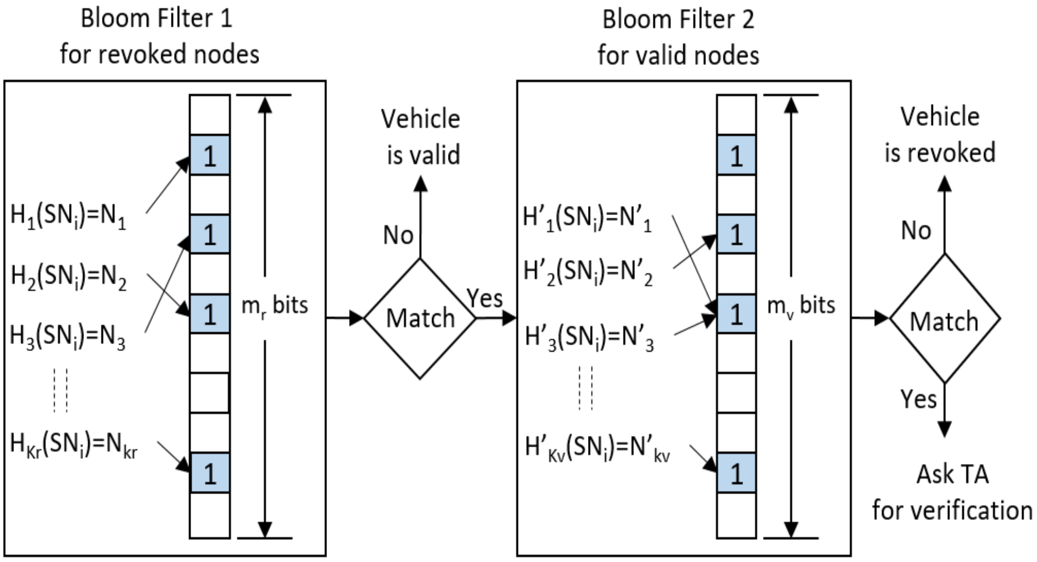

Figure 4. Two Bloom filters.

The rate of false positives in the revoked and the valid certificate Bloom filters are shown in Equations (1) and (2). K_r, N_r, and m_r are the number of hash functions used while composing a Bloom filter for the revoked certificates, the number of revoked certificates, and the bit vector size of the Bloom filter for the revoked certificates. Similarly, K_v, N_v, and m_v are the number of hash functions used while composing a Bloom filter for the valid certificates, the number of valid certificates, and the bit vector size of the Bloom filter for the valid certificates. The vehicle will not be able to verify the certificates if the false positive occurred in either of the two Bloom filters or both filters. Equation 3 represents the $CVFP$ (certificate verification failure probability), which corresponds to the probability that the revoked certificate filter causes a false positive and the certificate is valid or the valid certificate filter causes a false positive and the certificate is revoked. It can be observed that the probability of failure can be computed using six parameters including the number of valid certificates N'_v, the number of revoked certificates N_r, the size of the two Bloom filter vectors m_r and m_v, and the number of hash functions K_r and K_v.

Algorithm 1: Verifying the certificate in the TBFV scheme.

```
Data: $SN_i$ of the vehicle $i$
if $SN_i$ is not in the revoked certificate bit vector then
    return $SN_i = valid$;
end
if $SN_i$ is not in the valid certificate bit vector then
    return $SN_i = revoked$;
else
    request TA for further checking;
end
```

Using a single Bloom filter, a false positive rate for 1000 revoked vehicles can be calculated by using k, m, and N. Assuming 25,000 certificates of each vehicle, N = 25,000 × 1000 certificates. If a bit vector of $m = 2^{28}$ bits (32 MB) is chosen and six hash functions are assumed ($k = 6$), then the false positive rate of 0.616% is obtained, which is approximately one in every 160 certificates. It is observed that the Bloom filter compresses the revocation lists; however, the false positive may indicate a valid certificate as a revoked certificate, which can also cause an accident if the valid vehicle is revoked while sending crucial messages. However, in the two Bloom filter scheme, the verification failure probability can be reduced more than the false positive rate of the Bloom filter. The verification failure probability can be set by choosing the appropriate vector sizes and hash functions, i.e., if we increase the Bloom filter vector sizes, it reduces the verification failure probability. The verification failure probability of 0.1 can be obtained by selecting $m_r = 8N_r$ and $m_v = 1.5N_v$. The same probability of 0.1 can be achieved with $m_v = 2.5N_v$ and $m_r = 6N_r$, but since $N_v >> N_r$, the revocation information size in the latter one is higher than the first case. Thus, to use the TBFV scheme, it is required to determine the desired rate of failure probability and the optimal values of m_v and m_r pairs so that the desired verification probability can be achieved with the minimum revocation information size.

In our scheme, TA will manage and maintain the updated CRL. All the L-RSUs of the domains synchronize with the updated CRL and distribute it hierarchically to the M-RSUs and vehicular nodes. All vehicles will have the updated CRL, which contains the two Bloom filter of the revoked and valid vehicles. In every communication, a vehicle will compare the SN_i of the communicating node with the two Bloom filter and find out if it is valid or revoked. The concept of the hierarchical distribution of the CRL from the TA to the domain L-RSU, its M-RSU, and the vehicular nodes makes the CRL distribution very efficient and manageable.

5. Evaluation and Analysis

5.1. Security Analysis

In this section, a thorough analysis of the security strength of the proposed scheme is presented with respect to the various attack models discussed in Section 3.1.

5.1.1. Source Authentication and Privacy

When group keys are assigned to vehicles for communication, the L-RSU provides group keys only after the identity of vehicles is validated. Furthermore, the L-RSU maintains a database of the group keys, certificates, shared secret keys, and the timestamps of the vehicles in the domain. If a vehicle signs a message using its group private keys, then the L-RSU can trace its identity with the help of the TA when necessary. Furthermore, vehicles are assigned group keys for a domain, so vehicles do not use their private information; hence, the privacy of vehicles is preserved.

5.1.2. Anonymity

Once a vehicle is registered within a domain, the vehicle is provided with the group key for communication. Due to the feature of the group signature, the vehicle will remain anonymous with respect to other group members. After changing a domain, the vehicle needs to update group keys for further communication. Note that the original identity can be tracked down by the L-RSU when required.

5.1.3. Non-Repudiation

A vehicle cannot deny the message it has sent and the authenticity of its signature. Since the L-RSU maintains the database of issued group private keys, it can track the identity of the signer from its database table because only a vehicle having the group private key can generate the same signature.

5.1.4. Man-in-the-Middle Attack

In our scheme, the Diffie–Hellman key exchange protocol is adopted to share a symmetric key in the key establishment process for vehicular communication. The Diffie–Hellman protocol is known to be vulnerable to the man-in-the-middle attack [34]. However, our protocol does not suffer from this attack because a vehicle V_i encrypts the contents of the message during the key establishment process with its private key PK_{V_i}. Furthermore, if a legitimate vehicle tried to launch the man-in-the-middle attack using the public/private key pair generated by the TA, then the L-RSU and the TA could trace the identity of the vehicle.

5.1.5. Other Attacks

Sybil Attack

This is a type of security attack that is possible when a malicious node can use multiple identities while communicating. In our protocol, a group key is assigned to a vehicle by the RSU after validating its certificate which is issued by TA; thus, only a legitimate vehicle can get the group key, and only one group key is assigned to the specified vehicle. The vehicle encrypts the outgoing message using the group key, which is provided by the RSU. Hence, a vehicle cannot use multiple group keys to communicate, i.e., a malicious node cannot communicate with multiple identities.

Replay Attack

The replay attack in VANET occurs when the adversary re-injects the previously received message or the packets. Such attacks can be prevented using the timestamps on the message. This is implemented in our protocol to avoid replay attacks.

Message Alteration Attack

Such attacks are performed to modify, delete, or alter the content of the existing message. In our scheme, we used the group signature, which is itself a signature, and only the sender can create it. If the vehicle encrypts the message using the group private key, then the RSU decrypts it using the group public key and examines the integrity of the message. Hence, the fabrication/alteration attack is prevented. However, for the relay messages, the vehicle can deny or delete the message that is supposed to be forwarded to the next vehicle. Handling un-cooperative nodes has been studied in the ad-hoc context, and a similar approach can be implemented.

Collusion Attack

Even if the vehicle colludes and sends the fake messages, no matter how many vehicles collude, they have to use the group private keys for the communication, and their original ID can be traced by the authority on such an occasion. Further, if multiple vehicles colluded to send the fake messages, such messages would be reported to the RSU by the genuine vehicles, and the authority would trace such colluding malicious vehicles.

Revoking Malicious/Misbehaving Node

If the node is found to be misbehaving, then such a node must be detected and revoked from the vehicular networks. Due to the use of the CRL management system, our system is secure against such misbehaving nodes.

5.2. Performance Evaluation

We simulated the proposed scheme in SUMO [35] and NS-2 [36], as the mobility simulator and the network simulator, respectively. The IEEE 802.11p protocol was used in the simulation. The map of the simulation environment had a dimension of 3600 m × 3600 m, and we assumed that the vehicles ran at 51 km/h on average (which is identical to the average vehicle speed in the United States [37]) within a domain in a random fashion. We evaluated the performance of the proposed scheme from the following aspects: key establishment, communication overhead, and group key utilization. The performance of the proposed scheme has been evaluated in three aspects, namely key establishment, communication overhead, and group key utilization. Our simulation results show that the time required to establish keys could be reduced by using the group key within a domain, and with a larger size of domain, the same group key could be used by the vehicles for a longer time.

5.2.1. Key Establishment

In each group, it is required to use group keys by vehicles to communicate with each other. Without splitting the roles of the RSU into M-RSU and L-RSU, the key exchange procedure must be carried out by the vehicles with each RSU individually. Whenever a single vehicle reaches the boundary of one RSU, it needs to establish a new key with the next RSU to continue its communication. By using the proposed scheme SSKD, the communication between vehicles required only the group key within the whole domain. In our simulation, we assumed that vehicles can move in any direction for any distance. Each domain is defined as an area that is covered by four RSUs. Figure 5 shows that when domains are not used, with the increasing travel time of the vehicles, the average number of key establishments in PACP (pseudonymous authentication-based conditional privacy protocol), IBV, and ECDSA grow significantly. It is worth noting that during the time interval of 240 s, 16 distinct keys were exchanged by vehicles when domains were not used. However, when domains were used, only four distinct keys were exchanged in the same time interval.

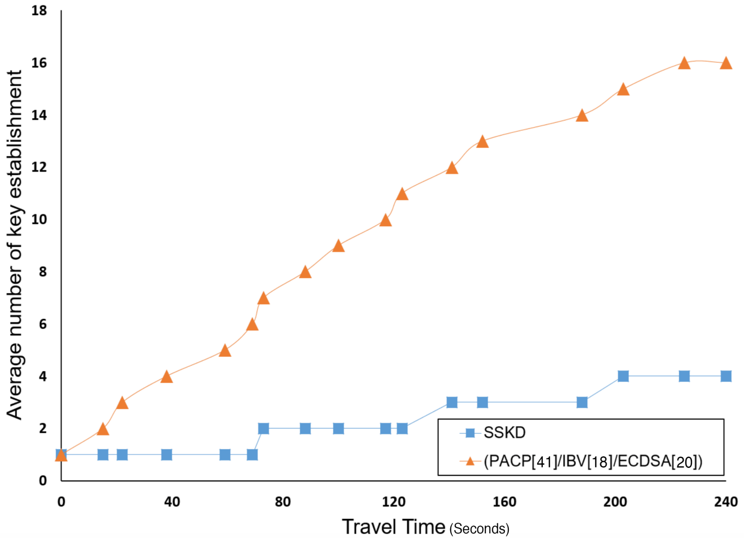

Figure 5. Average number of key establishments.

The authors in [17] studied the computation time of the group signature. In our experiments, we studied the time cost for the group signature that uses domain and the one that does not take advantage of using domain. We found that computing the group signature with domain took 3.6 ms less than computing the one without domain. The former also took 7.2 ms less time in terms of verification. When domain is not used, it took 172.8 ms, computed as 16 × (3.6 + 7.2), to sign and verify the 16 key establishments. On the contrary, when using a domain covered by four RSUs, the time cost was 43.2 ms, i.e., 4 × (3.6 + 7.2). Due to the fact that all RSUs were interconnected by a stable link, the time for forwarding their symmetric keys can be neglected. Accordingly, it is reasonable to assume that the time the randomly moving vehicles take to establish keys is almost identical to 43.2 ms, using a domain that is only as large as four RSUs. Compared to the scenario without using domain, the proposed scheme saved 75% of the time. Note that in real-world applications, more time could be saved when a larger domain size is used.

5.2.2. Group Key Utilization

After a vehicle has established the key, the duration of its traveling within the domain is considered as the group key utilization time. The purpose of measuring this time is to study how frequently the group key is used and to understand how the size of the domain affects the vehicle travel time on average. In our experiments, when simulating the vehicles, we tested different numbers of RSUs in a domain.

Figure 6 describes, after the group keys were established in varying sized domains, how the number of vehicles affects the group key utilization time. As is shown in the figure, the vehicles stayed within an RSU for around 30–40 s on average. If we added two RSUs to the domain, it took the vehicles about 45 s to travel. When more RSUs were added, i.e., the domain became larger in size, the average travel time would increase accordingly. When four RSUs were deployed in a domain, the result showed that the moving vehicles utilized the group key about 200% more than the ones that did not have a domain-wide group key. Therefore, we can conclude that with larger domains, the same group key can be used for a longer period of time.

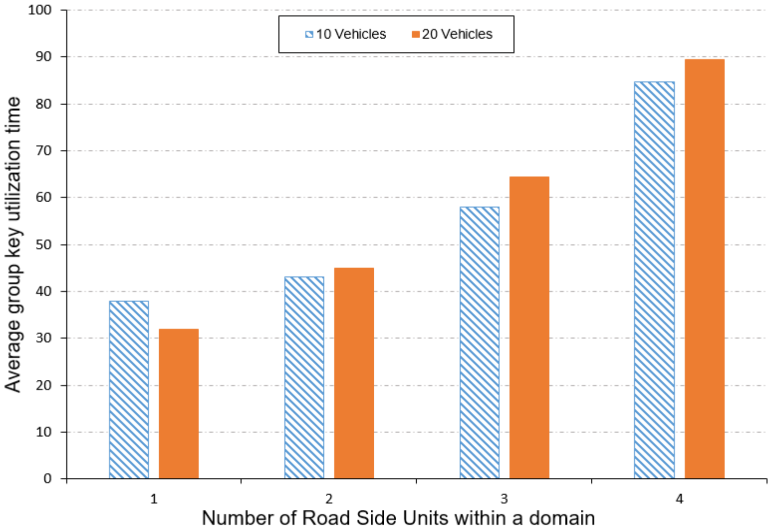

Figure 6. Group key utilization.

Table 3 shows the modified CRL format [27] in accordance with our proposed scheme. As we have used the hierarchical topology, overall, VANETs were split into domains that had domain leader L-RSU. The L-RSUs were enumerated by LR_{INDEX}, which has been highlighted as an additional field of the CRL format. Other additional fields include hash functions and the bit vectors of the two Bloom filters, which represent the domain and the revocation list based on the dual Bloom filter. One of the major components of the hash functions is the number of independent hash functions K_r and K_v that hashed the bit vector m_r and m_v of the dual Bloom filter. The hash functions also included the key components of CRL, namely a version, unsigned part, signed part, signature, and the certificate. The CRL version provides the information about the latest release. The unsigned field contains: craca_id, issue date, next CRL, PriorityInfo, which describe the CA identity, the timestamp of the issued CRL, the estimated time for the next CRL arrival, and the CRL priority, respectively. The trusted authority then signs the unsigned portion and appends it to the ECDSA signature. In this approach, the regional CRL had a size of $(126.5 + K_r + K_v + m_r + m_v)$ bytes.

Table 3. Regional CRL format.

Field	Description			Size(bytes)
Version		Certificate	Unit8	2
carca_id	Unisigned	CA_ID field	SIZE(8)	8
Issue Date		CRL issued time stamp	Unit32	8
Next CRL		Next Expected CRL	Unit32	8
Priorityinfo		CRL Priority	Unit8	2
LR_Index		***L-RSU index ID***		**2.5**
Hash_functions		***For revoked and valid certificate***	***Domain Variable***	***K_r***
				K_v
Two Bloom Filter		***Revoked bit vector***	***Domain Variable***	***m_r***
		Valid bit vector		***m_v***
Signature(ECDSA)		r	Data encryption	32
		s		32
Certificate	Signed	Public Key of TA	Authentication	32

The expected size of the CRL can be found with the values of K_r, K_v, m_r, and m_v. If the scheme used five different SHA-256 hash functions $H_1(), H_2(), ...H_5()$ for both bit vectors, then $K_r = K_v = 160$ bytes (with the SHA-256 hash functions, it took 32 bytes for each hash function). Rabieh et al. [26] provided the values of m_r, m_v for different certificate verification failure probability (CVFP). When CVFP = 0.05: $m_r = 8 \times N_r$ and $m_v = 3 \times N_v$; CVFP = 0.1: $m_r = 8 \times N_r$ and $m_v = 1.5 \times N_v$; and CVFP = 0.15: $m_r = 6 \times N_r$ and $m_v = N_v$. If we assume that 10% of the total certificates (N) were revoked, then the revoked certificates were $N_r = 0.1 \times N$, and the valid certificates were $N_v = 0.9 \times N$.

In Figure 7, we illustrate the size of the regional CRLs against the number of vehicles with three different verification failure probabilities. It can be seen that when each vehicle is assigned only one certificate, the lowest CFVP corresponded to the biggest size of CRL. For 40,000 vehicles, the CRL size is 18 KB when CFVP = 0.05; it is 11 KB when CFVP = 0.1; and 8 KB when CFVP = 0.15. Apparently, we can find the trade-off between CFVP and the size of the CRL. It is worth noting that, when the CVFP is very high, the query would require retransmission more frequently, and it also would add latency during the communication, which is not an optimal option in the scenario of vehicular communication. An appropriate value of CVFP can be set by considering network parameters like the delay requirement and resource utilization.

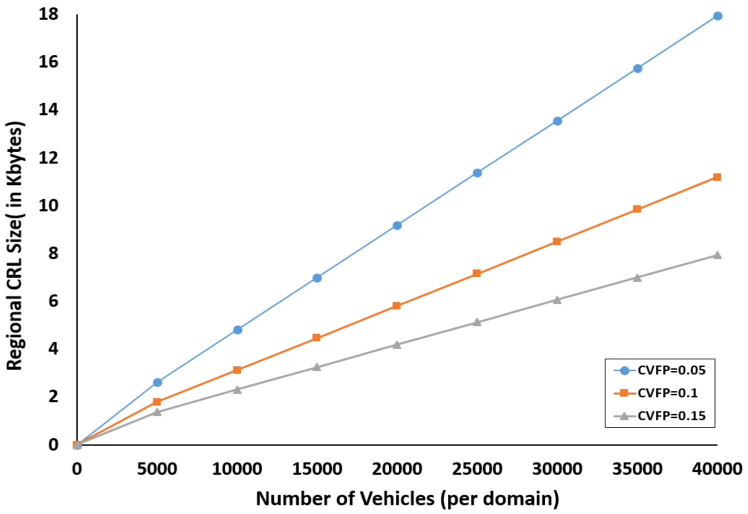

Figure 7. Regional CRL size with the domain size.

The scheme proposed in this paper provides the benefit of reduced CRL size with hierarchical domains. According to [38], there were approximately 63 million cars sold in America during the past decade. With one certificate per vehicle, if we set CFVP to 0.1 and the revocation probability to 10%, the global CRL size would be 17 MB. If we assume that each domain contained only 10,000 vehicles, then the regional CRL would be only 11 KB. The CRL size is thus reduced by a factor of 1600 times, meaning that most unessential network usage can be reduced.

5.2.3. Communication Overhead

In this subsection, we evaluate and compare the performance of our proposed scheme SSKM in terms of the verification delay with other schemes because the key generation and signing took similar constant time for all the schemes. In our scheme, when the vehicle establishes the group key and sends the message for VANET communication, the receiver (M-RSU or another vehicle) checks the authenticity of the requesting vehicle by comparing the challenge. The receiver has to compute R1, R2, R3, and R4. The most expensive part of the verification process is to compute R3. It consists of three multiplication and four pairing operations.

From the experiments in cryptographic pairing in [39] which observed the processing time for an MNT curve [40] of embedding degree k = 6 and 160-bit q, running on an Intel Pentium IV 3.0 GHZ machine, the following results were obtained: the multiplication time ($Tmul = 0.6$ ms) and pairing time ($Tpar = 4.5$ ms). T_{mtp} is the time for map-to-point in hash operation. Thus, the timing for verification of our proposed scheme can be calculated as: $3Tmul + 5Tpar$.

Here, we compare our signature algorithm scheme, which is Boneh–Boyen–Shacham (BBS) Group Signatures [5], with the other related signature algorithm schemes such as IBV [18], PACP [41], ECDSA [20], EPAS [19], and ABAKA [21] in terms of the verification delay. ECDSA is the signature algorithm used in the IEEE1609.2 standard, while PACP uses the BLS scheme, which is a short group signature scheme performed for signature aggregation. ABAKA and identity based verification (IBV) are the typical batch verification approaches adopted in VANET for anonymity and security, while EPAS is an identity based signature schemes with conditional privacy. The computational overhead of our scheme and other schemes is given in Table 4.

Table 4. Delay comparison of various signature schemes. SSKM, scalable and secure key management scheme; IBV, identity based batch verification; EPAS, efficient privacy-preserving authentication scheme.

Scheme	Verification Overhead	Delay
SSKM:	$3T_{mul} + 5T_{par}$	24.3 ms
IBV [18]:	$3T_{par} + T_{mtp} + T_{mul}$	14.7 ms
PACP [41]:	$4T_{par} + 2T_{mtp}$	12 ms
ECDSA [20]:	$4T_{mul}$	2.4 ms
EPAS [19]:	$5T_{mul}$	5 ms
ABAKA [21]:	$7T_{mul}$	4.2 ms

The verification overhead in the BBS scheme is higher compared to the other approaches. However, the BBS scheme had the feature of the group signature where multiple group public keys can be assigned for a single group private key, which is suitable for the authentication of a vehicle. The BBS scheme took a longer time to verify the signature, but in our approach, when a vehicle reached the domain, it asked for the key only once, while it would be verified throughout the domain. For example, for a single vehicle signature, our scheme took $3 * 0.6 + 5 * 4.5 = 24.3$ ms, whereas the IBV scheme took 14.7 ms. However, considering the domain size of 3 RSU (minimal), our approach still took 24.3 ms, whereas IBV would take $14.7 * 3 = 44.1$ ms. Thus, the BBS scheme in our approach outperformed other signature schemes.

Figure 8 shows the ratio of our scheme over other related schemes with respect to the verification time delay. As the domain can accommodate a number of RSUs in our scheme, the ratio would keep decreasing as the number of RSUs in the domain keeps increasing. It has been observed that as the domain contained seven RSUs, the ratio of verification delay time is below one for all the schemes, which entails that the delay associated with our scheme is less than the other signature. Thus, with the increase in the domain size, the efficiency of our scheme also increases.

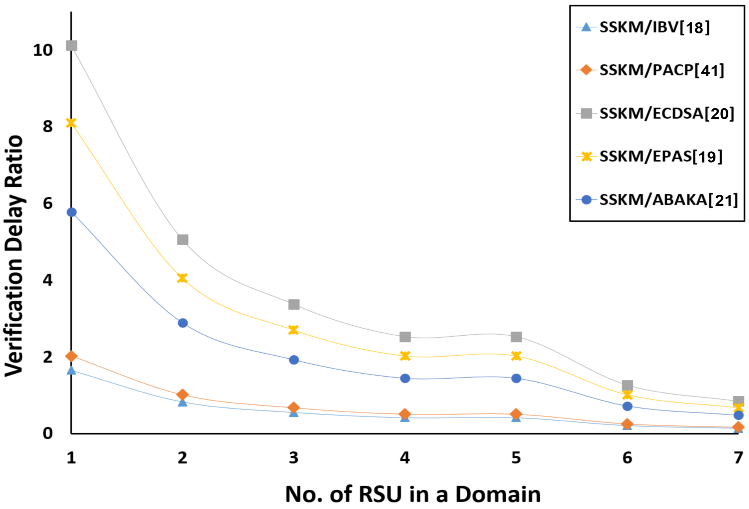

Figure 8. Verification delay ratio with multiple schemes.

6. Conclusions

In this paper, a scalable, secure, and efficient key management scheme is proposed for group signature-based authentication and the certificate revocation list in vehicular networks. It provides a scalable solution for vehicular networking security. The proposed scheme introduces the use of the domain with multiple RSUs into the framework. By doing this, a single group key could be utilized for a longer time without re-establishing a new one. Additionally, our scheme provides a secure key exchange protocol, which allows group keys within a domain to be delivered to vehicular nodes in a secure manner. On top of this, by separating the roles of RSU into L-RSU and M-RSU, the proposed scheme features a distributed key management mechanism. It also addresses the issue of the increased CRL size, which has been one of the major concerns in VANETs. Utilizing two Bloom filters in a hierarchical topology, our approach allows the minimized CRL size to be distributed for a small region; hence, an efficient and effective CRL management is achieved. To evaluate the performance of our scheme, we analyzed the possible security attacks and threats. Through our analytical evaluation and experiments, it was shown that our SSKM scheme is a scalable, secure, as well as efficient solution to vehicular networking.

Author Contributions: Conceptualization, K.L., J.J.; formal analysis, W.L.; investigation W.L.; methodology, K.L., X.W.; project administration, K.L.; validation, X.W.; writing—original draft, K.L.; writing—review & editing, W.L., X.W., and J.J.; supervision, J.J.

Funding: This research was supported by the National Research Foundation of Korea (NRF) grants funded by the Korean government (MSIT) (NRF-2019R1A2C1084168 & 2018R1A4A1023826).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Papadimitratos, P.; De La Fortelle, A.; Evenssen, K.; Brignolo, R.; Cosenza, S. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE Commun. Mag.* **2009**, *47*, 84–95. [CrossRef]
2. Hartenstein, H.; Laberteaux, K. *VANET Vehicular Applications and Inter-Networking Technologies*; John Wiley & Sons: Hoboken, NJ, USA, 2009; Volume 1.
3. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]

4. Chaum, D.; Van Heyst, E. Group signatures. In *Advances in Cryptology—EUROCRYPT'91*; Springer: Berlin, Germany, 1991; pp. 257–265.
5. Boneh, D.; Boyen, X.; Shacham, H. Short group signatures. In *Crypto*; Springer: Berlin, Germany, 2004; Volume 3152, pp. 41–55.
6. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A distributed key management framework with cooperative message authentication in VANETs. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 616–629. [CrossRef]
7. Chim, T.W.; Yiu, S.M.; Hui, L.C.; Li, V.O. VSPN: VANET-based secure and privacy-preserving navigation. *IEEE Trans. Comput.* **2014**, *63*, 510–524. [CrossRef]
8. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the IEEE INFOCOM 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
9. Buttyán, L.; Holczer, T.; Vajda, I. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *European Workshop on Security in Ad-hoc and Sensor Networks*; Springer: Berlin, Germany, 2007; pp. 129–141.
10. U.S. Department of Justice. Federal Bureau of Investigation. 2018. Available online: https://www.iii.org/fact-statistic/facts-statistics-auto-theft (accessed on 23 July 2017).
11. Lim, K.; Tuladhar, K.M.; Wang, X.; Liu, W. A scalable and secure key distribution scheme for group signature based authentication in VANET. In Proceedings of the 8th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference, New York, NY, USA, 19–21 October 2017; pp. 478–483.
12. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
13. Gerlach, M. Assessing and improving privacy in VANETs. In Proceedings of the Fourth Workshop on Embedded Security in Cars (ESCAR), Berlin, Germany, 14–15 November 2006; pp. 19–28.
14. Huang, L.; Matsuura, K.; Yamane, H.; Sezaki, K. Enhancing wireless location privacy using silent period. In Proceedings of the 2005 IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 13–17 March 2005; pp. 1187–1192.
15. Freudiger, J.; Raya, M.; Félegyházi, M.; Papadimitratos, P.; Hubaux, J.P. Mix-zones for location privacy in vehicular networks. In Proceedings of the 2007 ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), Vancouver, BC, Canada, 14 August 2007; number LCA-CONF-2007-016.
16. Sampigethaya, K.; Li, M.; Huang, L.; Poovendran, R. AMOEBA: Robust location privacy scheme for VANET. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1569–1589. [CrossRef]
17. Sun, X.; Lin, X.; Ho, P.H. Secure vehicular communications based on group signature and ID-based signature scheme. In Proceedings of the 2007 IEEE ICC International Conference, Glasgow, UK, 24–28 June 2007; pp. 1539–1545.
18. Zhang, C.; Lu, R.; Lin, X.; Ho, P.H.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the IEEE INFOCOM 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250.
19. Jia, X.; Yuan, X.; Meng, L.; Wang, L.M. EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication. *JSW* **2013**, *8*, 1914–1922. [CrossRef]
20. Ravi, K.; Kulkarni, S. A secure message authentication scheme for VANET using ECDSA. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–6.
21. Huang, J.L.; Yeh, L.Y.; Chien, H.Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2010**, *60*, 248–262. [CrossRef]
22. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. In Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, Montreal, QC, Canada, 10 September 2007; pp. 19–28.
23. Sun, Y.; Lu, R.; Lin, X.; Shen, X.; Su, J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3589–3603. [CrossRef]
24. Rigazzi, G.; Tassi, A.; Piechocki, R.J.; Tryfonas, T.; Nix, A. Optimized Certificate Revocation List Distribution for Secure V2X Communications. *arXiv* **2017**, arXiv:1705.06903.
25. Haas, J.J.; Hu, Y.C.; Laberteaux, K.P. Efficient certificate revocation list organization and distribution. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 595–604. [CrossRef]

26. Rabieh, K.; Mahmoud, M.M.; Akkaya, K.; Tonyali, S. Scalable certificate revocation schemes for smart grid ami networks using Bloom filters. *IEEE Trans. Dependable Secur. Comput.* **2017**, *14*, 420–432. [CrossRef]
27. *1609.2-2016—IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*; IEEE: New York, NY, USA, 2016; pp. 1–240.
28. Rosen, S.S. Tamper-Proof Electronic Processing Device. U.S. Patent 6,088,797, 11 July 2000.
29. Lim, K.; Manivannan, D. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Veh. Commun.* **2016**, *4*, 30–37. [CrossRef]
30. Raya, M.; Papadimitratos, P.; Gligor, V.D.; Hubaux, J.P. On data-centric trust establishment in ephemeral ad hoc networks. In Proceedings of the IEEE INFOCOM 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1238–1246.
31. Raya, M.; Jungels, D.; Papadimitratos, P.; Aad, I.; Hubaux, J.P. *Certificate Revocation in Vehicular Networks*; Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL: Lausanne, Switzerland, 2006.
32. Song, H.; Dharmapurikar, S.; Turner, J.; Lockwood, J. Fast hash table lookup using extended Bloom filter: An aid to network processing. *ACM SIGCOMM Comput. Commun. Rev.* **2005**, *35*, 181–192. [CrossRef]
33. Tuladhar, K.M.; Lim, K. Efficient and scalable certificate revocation list distribution in hierarchical VANETs. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 620–625.
34. Rivest, R.L.; Shamir, A. How to expose an eavesdropper. *Commun. ACM* **1984**, *27*, 393–394. [CrossRef]
35. Simulation of Urban Mobility. Available online: http://sumo.dlr.de/index.html (accessed on 22 June 2017).
36. NS-2. Available online: http://nsnam.sourceforge.net/wiki/index.php (accessed on 22 June 2017).
37. Insurance Institute of Highway Safety. 2008. Available online: http://www.iihs.org/iihs/sr/statusreport/article/43/1/1 (accessed on 7 July 2017).
38. Wagner, I. U.S. Car Sales. 2018. Available online: https://www.statista.com/statistics/199974/us-car-sales-since-1951/ (accessed on 7 July 2017).
39. Scott, M. Efficient Implementation of Cryptographic Pairings. 2007. Available online: http://www.pairing-conference.org/2007/invited/Scottslide.pdf (accessed on 23 August 2018).
40. Miyaji, A.; Nakabayashi, M.; Takano, S. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2001**, *84*, 1234–1243.
41. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]