International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.9-24
http://dx.doi.org/10.14257/ijsia.2014.8.2.02

A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs

Su-Hyun Kim and Im-Yeong Lee*

Department of Computer Software Engineering, Soonchunhyang University
{kimsh, imylee}@sch.ac.kr

Abstract

VANETs (Vehicular Ad-hoc Networks) are a next-generation networking technology that provides communication between vehicles or between a vehicle and an RSU (Road Side Unit) using wireless communication. A vehicle accident is likely to cause a serious disaster. Therefore, the VANET system provides an essential information exchange protocol for communication between vehicles. However, a key exchange scheme based on the proposed general network for a high-speed communication environment is not suitable for vehicles. In this paper, the first communication from the RSU passes only group keys. Then it updates the key value in the communication with the vehicle using Bloom filters to verify the proposed method. In the proposed scheme in VANET, dispersed operations are carried out in the RSU. By reducing to a minimum the number of keys exchanged, more secure group communication can be realized. In this paper, we proposed a message batch verification scheme using Bloom Filter that can verify multiple messages and handover authentication efficiently even for multiple communications with many vehicles.

Keywords: *VANET, key exchange, handover authentication*

1. Introduction

VANET (Vehicular Ad-hoc Network) is a type of MANET (Mobile Ad-hoc Network), which is a next-generation networking technology that provides communication between vehicles or between a vehicle and an RSU (Road Side Unit) using wireless communication.

VANETs are usually divided into V2V (Vehicle-to-Vehicle) communication or V2I (Vehicle-to-Infrastructure) communication. V2V communication can be established by the vehicle forming its own network and can provide information without assistance from the infrastructure. It is generally used to provide safety services including emergency information as well as anti-collision messages and alerts. Various requirements for security should be satisfied because V2V communication depends on information broadcast by internal network participants, and erroneous information could cause a fatal accident. Various studies on security technology using a group signature scheme, which could provide functions such as authentication, conditional privacy, and non-repudiation, have been undertaken.

In order to provide authentication and privacy for VANET using a group signature, Zhang *et al.*, proposed a process for issuing secret disposable group keys for a vehicle by a group administrator[1]. Hao studied group signatures and proposed a secure group secret key distribution protocol [2]. Sun *et al.*, studied a DKM (Distributed Key Management) system and proposed a regional protocol group administrator to update the secret key of the group[3]. There are a number of existing proposals such as for methods of authenticated and conditional

* Corresponding author: Im-Yeong Lee, imylee@sch.ac.kr

ISSN: 1738-9976 IJSIA

privacy features. However, a conventional group signature scheme is unsuitable for the VANET environment because it does not provide efficient group configuration. Further, to configure a group for inter-vehicle communication, a group manager for authentication will not work due to the key escrow problem.

In the present study, the first communication passed from the RSU is only group keys. Then it updates the key value in the communication from the vehicle itself using Bloom filters to verify the proposed method. In the proposed scheme, VANET-dispersed operations are carried out by the RSU. Reducing the number of key exchanges to a minimum provides the advantage of more secure group communication. In this paper, we proposed a message batch verification scheme using Bloom Filter that can verify multiple messages efficiently even for multiple communications with many vehicles.

This paper is organized as follows. Section 2 introduces relevant information needed to understand the methods suggested in this study. Section 3 investigates basic security requirements for VANET. Section 4 proposes suggestions. Section 5 analyzes the efficiency of these suggestions. Section 6 gives conclusions and outlines future research directions.

2. Related Studies

2.1. Bloom Filter

The Bloom filter can search data quickly and space-efficiently in a data structure that has the statistical characteristics suggested by Bloom[4]. Such a Bloom filter can store a large amount of data in a very small space and is capable of efficient utilization by applying it to various environments according to the mode of retrieval.

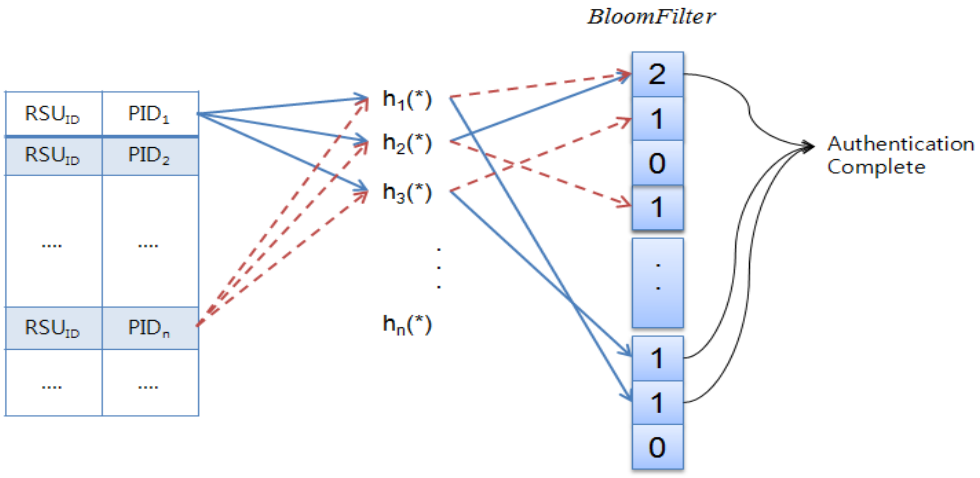

Figure 1. Example of Counting Bloom Filter

A Bloom filter is a bit array B that has m bits and can check quickly and easily if an element is included in a finite set $S = \{x_1, x_2,...x_n\}$ that has n elements. In order to implement mapping of each element to the Bloom filter, it maps the bit address space of the bit array B using k independent hash functions.

2.2. Counting Bloom Filter

A general Bloom filter can insert each element but cannot delete any. To delete a particular element, the bit values of locations defined by the hash function are reset from "1" to "0". Concurrently, the bit values of other elements that are not to be deleted may also be reset to "0". Hence, although these exist in Bloom filter, a false negative that implies do not exist can occur. In order to solve this problem, the suggested Bloom filter indicates how many items are input to corresponding locations by changing bits of the bit vector to count. Since only a counter is added to the existing Boom filter to obtain a counting Bloom filter, the probability of a false positive occurring is the same[5]. A counting Bloom filter that uses 3 or 4 bit for the counter is known to be safe[6] Figure 1.

2.3. Batch Verification Scheme

Batch verification scheme is a method that many messages signed can be verified at a single signature and verification cost. The concept was first introduced by Fiat in 1997 [7]. Currently many studies have been conducting to apply existing batch verification schemes to VANET.

Zhang and his fellows employed a batch verification technique to verify multi-signed messages in VANET efficiently [8]. Their scheme is to make RSU process batch verification on behalf of a vehicle. It turned out efficient in the situation dense with cars (per RSU). However, it is inefficient in that there aren't many vehicles per RSU. Furthermore it has a disadvantage of high overhead in processing ID-based signature verification.

RAISE is another batch verification scheme developed to tackle the overhead problem that is expected to bring out in car-concentrated areas [9]. In the system, RSU aggregates messages sent from vehicles in hash and transmit it to receiving vehicles. The receiving vehicles only checks if the received messages are included in the data sent from RSU. It makes authentication more efficient than existing verification schemes using operation by node. However, it should run unnecessarily frequent comparative processing, even more than the number of vehicles, so that it is unavoidable for it to compare as many times as the number of cars (n number of cars = n times of comparison).

3. Security Requirements

This chapter analyzed weaknesses of security in the vehicle communication environment and check security requirements to provide various services in the VANET environment.

3.1. Security Problems in VANET

VANET provided users with convenience by exchanging various information through communication among a car, a driver, and the external network. Direct efforts could be exerted on the safety and life of users in a case of emergency telegraph message such as the surrounding road conditions or car accidents differently from general multi-media information. The VANET sending and receiving message directly related to the life was a very important security issue. Car accidents might occur or the whole network became paralyzed to cause chaos if an attack with a malicious purpose inside or outside the network tapped and falsified information sent and received between vehicles to disturb. There was a intense need of studies suitable for the VANET environment because it had various characteristics such as the changeability of the node speed and the prediction of movement route.

There had been many studies on security techniques using a group signature scheme which could provide various security requirements such as authentication, conditional privacy, and non-repudiation in the VANET. The electronic signature base on PKI had been used in most of the studies because the inefficient aspect was shown according to the termination and renewal of a certificate in a case of the existing electronic signature base on PKI. However, there was also a need of the corresponding solution because the key escrow problem, a problem in the cipher system based on the exsiting ID, was applied as it was in the VANET environment.

Security threats related to message and system in the VANET were as follows.

Jamming (like DoS Attack): An attack that generates a signal which causes an obstacle in the communication of another vehicles within a certain network area

Forgery : A threat that another vehicles within a certain network area are contaminated with false information by an attack vehicle which generated false information.

In-transit Traffic Tampering: An attack that forges and falsifies information through drop, corruption, or modification in the transfer process of message or information while driving

Impersonation: An attack that makes other vehicles misperceive by changing vehicle condition information.

Privacy Violation: The invasion into personal privacy information related to a vehicle such as time, location, vehicle ID, and mobile information.

On-board Tampering: An attack that forges and falsifies inside information of a car.

3.2. Security Requirements

This section defined security requirements for the V2V authentication system that privacy was guaranteed. Users were exposed to many dangers such as DoS attack, communication disturbance, replay attack, forged attack, ID exposure attack, and vehicle chase because all of V2V communications sent and received data through wireless communication. The following security requirements should be satisfied to prevent such kinds of threats.

Authentication: A receiver should verify that a transmitted message was generated by a right user. A right user meaned a user who owned a right key which was not terminated to register in a trusted party of a system for the anonymous application differently from the authentication system based on a traditional public key. In other words, the concept of an authentication did not include the identification.

Anonymity: It meaned that any identity information about the sender should not be known from these messages even if an attack captured V2V messages. In other words, it meaned that the identity of a sender should not be known from transmitted messages and tt should not be identified whether two random messages were generated by the same sender.

Non-repudiation: A group member should not deny the message signed by an individual.

Traceability: A character that enabled to trace a special vehicle through the intervention of the third party to prepare the time that damage was occur when an accident occurred or due to the appearance of an attack. At this moment, the third party could cause a problem of privacy invasion if it was not a trusted party.

Unlinkability: it should not be know whether those were signed by members of the same group even if many different messages and signatures were given.

Conditional Privacy: The third party should not know the source of messages which exerted direct effects on the security of a vehicle driver. Group signed messages should be open by a group manager so that the identity should be identified when the dispute was occurred in addition to the privacy provision technique

4. Proposed Scheme

4.1. System Model

All the vehicles in the suggested system are pre-registered with a TA (Trusted Authority) before they are assigned to a network. It is assumed that all the vehicles perform all calculations for communication using an OBU (On-Board Unit) comprising TRH (Tamper-Resistant Hardware) installed in a vehicle, and all vehicles, and the TA synchronize time through an OBU. In order to form a group within communication range, the RSU forms a communication group by sending a message to vehicles within its communication range. It is presumed that an RSU is always a reliable object and has the superior arithmetic capacity than an OBU(Figure 2).

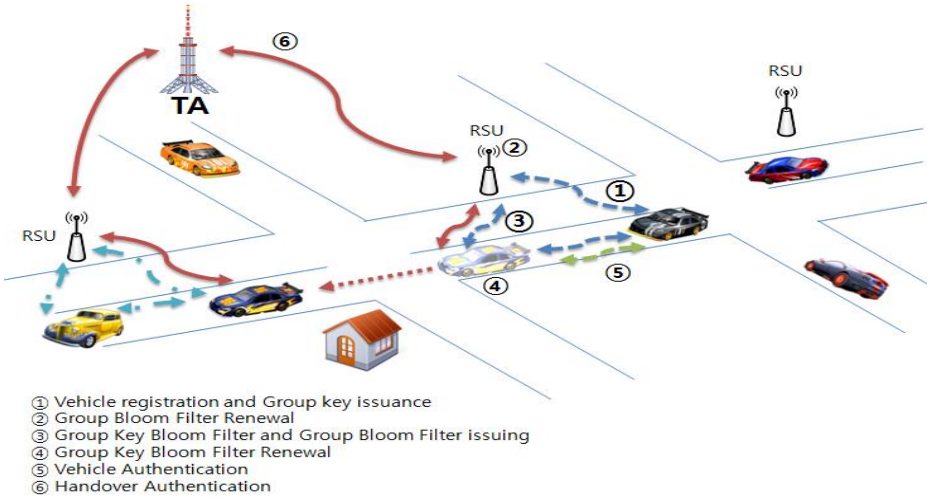

Figure 2. System Model

4.2. System Parameters

The protocol was developed using the system coefficients below in the suggested method.

- RID*: Vehicle identifier generated by OBU
- ID*: Vehicle identifier generated by OBU
- RSUID*: RSU identifier generated by OBU
- RN: Random number
- p, q: Prime numbers
- T_{exp}: Valid time of a vehicle public key
- s: Group secret key

- Y_{GA}: Group signature key
- d*: Private key of vehicle *
- Z_{q*}: Multiplication group of module q
- H(): One-way hash function
- PID*: Vehicle ID pair (ID*1, ID*2)
- P: Point on an elliptical curve
- G: P-generated cyclic group
- P_{pub1}, P_{pub2}: Public key pair generated by master keys (s_1 and s_2) of a TA
- (G, P, P_{pub1}, P_{pub2}): Public parameters
- GK*: Vehicle initial value of group key
- GKBF: Group key Bloom filter value
- GBF: Bloom filter value of vehicle PID information in communication group
- y: Initial value of group key renewal
- i: Transport value of group key renewal
- TS: Time stamp
- T_{REVOK}: Group key expiration time

4.3. Vehicle Registration Phase

Step 1: The vehicle generates a pair **of PIDs (ID_1,ID_2)** using the shared public parameters G, P, P_{pub1}, P_{pub2} through the **TA.** P_{pub1} and P_{pub2} are the pair of public keys generated by the master key (s_1,s_2) that the TA possesses.
- $ID_1 = r \cdot P$
- $ID_2 = RID \cdot H\ (r \cdot P_{pub1})$
- $PID = (ID_1, ID_2)$

The RSU forms a communication group by sending a group participation message to all of the vehicles that accessed the communication in the formation of the first group. It will form a GBF (Group Bloom Filter) using messages that are retransmitted from the vehicle. In this case, using the counting Bloom filter, duplicate elements increase the bit using the counter.

Step 2: The RSU encodes its identifier using the public key of the vehicle and transmits the resultant certificate to the vehicles that are within communication range.
- $RSU \rightarrow V: E_{KUV}(GK_V||y||TS||T_{REVOK}||CERT_{RSU})$

Step 3: A vehicle checks the identifier of the RSU and encodes this with the public key of the RSU and its own temporary ID that was generated in advance. The vehicle then sends a notification message that it belongs to the group and resends messages frequently.
- $V \rightarrow RSU: E_{KURSU}(RSU_{ID}||PID_V)$

Step 4: The RSU creates a GBF based on transmitted values. At this time, a counting Bloom filter is used for efficient updating and preparation for vehicle withdrawal.
- $H_1(RSU_{ID}||PID_V),H_2(RSU_{ID}||PID_V),..,H_i(RSU_{ID}||PID_V) = GBF$

4.4. Group Key Issue and Renewal Phase

4.4.1. Group Key Issue

The RSU broadcasts the Bloom filter value of the group key list to update this in each vehicle that belongs to that group. At this time, encoding is not required, because a new group key cannot be calculated without knowing the previous value of the group key now that the Bloom filter value of the group key to be newly updated is updated using the value of the initial group key.

RSU broadcasts the factor i, which is required for update, and the GBF, which is required for certificating the vehicle including the Bloom filter value of the group key ($GKBF_n$) to be newly updated.

-RSU → * : ($GKBF_n||i||Ts||T_{REVOK}$)

4.4.2. Group Key Renewal

The vehicle can verify whether it has been updated correctly, using the Bloom Filter value of the group key after updating its group key using the factor received from the RSU. The RSU does not update the group key of all vehicles, but the vehicle does so directly, and it is possible to verify if it is a real group key with a simple process. The arithmetic operation for updating the group key that is produced by the RSU can be dispersed.

A new group key to be used next time is updated with the factor i received from the RSU.

- $h(GK_1||y_{n-i})$ = ?$GKBF_n$

4.4.3. Group Bloom Filter Update

When no PID information is received from a vehicle, the RSU judges that it is out of communication range and updates the GBF. The updated GBF is broadcast to all vehicles within communication range of the RSU. Vehicles delete the previous GBF, and certification between vehicles is performed using the updated GBF.

4.5. Authentication Phase

4.5.1. Authentication between Vehicle

All messages are received and transmitted after encoding using the group key that is newly updated for each communication between vehicles. Each vehicle receives and transmits its own PID with the newly updated message to all vehicles with communication range.

- $V_1 \rightarrow V_2 : E_{GKBFn}(M)||PID_{v1}$

4.5.2. Communication Phase between a Vehicle and an RSU

An RSU receives and rebroadcasts the messages sent by the vehicles in the same group. The messages received by the RSU are verified using the group signature keys and checked to see if they are messages sent from eligible members Figure 3. Using the received messages, the RSU creates a Bloom filter and rebroadcasts them [10].

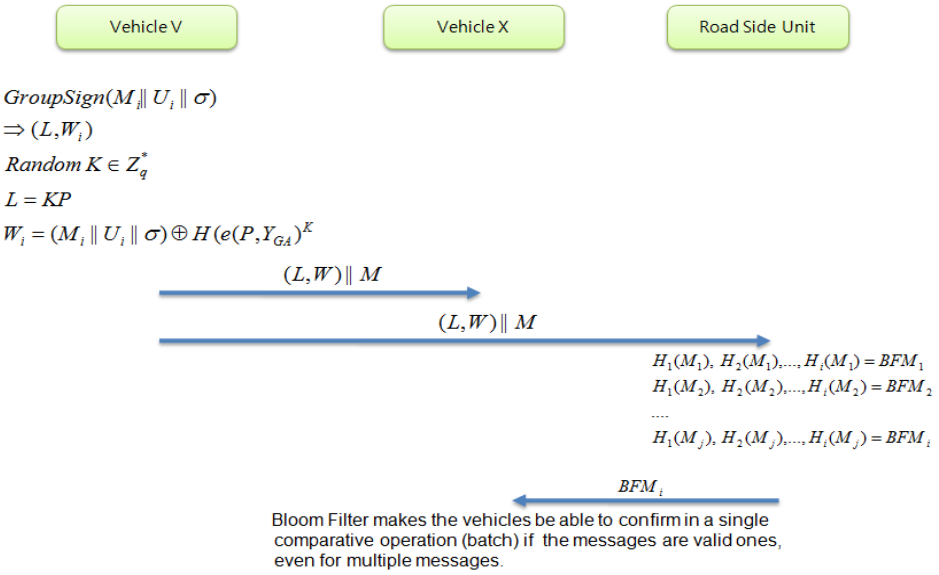

Figure 3. Communication Phase between a Vehicle and RSU

Step 1: Vehicle v signs the message using its own private signature key.
- $U = (M||ID_v) \oplus H(e(d_v, Y_{GA})$
- $\sigma = rP$
- UserSign $M = (U,\sigma)$

Step 2: The signature value is broadcast after the group signature process has been completed using a group signature key, so the personally signed message could be verified between the same group members.
- Random $K \in Zq^*$
- $L = KP$
- $W = (M||U||\sigma) \oplus H(e(P,Y_{GA})K$
- GroupSign $(M||U||\sigma) = (L,W)$

Step 3: Group members who receive broadcast messages verify the messages via a group signature key to ensure that it was transmitted by a rightful group member.
- GroupSign Verify(L,W)
  - $W \oplus H(e(Y_{GA},L) = (M||U||\sigma)_i$

Step 4: The RSU operates (processes) the received messages by a hash function algorithm and uses a Bloom filter to create BF_M.
- $H_1(M_1), H_2(M_1),...,H_i(M_1) = BF_{M1}$
  $H_1(M_2), H_2(M_2),...,H_i(M_2) = BF_{M2}$
  ...,
  $H_1(M_i), H_2(M_i),...,H_i(M_i) = BF_{Mi}$

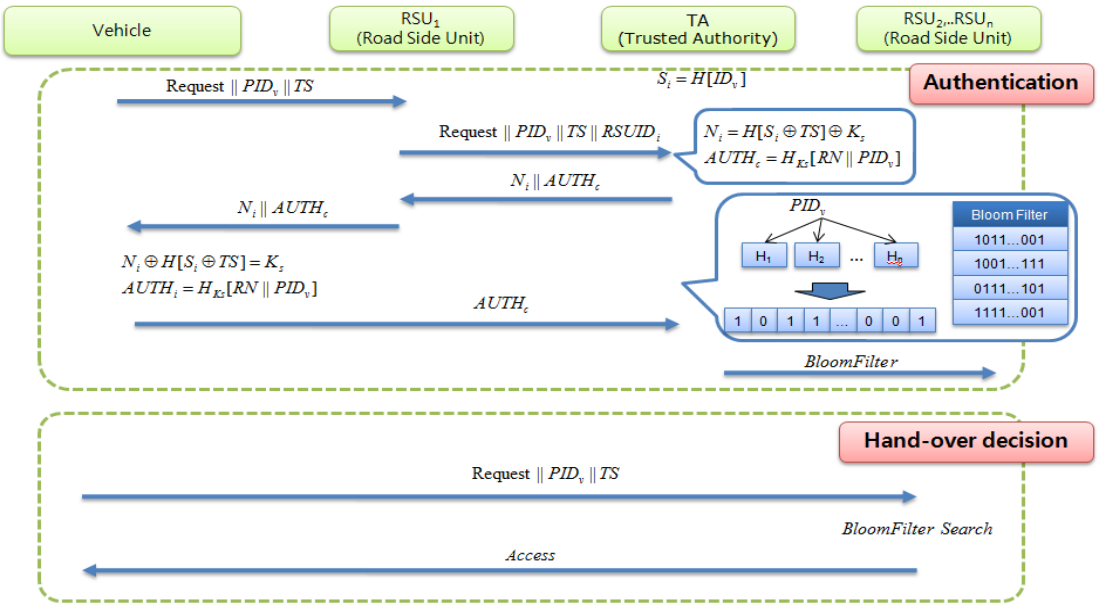

Figure 4. Handover Authentication

4.5.3. Handover Authentication

When moving between groups, the vehicle is typically subjected to a complex authentication every time. However, in the proposed method, a single authentication is required. After that, authentication is completed with just a simple search. Then, it is possible to minimize the operations of the RSU Figure 4.

Step 1: Vehicles deployed on a network share before the Si with the TA. The Si is calculated as a hash function value of the Vehicle ID.
- $S_i = H[ID_v]$

Step 2: When it comes into communication range of the RSU, the vehicle sends an authentication request message. Messages from the vehicle and their identifiers are received by the RSU, added together, and then send to the TA.

- Vehicle→RSU : Request||PID_v||TS
- RSU→TA : Request||PID_v||TS||$RSUID_i$

Step 3: The TA calculates the Ni. Then, it calculates the AUTH using the session key and sends it to the RSU.

- TA : $N_i = H[S_i \oplus TS] \oplus K_s$
  $AUTH_c = H_{KS}[RN||ID_v]$
- TA→RSU : N_i||$AUTH_c$
- RSU→Vehicle : N_i||$AUTH_c$

Step 4: The vehicle calculates Ks and AUTH, AUTH is sent to the TA for validation, and authentication is completed.

- Vehicle : $N_i \oplus H[S_i \oplus TS] = K_s$
  $AUTH_c = H_{KS}[RN||ID_v]$
- Vehicle→TA : $AUTH_c$.

Step 5: TA creates an authentication table using the Bloom filter and the PID of the vehicle. The TA transfers the authentication table to the RSU. When vehicle enters communication range of the RSU, authentication is completed by a simply search without another authentication operation.

5. Analysis of security and efficiency

5.1. Efficiency Analysis

5.1.1. Number of Group Keys Issued

In order to maintain vehicle speeds of 160 Km/h on a highway in a VANET environment, it takes about 44 seconds to pass 2 km of wireless access in vehicular environments (WAVE) communication data. Assuming that it is applied to a real environment, the number of transmitting group keys that can be issued from an RSU in 60 s was compared considering various environmental factors.

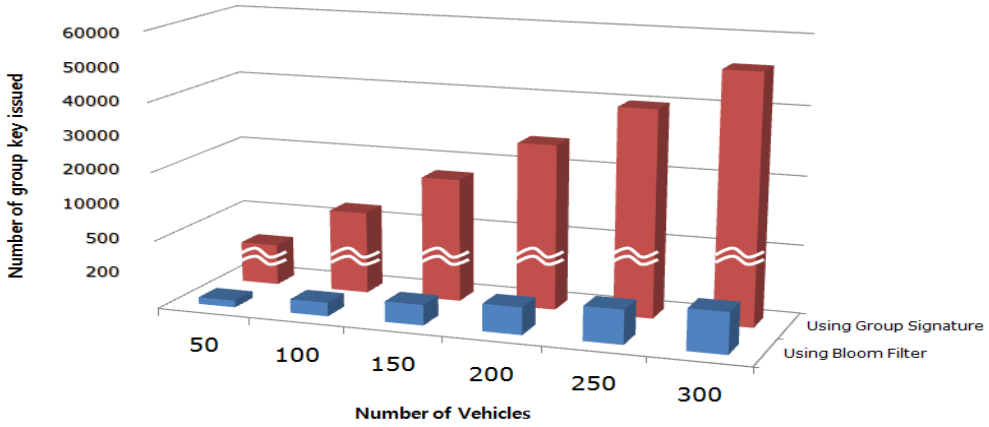

Figure 5. Number of Group Keys Issued

It was assumed that there are 50–300 vehicles within the communication range of an RSU. In general, the RSU transmits every 300 ms, and it receives the group key to be newly updated. However, this proposed system needs only one transmission with the group key updating list that comprises the first group key and a Bloom filter for each vehicle. Therefore, the process of transmitting group keys by the RSU can be reduced. However, when a vehicle moves out of communication range, the previous list of group key holders is deleted when communication with another RSU is accomplished through a message that includes the disposal time of the group key Figure 5.

5.1.2. Arithmetic Efficiency of Updating Group Key

This proposed system is the one that is capable of update and verification in the vehicle by transmitting Bloom Filter generated from taking the list of group key to be newly updated as

the value of hash. So, RSU has the merit that can disperse the concentrated arithmetic operation comparing with the existing system that RSU broadcasts the group key after updating and encoding it each time.

In this clause, the computational amount generated from the RSU and vehicle each are compared with the existing system. The coefficients used in the formula required for the comparison are as follows.

N_v: Number of vehicle
T: Number of group key renewal
E_T: Time required for encryption
D_T: Time required for decryption

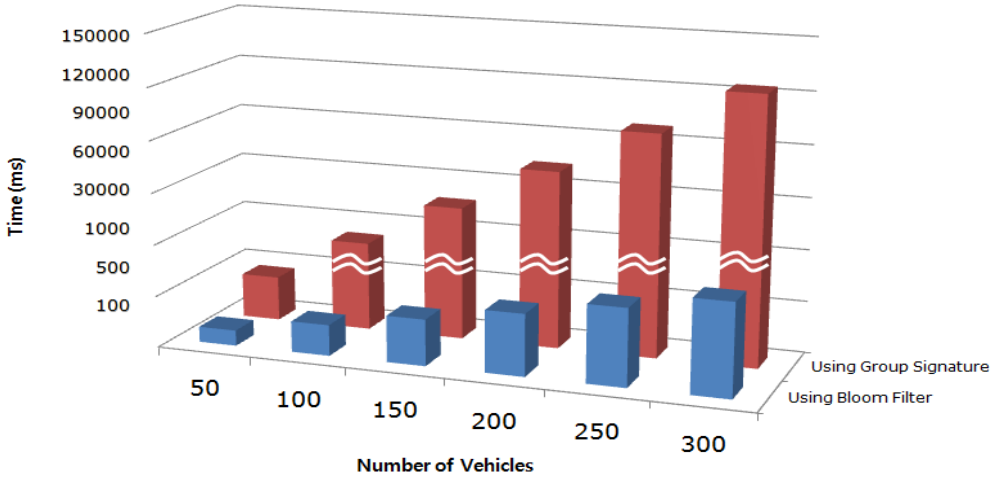

Figure 6. Comparison of Time Required for Group Key Renewal

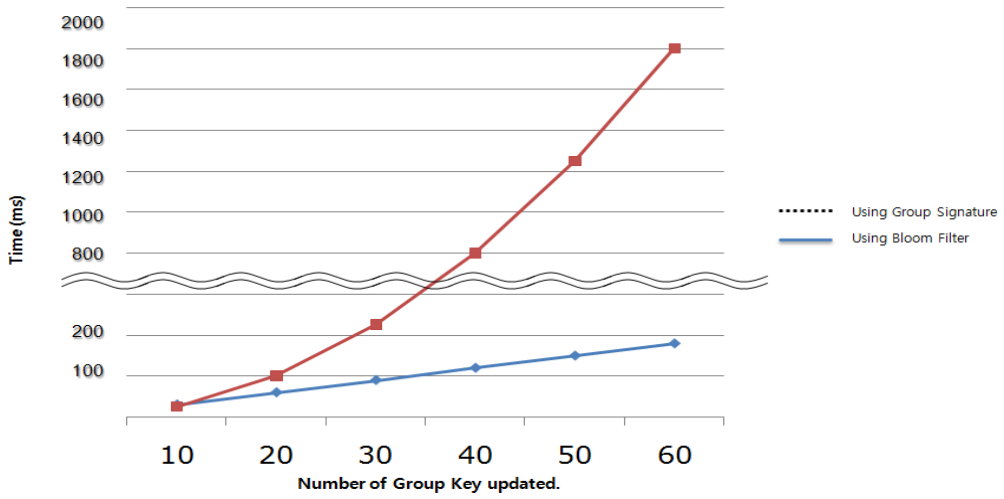

Figure 7. Comparison of Time Required for each Number of Group Rekeying of Vehicle

H_T: Time to generate Bloom Filter by taking hash

T_{VERIFY}: Time to verify the updated group key

RSU_{GS}: time required for arithmetic operations of RSU to which group signature was applied

RSU_{Bloom}: Time required for arithmetic operation of RSU that is applied by Bloom Filter

V_{GS}: time required for arithmetic operations of vehicle to which group signature was applied

V_{Bloom}: Time required for arithmetic operation of vehicle that is applied by Bloom Filter

RSU_{GS} and RSU_{Bloom} can be described with (1) and (2) each below.

$$RSU_{GS} = N_v \times T \times E_T \quad (1)$$

$$RSU_{Bloom} = N_v \times H_T \quad (2)$$

It was presumed that the communication for group rekeying was executed every second and the separate time value was not included because RSU_{Bloom} was accomplished with one time of communication only. Now that RSU_{NONE} is proportional to the number of vehicles, time required to update group rekeying increases rapidly as number of the vehicles increases. On the other hand, RSU_{Bloom} increases in proportion to number of vehicles, but it is capable of getting higher efficiency than RSU_{NONE} because each vehicle communicates just once at first Figure 6.

V_{GS} and V_{Bloom} is can be described with (3) and (4) each below.

$$V_{GS} = T \times D_T \quad (3)$$

$$V_{Bloom} = T(H_T + T_{VERIFY}) \quad (4)$$

VNONE is the time that each vehicle takes to decode the coded group key received from RSU to update group key and V_{Bloom} is the time that takes to update group key to be used next time regarding group key which receives first. At this time, T_{VERIFY} is the process that verifies if group key is updated normally comparing with the Bloom Filter that received the group key updated in the vehicle itself from RSU and it has the complexity as much as O(n) when it is presumed that it follows linear search method Figure 7.

5.1.3. Number of Communications

Since the vehicle speed is targeted at 160 km/h in a VANET environment, it takes about 44 s to transmit 2 km of WAVE communication data. Assuming that this is applied to an actual situation, the numbers of certification message communications between vehicles during 60 s were compared with respect to various environmental factors.

Based on the assumption that 50–300 vehicles are present within the communication range of an RSU, and one vehicle goes out of communication range each second, certification messages are transmitted every 300 ms until departing vehicles are out of communication range. However, the suggested method does not need separate certification message exchanges until the departing vehicle is out of communication range. This method is more efficient because certification with other vehicles is performed using a newly updated Bloom filter only when the vehicle moves out of communication range (Figure 8).

Table 1. Comparison of the Security Functions of Vehicles with Group Signature Scheme

		[11]	[12]	[13]	Proposed Scheme
Message Authentication		○	○	○	○
Conditional Privacy		○	△	×	○
User Tracing		○	○	×	○
Key escrow problem Solution		×	×	×	○
Batch Verification Scheme	Operation by Node	2P+10M	3P+M+3S	-	-
	Comparative Searching	-	-	In- Order Searching	Hashing Consequence Searching

(P: Paring, M: Multiplication, A: Addition)

5.1.4. Operational Efficiency

The proposed handover authentication scheme processing capabilities of the vehicle are considered. The vehicle uses only XOR and hash operations. The TA used the XOR and hash operation two times each. The same operation is done in the vehicle. With these operations, VANET authentication protocol implementation in the environment with a TA and vehicle real-time processing is possible.

5.1.5. Comparison of the Functions and Efficiency

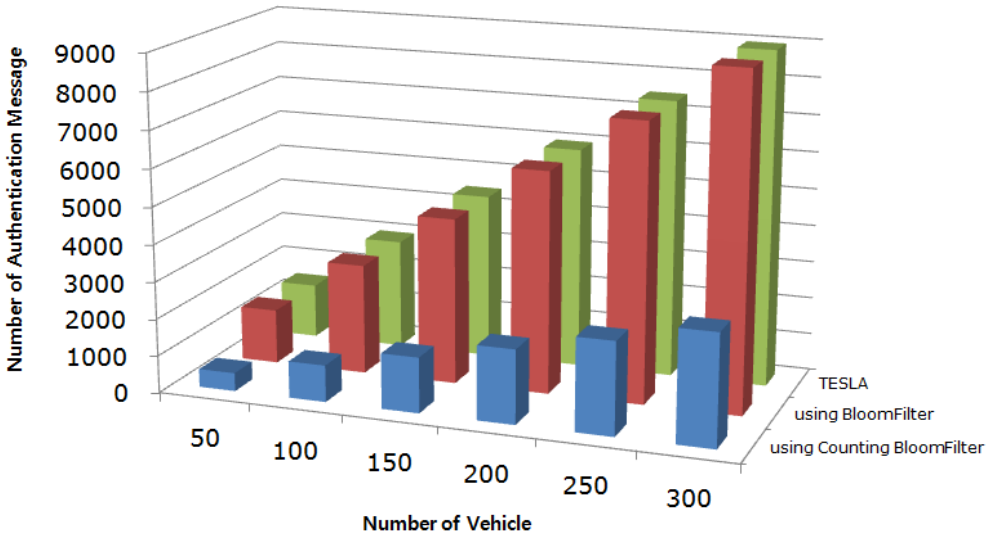

Figure 8. Number of Certification Messages Transferred

Table 1 summarizes a comparison of batch verification schemes applied to vehicle communication and proposed protocols. The scheme proposes a batch verification method by an RSU to reduce the overhead of operation by nodes. Because the RSU creates a Bloom filter in advance and transmits it, each node does not perform

unnecessary processes but only a simple comparison operation, which is sufficient to authenticate the messages.

5.2 Security analysis

5.2.1. Man-in-the-middle Attack

In this scenario, an assailant records a message transmitted between a group manager and group members and attempts to disguise his or her identity by calculating a signature key. However, only vehicle v can generate a private signature key without exposing its signature key to the channel to generate a signature key safely in the proposed technique. Therefore, an assailant could not generate a signature key with the message acquired through a man-in-the-middle attack. The information value exposed to the channel makes it impossible to calculate a private signature key composed of sδ-rδ with δe and sδ. AUTHi and $AUTH_C$ are calculated using the Si that is shared in advance in the handover process. The TA verifies the value of these two and performs a one-way authentication. In this case, the attacker does not know the values that are shared in advance. Therefore, it does not generate a valid AUTH value, so a man-in-the-middle attack is not possible.

5.2.2. Message Forgery Attack

The TA transmits to the vehicle Ni. At this time, Ni' is sent by an attacker, and the vehicle receives Ni'. The vehicle will fail to authenticate an invalid value (Ni' = H[Si $\oplus$ TS']). In addition, the attacker does not know the session key in AUTHi' Ni' $\oplus$ H[Si $\oplus$ TS] = H [Si $\oplus$ TS'] $\oplus$ Ks = Ks' (Nk). Therefore, this method is safe.

5.2.3. Privacy

The privacy of a signer is guaranteed, even if U was obtained via a group signature key, as U and σ were generated by rP so that the $(M||ID_v) \oplus H(e(d_v,Y_{GA})$ value, including a private key of a signer and the random value generated by a signer, are included.

6. Conclusion

In the present paper, a verification method that updates a group key in the vehicle using a Bloom filter is proposed to reduce the overhead of group rekeying by an RSU in the VANET environment where numerous vehicles are present. The number of communications and required time was optimized.

It is judged that more detailed comparative analysis of various existing methods is required by a simulation that considers various environmental factors based on the method proposed in this paper.

References

[1] J. Zhang, L. Ma, W. Su and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks", Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, **(2007)** November, pp. 138-142.

[2] Y. Hao, Y. Cheng and K. Ren, "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs", Proceedings of IEEE Global Telecommunications Conference, **(2008)** December, pp. 1-5.

[3] Y. Sun, Z. Feng, Q. Hu and J. Su, "An Efficient Distributed Key Management Scheme for Group-Signature Based Anonymous Authentication in VANET", Security and Communication Networksm, vol. 5, no. 1, **(2012)**, pp. 79-86.

[4] B. Bloom, "Space/Time Trade-Offs in Hash Coding with Allowable Errors", Comm. ACM, vol. 13, no. 7, **(1970)**, pp. 422-426.
[5] S.-W. Lee, D.-J. Park, T.-S. Chung, D.-H. Lee, S. Park and H.-J. Song, "A log buffer-based flash translation layer using fully-associative sector translation", ACM Trans. Embed. Comput. Syst., vol. 6, no. 3, **(2007)**, pp. 18.
[6] L. Fan, P. Cao, J. Almeida and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol", IEEE/ACM Trans. Netw., vol. 8, no. 3, **(2000)**, pp. 281-293.
[7] A. Fiat, "Batch RSA", Journal of Cryptogly, vol. 10, no. 2, **(1997)** March, pp. 75-85.
[8] C. Zhang, R. Lu, X. Lin, P. Ho and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks", Proc. of the IEEE INFOCOM 2008, **(2008)** April, pp. 246-350.
[9] C. Zhang, X. Ling and P-H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks", Proc. IEEE ICC 2008, Beijing, China, **(2008)** May, pp. 1451-1457.
[10] S.-H. Kim and I-Y. Lee, "A Study on Message Batch verification scheme using Bloom Filter in VANET", Computer Science and Convergence, vol. 114, **(2012)**, pp. 821-829.
[11] A. Wasef and X. Shen, "Efficient Group Signature Scheme Supporting Batch Verification for Securing Vehicular Networks", Proc of IEEE ICC, **(2010)**.
[12] C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen, "An Efficient Identity based Batch Verification Scheme for Vehicular Sensor Networks", Proc. of IEEE INFOCOM 2008, USA, **(2008)**.
[13] C. Zhang, X. Lin, R. Lu and P. -H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks", Proc. IEEE ICC 2008, Beijing, China, **(2008)** May 19-23.

Authors

Su-Hyun Kim received the B.S. and M.S. degrees in Depart of Computer Software Engineering from Soonchunhyang University, Korea, in 2010 and 2012, respectively. He is now a Ph.D. candidate in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include Cloud computing security, Secret sharing, etc.

Im-Yeong Lee is corresponding author. He received the B.S. degrees in Department of Electronic Engineering from Hongik University, Korea, in 1981 and the M.S. and Ph.D. degrees in Department of Communication Engineering from Osaka University, Japan, in 1986 and 1989, respectively. From 1989 to 1994, he had been a senior researcher at ETRI (Electronics and Telecommunications Research Institute), Korea. Now he is a professor in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include Cryptography, Information theory, Computer & Network security.