International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.241-248
http://dx.doi.org/10.14257/ijsia.2013.7.6.24

A Secure and Efficient Vehicle-to-Vehicle Communication based on Sensor Network

Su-Hyun Kim and Im-Yeong Lee

Soonchunhyang University
{kimsh, imylee}@sch.ac.kr

Abstract

The SMART Highway project combines road construction with advanced technology and vehicle telecommunication. A Vehicular Ad hoc Network (VANET) is the core technology of the SMART Highway, whose transport operation is based on road vehicle. The VANET is a next-generation networking technology that enables wireless communication between vehicles or between vehicles and a Road Side Unit (RSU). In the VANET system, a vehicle accident is likely to cause a serious disaster. Therefore, some information on safety is essential to serve as the key exchange protocol for communication between vehicles. However, the key exchange scheme of the general network proposed for a fast-moving communication environment is unsuitable for vehicles.

In this paper, the initial communication from the RSU is passed only with group keys. Then the key value in the communication is updated when the vehicle itself uses Bloom filters to verify the proposed method. In the proposed VANET scheme, the distributed operations are focused on the RSU and more secure group communication can be achieved by minimizing the number of key exchanges. Accordingly, communication between multiple vehicles more efficient and secure key exchange at the vehicle certification by signcryption and vehicle certification method that uses a counting bloom filter for more efficient certification is proposed.

Keywords: *VANET, signcryption, key exchange, BloomFilter*

1. Introduction

The SMART Highway project combines road construction with advanced technology and vehicle telecommunications. Its expected outcome is a world-leading intelligent road that is green, fast, and comfortable. The core objective of the SMART Highway is "securing safety" by means of "role reassignment" among the driver, vehicle and road, which are the three major traffic factors. This end will be achieved for a design speed of 160 km/h through an automatic system for prevention and detection of accidents. In other words, the SMART Highway aims to improve the functionalities of vehicles and roads by sharing, communicating and controlling information between driver, vehicle and road facilities through a combination of information road and automotive technologies. Other goals of the SMART Highway are to decrease the role and fatigue of the driver, raise the level of convenience, increase the safety of high-speed driving, and expand the road capacity. A Vehicular Ad hoc Network (VANET) is the core technology of the SMART Highway, whose transport operation is based on road vehicles. The VANET is a next-generation networking technology that enables wireless communication between vehicles or between vehicles and a Road Side Unit (RSU).

ISSN: 1738-9976 IJSIA

The VANET concept is usually divided into Vehicle-to-Vehicle(V2V) communication and Vehicle-to-Infrastructure(V2I) communication. V2V communication can be carried out by forming a vehicle own network without assistance from an information infrastructure. This is generally used to provide safety services that include emergency information as well as anti-collision and alert messages. However, the key exchange scheme based on the general network proposed for a fast-moving communications environment is unsuitable for vehicles.

In this paper, the initial communication from the RSU is passed only with group keys. Then, the key value in the communication is updated in the proposed method when the vehicle itself uses Bloom filters to verify. Moreover, in order to have smooth certification between fast-moving vehicles, the previous certification method used in existing networks cannot itself be applied. Accordingly, communication between multiple vehicles more efficient and secure key exchange at the vehicle certification by signcryption and vehicle certification method that uses a Counting Bloom filter for more efficient certification is proposed. The remainder of this paper is organized as follows. Section 2 introduces relevant techniques that are needed to understand the techniques suggested in this study. Section 3 investigates the basic security requirements for a VANET. Section 4 proposes a scheme. Section 5 analyzes the efficiency of the proposed scheme. Section 6 draws the conclusions and outlines the future research directions.

2. Related Studies

2.1. Bloom Filter

A Bloom filter searches for data fast and space-efficiently because its data structure has the statistic characteristic suggested by H. Bloom [1]. It can save a large amount of data in a very small space and efficiently utilize such data by applying it to various environments according to the mode of its retrieval.

A Bloom filter is a one-bit vector B that has m(ea) bits and enables easy checking if each element is included in the finite S = {x_1, x_2, ..., and x_n} that has n(ea) elements. To map each element to the Bloom Filter, the bit address space of bit vector B must be mapped using the k(ea) of the hash function, which is independent each other.

2.3. Signcryption

Zheng was Signcryption method proposed in 1997 that the encryption and signing feature are mixed [2]. Signcryption is run concurrently in a single logical step sign and encrypt based on multiplication group. It is an effective encryption technique that significantly reduces the computation time. In 1998, proposed a method which is based on elliptic curve and summed group [3].

2.4. VANET(Vehicle ad-hoc Network)

Confidentiality and authentication in order to meet the security requirements of the VANET, various groups signature technology that provides the functionality of the privacy conditions have been proposed.

In order to provide authentication and privacy conditional VANET, using a group signature, Zhang et al proposed a process of disposal group secret key of a vehicle by a group administrator [4]. Hao was applied to group signatures. Proposed a secure group secret key distribution protocol [5]. Sun *et al.*, was applied (DKM) distributed key management system. Proposed a protocol group administrator of the region to update the secret key of the group [6]. Existing proposals such as the way they are authenticated and conditional privacy

features. However, conventional group signature scheme is unsuitable to the VANET environment. It does not provide efficient group configuration on. Also configure a group of inter-vehicle, Group manager for authentication did not work, the key escrow problem will occur.

4. Proposed Scheme

4.1 System Models

All of the vehicles in the suggested system are pre-registered with a Trusted Authority (TA) before they are distributed on a network. It is assumed that all vehicles perform all calculations for communication using the Tamper-Resistant Hardware (TRH) of the On-Board Unit (OBU) loaded into the vehicle and that all of the vehicles and TAs synchronized times through the OBU. To produce the group within the communication range, the RSU generates one communication group by sending a message to the vehicles that access the communication. It is presumed that the RSU is always reliable and that its arithmetic capacity is superior to that of the OBU.

4.2 System Parameters

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

-RID*:vehicle’ s identifier generated by OBU

-PID*:vehicle’ s ID pair (ID*1,ID*2)

-P: point on elliptical curve

-G: P-generated cyclic group

-Ppub1,Ppub2:public key pair generated by master keys (s1ands2) of TA

-(G, P, Ppub1,Ppub2):public parameters

-GK*: vehicle’ s 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. Initial Setting

The vehicle generates a pair of PIDs (ID_{V1} and ID_{V2}) by using the shared public parameters G, P, P_{pub1} and P_{pub2} through the Trusted Authority(TA), where. P_{pub1} and P_{pub2} comprise the pair of public keys generated by the master keys (s_1 and s_2) of the TA.

- $ID_{V1} = r \cdot P$

- $ID_{V2} = RID \cdot H (r \cdot P_{pub1})$

- $PID_V = (ID_{V1}, ID_{V2})$

4.4. Vehicle Registration

The RSU generates one communication group by sending the group participation message to all of the vehicles that access the communication in the generation of the first group. It will generate a (Group BloomFilter) GBF using messages that are retransmitted from the car. In this case, use the Counting BloomFilter. Duplicate elements increases the Bit using the Counter.

Step 1: The RSU encodes its identifier using the public key of the vehicle and transmits the resultant certificate to the vehicles that are within the communication range.

- RSU → V: $E_{KUV}(GK_V||y||TS||T_{REVOK}||CERT_{RSU})$

Step 2: A vehicle that checks the identifier of the RSU encodes this with the public key of the RSU and its own temporary ID that is generated in advance. The vehicle then sends a notification message that it belongs to the group that sends messages frequently.

- V → RSU: $E_{KURSU}(RSU_{ID}||PID_V)$

Step 3: The RSU creates Group Bloom Filter(GBF) based on transmitted values. At this time, a Counting Bloom filter is used for efficient updating preparation for vehicle withdrawal.

- $H_1(RSU_{ID}||PID_V),H_2(RSU_{ID}||PID_V),....,H_i(RSU_{ID}||PID_V)=GBF$

4.5. Group Key Issue

The RSU broadcasts the Bloom filter value of the group key list to update this in each vehicle that belongs to the same group. Vehicle can verify have been updated correctly by comparing the GroupKey BloomFilter Value of Vehicle and updated in BloomFilter Value of GroupKey received via the RSU Signcryption from the Vehicle. RSU is not updating the group key for all vehicles. It can be easily verified that the vehicle will be updated directly. It can be distributed group key update operations focused on RSU.

Step 1: After applying the method Signcryption information required to verify the first group key, RSU looks like forwards it to the car. In this case, the message is sent, and message encryption is done at the same time signature of RSU Signcryption.

Random x

$w = y_{RSU}^{x} \bmod p$

$k = H_1(w)$

$r = H_2(m, RSU_{ID}, w)$

$s = x/(r + x_v) \bmod q$

$c = E_k(m)$

$m = (GKBF \parallel i \parallel TS \parallel T_{REVOK})$

- RSU→V : (c,r,s)

Step 2: Vehicle receive messages from the RSU that are approved by signcryption and they verify the RSU and the encryption of messages by unsigncryption. The vehicle receives c, r, and s, distinguishes message w from m, and compares them with the received r value to verify that they are correct using unsigncryption.

$w = (yv \bullet g^{r})^{s \bullet x_{RSU}} \bmod p$

$k = H_1(w)$

$m = D_k(c)$

- V : $r ? = H_2(m, RSU_{ID}, w)$

4.6. Group Key Renewal

The vehicle can verify that it has been updated correctly by using the Bloom filter value of the group key after the group key is updated through the factor received from the RSU. Now that the RSU does not update the group key the vehicles do so directly and can validate the group key with a simple process, the arithmetic operations for updating the group key were focused on the RSU can be distributed.

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

- $h(GK_V||y+i) \stackrel{?}{=} GKBF$

4.7. 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 the same communication range same as the GBF issue. Vehicles remove the previous GBF and certification between vehicles is performed using the updated GBF.

4.8. Authentication between Vehicles

During communication between vehicles, all messages are sent and received by encoding with the group key. At this time, each vehicle determines whether the message is from the proper vehicle by receiving PIDs from other vehicles in addition to messages encoded with the group key and comparing with the GBF received from the RSU.

Each vehicle transmits and receives its own PID in newly updated messages to and from the vehicles within the communication range.

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

5. Efficiency Analysis

5.1. Number of Group Keys Issued

Since that the speed of the vehicles is intended to be maintained at 160 km/h in a SMART Highway environment, it takes about 44s to pass through 2km of the Wireless Access in Vehicle Environments(WAVE) communication range. The WAVE was applied to a real environment and, the numbers of transmitting group keys issued from the RSU in 60s were compared, while considering various environmental factors.

It was presumed that there were 50-300 vehicles within the communication range of the RSU. The communication is generally performed every 300ms and the group key to be newly updated is received. However, since the proposed system needs only a single communication per vehicle with the group key updating list that is composed of the first group key and the Bloom filter, the process of transmitting the group key can have a reduced focus on the RSU. If a vehicle leaves the communication range, the previous list of group keys is deleted when communication with another RSU is established through a message that includes the disposal time of the group key(Figure 1).

5.3. Number of Communications

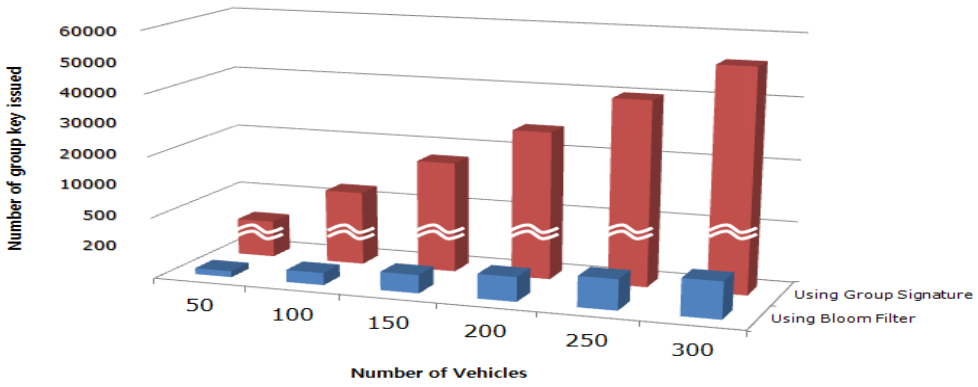

Figure 1. Number of Group Keys Issued

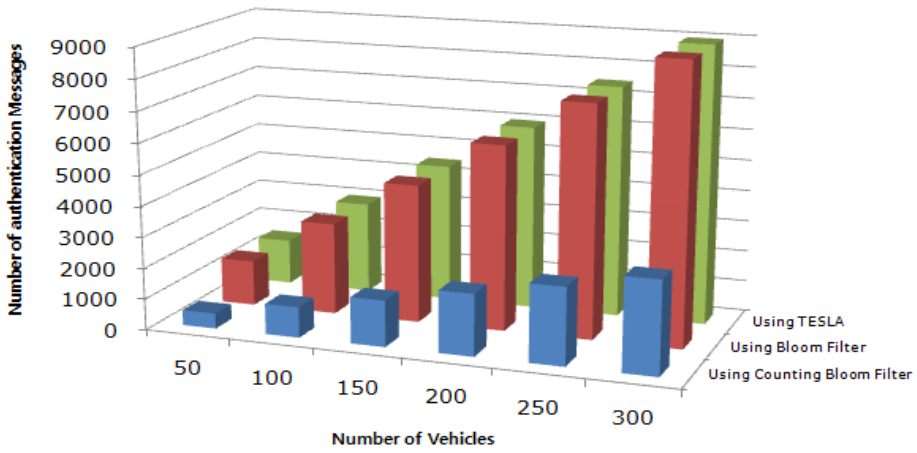

Figure 2. Number of Certification Messages Transferred

Since the vehicle speed is targeted at 160km/h in a SMART highway environment, it takes about 44s to pass through 2km of WAVE communication range. Assuming that this is applied

to an actual situation, the numbers of certification message communications between vehicles during 60s were compared with respect to various environmental factors.

Based on the assumption that 50~300 vehicles exist within the RSU communication range and one vehicle goes out of communication range each second, certification messages are transmitted every 300 ms until opposing vehicles are out of communication range. However, the suggested method does not need separate certification message exchanges until the opposing vehicle is going out of communication range. This method is more efficient because the certification with other vehicles is performed using a newly updated Bloom filter only when the vehicle is no longer within communication range (Figure. 2).

6. Conclusion

In this paper, a verification method that updates group keys in vehicles and uses a Bloom filter has been proposed to reduce the overhead of group rekeying focused on the RSU in a VANET environment with numerous vehicles. The number of communications and the temporal efficiency were maximized.

It is considered that a more detailed comparative analysis of the proposed method and various existing methods are required in the form a simulation that considers various environmental factors on the basis of the proposed method.

References

[1] B. Bloom, "Space/Time Trade-Offs in Hash Coding with Allowable Errors", Comm. ACM, vol. 13, no. 7, **(1970)**, pp. 422-426.

[2] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature and Encryption) << Cost(Signature) + Cost(Encryption)", Advances in Cryptology, Proceedings of CRYPTO'97, LNCS, Springer-Verlag, vol. 1294, **(1997)**, pp. 165- 179.

[3] Y. Zheng, "Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes", IEEE P1363a: Standard Specifications for Public-key Crypto graphy: Additional Techiques, **(1998)**.

[4] 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)**, pp. 138-142.

[5] 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)** pp. 1-5.

[6] 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.

Authors

Su-Hyun Kim

2012-present: Ph.D. Candidate, Computer Software, Soonchunhyang University.

February 2012: Master of Science, Computer science, Soonchunhyang University.

February 2010: Bachelor of Science, Computer science, Soonchunhyang University.

Im-Yeong Lee

1994-present: Professor, Computer Software, Soonchunhyang University.
1985-1994: Electronics and Telecommunications Research Institute, Senior Researcher
February 1989: Doctor of Communication Engineering, Osaka University.
February 1986: Master of Communication Engineering, Osaka University.
February 1981: Bachelor of Science, Electronics Engineering, Hongik University.