Secure Multicast using Proxy Re-Encryption in an IoT Environment

SuHyun Kim[*], YongWoon Hwang[**], JungTaek Seo[***]
IoT Security & Privacy Research Center, Soonchunhyang University, Korea[*]
Department of Computer Software Engineering, Soonchunhyang University, Korea[**]
Department of Computer Information Security, Soonchunhyang University, Korea[***]
e-mail : [kimsh[*],hyw0123[**], seojt[***]]@sch.ac.kr
Corresponding author: JungTaek Seo[***]

Received September 26, 2017; revised December 12, 2017; accepted January 7, 2018; published February 28, 2018

Abstract

Recently interest in Internet of Things(IoT) has attracted significant attention at national level. IoT can create new services as a technology to exchange data through connections among a huge number of objects around the user. Data communication between objects provides not only information collected in the surrounding environment but also various personalized information. IoT services which provide these various types of data are exposed to numerous security vulnerabilities. If data is maliciously collected and used by an attacker in an IoT environment that deals with various data, security threats are greater than those in existing network environments. Therefore, security of all data exchanged in the IoT environment is essential. However, lightweight terminal devices used in the IoT environment are not suitable for applying the existing encryption algorithm. In addition, IoT networks consisting of many sensors require group communication. Therefore, this paper proposes a secure multicast scheme using the proxy re-encryption method based on Vehicular ad-hoc networks(VANET) environment. The proposed method is suitable for a large-scale dynamic IoT network environment using unreliable servers.

Keywords: Internet of Things, Light-weight device, Proxy re-encryption

A preliminary version of this paper was presented at APIC-IST 2017, and was selected as an outstanding paper.
This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Promotion)
This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry and Energy (MOTIE) of the Republic of Korea (No. 20162220200010).

1. Introduction

Internet of Things(IoT) refers to a network that collects and processes information from all terminal devices connected to the network and provides new services. IoT can create new services as a technology to exchange data through connections among a huge number of objects around the user. Data communication between objects provides not only information collected in the surrounding environment but also various personalized information. IoT services which provide these various types of data are exposed to numerous security vulnerabilities. If data is maliciously collected and used by an attacker in an IoT environment that deals with various data, security threats are greater than those in existing network environments. Attacks such as spam messages sent through a refrigerator or a smart TV can cause inconvenience to users and more aggressive attacks can even threaten users' lives. Automotive and medical device hacking can even lead to life-threatening attacks on users. Personal information collected on the IoT platform can also cause an invasion of privacy problem. For example, analyzing the power consumption pattern of a smart meter can help to analyze users' life patterns. Data collected to provide personalized services can provide a more convenient service, yet users may be unwilling to expose their personal information to service providers. In order to prevent damage from these various personal information management and security threats, it is essential to secure the data transmitted in the IoT environment.

However, lightweight terminal devices used in the IoT environment are not suitable for applying the existing encryption algorithm. This is because the security solution that implements the existing encryption algorithm is difficult to use in small lightweight devices and the intrusion path is continuously diversified due to the complex network structure consisting of a huge number of nodes. Therefore, this paper proposes a secure multicast scheme using the proxy re-encryption method based on Vehicular ad-hoc networks(VANET) environment. The proposed method provides inter-vehicle authentication through group communication using a Bloom filter, and provides more efficient and secure encrypted data for encryption communication between authenticated vehicles using the proxy re-encryption method. The proposed method is suitable for a large-scale dynamic IoT network environment using unreliable servers.

2. Related Work

2.1 Security Vulnerbility of IoT(Internet of Things)

The Internet of Things(IoT) refers to a network to which all devices are connected and that enables the information of all these devices to be collected, processed, and modified to provide new services. There are many devices around us. Such as smart TV, watch, refrigerator. However, existing devices are not considered security.

Fig. 1 shows the IoT network in general. A number of IoT devices are connected to the gateway. Gateways are controlled and centralized by the cloud. IoT devices communicate with each other or send device information to the gateway. At this time, communication between devices frequently occurs. However, IoT is very vulnerable to security. As such, IoT has various security vulnerabilities. This vulnerability brings vulnerabilities to existing networks. In addition, a security threat to the IoT devices is added. Passive attacks, such as spam messages sent via refrigerators or Smart TVs, may result in damage to these devices, and more

aggressive attacks may threaten the user′s life by hacking vehicle communication systems and medical devices.

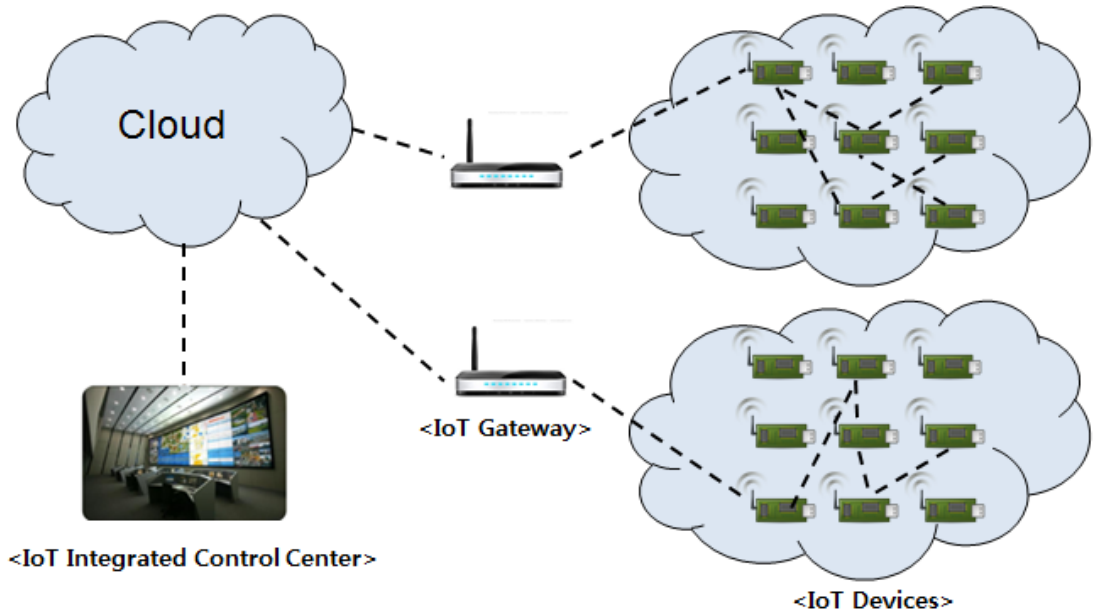

Fig. 1. IoT Networks

2.2 Bloom Filter

A Bloom filter searches for data rapidly and compactly because its data structure has the statistical characteristics suggested by Bloom[2]. It can save a large amount of data in a very small space and efficiently utilize that data through application in various environments according to the mode of retrieval.

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

2.3 VANET(Vehicle ad-hoc Network)

VANET (Vehicular Ad-hoc Network) is a type of MANET (Mobile Ad-hoc Network) that is the next-generation networking technology to provide communication between vehicles or between a vehicle and RSU (Road Side Unit) using wireless communication. This VANET is usually divided into V2V (Vehicle-to-Vehicle) communication or V2I (Vehicle to Infrastructure) communication. Following is table of comparing MANET and VANET(**Table 1**). MANET is proportional to human walking speed. But VANET is proportional to vehicle speed due to vehicle built terminal. Because of big difference in mobility, network topology change, node density, moving pattern are differentiated.

Table 1. Comparison between MANET and VANET

Category	MANET	VANET
Mobilty	Medium/Low speed (walking speed)	High speed (maximum 200 Km/h)
Network topology change	Slow	Fast
Node density	Low and slow change	High and fast change
Credibility level for message transmission and content	Medium (depend on application)	Very high (mostly safety related message)
Node location acquisition method	Triangulation using radio signal intensity and ultrasonic wave	GPS
Node moving pattern (speed and direction)	Moved to random location (random)	Have moving path specified by

To allow confidentiality and authentication (so as to meet the security requirements of the VANET), various groups signature technologies that provide the functionality of privacy conditions have been proposed.

To provide authentication and privacy conditions to VANET using a group signature, Zhang et al. proposed the use of a disposal group secret key for each vehicle, created by a group administrator[5]. Hao has applied this method to group signatures, along with a secure group secret key distribution protocol[6]. Sun et al. developed a distributed key management(DKM) system in which a protocol group administrator of the region updates the secret key of the group[7]. Existing proposals include authentication methods and conditional privacy features; however, conventional group signature schemes are unsuitable for use in the VANET environment. Conventional schemes do not provide efficient group configurations. Furthermore, when configuring a group with inter-vehicle communication, the use of a group manager for authentication was not successful, because the key escrow problem occurred.

2.3 Security Vulnerbility of VANET

VANET has various security threatening. The typical method is Bogus information(**Fig. 2**). Bogus information is corrupting other driver's behaviors as spreading fault information in the network. Next vulnerbility is on-board tampering(**Fig. 3**). The on-board tampering is a fake and falsification attack to various information inside vehicle. Other than previous two kinds of attack, there are Jamming, Forgery, In-transit Traffic Tampering, Impersonation, Privacy Violation(**Table 2**).

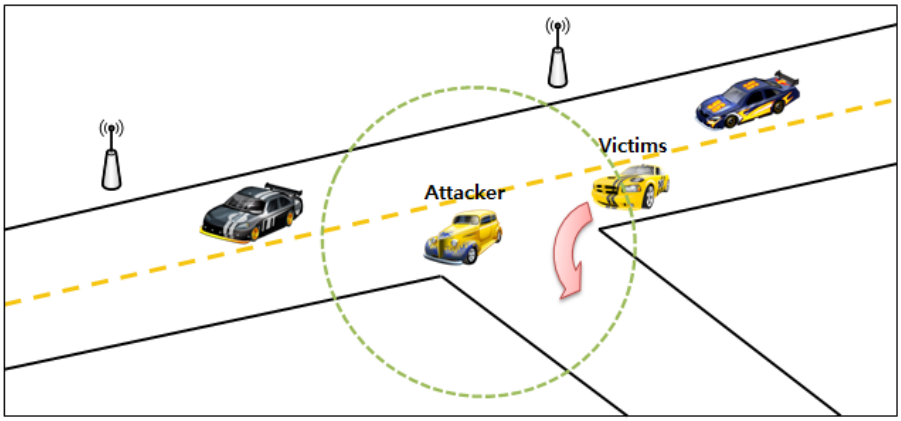

Fig. 2. Bogus information attack

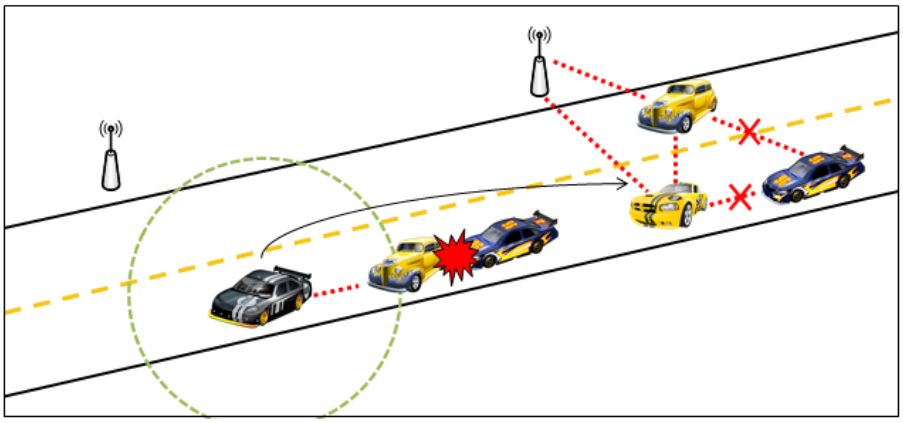

Fig. 3. On-board tampering attack

Table 2. Security Vulnerbility of VANET

Vulnerability	Details
Jamming (like DoS Attack)	Attacking by cause communication problems of other vehicles within certain networks.
Forgery	Threatening as contaminating other vehicles with fault information by target vehicle already contaminated.
In-transit Traffic Tampering	Information falsification attack with Drop, Corrupt, or Modify in transmitting message or information on driving.
Impersonation	Attack causing misconception by other vehicles by faking vehicle condition information. (Example: Transmitting own vehicle information as emergency vehicle, letting other vehicle slow down speed.
Privacy Violation	Violation personal private information related to vehicle such as time, location, vehicle ID, moving path, etc.

3. Proposed Method

3.1 System Models and Assumption

VANET is composed with following two kinds of OBU and RSU(**Fig. 4.**).

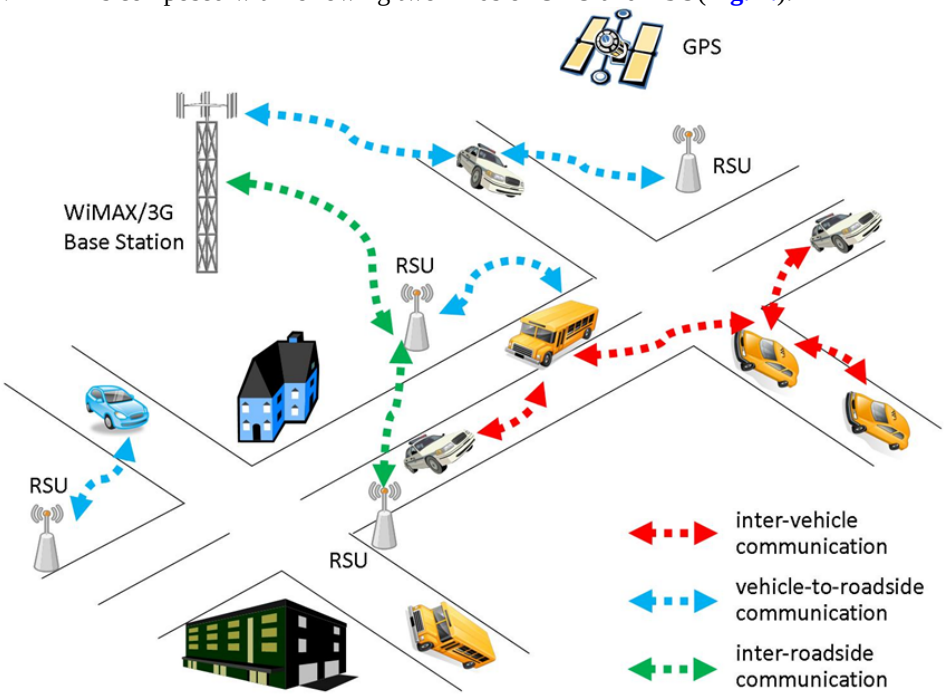

Fig. 4. Structure of VANET

OBU is communication equipment installed in the vehicle. Communication is made with vehicle or RSU through OBU. RSU is communication equipment located around road.

One vehicle is assumed to be one terminal device, and all terminal devices on the system are pre-registered from the Trusted Authority(TA) before being distributed to the network. All the devices are assumed to have performed all calculations on communication using tamper resistant hardware (TRH) loaded into all the devices and it is also assumed that the TA synchronizes time through the devices. The TA generates a group within the communication range by sending a message to all devices with access to the communication range. The TA is always presumed to be a reliable object with arithmetic capacity superior to that of the devices. The Road Side Unit(RSU) located around the road is assumed to be an untrusted object, and the encrypted data is exchanged via the RSU when the inter-vehicle encrypted data communication is performed(**Fig. 5.**).

Like this, this research assumes an IoT network environment in which encrypted data is exchanged through group authentication among dozens of sensor nodes (vehicles). In the network environment, each node shares information with other nodes in other locations to communicate with an RSU acting as a gateway. In this case, the number of encryption/decryption increases in proportion to the number of nodes if the existing public key encryption is used. For example, if there are 50 sensor nodes on the network, each node must perform 50 encryption/decryption operations. However, proxy re-encryption is performed using an RSU that is an untrusted object in the proposed method. Each vehicle encrypts its message using its public key when authentication is complete. The encrypted message is forwarded to the RSU, which computes the re-encryption and delivers it to each vehicle.

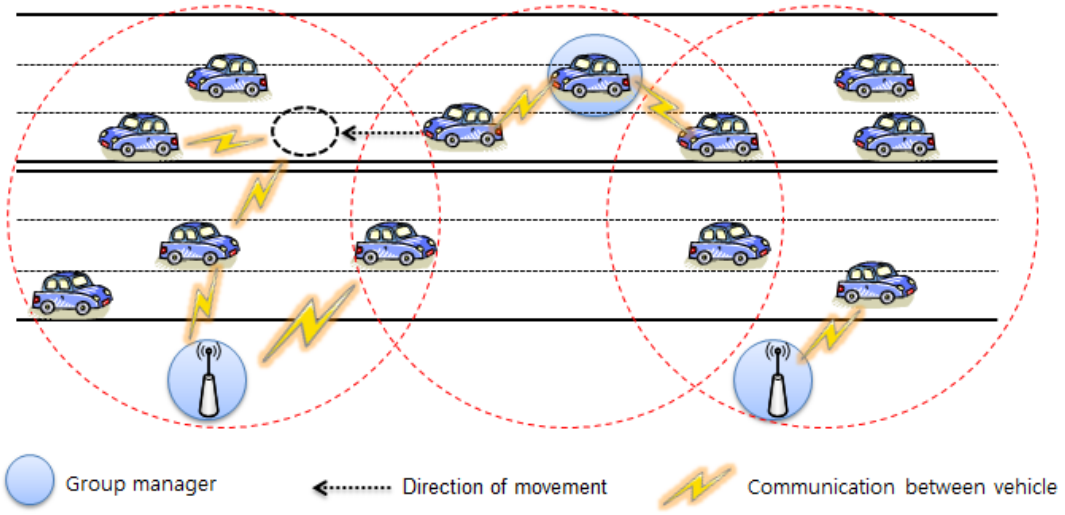

Fig. 5. Communication in VANET

3.2 System Parameters

The protocol was planned using the following system coefficients in the suggested method[8][9].

. RID*: vehicles identifier generated by OBU
. PID*: vehicles ID pair (ID_{*1}, ID_{*2})
. P: point on elliptical curve
. G: P-generated cyclic group
. P_{pub1}, P_{pub2}: public key pair generated by master keys (s_1 and s_2) of TA
. (G, P, P_{pub1}, P_{pub2}): public parameters
. GK*: vehicle initial value of group keys
. GKBF: group key Bloom filters value
. GBF: Bloom filter value of vehicles PID information in communication group
. y: initial value of group keys renewal
. i: transport value of group keys renewal
. TS: time stamp
. T_{REVOKE}: group key expiration time
. e : bilinear mapping, $G \times G -\rangle\ G_T$
. $sk*$: private key of *
. $pk*$: public key of *

3.3 Vehicle authentication phase

(1) Initial setting process

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.

$$\mathrm{ID}_{V1} = \mathrm{r} \cdot \mathrm{P}$$
$$\mathrm{ID}_{V2} = \mathrm{RID} \cdot \mathrm{H}\,(\mathrm{r} \cdot \mathrm{P}_{pub1})$$
$$\mathrm{PID}_{V} = (\mathrm{ID}_{V1}, \mathrm{ID}_{V2})$$

(2) Process of registering devices

The RSU generates one communication group by sending the group join message to all of the vehicles that access the communication in the generation of the first group.

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

$$\mathrm{RSU} \rightarrow \mathrm{V}: \mathrm{E}_{KU_V}(\mathrm{GK}_V \,||\, \mathrm{y} \,||\, \mathrm{TS} \,||\, \mathrm{T}_{\mathrm{REVOKE}} \,||\, \mathrm{CERT}_{RSU})$$

Step 2: A vehicle that checks the ID of the Road Side Unit encodes this with the public key of the Road Side Unit 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.

$$\mathrm{V} \rightarrow \mathrm{RSU}: \mathrm{E}_{KU_{RSU}}(\mathrm{RSU}_{ID}||\mathrm{PID}_V)$$

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

$$\mathrm{H}_1(\mathrm{RSU}_{ID}||\mathrm{PID}_V), \mathrm{H}_2(\mathrm{RSU}_{ID}||\mathrm{PID}_V), \ldots, \mathrm{H}_i(\mathrm{RSU}_{ID}||\mathrm{PID}_V) = \mathrm{GBF}$$

(3) Issuing stage

The RSU broadcasts the Bloom filter value of the group key list to update this in each vehicle that belongs to the same group. At this time, the 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 expired group key is updated through the value of the initial group key.

The RSU broadcasts not only the factor i required for the update but also the GBF required for the certification of the vehicle, including the Bloom filter value (GKBF) of the group key to be updated. The RSU broadcasts the GBF necessary for vehicle certification by encoding it with the previously distributed group key.

$$\mathrm{RSU} \rightarrow *: (\mathrm{GBF}||\mathrm{GKBF}||\mathrm{i}||\mathrm{TS}||\mathrm{T}_{\mathrm{REVOKE}})$$

(4) Group key renewal phase

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 but the vehicles do so directly and can validate the group key with a simple process, the arithmetic operations for updating the group key that 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.

$$h(GK_V||y+i) \leftrightharpoons GKBF$$

(5) 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.

(6) Authentication between Vehicle

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.

$$V_1 \rightarrow V_2 : E_{GK}(M)||PID_{V1}$$

3.4 Data re-encryption phase

Each vehicle encrypts its message using its public key when authentication is complete. The encrypted message is forwarded to the RSU, which computes the re-encryption and delivers it to each vehicle.

(1) Data Encryption

Each vehicle generates data to be transmitted as follows:

$$\begin{gathered} \text{random } r \in Z_q \\ A = pk_a{}^r \\ B = e(g,g)^{sk_a \cdot r} \\ C = e(g, H(pk_a))^r \cdot m \\ E = (A, B, C) \end{gathered}$$

(2) Re-encryption Key Generation

Like this, this research assumes an IoT network environment in which encrypted data is exchanged through group authentication among dozens of sensor nodes (vehicles). In the network environment, each node shares information with other nodes in other locations to communicate with an RSU acting as a gateway. In this case, the number of encryption/decryption increases in proportion to the number of nodes if the existing public key encryption is used. For example, if there are 50 sensor nodes on the network, each node must perform 50 encryption/decryption operations. However, proxy re-encryption is performed using an RSU that is an untrusted object in the proposed method.

$$A' = pk_b{}^{r}$$
$$rk_{a\to b} = (A', pk_b{}^{-sk_a})$$

(3) Data Re-encryption

The RSU replaces A' received from the vehicle a with A, performs re-encryption using the encrypted text and the re-encryption key received from a and the public key of the vehicle b. The re-encrypted text generated here can be decrypted by the vehicle b with its own private key

$$\begin{aligned} B' &= e(A, rk_{a\to b}) \\ &= e(A, pk_b{}^{-sk_a}) = e(A, g^{\frac{sk_b}{sk_a}}) \\ &= e(g^{sk_a\cdot r}, g^{\frac{sk_b}{sk_a}}) = e(g,g)^{sk_b\cdot r} \end{aligned}$$

$$E = (A', B', C)$$

(4) Decryption

The vehicle b decrypts the re-encrypted text received from the RSU using its own private key as shown in the following equation.

$$\begin{aligned} m &= C/e(A', H_2(pk_a))^{-sk_b} \\ &= \frac{e(g, H_2(pk_a))^{r}\cdot m}{e(A', H_2(pk_a))^{-sk_b}} \\ &= \frac{e(g, H_2(pk_a))^{r}\cdot m}{e(pk_b{}^{r}, H_2(pk_a))^{-sk_b}} = \frac{e(g, H_2(pk_a))^{r}\cdot m}{e(g^{sk_b\cdot r}, H_2(pk_a))^{-sk_b}} \\ &= \frac{e(g, H_2(pk_a))^{r}\cdot m}{e(g, H_2(pk_a))^{sk_b\cdot r\cdot -sk_b}} = m \end{aligned}$$

4. Analysis of the Proposed Method

4.1 Number of group key issuance

Assume that there exist 50~300 devices within the communication range of the TA. In the general case, the communication is performed per 300 ms and it receives the group key to be newly updated. However, because the proposed system only needs to communicate once with the group key updating list composed of the first group key and Bloom Filter per device, the process of transmitting the group key focused on the TA can be reduced. However, in the case of devices that are no longer within communication range, the previous list of group keys is deleted when communication with another TA is established by sending a message that includes the disposal time of the group key.

4.2 Arithmetic efficiency of updating the group key

The proposed system is capable of updating and verifying devices by transmitting a Bloom Filter generated by taking the list of group keys to be newly updated as the hash value. Thus, the advantage of the TA is that it can disperse concentrated arithmetic operations compared

with the existing system in which the TA broadcasts the group key after updating and encoding it each time.

In this section, the computational amount generated by the TA and each of the devices is compared with that of the existing system. The coefficients used in the formula required for the comparison are as follows.

4.3 Communication Traffic

Fig. 6 is a graph showing the comparison of the encryption speed of the proposed method and the network using the existing public key encryption. The proposed method takes some computational time. However, the existing method increases the number of encryption operations by the number of nodes, yet the proposed method can pass encrypted data to all nodes on the network with only one encryption operation. Decryption operations are rather similar or faster than the existing method. It is clear that this is more advantageous in an environment where many terminal devices are used (**Fig. 7**).

4.4 Efficiency in Data Sharing

A proxy server that does not need to check reliability is used to enable secure and efficient data sharing between nodes to be carried out. Moreover, the problem caused by the limited data storage capacity of lightweight devices, such as Atmega128, can be solved with efficient data sharing.

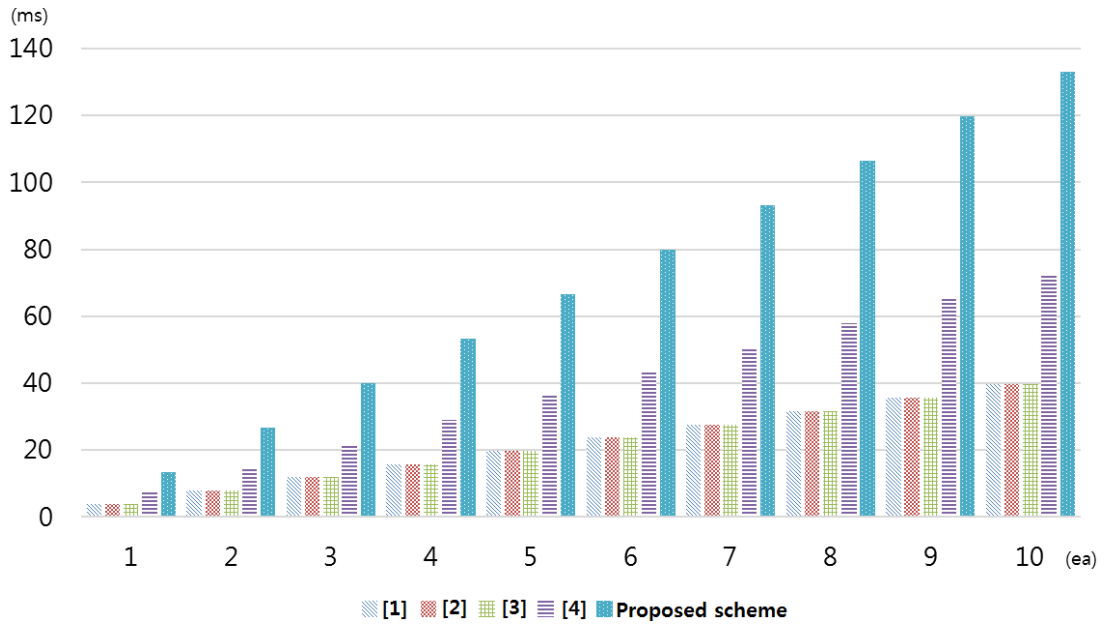

Fig. 6. Comparing the encryption method with the existing network

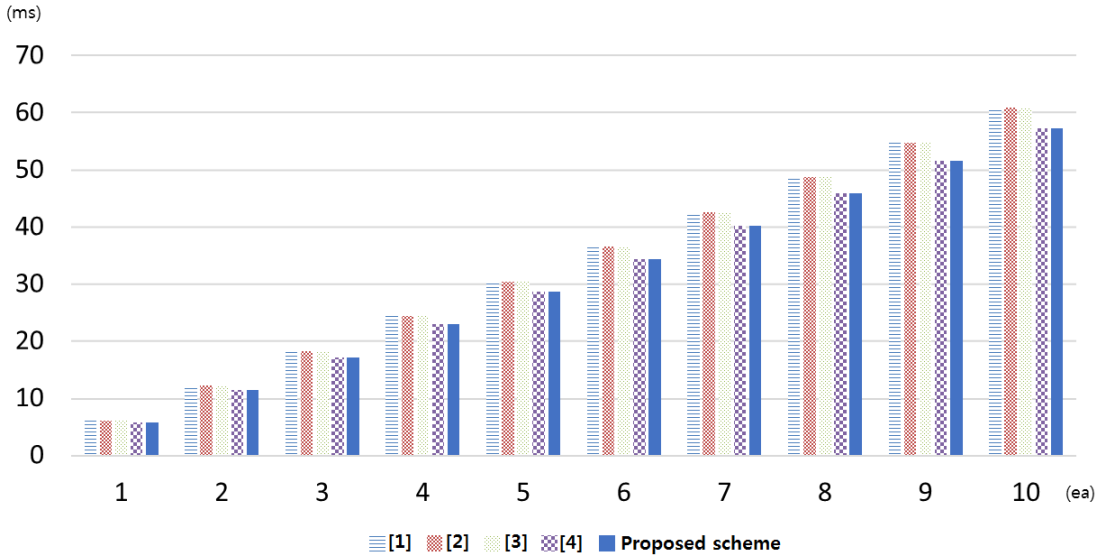

Fig. 7. Comparing the decryption method with the existing network

5. Conclusion and Future Research Direction

This paper proposed a verification method that updates the group key in IoT devices. The method uses a Bloom Filter to reduce the overhead of the group rekeying procedure focused on the TA in an IoT network environment in which numerous devices exist. This approach made it possible to minimize the number of communication messages and the time required for communication. The proposed method presented a more secure and efficient data management method among many nodes in various IoT environments including VANET. It is inefficient to use the public key encryption in the existing IoT network environment, yet the proposed method provides a more efficient communication environment. This method also provides enhanced security by using the proxy re-encryption method based on elliptic curve cryptography suitable for lightweight terminal devices.

In future, simulated experiments would be required to perform a comparative analysis in more detail than various existing methods by considering various environmental factors based on the method proposed in this paper.

References

[1] Liu, Zhe, et al. "Reverse product-scanning multiplication and squaring on 8-bit AVR processors," in *Proc. of International Conference on Information and Communications Security*, Springer International Publishing, 2014. Article (CrossRef Link).

[2] Ivan, Anca-Andreea, and Yevgeniy Dodis. "Proxy Cryptography Revisited," NDSS. 2003. Article (CrossRef Link).

[3] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC) 9.1*, pp.1-30, 2006. Article (CrossRef Link).

[4] Blaze, Matt, Gerrit Bleumer, and Martin Strauss. "Divertible protocols and atomic proxy cryptography," *Advances in Cryptology—EUROCRYPT'98* , pp.127-144, 1998. Article (CrossRef Link).

[5] Bloom, Burton H, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM 13.7*, pp. 422-426, 1970. Article (CrossRef Link).
[6] Raya, Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. "Securing vehicular communications," *IEEE Wireless Communications 13.5* , 2006. Article (CrossRef Link).
[7] Marimuthu, K., et al. "Scalable and secure data sharing for dynamic groups in cloud," in *Proc. of Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on. IEEE*, 2014. Article (CrossRef Link).
[8] Kim, Su-Hyun, and Im-Yeong Lee. "A secure and efficient vehicle-to-vehicle communication scheme using bloom filter in vanets," *International Journal of Security and Its Applications 8.2*, pp.9-24, 2014, Article (CrossRef Link).
[9] Kim, Su-Hyun, and Im-Yeong Lee, "A Secure and Efficient Vehicle-to-Vehicle Communication based on Sensor Network," *International Journal of Security and Its Applications 7.6*, pp. 241-248, 2013. Article (CrossRef Link).
[10] Kar, Jayaprakash, and Banshidhar Majhi. "A novel deniable authentication protocol based on Diffie-Hellman algorithm using pairing technique," in *Proc. of Proceedings of the 2011 International Conference on Communication*, Computing & Security. ACM, 2011. Article (CrossRef Link).
[11] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC) 9.1*, pp.1-30, 2006. Article (CrossRef Link).
[12] Blaze, Matt, Gerrit Bleumer, and Martin Strauss. "Divertible protocols and atomic proxy Cryptography," *Advances in Cryptology—EUROCRYPT'98* , pp. 127-144, 1998. Article (CrossRef Link).
[13] Maity, S., and J. H. Park. "Powering IoT devices: a novel design and analysis technique," *J. Converg 7*, pp.1-17, 2016. Article (CrossRef Link).
[14] Kwon, Taeyean, et al. "Efficiency of LEA compared with AES," *JoC6.3*, pp.16-25, 2015. Article (CrossRef Link).
[15] Keegan, Nathan, et al. "A survey of cloud-based network intrusion detection analysis," *Human-centric Computing and Information Sciences 6.1*, pp.19, 2016. Article (CrossRef Link).
[16] X. Lin, X. Sun, P.-H. Ho and X. Shen. "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," *IEEE Trans. on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007. Article (CrossRef Link).

Su-Hyun Kim
February 2016: Doctor of Computer Science, Soonchunhyang University.
February 2012: Master of Science in Computer science, Soonchunhyang University.
February 2010: Bachelor of Science in Computer Science, Soonchunhyang University.

Yong-Woon Hwang
February 2018: Master of Science in Computer science, Soonchunhyang University.
February 2016: Bachelor of Computer Software, Soonchunhyang University.

Jung-Taek Seo received his degree in information security from the graduate school of Information Security, Korea University, in 2006. From November 2000 to February 2016, he has worked for National Security Research Institute as a senior researcher as well as the head of Infrastructure Protection Research Department. Currently, he is an assistant professor in Department of Information Security Engineering, Soonchunhyang University. He has been a Principal Investigator of several govern ment sponsored research project in SCADA, Smart Grid, nuclear power plants. Recently, he has been actively working in the area of smart grid, in particular with respect to standard and policies. His research interest includes SCADA, Smart Grid, nuclear power plants, Smart City, CPS (Cyber Physical System).