International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:6, No:4, 2012

The Possibility to Resolve the Security Problems through the LTE in Vehicular Ad-hoc Networks

Sun-Hee Han, Hun-Jung Lim, and Tai-Myoung Chung

***Abstract*—**Vehicular Ad-Hoc Networks (VANET) can provide communications between vehicles or infrastructures. It provides the convenience of driving and the secure driving to reduce accidents. In VANET, the security is more important because it is closely related to accidents. Additionally, VANET raises a privacy issue because it can track the location of vehicles and users' identity when a security mechanism is provided. In this paper, we analyze the problem of an existing solution for security requirements required in VANET, and resolve the problem of the existing method when a key management mechanism is provided for the security operation in VANET. Therefore, we show suitability of the Long Term Evolution (LTE) in VANET for the solution of this problem.

***Keywords*—**VANET, Privacy, Security, LTE

I. INTRODUCTION

VEHICULAR ad-hoc networks (VANET) is a combined technology of Mobile Ad-hoc Network which establishes networks between devices, Mobile IPv6 and Proxy Mobile IPv6 which provide devices a mobility, and network mobility, depending on vehicle's characteristics. Recently, many studies on communications between vehicles, and vehicles to infrastructures are being done, because of the development and extension of wireless communications. Also, Intelligent Transportation System (ITS) can provide faster and safer traffic systems, so the interest in the studies and the commercializing VANET is growing. In VANET, the studies are being conducted mainly in network and security aspects. VANET can be divided into two ways, a Vehicle-to-Infrastructure (V2I) communication, and a Vehicle-to-Vehicle (V2V) communication by communication method. The V2I communication is a communication between a vehicle and Road Side Unit (RSU), which is connected with an existing infrastructure and mainly provides convenience to users such as multimedia. The V2V is a communication between nearby vehicles, and is used for exchanging urgent messages mainly about preventing accidents. There are two services provided by vehicular communications, which are safety message and non-safety message. Safety message is mostly transferred by V2V communication, and it is life-critical. To provide the safe service, it should provide authentication and security service.

Sun-Hee Han is with the Department of Electrical and Computer Engineering, University of Sungkyunkwan, South of Korea (phone: +82-10-9212-9575; fax: +82-31-299-6673; e-mail: shhan@imtl.skku.ac.kr).

Hun-Jung Lim is with the Department of Electrical and Computer Engineering, University of Sungkyunkwan, South of Korea (e-mail: hjlim99@imtl.skku.ac.kr)

Tai-Myoung is with School of Information Communication Engineering, University of Sungkyunkwan, South of Korea (e-mail: tmchung@ece.skku.ac.kr).

There is a possibility that the message about safe driving is false information or the contents can be manipulated, if then, that can cause accidents.

Because of that, it is hard to introduce services from VANET without a proper security mechanism. Therefore, the message authentication should be provided. However, if messages are exchanged by an existing digital signature, that will cause the privacy threats. In terms of VANET, the studies are still being carried out to satisfy these privacy issues and the security mechanism at the same time. In addition, the high cost and the shortage of the RSU at the early stage of introduction become an obstacle for vitalizing vehicular communication. Thus, we chose LTE network as a solution to the privacy and security problem while reducing the initial building cost for vehicular communication system. And this paper analyzes LTE security service to find if LTE is suitable to provide vehicular communication service

This paper is organized in the following. In Section II, we describe VANET communication based on Long Term Evolution (LTE) through performance evaluation. And, in Section III, we explain the security requirement in VANET and problem of the existing solution for security requirement, and show the key management mechanisms and problem of the existing method for key management in VANET. In Section IV, we describe LTE suitability in VANET, and in Section V, we conclude this paper.

II. RELATED WORK

A. The possibility of utilizing through the LTE in VANET

In the previous study, we conducted a field test to prove that LTE is usable in VANET environment. Table I shows performance evaluation result the delay in third-generation (3G) and the fourth-generation (4G) by speed.

TABLE I
THE DELAY IN 3G AND 4G

Speed	4G (LTE)	3G (HSUPA)
0Km/h	36.7ms	80ms
40~50Km/h	37.7ms	82.6ms
80~90Km/h	45ms	92.2ms
100~110Km/h	64.1ms	94ms

According to the performance evaluation result in VANET, both 3G and 4G met the non-safety message's delay requirement, which is under 100ms. However, this test is not considered the operation time because the test is performed by the ping. If the delay added the operation time for cryptography of 20ms about the upper layer, 3G not satisfied. Therefore, it is proved that LTE is proper for providing non-safety application service.

TABLE II
THE SECURITY REQUIREMENTS IN VANET

Security Requirements	Definition	Problem	Existing Solution	Problem of existing solution
Identification & Authentication	· Identification : Should be able to identity a valid user · Authentication : The process of verifying a user's identity	· Privacy threats by tracking identification information	· Anonymous Authentication [4] · Silent Period [5] · Mix-zone [6]	· When an accident occurs, there is a problem of verifying the identification · No suitable in VANET which exchanges messages periodically · Old & new ID traceable
Integrity	· The message should not be manipulated	—	· SHA-256 hash Function	—
Confidentiality	· The message should not be disclosed to an unauthorized third party	· Computation efficiency	· Elliptic Curve Integrated Encryption System (ECIES)	· Defined in IEEE 1609.2 Standard [7] · The key exchange protocol has not been defined in IEEE 1609.2 Standard
Non-repudiation (Signature)	· A sender should not be able to deny the transmission of data	· Computation efficiency · When using the Digital Signature, it takes place privacy threats by ID's exposure	· Group Signature [3]	· Hard to define group members · Computationally expensive
Privacy (Conditional)	· Prevent an unauthorized third-party from identifying the information of users and user's ID	· A necessity of conditional privacy	· Group Signature [3]	· Hard to define group members · Computationally expensive
Availability (Data trust)	· System availability : Can be guaranteed by performance of an encryption algorithm and TPD · Sensing data availability : Should be guaranteed reliability about the sensor information of vehicle	· The malfunction of sensors · The measured value can be manipulated by surroundings	· Navigation Message Authentication (NMA) [11]	· Out of scope

III. SECURITY IN VANET

A. The Security Requirement in VANET

Basic security requirements in network security are divided into six parts, Identification, Authentication, Integrity, Confidentiality, Non-repudiation, and Availability [9]. Because there is a threat to track vehicles' location in VANET, we decided Privacy to be added into security requirements for VANET. This section describes existing solutions and considerable problems to meet the security requirements for VANET's characteristics. Table II shows the security problems in VANET.

1) Identification and Authentication

Identification means identifying valid users, and Authentication means a process to identify the users' identity. In VANET environment, there are concerns about privacy because tracking identifiable information is possible. The existing solutions for this problem are Anonymous authentication, Silent-period, and Mix-zone. When changing ID periodically, it is possible to notice the changes by tracking old and new IDs. Therefore, the mix-zone concept was proposed to solve this problem. The Mix-zone concept is changing IDs of all the vehicles at the same time in certain regions. However, the changed IDs can also be tracked, so the silent-period method of Wireless Sensor Network (WSN) is proposed, which is that each node stops sending messages for a certain period at random before the changes of IDs. However, it is not suitable for VANET environment because it exchanges messages periodically. If the message is not delivered during the certain period, then that may cause an accident.

2) Integrity

Integrity means that messages cannot be manipulated. It should be possible to be checked by receivers if the received messages have been manipulated during transmission. The hash function for an integrity check is generally used Secure Hash Algorithm (SHA). The VANET provide the data integrity by comparing the hash values. In VANET, SHA-256 is recommended as a default because of the cryptographic requirement of a 128-bit long-term security level [7], [12]. It is described by the IEEE 1609.2 Standard [7].

3) Confidentiality

Confidentiality means that when sending messages, they should not be exposed to an unauthorized third party. In VANET, Safety messages and Non-safety messages are transmitted. The safety message is not required confidentiality as emergency message to notify an accident. On the other hand, when sending a Non-safety message which provides multimedia or a web service, confidentiality is required. To provide the confidentiality by preventing the manipulation of message by the eavesdropping, the message needs the encryption. The encryption is provided by using a symmetric key, and it uses an asymmetric key to share a secret key in VANET. However, there can be a performance problem in computation. Thus, it should be encrypted as Elliptic Curve Cryptosystem (ECC) of which speed is faster than other algorithms in calculation, and it is easy to implement both S/W and H/W. It is described in the IEEE 1609.2 standard. However, the protocol for the key exchange is not defined yet.

TABLE III
THE KEY MANAGEMENT IN VANET

Key Management	Definition	Proposed method	Considerations
Key Establishment	The process of generating keys for the cryptographic operation	· Selecting random key by RSU · Generating the master key by OBU [10]	· The environment in which RSU is not installed enough · A vehicle revocation mechanism
Key Distribution	The process to share generated keys between the sender and the receiver	· ECDH key exchange protocol [7]	· Privacy problem
Key Usage	Using the key to provide message generation, distribution, verification, and revocation securely	· Signature: ECDSA · Encryption: ECIES (Asymmetric) · Encryption: AES (Symmetric) · Hash : SHA-256 hash function [7], [12]	· Computation efficiency
Key Revocation (CRL)	When the key is expired or an untrusted vehicle is detected, the public key is revoked.	· Delta CRL [1] · Partitioned CRL [7] · Compressed CRL [1]	· ID should be frequently changed for privacy protection → The key update is frequent → Increase the CRL size → A problem of the CRL distribution

4) Non-repudiation (Signature)

Non-repudiation means that the sender should not be able to deny the transmission of messages. The safety message is not required the confidentiality, however, to prevent responsibility avoidance in case of an accident, a digital signature is needed to make the receiver not deny the received message. In the beginning, VANET studied the using of a RSA signature to satisfy non-repudiation. However, RSA signatures are computationally expensive as well as the size of certificate and of signature is very large. Because the operation time of the RSA signature is slow in calculation, currently, VANET uses the ECC to solve this problem. This is standardized by IEEE 1609.2 as explained in the integrity section. However, when signing, the privacy problem can occur because of the exposure of IDs. Therefore, Group Signature is proposed to generate signatures by issuing the secret key from the key distribution center. The Group Signature is verified as the public key of group, which is provided without the exposure of the ID. However, there is still a problem which the group member is not clearly defined yet.

5) Privacy (Conditional)

Privacy means preventing that users ID and private information from exposing to unauthorized third party. To prevent the exposure of ID, VANET provides Group Signature, but it still has a problem that group member is not clearly defined. When an inquiry of identity is needed in a situation like an accident, then the information can be provided by Trusted Group Manager (TGM). In this manner, if the group signature is used the anonymity can be assured because the signer is an unbeknown, and it provides the conditional anonymity by informing the identification in the specific situation.

6) Availability (Data trust)

In VANET, availability is divided, system availability and sensing data availability. However, this is related with the hardware security. Therefore it is not considered in this paper.

B. The Key Management in VANET

When a cryptographic operation is performed in Vehicular Communication, it needs the key which is OBU installed in vehicles. In addition, vehicles should be able to get the keys safely for secure communication each other [1]. Also, if malicious vehicles are detected, then the system should provide services for key update and key revocation. In this process, the key management is required. The key management is accomplished through the key establishment, key distribution, key usage, and key revocation phase. Table III shows the considerations about the key management in VANET. The followings are main mechanisms provided by the key management.

1) Key establishment

The Key establishment is operation process to generate public key and private key by using cryptographic operation for secure communication. There are two ways of generating keys in VANET. In general, there is the method by Road Side Unit (RSU) and by On-Board Unit (OBU). The method generated by RSU should provide sufficient RSUs. Thus, Zhang et al. proposed a method to generate the key in vehicle [10]. According to this proposed method, a master key of an identity-based Public Key Generator (PKG) is stored in TPD and each vehicle generates anonymous public key pairs using the master key. However, this method has a problem that it does not provide revocation mechanism required in VANET.

2) Key distribution

The key distribution means distributing the keys to secure data transmission. In IEEE 1609.2 Standard, Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol is specified [7]. However, ID of the user would be exposed when the user signs to key exchange in VANET. Therefore, VANET is considered as privacy threats by threats of tracking.

3) Key Usage

The key usage means using the key to provide message generation, distribution, verification, and revocation securely. The security requirements are satisfied by using the key in signature techniques, encryption mechanisms, and hash

function. The signature scheme used in VANET to provide authentication is based on the Elliptic Curve Digital Signature Algorithm (ECDSA). It is provided the key with a length of 256 in general and the key with a length of 224 in safety message based on the V2V communication. Among the encryption schemes for confidentiality, an asymmetric method uses Elliptic Curve Integrated Encryption System (ECIES) and a symmetric method uses Advanced Encryption Standard (AES). Also, the SHA-256 algorithm is used for an integrity check as hash function. It is described in IEEE 1609.2 Standard.

4) Key Revocation

The key revocation means that it revokes the key and the certificate when a malicious node or the device malfunction is detected. In VANET, the ID should be periodically changed for privacy protection. Therefore, the certificate also periodically should be issued. An expired certificate should be updated and a detected attack is revoked by the public key. In addition, the information is known to all vehicles. Therefore, the CRL is distributed and the size of the canceled public key list becomes very large because the ID should be frequently changed. When driving, the time in which CRL can be distributed through the RSU is very short. Additionally, receiving the whole CRL within range of the RSU communication is greatly difficult because the CRL size is very large. Accordingly, the studies for the solutions of the CRL distribution problem have been conducted. The solution for the problem is to use Delta CRL, Partitioned CRL, and Compressed CRL [2]. Firstly, the Delta CRL only lists those certificates that are added from the last update to reduce the sending cost of Base CRL that is distributed to the whole lists of CRL. The Partitioned CRL is hierarchically divided into groups for rapid search and distribution of CRL. The Compressed CRL compresses the CRL through the Bloom filter. It checks the result value of certificates through the Bloom filter.

IV. The Possibility to Resolve of the Security Problems in VANET through the LTE

In this section, we present the methods to solve the considerations of security when the LTE is used in VANET. To provide VANET communication, the cost and time for constructing the infrastructure will be needed. Thus, the using of LTE in VANET is anticipated that the commercialization of VANET is activated more quickly. The Table IV shows the solution in LTE for the unresolved issues of the security in VANET.

TABLE IV
The Solutions to Resolve the Security Considerations of VANET through the LTE

No	*Consideration of the VANET Security*	*Solution in the LTE*
1)	When the RSU is not sufficiently installed	The HSS sends the IMSI and LTE key to MME when the device is connected in LTE
2)	Problem of privacy protection by the exposure of ID	Alternates the IMSI by generating the GUTI that the temporary ID

1) According to existing studies about VANET, the key can be generated by RSU. However, the key generation cannot be provided by RSU because the density of RSU placement has not yet been determined. Therefore, if the LTE is used, this problem will be solved through the Authentication and Key Agreement (AKA) protocol. The authentication protocol performs an authentication of device through the key information sent from Home Subscriber Server (HSS). The HSS has the International Mobile Subscriber Identity (IMSI) and the master key of the EPS called LTE key. It sends the key information to Mobility Management Entity (MME) for authentication of the users' device. Even though the RSU is not installed, the key generation is able to make use through an allowed key exchange mechanism that the AKA. Therefore, the LTE is anticipated that it is a suitable for VANET by generating the key through the AKA authentication protocol.

2) In LTE, the identifier is used to GUTI (Globally Unique Temporary Identifier) instead of the IMSI for solving the problem of privacy protection. When the device initially connects, it requests the registration as IMSI. And the GUTI is allocated from the MME. After this, if the device re-connects in other networks it can be solved the problem of privacy protection by using the GUTI.

V. Conclusion

In this paper, we shown the existing proposed methods for satisfying the security requirement in VANET and described the unresolved problems in VANET. In addition, the key management necessarily needs for this security requirement. Thus, the considerations about the problems among the existing solutions in the key management are also examined. To solve the problems, we looked for the possibility to apply the LTE in the VANET by studying the security of LTE. Through it, even though the RSU is not installed yet, it is anticipated that the vehicular network will be provided the services through the LTE.

Acknowledgment

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2010-0020210)

References

[1] Hannes Hartenstein and Kenneth P. Laberteaux, "VANET Vehicular Applications and Inter-Networking Technologies," WILEY, pp299 – 363, Dec. 2009.
[2] Michael E. Nowatkowski, "Certificate Revocation List Distribution in Vehicular Ad hoc Network," Georgia Institute of Technology, May. 2010.
[3] D. Chaum and E. van Heyst, "Group signatures," Proc. Eurocrypt, vol. 547, pp. 257 – 265, 1991.
[4] Shuai Zhang, Jun Tao, Yijia Yuan, "Anonymous authentication-oriented vehicular privacy protection technology research in VANET," International Conference on Electrical and Control Engineering (ICECE), pp.4365-4368, Sept. 2011
[5] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET", IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1569 – 1589, 2007.
[6] J. Freudiger and M. Raya, "Mix-zones for location privacy in vehicular networks," Proc. WiN-ITS, Aug. 2007.

[7] Steve M. Mills et al., "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages," Intelligent Transportation Systems Committee, Jul. 2006.
[8] Maxim Raya, Jean-Pierre Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, pp. 39-68, 2007.
[9] William Stallings "Cryptography and Network Security" 4th Ed. Pearson Education
[10] C.Zhang, et al., "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proceedings – IEEE INFOCOM., vol. 5473, pp. 309 – 324, Apr. 2009.
[11] Panagiotis Papadimitratos, Aleksandar Jovanovic, "Protection and Fundamental Vulnerability of GNSS," IEEE International Workshop Satellite and Space Communications 2008, pp. 167 – 171, Oct. 2008.
[12] "Vehicle Safety Communications – Applications (VSC-A)", National Highway Traffic Safety Administration, Appendix Volume 3, Sep. 2011.