Analysis of Security Problems in Vehicular Ad-hoc Networks using LTE Cellular Network

Alisha Siwach¹ and Dinesh Verma²

¹,²PDM College of Engineering, Bahadurgarh, Haryana
¹ales92siwach@gmail.com and ²erdineshverma@gmail.com

Abstract
VANET is composed of Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) communication. Recently, a vehicle ad hoc network for Intelligent Transport System (ITS) have become able to provide the safety and convenience services such as electronic toll collection system. To provide the proper services, VANET needs infrastructure over the country. Thus we have to spend a huge sum of money, time and human resources. In this reason several studies have been made on the usage of cellular networks instead of new protocols. The purpose of this study is to access a performance evaluation of the suitability of cellular networks for VANET. Here, we show the suitability of the Long Term Evolution (LTE) for the solution of security problems. 

Keywords: VANET, LTE, OBU.

1. Introduction

A vehicle can communicate with other vehicle and infrastructure with the help of ad-hoc networks. These communications are able to provide entertainment services, conveniences, and safety for drivers. Typically, VANET is composed of Vehicle to Infrastructure (V2I) communication and Vehicle to Vehicle (V2V) communication. To use V2I communication, Road Side Units (RSUs) must be installed. With RSU access point, vehicles can access the data stored in the RSU or even access the Internet through these RSUs. But we have to spend an enormous amount of money and human resources to build a new infrastructure. Several studies have been made on the usage of cellular networks instead of new protocols.

There is a possibility that any message transferred by other vehicular network is a false information or the contents can be manipulated, if then, that can cause accidents. Thus it becomes necessary that VANET services are provided with 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 problems.

Long Term Evolution (LTE) is a 4G technology which includes some new extraordinary features that were never before used in wireless and mobile communications and which give LTE an advantage compared to other technologies. Apart from that, some features that were included in older releases of the current mobile telephony standard, called Universal Mobile Telecommunications System (UMTS), were improved and refined in order to provide LTE with the capability of performing better than any other mobile communications standard.

This paper is organized as follows. Section 2 introduces the VANET Components. In section 3, various security attacks in VANET are described. Security requirements in VANET are described in section 4. Thereafter key management is shown in section 5 and then consideration of security problems through LTE is given in section 6. Finally we conclude this paper in section 7.

2. VANET Components

1) Components

i. OBUs (On Board Units): OBU is one of VANET components. It is a communications modules that provides a communication network for inter-vehicle and between vehicle and infrastructure.

ii. RSUs (Road Side Units): RSU is a communication device. Typically, RSU is installed on the road side. RSU sends a non-safety message mostly that is driver-friendly information such as traffic information, authentication messages, multimedia messages, and etc.
2) Message Types

VANET offers two types of messages. The safety message includes an emergency message such as emergency vehicle approach warning, pre-crash warning. This message requires the short delay unlike the non-safety message because it is a matter of emergency. When the vehicle receives safety messages, it should respond to the messages quickly. Typically, the safety message is received by the vehicles around through V2V communications. The non-safety messages are convenience messages for drivers. They include multimedia information, software upgrade message, and information of traffic jam on the route. These messages are large data typically. Therefore, the non-safety message is required throughput unlike the safety message.

3) Communication Types

i. V2I Communication: V2I communication is transmission mode between infrastructure and vehicle. It includes both safety messages and non-safety messages.

ii. V2V Communication: V2V communication is used for sending an emergency message. When an accident is occurred, each vehicle transmits safety messages via V2V communications to warn other vehicles in the roadway. In special cases, the V2V communication is used for sending non-safety messages.

3. Various Security Attacks in VANET

In this paper, we concentrate on attacks perpetrated against the message.

1) Denial of Service attack: This attack happens when the attacker takes control of a vehicle’s resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application’s information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles.

2) Message Suppression Attack: An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points. For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the warning and forced to wait in the traffic.

3) Fabrication Attack: An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates, identities.

4) Alteration Attack: This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested.

5) Replay Attack: This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending.

4. Security Requirements in VANET

1. Authentication & Identification: In Vehicular Communication, every message must be authenticated to make sure for its origin and to control authorization level of the vehicles. To do this, vehicles will assign every message with their private key along with its certificate, at the receiver side. The receiver will receive the message and check for the key and certificate. Once this is done, the receiver verifies the message. Signing each message with this, causes an overhead. To reduce this overhead we can use the approach ECC (Elliptic Curve Cryptography), the efficient public key cryptosystem.

2. Availability: Vehicular network must be available all the time. For many applications, vehicular networks will require real-time, these applications need faster response from sensor networks or even Ad Hoc Network. A delay in seconds for some applications will make the message meaningless and maybe the result will be wrong. Attempting to meet real-time demands makes the system vulnerable to the DoS attack. In some messages, a delay in millisecond makes the message meaningless.
3. **Non-repudiability**: Non-repudiability will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes. Any information related to the car like: the trip route, speed, time, any violation will be stored in the TPD, any official side holding authorization can retrieve this data.

4. **Privacy**: Privacy means preventing that users ID and private information from exposing to unauthorized third parties. 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 the Trust Group Manager (TGM). In this manner, if the group signature is used the anonymity can be assured because the signer is an unknown, and it provides the conditional anonymity by informing the identification in the specific situation.

5. **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.

6. **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.

5. **Key Management in VANET**

The followings are main mechanisms provided by the key management.

1) **Key Establishment**: The Key Establishment is the 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. 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. 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.

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.

6. **Consideration of VANET Security through LTE**

1) **When the RSU is not sufficiently installed**: According to existing methods, keys can be generated by RSU. But the whole key generation cannot be provided by RSU because the density of placement of RSU is not determined. Therefore, LTE is used and the problem will be solved through Authentication & Key Agreement Protocol (AKA). The Home Subscriber Server sends the key information to AKA. The HSS has International Mobile Subscriber Identity (IMSI) & the master key called LTE key. The HSS sends these keys to AKA, then AKA sends the key information to Mobile Management Identity (MME) for the authentication of device.

2) **Problem of privacy protection by exposure of ID**: In LTE, the identifier is used as Globally Unique Temporary Identifier (GUTI) instead of IMSI for solving the privacy problem. When the device initially connects, it requests the registration as IMSI, and the GUTI is allocated from MME. So if the
device reconnects in other network, it can solve the problem of privacy protection by using GUTI.

7. Conclusion

In this paper, we have shown the existing proposed methods for fulfillment of the security requirements 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.

References