ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 687-694
doi: 10.18178/wcse.2016.06.122

An Immediate Authentication Protocol for Exchanging Safety Messages in Heterogeneous VANET

Ji-Young Park and Hyoung-Kee Choi [+]

Sungkyunkwan University, Seoul, South Korea

Abstract. Vehicular Ad Hoc Networks (VANETs) improves road safeties and user experiences through Vehicle to Vehicle (V2V) communications in heterogeneous networks. Punctuality and protection on safety messages are critical as misuses of safety messages may result in deadly accidents roads. This study is geared toward to improving efficiency of safety messages by minimizing delays for prompt alerts for critical events on roads. Furthermore, integration of safety messages is confirmed by a specially designed authentication mechanism. Authenticating messages with symmetric cryptography enhances computational delays in the first hand. A pre-authenticated messages with a tight scheduling further reduces transfer delays. Especially, it is proposed the way to provide the authentication immediately for the case of event-triggered message because the kind of it is limited. And broadcasting messages among nearby vehicles in the 802.11p network are replaced multicasting among selected vehicles in the LTE network. In this way, secrecy in the VANET is fortified by message authentication.

Keywords: VANET, safety message, immediate authentication, delay, TESLA, heterogeneous network.

1. Introduction

VANET is a network that improves the suitability of wireless communication for vehicles. It provides general data transmission services and urgent alarm services. In particular, its communication purposes include increased safety, efficient movement in a traffic jam, and passenger convenience.

Communication types are divided into three categories in terms of providing services [1]. First, the Safety System reduces the hazards of traffic accidents by collecting information from the sensors. One of the most important requirements that the message transmitted is reliable and transmit to the other side in time limit. Second, the traffic efficiency application service optimizes vehicle flow and manages the previous traffic congestion about increasing the capacity of the road, relieving the traffic jam, and reducing the cost of road congestion. Finally, the infotainment application provides entertainment services, Internet access, and information for the convenience of the passengers. Due to the direct connection to life, the Safety System's message can be fatal in an emergency situation. Therefore, security is very important to prevent any security breach. It should be delivered in time, and there is a need for a study to increase the security in a brief time period.

The Safety Message must be certificated for reliability and transmitted to a nearby vehicle in order to notify and prepare for a potentially dangerous situation. This can be seen in the delay and security parts. In order to solve the problem, it aims to provide trustworthy safety messages near a large number of cars without delay. Moreover, it is supplied in the following procedure. First, the vehicle uses a direct broadcast method to the surrounding vehicles. The direct communication between the vehicles is faster than passing through the LTE infrastructure. Previously, message broadcasting experienced difficulty due to an authentication problem. Second, the solution to the problem is a proposal that allows a vehicle to send messages based on verified contents. For the increased security of the broadcast message, after the source

[+] Corresponding author. Tel.: + 82.31.290.7975
E-mail address: meosery@skku.edu

vehicle authentication, it should allow certification via broadcast message from the source vehicle including the key. Finally, the proposal includes an instant certification aimed specifically at event-triggered messages by using the TESLA. It enables prompt sending of the message without delay during the event.

The rest of the paper is organized as follows. Session 2 contains the review on the related work about the safety message in heterogeneous VANET. Session 3 presents the background on safety message and heterogeneous network. In section 4 describes the algorithm of an efficient immediate authentication for the safety message. Then session 5 presents the performance evaluation and comparison with the existing approaches. Finally, conclusions are drawn in session 6.

2. Related Work

In VANET, there are studies that use the heterogeneous network, and these can be divided into the following types. First, there is a research on how to send a safety message in the heterogeneous network that is related to minimizing the time for data transmission. The second part deals with improved security in the heterogeneous network.

The heterogeneous network transmits the safety messages to pre-designated vehicles via multicasting [7][8][9]. And the safety message should be sent to the nearby vehicles which isn't pre-designated from vehicles already receiving the data in the LTE network because that message should be transmitted to all of the vehicles within the area. The application of Unicast results in a 1:1 ratio of communication with the LTE network overhead, while the use of the broadcast method for sending messages into the vehicles can create a problem with certification. As a result, the vehicles transmitted messages using the multicast, and performed an authentication process by using the possession key and resending the failed delivery of messages to the vehicle. During this time, the topology frequently changes on account of the rapid transition of vehicles and, consequently, there is a need for a key update for multicast. The vehicles have to be given multicast messages; therefore, a delay occurs in the re-transmission. In order to resolve the verification and key update problems, the whole car uses a broadcast method that gets rid of the delay in sending a message on inter-vehicle communication, and the certification problem created by the broadcast method is solved through a symmetric-key message transmission. The detailed contents are shown in session 4.2. In addition, the emergency message delivered to the nearby vehicles is more important than the transmitted message via the infrastructure, which is required for a long distance communication. As a result, the vehicle uses a broadcast method that is not conducted through the LTE network infrastructure.

There are studies regarding the factors that improve the TESLA and apply it into the VANET for an overall improvement of the heterogeneous network security. The VANET Authentication with Signatures and Prediction-Based TESLA (VSPT) is a high arithmetic-speed that uses MAC [11]. TESLA has a delay because it waits for the next packet and processes the certification [10]. However, VSPT uses a method that processes a pre-certificate, anticipates the next packet, and then sends it for instant message verification. The message can be verified as soon as the packet has been obtained. The VSPT that is capable of processing the certification, however, needs to wait for the next message, which is hard to forecast during an emergency. For this reason, using it is difficult during an emergency situation. The main contribution of this paper suggests the method of certification and successful message transmission. Prediction of the next urgent message is difficult, albeit limited. The additional message of an event-triggered message is created and given immediate certification.

3. Background

3.1. Preliminary

3.1.1. Limited urgent message types

We cannot predict what kind of emergency situation will happen; however, the types of urgent messages are limited. Detailed contents, such as the exact GPS locator and target vehicle, are difficult to manage. But the urgent message contents, such as landslide occurrence, car crash occurrence, and emergency truck evasion, are restricted message size and needed a fast preparation.

3.1.2. Messages certification

A source vehicle creates and sends a broadcast message. A V2V communication, involving the exchange of information among several vehicles with one vehicle, is required for the verification of the safety message authenticity. This verification is not certain which car the message originated from; however, it means that the message coming from the vehicle is valid.

3.1.3. Meaning of immediate authentication

Immediate authentication can process verification upon receiving the message. When using PKI with the latest CRL, it can process the certification of the message via the public key. The original TESLA that uses a symmetric key can verify after one period under a new key disclosure. Prompt certification, which has been stated in this paper, does not mean a delay on certification, but instead it is the possibility of verification upon receiving a message.

3.2. Problem of Safety Message in WAVE

Security message is delay sensitive, and it requires certification prior to reducing and preventing possible traffic accidents. Based on the content of the message sent, we categorized this into two message types, namely, periodic sending message method and event-triggered method [1]. The periodic message method is broadcasted periodically, such as taking a beacon or heartbeat message's role. It delivers information, such as presence, position, kinematics, and basic status. This method periodically transmits messages with a signature that uses ECDSA and an allocated channel for the security message [1]. As soon as a traffic accident takes place, the event-triggered method sends a message of warning to nearby drivers in order to prevent other hazards, such as a potential crash, additional accident, and so on. This method transmits messages by using the same channel allocated for the security message with the use of ECDSA, which is signed by the sender.

Vehicle communication standard, WAVE, is not suitable for sending security messages due to the following reasons. First, it has an unbounded delay via WLAN. WAVE utilizes various channels for sending normal messages and control messages, unlike WLAN that utilizes only one channel. However, the use of a competition mode method still creates unbounded delay that is not suitable for a rapid communication. There are many topology changes due to high mobility that frequently impede the transition and result in a reduced efficiency of the whole network. Second, the WAVE protocol has limitations regarding intermittent and short-lived V2I when transmitting a security message. There are many places where RSU installation is rare or not as high installation cost, and the links trip out or delay, thereby causing a limited communication range. Finally, it is not good in terms of security. WAVE protocol uses ECDSA as its encryption mechanism. The message sent through wireless communications into the cars has a certification-based digital signature. However, it has problems, such as the CRL management [4], and unsuitable standard in a super-high-speed communication. Due to the low efficiency of the elliptic curve encryption algorithm, verification and forgery prevention are both needed for applying an actual security.

3.3. Heterogeneous Network for VANET

The Safety Message transmission problem is solved by adding LTE on long range communications (V2I) [2]. First, LTE is a commercial cellular based system, so an immediate application is possible without installing a base station and solving connectivity interruption issues due to the limitation of the RSU. Moreover, LTE is developed for the quick wireless communications of the mobile node. So, LTE has a wide coverage, which is good for mobility supply with an LTE Infrastructure that can be used as part of a V2V bridge. In terms of security, mutual certification, and message encryption via symmetric key, it can quickly process the certification and encryption performance as compared to the existing ECDSA that uses the PKI method. The LTE is a pure cellular-based communication; however, the short range communication that uses the existing WAVE's V2V communication compensates the part unsupported by the LTE [6]. As can send an inter-vehicular emergency message and communicate without a base station, applying V2V communication cannot be used in destroyed station by disaster, accident and so on but also its overhead reduces. Also, it has less than V2I's delay.

Therefore, the heterogeneous network selects the advantages of WAVE and LTE by using WAVE as a V2V communication method in short range communications, and using the V2I communication method for

applying LTE in long range communication.

3.4. Goal of design

Among the three types of VANET, safety service is the most important in security because it should be conducted promptly upon creating the message. The safety message can become fatal due to falsification of information. In order to improve the shortcomings of WAVE, the heterogeneous network targets the reduction of the delay caused by authentication for prompt safety message transmission. The vehicle broadcasts directly to nearby vehicles, but the delay occurs because of the process in passing several hops. However, a broadcast message sent from pre-certificated vehicles are immediately considered as authentic. By using the hash chain for the key update, a vehicle can conduct a key update and an efficient verification by using a symmetric key. Finally, the target promptly verifies event-triggered messages for more efficiency.

4. Proposed Protocol

The proposal protocol can be divided into two parts. Session 4.1 explains that each vehicle has been certified previously through the LTE network using EPS-AKA, and the value has been safely made by the eNB. The value is used to prove that the vehicle has been verified by the eNB before sending messages. Session 4.2 suggests a method for prompt authentication and completed certification to improve originally TESLA that message was completed authentication wait next one period. In addition, we propose an immediate authentication and transmission for an emergency message as soon as happen which is difficult problem using the periodic messages. A detailed explanation about each part of the protocol follows.

4.1. Source Vehicle Authentication with LTE infrastructure

EPS – AKA, which is the conventional authentication method for the LTE, is used for mutual authentication between the device and the wireless communication network [5]. The LTE K and IMSI are stored in the user device and network as fixed values. After the mutual authentication by using these values, the eNB and the UE are used to generate the symmetric key, K_{Upenc}, to encrypt and decrypt the packet. In the same way, after performing a mutual authentication between the LTE network and the vehicle through EPS-AKA, each symmetric key for the secret communication is possible through the K_{Upenc} ***(M1)***. The following shows the process of verifying a value that eNB generates and receiving this value safely.

M1: The encrypted data can only be opened by K_{Upenc}, which is the source vehicle, because the eNB and the vehicle deliver messages encrypted with a shared symmetric key. The source vehicle holds this information and transmits to the surrounding vehicles to perform the authentication from the other vehicles.

M2: The vehicle pre-certification is conducted thereafter for message broadcasting. For a rapid communication, a broadcast method of V2Vcommunication is used, and not the V2I communication. The non-interactive zero-knowledge method verifies the source vehicle's certified value that has been transferred from the eNB [12][13]. During this time, the hash chain's value, K_0, is used to authenticate the broadcast message and safely transport it later on. The verification is possible by using the general non-interactive zero-knowledge method. The process to authenticate the source vehicles has been omitted due to the paper's topic.

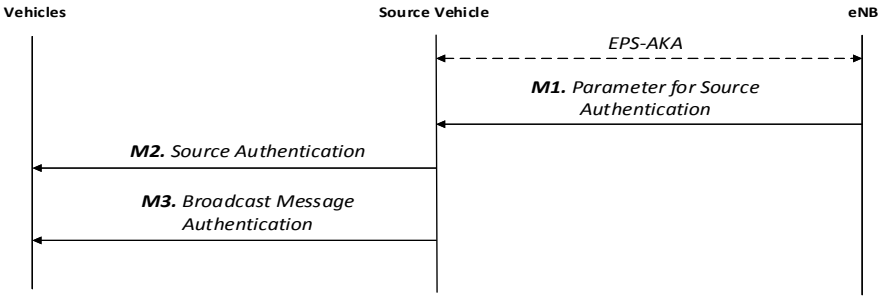

Fig. 1: Full flow of proposed protocol.

4.2. Verification of Broadcast Message

After verifying the source vehicles at the previous stage, K_0 has been proven to be authentic. Therefore, the message from a vehicle that received certification is determined as the message that can be trusted. The

following shows how a vehicle as the receiver authenticating the message when the source vehicle broadcast a safety message in a periodic or event-triggered manner.

Key generation

K_0, which is the seed from ***M2,*** is the value hashed in n time. K_0 is the certified key and the source vehicles reveal the key in K_1. For example, if K_0 is the trusted value when K_1 was released, there is $K_0=H(K_1)$ because the hash is a one-way function through K_0, and K_1 is certification available. The source vehicle has one disclose key for every cycle to authenticate themselves through hash relations.

Periodic message

This is a periodically transmitted message and it can be included in the detailed information if needed. In Fig. 2, the transmitted packet2 (P_2) was divided into four parts. The (m_{2_B}, $k_{3,3}$) of the packets are parts of the actual transmitted message, while the key value, $k_{3,3}$, is the key for an event-triggered message, which will be explained in the next session (Immediate authentication for an event-triggered message). The second part of the packet, it is possible to generate beforehand a MAC value for immediate authentication. Because the types of emergency messages, is limited (Refer Table 1); therefore, a MAC value about an urgent message that will occur can be generated in advance. The MAC value is not made public until the key is released because it is made by using the next unexposed key. Furthermore, the MAC constructor adds a random value that no one knows except for the constructor into the message to prevent a takeover at the coordinated time. The third part of the packet prepares the time when no immediate authentication has been performed. An immediate authentication is non-existent if the packet is missing or damaged. However, the message authentication is required, as well as the preparation for a not pre-defined message. The MAC value generates by using a key, which has not yet been disclosed, in the same way as the original TESLA. The MAC value of a message can be checked because the vehicle is capable of creating all keys used previously based on the key that is opened thereafter. Finally, in the current cycle, the last part of the packet transports the disclosed key and the random values for immediate authentication. In Fig 3, the process of a prompt certification is showed by using a key and a random value. The key K_3 is examined for verifying the authenticity of the current message of the packet. If it satisfied $K_2=H(K_3)$ operation, K_2 is already a proven value, and K_3 can be trusted through a one-way hash function. This message verification is completed if the MAC operated $MAC_{K3}(m_{3\_A}, R_{3,1})$ by using K_3 matches that are calculated in advance at the previous packet(P_2). When using the same random value, an attacker can arbitrarily generate a MAC value on other pre-defined messages; therefore, each message should have different random values to prevent it.

For this reason, pre-defined messages, which are received through the above method, can accomplish immediate authentication, and the certification is available through the next message even if it is not pre-defined or occurs a packet loss.

Event-triggered message

Emergency messages are sent between periodic messages, if needed. In right what happened, source vehicles generate the message and broadcasts this to the nearby vehicles. Table 1 shows an instance when the emergency message is transferred for immediate authentication. Upon receiving, the message authentication is possible because the periodic message already set up the MAC value of the pre-defined messages.

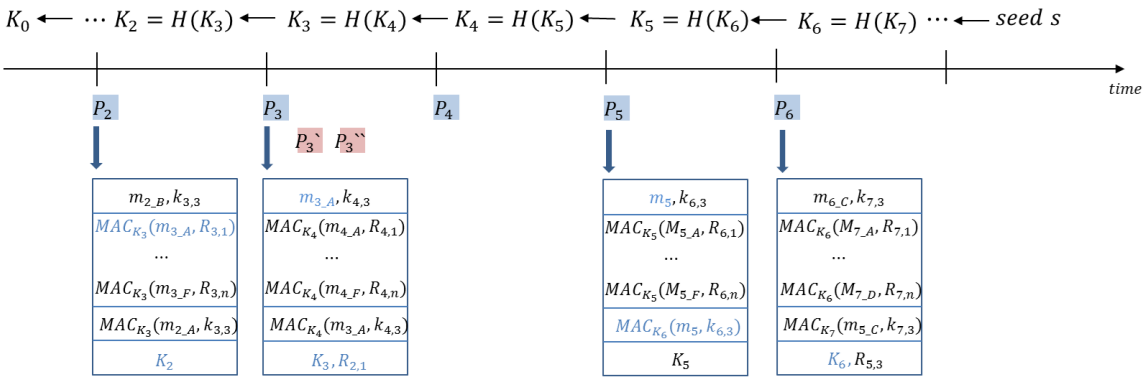

Fig. 2: Chained keys and packet generation for periodic message.

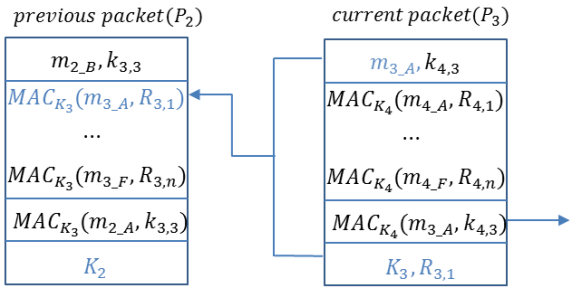

Fig 3. Method of immediate authentication.

Table 1. Kinds of safety messages.

Type	Message contents
A	Safety notice
B	Change lanes
C	Driving problem(like load problem)
D	Emergency vehicle avoidance
E	Break
F	Accident occurrence

Immediate authentication for event-triggered message

It has a limited number that event-triggered messages are possible to be transferred between periodic cycles. As a result, the temporary key is generated and it can be used during each period. If the packet generator does not know the next key, it cannot create a temporary key because the ephemeral key is using the disclosed key with a hash (Fig. 4). The event-triggered packet (P_3', P_3'') exist between the periodic packets, to which authentication is possible to use already disclosed key. There is no disclosed MAC value with regard to the same message because the event-triggered messages are generated on a new case, and not the previous events. Therefore, both the key and random value are known in order to create the MAC value. The key has already been revealed, but the random value is transmitted with the event-triggered message. For this reason, it is difficult for the attackers to manipulate the messages. For example, the messages transmitted from P_3' have $MAC_{K3}(m_{3\_C}, R_{3,3})$ in P_2. K_3 is already disclosed in P_3 but, in order to authenticate m_{3_C}, the transmitted $R_{3,3}$, that was transferred from P_3', should be recognized along with it. A prompt certification about the message of P_3' is possible if it has the same value transferred in P_2 as $MAC_{K3}(m_{3\_C}, R_{3,3})$. In addition, the receiver is able to confirm that the event-triggered message is now created by a temporary key included at the end of the packet.

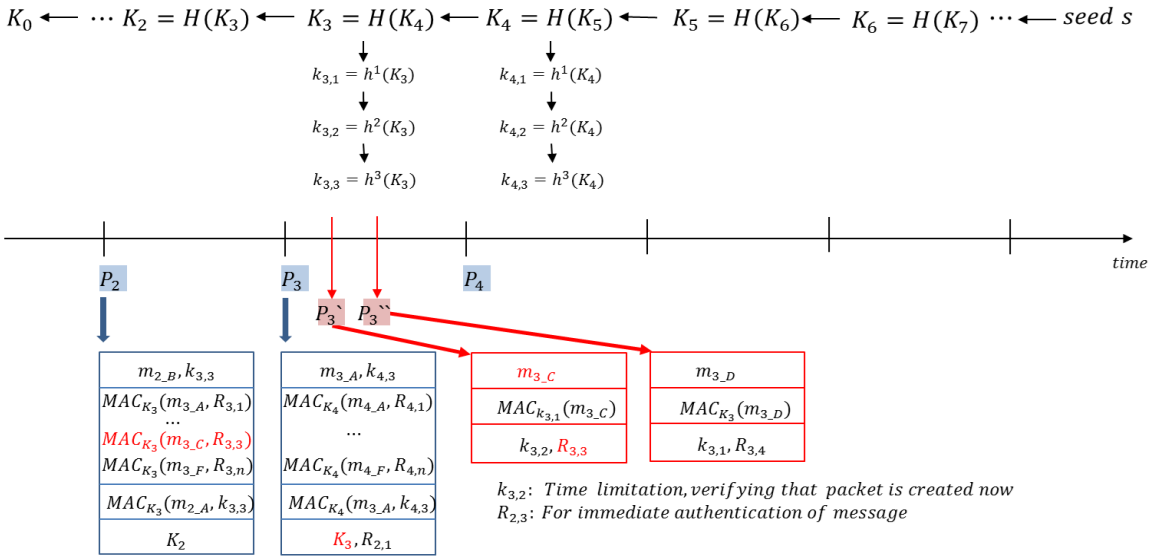

Fig. 4: Chained keys and packet generation for event-triggered message.

5. Evaluation

Following evaluation is fulfilled for performance test of suggested protocol. A Table 2 defines parameter generally used in VANET. On characteristic of an urgency message, the certification of the message is completed in 50ms, or it is cognized as out of date.

Table 2. Parameters

Parameter	Value
ECDSA generation time	7 ms
ECDSA verification time	22 ms
Hash or MAC operation time	1 μs

5.1. Authentication Delay

ECDSA and TESLA ways are compared by delay time for certification [11]. In ECDSA, the more packet mount increases, the more time required is needed. That make packet's mount over standard get waiting time (Fig. 5). TESLA, before disclosing MAC key, doesn't authenticate. And, delay about 1 interval always exists. Whereas, proposal protocol previously sends MAC value of the message to be certificated and then there is no delay for message's verification. When periodic time is 100ms, TESLA will have 100ms delay and proposal only have calculation delay for MAC. On the other hand, ECDSA have 22ms verification time. It is smaller than TESLA's waiting time. But unlike TESLA which has 1 interval waiting time and short verification time, the more the vehicle is increased, ECDSA verification time will be increased.

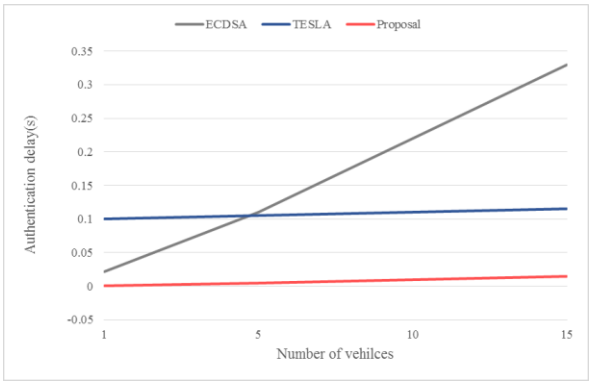

Fig. 5: Authentication delay.

5.2. Comparison delay when increasing amount of advance authenticated message

Because Emergency messages types are limited, the message authenticator can be created and certificated in advance. In that time when the types increasing, the delay is measured (Fig. 6). First, the cost of creating, delay message increase in sender side. As one of them arising, overhead that one of MAC values can be calculated takes place. But, that MAC calculation is very short doesn't make much effect in whole message's creation. In Receiver side, given messages computation and search make delay, calculation of one message don't create an additional delay.

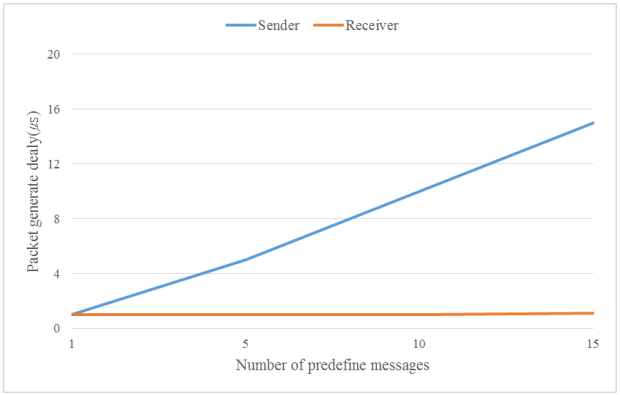

Fig. 6: Packet generation delay of pre-defined messages.

5.3. Success rate of emergency message reception as a period

The shorter Periodic message's period is, the more potential that emergency message can be sent and gotten in time limitation increase (Fig. 7). But, as many messages sent, there is concern about broadcast storm. However, in proposal method, although periodic message cycle is long, prompt certification of event-triggered message can be done and besides decrease the probability of broadcast storm occurrence. This evaluation doesn't consider broadcast storm. We anticipate that reception success rate of emergency message will decrease when the more periodic have long term. For example, when periodic time is 50ms, all emergency message which is generated in periodic time can be received. But if periodic time is 100ms, possible to receive message is only 50%. Because only emergency message, which is generated after 50ms based periodic time, can be received.

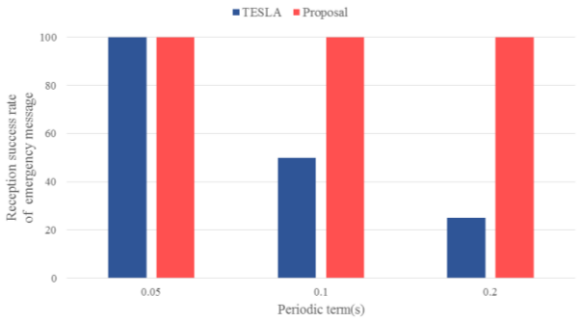

Fig. 7: Reception success rate of period time.

6. Conclusion

A limitation is found of the transmitting safety message of heterogeneous network combining strengths of LTE and WAVE. We raise the efficiency of delivering safety message by broadcast verified contents which are generated vehicle certificated by LTE network. For enhancing the usability of safety message, proposed to the immediately authenticating mechanism. This paper arbitrarily worked performance evaluation but the later simulator is necessary.

7. Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. NRF-2013R1A1A2013154)

8. References

[1] Kenney, John B. "Dedicated short-range communications (DSRC) standards in the United States." *Proceedings of the IEEE 99.7 (2011):* 1162-1182.

[2] Araniti, Giuseppe, et al. "LTE for vehicular networking: a survey." *Communications Magazine, IEEE 51.5* (2013): 148-157.

[3] Hartenstein, Hannes, and Kenneth Laberteaux, eds. VANET vehicular applications and inter-networking technologies. Vol. 1. *John Wiley & Sons*, 2009.

[4] Lin, Xiaodong, and Rongxing Lu. Vehicular Ad Hoc Network Security and Privacy. *John Wiley & Sons*, 2015.

[5] 3GPP-TS36.300 v8.5.0, “E-UTRAN Overall Description”. 2008.

[6] Zheng, Kan, et al. "Reliable and efficient autonomous driving: the need for heterogeneous vehicular networks." *Communications Magazine, IEEE* 53.12 (2015): 72-79.

[7] Atat, Rachad, et al. "Delay efficient cooperation in public safety vehicular networks using LTE and IEEE 802.11 p." *Consumer Communications and Networking Conference (CCNC), 2012 IEEE*. IEEE, 2012.

[8] Javed, Muhammad Awais, Duy Trong Ngo, and Jamil Yusuf Khan. "A multi-hop broadcast protocol design for emergency warning notification in highway VANETs." *Eurasip journal on wireless communications and networking 2014.1* (2014): 1-15.

[9] Ucar, Seyhan, Sinem Coleri Ergen, and Oznur Ozkasap. "Multi-hop cluster based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination." (2015).

[10] Perrig, Adrian, et al. "Efficient and secure source authentication for multicast." *Network and Distributed System Security Symposium, NDSS.* Vol. 1. 2001.

[11] Lyu, Chen, et al. "Efficient, fast and scalable authentication for vanets." *Wireless Communications and Networking Conference (WCNC), 2013 IEEE.* IEEE, 2013.

[12] D.R. Stinson. Cryptography - Theory and practice (3rd ed). *Chapman & Hall/CRC Press, 2006.*

[13] Feige, Uriel, Amos Fiat, and Adi Shamir. "Zero-knowledge proofs of identity." *Journal of cryptology 1.2 (1988):* 77-94.