ISSN 2586-1816 / e-ISSN 2586-4440
융합정보논문지 제7권 제6호 pp. 97-102, 2017 DOI : https://doi.org/10.22156/CS4SMB.2017.7.6.097

Review on Security Communication Environment in Intelligent Vehicle Transport System

Jin-Keun Hong*

Department of Information Communication, Baekseok University

지능형 차량 교통체계에서 보안 통신 리뷰

홍진근*

백석대학교 정보통신학부

Abstract In this paper, we have interested in cooperative intelligent transport system and autonomous driving system, and focused on analysis of the characteristics of Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Basis Service (DENM) message, which is key delivery message among cooperative intelligent transport system (C-ITS) characteristics for research objectivity. For research method, we also described V2X communication, and also analyzed the security certificate and header structure of CAM and DENM messages. We described CAM message, which is a message informing the position and status of the vehicle. And the DENM message is presented a message informing an event such as a vehicle accident, and analysis security communication, which is supported services. According to standard analysis result, 186 bits or 275 bits are used. In addition to the security header and the certificate format used for vehicle communication, we have gained the certificate verification procedure for vehicles and PKI characteristics for vehicles. Also We derived the characteristics and transmission capability of the security synchronization pattern required for V2X secure communication. Therefore when it is considered for communication service of DENM and CAM in the C-ITS environment, this paper may be meaningful result.

Key Words : Communication, ITS, WAVE, V2X, Authentication

요 약 본 논문에서는 연구목적과 관련하여, 협업 지능형교통체계와 자율주행체계에 관심을 가지고 있으며, C-ITS 특성 가운데 핵심 전달 메시지인 CAM과 DENM 특성 분석, 또한 V2X 통신의 보안 특성과 함께 CAM 및 DENM 메시지의 보안 인증서 및 헤더 구조를 중심으로 분석에 초점을 맞추고 있다. 연구방법에 대해, 우리는 CAM 메시지인 차량의 위치와 상태를 알리는 메시지를 분석하고, DENM 메시지인 차량 사고와 같은 이벤트를 알리는 메시지를 분석하고, 이를 지원하는 보안통신 특성을 분석한다. 차량통신에 사용하는 보안헤더와 인증서 형식과 함께, 차량용 서명된 인증서 검증 절차, 그리고 차량용PKI 특성을 얻었다. 아울러, V2X 보안통신을 위해 필요로 하는 보안 동기패턴에 대한 특성과 전송능력에 대해서도 함께 유도할 수 있었다. 그러므로 본 논문은 C-ITS 환경에서 DENM 및 CAM을 전송하는 통신 서비스를 위한 보안 특성을 고려할 때 의미 있는 결과라 할 수 있다.

키워드 : 통신, 지능형 교통체계, WAVE, V2X, 인증

Received 2017-11-22 Revised 2017-12-06 Accepted 2017-12-20 Published 2017-12-31
*Corresponding author : Jin-Keun Hong (jkhong@bu.ac.kr)

1. Introduction

Recently, the Korean government has been studying the development of traffic-communication integrated simulator and application of service scenarios as part of road traffic advancement project in order to complement the next generation ITS project. The wireless access in vehicular environment (WAVE) is an improved communication technology applied between vehicle and vehicle, whereas dedicated short range communication (DSRC) is used for short distance dedicated communication in intelligent transportation system. In general, V2X communication is a communication between a vehicle and a vehicle on a road within a 300-meter radius of an urban area. However, WAVE provides communication exchange in high speed environment up to 200km/h and supports V2X (V2V, V2I, V2P, etc.) service. The WAVE adopts IEEE 1609.1 standard for resource management, IEEE 1609.3 standard for network service, and IEEE 1609.4 standard for multi-channel operation. Of course, WAVE supports IEEE 802.11p for MAC and physical layer services. On the other hand, in open areas, transmission and reception are possible up to kilometers. In this case, the used frequency band is 5.8~5.9GHz band, and wireless access to the license-exempted country information infrastructure is possible. The WAVE complies with IEEE802.11p standard, and the channel bandwidth is 10MHz and 20MHz. The WAVE, which provides V2X communication, adheres to the security message standard or security communication procedure defined in IEEE1609.2 for communication security. This specification provides a WAVE message authentication mechanism, a user authentication mechanism, and provides a pseudonym authentication mechanism for the purpose of user protection. The composition of this paper first discusses the view of related research in Chapter 2. In Chapter 3. we discuss convergence software technology in 4th industrial revolution environment. In Chapter 4, we will look at quality characteristic of convergence software. In Chapter 5 several conclusions are reviewed.

2. Related Research

Muhammad Awais Javed et al. have studied security, QoT, and safety in C- environment[1]. Emilia Bubenikova and others have issued warning about driving lane crossing in C-ITS application and implementation[2]. Houda et al. studied a new service advertising message for the ETSI ITS environment[3]. Brigitte et al. presented the standards and implementation procedures of the C-ITS security framework in Europe[4]. Mohamed et al. have studied the security implications of collaborative perception in a dense network of vehicles[5]. Alexander Paier looks at intelligent concepts of situations in European collaborative ITS environments[6]. William et al. studied threats and countermeasures in WAVE service advertising[7]. Pierpaolo et al. studied the security of C-ITS messages[8]. Lei Chen et al. studied the C-ITS EU standard[9]. Wai et al. are interested in vehicle networks and applications[10]. Laszlo et al. are interested in the extension of the ITS terminal structure, focusing on the low power sensor network environment[11]. IEEE P1609.0/D9 presents a draft guide for wireless access in vehicle environments[12]. Sofiane et al. have studied lightweight trust aware relaying techniques for vehicle networks[13]. Mohammad et al. have studied lightweight authentication and key agreement protocols in ad hoc networks[14]. Yin et al. focused on safety in vehicle control networks[15]. The studies mentioned so far focus primarily on the importance of security threats, services, and technology in the C-ITS communication environment. It can also be seen that robust security is required in vehicle networks.

We will now describe the CAM and DENM messages, which are the main messages that pass between vehicles and between vehicles and infrastructure.

3. CAM & DENM Structure

3.1 Cooperative Awareness Message (CAM)

The CAM message exchanges this message with neighboring vehicles with information about the location and status of the vehicle. The cooperative awareness message (TS 102 637-2 V1.21) of the ITS communication structure that transmits the location, speed, and time of Europe is as follows. Fig. 1 shows format and information of CAM.

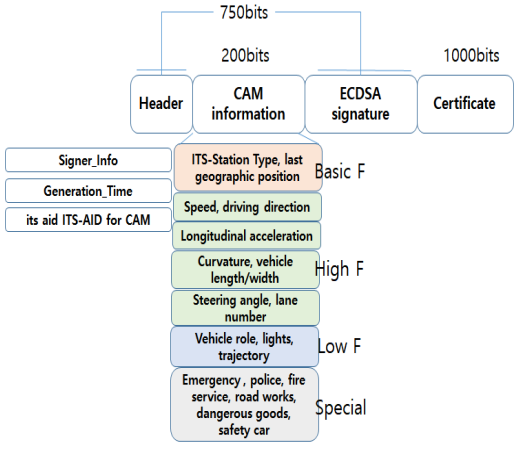

Fig. 1. CAM format and information

The security headers used for CAM signatures include protocol version (1 byte), protocol header field (1 byte), Singer_info (1 byte), certificate_ digest_with_sha256 (1 byte), hashedid8 digest (8 bytes), its_aid (1 byte), ITS-AID (1 byte for CAM), signed (1 byte), length (1 byte), signature (1 byte), ecdsa_nistp256_with_sha_256 (1 byte), x_coordinate_ only 1 byte).

3.2 Decentralized Environmental Notification Basis Service (DENM)

The DENM message is a response message triggered by an event such as an incident being detected. The basic service message (Signer_info, generation_time, generation_location, its_aid, signature) that notifies the warning of the distributed environment has the following structure (TS 102 637-3 V1.1.1).

The minimum short message with the exception of the certificate and signature value is 186 bits for European standards (ETSI 102637 1-3) and 275 bits for US standards (SAE J2735). However, the length of the message, including the signature value and the certificate, reaches 2000 bits for both US and European standards. Fig. 2 shows format and information of DENM.

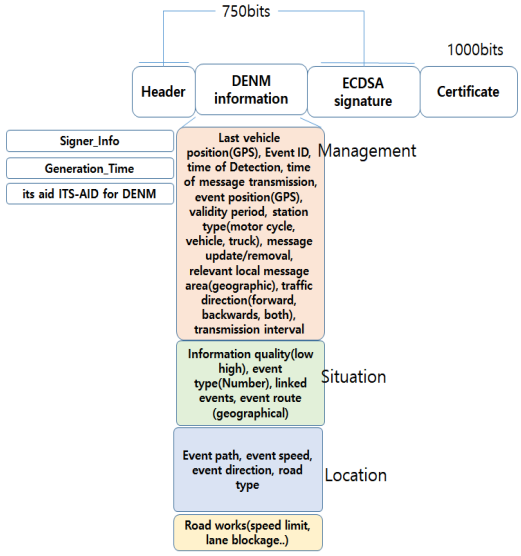

Fig. 2. DENM format and information

3.3 Security header and certificate formats

The message structure for transmitting the security header and the certificate format (TS 103 097 V1.1.1) is as follows.

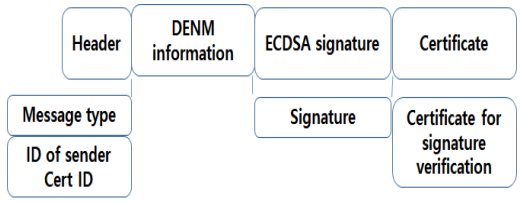

Fig. 3. ETSI DENM header and certificate format European ETSI uses the following certificate formats. Fig. 3 shows header and certification formation of ETSI DENM.

3.4 The procedure of signed certificate validation

First, configure the certificate chain. Confirm that the certificate is not withdrawn in the chain. Check the certificate chain according to the correspondence. Next, verify that the message matches the certificate and that the message matches internally and matches the transport layer. Cryptographic verify signatures on explicit certificates. Check the replay attack and check for freshness. Once again, it is important to verify the consistency of the certificate between the signed certificate and the signed communication.

- It verify that the communication occurs within the geographical location specified in the certificate (eg latitude = 38,887,410, longitude = -70,001,010, radius = 10)
- It check whether the communication is generated within the validity period of the certificate.
- It ensure that the communication release time is within the validity period of the certificate.
- It ensure that the information in the communication matches the operational permissions given to the certificate, where the correspondence is determined using the rules specified by the source maintaining the PSID (eg PSID = E0 00 00 01).
- The public key indicated by the certificate must be used to verify the signature cryptographically on the communication.

In other words, the signed data is encoded according to the data structure, including the PSID in the encoding, and if the PSID information element in the signed data is one of the authorization PSIDs of the certificate, the signed data matches the permission in the signing certificate.

3.5 Characteristics of PKI Certificate

The characteristics of the PKI certificates used in vehicles are as follows. Europe uses RCA, LTCA, and PCA, while root CA, enrolment CA, intermediate CA, and PCA are used. Key backups have this capability in the United States. In Europe, RSA private keys and motion sensor master keys are personally backed up, stored and restored.

4. Security Communication of V2X Vehicle

4.1 Communication Technology

The V2V communication for C-ITS application is transmitted between the vehicle ITS terminal and the vehicle ITS communication unit by a communication frame, which is composed of ITS MAC-GeoNetworking -Security-CAM/DENM. Here, when transmitting from the vehicle ITS communication unit to the application unit of the ITS terminal, the CAM/DENM message is transmitted through the gateway of the network layer. The frame structure for V2X communication is shown in the following Fig. 4. This structure has 12 symbols, and the OFDM symbol is assigned a rate (4 bits), a reserved bit (1 bit), length information (12 bits), parity information (1 bit), and a tail (1 bit), service (16 bits) and a PSDU. The OFDM symbol has a variable length. For WAVE transmission, it has RTS/CTS signal. RTS is composed of data transmission time+ACK transmission time+CTStransmission time+3*SIFS (short inter-frame space, 32 usec).

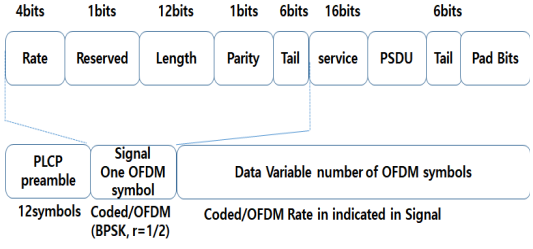

Fig. 4. Structure of V2X frame

In case of CTS signal, the RTS packet is the response signal of the device which receives the RTS packet, and it is calculated as RTS interval value-CTS transmission time-SIFS time value.

4.2 Capacity Evaluation of Security Communication

If the V2X security communication uses 15-bit security synchronization bits, it can be expressed as follows in equation (1).

$$P(Q=n)=\sum_{k=n}^{15}P(S=k)\left(\frac{k}{n}\right)P_d^n(1-P_d)^{k-n} \quad (1)$$

$$\text{Here } P_d^n=\sum_{j=0}^{d}\binom{n}{0}P_t^j(1-P_t)^{n-j}$$

P_d^n is detection probability about d bits out of n bits. it is selected a 15 bit string that matches 12 out of 15 iteration for majority voting process. n is not zero. P_t^j is probability of j-th occurred bit and $(1-P_t)^{n-j}$ is probability of 1-P_t^j of n-j th occurred bit. When security synchronization is detected with a margin of 2 bits, n is 2. The probability P is shown in the following Fig. 5.

Fig. 5 shows probability of synchronization detection in secure communication channel.

In Fig. 5, the probability of P_d^n shows the probability of synchronization detection for a given channel (BER = 0.1, 0.01, 0.001).

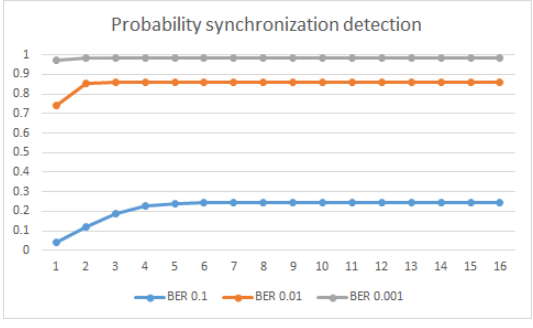

Fig. 5. Probability of synchronization detection

5. Conclusion

In this study, we describes the characteristics of security authentication based on CAM and DENM structure and based on communication frame in V2X vehicle security communication environment. The majority voting structure is applied, and the transmission characteristics of the synchronization pattern of three (31,15) bit structures out of five are simulated.

ACKNOWLEDGMENTS

This research paper is made possible through the project funding of Industry Academia Cooperation Group in Baekseok University.

REFERENCES

[1] M. A. Javed & E. B. Hamida. (2017). On the interrelation of security, QoS, and Safety in Cooperative ITS. *IEEE Transaction on Intelligent Transportation Systems, 18(7),* 1943-1957.
DOI : 10.1109/TITS.2016.2614580

[2] E. Bubenikova, M. Franekova, P. Holecko. (2016). Conceptual design of driving lane-crossing alarm threshold in C-ITS applications and its implementation. *In Cybernetics & Informatics (K&I), 2016* (pp.1-6). USA : IEEE.
DOI : 10.1109/CYBERI.2016.7438598

[3] H. Labiod, A. Servel, G. Seggara, B. Hammi, J. P. Monteuuis. (2016). A new service advertisement message for ETSI ITS environments : CAM-Infrastructure. *NTMS, 2016 8th IFIP International Conference on* (pp. 1-4). USA : IEEE.
DOI : 10.1109/NTMS.2016.7792428

[4] B. Lonc, P. Cincilla. (2016). Cooperative its security framework : Standards and implementations progress in europe. *WoWMoM, 2016 IEEE 17th International Symposium* (pp. 1-6). USA : IEEE.
DOI : 10.1109/WoWMoM.2016.7523576

[5] M. B. Brahim, E. B. Hamida, F. Filali, N. Hamdi. (2015). Performance impact of security on cooperative awareness in dense urban vehicular networks. *WiMob, 2015 IEEE 11th International Conference on* (pp. 268-274). USA : IEEE.
DOI : 10.1109/WiMOB.2015.7347971

[6] A. Paier(2015). The end-to-end intelligent transport

system (its) concept in the context of the european cooperative its corridor. *ICMIM, 2015 IEEE MTT-S International Conference on* (pp. 1-4). USA : IEEE.
DOI : 10.1109/ICMIM.2015.7117948

[7] W. Whyte, J. Petit, V. Kumar, J. Moring, R. Roy. (2015). Threat and Countermeasures Analysis for WAVE Service Advertisement. *ITSC, 2015 IEEE 18th International Conference on* (pp. 1061-1068). USA : IEEE.
DOI : 10.1109/ITSC.2015.176

[8] P. Cincilla & A. Kaiser. (2015). Security of C-ITS messages : A practical solution the ISE project demonstrator. *NTMS, 2015 7th International Conference on* (pp. 1-2). USA : IEEE.
DOI : 10.1109/NTMS.2015.7266520

[9] L. Chen, C. Englund. (2014). Cooperative ITS-EU standards to accelerate cooperative mobility. *In Connected Vehicles and Expo (ICCVE), 2014 International Conference on* (pp. 681-686). USA : IEEE.
DOI : 10.1109/ICCVE.2014.7297636

[10] W. Chen, L. Delgrossi, T. Kosch, T. Saito. (2017). Automotive networking and applications. *IEEE communication magazine, 55(6),* 180-180. USA : IEEE.
DOI : 10.1109/MCOM.2017.7946942

[11] L. Viragg, J. Kovacs, A. Edelmayer. (2013). Extension of the ITS station architecture to low-power pervasive sensor networks. *In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 1386-1391). USA : IEEE.
DOI : 10.1109/WAINA.2013.252

[12] IEEE. D*raft guide for wireless access in vehicular environment (WAVE)-Architecture.* 1-104. USA : IEEE.

[13] M. Wazid, A. K. Das & N. Kumar. (2017). Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *Journal of IEEE Access, 5,* 14966-14980. USA : IEEE.
DOI : 10.1109/ACCESS.2017.2723265

[14] S. Dahmane, C. A. Kerrache, N. Lagraa, P. Lorenz. (2017). WeiSTARS : A weighted trust-aware relay selection scheme for VANET. *In Communications (ICC), 2017 IEEE International Conference on* (pp. 1-6). USA : IEEE.
DOI : 10.1109/ICC.2017.7996451

[15] Y. Zhang, M. Chen, N. Guizani, D. Wu, Victor C. M. Leung. (2017). Sovcan : Safety-oriented vehicular controller area network. *IEEE Communications Magazine, 55(8),* 94-99.
DOI : 10.1109/MCOM.2017.1601185

저 자 소 개

홍 진 근(Jin-Keun Hong) [정회원]

- 1991년 2월 : 경북대학교 전자공학과 공학사
- 2000년 2월 : 경북대학교 전자공학과 정보통신공학 공학박사
- 2004년 3월 ~ 현재 : 백석 대학교 정보통신학부 교수

<관심분야> : 융합보안, 융합교육, 디지털미학