JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항행 및 항법

**J. Adv. Navig. Technol.** 22(5): 391-399, Oct. 2018

# 자율협력주행을 위한 V2X 보안통신의 신뢰성 검증

# Reliability Verification of Secured V2X Communication for Cooperative Automated Driving

**정 한 균[1] · 임 기 택[1] · 신 대 교[1] · 윤 상 훈[1] · 진 성 근[1] · 장 수 현[1] · 곽 재 민[2*]**
[1]전자부품연구원 모빌리티플랫폼 연구센터
[2]목포해양대학교 항해정보시스템학부

**Han-gyun Jung[1] · Ki-taeg Lim[1] · Dae-kyo Shin[1] · Sang-hun Yoon[1] · Seong-keun Jin[1] · Soo-hyun Jang[1] · Jae-min Kwak[2*]**
[1]Mobility Platform Research Center, Korea Electronics Technology Institute, Gyeonggi-do, 13509, Korea
[2]Division of Navigation Information System, Mokpo National Maritime University, Jeollanam-do, 58628, Korea

**[요 약]**

V2X 통신이란 차량이 유무선망을 통해 다른 차량, 인프라, 네트워크, 보행자 등과 같은 객체들과 정보를 교환하는 기술이다. V2X 통신 기술은 최근 꾸준히 연구되어 왔으며 자율주행 차량 기술과 결합된 자율협력주행 기술에 중요한 역할을 수행해왔다. 자율주행 차량은 V2X 통신을 통해 외부 정보를 수신함으로써 차량 센서의 인식범위를 확장시키고 보다 안전하고 자연스런 자율주행을 지원할 수 있다. 이러한 자율협력주행 차량을 공공도로에서 운행하기 위해서는 V2X 보안통신의 신뢰성이 사전에 검증되어야 한다. 본 논문에서는 자율협력주행을 위한 V2X 보안통신에 대한 테스트 시나리오와 테스트 절차를 제안하고 검증 결과를 제시한다.

**[Abstract]**

V2X communication is a technology in which a vehicle exchanges information with various entities such as other vehicles, infrastructure, networks, pedestrians, etc. through a wired or wireless network. Recently, V2X communication technology has been steadily developed and recently it has played an important role in autonomous cooperation driving technology combined with autonomous vehicle technology. Autonomous vehicles can utilize the external information received via V2X communication to extend the recognition range of existing sensors and to support more safe and natural autonomous driving. In order to operate these autonomous cooperative vehicles on public roads, the security and reliability of autonomous V2X communication should be verified in advance. In this paper, we present test scenarios and test procedures of secure V2X communication for cooperative automated driving and present verification results.

**Key word :** Cooperative automated driving, Vehicle to everything, Wireless access in vehicular environments, Security, IEEE1609.2.

**https://doi.org/10.12673/jant.2018.22.5.391**



**Received** 19 September 2018; **Revised** 1 October 2018
**Accepted (Publication)** 24 October 2018 (30 October 2018)

***Corresponding Author; Jae-Min Kwak**

**Tel:** +82-61-240-7268
**E-mail:** kjm@mmu.ac.kr

## Ⅰ. 서 론

최근 V2X (vehicle to everything) 통신 기술을 이용하여 자율주행 차량의 인식범위를 확장함으로써 보다 안전하고 자연스런 자율주행을 가능케 하기 위한 연구 활동이 활발히 진행되었다. 자율협력주행은 개별 차량에 의한 자율주행을 수행하는 것뿐만 아니라 차량 간 또는 차량과 외부의 장치들 간의 정보교환을 통해 보다 높은 완성도의 자율주행을 지원할 수 있게 한다[1].

보안은 이러한 자율협력주행에 있어서 가장 중요한 기술 요소 중에 하나이다. 만일 차량이 통신 중에 교환되는 정보의 신뢰성이 확보되지 않는다면, 그 정보는 자율주행을 수행하는데 사용될 수가 없다. 특히 무선 매체를 통한 통신기술이 사용되는 경우 해킹과 공격에 보다 쉽게 노출되는 경향이 있고, 해커에 의해 악의적으로 조작된 정보가 자율주행에 사용된다면 매우 치명적인 결과로 나타난다[2]. 이러한 중요성으로 최근 V2X 통신에서의 보안에 관한 연구가 다양하게 진행되고 있다[3]-[5].

IEEE 1609.2 WG은 V2X 통신에 적용되는 보안기술에 대한 표준을 수립하였다. 이 표준 기술은 비대칭 보안 알고리즘을 기반으로 하는 개인 키 및 인증서를 사용하여 정보 발신자의 신원과 자격 증명을 확인하고 메시지 변조를 방지하는 기능을 제공한다. 이 기술을 사용하면 인증되지 않은 발신자가 전송 한 정보 또는 변경된 정보를 감지 할 수 있으므로 신뢰할 수 있는 정보만이 자율주행에 사용될 수 있다.

기존의 연구논문들은 주로 V2X 환경에서의 보안 기술인 IEEE 1609.2 또는 PKI (public key infrastructure) 시스템에 대해 소개하거나[6], 이를 효율적으로 사용하거나 보안을 강화하기 위한 기법[7],[8], 그리고 IEEE 1609.2 보안 표준의 구현에 대한 내용을 다루고 있다[9].

기존의 논문에서는 표준을 기반으로 한 V2X 보안기술의 신뢰성에 대한 현장검증 연구결과나 실제 차량 및 도로 상황에서 시스템의 신뢰성을 검증하기 위한 방안을 제시한 연구결과는 찾기 어렵다. 따라서 본 논문에서는 표준을 기반으로 한 V2X 보안통신 기술을 소개하고 자율협력주행을 위한 보안통신을 검증하기 위한 현장 테스트 시나리오 및 절차를 제안하고 보안통신에 대한 신뢰성 테스트 검증 결과를 제시한다.

## Ⅱ. V2X 보안통신

자율협력주행 차량에서의 V2X OBU(on-board unit)는 V2X RSU(road-side unit)로부터 낙하물, 장애물, 정지차량과 같은 돌발상황에 대한 검지정보, 공사정보, 그리고 날씨로 인한 노면상태 정보와 같은 다양한 도로 정보들을 수신하여 자율협력주행 제어용 ECU(electronic control unit)로 전달함으로써 자율협력주행 차량이 전방충돌 방지기능을 수행하도록 한다.

현재, V2X 통신프로토콜은 IEEE에서 정의한 WAVE (wireless access in vehicular environments) 통신기술에 기반하고 있으며, 도로 정보를 전달하는 메시지는 SAE (society of automotive engineers)에서 정의한 DSRC (dedicated short range communication) 메시지 셋을 사용한다. V2X 통신기술과 메시지는 다음의 표준기술들로 구현될 수 있다.

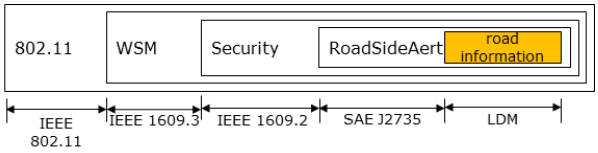



**그림 1.** 도로정보 메시지 형식

**Fig. 1.** Road information message format.

- PHY/MAC layer : IEEE 802.11[10], IEEE 1609.4[11]
- Network layer : IEEE 1609.3[12]
- Security : IEEE 1609.2[13]
- Message set : SAE J2735[14]

본 논문에서는 그림 1과 같이 도로 정보는 LDM (local dynamic map) 형식으로 기술하고, SAE J2735 규격에 정의된 RoadSideAlert[14] 메시지에 수납하여 RSU로부터 차량 내의 V2X OBU로 전달된다. RoadSideAlert 메시지는 보안기능을 지원하기 위해 IEEE 1609.2에 정의된 보안 메시지 내에 수납된 후 WSM (wave short message)에 실려 전송된다.

도로정보는 자율협력주행에 활용되는 정보이므로 정보의 신뢰성이 매우 중요하며, IEEE 1609.2 표준에서는 공개 키와 인증서기반의 보안기술을 통해 정보보안 기능을 제공하도록 하고 있다. 도로 정보가 차량으로 전송될 때에는 다음과 같은 보안조건을 만족시켜야 한다.

- 차량은 인가되지 않은 RSU에 의해 보내진 메시지를 구별해 낼 수 있어야 함
- RSU가 전송한 메시지가 변조된 경우, 차량은 이를 감지할 수 있어야 함

WAVE 통신에서는 메시지 송신 장치의 자격 확인 및 메시지 변조 여부를 감지하기 위해 공개 키 및 인증서 기반의 보안기술을 적용하고 있다. 본 논문에서의 보안 시스템에서는 다음 절차에 따라 보안환경을 구성하고 보안통신을 수행하게 된다.

- 인증서 발행
- 제품 초기화 (개인 키 및 인증서 탑재)
- 보안통신 수행 (도로정보 전송)

### 2-1 인증서 발행

모든 인증서는 인증된 발행 서버인 CA (certificate authority)에서만 발행이 가능하다. 인증서 발행 권한이 있는 CA는 인증된 장치들에게 그림 2와 같이 다음의 인증서를 발행한다.

• CA 인증서 : 자기 자신에 대한 인증서
• RSU 인증서 : 기지국 RSU가 사용하는 인증서
• OBU 인증서 : 차량용 통신모듈 OBU가 사용하는 인증서

CA 인증서는 모든 장치에 저장되며, 각 장치별 인증서를 검증하는데 사용된다. 장치별 인증서는 각 장치에 저장되고, 메시지와 함께 전송되어 수신측에서 메시지 서명을 검증하는데 사용된다.

### 2-2 제품 초기화

CA에 의해 발행된 키와 인증서들은 각각의 장치 내부에 탑재된다. 키 및 인증서 저장 절차는 그림 3과 같은 제품 초기화 단계의 보안 환경에서 인가된 사용자에 의해 수행된다.

• RSU : CA 인증서, RSU 인증서, 개인 키 탑재
• OBU : CA 인증서, OBU 인증서, 개인 키 탑재

### 2-3 보안통신 수행

보안통신을 수행하기 위한 절차를 그림 4에 나타내었다. 보안통신을 수행하기 위해 RSU는 메시지에 대한 서명을 생성하여 인증서와 함께 전송한다. 이를 수신한 OBU는 인증서 검증 및 메시지 서명 검증을 수행하여 성공한 경우에만 정보를 자율협력주행 제어용 ECU로 전달한다.

RSU는 자신의 개인 키를 이용하여 도로정보 메시지에 대한 서명을 생성하고, RSU 인증서, 도로정보, 서명을 메시지에 수납하여 전송한다.

**① 메시지에 대한 서명 생성**
- RoadSideAlert 메시지에 대한 메시지 다이제스트 생성
- 개인 키와 메시지 다이제스트를 서명생성 알고리즘에 입력하여 메시지 서명생성

**② 보안메시지의 구성과 전송**
- RSU 인증서, RoadSideAlert 메시지, 메시지 서명을 포함하는 보안 메시지 생성
- 생성된 보안 메시지를 WSM 패킷에 수납하여 전송

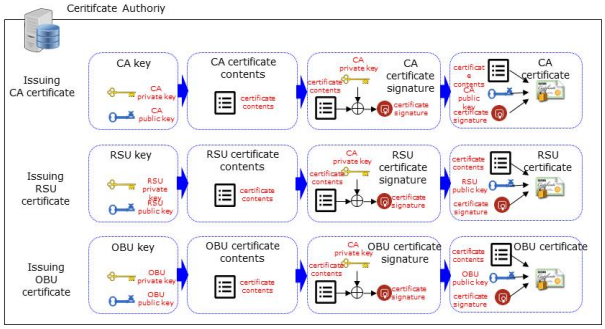



**그림 2.** 인증서 발행
**Fig. 2.** Issuing certificate.

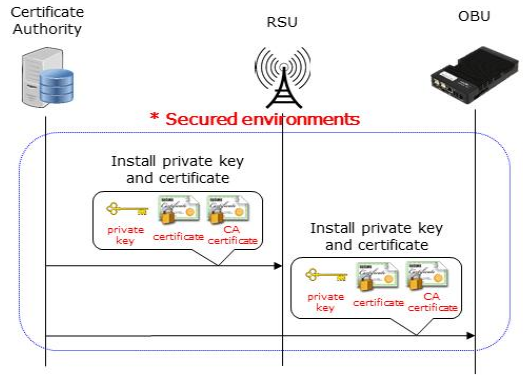



**그림 3.** 제품 초기화 절차
**Fig. 3.** Product initialization process.

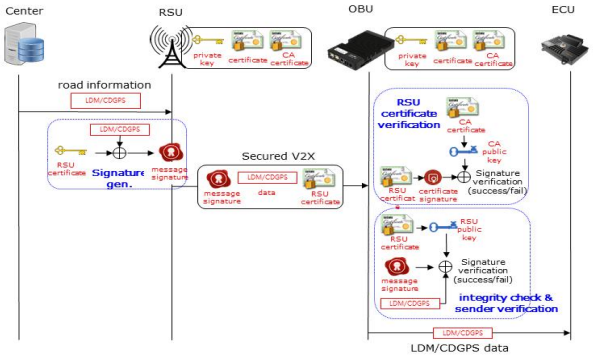



**그림 4.** 보안통신 절차
**Fig. 4.** Secure communication procedure.

자율협력주행 차량용 V2X 통신모듈이 장착된 OBU는 메시지 수신시, 수신된 RSU 인증서를 검증하고 RSU 자격검증 및 메시지 무결성 검증을 수행한다.

**① 보안 패킷 내에 포함된 기지국 인증서의 유효성을 다음 절차에 따라 검증함**
- 기지국 인증서에 포함되어 있는 인증서 서명을 추출
- 기지국 인증서에 대한 인증서 다이제스트를 생성
- 보유하고 있는 CA 인증서에 포함되어 있는 CA 공개 키를 추출
- 인증서 서명, 인증서 다이제스트, CA 공개 키를 서명검증 알고리즘에 입력하여 서명 검증을 수행. 결과가 성공인 경우 수신된 기지국의 인증서는 CA에 의해 정상발급된 인증서임을 확인할 수 있고, 결과가 실패 인 경우 수신된 기지국 인증서는 CA에 의해 정상발급된 인증서가 아니거나, 다른 CA에 의해 발급된 인증서이므로 수신된 패킷은 폐기하고 검증 절차를 종료함

**② 기지국 인증서에 대한 유효성 검사가 성공하면 OBU는 수신된 메시지의 유효성을 검증함**
- 기지국 인증서에 포함되어 있는 기지국 공개 키를 추출
- RoadSideAlert 메시지에 대한 메시지 다이제스트를 생성
- 수신된 메시지서명, 메시지 다이제스트, 기지국 공개 키를

서명검증 알고리즘에 입력하여 서명검증을 수행. 결과가 성공인 경우, 수신된 RoadSideAlert 메시지는 신뢰할 수 있는 장치가 전송하였으며 중간에 변조되지 않았다고 판단할 수 있으므로 해당 메시지는 자율협력주행 제어용 ECU로 전달되고, 결과가 실패인 경우, 수신된 RoadSideAlert 메시지는 신뢰할 수 없는 장치가 전송하였거나 중간에 변조되었다고 판단되어 해당 메시지는 자율협력주행 제어용 ECU로 전달되지 않음

## Ⅲ. V2X 보안통신 테스트 시나리오

자율협력주행 차량은 인가된 V2X RSU가 송신하는 인증된 메시지에 포함된 정보만을 취득하여 차량을 제어하는데 사용한다. 인가 상황 및 비 인가 상황에 대한 보안기능의 동작을 검증하기 위해 표 1에 제시된 바와 같이 5가지 시나리오를 정의하고 시험을 수행하였다.

테스트를 위한 공통시험 환경은 다음과 같이 설정하였다.

- 시험도로에 설치된 RSU에 대한 설정
  - 사전에 공인 CA로부터 발급받은 RSU 개인 키, RSU 인증서, CA 인증서를 내부에 저장
  - 사전에 비공인 CA로부터 발급받은 RSU 개인 키, RSU 인증서, CA 인증서를 내부에 저장
  - 공인 CA가 타 RSU에 대해 발급한 RSU 인증서를 내부에 저장
  - 도로정보를 서명 메시지 형태로 송신할 수 있는 상태로 설정

- 자율협력주행 차량의 OBU를 다음의 상태로 설정
  - 사전에 공인 CA로부터 발급받은 OBU 개인 키, OBU 인증서, CA 인증서를 내부에 저장
  - 서명 메시지를 수신할 수 있는 상태로 설정

- 자율협력주행 차량을 RSU의 통신범위 밖의 주행 시점에 위치시킴
  - V2X RSU의 통신범위는 통상 기지국 설치 지점을 기준으로 반경 500m에서 1km 이내임. 차량의 가속 및 감속을 고려하여 통신범위로부터 500m, 즉 RSU 설치지점으로부터 1.5km 이격된 지점을 주행 시작지점으로 설정함.

- 도로정보 생성 서버(시험도로 운영센터 내 위치)는 사전에 협의된 시험도로 상 장애물의 위치를 포함한 도로정보를 생성함.

### 3-1 정상동작 상황에서의 테스트 시나리오

본 시나리오에서는, 자율협력주행 차량용 OBU가 정상적으로 서명된 도로정보를 수신할 때, 해당 정보를 자율협력주행 제어용 ECU로 전달하는 것을 검증한다.

**표 1.** 테스트 시나리오
**Table 1.** Test scenarios.

| Scenario | Description |
|---|---|
| Normal operation | The OBU forwards the information to the ECU for autonomous cooperation driving when receiving the road information normally signed by the authorized RSU |
| Unsecured message (Unauthorized situation) | The OBU does not forward the information to the ECU for autonomous cooperation driving when receiving unsigned road information. |
| Unauthorized CA (Unauthorized situation) | The OBU does not forward the information to the ECU for autonomous cooperation driving when receiving road information from a RSU having a certificate issued by a CA other than authorized CA. |
| Unauthorized RSU (Unauthorized situation) | The OBU does not forward the information to the ECU for autonomous cooperation driving when receiving road information from the RSU which uses the certificate of the other device. |
| Message tampering (Unauthorized situation) | The OBU does not forward the information to the ECU for autonomous cooperation driving when receiving the altered road information. |

**표 2.** 정상동작시의 테스트 시나리오
**Table 2.** Test scenario for normal operation.

| Test procedure | |
|---|---|
| Step | Description |
| 1 | The vehicle is located at the start point of driving (1.5 km far from the RSU). |
| 2 | The RSU receives the road information from the center and starts to transmit.<br>When the road information is transmitted, the message is signed with the RSU private key issued by authroized CA. |
| 3 | The driver of vehicle accelerates the vehicle toward the RSU.<br>The OBU starts to save logs related to V2X communication and security processing. |
| 4 | Confirmed that vehicle decelerates when approaching the obstacle position. |
| 5 | Check the log of the OBU to confirm the processing status of communication security. Confirm that the log contains the following contents.<br>- Logs that can confirm message reception from RSU.<br>- Logs to verify successful security verification of received messages<br>- Logs which can confirm that the received road situation information has been forwarded to ECU. |

### 3-2 비 보안 메시지에 대한 테스트 시나리오

본 시나리오에서는 자율협력주행 차량용 OBU가 서명되지 않은 도로정보 수신시, 해당 정보를 자율협력주행 제어용 ECU로 전달하지 않는 것을 검증한다.

### 3-3 비 인가 CA에 대한 테스트 시나리오

본 시나리오에서는 자율협력주행 차량용 OBU가 공인 CA가 아닌 비공인 CA가 발행한 인증서를 보유한 RSU로부터 도로정보 수신시, 해당 정보를 자율협력주행 제어용 ECU로 전달하지 않는 것을 검증한다.

**표 3.** 비 보안 메시지에 대한 테스트 시나리오
**Table 3.** Test scenario for unsecured message.

| Test procedure | |
|---|---|
| Step | Description |
| 1 | The vehicle is located at the start point of driving (1.5 km far from the RSU). |
| 2 | The RSU receives the road information from the center and starts to transmit.<br>When the road information is transmitted, it is transmitted in an unsigned form. |
| 3 | The driver of vehicle accelerates the vehicle toward the RSU.<br>The OBU starts to save logs related to V2X communication and security processing. |
| 4 | Confirmed that the vehicle does not decelerate when approaching obstacle position. |
| 5 | Check the log of the OBU to confirm the processing status of communication security. Confirm that the log contains the following contents.<br>- Logs that can confirm message reception from RSU.<br>- Logs that check whether the received message is a unsecure message.<br>- Logs that confirm that the received road situation information has not been forwarded to ECU. |

**표 4.** 비 인가 CA에 대한 테스트 시나리오
**Table 4.** Test scenario for unauthorized CA.

| Test procedure | |
|---|---|
| Step | Description |
| 1 | The vehicle is located at the start point of driving (1.5 km far from the RSU). |
| 2 | The RSU receives the road information from the center and starts to transmit.<br>When the road information is transmitted, it is transmitted with the certificate after signing the message with the private key issued by the other CA other than authorized CA |
| 3 | The driver of vehicle accelerates the vehicle toward the RSU.<br>The OBU starts to save logs related to V2X communication and security processing. |
| 4 | Confirmed that the vehicle does not decelerate when approaching obstacle position. |
| 5 | Check the log of the OBU to confirm the processing status of communication security. Confirm that the log contains the following contents.<br>- Logs that can confirm message reception from RSU.<br>- Logs that verifies if OBU does not have a CA certificate that can validate received messages and certificates.<br>- Logs that confirm that the received road situation information has not been forwarded to ECU. |

### 3-4 비 인가 RSU에 대한 테스트 시나리오

본 시나리오에서는 자율협력주행 차량용 OBU가 타 장치의 인증서를 복제하여 사용하는 RSU로부터의 도로정보 수신 시, 해당 정보를 자율협력주행 제어용 ECU로 전달하지 않는 것을 검증한다.

**표 5.** 비 인가 RSU에 대한 테스트 시나리오
**Table 5.** Test scenario for unauthorized RSU.

| Test procedure | |
|---|---|
| Step | Description |
| 1 | The vehicle is located at the start point of driving (1.5 km far from the RSU). |
| 2 | The RSU receives the road information from the center and starts to transmit.<br>When the road information is transmitted, the message is signed with the private key generated by the authorized CA and is transmitted with the certificate issued to the other RSU. |
| 3 | The driver of vehicle accelerates the vehicle toward the RSU.<br>The OBU starts to save logs related to V2X communication and security processing. |
| 4 | Confirmed that the vehicle does not decelerate when approaching obstacle position. |
| 5 | Check the log of the OBU to confirm the processing status of communication security. Confirm that the log contains the following contents.<br>Logs that can confirm message reception from RSU.<br>Logs that verifies that signature verification for a received message has failed.<br>Logs that confirm that the received road situation information has not been forwarded to ECU. |

**표 6.** 메시지 변조에 대한 테스트 시나리오
**Table 6.** Test scenario for message tampering.

| Test procedure | |
|---|---|
| Step | Description |
| 1 | The vehicle is located at the start point of driving (1.5 km far from the RSU). |
| 2 | The RSU receives the road information from the center and starts to transmit.<br>When the road information is transmitted, the road information data is arbitrarily changed after the message is normally signed. |
| 3 | The driver of vehicle accelerates the vehicle toward the RSU.<br>The OBU starts to save logs related to V2X communication and security processing. |
| 4 | Confirmed that the vehicle does not decelerate when approaching obstacle position. |
| 5 | Check the log of the OBU to confirm the processing status of communication security. Confirm that the log contains the following contents.<br>Logs that can confirm message reception from RSU.<br>Logs that verifies that signature verification for a received message has failed.<br>Logs that confirm that the received road situation information has not been forwarded to ECU. |

### 3-5 메시지 변조에 대한 테스트 시나리오

본 시나리오에서는 자율협력주행 차량용 OBU가 변조된 도로정보를 수신시, 해당정보를 자율협력주행 제어용 ECU로 전달하지 않는 것을 검증한다.

## Ⅳ. 시험도로에서의 V2X 보안통신 시험 및 결과

제안한 테스트 시나리오를 기반으로 각각의 상황에서 수행되어야 하는 예상 동작들이 잘 수행되는 지를 검증하기 위해, 여주 시험도로에서 각 시나리오별 테스트를 수행하고 그 결과를 제시한다.

테스트를 수행하기 위해 자율협력주행 차량 OBU에 사전에 공인 CA에서 해당 OBU를 대상으로 발급한 개인 키, 인증서, CA 인증서를 탑재시키고, 시험도로에 설치된 V2X RSU에서 임의의 도로정보를 포함한 메시지를 약 1초 주기로 반복 송신하였다. 자율협력주행 차량은 V2X RSU의 통신범위를 왕복 주행하면서 V2X OBU의 통신 및 보안 로그를 저장하여 확인하였다.

### 4-1 정상동작 상황에서의 테스트 결과

시험도로 상의 V2X RSU에 사전에 공인 CA에서 해당 RSU를 대상으로 발급한 개인 키와 인증서를 탑재하고, 해당 개인 키로 서명된 도로정보를 인증서와 함께 주기적으로 송신하였고 이를 그림 5와 같이 확인할 수 있다. 차량을 V2X RSU 통신범위 내에서 왕복주행하면서 V2X OBU에 저장되는 로그를 확인한 결과, 그림 6과 같이 V2X OBU가 RSU로부터 수신된 도로정보를 검증하고 자율협력주행 제어용 ECU로 전달함을 확인하였다.

### 4-2 비 보안 메시지에 대한 테스트 결과

비 보안 메시지에 대해 테스트를 위해 시험도로 상의 V2X 기지국인 RSU는 서명되지 않은 도로 정보를 주기적으로 송신하게 하고 그림 7과 같이 확인하였다. 차량은 V2X 기지국인 RSU의 통신범위 내에서 왕복주행하며 V2X OBU에 저장되는 로그를 확인하였다. 그림 8과 같이 로그를 통해 V2X OBU가 RSU로부터 수신된 도로 정보를 검증하고 자율협력주행 제어용 ECU로 전달하지 않는 것을 확인하였다. 즉, 서명되지 않은 비 보안 메시지가 ECU로 전달되지 않는 다는 것이 검증되었다.

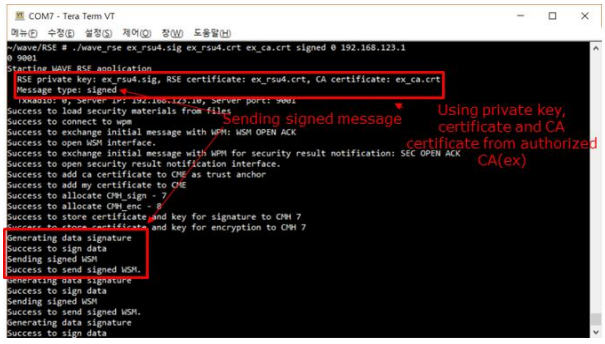



**그림 5.** 정상동작 상황에 대한 테스트 결과 1(RSU측 화면)
**Fig. 5.** Test result for normal operation 1(display at RSU).

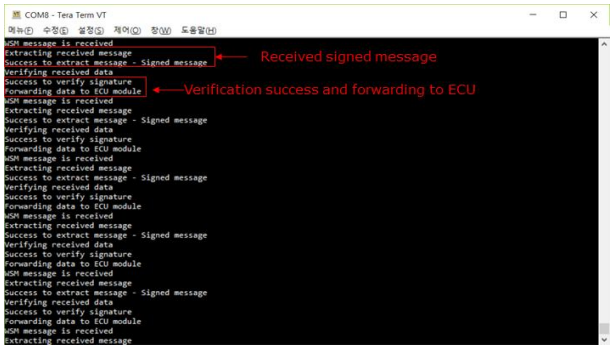



**그림 6.** 정상동작 상황에 대한 테스트 결과 2(OBU측 화면)
**Fig. 6.** Test result for normal operation 2(display at OBU).

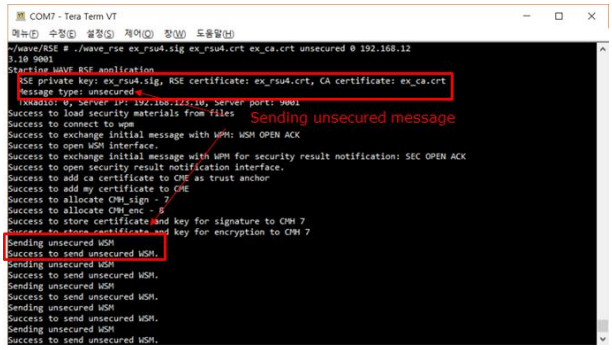



**그림 7.** 비 보안 메시지에 대한 테스트 결과 1(RSU측 화면)
**Fig. 7.** Test result for unsecured message 1(display at RSU).

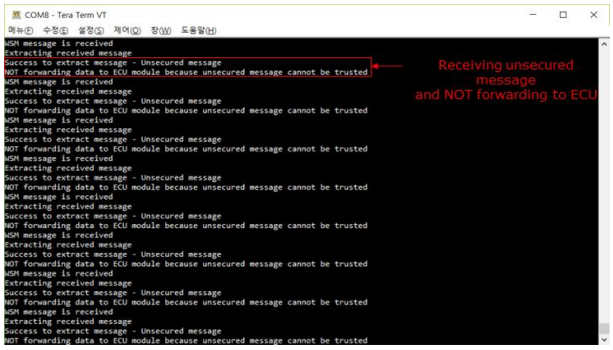



**그림 8.** 비 보안 메시지에 대한 테스트 결과 2(OBU측 화면)
**Fig. 8.** Test result for unsecured message 2(display at OBU).

### 4-3 비 인가 CA에 대한 테스트 결과

시험도로 상의 V2X RSU에 공인 CA가 아닌 비공인 CA에서 발행한 개인 키와 인증서를 탑재하고, 해당 개인 키로 서명된 도로정보를 인증서와 함께 주기적으로 송신하고 그림 9와 같이 확인하였다. 차량이 V2X RSU 통신범위 내에서 왕복주행하면서 V2X 통신모듈이 탑재된 OBU에서 RSU로부터 수신된 도로정보를 검증하고 자율협력주행 제어용 ECU로 전달하지 않는 것을 그림 10과 같이 확인하였다. 즉, 공인되지 않은 CA가 발행한 인증서의 경우 RSU에서 전달된 도로정보가 ECU로 전달되지 않는 다는 것이 검증되었다.

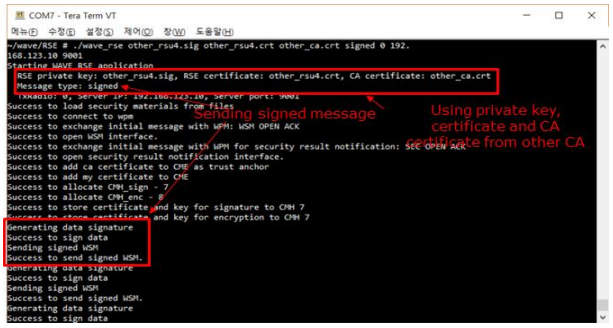



**그림 9.** 비 인가 CA에 대한 테스트 결과 1(RSU측 화면)

**Fig. 9.** Test result for unauthorized CA 1(display at RSU).

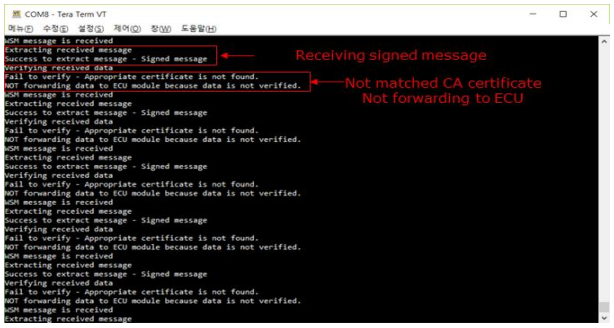



**그림 10.** 비 인가 CA에 대한 테스트 결과 2(OBU측 화면)

**Fig. 10.** Test result for unauthorized CA 2(display at OBU).

### 4-4 비 인가 RSU에 대한 테스트 결과

비 인가 RSU에 대한 테스트를 위해 시험도로 상의 V2X RSU에 공인 CA가 다른 RSU를 대상으로 발행한 인증서를 사전에 탑재시키고, 실제 기지국의 개인 키로 서명된 도로정보를 인증서와 함께 주기적으로 송신하여 그림 11과 같이 확인하였다. 차량을 V2X 기지국인 RSU의 통신범위 내에서 왕복주행하면서 V2X OBU에 저장되는 로그를 확인하였다. 그림 12와 같이 로그를 통해 V2X OBU가 기지국으로부터 수신된 도로정보를 검증하고 자율협력주행 제어용 ECU로 전달하지 않는 것을 확인하였다. 즉, 타 장치의 인증서를 복제하여 사용하는 RSU로부터의 도로정보를 ECU로 전달하지 않는 것을 검증하였다.

### 4-5 메시지 변조에 대한 테스트 결과

메시지 변조에 대한 테스트를 위해 시험도로 상의 V2X RSU에 사전에 공인 CA에서 해당 기지국을 대상으로 발급한 개인키와 인증서를 탑재하고, 해당 개인 키로 서명 생성 후 도로 정보를 임의로 변조하여 인증서와 함께 주기적으로 송신하고 그림 13과 같이 확인하였다. 차량을 V2X RSU 통신범위 내에서 왕복주행하면서 V2X OBU의 통신모듈에 저장되는 로그를 확인하였다. 그림 14와 같이 로그를 통해 V2X OBU가 RSU로부터 수신된 도로정보를 검증하고 자율협력주행 제어용 ECU로 전달하지 않는 것을 확인하였다. 즉 메시지가 변조된 도로정보 수신시 ECU로 전달되지 않음을 검증하였다.

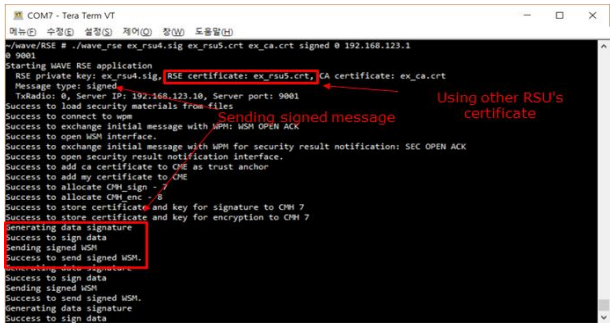



**그림 11.** 비 인가 기지국에 대한 테스트 결과 1(RSU측 화면)

**Fig. 11.** Test result for unauthorized RSU 1(display at RSU).

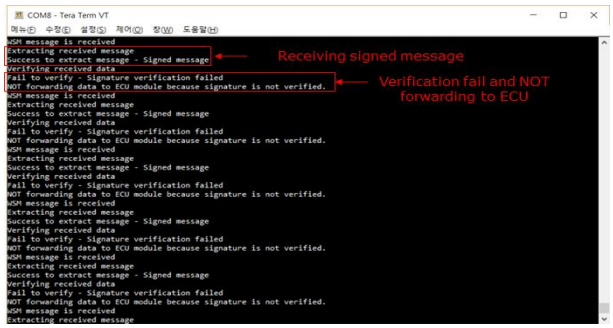



**그림 12.** 비 인가 기지국에 대한 테스트 결과 2(OBU측 화면)

**Fig. 12.** Test result for unauthorized RSU 2(display at OBU).

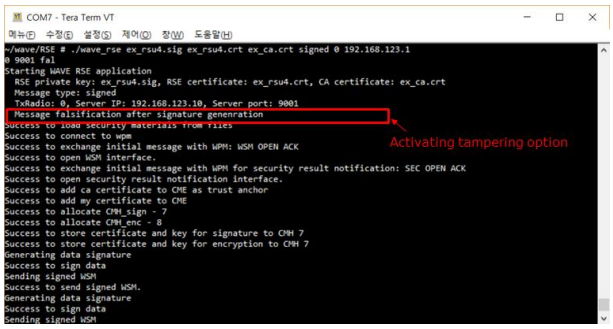



**그림 13.** 메시지 변조에 대한 테스트 결과 1(RSU측 화면)

**Fig. 13.** Test result for message tampering 1(display at RSU).

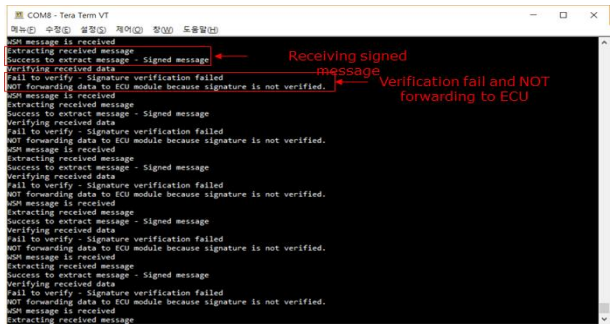



**그림 14.** 메시지 변조에 대한 테스트 결과 2(OBU측 화면)

**Fig. 14.** Test result for message tampering 2(display at OBU).

## Ⅳ. 결 론

본 논문에서는 자율협력주행 차량에 적용되는 V2X 보안통신의 신뢰성을 검증하기 위한 절차와 테스트 시나리오를 제안하고 테스트 결과를 제시하였다. 국내의 자율협력주행에 적용하기 위한 V2X 통신기술은 현재 미국에서 정의한 IEEE 1609.2 보안표준과 비대칭 키 기반의 인증서 보안 시스템을 따르고 있다. V2X 통신의 보안 신뢰성을 검증하기 위해서 1가지의 정상상황과 4가지의 비정상상황에 대한 테스트 시나리오를 설정하였다. 또한 각각의 상황에서 수행되어야 하는 예상 동작들이 잘 수행되는 지를 검증하는 절차를 수립하여 테스트 해본 결과 원활한 보안통신이 이루어질 수 있도록 정상 동작함을 확인하였다.

제안한 자율협력주행 차량의 보안통신 검증 시나리오 절차와 테스트 결과를 활용하여 향후 자율협력주행 차량의 실 도로 운영환경에서 V2X 보안통신이 이루어질 수 있도록 실증 연구가 추가로 진행될 필요가 있다.

## Acknowledgement

본 연구는 국토교통부 교통물류연구개발사업의 연구비지원(18TLRP-B101406-04)에 의해 수행되었습니다.

## References

[1] K. T. Lim, “Vehicle communication system technology evaluation and management service,” *KEIT PD Issue Report*, Aug. 2016.

[2] H. L. Vinh and A. R. Cavalli, “Security attacks and solutions in vehicular ad hoc networks: a survey,” *International journal on AdHoc networking systems (IJANS)*, Vol. 4, No. 2, pp. 1−20, April 2014.

[3] K. Bian, G. Zhang, and L. Song, “Security in use cases of vehicle-to-everything communications,” *IEEE 86th Vehicular Technology Conference*, Toronto, Canada, pp, 1-5, Sept. 2017.

[4] P. Knapik, E. Schoch, and F. Kargl, “Electronic decal: a security function based on V2X communication,” *IEEE 77th Vehicular Technology Conference*, Toronto, Canada, pp. 1-5, June 2013.

[5] J. Khan, “Vehicle network security testing,” *Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, Chennai, India, pp. 119-123, May 2017.

[6] J. B. Kenney, “Dedicated short-range communications (DSRC) standards in the United States,” *Proceedings of the IEEE*, Vol. 99, Issue 7, pp. 1162 − 1182, June 2011.

[7] M. Khodaei, H. G. Jin, and P. Papadimitratos, “SECMACE: scalable and robust identity and credential management infrastructure in vehicular communication systems,” *IEEE Transactions on Intelligent Transportation Systems*, Vol. 19, Issue 5, pp. 1430 − 1444, May 2018.

[8] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, “Group-based authentication in V2V communications,” *Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, Beirut, Lebanon, pp. 173 - 177, May 2015.

[9] C. B. Jeong and Y. M. Kim, “Implementation of efficient SHA-256 hash algorithm for secure vehicle communication using FPGA,” *International SoC Design Conference (ISOCC)*, Jeju, South Korea, pp. 224 − 225, Nov. 2014.

[10] IEEE Computer Society, IEEE Standard for Information Technology - Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications, 2012.

[11] IEEE Vehicular Technology Society, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation, IEEE 1609.4, 2016.

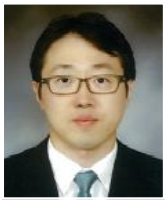
[12] IEEE Vehicular Technology Society, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, IEEE 1609.3, 2016.

[13] IEEE Vehicular Technology Society, IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE 1609.2, 2016.

[14] SAE J2735, Dedicated Short Range Communication (DSRC) Message Set Dictionary, 2016.

**정 한 균** (Han-gyun Jung)
2007년 2월 : 한국항공대학교 대학원 정보통신공학과 (공학석사)
2013년 : 한국항공대학교 대학원 정보통신공학과(공학박사수료)
2008년 4월 ~현재 : 전자부품연구원 모빌리티플랫폼연구센터 선임 연구원
※관심분야 : V2X 통신기술, 스마트카 전장시스템

**신 대 교** (Dae-kyo Shin)
2000년 7월 : 아주대학교 대학원 전자공학전공 (공학석사)
2010년 : 고려대학교 대학원 전자전기공학전공 (공학박사수료)
2000년 8월~2003년 11월 : eMDT 주임연구원
2003년 12월~현재 : 전자부품연구원 모빌리티플랫폼연구센터 책임연구원
※관심분야 : V2X 통신기술, 스마트카 전장시스템



**윤 상 훈** (Sang-hun Yoon)
1998년 : 한양대학교 대학원 전자공학전공 (공학석사)
2008년 : 한양대학교 대학원 전자공학전공 (공학박사)
2012년 7월~현재 : 전자부품연구원 모빌리티플랫폼연구센터 선임연구원
※관심분야 : V2X 통신기술, 스마트카 전장시스템

**진 성 근** (Seong-keun Jin)
2008년 2월 : 한국외국어대학교 컴퓨터공학과 (공학사)
2010년 2월 : 한양대학교 대학원 전자컴퓨터통신공학과 (공학석사)
2009년 12월~현재 : 전자부품연구원 모빌리티플랫폼연구센터 선임연구원
※관심분야 : V2X 통신기술, SoC, Embedded System

**장 수 현** (Soo-hyun Jang)
2011년 2월 : 한국항공대학교 대학원 전자공학전공 (공학석사)
2015년 8월 : 한국항공대학교 대학원 전자공학전공 (공학박사)
2015년 9월~현재 : 전자부품연구원 모빌리티플랫폼연구센터 선임연구원
※관심분야 : V2X 통신기술, SoC, Embedded System

**임 기 택** (Ki-taeg Lim)
1996년 2월 : 한양대학교 대학원 전자공학과 (공학석사)
2013년 2월 : 한양대학교 대학원 전자컴퓨터공학과 (공학박사수료)
1996년 3월~현재 : 전자부품연구원 모빌리티플랫폼연구센터 센터장
※관심분야 : V2X 통신기술, 스마트카 전장시스템

**곽 재 민** (Jae-min Kwak)
1999년 8월 : 한국항공대학교 대학원 통신정보공학과 (공학석사)
2002년 8월 : 한국항공대학교 대학원 통신정보공학과 (공학박사)
2002년 7월~2003년 7월 : 한국전자통신연구원 네트워크 연구소 (Post-doc.)
2003년 7월~2008년 2월 : 전자부품연구원 SoC 연구센터 책임연구원
2008년 3월~현재 : 목포해양대학교 항해정보시스템학부 부교수
※관심분야 : 디지털 통신 시스템, 유무선 통신신호처리