ETRI

2018
Electronics and
Telecommunications
Trends

4차 산업혁명 사회의 초연결 지능과 신뢰 인터넷 기술 특집

자율주행 자동차 보안기술 동향

Security Trends for Autonomous Driving Vehicle

권혁찬 (H.C. Kwon, hckwon@etri.re.kr) 시스템보안연구그룹 책임연구원/PL
이석준 (S.J. Lee, junny@etri.re.kr) 시스템보안연구그룹 책임연구원
최중용 (J.Y. Choi, choijy725@etri.re.kr) 시스템보안연구그룹 선임기술원
정병호 (B.H. Chung, cbh@etri.re.kr) 시스템보안연구그룹 책임연구원
이상우 (S.W. Lee, ttomlee@etri.re.kr) 시스템보안연구그룹 책임연구원
나중찬 (J.C. Nah, njc@etri.re.kr) 시스템보안연구그룹 책임연구원/그룹장

As the traffic environment gradually changes to autonomous driving and intelligent transport systems, vehicles are becoming increasingly complicated and intelligent, and their connectivity is greatly expandinged. As a result, attack vectors of such vehicles increasing, and security threats further expanding. Currently, various solutions for vehicle security are being developed and applied, but the damage caused by cyber attacks is still increasing. In recent years, vehicles such as the Tesla Model S and Mitsubishi Outlander have been hacked and remotely controlled by an attacker. Therefore, there is a need for advanced security technologies to cope with increasingly intelligent and sophisticated automotive cyber attacks. In this article, we introduce the latest trends of autonomous vehicles and their security threats, as well as the current status and issues of security technologies to cope with them.

* DOI: 10.22648/ETRI.2018.J.330108

* 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No. B0717-16-0097, 자율주행차량을 위한 V2X 서비스 통합 보안 기술 개발].

Ⅰ. 서론

자동차, 교통 환경이 점차 자율주행, 지능형 교통시스템으로 발전하면서, 자동차는 점점 복잡화, 지능화되고 도로/교통 인프라와 자동차 간의 연결성도 대폭 확대되고 있다. 현재 센서와 소프트웨어에 의한 자율형 주행 서비스는 점차 차량 간 및 차량과 인프라 간 연동/협력을 통한 협력 자율주행 환경으로 진화가 예측된다. 실제 국내의 C-ITS 사업, 미국 미시간주의 M-City, 유럽의 ITS Corridor 프로젝트의 경우 IEEE 802.11p 및 1609.x 국제 표준규격의 차량 간 통신 기능을 포함하여 협력 자율주행에 대한 실증이 진행되고 있다.

이러한 자동차의 지능화 및 연결성 확대는 다양하고 보다 정밀한 자율주행 서비스가 가능한 면이 있지만, 사이버 공격을 위한 벡터가 증가하여 보안 위협 역시 확대되는 문제가 있다. 최근의 사례로, 2014년에 찰리밀러와 발라섹은 지프 체로키를 해킹 후 원격 조정하여 시속 100km로 주행 중인 지프 체로키 차량을 급정거시키고, 핸들을 임의로 조작하여 차량을 배수로로 곤두박질시키기도 하였다. 2016년에 펜테스트파트너스社는 미쓰비시 아웃랜더 차량의 와이파이 접속구간을 해킹하여 원격에서 차량의 잠금을 해제하고 헤드라이트, 공조장치 등을 임의로 제어한 사례도 있다. 같은 해인 2016년에 중국 텐센트의 보안자회사 킨시큐리티랩은 테슬라의 웹 브라우저의 무선 접속과정에서 해킹에 성공하여 14마일 떨어진 곳에서 주행 중인 차량의 브레이크를 조작하여 급정거시킨 사례도 있다. 테슬라는 이러한 공격에 대해 바로 보안패치를 하였으나, 다음 해인 2017년 킨시큐리티랩은 패치된 시스템의 보안망을 뚫고 다시 해킹에 성공하여 Escar Europe 2017 등에서 발표하기도 하였다.

자동차 보안을 위한 다양한 보안 솔루션들이 개발·적용되고 있으나 지속해서 피해 사례가 보고 되는 등 점점 지능화되고 고도화되는 자동차 사이버 공격에 대한 대응책이 필요한 상황이며, 자율주행 新산업의 안착을 위해서도 자동차 보안성의 조기 확보는 필수적인 상황이다.

본고에서는 자율주행 자동차의 최신 동향과 그에 따른 보안 위협 요소들을 살펴보고, 이에 대응하기 위한 보안기술 현황 및 전망을 살펴보고자 한다.

Ⅱ. 자율주행 자동차 동향

자율주행 수준을 미국자동차공학회(SAE: Society of Automotive Engineers)는 1~5단계로 미국도로교통안전국(NHTSA: National Highway Traffic Safety Administration)은 1~4단계로 정의한다. 〈표 1〉은 SAE에서 정의한 자율 주행 단계를 소개한다. NHTSA의 4단계는 SAE의 4~5단계에 해당한다.

현재, 테슬라 등 상용 자율주행 자동차의 수준은 2~3단계 정도이다. 현재 차량에 장착된 카메라, 레이더, 라이더 등의 센서와 자율주행 소프트웨어에 의해 구동되는 자율형 주행(Autonomous driving)은 점차 차량과 차량 및 도로 인프라와의 협력을 통한 협력형 주행(Cooperative driving) 형태로 발전할 것으로 예측된다. SAE의 3단계 이상의 자율주행이 현실화되기 위해서는 자율형 주행과 협력형 주행이 합쳐진 협력 자율주행 형

〈표 1〉 자율 주행 단계(SAE)

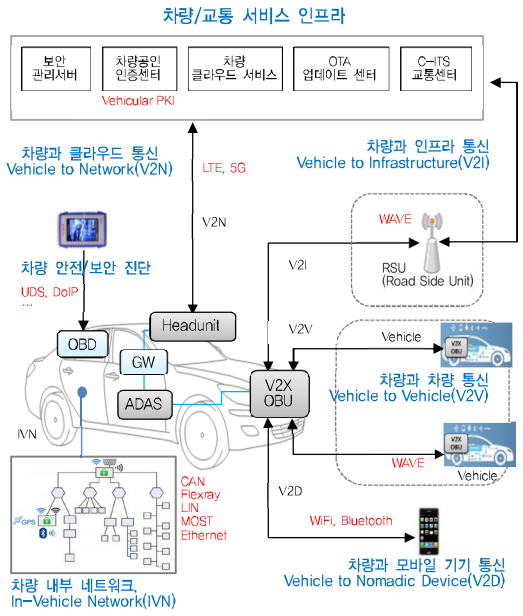
단계	기능	설명
1	단일 주행 보조기능	- 단일 기능의 운전자 보조 시스템 활용 - 크루즈 컨트롤, 차선유지 등 - 운전자가 직접 운전
2	복수 주행 기능 융합 보조	- 2개 이상의 주행기능이 융합 보조 - 차선유지, 적응형 크루즈 컨트롤 등 - 운전자는 주행상황 항상 주시
3	제한된 자율주행	- 특정 도로 조건에서 제한된 자율주행 - 고속도로 자율 주행 등 - 운전자는 위급상황시 개입
4	완전 자율주행	- 모든 도로 조건에서 자동 제어 - 운전자 탑승
5	무인 완전 자율주행	- 모든 도로 조건에서 자동 제어 - 무인 운전

태가 되어야 한다는 시각도 많다. 자율주행을 위한 자동차 기술의 최근 트랜드는 크게 연결성 확대 및 자동차 내부 네트워크의 효율화 측면으로 정의할 수 있다.

1. 연결성의 확대

(그림 1)은 자율주행 자동차의 다양한 연결성을 보여준다. 자동차의 연결성을 분류하면 차량과 차량 간 통신(V2V: Vehicle-to-Vehicle), 차량과 인프라 간 통신(V2I: Vehicle-to-Infrastructure), 차량과 디바이스 간 통신(V2D: Vehicle-to-Device), 차량과 네트워크(클라우드 등)와의 통신(V2N: Vehicle-to-Network)으로 구분할 수 있으며, 그 외에 차량 안전/보안 진단을 위한 연결성 및 다양한 차량 내부의 네트워크 간 통신 등이 존재한다[1].

차량과 차량 및 차량과 인프라 간 통신을 위해 WAVE 프로토콜 기반의 V2X(Vehicle-to-Everything) 기술에 대한 기술 개발 및 실증이 각국에서 활발히 이루어지고 있다. WAVE 통신 기술은 IEEE 802.11a/g 무선 통신기술을 차량 주행환경에 최적화한 기술로 차량과 차량 간



(그림 1) 자동차의 연결성

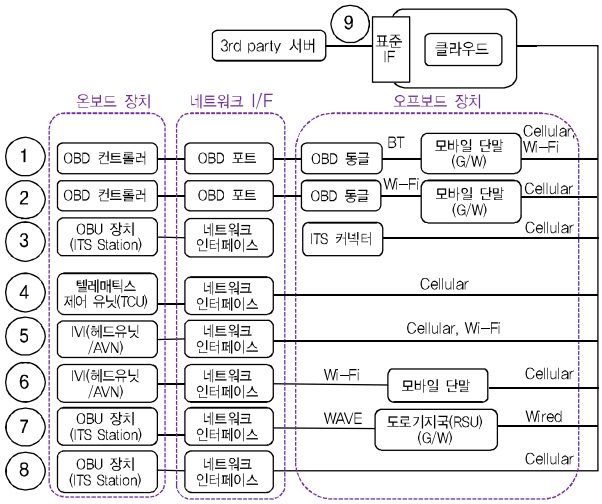
(V2V), 차량과 인프라 간(V2I) 통신에 이용된다. WAVE 통신은 100ms 이내로 지연시간을 최소화하고, 160km 이상의 고속이동성을 지원하며, ITS(지능형 교통시스템) 전용 주파수 대역을 사용하는 등 차량 간 통신환경에 최적화된 기술이다. 또한, 기지국이 필요하지 않은 D2D(Device-to-Device) 통신 방식을 이용하기 때문에 별도의 인프라 구축이나 통신망 사용료 등이 발생하지 않는 장점도 있다.

관련 표준은 IEEE에서 개발하였으며, 물리와 MAC 계층을 정의한 802.11p, 보안 규격을 정의한 1609.2, 네트워크 및 전송 계층 서비스 규격을 정의한 1609.3, MAC 계층의 멀티채널 오퍼레이션을 정의한 1609.4, WAVE 서비스를 위한 ID 할당 규격인 1609.12 등이 있다. 또한, 차량 간 통신에 사용되는 메시지 집합은 SAE의 J2735에 정의되어 있으며, 메시지 전송에 대한 성능 요구사항은 SAE의 J2945에 정의되어 있다. 최근에는 3GPP에서 LTE 규격(release 14)에 차량 간 V2X 통신 기능을 추가하여 확장하였다[2]. 차량 간 통신 환경에 맞게 LTE direct, LTE broadcast 등의 규격을 포함하고 ITS 전용 주파수대를 지원하여 이동통신 기반의 V2V, V2I, V2N 통신 서비스 적용이 가능하게 되었다.

스마트 폰 등을 통한 다양한 부가서비스를 제공하기 위한 V2D 통신도 활성화되어 있다. V2D를 통해 멀티미디어 서비스, 텔레매틱스, 미러링 등의 서비스가 가능하다. 대표적인 미러링 서비스로 애플의 카플레이, 구글의 안드로이드 오토, CCC(Car Connectivity Consortium)의 미러링크 등이 있다.

차량 안전/보안 진단을 위한 표준으로는 ISO 14229-1~4에서 정의된 UDS(Unified Diagnostics Service)와 인터넷 프로토콜을 통한 진단 표준인 DoIP(Diagnostics over IP) 등이 있다.

또한, 최근에는 차량과 클라우드 간(V2N) 연계 서비스도 크게 증가하고 있으며, 차량과 클라우드 간 통신 및 데이터 공유를 위한 다양한 표준이 개발되고 있다.



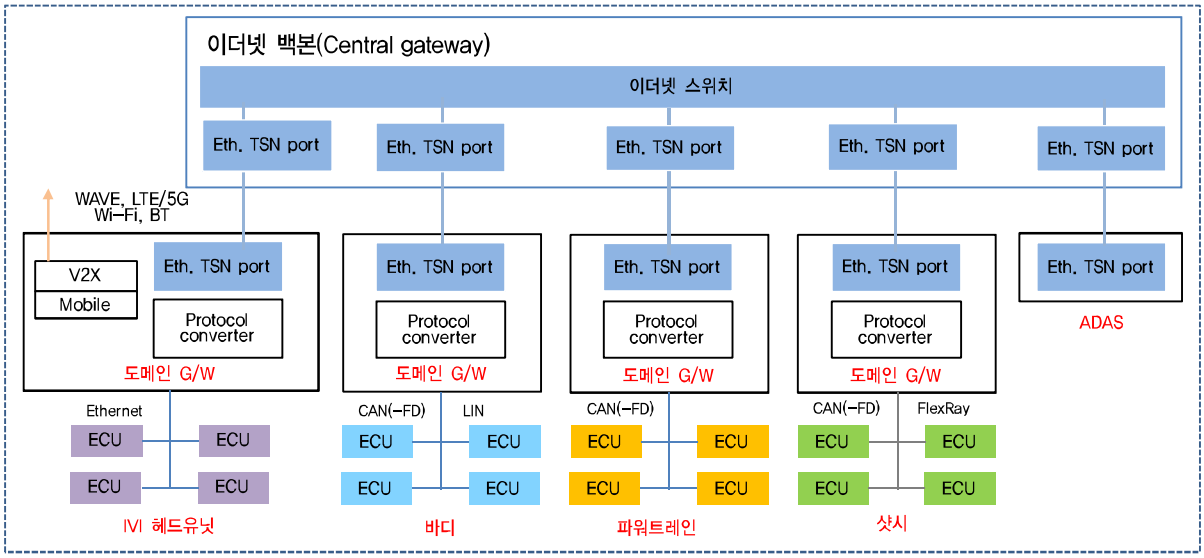
(그림 2) 자동차 데이터의 클라우드 전송 방식[4]

[출처] 권혁찬, "클라우드 커넥티드 자동차 보안 요구사항," 사물 인터넷 포럼 표준(IoTFS-0139), 2017. 12.

현재는 클라우드 기반으로 차량 진단, 부품관리, 이상 징후/위협 탐지, OTA 등을 위한 서비스가 일부 제공되고 있다[3]. 현재, 콘티넨탈, 보쉬 등의 부품업체 및 도요타, 벤츠, GM 등 많은 OEM에서 클라우드 연계 플랫폼 및 서비스 개발을 매우 활발히 진행하고 있다. 또한, 이스크립트, 아거스, 하만, 파나소닉, IBM 등의 업체들에서는 차량의 실시간 정보를 클라우드에서 머신 러닝 등 지능형 분석을 통해 알려지지 않은 보안 위협을 탐지하기 위한 기술개발도 매우 활발하여 일부 솔루션들을 발표하기도 하였다.

클라우드 연계를 위한 관련 표준으로는 ISO TC22에서 진행 중인 Extended Vehicle(20077-1, 20078-1~4), 3GPP의 V2N, In-Vehicle Infotainment(IVI) 플랫폼 표준인 GENIVI의 RVI(Remote Vehicle Interaction), W3C의 Vehicle Information API 등이 있다. (그림 2)는 현재 서비스되거나 개발 중인 표준을 기반으로 차량의 데이터를 클라우드로 전송하기 위한 방식을 9가지로 구분하여 보여준다[4].

(그림 2)의 ①~③은 표준 어댑터 기반의 연결구조로 차량의 온보드 장치에 OBD 동글이나 ITS 커넥터 등을 장착하여 차량의 데이터를 클라우드로 전송하는 방식이다. ④~⑧은 차량에 탑재된 온보드 장치와 클라우드 연동을 위한 애플리케이션을 통해 클라우드로 차량 데이터를 전송하는 방식이다. ⑨는 표준 서버 인터페이스를 통한 연결 방식으로 예를 들어 OEM에서 클라우드 서버 및 관련 데이터를 직접 관리하고, 제3의 기관에게는 표준화된 인터페이스를 통해 차량의 데이터 일부를 공유하는 방식이다.



(그림 3) 차량용 이더넷 백본이 적용된 IVN

2. 내부 네트워크의 효율화

현재 자동차의 내부에는 CAN, LIN, FlexRay, MOST 등의 네트워크가 혼재되어 있으며, 자율주행 등 신규 서비스가 출현하면서 대용량 전송, 케이블 비용 절감, 통신의 효율성 및 확장성 등을 위해 차량용 이더넷 도입이 적극적으로 추진되고 있다. 현재 AVM(Around View Monitoring)이나 오디오/비디오 및 실시간 카메라 영상 등의 전송을 위해 점차적으로 도입되고 있는 차량용 이더넷은 점차 자동차 백본으로 적용이 확대될 전망이다. 실제로 BMW는 2018년에 이더넷 백본 도입 차량을 출시할 예정이라고 발표하기도 하였다. 차량용 이더넷 관련 표준으로는 BroadR-Reach의 AVB(Audio Video Broadcasting), SAE의 TTEthernet(Time-Triggered Ethernet, SAE AS6802), IEEE 802.1 Working Group의 TSN(Time-Sensitive Networking) 등이 있다. (그림 3)은 차량용 이더넷이 백본에 적용되는 경우 예상되는 차량 내부 네트워크 구성도이다.

Ⅲ. 자율주행 자동차 보안 기술 동향

본 장에서는 자율주행 자동차의 보안 기술 동향을 살펴본다.

1. 보안 위협 및 보안 기술 현황

본 절에서는 자율주행 자동차에 대한 보안 위협과 현재 적용 또는 연구되고 있는 보안 기술들에 대해 소개한다. 자동차에 대한 다양한 보안 위협과 이에 대응하기 위한 다양한 보안 솔루션들이 연구 개발되고 있으나, 결국 자동차에 있어서 가장 큰 보안 문제는 인가되지 않은 데이터가 차량 내부 네트워크로 주입되는 것과 DoS 등의 공격을 통해 자동차의 가용성이 침해되는 것이다. 이러한 목적을 위해 다양한 공격방법 및 위협이 존재한다. 〈표 2〉는 자율주행 자동차에 대한 보안 위협을 플랫폼, 네트워크, 관리/진단 측면에서 구분하여 정리하였으며,

〈표 2〉 자율주행 자동차 보안 위협

분류	보안 위협
전장 플랫폼	– ECU 소프트웨어 결함, ECU 리버스 엔지니어링 – ECU 펌웨어 해킹 및 위/변조 – 위장 ECU 장착 – IVI(In-Vehicle Infotainment) 해킹, 악성 감염 스마트 센서 물리 공격(블라인딩, 스푸핑, 재밍)
내부 네트워크	– 차량 내부네트워크에 악의적인 제어 메시지 주입 – 정상적인 내부네트워크 방해(패킷 삽입, 삭제, 임의조작, 지연 등), 도청 – DoS, 리플레이, 스푸핑, 패킷 폐기 공격
외부 네트워크	– 무선 통신망 해킹, DoS 공격 – 위장 OBU(Onboard Unit), RSU(Road Side Unit) – 악의적인 차량(Misbehavior Vehicle) – 거짓 정보(Fake message) 제공 – 차량 접속 기기 해킹
관리, 진단	– 프라이버시 침해, OBD-II 해킹 – 원격 업데이트 및 진단 프로토콜 해킹 – 해킹에 의한 사고원인 분석/증거 보존의 어려움

〈표 3〉 자율주행 자동차 보안 기술

분류	보안 기술
전장 플랫폼 보안	– 시큐어 부트, 시큐어 플래싱, 접근제어 – 애플리케이션 샌드박스, 플랫폼 가상화 – HSM(Hardware Security Module) – 부채널 방지 – Autosar CSM(Cryptographic Security Manager), SecOC(Secure Onboard Communication)
내부 네트워크 보안	– 침입 탐지 시스템(IDS), 차량용 방화벽(F/W) 침입 방지 시스템(IPS) – ECU 인증, 키관리, 암호화 – 위협탐지(Rule-Based, Machine Learning-Based)
외부 네트워크 보안	– V2X 메시지 인증, 암호화 – 차량 PKI, V2X 메시지 서명(고속) 검증 – IEEE 1609.2, CAMP VSC3
보안 관리, 진단	– 보안 모니터링, 보안 취약성 분석 – 차량 이상징후, 비정상 행위 분석 – 원격 SW/FW 보안 업데이트 – J2735 기반 보안성 평가 – 포렌식 및 사고 원인 분석 기술

〈표 3〉은 현재 개발 중이거나 일부 적용되고 있는 보안 기술들을 분류하였다.

전장 플랫폼 관련, 자동차의 기능이 고도화되면서 고성능 ECU가 탑재되는 추세이며 AUTOSAR 표준 플랫폼 적용도 조금씩 확대되고 있다. AUTOSAR는 버전 4.0 이후부터 보안규격이 포함되어 있으며, HSM 기반의 보안 기능을 제공하고 있다. VECTOR, ETAS,

Electrobit 등이 AUTOSAR 솔루션을 보유하고 있다. 국내에서는 현대 오토론이 AUTOSAR를 개발하고 있다. 현재 ECU 관련 보안 기술로는 시큐어 부트, 시큐어 플래싱, 시큐어 접근제어 등의 기술이 있으며, 이러한 기술들은 ECU 보호뿐 아니라 SOTA/FOTA 등 최근 안전한 원격 업데이트를 위한 요소기술로도 활용되고 있다. 자동차의 연결성이 확대되면서 IVI 헤드유닛 플랫폼 보호에 대한 연구도 최근 활발히 진행되고 있다. 애플리케이션 샌드박스, 시큐어 부팅 등의 기술이 일부 적용되고 있으며, 특히 헤드유닛의 전장연결 영역을 보호하기 위해 플랫폼 가상화를 통한 분리(Isolation), Adaptive Autosar, Secure SocketCAN, 방화벽 등 연구가 활발히 진행되고 있다.

ETRI는 IVI 오픈 플랫폼 표준인 GENIVI 상에서 리눅스의 보안 모듈인 LSM(Linux Security Module)을 확장하여, 커널 레벨 Socket API 후킹을 통한 정책기반 접근제어 모듈을 개발하고 있다.

차량 내부 네트워크 보안은 방화벽, IDS 등의 기술이 개발되어 일부 적용되고 있다. 현재는 알려진 위협 탐지 기술 중심이며, 규칙(Rule) 및 화이트리스트 기반의 탐지 기술이 주류를 이룬다. 국외에서는 하만, 아거스, 시만텍 등에서 국내에서는 펜타시큐리티, 페스카로 등에서 차량용 방화벽 기술을 개발하였다. 최근에는 알려지지 않은 위협 탐지를 위해 인공지능 기반 이상징후, 비정상 행위 분석 기술에 대한 연구도 활발히 진행되고 있다.

차량 외부 통신 보안은 차량간 V2X 보안의 경우 IEEE 1609.2 및 CAMP VSC3 표준 기반으로 기술개발이 이루어져 현재 국내, 국제적으로 테스트베드를 구축하여 실증하는 단계에 있다. IEEE 1609.2는 차량과 차량, 차량과 도로기지국간의 통신 보안 규격으로 메시지 인증, 무결성, 기밀성 보장 및 자동차 인증서 관련 내용이 포함된다. 차량 간 인증은 IEEE 1609.2와 CAMP VSC3에서 정의한 SCMS라고 하는 차량용 PKI (Vehicular PKI) 기술이 적용된다. 국내에서는 한국정보인증, ETRI, 현대오토에버, 하이게인안테나 등이 차량 PKI 기반의 자율주행 V2X 통합 서비스 보안 기술개발을 과학기술정보통신부 사업의 일환으로 진행하고 있다. 〈표 4〉는 자율주행 자동차 보안 표준을 정리하였다.

〈표 4〉 자율주행 자동차 보안 표준

표준명	개요
IEEE 1609.2	– 자동차 및 기지국과의 WAVE 통신을 위한 보안 통신 규격(암호, 인증, 디지털 서명 등)
IEEE 1616	– 자동차 EDR(Event Data Recorder 표준)
CAMP VSC3	– 프라이버시를 보존하는 자동차 PKI 표준
EVITA	– HSM 기반의 전자제어장치(ECU)보안 플랫폼 규격
AUTOSAR	– 자동차 전용 임베디드 소프트웨어 표준으로 4.1버전 이후로 암호 등 보안 규격이 포함
ISO 14229	– 자동차 통합 진단 표준 • 14229-1: ECU 에 대한 통합진단 • 14229-2: 세션 레이어 서비스 • 14229-3: CAN 네트워크 통합진단 • 14229-4: FlexRay 네트워크 통합진단
ISO TC22 SC31 WG2	– 자동차 진단 프로토콜 표준(진행 중)
ISO TC22 SC31 WG6	– Extended vehicle, 차량 클라우드 서비스를 위한 인터페이스 표준(진행 중: DIS20077-1,2, NP 20078-1~4), 보안규격 포함(진행 중)
ITU-T X.1373	– 보안 제어 기능을 갖춘 안전한 자동차 소프트웨어 업데이트 절차
ITU-T itssec-2	– 차량 V2X 통신 시스템에 대한 보안 가이드라인 (진행 중)
ITU-T itssec-3	– 차량 접속 디바이스에 대한 보안 요구사항(진행 중)
ITU-T itssec-4	– 차량 전장의 침입탐지 시스템 구성 방법(진행 중)
ITU-T itssec-5	– 차량 클라우드 edge 컴퓨팅 보안 가이드라인 (진행 중)
ETSI TS 102	– 지능형 교통시스템(ITS)을 위한 보안 표준 • 731: ITS 보안 구조 및 서비스 • 893: ITS 보안 취약점 및 위협 분석 • 941: ITS 프라이버시 보호 기술 • 942: ITS 접근제어 기술 • 943: ITS 보안 구조 및 서비스

2. 보안 기술 동향 및 이슈

본 절에서는 자율주행 자동차 보안 관련 이슈 중 분석

기술, 자동차용 이더넷 보안 및 V2X 보안 고속화 관련 연구 동향을 소개한다.

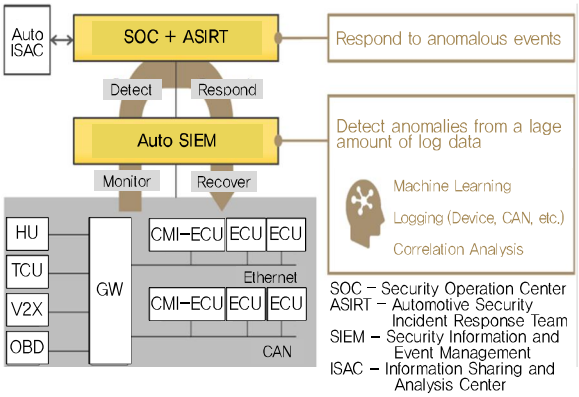
가. 분석(Analytics) 기술

자동차 보안 기술이 개발 및 적용이 활발히 이루어지고 있으나, 최근까지 지속적으로 해킹 사례가 보고되는 등 알려진 공격 대응 및 사후조치 수준의 기술적 한계 극복의 필요하다.

인텔[5]은 미래 자동차 안전을 위한 보안 기술을 4가지로 분류하였으며–(1) Secure the Platform (2) Secure the Communication (3) Secure the Backend (4) Secure Analytics, 파나소닉[6]은 자동차 보안을 위한 라이프 사이클을 3단계로 정의하였다–(1) Detection (2) Response (3) Protection. 인텔 분류의 Analytics와 파나소닉 분류의 Detection & Response 단계의 핵심은 지능형 분석이다. 파나소닉의 분류 중 Protection은 알려진 공격에 대응하기 위한 모든 기술을 포함하며, Detection과 Response는 알려지지 않은 공격을 탐지 대응하는 기술로 머신러닝 기반의 이상징후 탐지 알고리즘이 필요하다고 강조한다. 해외에서는 이러한 인공지능 기반의 분석 기술에 대한 연구가 매우 활발하며 관련 솔루션들도 일부 발표되고 있다.

시만텍[7]은 딥러닝을 기반으로 차량 내부네트워크의 트래픽을 학습하여 차량의 정상, 비정상 행위를 탐지하는 솔루션 'Anomaly detection for automotive'를 출시하였다. 이 솔루션의 특징은 시만텍 장치를 OBD–II 포트에 연결 후, 일정 시간 운전자의 주행 데이터를 딥러닝으로 분석, 학습하여 모델을 만들고, 이를 기반으로 주행 과정에서 발생하는 차량의 조작(브레이크, 엑셀, 핸들 등)이 운전자에 의한 것인지 해킹에 의한 것인지를 판별한다. 전장 메시지의 패턴, 페이로드 내용, 트래픽 주기, 차량의 상태 등이 학습, 분석및 탐지에 사용된다.

이스크립트의 IDPS(Intrusion Detection and Prevention System)는 3단계 방어(Firewall, Intrusion Detection, Monitoring & Analysis) 솔루션이 통합된 제품이며, 클라우드에서 2차 분석 결과를 피드백하여 차량 보안 시스템에 적용하는 구조를 갖는다. 하만, 아거스, IBM, 시스코 등도 클라우드 분석 기반의 위협 탐지 대응 솔루션을 개발하였다. 국내에서는 고려대학교 김휘강 교수 연구진이 머신러닝 기반의 차량 이상징후 탐지 알고리즘에 대한 연구를 진행하고 있다.



(그림 4) 파나소닉의 자동차 보안 시스템 구조[6]

[출처] T. Haga, R. Takahashi, T. Sasaki, T. Kishikawa, J. Tsurumi, and H. Matsushima, "Automotive SIEM and Anomaly Detection Using Sand–Sprinkled Isolation Forest," ESCAR Europe, Berlin, Germany, Nov. 2017.

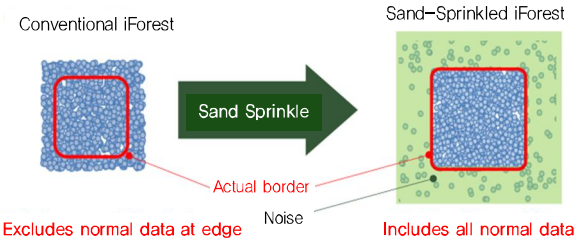
최근에는 파나소닉에서 클라우드 및 머신러닝 기반의 이상징후 탐지 기술인 AUTOSIEM[6]을 개발하여 ESCAR Europe 2017, ITS World Congress 2017 등 에서 발표하기도 하였다. 파나소닉에서 제안한 탐지 구조는 (그림 4)와 같다.

파나소닉은 자동차의 이상징후 탐지를 위해 머신러닝 기반의 Sand Sprinkled iForest(Isolation Forest) 기법을 개발하였다. 1차 과정은 다음과 같은 단계로 구성된다.

(1) Partitioning(sparse area=abnormal, dense area=normal)

(2) Generating binary tree(depth=anomaly level)

(3) Evaluation(normal or anomaly)



(그림 5) Sand sprinkled isolated forest 기법[6]

[출처] T. Haga, R. Takahashi, T. Sasaki, T. Kishikawa, J. Tsurumi, and H. Matsushima, "Automotive SIEM and Anomaly Detection Using Sand-Sprinkled Isolation Forest," ESCAR Europe, Berlin, Germany, Nov. 2017.

1차 과정에서 FPR(False Positive Rate)이 높게 나오는 문제가 발생하는데, 실험결과 Evaluation을 위한 경계(Border)를 중심으로 밀도가 높은 중앙의 데이터는 정상 데이터이지만 가장자리에 위치한 밀도가 낮은 데이터의 상당부분은 False positive 데이터들이었다. 이 문제를 해결하기 위해 파나소닉 연구진은 비정상적인 노이즈를 뿌리고 학습하는 방법을 통해 Evaluation Border 영역을 조정하는 방식인 Sand Sprinkled iForest 기법을 개발하여 적용하였다[(그림 5) 참조]. 이 기법을 통해 기존의 iForest 방식 대비 FPR이 26% 감소하였다고 한다.

현재 자동차 보안을 위한 지능형 분석에 대한 연구가 매우 활발히 진행되고 있으나 여전히 해결해야 할 이슈들이 존재한다.

한 가지 이슈는 즉각적인 대응이 필요한 자동차의 특성에 따른 실시간 대응 이슈가 있다. 이러한 이슈와 관련하여 실시간을 필요로하는 탐지/대응은 자동차에서 수행하고 그레이 영역에 해당하는 의심 트래픽은 클라우드에서 2차 분석은 수행하는 방식도 제안되고 있으며, 향후 5G 통신이 적용되면 문제가 없다는 시각도 있다. 또한, 클라우드로 전송하는 트래픽을 줄이기 위한 기법들(필터링, 샘플링, 데이터 압축, 동적 리포팅 등)에 대한 연구도 파나소닉 등에서 일부 진행되고 있다[8].

또 다른 이슈로 차량 간 CAN DB 및 전장 구조가 상이한 상황에서 다양한 차량에 적용 가능한 모델을 도출할 수 있는가 하는 이슈, 차량 내의 다양한 소스로부터 생성된 로그들의 연계분석 이슈 등도 있다.

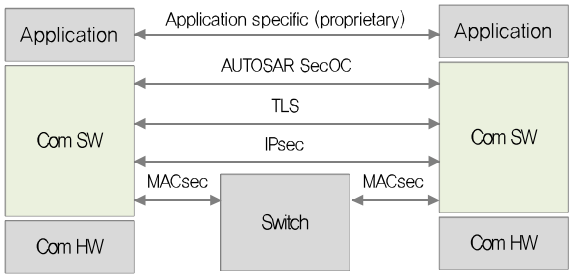
이처럼 여러 해결이 필요한 이슈들이 있기는 하지만, 알려지지 않은 공격 및 공격 감행 전 이상징후를 사전에 예측하기 위해서는 인공지능 기반의 분석서비스의 대안은 없는 상황이다.

이러한 지능 분석 기술은 자동차의 위협 예측, 이상징후 탐지뿐 아니라 사고/오동작이 발생할 때 원인분석 등 다양한 보안 서비스에도 활용이 가능하다. 최근에는 전장에서 공격 발생시 공격 ECU 탐지에 대한 연구도 등장하기도 하였다. CAN 네트워크는 메시지 ID 기반의 브로드캐스트 통신 방식으로 CAN 메시지에 송신자 및 수신자의 ID 정보가 없고 ECU에 대한 인증도 적용되지 않기 때문에 공격이 발생한 경우 공격자 ECU 및 피해 ECU의 식별이 매우 어렵다.

미시건 대학교 연구진[9]은 2017년 ACM CCS 행사에서 CAN ID 기반 전송 우선순위(Priority), 전압차에 의한 통신 특성, ECU 메시지 중 변하지 않는 필드의 전압 등을 핑거프린트 프로파일로 사용하여 공격 ECU를 탐지하는 기법을 제안하였다. 공격 탐지를 위하여 CAN 네트워크 내에 별도로 설치된 Fingerprinting ECU가 ECU 통신주기와 CAN 네트워크에서 전압 출력 변화를 기계 학습하여 트랜시버의 사용 전압을 Fingerprint한다. 미시건대는 상용차 2건에 실증 실험을 통해 98% 수준의 탐지 정확도를 확보하였다고 한다.

나. 차량 이더넷(Automotive Ethernet) 보안

최근 들어 자율주행 등 다양한 지능형 서비스를 제공하기 위해 자동차 내부에서 영상 등 대용량 데이터의 전송과 더욱 효율적이고 확장성 있는 네트워크 구조들이 필요하게 되었고, 이를 위해 등장한 것이 차량용 이더넷(Automotive Ethernet)이다.



(그림 6) 차량용 이더넷 온보드 통신 보안[10]

[출처] Elektrobit, "Secure Automotive Ethernet for Automated Driv-ing: Multi-level Security Architecture," Technical Paper, elektrobit.com, 2016.

차량 이더넷은 기존의 BUS 방식의 차량 내부 네트워크와는 통신구조, 특성 등이 상이하기도 하며, 이더넷 도입에 따른 프로토콜의 복잡성, 안전/비안전 영역간 통신 연결성 확대 등으로 인해 새로운 방식의 보안 기술 적용이 필요한 상황이다.

차량용 이더넷 보안 관련 연구는 해외의 Escrypt, Electrobit가 가장 발 빠르게 진행하고 있다. 차량 이더넷 보안을 위해 일반적으로 다음의 4계층의 보안 적용 단계가 필요하다고 정의된다.

(1) 네트워크에 대한 접근 제어: 중앙 게이트웨이를 통한 접근제어, 네트워크 분리 또는 VLAN을 통한 보안 영역(Security zone) 설정/관리 등.

(2) 온보드 보안 통신: 키 관리, 메시지 인증 코드, HSM, 암호화 등 적용을 통한 ECU간 보안 통신.

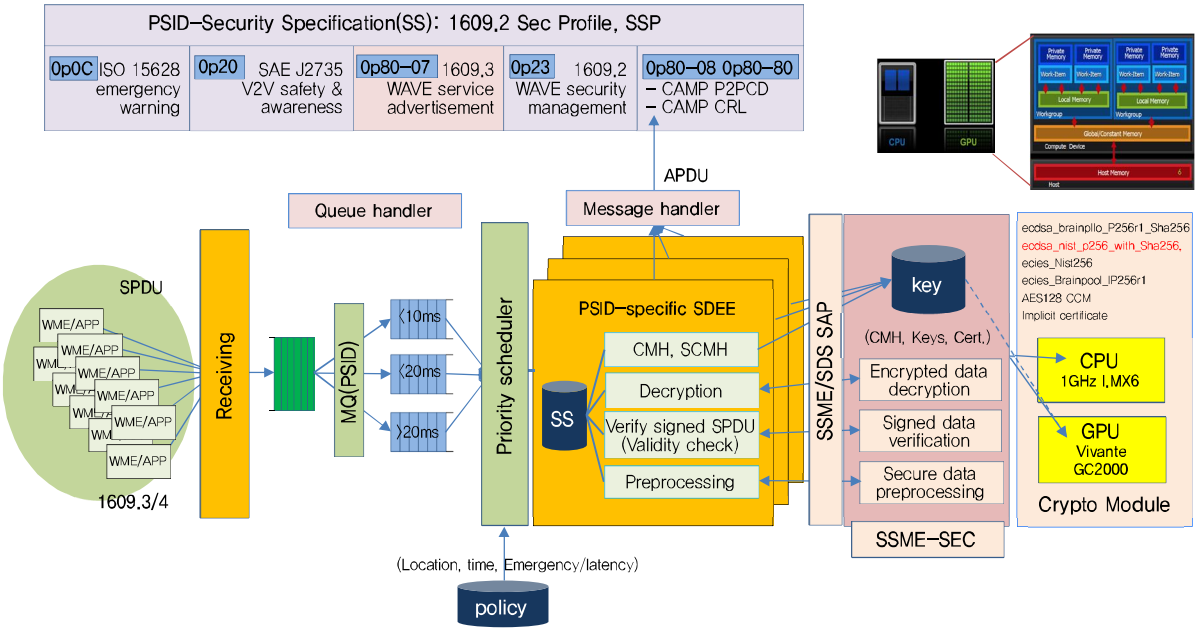
(3) 데이터 사용 정책: 차량의 상태 및 ECU 신뢰도 기반의 메시지 및 기능 사용 정책 적용.

(4) 네트워크 이상 징후 탐지 및 대응: 차량 이더넷 통신 과정에서의 비정상 행위, 이상징후 등을 탐지하여 대응.

(그림 6)은 차량 이더넷 기반 온보드 통신에 적용 가능한 보안 표준 프로토콜을 보여준다.

다. 고속화 이슈

차량 간 V2V 메시지 전송에 대한 성능 요구사항은 SAE의 J2945에 정의되어 있는데, SAE의 J2945에서는 차량 간 주기적으로 브로드캐스트 전송하는 안전메시지(BSM: Basic Safety Message)를 100ms 주기로 전송하도록 요구하고 있다. 즉 초당 10개의 BSM을 브로드캐



(그림 7) V2X 1609.2 메시지 고속 처리 및 ECC 고속 서명 검증 구조(ETRI)

스트 하도록 되어 있는 것이다. 만약 특정 차량 주변에 100대의 차량이 있다면 이 자동차는 1초에 1,000개의 BSM 메시지를 수신하게 된다.

이처럼 V2X 통신에 있어서 메시지의 고속 처리는 매우 중요하며 보안 관점에서는 차량 간 메시지의 서명 검증 고속화가 큰 이슈가 된다. 현재 OBU에는 서명키의 안전한 저장 및 안전한 서명 처리를 위해 HSM이 들어가 있으나 HSM은 CPU에 비해 낮은 클럭 스피드와 버스 딜레이 등의 요소로 고속 서명 검증 성능 확보에 어려움이 있다. 최근에는 고성능 CPU를 통해 SW 적으로 서명을 검증하거나, WAVE 모뎀에 ECC 가속을 위한 Co-processor를 탑재하여 고속 서명 검증을 하려는 시도가 있다. 또한, 별도의 하드웨어 지원 없이 병렬처리 기반의 고속화하는 기술도 연구되고 있다. ETRI에서는 OBU 및 RSU 장치로 활용되는 범용 보드 상에서 멀티 코어 CPU와 GPGPU 기반의 ECC 고속 서명 검증 및 멀티 프로세싱 스케쥴러 기반 Dot2(1609.2) 메시지 고속 처리 기술을 개발하고 있다. (그림 7)은 ETRI에서 개발 중인 1609.2 보안이 적용된 V2X 보안 메시지에 대한 고속 병렬처리 구조를 보여준다.

Ⅳ. 결론

100여 개의 ECU, 복잡한 소프트웨어 및 수많은 내/외부 연결성을 갖는 자동차는 다양한 보안 위협에 노출되어 있다. 현재 다양한 형태의 보안 솔루션들이 연구되어 자율주행 자동차에 적용되고 있기는 하지만, 최근까지 보안 공격 사례가 보고되는 등 여전히 기술적 한계를 보이고 있다. 본 고에서는 자율주행 자동차의 최근 트렌드와 보안위협현황 및 현재의 보안 기술들을 살펴보고, 현재의 보안 이슈로 분석 기술, 차량 이더넷 보안, V2X 보안 고속화 기술에 대해 살펴보았다. 본고에서 살펴본 이슈 외에도 자동차/개인의 프라이버시 보호, 자율주행 센서에 대한 물리 공격 대응, 자율주행 사고/오동작에 대한 원인분석 및 포렌식을 통한 증거 보존 등 다양한 보안 이슈들이 존재하며 관련 연구개발이 연구소, 기업, 학교 등에서 다양한 형태로 진행되고 있다.

자율주행 서비스는 자동차, 도로, 교통, ICT 인프라 등 다양한 산업이 융/복합되어 완성되는 기술이다, 보안기술 역시 다양한 산업 인프라를 고려한 형태로 설계 및 적용이 필요할 것으로 예측된다.

약어 정리

AUTOSAR	AUTomotive Open System Architecture
CCC	Car Connectivity Consortium
ECU	Electronic Control Unit
FOTA	Firmware Over-The-Air
HSM	Hardware Security Module
OBD	On-Board Diagnostics
SCMS	Security Credential Management System
SOTA	Software Over-The-Air
V2D	Vehicle-to-Device
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2V	Vehicle-to-Vehicle

참고문헌

[1] IITP, 과학기술정보통신부, “지능형 자동차 보안 위협 및 대응 방안 보고서,” 2017. 7.

[2] Qualcomm, “Leading the World to 5G: C-V2X Technologies,” 2016

[3] 권혁찬, “연결성 관점에서의 스마트카 동향 및 보안 이슈,” 정보와 통신, 한국통신학회, 제7권 제4호, 2017. 10, pp. 17-23.

[4] 권혁찬, “클라우드 커넥티드 자동차 보안 요구사항,” 사물인터넷 포럼 표준(IoTFS-0139), 2017. 12

[5] M. Schunter, “Vehicle-to-Cloud Research Challenges for Intelligent Vehicle,” *ESCAR Europe*, Berlin, Germany, Nov. 2017.

[6] T. Haga, R. Takahashi, T. Sasaki, T. Kishikawa, J. Tsurumi, and H. Matsushima, “Automotive SIEM and Anomaly Detection Using Sand-Sprinkled Isolation Forest,” Berlin, Germany, Nov. 2017.

[7] Symantec, “Anomaly Detection for Automotive,” White

paper, 2016

[8] T. Kishikawa, “Auto SIEM: Security Information and Event Management for Connected Vehicles,” ITS World Congress, Montreal, Canada, 2017.

[9] K.T. Cho and K.G. Shin, “Viden: Attacker Identification on in-Vehicle Networks,” *Conf. Comput. Commun. Security*, Dallas, TX, USA, Nov. 2017.

[10] Elektrobit, “Secure Automotive Ethernet for Automated Driving: Multi-level Security Architecture,” Technical Paper, elektrobit.com, 2016.