ETRI

2018
Electronics and
Telecommunications
Trends

# 오토모티브 이더넷 보안 기술

## Trends in Automotive Ethernet Security Technology

**정보흥** (B.H. Chung, bhjung@etri.re.kr) 시스템보안연구그룹 책임연구원/PL
**김대원** (D.W. Kim, dwkim77@etri.re.kr) 시스템보안연구그룹 선임연구원
**전부선** (B.S. Jeon, bsjeon@etri.re.kr) 시스템보안연구그룹 책임연구원
**주홍일** (H.I. Ju, juhong@etri.re.kr) 시스템보안연구그룹 책임연구원
**나중찬** (J.C. Na, njc@etri.re.kr) 시스템보안연구그룹 책임연구원/그룹장



In recent years, automobiles have evolved from simple transportation to convergence devices, and have combined the Internet of things, high-speed communications, and artificial intelligence technologies to provide people with social and cultural benefits. To provide services such as a smart traffic analysis, autonomous driving, and unmanned driving, automobiles applying these technologies are required to perform various types of sensing and image analyses for vehicle recognition and distance measurements. addition, there has been a rapid increase in the need to introduce an automotive Ethernet, that can provide a wide bandwidth to support. such technologies. In this article, we survey the latest trends in automotive Ethernet based automobiles and their security threats, and analyze the status and prospects of security technologies applied to cope with them.

* DOI: 10.22648/ETRI.2018.J.330508

*이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No.2018-0-00312, 오토모티브 이더넷 기반 차량 보안 위협 예측, 탐지, 대응 및 보안성 자동 진단기술 개발].

## Ⅰ. 서론

최근 들어 자동차는 단순한 운송수단에서 사물인터넷, 초고속통신, 인공지능기술 등이 융합되어 사람들에게 사회적, 문화적으로 유익함을 제공하는 방향으로 진화하고 있다. 예를 들면, 차량운행 시 차선변경을 시도하려는 경우 앞 유리창에 “주의, 오토바이가 좌측 10m 후방에서 80km 속도로 접근 중”과 같은 경고와 함께 운전자의 개입 없이 자동차가 스스로 속도를 늦추고 오토바이 통과 후 차선변경을 수행하는 편리한 기능을 제공하는 것이 가능하다. 또한, 도로상의 신호등과 연계하는 스마트 트래픽 관리 기술을 적용하여 공회전시간을 40%, 운전시간 26% 감소시키고, 차량 간 통신기술을 통해 사고율 79% 감소를 이룩할 수 있을 것으로 예측하고 있다[1]. 이러한 기술을 적용한 지능형 자동차는 스마트 트래픽 분석, 자율주행, 무인주행 등의 서비스 제공을 위해 전통적인 자동차에 비해 차량인식, 거리측정 등을 위한 다양한 센싱, 영상정보를 통한 복합분석이 필수적이고 이를 지원할 수 있는 넓은 대역폭 확보가 가능한 오토모티브 이더넷 도입 필요성이 급속도로 증가하고 있다[2]-[4].

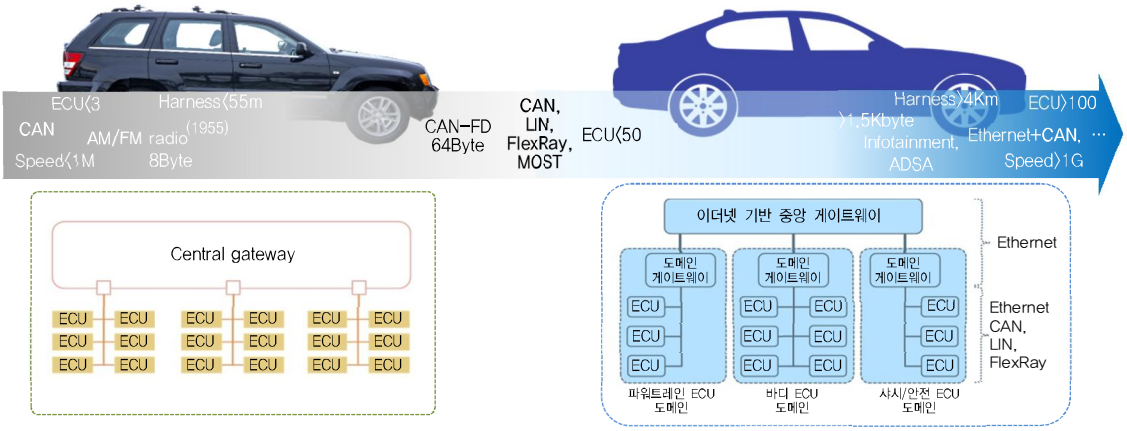
특히 오토모티브 이더넷을 도입하게 되면 앞차의 급제동과 같은 돌발 상황에 대한 추돌경고, 사고방지를 위한 커넥티드 서비스를 제공하기 위해 다양한 센서(거리인식, 차선인식)를 통합하고 점차 인공지능 기술까지 접목된 형태로 진화할 것으로 예측되고 있다[3]. 이에 따라, 구글, 테슬라를 비롯한 다수의 자동차 회사가 지능형 자동차(자율주행 자동차+커넥티드 서비스) 개발을 가속화하고 있다. 또한, 기존의 CAN(Controller Area Network)/LIN(Local Interconnect Network)/FlexRay/MOST(Media Oriented Systems Transport) 등과 같은 레거시 차량 네트워크와 더불어서 대용량 전송, 확장성이 높은 이더넷을 차량 네트워크로 도입하고 있다. 하지만 2016년 자율주행차 첫 사망사고에서부터 최근(2018년) 미국에서 잇따라 발생한 우버/테슬라 사고와 같은 자율 주행차 관련 안전사고에 대한 우려와 자동차를 해킹하여 교통사고를 유발하거나 자동차를 훔치고, 중요정보를 암호화해 금전을 요구하는 랜섬웨어 공격과 같은 자동차 대상 사이버 위협에 대한 우려가 커지고 있다[5]-[7]. 이는 기존의 레거시 네트워크는 보안을 고려하지 않은 채로 도입되었고 이더넷 또한 보안성보다는 2D/3D카메라/레이더/라이더센서를 활용한 무인주차시스템 등과 같은 서비스를 위한 이더넷의 넓은 대역폭 확보를 위하여 도입을 추진하고 있기 때문이다.

본고에서는 오토모티브 이더넷 기반 자동차 최신 동향과 그에 따른 보안 위협 요소들을 살펴보고, 이에 대응하기 위한 보안기술 현황 및 전망을 살펴보고자 한다.

## Ⅱ. 오토모티브 이더넷 기술 동향

최근 들어 국내/외적으로 운전자 지원(Advanced Driver Assistance) 기능을 추가하여 자동차 안전 및 운전자 편의를 향상시키고, 운전부하를 경감할 수 있는 지능형 자동차에 대한 관심이 높아지고 있다. 이들 자동차는 졸음운전 감지장치, 자동주차기능, 추돌예방 레이더, 움직이는 전조등, 후방사각 안내, 탈선경보시스템 등의 다양한 서비스를 운전자에게 제공한다. 예를 들어, 운전보조시스템을 위한 고해상도 영상지원과 같은 서비스를 효과적으로 지원하기 위해서는 오토모티브 이더넷을 차량에 도입하는 것이 시급하며, 다수의 자동차회사가 이를 위한 연구개발을 추진하고 있으며, 일부 차량에는 이미 적용되어 있다.

시스템 관점에서 자동차는 ECU, 센서 및 액추에어터, ECU 간 통신을 위한 자동차 내부 네트워크가 상호 연계하여 자율주행과 같은 주요기능을 수행한다. 이들 ECU는 (그림 1)에서 보는 바와 같이 그 목적과 특성에 따라 파워트레인, 섀시, 바디, 인포테인먼트 등의 4가지 도메인으로 분류 가능한 ECU들로 구분된다. 따라서,




(그림 1) 오토모티브 이더넷 기술 동향

[출처] 과학기술정보통신부, 정보통신기술진흥센터, "지능형 자동차 보안 위협 및 대응방안 보고서(2017)," 2017. 12의 그림 일부 수정.

효과적인 미래지향적 차량 서비스를 제공하기 위해서는 2020년경에는 차량 내 백본 네트워크로는 고해상도 영상지원 등이 가능한 이더넷을 차량의 기본적인 기능을 위해서는 기존의 레거시 방식을 하부 네트워크로 차용한 혼합형 네트워킹 방식이 차량 내부 네트워크로 사용될 것으로 예측되고 있다.

차량에는 변속기 ECU, 에어백 ECU, 원격시동 ECU와 같이 다양한 기능을 수행하는 ECU가 최소 100여 개 이상 장착되어 있다. 오토모티브 이더넷 자동차는 이들이 동시에 안전하게 수행되도록 하기 위해 개별 ECU에 실시간 운영체제 적용과 콤포넌트 단위 SW배포와 모듈화가 가능한 ECU 미들웨어 플랫폼인 AUTOSAR (AUTomotive Open System ARchtecture) 적용을 확대하고 있는 추세이다. 고화질 영상처리와 같은 대용량 데이터 지원 및 내부 트래픽 대역폭 확대 요구에 따라서 자동차 내부통신 네트워크 기술 발전전망을 예측한 자료에 의하면 2020년까지 엔진, 변속기제어, Braking Control, 카메라 기반 ADAS, 도어 및 시트제어, AV 엔터테인먼트를 비롯한 진단을 위한 OBD-II(On-Board Diagnostics-II)에 걸쳐 대부분의 ECU가 기존의 레거시 네트워크 방식에서 오토모티브 이더넷에 연결될 것이라고 한다[8].

오토모티브 이더넷 도입에 따라 자동차와 자동차 외부 시스템 간의 통신 방식도 다양화되고 있다. IEEE/3GPP는 WAVE(Wireless Access in Vehicular Environments) 기반 V2X(Vehicle to Everything) 통신기술 개발, 실증이 추진되고 있고, 2020부터는 LTE, 5G 기술이 도입 적용되며, LTE 기반의 V2V(Vehicle to Vehicle) 기술과 도로 기지국과 WAVE 규격을 사용하여 연동하는 서비스형태로 발전할 것으로 예상한다. 텔레매틱스, 사용자 맞춤형 자율주행 등의 서비스를 사용자에게 효과적으로 제공하기 위해 자동차 앱과 모바일 디바이스 앱과의 통합을 추진하고, 이전의 자동차 환경에서는 활용이 어려웠던 이상징후, 위협탐지, 비정상 행위 및 오류원인 분석 등의 고성능 연산을 빠르게 수행하는 클라우드 서비스를 적극적으로 도입할 예정이다. 최근에는 자동차 결함으로 인한 리콜 비용을 최소화하기 위해 원격 소프트웨어(SOTA: Software Over The Air), 펌웨어 업데이트(FOTA: Firmware Over The Air) 관련 표준제정과 기술 개발이 활용히 진행 중이며, 차량 외부에 위치한 서버에서 차량 관련 데이터를 효과적으로 획득하기 위해서 OBD-II를 통한 자동차 데이터 접근(In-Vehicle Interface)하는 방식에서 자동차 OEM이 관리하는 백앤드 서버에서 제공하는 표준 API를 통해 접근

(Extended-Vehicle Interface)하는 방식에 대한 발전될 예정이다.

자동차 안전성 진단 및 사고원인 분석은 전통적으로 최우선 가치로 고려되며, 이는 오토모티브 이더넷이 도입되더라도 변하지 않는 가치이다. EDR(Event Data Recorder)은 주행상태 기록 중심의 급발진 원인분석을 수행하기 위한 기초자료를 수집하는 장치이며, 국외에서 의무장착 확대를 추진하고 있다. 오토모티브 이더넷이 적용된다면 이에 비해 차량 내외부 영상/음성, 외부통신 정보 등을 포함하는 대용량 데이터 기록까지 가능한 ADR(Accident Data Recorder) 도입이 확대될 것이다.

## Ⅲ. 오토모티브 이더넷 기반 보안기술 동향

자동차와 인터넷의 연결 필요성으로 인해 자동차 대상의 사이버 공격 경로가 증가하고 있으며, 이러한 공격을 통해 임의의 원격조정을 수행하여 최악의 경우 자동차를 무기로 이용한 공격 가능성까지 대두되고 있다. 따라서, 이러한 자동차 대상의 보안 위협 및 공격 경로를 분석하여 효과적인 보안기술을 제공할 수 있어야 한다.

자동차 대상의 보안 위협과 공격 경로와 대상은 (그림 1)에서 보는 것처럼 ECU/센서/액추에이터, 내부 네트워크, 게이트웨이, 외부경로의 크게 4가지로 설명되고 있다. 이는 다양한 유무선 인터페이스를 통한 연결성 증가에 따른 차량 내부 네트워크 불법 침투 가능성 증가, 보안 설계가 미흡하여 다양한 공격 탐지에 한계를 가짐, 사이버공격 사고 발생 시 원인분석 미흡을 그 원인으로 보고 있다[9], [10].

### 1. 보안 위협 및 공격 경로

자동차를 대상으로 한 보안위협은 크게 자동차 내부 시스템 보안 위협, 자동차 외부 시스템 보안 위협, 자동차 보안/안전 진단 시스템 보안 위협으로 나누어 볼 수 있다.

내부 시스템 관점의 보안위협으로는 ECU, 센서, 액추에이터, 자동차 내부통신 보안위협 등이 있다. ECU는 저사양 시스템으로 자원제약 및 보안설계 미흡으로 불법접근/권한상승, 인증우회 등 다양한 공격에 취약한 특성을 가지고, ECU 대상 펌웨어, 소프트웨어 변조가 어렵지 않게 가능하다. 2016년 BBC News에서는 결함있는 SW 업데이트로 인해 상용차의 인포테인먼트 시스템이 반복적으로 재부팅됨을 보였다. 또한, 별다른 인증과정 없이 ECU로부터 전달되는 제어명령을 센서, 액추에이터가 수행하는 위협도 존재한다. 다양한 보고서에서 ECU에 대한 버퍼 오버플로우 공격, 메모리 손상, ECU펌웨어 불법수정 등의 다양한 공격이 가능함을 보였다. 또한, 위장 ECU를 통한 도청/해킹으로 원격제어, 텔레매틱스 시스템 인증 취약점이용 불법접속, 인포테인먼트 시스템의 웹 어플리케이션 비밀번호 초기화 등의 다양한 사례가 보고되어 있다.

자동차 내부통신은 버스 기반의 브로드캐스팅 방식의 내부통신 방식에 보안성 고려가 부족하여 통신과정의 도청, 리플레이, 스푸핑 등의 공격에 취약하다. CAN은 브로드캐시트 통신, 메시지 ID 기반 통신, 8byte로 제한된 데이터 페이로드 등 프로토콜의 구조적 문제로 공격이 쉽고, 보안기술 적용이 쉽지 않다는 특징을 가진다. LIN은 파워윈도우, 전동시트 등 안전과 무관한 기능에 주로 사용되는 저가형 프로토콜로 단순한 오류처리 메커니즘으로 취약성이 존재한다. FlexRay는 전송오류에 대한 무결성 보호 특성 제공을 위해 CRC 검사 값이 포함되어 기초적인 보안이 제공된다고 할 수 있으나, 메시지에 대한 읽기, 인증, 재생공격 등에 대한 방어를 위한 보안요소는 고려되어 있지 않다는 특징을 가진다. 따라서, 위장 ECU를 통한 도청/해킹으로 원격제어, 텔레매틱스 시스템 인증 취약점을 이용한 불법접속, 인포테인먼트 시스템의 웹 어플리케이션 비밀번호 초기화 등의 다양한 사례가 보고되어 있다.

외부 시스템 관점에서는 V2V, V2I(Vehicle to Infrastructure), V2D(Vehicle to Device), V2N 통신위협이 있다. V2V/V2I 측면에서는 외부통신 네트워크에 위장 OBU(On-Board Unit), RSU(Road Side Unit) 또는 V2X DoS 공격 및 통신 네트워크에 대한 통신방해 등을 수행하여 자동차 사고 유발 및 서비스 오작동이 가능하다. V2D 통신측면에서는 서비스 앱이 설치된 모바일 디바이스를 해킹하여 이 디바이스에 연결된 자동차를 임의로 제어가 가능하다. 실제로 스마트폰과 자동차 인포테인먼트 시스템을 연결하는 MirrorLink 취약점을 이용한 위협 가능성을 입증하였다. V2N 통신위협으로는 자동차가 네트워크 또는 클라우드 연결 시 다양한 위협에 노출된다는 것이다. 예를 들어, 자동차에 적용된 Wi-Fi 암호 단순성 및 취약점을 통한 원격조작에 대해서 다수의 자료에서 경고하고 있다. 이에 따라 자동차 보안성 강화를 위해 클라우드 기반 서비스 구조를 도입하려고 시도하고 있으나 빅데이터 분석과정에서 자동차의 위치, 주행정보 등의 운전자에 대한 프라이버시 침해 가능성에 대한 우려가 커지고 있다.

자동차 보안/안전 진단 시스템 관점에서는 ODB-II 포트위협과 보안성 진단 제한적이다. ODB-II 포트는 기본적으로 인증 절차 없이 접근가능 하도록 설계되어 있어 이에 대한 해킹 후 공격자가 자동차를 임의 제어할 수 있음이 알려져 있다. 즉, 3G 인터페이스를 지닌 ODB-II 동글을 포트에 연결한 후, 멀웨어 감염된 스마트폰 앱을 통해 자동차에 메시지를 전송하여 자동차 윈도를 임의로 개폐할 수 있음을 보였다. 또한, 자동차에 대한 보안성 진단은 사이버 위협이 고려되지 않은 기능안전성 진단 중심이므로 ECU 및 자동차 구성요소에 대한 보안 취약성 사전 검증 기술은 부족한 상태이다.

### 2. 이더넷 도입에 따른 환경 변화

자동차에 오토모티브 이더넷 도입하게 되면 이에 따른 다양한 이슈와 환경적 변화요인이 발생하며, 이를 크게 5가지 측면에서 설명한다[11]. 먼저, 자동차 네트워크 토폴로지 관점에서는 혼합네트워킹 방식으로 변화가 된다. 이는 기존의 CAN, LIN과 같은 버스/브로드캐스팅 방식의 레거시 네트워킹만을 사용하던 방식에서 이더넷과 기존의 레거시 네트워크가 공존하는 혼합 네트워크 형태 적용 필요하기 때문이다. 따라서, 레거시 ↔ 이더넷을 관리/제어할 수 있는 보안 게이트웨이 연구개발이 필요하다. 물리 레이어 관점에서는 저대역폭, 단방향 통신에서 고대역폭, 양방향 통신으로 변화가 이루어진다. 이는 자동차에 많은 수의 센서, 액추에이터를 추가하고 이들 간의 많은 양의 데이터 처리가 필요해진다. 특히, 카메라 같은 경우는 해상도 및 장치 수 증가 따라 최소 100Mbps 이상의 고대역폭이 필요하게 되기 때문이다. 네트워크 참여자 관점에서는 소량, 정보전달 중심에서 대량, 신뢰성 있는 정보 전달로 변화가 이루어진다. 일반적으로 자동차 네트워크의 참가자는 ECU이고, 혼합 네트워킹 방식을 통해 네트워크 참여자를 가장한 스푸핑 또는 오작동 발생 시도 등이 증가할 것이므로 신뢰성 있는 참가자가 자동차 네트워크에 연결될 수 있도록 엄격하게 제어할 필요가 있기 때문이다. 통신데이터 관점에서는 타임동기화, 단순데이터 전달 중심에서 데이터 실시간성, 정확성/신뢰성 강화로 변화가 이루어진다. 이는 네트워크 구조 및 참여자 등의 변화에 따라서 실시간성, 정확성, 신뢰성이 데이터 통신의 가장 중요한 요소가 되기 때문이다. 마지막으로, 시스템 관점에서는 소량, 지역적 비제한적 연동 중심에서 대량, 광역적, 제한적 연동으로 변화기 이루어진다. 이전의 레거시 방식에서는 소량데이터를 근거리 참여자에게 제한 없이 전달하는 방식이었다면 변화된 환경에서는 이들 객체 간의 상호작용이 다양해지고 자동차 내부 네트워크로 연결된 전달할 수 있어야 한다. 단, 이들 객체 간 상호연동 시 비정상적인 메시지 전달은 오작동을 초래할 수 있

고 이는 자동차에서는 심각한 위협이 될 수 있기 때문에 상호작용에 대해 범위와 권한을 명시적으로 엄격히 제한할 필요가 있기 때문이다.

### 3. 오토모티브 이더넷 보안 기술

오토모티브 이더넷 도입 확대와 더불어 자동차 보안성을 높이기 위해서는 위협예측, 개발생명 전주기 보안성검증, 심층 분석/방어를 통한 선제 대응 강화가 필요하다. 또한, 개별적인 자동차 구성요소 단위뿐만 아니라 인프라 전체적인 관점에서 보안 기술 도입을 고려해야 한다. 따라서, 앞으로의 자동차 보안 기술은 개발 전주기 과정의 보안성 시험 및 심층분석을 위한 클라우드 기반 보안서비스 기술 필요성이 점차 증가할 것이다. 그리고 권한 있는 사람만이 자동차에 대한 내부/외부 통신 네트워크에 대한 접근을 허용하고 연관된 ECU/센서 등과 같은 하부의 개별 디바이스까지 직접 제어하는 다단계 보안기술을 도입 접목할 것이다. 특히, 미래 지향적인 자동차 기술개발을 위해 대역폭 및 상호운용성 관점에서 도입한 오토모티브 이더넷 네트워크 보안기술이 가장 주목받게 될 것이다.

〈표 1〉, 〈표 2〉는 오토모티브 이더넷 보안기술 관점에서 국내외 관련 기관의 기술 및 제품 동향을 표로 정리한 것이다. 세계 자동차 시장의 급속 성장에 따라, 국내/외 차량 이더넷 관련 보안제품 개발을 목표로 다수의 업체 및 기관이 차량용 방화벽, 동적 취약성 분석, ECU 보호 솔루션 등의 다양한 차량용 보안 제품 개발을 추진 중에 있다.

오토모티브 이더넷 적용을 고려한 자동차 보안기술은 자동차 전장 플랫폼, 내부통신 네트워크, 외부통신 네트워크, 보안/안전 진단, 보안 모니터링 및 관리로 구분하

**〈표 1〉 국내 관련기관 및 제품동향**

| 기관기업(국가) | 기술/제품 상세 |
|---|---|
| 펜타 시큐리티 | – 차량용 방화벽, 전장용 키관리, V2X 보안통신 및 PKI 기술로 구성된 AutoCrypt 보안 솔루션 개발 |
| 페스카로 | – 하드웨어 보안 모듈(HSM)기반 ECU 보호 솔루션, 차량용 방화벽 개발 |
| 현대오토에버 | – V2X, V2N 등의 차량 외부네트워크 보안 및 차량 전장 네트워크 보안 솔루션 개발 중 |
| 인포뱅크 | – AUTOSAR 4.1.2 규격의 ECU 보안 S/W 플랫폼인 Basic Crypto S/W 컴포넌트와 CSM(Crypto Service Manager)을 활용하여 '자동차 전장 ECU간 보안 전송 기술'을 개발 |
| 자동차부품연구원 | – 국토부의 지원을 받아 자율주행 자동차 내부통신 보안 안전성 평가기술 개발 중 |
| 고려대학교 | – 머신러닝 기반의 차량 이상징후 탐지 알고리즘 개발 |
| ㈜지아이티 | – 차량 종합 진단시스템 개발과 모바일 기반의 진단서비스 중심으로 차량 안전 관련 정비 시장의 최고의 진단 솔루션을 제공 |
| 슈어소프트테크㈜ | – 자동차에 탑재되는 모든 SW의 오류를 탐지하는 차량 SW 테스팅 도구를 출시 |

[출처] ETRI, "오토모티브 이더넷기반 차량 보안위협 예측,탐지,대응 및 보안성 자동진단 기술개발," 공고번호:제2018-0069호, 사업계획서 2018.

**〈표 2〉 국외 관련기관 및 제품동향**

| 기관기업(국가) | 기술/제품 상세 |
|---|---|
| ARGUS CYBER SECURITY (이스라엘) | – 자동차 연결성, 내부네트워크 ECU 등 자동차에 대해 발생할 수 있는 공격을 탐지할 수 있는 보안솔루션 공급 |
| HARMAN (미국) | – 자동차 내·외부 네트워크 및 ECU보안 솔루션(ECUSHIELD, TCUSHIELD) 제품을 출시 |
| CISCO SYSTEMS INC.(미국) | – 클라우드 기반의 차량 악성코드 탐지, 차내망 이상징후 탐지 등 솔루션 개발 |
| ESCRYPT (독일) | – 자동차 보안 기술을 선도하는 글로벌 기업으로 PRESERVE, EVITA, OVERSEE 등 글로벌 규모의 자동차 보안 R&D 수행 |
| Symantec (미국) | – OBD-II 동글 형태로 장착가능한 자동차 이상징후 탐지 기술 개발. DPI 및 머신러닝 적용 |
| Electrobit(미국) | – 차량 이더넷 보안 구조 설계 연구 |
| EURECOM (프랑스) | – HW와 함께 에뮬레이터의 실행을 조정하면서 디바이스 바이너리 SW에 대한 동적 보안취약성 분석에 관한 연구를 수행 |
| Opal Security (프랑스) | – 디바이스의 다양한 하드웨어 인터페이스 대상으로 동적 보안취약성 분석 또는 디버깅을 위한 HW 프레임워크를 출시 |

[출처] ETRI, "오토모티브 이더넷기반 차량 보안위협 예측,탐지,대응 및 보안성 자동진단 기술개발," 공고번호:제2018-0069호, 사업계획서 2018.

여 살펴본다.

자동차 전장 플랫폼 측면에서는 시큐어 부트, 시큐어 플래싱, 시큐어 접근제어 및 ECU 가상화 솔루션 개발이 진행 중이다. 이는 ECU용 시큐어 부트/플래싱/접근제어 솔루션 또는 ADAS 및 AUTOSAR 통합플랫폼을 하이퍼바이저 형태로 ECU에 적용하는 방식이다. 최근에는 자동차 ECU 미들웨어 플랫폼 표준규격인 AUTOSAR 적용이 확대되고 이에 따라 AUTOSAR에 정의된 보안기능을 활용하여 보안통신, 공격방어 등의 보안성 강화를 추진하고 있다[12], [13]. 이를 위해 Elektrobit, ETAS, VECTOR사 등은 AUTOSAR 4.3 이상을 자동차에 적용하는 목표로 하고, 보안을 위해 CSM을 적용할 것을 제시하고 있다. 또한, 하드웨어 가속 기능을 활용하여 보안성을 강조하기 위해 자동차용 HSM(Hardware-based Security Module) 제품이 일부 출시되고 ECU에 적용, 연계하기 위한 시도가 이루어지고 있다. 국내에서도 자동차 ECU 가상화 기술을 통한 보안성 강화 및 시스템 안전성 보장기술을 시도한다든지 AUTOSAR 규격에 적용 가능한 보안모듈을 개발을 추진하고 있다. 또한, ECU 펌웨어 무결성 및 실행환경 안전성 보장을 위한 HSM 응용기술 개발도 추진 중이다.

자동차 내부통신 네트워크 측면에서는 현재까지는 CAN 중심의 방화벽, IDS 연구가 중심이었다. 유럽의 Oversee 프로젝트에서 자동차 방화벽 및 접근제어 기술 개발을 수행하였고, Towersec, Harman, Symantec 등에서 솔루션을 출시하였다. 그러나, 내부통신이 CAN에서 고대역폭, 대용량 데이터를 요구하여 이더넷 도입 필요성이 증가함에 따라 이더넷 통신보안에 대한 연구가 시도되고 있다. 즉, ESCRYPT, ElekTrobit, NXP 등에서 자동차 이더넷 보안을 위한 기술적 요구사항 및 구조 등을 제안하고, 후속 연구를 중장기 연구로써 진행하고 있다. 그러나, 자동차 내부 통신 네트워크(IVN: In-Vehicle Network) 보안에 특화된 별도의 표준 규격은 없으며 CAN 통신상의 기밀성 및 무결성 보장, CAN 메시지 인증, 비정상 CAN 패킷 유입 방지와 같이 CAN 통신 중심의 보안기술이 주류를 이르고 있다. 국내에서도 주로 CAN 중심의 보안기술 및 연구개발이 수행되었으며, 차량 내부 네트워크 침입탐지를 위한 차량 탑재형 IDPS 관련 연구들이 진행되고 있으나 오토모티브 이더넷 보안기술은 이제 연구가 시도되고 있는 수준이다.

자동차 외부통신 네트워크 측면에서는 미국, 유럽 등 다수의 프로젝트에서 IEEE 1609.2 등 국제표준을 준용한 사업이 진행 중이며, WAVE기반 V2X 통신보안과 CAMP VSC3(Crash Avoidance Metrics Partnership Vehicle Safety Communications 3)에서 자동차용 PKI 기반 인증서 관리 규격(SCMS: Security Credential Management System)과 같은 내용을 다루고 있다. 또한, 유럽의 Car2Car 컨소시엄에서는 ITS 통신 단말 신뢰보증 등급 기준 제정을 목표로 진행 중에 있다. 국내에서도 WAVE 기반 V2X 통신보안 중심의 기술개발이 진행 중이며, 자동차 PKI, V2I/V2V 신뢰성 보장, 1609.2 통신 보안처리 고속화 등과 같은 서비스 보안 기술 개발도 진행 중이다. 하지만, 자동차 및 도로기지국과 CITS(Cooperative-Intelligent Transport Systems)와 연계시 신뢰성 확보가 가능한 상호 인증 및 통합 보안 관제 분야는 연구를 시작하는 초기 단계이다.

자동차 보안/안전 진단 측면에서는 ECU 보안에 대한 사전검증은 아직 일반적으로 진행되지 않고 있어 ECU와 같은 자동차 IT부품에 대한 상세 보안평가 및 자동 취약성 분석을 위한 연구가 시도되고 있다. 2015년 SAE(Society of Automotive Engineers)는 사이버보안을 위한 자동차 개발 프로세스 및 가이드라인(J3061)을 정의하였고, 미국에서는 2014~2016년 다양한 유형의 ECU 보안취약점과 CAN 프로토콜이 적용된 자동차 ECU 보안 취약성 연구를 수행하였다. 그러나 사이버 공격에 의한 자동차 사고 원인규명 관련해서는 연구가

부족한 실정이고, 자동차내 일부분 장치에 대한 포렌식 기술 연구가 진행 중이다. 2017년 Berla에서는 인포테인먼트 시스템에 대한 포렌식 기술(iVe)을, 2016부터 Irdeto에서는 자동차/범죄 소송용만을 위한 포렌식 기술을 개발 중이다. 국내에서는 자동차와 외부 연결지점에 대한 비인가 접근여부를 조사, 분석을 목적으로 하는 모의해킹 취약점 진단을 수행하고 있다. 일반적인 자동차 사고원인 분석을 위한 EDR, CDR(Crash Data Retrieval) 장치가 있으나, 해킹에 의한 사고원인 분석을 수행하는 연구는 미흡한 실정이다.

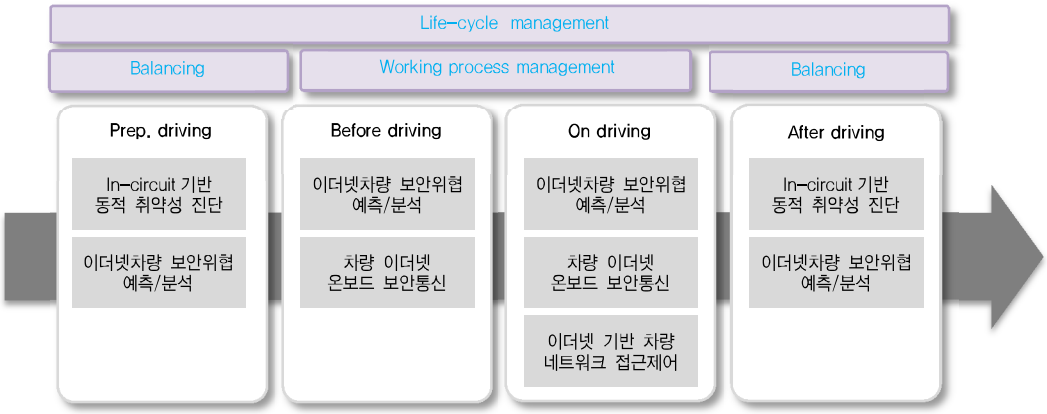
자동차 보안 모니터링 및 관리 측면에서는 ECU W/FW 업데이트를 위해 암/복호화 등의 다양한 보안기법을 적용한 제품 개발이 진행 중에 있다. ITU-T에서는 자동차 ECU 원격 업데이트를 위한 보안 표준규격(x.1373) 2017년 제정하였다. 최근에는 알려지지 않은 침입탐지 또는 상세분석을 위해 클라우드 환경을 활용하여 비정상 행위탐지까지 가능한 기술개발 목표로 연구 및 표준화가 진행 중에 있다. 또한, 2017년부터 도요타, MIT 미디어 연구소 등은 블록체인 기술을 도입하기 위한 연구를 착수하고 있다. 국내에서는 2012~2015 AVN ECU(Audio Video Navigation system Electronic Control Unit)에 대한 SW 업데이트 기술개발 프로젝트가 진행되었으며, 국내 OEM은 해외 업체와의 협력을 통해 SOTA/FOTA 솔루션을 확보하려는 추세이다. 또한, 알려지지 않은 침입탐지 또는 상세분석을 위한 클라우드 기반 비정상 행위 탐지분야는 학계를 중심으로 기초연구가 시도되는 수준이다.

## Ⅳ. 결론

오토모티브 이더넷 보안기술은 자동차에 이더넷 도입 확대에 따라 자동차 보안성을 높이기 위해서 위협예측, 보안성검증, 심층 분석/방어를 효과적으로 제공하기 위해 반드시 개발이 필요한 기술이다.

본고에서는 자동차 보안성 및 안전성을 위해 관심을 받는 오토모티브 이더넷 보안기술의 전반적인 동향과 향후 필요한 기술적 이슈들을 살펴보았다. 세계적으로 이더넷 기반의 자동차 시장이 급속 성장할 것으로 예측되고, 이에 따라 국내/외적으로 오토모티브 이더넷 관련 보안 제품 개발에 대한 관심 증가하고 있으나, 아직까지는 레거시 네트워크 중심의 기술개발이 주류임을 확인하였다. 또한, 이들 기술을 자동차 내부, 외부, 보안/안전 진단, 모니터링 및 관리측면에서 현재의 기술수준과 한계 및 해결해야 할 이슈들이 있음을 확인하였다.

오토모티브 이더넷은 현재 대부분 자동차에 적용된 버스 방식의 레거시 네트워크와 네트워크 구조, 통신 프로토콜, 서비스, 성능 요구사항이 상이하여 이에 특화된




(그림 2) 오토모티브 이더넷 보안 기술 적용 방안

보안기술 개발, 적용이 필요하다. 따라서, 이더넷 기반 차량 네트워크의 안전한 통신을 보장하고, 사이버 위협 예측 및 원인분석을 통해 선제적 대응과 보안성 자동진단이 가능한 보안기술을 개발하여야 한다. 이들 기술은 계층적이며 다양한 방식으로 제공되어야 한다. 따라서, (그림 2)와 같이 ECU 또는 ECU 간 연동 차원에서 동적 취약성 진단이 가능한 동적 취약성 진단 기술, 오토모티브 이더넷 자동차를 대상으로한 보안 위협 예측/분석 기술, 자동차 내부 온보드 네트워킹의 보안을 강화한 온보드 보안통신 기술, 오토모티브 이더넷 자동차에 대한 임의적이고 불법적인 접근/조작을 차단할 수 있는 이더넷 기반 자동차 네트워크 접근제어 기술 개발이 시급한 시점이라고 판단된다.

## 약어 정리

| | |
|---|---|
| ADR | Accident Data Recorder |
| AUTOSAR | AUTomotive Open System ARchtecture |
| AVN | Audio Video Navigation system |
| CAMP VSC3 | Crash Avoidance Metrics Partnership Vehicle Safety Communications 3 |
| CAN | Controller Area Network |
| CDR | Crash Data Retrieval |
| C-ITS | Cooperative-Intelligent Transport Systems |
| ECU | Electronic Control Unit |
| EDR | Event Data Recorder |
| FOTA | Firmware Over The Air |
| HSM | Hardware-based Security Module |
| IVN | In-Vehicle Network |
| LIN | Local Interconnect Network |
| MOST | Media Oriented Systems Transport |
| OBD | On-Board Diagnostics |
| OBU | On-Board Unit |
| RSU | Road Side Unit |
| SAE | Society of Automotive Engineers |
| SCMS | Security Credential Management System |
| SOTA | Software Over The Air |
| V2D | Vehicle to Device |
| V2I | Vehicle to Infrastructure |
| V2V | Vehicle to Vehicle |
| V2X | Vehicle to Everything |
| WAVE | Wireless Access in Vehicular Environments |

## 참고문헌


[1] Intel, "The Intelligent Car(Almost) as Smart as You," 2014. Available: http://download.intel.com/newsroom/kits/ces/2014/pdfs/TheIntelligentCar_infographic.pdf

[2] P. Hank et al., "Automotive Ethernet: In-Vehicle Networking and Smart Mobility," In *Proc. Conf. Des., Automation Test in Eur. Grenoble*, France, Mar. 18-22, 2013. pp. 1735-1739.

[3] Intel, "Car of the Future-Trends in Next-Generation Automotive Safety and Security," 2017. Available: https://www.intel.com/content/dam/www/public/us/en/documents/guides/safety-and-security-campaign-guide.pdf

[4] J. Laštinec, "Security Extension of Automotive Communication Protocols Using Ethernet/IP," *Inform. Sci. Technol. Bulletin ACM Slovakia*, vo. 9, no. 1, 2017, pp. 49-56.

[5] 김미경, "자율 車첫 사망…진화의 과정? AI의 한계?," 서울신문, 2016. 07. 01. http://www.seoul.co.kr/news/newsView.php?id=20160702001011

[6] 연합뉴스, "우버 자율주행차 첫 보행자 사망사고…안전성 논란 증폭," 연합뉴스, 2018. 03. 20. http://www.yonhapnews.co.kr/bulletin/2018/03/20/0200000000AKR20180320003951075.HTML

[7] M. Wolf et al., "WANNADRIVE? Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles," ESCRYPT GmbH, pp. 1-14. Available: https://www.escrypt.com/sites/default/files/documents/Ransomware-against-cars.pdf

[8] H.-Y. Lee and D.-H. Lee, "Security of Ethernet in Automotive Electric/Electronic Architectures," *J. Institute Internet, Broadcast. Commun.*, vol. 16, no. 5, Oct. 31, 2016, pp. 39-48.

[9] A. Talic, "Security Analysis of Ethernet in Cars," MS Thesis, KTH Royal Institute of Technology, 2017.

[10] C. Church, "The Connected Vehicle: Vulnerabilities, Future, and Security," Infosec Writers, Apr. 19, 2017. Available: http://www.infosecwriters.com/articles/2017/04/19/connected-vehicle-vulnerabilities-future-and-security

[11] D. Zelle et al., “On Using TLS to Secure In-Vehicle Networks,” In *Proc. Int. Conf. Availability, Reliability Security,* Reggio Calabria, Italy, Aug. 29-Sept. 1, 2017. pp. 67:1-67:10.

[12] 권혁찬 외, “자율주행 자동차 보안기술 동향,” 전자통신동향분석, 제33권 제1호, 2018. 02, pp. 78-88

[13] 이호용, “자동차 보안의 과거 현재, 그리고 미래,” Automotive Electronics, 2015. 03.