Transactions of KSAE, Vol. 26, No. 2, pp.240-253 (March, 2018)

pISSN 1225-6382 / eISSN 2234-0149
DOI https://doi.org/10.7467/KSAE.2018.26.2.240

자율 주행 차량의 In-Vehicle 시스템 관점에서의 공격 시나리오 도출 및 대응 방안 연구

서 은 비 · 김 휘 강*

고려대학교 정보보호대학원 정보보호학과

Security of Self-Driving Car from the Point of View of In-Vehicle System

Eunbi Seo • Huy Kang Kim*

Information Security, Korea University, Seoul 02841, Korea

(Received 25 October 2017 / Revised 8 January 2018 / Accepted 8 January 2018)

Abstract : As the technology of self-driving cars are being developed, security and safety are becoming important issues. The communication channel of the self-driving car is divided into external network and internal network. The external network is used for inter-vehicle communication or vehicle-to-infrastructure communication. On the other hand, the internal network, which is called the In-Vehicle network, is used to control the functions of the vehicle. Although the In-Vehicle network is a critical part of the vehicle, it is exposed to many threats. In this paper, we examined the primary functions of self-driving cars and reviewed the recent studies on the security of self-driving cars. Furthermore, we derived various attack scenarios from the In-Vehicle system perspective and analyzed the security requirements.

Key words : Security(보안), Self-driving car(자율주행자동차), In-Vehicle system(자동차 내부 시스템), IDS(침입 탐지 시스템), Security of requirement(보안 요구 사항)

1. 서 론

사물 인터넷(IoT) 기술의 발전과 함께 다양한 IT 기술을 적용하여 운전자의 편의성을 증대시키는 자율 주행 자동차의 시장이 확대되고 있다. 2016년 시장조사기관 IHS의 자료에 따르면 완전 자율 주행 자동차의 전 세계 연간 판매량은 2025년경 23만대에서 2035년 1,180만대에 이를 것으로 전망되며, 시장조사기관 ABI에서는 부분 자율 주행 자동차를 포함 연간 판매량이 2025년 110만대에서 2035년 4,200만대로 늘어날 것으로 예측하였다.[1,2)]

이처럼 자율 주행 자동차 시대의 도래로 인해 제조사뿐만 아니라 ICT 기업들 또한 자율주행으로 대표되는 커넥티드 카 시장에 참여하면서, 자율주행 자동차에 대한 보안 기술은 자율 주행 자동차의 대중화를 위한 선결 조건이 되었다. 자율 주행 자동차의 보안 사고는 물질적 피해뿐만 아니라 운전자와 보행자의 안전에 직접적인 해를 가할 수 있으므로, 새로운 기술의 도입 및 확산에 따른 규제와 보안 사고에 관한 적절한 가이드라인이 필요하다.

자율 주행 자동차는 내부 장치 간 효율 적인 통신을 위해 수많은 전자 제어 시스템 및 소프트웨어를 탑재하고 있으며, 다양한 내부 네트워크 통신 기법

*Corresponding author, E-mail: cenda@korea.ac.kr

(CAN, LIN, FlexRay)을 사용한다. 대부분의 차량에 적용되는 CAN 프로토콜은 ECU 간 정보의 전송 및 교환을 통해 차량 내부 네트워크의 수많은 전자 제어 장치를 제어하고, 상황에 맞는 명령을 수행하여 자동차를 구동한다. 이는 공격자가 CAN 버스 시스템에 진입할 경우, 각 시스템을 제어할 수 있는 변조 메시지를 통해 해당 차량의 In-Vehicle 시스템을 악의적으로 조작할 수 있게끔 한다. 뿐만 아니라 최근 출시된 자동차 내 내장되는 최대 1억 라인의 소프트웨어 코드는 공격자가 해당 차량을 제어할 수 있는 수많은 취약점을 갖고 있다. CAN 버스 시스템에 진입한 공격자는 악성 코드를 삽입하여 ECU를 장악한 후 자동차의 급발진 및 브레이크 페달 무력화 등의 안전에 직결적인 영향을 미치는 공격을 수행할 수 있다.

자율 주행 자동차의 In-Vehicle 시스템 내 진입할 수 있는 경로 중 하나는 V2X(Vehicle to Everything)이다. V2X 네트워크는 자율 주행과 외부 통신을 이어주는 네트워크 통신 기술로 차량 간 통신인 Vehicle to Vehicle(V2V), 차량과 인프라 간 통신인 Vehicle to Infra(V2I), 차량과 모바일 기기 간 통신인 Vehicle to Nomadic Device(V2N)으로 분류된다. 공격자는 V2V 통신 네트워크에 변조된 메시지를 주입하여 사고가 발생한 차량이 있음에도 인지하지 못하도록 하여 2차 충돌 사고를 발생시키거나, 특정 차량의 특정 위치, 특정 시점의 메시지를 기록한 후 또 다른 차량에 Replay 공격을 통해 얼음 길 등 주변 환경과 맞지 않은 속도를 내도록 하여 사고를 유발할 수 있다. 그밖에 DoS 공격을 통해 차량 간 통신을 무력화하는 등, V2V 통신을 악의적으로 이용할 수 있는 방법은 다양하다. 또한 V2I 네트워크 통신의 도청을 통해 요금 징수, 위치 기반 서비스에 대한 지불 등 금융 결제와 관련 운전자의 개인 정보를 탈취하여 악용할 수 있다. V2N은 공격자가 In-Vehicle 시스템에 진입할 수 있게끔 하는 대표 경로이며 공격자는 차량과 모바일 기기를 연결하는 인포테인먼트 시스템을 통해 In-Vehicle 시스템에 접근한다. 한 예로 블루투스 시스템은 차량과 연결된 스마트폰의 앱을 이용하여 In-Vehicle 내 악성 코드를 삽입할 접근 포인트를 제공한다. 또한 차량 내 오디오, 비디오, 네비게이션 시스템을 지칭하는 AVN 시스템 또한 펌웨어 취약점 공격이 가능하며, GPS나 위성 라디오 채널이 악용될 수 있다.

다양한 센서 기능을 탑재한 자율 주행 자동차는 공격자가 해당 센서를 이용하여 In-Vehicle 시스템에 접근할 수 있는 또 다른 경로를 제공한다. 자율 주행 자동차는 레이더(라이더) 센서 기술 및 정밀 지도 기술, 무선 통신 등을 융합하여 주행 환경 상의 다양한 대상 및 물체를 인지한다. 이러한 센서는 외부 신호를 직접적으로 받아들이므로, 다양한 보안 프로토콜을 사용하는 다른 통신보다 쉽게 공격에 노출 될 수 있다. 센서를 이용해 주변 상황을 판단하는 과정을 의도적으로 조작하여, 센서와 In-Vehicle 시스템 간 통신 내의 메시지를 조작해 차선 및 장애물 등의 인식을 방해할 수 있다. 또한 자율 주행 자동차의 탐지 센서인 라이더 역시 특정 주파수 음파에 노출하는 등 기만 공격에 취약한 실정이다. 자율 주행 차량 내 주행상황 인지를 위한 영상 기반 모듈도 형상정보와 거리정보 등을 조작하는 등 공격자에 의해 악용될 여지가 있다.

이처럼 인지 및 판단 기술을 필수적으로 요하는 자율 주행 자동차는 외부 통신과 차량 내부 시스템 내 다양한 모듈 및 탑재된 코드로 인해 안전과 직결되는 수많은 취약점을 가질 수 있다. 본 논문에서는 자율주행 자동차의 In-Vehicle 시스템을 공격할 수 있는 다양한 시나리오를 도출하고 탐지 방안을 제안하여 자율 주행 자동차의 보안 사고에 대한 요구사항 및 해결책을 연구하는 것을 목표로 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 자율 주행 자동차 관련 연구, 기능 및 개발 현황을 살펴본다. 제 3장에서는 보안적 관점에서 자율 주행 차량의 취약점을 도출한다. 제 4장에서는 자율주행의 일부 기능을 대상으로 보다 상세한 In-Vehicle 시스템 공격 시나리오를 정의하고, 이에 대한 대응 방안을 논의한다. 제 5장에서는 자율 주행 차량의 보안 요구 사항을, 제 6장에서는 본 논문의 시사점에 대해 서술한다.

2. 자율 주행 자동차 동향

2.1 자율 주행 자동차 기술 단계

자율 주행 자동차의 정의는 기술 단계 및 차량 제

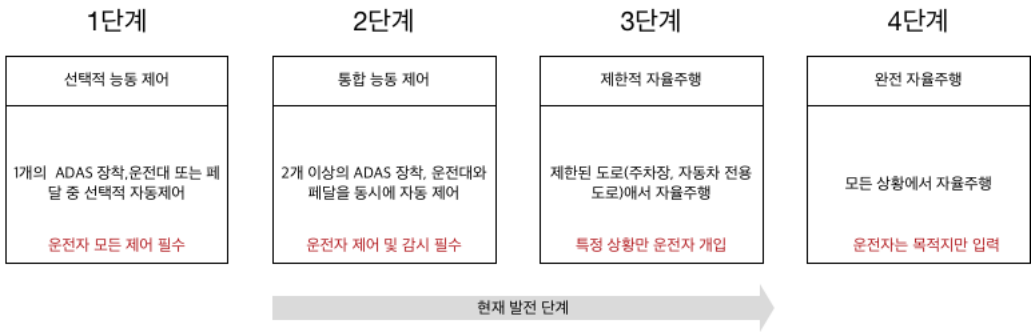


Fig. 1 ADAS Tech technical step

어를 돕는 ADAS 센서의 결합 정도에 따라 다양하다. Fig. 1은 미국 도로 교통 안전국 NHTSA에서 제시한 자율주행 자동차 기술 단계로, 크게 4단계에 따라 자율주행 자동차를 분류하고 있다.[3] 각 단계는 운전자의 간섭에 따라 구분되며 차량 내 ADAS의 결합 정도가 자율주행 자동차의 기술 단계를 구분하는 척도가 될 수 있다.

ADAS는 운전 보조 장치로 운전 시 위험 상황을 감지하는 센서를 통해 운전자에게 위험을 경고하여 대처할 수 있도록 하는 안전장치이다. ADAS가 제공하는 기능에는 어드밴스드 크루즈 컨트롤, 사각지대 모니터링, 차선 이탈 경고, 자동 점등/소등, 차선 유지 보조 및 충돌 경고 시스템, 자동 조향, 브레이크 조작 등이 포함된다. 능동적인 ADAS의 경우 자동차 움직임을 부분적으로 제어함으로서 사고를 방지하기 때문에 ADAS 기술은 4단계의 완전 자율주행 자동차를 위한 중요한 기반이라고 볼 수 있다.

기술 단계 내 2단계에서 3단계로의 발전은 차량 사고의 주체가 운전자에서 자율주행 자동차로 변경된다는 점에서 큰 의미를 가진다. 현재 국내의 자동차 주행에 대한 법률은 2단계까지만 허용되고 있으며, 3단계 환경에서 사고가 발생할 경우 운전자와 자동차 제조사 간 복잡한 법률문제가 발생할 수 있다.[4] 따라서 운전자의 안전 및 차량 보안을 위해, 차량의 주변 환경에서 발생 가능한 모든 상황들에 대응할 수 있는 ADAS 시스템의 구현이 요구된다.

2.2 자율 주행 자동차 기능 및 구조

자율주행 자동차는 크게 센싱, 신호처리(인지), 판단, 제어 프로세스로 구성된다.[5] ADAS 센서를 통해 차량의 주변 환경 정보를 수집하고, 수집된 정보를 처리하여 지형, 장애물, 보행자 등의 정보를 차량에 제공한다. 차량에서는 제공받은 정보를 통해 위험 상황 유무 등의 상황 판단 및 주행 전략을 결정하며, 제어 시스템에서는 결정된 주행 전략에 따라 차량을 제어하게 된다. Fig. 2는 자율주행 자동차 동작 과정을 보여준다. 본 논문에서는 자율주행 자동차의 각 기술 단계에 따라 동작 원리를 서술하고, 이를 기반으로 안전성 및 보안성을 증명할 수 있는 자율주행 자동차를 위한 요구 사항을 논의한다.

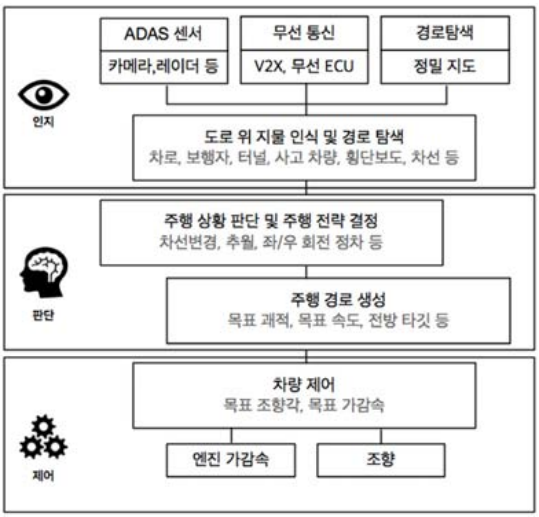


Fig. 2 Key function of self-driving car

2.2.1 ADAS 센서

ADAS는 Advanced driver-assistance systems의 약자로, 복잡한 차량 제어 프로세스에서 운전자를 도

우며 자율 주행 자동차의 관점에서는 궁극적으로 운전자를 대체할 수 있도록 개발된 시스템이다. ADAS 기술 개발의 궁극적 목표는 자율주행 자동차의 상용화이며, 따라서 NHTSA의 자율주행 자동차 기술 단계에 따라 발전되고 있다. 즉 기존의 ADAS를 조합하거나 개선함으로써 다양한 도로 상황에 대응할 수 있는 자율 주행 자동차 시스템이 개발되고 있다.[6)]

자율주행 기능을 지원하는 주요 ADAS 인식 센서 시스템은 대부분 2개 이상의 센서 기술의 결합으로 구성된다. 특히 ADAS는 카메라, 단거리/장거리 레이더, 라이다 등의 융합 센서로 발전되고 있다. 이러한 융합 센서는 각 센서의 부족한 부분을 서로 보완하며 자율 주행 자동차의 주변 상황을 인지하기 위해 활용될 수 있으며, 또한 고가의 고사양 센서를 대체할 수 있다.

향후 완전 자율 주행 자동차는 자율 주행 기능을 지원하는 ADAS 시스템들의 조합으로 구성되므로, ADAS 시스템에 대한 보안 연구는 완전 자율 주행 차량의 In-Vehicle 보안 연구에 있어 중요한 의미를 가진다. 자율 주행 기술이 발전함에 따라 센서와 시스템간의 복잡성은 지속적으로 증가할 것이며, 이를 제어할 수 있는 차량 내부 네트워크 시스템 발전 또한 함께 도모되어야 한다.

2.2.2 인지 기능

2016년 5월, 하얀 트레일러를 하늘로 착각해 발생한 테슬라 자율주행 자동차 사고와 같이, '인지-판단-제어 프로세스' 중 인지 기능에 미세한 오류가 발생한 경우 대형 인명 사고로 직결될 수 있다.[7)] 즉 자율 주행 자동차의 정확한 인지 기술이 선행되어야 완전한 자율 주행 환경의 구현이 가능하다.

앞서 언급한 카메라, 레이더 등의 ADAS 센서는 이러한 인지 능력을 향상시키는 보완재로서 자율주행 차량에 적용되고 있다. 그러나 차량의 사각 지대 및 악천후와 같은 상황으로 인해 실제 상용화 시 어려움이 따른다. 이처럼 측위 센서에 대한 한계가 부각됨에 따라 정밀지도를 통해 자율주행 차량의 기존 센서를 보완하여 오차 범위를 축소시키려는 연구가 진행되었다.

정밀지도는 주행 경로에 대한 상세한 정보를 사전에 제공하며, 따라서 주행 중 실시간으로 습득해야 하는 데이터 용량을 감소시켜 측위 센서에 대한 의존도를 경감시킬 수 있다.[8)] 즉 매우 적은 양의 센서 정보로도 자율 주행이 가능해질 수 있으며, 이를 통해 자율 주행 차량의 안정성 및 신뢰성을 높일 수 있다. 차량의 위치를 추정하는 측위 기술 또한 자율주행 자동차의 ADAS 시스템에 반드시 필요한 기술 중 하나이다. 센서 융합 기반의 정밀 측위 시스템은 기존 GPS와 함께 ADAS 센서(카메라, 레이더 등) 및 정밀 지도를 융합하여 자동차의 위치를 추정한다.

정밀지도 활용의 사례 중 하나인 구글의 자율주행 자동차는 관성항법과 더불어 Velodyne lidar의 Infrared reflectivity를 기반으로 생성한 정밀지도를 사용하고 있다.[8)] Google Car 상단에 달린 Velodyne lidar를 이용하여 Fig. 3의 좌하단과 같은 Infrared reflectivity를 얻고, 고가의 DGPS와 INS을 이용해 실시간으로 획득한 Infrared reflectivity와 비교하여 가장 잘 정합되는 위치를 차량의 위치로 추정한다.

지능형 교통체계인 ITS(Intelligent Transport System)의 도입은 자율주행 차량의 인지 능력 및 판단 알고리즘을 향상시키며, 센서 및 정밀 지도로 인지할 수 없는 사각지대에 대한 도로 상황 및 차량의 주행 정보를 인지하도록 한다. 차량의 통신 네트워크는 차량을 중심으로 내부망과 외부망으로 구분할 수 있다. 차량 내부망인 IVN(In-Vehilce Network)은 멀티미디어 기기 접속을 위한 MOST, ECU간 통신을 위한 CAN, 브레이크나 조향 장치 등을 제어하는 X-by-Wire 등이 있다. 차량 외부망은 차량 간 통신망

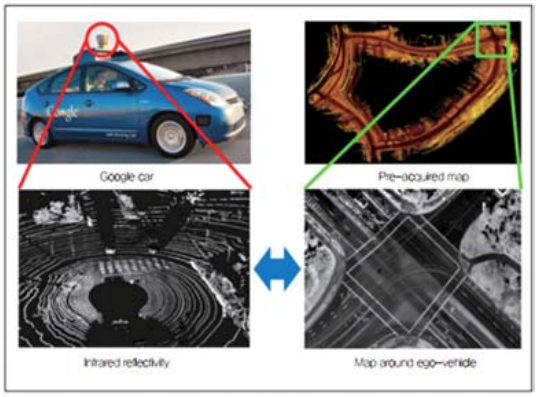


Fig. 3 Self-driving car of google

인 V2V, 차량과 인프라 통신망인 V2I, 그리고 차량과 사용자 단말 간 V2N으로 분류되며, 이를 통합하여 V2X라 부른다.[9)]

완전한 자율 주행 자동차의 개발을 위해서는 통신 네트워크 환경의 구축이 필수적이지만, 이는 해킹 공격을 가능하게 하는 수많은 경로를 제공할 수 있다. 따라서 자율 주행 차량의 발전과 더불어 V2X 통신의 보안 기술 및 보안 취약점에 대한 연구가 병행되어야 한다.

2.2.3 판단/제어 기능

자율주행을 위한 판단 기능은 SW를 통해 이루어지며, HW와 연계되어 자율 주행 차의 핵심적인 역할을 수행하게 된다. Fig. 4는 자율 주행 자동차에 장착될 수 있는 판단 및 제어 시스템의 데이터 흐름도이다.[10)]

GPS, 카메라, 레이더, 정밀 지도 등 앞서 언급한 인지 센서들은 특정 양의 전담 센서 프로세싱을 맡고 있으며, 수집된 정보는 다음 시스템 단계에서 Action angine에 의해 사용된다. 이를 위해 서로 다른 프로세싱에서 나온 센서들의 정보와 V2X 통신에서 비롯된 정보를 융합하게 된다.

지도 및 관련 클라우드 시스템은 추가 입력정보를 제공하며, 자율 주행 자동차는 모든 센서 블록에서 나온 출력 정보를 이용해 자율 주행 차량의 주변 환경에 대한 3D 정보를 생성한다. 생성된 3D 정보는 주행 상황을 판단하는 '행동 엔진' 소프트웨어에 의해 사용되어 전체 시스템에 의사결정을 내리게 된다.

제어 단계는 브레이크, 엔진 핸들 등의 조작을 말하며, 액츄에이터 모듈 내 HW 및 SW에 의해 동작된다. 제어 소프트웨어의 경우 오랜 기간 양상화 과정을 거치며 안정된 상태의 기술을 개발하고 있다.[11)] ESC, MDPS, 엔진 제어 시스템 등은 이미 양산 차량에 적용되고 있으며, 판단 단계의 명령에 따라 단순히 조절하는 기능을 수행하므로 기존 차량의 구현 방식과 크게 다르지 않다. 향후 센서 기술이 발전되고, 정보처리 양이 증가함에 따라 판단 소프트웨어가 자율주행 차량의 성능을 결정하는 차별화 요소가 될 것이라 전망한다.

3. 자율 주행 자동차 보안 취약점

차량에 ICT 기술이 도입됨에 따라 악성 바이러스 및 외부 해커에 의한 침입 우려가 높아지고 있다. 더

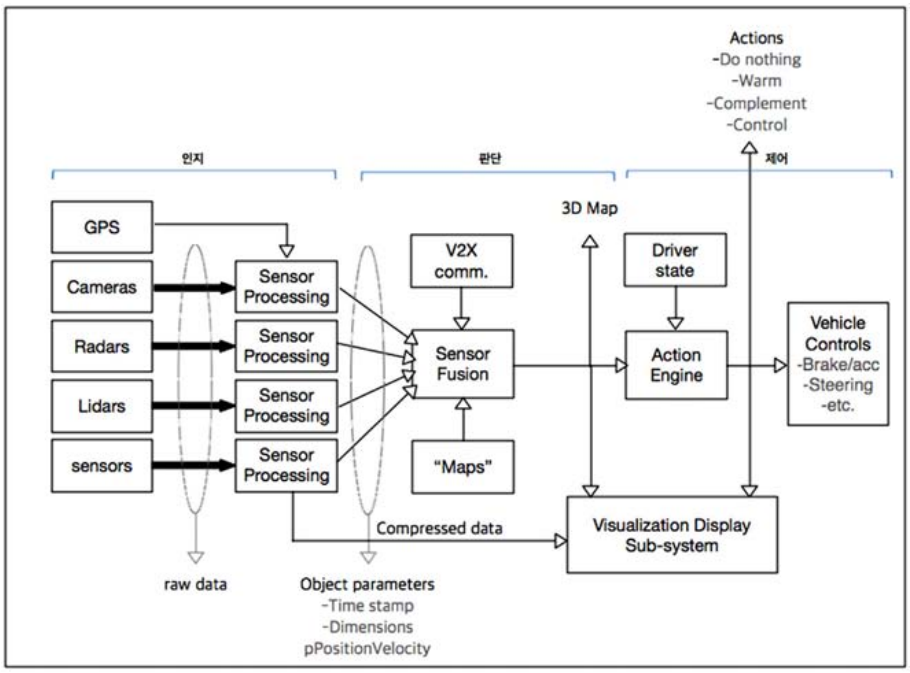


Fig. 4 Data flow diagram of self-driving car

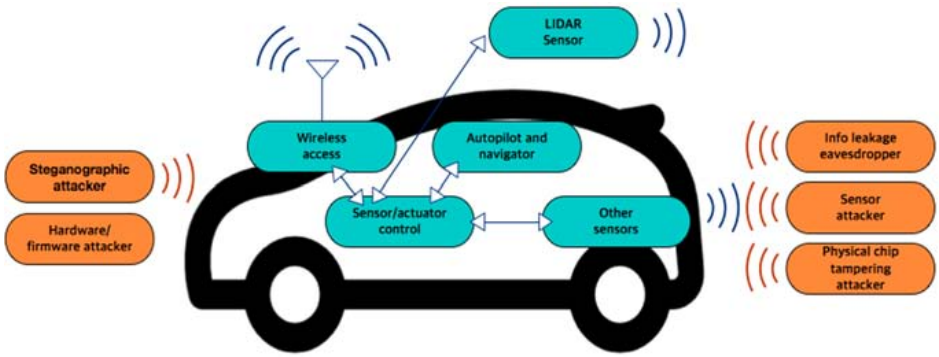


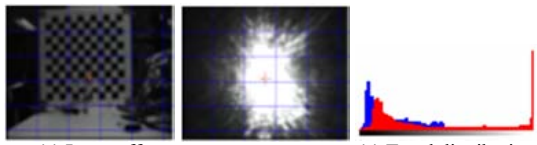
Fig. 5 Vulnerability of self-driving car

욱이 자율 주행 자동차의 경우, 차량 내부 및 외부에서의 대응방법이 함께 고려되는 등 지능형 차량의 통신 환경에 적합한 보안 기술이 요구되고 있다.[12] Fig. 5는 자율주행 자동차 내에서 발생할 수 있는 잠재적 취약점들을 보여주고 있다.[13] 그러나 인터넷 상의 임베디드 프로세스 간 정보 공유 기술의 경우 광범위한 연구가 진행되고 있는 반면, 자율주행 자동차에 대한 보안 기술의 연구는 미비한 실정이다.

3.1절부터 3.3절에서는 자율 주행 자동차의 보안 사고 사례 및 잠재적 취약점 소개를 통해 자율 주행 자동차의 보안 기술 발전에 대한 필요성을 논의한다.

3.1 자율 주행 자동차 근접 취약점

완전한 자율 주행 자동차의 단계에서는 다양한 센서 정보의 융합으로 안전한 주행을 위한 의사결정을 내리게 된다. 즉 센서 데이터를 저하시키는 모든 공격들은 운전자의 생명에 직결되는 보안 사고를 초래할 수 있다. Petit 등[14]은 가상의 공격자 및 도로 상황을 설정하고, 자율주행 차량에 탑재할 수 있는 MobileEye C2-270의 카메라와 ibeo LUX 3의 라이더에 대한 다양한 원격 공격을 시연하였다. 먼저 카메라 공격의 경우 광원, 광원과 카메라 사이의 거리, 환경(밝을 때/ 어두울 때)을 변수로 선정하고, 카메라에 빛을 가해 공격을 수행하여 가장 효과적인 공격의 조건을 도출하였다. 또한 공격자가 지속적으로 빛을 가할 경우 카메라의 자동 제어 기능은 각 프레임의 셔터 속도 및 전자 저하량 등을 조절하여 정상 상태로의 복구를 시도한다. Petit 등[14]은 이를 이용하여 자동 제어 기능에 혼란을 주고 자동복구를



(a) Laser off (b) Laser on (c) Tonal distribution

Fig. 6 Camera attack result

막을 수 있는 공격을 시연하였다. Fig. 6은 제안한 블라인딩 공격의 실험 결과로, 차량용 카메라에 빛을 가할 시 전방의 체스판을 인지하지 못하는 것을 볼 수 있다.

라이더 공격의 경우 신호가 반사되어 돌아오지 않으면 주변에 물체가 없다고 인지하며, 빛의 펄스만을 사용하기 때문에 공격에 매우 취약할 수 있다. 라이더에 대한 공격 목표는 가짜 객체 생성 및 Relay, Jamming, Spoofing 등의 공격을 수행하는 것이다. Petit 등[14]은 두 개의 송수신기를 위치하여 라이더에 의해 전송되는 동일한 전압 신호를 다른 위치에서 재전송하는 Relay 공격을 시연하였으며, 이를 통해 차량의 위치를 변조할 수 있는 것을 증명하였다. Fig. 7은 라이더의 Relay 공격에 대한 결과이다. 공격이 발생하기 전 라이더는 1 m 앞에 있는 벽(그림 하단의 작은 노란색 수평선)만 감지하는 반면, Relay 공격 수행 시 라이더는 20 m와 50 m 거리의 물체를 수신한다. 즉 이는 펄스를 조작하여 가짜 물체를 생성할 수 있는 것을 보여준다.

3.2 자율 주행 자동차 원격 액세스 취약점

자율 주행 자동차는 CAN 버스와 임베디드 프로세서 시스템을 통해 다른 차량 또는 다양한 인프라와

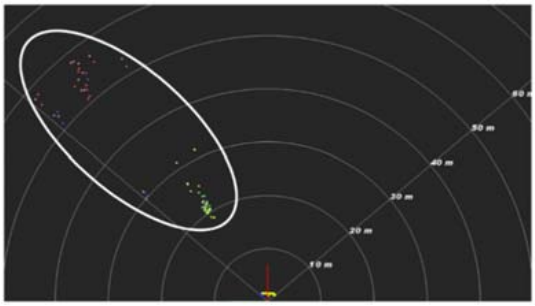


Fig. 7 Ridar attack result

의 무선 통신을 수행한다. 공격자는 차량에 탑재된 소프트웨어 및 펌웨어를 업데이트 하여 악의적인 코드를 삽입하거나, Dos 공격, 도청 등을 수행할 수 있으며 이는 협력 자율주행 환경에 혼란을 야기할 수 있다.

Ishtiaq Roufa 등[15]은 차량으로부터 약 40 m 거리에서 무선 네트워크로 통신하는 타이어 압력 센서 모듈 TPMS의 도청이 가능하다는 것을 증명하였다. 향후 다양한 자율 주행 기능을 지원하기 위해 필요한 전선이 증가함에 따라, 복잡한 전선 양을 줄일 수 있는 무선 통신에 대한 기술이 함께 발전할 것이다. 즉 TPMS와 같은 무선 통신에 대한 취약점 연구는 완전한 자율 주행 단계로 가기 위한 발판이 될 수 있다.

완전 자율 주행 기능의 단계에서는 협력 자율주행 환경을 위한 V2X 통신 보안 기술이 필수적으로 요구되고 있다. Fig. 8은 V2X의 데이터 라이프 사이클을 표현하고 있으며 이를 통해 차량 내부의 온보드 센서 공격을 포함한 전체적인 V2X의 공격자 모델을 도출할 수 있다.[16]

센서 데이터의 경우 차 내 ECU에 의해 처리되며 무선 통신 장치에 의해 다른 차량으로 전송된다. 이 단계를 Data in transit 이라 정의한다. 또한 사용자의 개인 정보 보호를 위한 메타 데이터가 센서 데이터

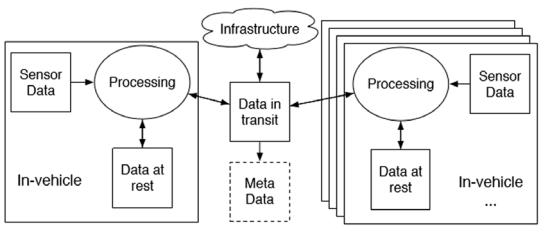


Fig. 8 Life-cycle of v2x data

TABLE I. ATTACKERS IN THE DATA LIFECYCLE

Data lifecycle	Sensor Confusion	Evil Mechanic	Communication
Data acquisition	✓		
Data processing		✓	
Data at rest		✓	
Data in transit			✓
Metadata			✓

Fig. 9 Attackers of v2x

에 추가되며, 인접 차량에서 수신한 데이터는 스택에 의해 처리, 저장 및 사용된다.

Fig. 9는 데이터의 라이프 사이클 내 공격자를 도출한 표이다. 공격자는 센서 데이터 융합 과정 시 혼란을 줄 수 있으며, 데이터 처리 및 저장 시 재밍 등의 물리적 공격을 수행할 수 있다. 또한 데이터 및 메타 데이터의 통신 과정에서 Spoofing, Dos 등의 공격이 가능하다. Petit 등[14]은 멀티 홉 방식의 V2X를 고려하지 않았으며, 초기 배치를 가정하고 단일 홉 방식의 V2X에 대한 취약점을 분석하였다. 향후 인프라 서비스와의 통신은 LTE 상의 IP와 같은 멀티 홉 방식의 라우팅 서비스 통신 채널을 통해 구성될 것이다.

3.3 자율 주행 자동차 물리적 취약점

다수의 ECU와 CAN 네트워크 및 차량에 탑재된 소프트웨어는 하드웨어 모듈을 공격할 수 있는 경로를 제공한다. CAN 네트워크에 대한 보안 취약점은 현재까지 활발히 연구되어 왔다. Wolf 등[17]은 공격자가 물리적 또는 논리적으로 차량에 접근할 수 있다고 가정하고, 차량 내 버스 시스템(LIN, CAN, MOST, FlexRay, Bluethooh)에 대한 공격을 시연하였다. 또한 Koscher 등[18]은 ECU에 침투할 수 있는 공격자가 운전자의 안전에 직결되는 시스템을 제어할 수 있으며 브레이크 고장, 휠 제어, 엔진 정지 등의 공격을 수행할 수 있는 것을 보여주었다. Checkoway 등[19]은 CD 플레이어, 블루투스 및 셀룰러 라디오 등의 원격 공격을 수행하였으며, 무선 통신 채널 공격의 경우 장거리에서 차량을 제어하거나 위치 추적, 오디오 도청 등이 가능한 것을 증명하였다. 향후 차량에 센서 융합 기능 및 V2X의 통신이 결합됨에 따라 자율 주행 차량에서의 물리적 취약점 및 내부 네트워크의 보안에 대한 연구가 활발히 이루어질 것이라 전망한다.

4. 자율 주행 자동차 In-Vehicle 보안 연구

자율주행 자동차의 외부 통신 및 인지 기술의 보안이 강화되더라도, In-Vehicle 제어 시스템이 취약할 경우 궁극적으로 심각한 안전사고를 일으킬 수 있다.

차량에 여러 IoT 전자 제어 장치가 탑재되며 차량 해킹 우려가 계속적으로 높아짐에 따라, 전자제어장치(ECU)로 하여금 자율적으로 해커로부터의 공격을 막을 수 있도록 하는 침입 탐지 시스템(IDS)의 연구가 활발히 이루어졌다. 예컨대 송현민 등[20]과 곽병일 등[21]은 CAN 메시지의 시간 간격 분석을 기반으로 차량 내부 네트워크의 침입 탐지 알고리즘을 제안하였으며, BI등은 차량 센서로부터 운전자의 운전 패턴을 분석하여 In-Vehicle 내 전자 장치 취약점을 악용하는 자동 도난 공격을 탐지할 수 있는 운전자 검증 방법을 제안하였다.

그러나 현재 상용화된 자동차가 아닌 자율 주행 자동차 내에서의 In-Vehicle 연구의 경우 추상적 형태로 인해 표면적인 연구만 이루어지고 있으며, 자세한 시나리오 및 실제 실험 연구가 부족한 실정이다. 다양한 센서들의 융합 정보로 작동되는 자율 주행 차량이라도 In-Vehicle 내에서의 공격이 일어난다면, 주행 상황과 맞지 않는 제어를 수행하여 심각한 안전사고를 일으킬 수 있다. 또한 운전자가 관여하지 않는 완전 자율 주행 단계에서는 악의적 공격 또는 안전사고가 발생하였을 시 실시간으로 대응하기 어렵다.

4.1절과 4.2절에서는 자율 주행 자동차의 In-Vehicle 시스템에 대한 공격 시나리오를 도출하고 이에 대한 대응책을 논의한다.

4.1 In-Vehicle 공격 시나리오

Fig. 10은 본 논문에서 제안한 완전 자율 주행 자동차의 가상 시스템에 대한 공격 시나리오를 보여준다. Action Engine은 Sensor Fusion을 통해 융합된 센서 데이터를 기반으로 적절한 의사 결정을 내려 자율 주행 차량의 시스템을 제어한다. 이 때 Action Engine의 Input 또는 Output을 조작하여 자율 주행 차량의 In-Vehicle 공격을 수행할 수 있다. 완전 자율 주행 단계에서의 In-Vehicle 프로토콜은 아직 규정되지 않았으므로 본 논문에서는 현재 상용화된 ADAS 시스템의 무선통신에 적용되고 있는 CAN 프

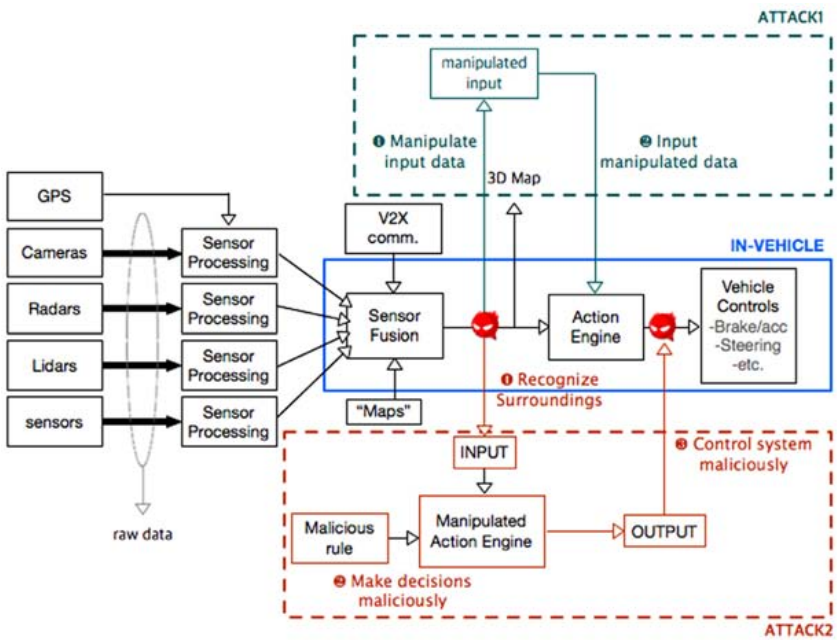


Fig. 10 Virtual attack scenario of self-driving car

로토콜로 가정한다. ADAS 센서 시스템은 수집된 아날로그 형식의 센서 데이터를 CAN 프로토콜로 변환하는 각 마이크로 컨트롤러를 가지고 있다.

ATTACK 1은 Action Engine의 Input 데이터를 변조하는 방법이다. 공격자는 Sensor Fusion으로부터 수집된 데이터를 변조하여 Action Engine에 입력한다. 변조된 데이터를 입력받은 Action Engine은 주행 상황과 맞지 않는 잘못된 시스템 제어를 수행하여 보안 사고를 발생시킬 수 있다.

ATTACK 2는 Action Engine의 Output 데이터를 변조하는 방법으로, Sensor Fusion으로부터 생성된 데이터를 도청하여 공격 차량의 주행 상황을 인지한 후 공격을 수행한다. 공격자는 기존의 Action Engine을 조작하거나, Sensor Fusion으로부터 생성된 데이터가 변조된 다른 Action Engine으로 우회하도록 하여 주행 상황과 맞지 않는 Output을 생성할 수 있다. 이 때 변조된 Action Engine의 경우 악의적 주행 판단을 수행하는 프로세스인 Malicious rule을 사용한다. 예컨대 Table 1과 같이 Malicious rule에 따라 In-Vehicle 시스템을 제어하여 경로 이탈, 제동 장치 이상, 비정상적인 차선 변경 등의 사고를 유발할 수 있다.

Fig. 10의 ATTACK 1과 같이 Sensor Fusion으로부터 생성된 데이터를 조작하는 것은 사실상 어렵다. 자율 주행 차량은 인지, 판단, 제어라는 단계적 모듈로 구성되며, 도로 상황, 차량 간 통신, 3D MAP 등의 정보를 융합하여 동작하게 된다. 공격자는 차량 내 탑재된 수많은 융합 센서들의 원리를 파악하여, 연관 관계가 맞도록 데이터를 조작해야 ATTACK 1과 같은 공격을 수행할 수 있다. 그러나 ATTACK 2는 In-Vehicle 내 판단 및 제어 시스템의 메시지를 조작하므로, 자율 주행 차량의 인지 기능과 관계없이 공격이 수행될 수 있다. 즉 In-Vehicle 시스템 공격자는 주행 상황을 인지하지 않아도 Dos 공격, Spoofing 공격 등을 통해 서비스 마비, 시간 지연 등을 발생시켜 올바른 주행 판단을 무력화할 수 있다.

Table 1 Malicious rule example

Cross track	Path / GPS / Steering angle / Wheel velocity
Break error	Brake switch / RPM / Straight radar
Abnormal lane change	Wheel velocity / RPM / Steering angle / Side sensor / Headlight

4.2 In-Vehicle 공격 탐지 시나리오

실 도로 상에서 주행하게 될 자율 주행 자동차의 안전성 검증을 위해서는 주행 시 발생할 수 있는 여러 상황에 대한 안전성 확보 및 평가 방안이 요구된다.[22] 이 중 자율 주행 자동차의 In-Vehicle IDS 연구는 CAN bus 내 제어 메시지만을 다루는 기존 CAN 프로토콜의 IDS와는 확연히 다른 방향으로 연구되어야한다. Table 2는 도로 위에서 발생할 수 있는 차량 상황을 기술한 표이다. 공격자는 융합 센서로부터 얻은 차량 상황 정보와 맞지 않는 잘못된 차량 동작(직진/감속/가속/정차/후진/추월/차선 변경/좌,우회전/커빙 등)을 수행하여 안전사고를 유발할 수 있다. 따라서 차량 상황을 나타내는 센서 데이터와 판단 프로세스에 의해 생성되는 제어 메시지를 비교하여, 차량 상황에 맞는 제어 메시지가 수행되는 지를 탐지할 수 있는 IDS 시스템이 구현되어야 한다. 예컨대 특정 상황을 나타내는 융합 센서 정보와 맞지 않는 제어 메시지가 발견될 경우, 이를 이상 징후라 판별할 수 있다.

본 논문에서는 자율 주행 환경에서 발생할 수 있는 도로 상황과, 해당 상황과 관련된 제어 시스템을 분석하여 향후 자율주행 차량의 IDS rule로 활용할 수 있는 다양한 시나리오를 도출한다.[23]

Table 2 Surroundings of road

Vehicle situation	Explain
Road classification	Expressway/downtown road etc.
Road condition	Dry/wet/icy road etc.
Road shape (horizontality)	Straight/the left/the right /curved road etc.
Road shape (verticality)	Flatland/uphill/downhill road etc.
Climate and visibility	Low/high/normal intensity of illumination etc.
Average vehicle speed	Low(-15)/normal(15-45)/ high medium(45-80)/high(80-) speed etc.
Objects arround	The front/the real vehicle /bicycle/infra/pedestrian/hole etc.

4.2.1 SCENARIO 1

도로 형상에 따라 다양한 주행 상황이 발생할 수 있다. Fig. 11과 같이 커브 길을 주행하는 자율 주행 차량의 전방 센서가 다른 차선의 차를 잘못 인식하거나 커브로 인해 전방 차량을 인지하지 못해 충돌이 발생할 수 있다. 따라서 자율 주행 차량은 차선 인식 시스템, 전방 카메라 및 센서, 3D MAP 등의 정보를 융합하여 커브 길을 인지하고, 차량의 RPM, 속도, 휠 각도, 조향각, 전방 센서 각도 등을 조정하여 안전한 자율 주행 기능을 지원해야 한다. 앞서 언급한 것과 같이, 커브 길이라는 차량 상황과 맞지 않는 제어 메시지가 발견될 경우, 이를 이상 징후로 판별한다.

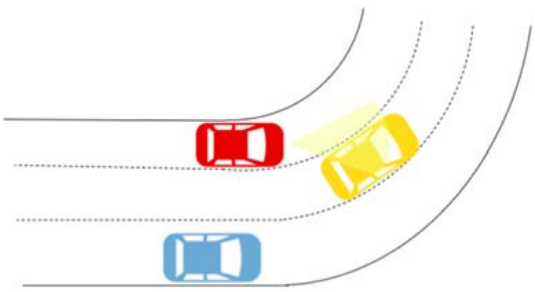


Fig. 11 Scenario 1

4.2.2 SCENARIO 2

자율 주행 차량이 주변 물체를 인지하지 못할 경우, 심각한 인명 피해가 발생할 수 있다. Fig. 12와 같이 자율주행 차는 전방 센서, 앞 차량의 속도 및 전조등(V2X 통신), 앞 차량의 후방 센서 등을 통해 전방 차량을 인지한다. 또한 속도, RPM, 전조등, 조향각, 휠 각도 등을 제어하여 적절한 안전거리를 유지해 전방 차량과의 충돌을 방지한다. 그러나 '전방 차량이 있는'상황에서 차량 조명이 급격히 변화할 경우 전방 센서 또는 앞 차량의 후방 센서가 올바르게 작동하지 않을 수 있다. 앞서 자율주행 자동차의 근접 취약점 중 빛을 가하여 센서를 무력화 한 Petit 등[14]의 실험 결과와 같이, 공격자는 In-Vehicle 시스템 내 전조등을 제어하여 시스템의 오작동을 일으킬 수 있다. 따라서 전방 차량이 있을 때 급격한 전조등 변화가 일어나거나, 적합하지 않은 속도 등의 제어 메시지가 발견될 경우, 이를 이상 징후로 판별할 수 있어야 한다.

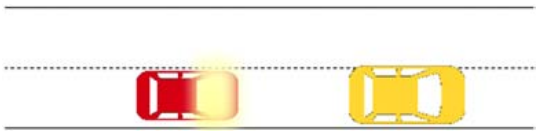


Fig. 12 Scenario 2

4.2.3 SCENARIO 3

빙판 길, 빗길 등의 노면 조건 및 악천후의 상황 등은 자율주행 환경에서 수많은 변수를 제공한다. 자율 주행 차는 온도 및 습도 센서를 통해 노면 상태를 측정하여 차량 상황에 맞는 주행 판단을 내릴 수 있어야 한다. Fig. 13과 같이, 차량이 젖은 노면에서 주행할 경우, 물속의 타이어 궤적을 차선으로 잘못 인식하여 잘못된 차선 변경을 수행할 수 있다. 또한 도로에 습기가 많을 경우에도 차선을 인식하지 못할 가능성이 있다.

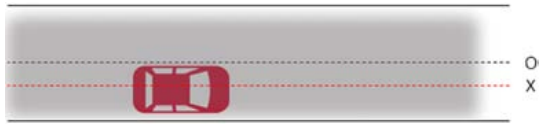


Fig. 13 Scenario 3.1

빙판길의 경우, Fig. 14와 같이 전방 센서에 의해 감지된 제동 거리의 범위를 넘어설 수 있다. 자율 주행 차는 악천후거나 도로 상태가 좋지 않은 상황을 인지하여 속도를 낮추거나 제동 거리를 늘리는 등 안전한 주행을 지원해야 한다. 만약 속도 증가, 급격한 휠 각도 등 노면 조건 및 기후에 맞지 않는 제어 메시지가 발견될 경우, 이를 이상 징후로 판별하여 안전사고를 예방한다.

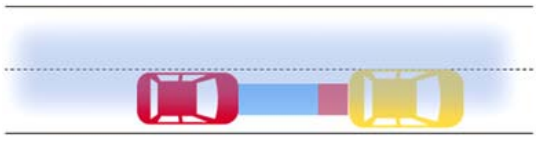


Fig. 14 Scenario 3.2

5. 자율 주행 자동차 보안 요구 사항

현재 상용화된 자동차 내 애플리케이션은 CAN, FlexRay, LIN으로 연결되어 있으며, 이 중 CAN은 차량 통신 분야에서 가장 대중화된 프로토콜이라

볼 수 있다.[24] 그러나 CAN의 경우 보안에 대한 고려 없이 설계 된 프로토콜로, 자율 주행 환경에서의 보안 메커니즘을 적용하기에는 여러 문제가 따른다. 예컨대 CAN은 송신 장치에 대한 정보를 갖지 않는 브로드 캐스트 방식이므로, Spoofing 공격이나 CAN 버스를 통해 ECU에 접근하는 것이 매우 용이하다. CAN의 보안 위협에 대응하기 위해선 메시지 인증 코드를 사용하거나 ECU 그룹을 관리할 수 있는 암호학적 알고리즘의 결합 등이 수행되어야 한다. 그러나 제한된 메시지 길이에 따른 용량 부족, 단방향 통신으로 인한 송신자의 정보 부재, 실시간 연산 처리 문제 등 기존 CAN 프로토콜의 보완을 통해서도 해결할 수 없는 한계점이 존재한다.

자율 주행 자동차는 ITS 환경을 구축할 수 있도록 내부 통신 하드웨어의 보안과 더불어 무선 통신용 하드웨어의 보안, 통합형 보안 마이크로 컨트롤러 등의 개발이 요구된다. 즉 센싱 - 판단 - 제어로 모듈화 된 자율 주행 시스템 및 V2X 통신 시스템을 모두 포괄할 수 있는 새로운 보안 기술의 연구가 필요하다.

Fig. 15는 자율 주행 자동차의 5가지 구성 요소에 따른 보안 요구사항으로, 외부 환경과의 인터페이스, 게이트웨이, ECU 간 네트워크, 판단 SW가 탑재된 MCU/MPU, 차량에 접근을 허용하는 모든 애플리케이션으로 구성된다.[25] 외부 환경과의 인터페이스의 경우 기존 통신 규격과는 다른 새로운 프로토콜 규격에 대한 연구가 이루어져야 하며, 대표적으로 IEEE 1609에서는 ITS 환경의 통신에 적합한 프로토콜인 WAVE의 표준화를 진행 중이다.[26]

Table 3과 같이, IEEE1609.2에서는 보안 메시지 규격과 보안 통신을 위한 처리 절차를 기술하고 있다. 물리계층인 IEEE 1609.2 기술 규격은 100 msec마다 차량 상태 정보 메시지를 교환하도록 규정하고 있으며, 디지털 서명 기술의 경우 차량 통신 환경에 적합한 타원 곡선 암호를 기반으로 정의하고 있다. 이와 같이 자율주행 자동차의 보안을 위해서는 하드웨어 기반의 고속 암호화 기술이 개발되어야 한다.[27]

IEEE 1609.2 규격에서는 프라이버시 보호를 위한 인증 기술이 정의되어 있지 않지만, 향후 자율 주행

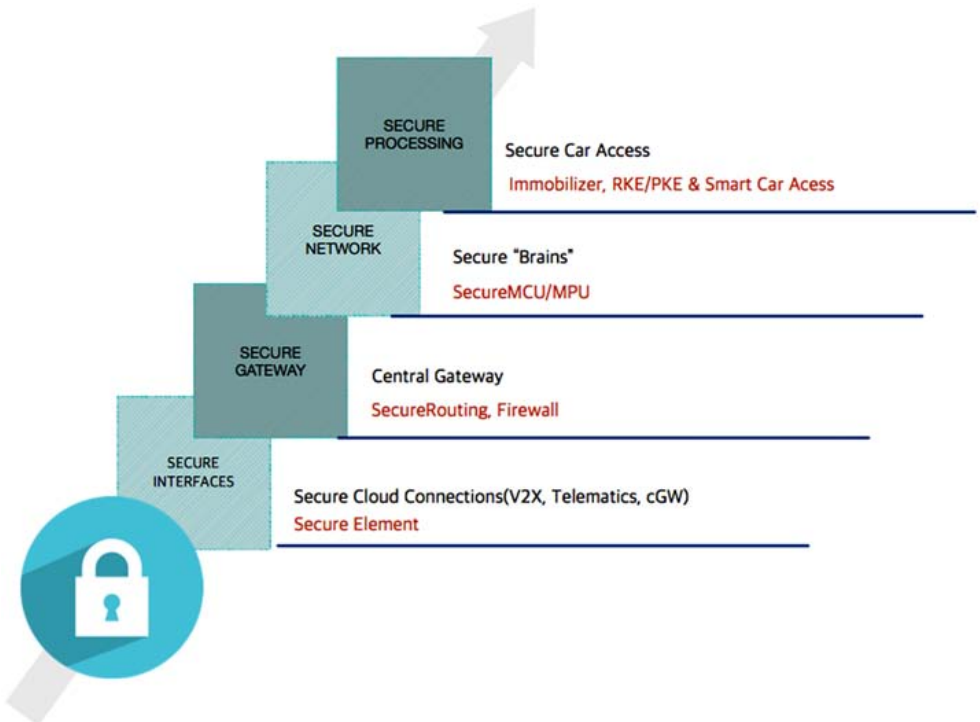


Fig. 15 Security of requirement for self-driving car

Table 3 Standardization of wave

Number	Title
IEEE 1609.0	Architecture
IEEE 1609.1-2006	Resource manager
IEEE 1609.2-2013	Security services for applications and management messages
IEEE 1609.3-2010	Networking services
IEEE 1609.4-2010	Multi-channel operation
IEEE 1609.11-2010	Over-the-airelectronic payment data exchange protocol for intelligent transportaion systems(ITS)

자동차의 상용화를 위해서는 운전자의 프라이버시 보호 연구가 선행되어야 하므로, 차량 통신 환경에 적합한 프라이버시보호형 인증 기술 또한 요구된다.[28)]

앞서 설명한 공격 시나리오인 Fig. 10에서 Sensor Fusion으로부터 내부 하드웨어인 Action Engine까지의 통신 과정은 향후 무선 통신으로 통합되어 발전할 가능성이 높다. 무선 통신 시스템의 한 사례로 여러 센서(압력 온도, 가속도 등)의 입력 값을 융합하여 전처리 과정 후 MCU로 전송하는 TPMS 시스템이 있다.[29)] 완전 자율 주행 자동차는 무선 통신을 지원하는 ADAS 시스템의 조합으로 구성될 수 있으므로, 차량 내 ECU나 통신 인터페이스의 무결성을 보장할 수 있는 하드웨어 안전 모듈(HSM)의 탑재가 필수적으로 요구된다.

본 논문에서는 자율 주행 환경에서 발생할 수 있는 안전사고에 관한 시나리오를 도출하고 이에 대한 대응 방안을 논의하였다. 앞으로 자율 주행 환경이 도래함에 따라 본 논문의 일부 시나리오를 포함한 무수히 많은 안전사고가 발생할 수 있다. 다양한 공격 요인들을 고려하여 수많은 주행 상황에 대해 스스로 올바른 판단을 내릴 수 있을 경우 '자율 주행 차량은 충분히 안전하다'고 간주할 수 있지만, 궁극적으로 완전 자율 주행 단계에서의 정확도를 99.99 %로 만드는 작업은 매우 어렵다. 따라서 자율 주행 차량 기능에 운전자의 피드백을 결합시키는 Human-in-the-loop 패턴을 도입할 필요성이 있다. 테슬라는 최근 Human-in-the-loop 패턴을 따르는 자율 주행 테스트를 수행하고 있다.[29)] 즉, 자율 주행 환경에서 운전자가 스티어링 휠을 쥐고 있다고 가정하며, 이는 99.99 %의 안정성을 보장할 수 없는 자율 주행 차량의 안전을 위한 해결책이 될 수 있다.

6. 결 론

ICT 기술의 도입으로 인해 사용자의 편의성 및 안전성을 증가시킬 수 있는 자율 주행 자동차에 대한 관심이 고조되고 있다. 그러나 자율 주행 자동차의 보안 사고는 인명사고로 직결될 수 있으며, 이에 따라 자율 주행 자동차의 보안 연구의 필요성이 대두되고 있다. 국내외 수많은 IDS 시스템에 대한 연구 및 V2X 무선 통신 보안에 대한 연구가 활발히 진행되고 있지만, 다양한 센서 기능을 탑재한 자율 주행 차량의 In-Vehicle 시스템 보안에 대한 연구는 미비한 상황이다. 본 논문에서는 자율주행 자동차 기술에 대한 개괄적인 소개 및 자율 주행 자동차의 보안 취약점에 대해 간략히 살펴보았으며, 다양한 시나리오를 도출하여 자율 주행 자동차의 In-Vehicle 공격 및 탐지 방안에 대해 논의하였다. 향후 본 논문에서 제시한 다양한 시나리오를 아우를 수 있는 자율 주행 자동차의 보안 기술이 개발된다면, 완전한 자율 주행 환경은 더 이상 먼 미래가 아닌 현실이 될 것이라 기대한다.

References

1) IHS Markit, IHS Clarifies Autonomous Vehicle Sales Forecast, http://news.ihsmarkit.com/press-release/automotive/autonomous-vehicle-sales-set-reach-21-million-globally-2035-ihs-says, 2016.
2) ABI Research, Autonomous Behicles, https://www.abiresearch.com/market-research/product/1016486-autonomous-vehicles/, 2013.
3) M. Nukala, A Constellation of Innovations is Needed for Autonomous Driving…, https://medium.com/@murthynukala/a-constellation-of-innovations-is-needed-for-autonomous-driving-4b3cf6f98148, 2016.
4) S. R. Kang, KERI Brief, Status and Improvement of Legal System of Autonomous Vehicles, 2016.
5) LG Innotek, World of the Autonomous Car, http://blog.lginnotek.com/549, 2016.
6) FESCARO, Trends of the Autonomous Car,

http://www.fescaro.com/2016/11, 2016.
7) C. Thompson, New Details about the Fatal Tesla Autopilot Crash Reveal the Driver's Last Minutes, http://www.businessinsider.com/details-about-the-fatal-tesla-autopilot-accident-released-2017-6, 2017.
8) J. K. Suhr, J. G. Jang, D. H. Min and H. G. Jung, "Sensor Fusion-based Precise Vehicle Localization System," KSAE Annual Conference Proceedings, 2015.
9) M. Wolf, A. Weimerskirch and T. Wollinger, "State of the Art: Embedding Security in Vehicles," EURASIP Journal on Embedded Systems, 2007.
10) F. Mujica, Scalable Electronics Driving Autonomous Vehicle Technologies, Texas Instruments White Paper, 2014.
11) Korea Investment & Securities, Frenemies of the Autonomous Car, 2016.
12) B. I. Kwak, M. R. Han, A. R. Kang and H. K. Kim, "A Study on Detection Methodology of Threat on Cars from the Viewpoint of IoT," Journal of the Korea Institute of Information Security & Cryptology, Vol.25, No.2, pp.411-421, 2015.
13) A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth and K. Venkatasubramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," IEEE Micro, Vol.33, No.1, pp.80-86, 2013.
14) J. Petit, B. Stottelaar, M. Feiri and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and Lidar," Black Hat Europe, 2015.
15) R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb and I. Seskarb, "Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study," 19th USENIX Security Symposium, pp.11-13, 2010.
16) J. Petit, M. Feiri and F. Kargl, "Revisiting Attacker Model for Smart Vehicles," Wireless Vehicular Communications(WiVeC), pp.1-5, 2014.
17) M. Wolf, A. Weimerskirch and T. Wollinger, "State of the Art: Embedding Security in Vehicles," EURASIP Journal on Embedded Systems, 2007.
18) K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway and S. Savage, "Experimental Security Analysis of a Modern Automobile," IEEE Symposium on Security and Privacy(SP), 2010.
19) S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," Proceedings of USENIX Security, 2011.
20) H. M. Song, H. R. Kim and H. K. Kim, "Intrusion Detection System based on the Analysis of Time Intervals of CAN Messages for In-vehicle Network," International Conference on Information Networking(ICOIN), 2016.
21) B. I. Kwak, J. Woo and H. K. Kim, "Know Your Master: Driver Profiling-based Anti-theft method," Privacy, Security and Trust, 2016.
22) H. S. Chae, Y. W. Jeong, K. S. Yi, I. S. Choi and K. C. Min, "Safety Performance Evaluation Scenarios for Extraordinary Service Permission of Autonomous Vehicle," Transactions of KSAE, Vol.24, No.5, pp.495-503, 2016.
23) MyCarDoesWhat, Deeper Learning, https://mycardoeswhat.org/deeper-learning//adaptive-cruise-control/, 2017.
24) A. Hafeez, H. Malik, O. Avatefipour and P. Rongali, "Comparative Study of CAN-Bus and FlexRay Protocols for In-Vehicle Communication," SAE 2017-01-0017, 2017.
25) Extremetech, Qualcomm May Acquire NXP Semiconductor in $30 Billion Deal, https://www.extremetech.com/electronics/236599-qualcomm-may-acquire-nxp-semiconductor-in-30-billion-deal, 2016.
26) Intelligent Transportation Systems Committee, IEEE Standard for Wireless Access in Vehicular Environments-security Services for Applications and Management Messages, 2013.
27) Korea Communications Agency, Trends and Prospects of Vehicle Communication Security Technology in Intelligent Transportation System, 2014.

28) Business Wire, Freescale Introduces World's Smallest Integrated Tire Pressure Monitoring System, http://www.businesswire.com/news/home/20141020005220/en/ Freescale-introduces-world's-smallest-integrated-tire-pressure, 2014.

29) A. Marshall, Tesla Bears Some Blame for Self-driving Crash Death, Feds Say, Wired, https://www.wired.com/story/tesla-ntsb-autopilot-crash-death/, 2017.