정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

# 자율 주행 자동차 보안 위협 및 기술 동향

권 순 홍*, 이 종 혁*

요 약

IT 기술을 차량에 적용하여 사람의 조작 없이 차량 스스로 운행하는 자율 주행 자동차에 대한 연구가 활발하게 진행되고 있으며 상용화 및 대중화에 집중하고 있는 추세이다. 자율 주행 자동차의 경우, 보안 취약점을 통한 공격을 통해 오류를 발생시킬 경우, 운전자 또는 보행자에게 직접적인 해를 끼칠 수 있어 보안 취약점 및 보안 기술에 대한 연구는 자율 주행 자동차 상용화 및 대중화에 있어 핵심적인 부분이라고 할 수 있다. 본 논문에서는 현재 자율 주행 자동차의 기술 단계와 작동 원리에 대해 설명하며, 자율 주행 자동차의 보안 위협 요소를 살펴보고, 보안 위협으로부터 운전자 또는 보행자를 보호할 수 있는 보안 기술 현황에 대해 설명한다.

## Ⅰ. 서 론

IoT 기술의 발전을 기반으로 우리의 삶의 질은 더더욱 향상되고 있으며, IT 기술을 차량에 적용하여 사람의 조작없이 차량 스스로 운행하는 자율 주행 자동차가 개발되어 운전자로 하여금 편리성을 증대시켰다. 자율 주행 자동차 시장은 매년 증가하고 있는 교통 사고의 감소, 운전에 대한 접근성, 차량 운행 중 차내에서 다양한 업무 가능, 자율적인 교통 흐름 파악으로 인한 원활한 이동 가능등의 장점으로 인해 매년 확대되고 있는 추세이다. Gater.Inc에 따르면 2023년까지 운전자 또는 승객의 감독없이 자율 주행을 가능하게 하는 하드웨어가 장착된 차량은 2018년 137,129대에서 745,705대에 도달할 것이고, 2019년에는 332,932대에 이를 것이라고 예상하였다 [1].

이와 같이 자율 주행 자동차의 등장으로 제조사 및 ICT 기업들은 자율 주행 자동차 시장에 참여하여 상용화를 위해 자율 주행 자동차 사용 중 발생할 수 있는 보안 위협으로부터 운전자 및 보행자를 보호할 수 있는 보안 기술을 연구하고 있다. 자율 주행 자동차 보안 사고의 경우, 물리적인 피해뿐만 아니라 운전자 및 보행자에게 직접적인 해를 가할 수 있기 때문에 자율 주행 자동차 대중화에 있어 자율 주행 자동차 보안 기술은 핵심 기술이라고 말할 수 있다 [2]. 본 논문에서는 지속적으로 개발되고 있는 자율 주행 자동차 기술 동향에 대해 확인하며, 자율 주행 자동차에서 발생하고 있는 보안 위협과 보안 위협으로부터 안전한 자율 주행 자동차를 위한 보안 기술 동향에 대해 설명한다.

본 논문의 구성은 다음과 같다. 2장에서는 자율 주행 자동차 기술 동향에 대해 설명한다. 3장에서는 자율 주행 자동차에서 발생하고 있는 보안 위협에 대해 설명하며, 4장에서는 자율 주행 자동차에 적용되어 있는 보안 기술에 대해 설명한다. 마지막으로 4장에서는 본 논문의 결론을 맺는다.

## Ⅱ. 자율 주행 자동차 동향

### 2.1. 자율 주행 자동차 기술 단계

자율 주행 자동차는 자동차 관리법 제 2조 제1호의 3에 따라 ‘운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차’로 정의된다 [3]. 자율 주행 자동차의 개발 단계의 경우, 운전자 주행 개입에 따라 SAE에서 정의하고 있는 자율 주행 자동차 기술 6단계를 기준으로 분류하고 있다. SAE에서 정의하고 있는 자율 주행 자동차 기술 6단계의 경우, [표 1]과 [그림 1]을 통해 확인할 수 있다 [6]. [표 1]과 [그림 1]을 통해 확인할 수 있듯이, 레벨 0~2단계의 경우, 자율 주행 시스템에 온전히 주행을 맡기는 것이 아닌 운전자가 급작스러운 상황에 적절하게 대응하는 것을 요구하고

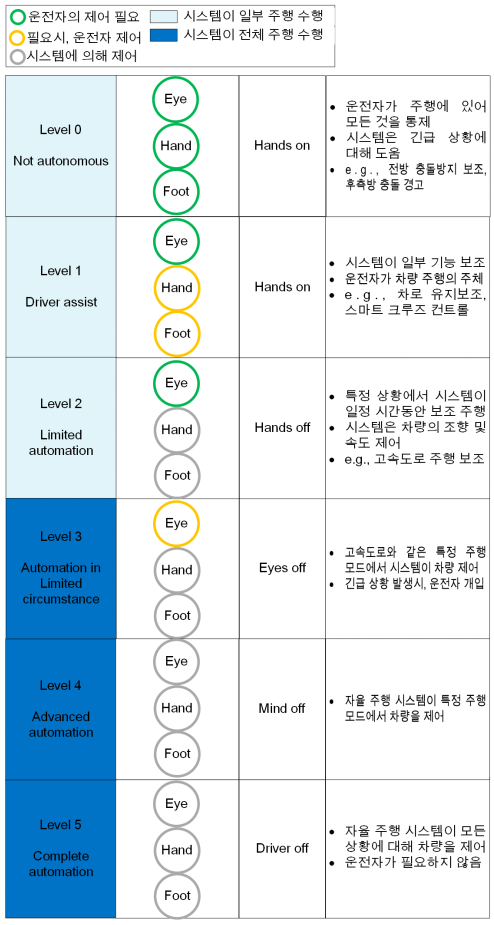
* 세종대학교 정보보호학과 프로토콜공학 연구실(대학원생, soonhong@pel.sejong.ac.kr, 부교수, jonghyouk@sejong.ac.kr)

〔표 1〕 자율 주행 자동차 발전 단계(SAE)

| 단계 | 설명 | 주행 제어 주체 | 차량 운행 주체 |
|---|---|---|---|
| 00 | 주행에 있어 운전자가 모든 것을 통제 | 인간 | 인간 |
| 01 | 주행에 있어 시스템이 일정 부분 개입 속도 유지, 차간거리 유지, 차선 유지등 | 인간 및 시스템 | 인간 |
| 02 | 특정 상황에서 시스템이 일정 시간동안 보조 주행 특정 상황 발생시, 운전자가 즉시 개입 | 시스템 | 인간 |
| 03 | 고속도로와 같은 조건에서 시스템이 자율 주행 특정 상황 발생시, 운전자가 즉시 개입 | 시스템 | 인간 |
| 04 | 제한된 상황을제외한 대부분의 도로에서 시스템이 자율 주행 | 시스템 | 시스템 |
| 05 | 탑승자는 목적지만 입력 후, 시스템이 자율 주행 | 시스템 | 시스템 |

있으며, 이러한 급작스러운 상황에 대해 시스템에서 대응해주는 기술의 경우, 레벨 3~5단계로 정의되어 있다. 현재 자동차 산업에서 자율 주행 자동차 상용화를 위해 개발하고 있는 제품군들은 시스템이 운전자의 주행 관련 조작까지 담당하는 ADAS(Advanced Driver Assistance System) 기능을 다수 결합하여 사람이 주행 환경을 모니터링해야하는 레벨 2 제품군과 사람이 아닌 자율 주행 시스템이 주행 환경을 모니터링하는 레벨 3 제품군이다. 현재 자율 주행 자동차는 레벨 3을 완성해가고 있으며, 2019년 아우디는 시속 60km 범위 내에서 레벨 3의 자율 주행이 가능한 5세대 A8을 유럽 내에 출시하였으며, 포드와 볼보의 경우, 레벨 4 자율 주행 시스템에 초점을 맞춰 개발 진행 중에 있다 [4].

앞서 언급한 바와 같이, 자율 주행 자동차의 경우, ADAS와의 결합 정도에 따라 6단계로 자율 주행 자동차를 분류하고 있다. ADAS는 첨단 감지 센서와 GPS, 통신, 지능형 영상 장비를 이용하여 자율 주행 중 발생할 수 있는 예외 상황에 대해 차량 스스로 상황에 대해 인지하고, 상황에 알맞은 행동을 판단하여 시스템이 자동차를 제어하거나 운전자에게 위험 요소에 대해 파악할 수 있도록 알려주는 운전자 보조 시스템이다. ADAS의 주요 기능은 주행 시 운전자에게 주변 환경에 대해 인지하도록 만들어주는 보조 역할을 수행한다

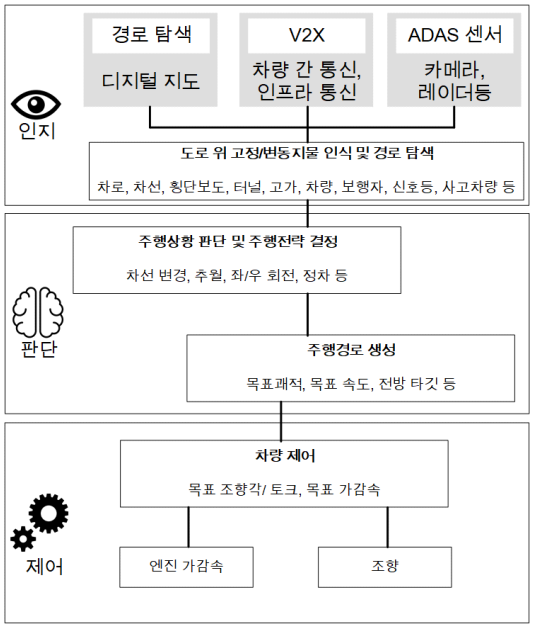



〔그림 1〕 자율 주행 단계에 따른 운전자 개입

(e.g., 적응형 크루즈 컨트롤, 차선 유지/변경 보조 시스템, 주차 조향, etc.). ADAS의 기능은 레벨 5단계 자율 주행 자동차를 위한 핵심적인 기술이며, 자율 주행 자동차의 주행 중 운전자의 안전과 보안을 위해 차량 주변에서 발생할 수 있는 예외 상황에 대해 적절히 대응할 수 있는 구현이 요구된다 [5].

## 2.2. 자율 주행 자동차 원리

자율 주행의 기본 원리는 인지, 판단, 제어를 통해 이루어진다. 인지 기술은 자율 주행 자동차가 스스로 교통 상황이나 운행 환경등 주변 환경을 파악하고, 적절하게 대응할 수 있게 하는 단계로서, GPS, 카메라, 레이더등을 이용하여 현재의 주행 환경 정보에 대해 인식하고 수집하는 단계이다. 판단 기술은 인지 기술을




〔그림 2〕 자율 주행 자동차의 작동 원리

통해 수집한 주행 환경 정보를 기반으로 자율 주행 자동차 스스로 가장 적절한 결정을 수행하는 단계로서, 인지 기술과 연관되어 두 기술의 조화 정도에 따라 자율 주행의 완성도가 결정된다. 제어 기술은 인지 기술과 판단 기술을 기반으로 하여 특정 주행 상황에 따라 자율 주행 자동차 스스로 엔진 구동이나 주행 방향등을 결정하여 사고 예방 및 안전 운전을 수행하는 단계이다. 다음 [그림 2]를 통해 자율 주행 자동차의 작동 원리를 파악할 수 있다 [5]. 다음으로 각 기술의 작동 원리와 보안 관점에서 기술의 중요성에 대해 설명한다.

### 2.2.1. 인지 기술

자율 주행 자동차에서 인지 기능은 인간의 눈의 역할을 수행한다. 우리는 주변 환경에 대해 눈을 통해 각종 정보를 보고 받아들인다. 이처럼 자율 주행 자동차 역시 차량에 부착된 카메라, 레이더, 라이다와 같은 ADAS 센서를 통해 주변 환경을 인식하고, 각종 정보를 수집한다. 인지 기술은 자율 주행 자동차의 가장 중요한 기술로서 꼽을 수 있다. 2018년 3월 미국 애리조나에서 우버 자율 주행 자동차가 길을 건너던 사람을 다른 차로 인식하여 치어 숨지게 한 사건과 같이 인식 기술의 오류는 사람에게 직접적인 해를 가할 수 있다. 즉, 자율 주행 자동차가 상용화 및 대중화가 되기 위해서는 정확히 주변 환경에 대해서 인식할 수 있는 인지 기술이 요구되어진다.

사람의 경우, 눈 앞에 장애물을 보면 직관적으로 종류를 구분할 수 있지만, 카메라, 레이더, 라이다와 같은 ADAS 센서의 경우에는 차량의 사각지대, 역광과 같은 자연적인 문제로 인해 사람, 동물, 생물과 무생물을 구분하는 능력이 떨어져 여전히 문제로 인식되고 있다. 이러한 측위 센서의 오차를 줄이기 위한 연구도 지속적으로 진행되고 있으며 도로와 주변 지형의 정보를 담아 지형 및 지물에 대해 오차범위 10~20cm 이내에서 식별할 수 있는 정밀 지도를 이용하여 이를 보완하고자하였다. 정밀 지도를 통해 자율 주행 차량의 오류 감소, 자율 주행 차량의 AI 학습 능력 향상, 실시간 분석해야 하는 데이터 용량 감소, 친환경성 향상 및 배터리 효율 관리 지원, 정적 정보와 동적 정보 제공등의 이점을 얻을 수 있다 [7].

현재에는 센서 융합 기반의 정밀 측위 시스템은 기존의 위성 정보를 활용하는 GPS 방법과 ADAS 센서 및 정밀 지도 기술을 융합하여 자차의 위치를 추정한다 [8]. 이와 같은 센서 융합 기반의 정밀 측위 시스템은 다임러의 자율 주행 자동차를 통해 예로서 설명이 가능하다. 다임러의 자율 주행 자동차의 경우, 위성 정보를 활용하는 전파 항법, 관성 항법과 스테레오 카메라와 사전에 생성한 정밀 지도를 사용한다. 다임러는 자차의 위치를 추정하기 위해 스테레오 카메라, DGPS(Differential GPS)와 INS(Inertial Navigation System)를 기반으로 생성한 차선 수준 지도와 특징 수준 지도를 사용한다. 스테레오 카메라를 통해 획득한 차선 정보와 차선 수준 지도에 존재하는 차선 정보를 비교한 결과와 후방 카메라에서 취득한 특징 정보와 특징 수준 지도에 저장되어 있는 특징 정보를 비교한 결과를 결합하여 현재 자율 주행 자동차의 위치를 추정한다 [8].

ADAS 그리고 정밀 지도를 통해 주변 환경을 인식하는 방법와 함께 V2X(Vehicle to Everything)를 활용하여 주변 환경을 인지한다. 차량의 통신 네트워크는 크게 내부망과 외부망으로 분류가 가능하며 차량 내부망인 IVN(In-Vehicle Network)은 엔진 제어기(ECU), 변속 제어기(TCU), 브레이크 제어기(BCU)를 위한 CAN, 브레이크, 조향 장치등을 제어하는 X-by-Wire,

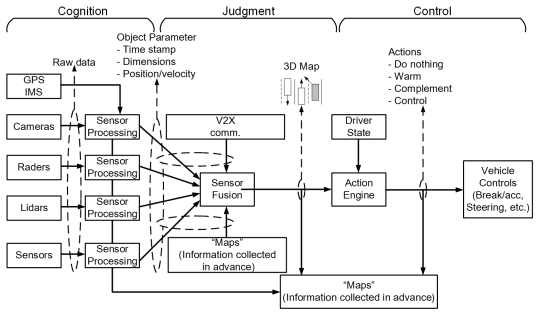
MOST, LIN, FlexRay 등이 있다. 차량 외부망은 V2V(Vehicle to Vehicle), V2I(Vehicle to Infra), V2P(Vehicle to Pedestrian), V2N(Vehicle to Nomadic Devices)등으로 분류되며, 도로 위의 차량에 적용 가능한 모든 형태의 통신 기술을 포함하여 V2X(Vehicle to Everything)라고 칭한다[5].

ITS(Intelligent Transport System)는 도로와 차량을 지능화하는 시스템으로써 자율 주행 시스템에 있어 필수 요소이며, 이와 같은 서비스를 구현하기 위해서는 V2X 통신 기술이 요구된다 [5]. V2X 통신의 경우, 자율 주행 자동차로 하여금 공격자가 공격을 수행할 수 있는 다수의 경로를 제공한다. 이에 따라 자율 주행 자동차 보안과 함께 V2X 통신 보안 연구가 필수적이라고 말할 수 있다.

### 2.2.2. 판단/제어 기술

자율 주행에 있어 판단 기술은 인지 기술을 통해 자율 주행 자동차의 위치가 추정되고, 주변 환경에 대한 정보를 획득한 후에는 주행 과정에 있어 자율 주행 자동차가 상황에 맞게 수행해야 하는 행동에 대해 판단한다. 자율 주행 자동차의 경우, 정밀 지도를 통해 도로 정보를 얻고, 목적지까지의 최적화된 경로를 결정하고, 주행 경로를 생성하며 상황에 따라 차선 변경 또는 추월을 수행한다. 다음의 [그림 3]은 자율 주행 자동차의 주요 기능에 따른 동작 과정에 대해 설명하고 있다 [9]. 앞서 말한 인지 과정에서는 GPS, 카메라, 레이더, 라이다, 센서, 정밀 지도등을 통해 자차의 위치를 추정하고 주변 환경에 대한 정보를 수집한다고 하였다. [그림 3]을 통해 확인할 수 있듯이, 수집된 정보(raw data)는 센서 프로세싱을 통해 Sensor Fusion을 위한 객체 파라미터를 생성한다. 단일 센서 또는 둘 이상의 센서를 결합하여 온보드 센서에 의해 제공되는 객체 파라미터는 인근 차량 및 인프라 자체의 추가 정보와 결합된다. 이와 같이 결합된 정보의 경우 Action 엔진 소프트웨어에 의해 사용되어지며 이를 통해 상황에 따른 적절한 행동을 판단한다.

이후, 제어 기능에서는 브레이크 제어, 주행 방향, 조향등을 결정하며 실질적으로 주행을 시작하는 단계로서 설명이 가능하다. 인지 기술을 통해 수집된 정보를 기반으로 판단 기술에 의해 상황에 따른 적절한 행동을 파악하고 판단 단계의 결정에 따라 단순히 행동을 수행하는 기능을 수행하므로 기존 차량의 방식과 크게 다르지 않다. 점차 센서의 기술이 다양화되고 발전됨에 따라 판단/제어 소프트웨어는 자율 주행 자동차의 핵심 소프트웨어이며 이에 대한 보안은 자율 주행 자동차의 안전성과 관련하여 중요한 요소가 될 것으로 생각된다.




〔그림 3〕 자율 주행 자동차 주요 기능에 따른 동작 과정 〔9〕

## Ⅲ. 자율 주행 자동차 보안

본 장에서는 자율 주행 자동차에 존재하는 보안 취약점 및 사례에 대해 설명하며, 자율 주행 자동차 보안 위협으로부터 보안하기 위해 적용되어 있는 보안 기술에 대해 설명한다.

### 3.1. 자율 주행 자동차 보안 위협 동향

기존 차량과 비교하여 자율 주행 차량의 경우, 외부 네트워크를 통해 차량 대 차량 및 차량 대 인프라간의 통신을 수행한다. 이처럼 외부에 노출되는 외부 네트워크를 통해 공격자는 보안 취약점을 이용하여 공격을 수행함으로써 사람에게 직접적인 피해를 입힐 수 있다. 또한, 자율 주행 차량은 센싱을 통해 방대한 양의 정보를 수집하고 이를 딥러닝 알고리즘을 통해 처리한다. 자율 주행 차량이 딥러닝을 통해 방대한 양의 정보를 처리할 때, 공격자는 정상적이지 않은 데이터를 주입함으로써 예상치 못한 상황을 야기시킬 수 있다. 자율 주행 자동차가 상용화 및 대중화되기 위해서는 이와 같은 문제가 발생하면 안되므로 철저한 하드웨어 및 소프트웨어 테스트가 요구된다.

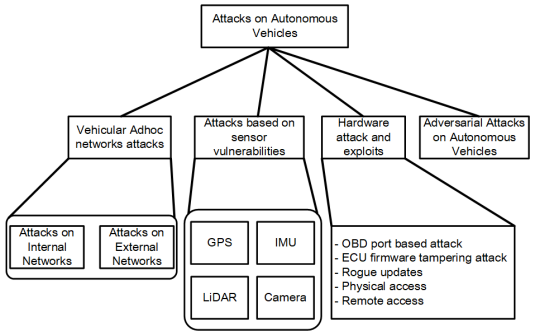
〔표 2〕 자율 주행 자동차에서 발생 가능한 보안 위협〔10〕

| Classification | Security threats |
|---|---|
| Platform | - ECU software fault<br>- ECU reverse engineering<br>- Masquerade ECU mounted<br>- IVI hack, Spoofing, Jamming |
| Internal Network | - Malicious control message injection<br>- Normal internal network interruption(packet insertion, deletion, etc.)<br>- DoS, Spoofing, etc. |
| External Network | - Wireless Network hack<br>- Masquerade OBU, RSU<br>- Misbehavior vehicle<br>- Provide fake message<br>- Vehicle access device hack |
| Management, Diagnosis | - Invasion of privacy<br>- Remote update and diagnostic protocol hack |

자율 주행 자동차에는 다양한 센서들이 탑재되어 있으며, 외부 네트워크를 통해 차량 대 차량, 차량 대 인프라간 통신을 수행하여 자율 주행을 원활하게 수행한다. 이는 공격자로 하여금 다양한 공격을 수행할 수 있게하며, 물리적 피해 또는 인간에게 직접적인 피해를 입힐 수 있다. 다음 [표 2]는 자율 주행 자동차에서 발생할 수 있는 보안 위협에 대해 정리하고 있으며 [10], [그림 4]는 자율 주행 자동차에서 가능한 공격에 대해 확인할 수 있다 [11].

### 3.1.1. GPS(Global Positioning System)

자율 주행 자동차에 있어 GPS는 자차의 위치 추정에 있어 매우 중요한 역할을 한다. GPS를 통해 자차의 위치 추정을 수월하게 수행하기 위해서는 GPS 데이터를 쉽게 얻을 수 있어야한다. GPS를 위한 공공 영역에 위성의 수가 증가하게 되었으며, 이를 기반으로 하여 GPS 데이터를 쉽게 얻을 수 있는 구조가 형성되었으며, 공격자는 정상적인 데이터에 대해 자유로운 접근이 가능함에 따라 잘못된 위치 정보를 제공하거나 차량의 경로를 제어하기 위해 GPS 데이터를 오도/조작하여 시스템에 알려준다. 이것은 운전자 또는 보행자의 안전에 직접적인 영향을 끼칠 수 있다. GPS 위치 정보에 대해 자율 주행 시스템에 오도하는 것은 공격자가 올바르지 않은 신호/데이터를 전송하는 GPS 스푸핑 및




〔그림 4〕 자율 주행 자동차에서 발생 가능한 공격〔11〕

재밍 공격을 통해 수행한다. 이를 통해 GPS 수신기가 더 강한 신호를 수신하도록 프로그래밍되고, 점차 차량의 위치가 시스템에서 원하는 목표가 아닌 공격자가 원하는 목표로 수정됨에 따라 예측하지 못한 상황이 발생하게 된다 [11].

### 3.1.2. IMU(Inertial Measurement Unit)

IMU는 자이로스코프와 가속도계의 조합으로 차량의 속도, 가속 및 방향 데이터를 제공한다. IMU는 GPS 오류를 보완할 수 있으며, 차량의 위치, 차량의 주행 방향, 경사와 같은 주변 환경을 모니터링하고 진단한다. IMU는 GPS의 치명적인 오류를 보완하는 역할을 하고 있기 때문에 자율 주행 자동차를 통한 주행에 있어 중요한 역할을 수행한다고 볼 수 있으며, 신뢰할 수 있는 보안을 제공해야 한다. 하지만, 공격자가 스푸핑 및 재밍 공격을 통해 IMU의 기능을 상실하게 될 경우, 치명적인 상황을 초래할 수 있다. 예를 들어, IMU의 기능이 상실하게 될 경우, 주행 중 경사로를 인식하지 못하고, 이에 따라 속도 조절을 하지 못하여 주변 차량과 예기치 못한 사고가 발생할 수 있다 [11].

### 3.1.3. LiDAR(Light Detection And Ranging)

LiDAR는 매 초마다 레이저 빔을 주변에 발사하여 반사되는 시간을 측정해 환경, 장애물 감지등을 인지하고 이를 3D 지도로 만들어낸다. 이는 자율 주행 자동차에 있어 실질적으로 사람의 눈과 같은 역할을 수행하고 있기 때문에 자율 주행 자동차의 주행에 있어 중추적인 역할을 수행한다고 말할 수 있다. 하지만, 공격자가 동일한 주파수의 신호를 스캐너에 보내고 물체가

탐지되었다고 오도할 경우, 이는 자율 주행 차량을 천천히 주행하도록 이끌거나 멈추게 만들 수 있다. 이외에도 2018년 3월에 발생한 테슬라의 자율 주행 차량의 사고는 자연 현상(태양의 역광)으로 인해 문제가 발생한 것으로 알려져 있다 [11]. LiDAR의 경우, 자율 주행에 있어 중추적인 역할을 수행하고 있기 때문에 보안 위협으로부터 보호할 수 있는 보안 기술 및 자연 현상으로부터 발생할 수 있는 예기치 못한 상황에 대해 보호할 수 있는 기술이 요구된다.

### 3.1.4. 카메라

카메라는 차선 감지, 교통 신호 인식, 헤드 라이트 감지, 장애물 감지등을 인식하는데 사용된다. 카메라의 경우, 공격자가 반대쪽에서 오는 차량의 시스템을 조작하여 하이빔 또는 헤드 라이트를 통해 카메라를 빛으로 가림으로써 기능이 부분적으로 비활성화되는 현상이 발생할 수 있다. 이는 물체를 잘못 탐지하거나 아예 탐지 못하여 운전자 또는 보행자에 안전 문제를 발생시킬 수 있다. 카메라의 기능 오류 또한 상황에 따라 심각한 상황의 원인이 될 수 있으므로 보안 기술 및 인식 오류에 대한 문제 해결 기술이 요구되어진다 [11].

### 3.1.5. V2X 네트워크 공격

차량 네트워크에 있어 자동차 개념과 새로운 기술을 융합하여 자동차 대 자동차 및 자동차 대 인프라간 통신이 가능하다. 이는 스마트폰, 클라우드 및 기타 장치에 연결하여 V2X를 통한 통신을 가능하게 한다. 일반적으로 자동차는 와이파이, 블루투스 및 GSM 프로토콜을 통해 스마트폰과 통신하며 이러한 통신 채널의 경우 본질적으로 취약하고 공격자가 악용할 수 있는 알려진 버그 및 취약점을 포함하고 있다. 일반적으로 스마트폰은 인증되지 않은 외부 장치와 상호 작용이 가능하기 때문에 자율 주행 자동차에 있어 스마트폰과의 연결은 차량에게 잠재적인 취약점을 가지게 한다. 또한, 데이터 센터가 손상될 경우, 차량이 인증되지 않은 기타 서버와 통신할 수 있으므로 클라우드에서 데이터를 전송하고 수신하는 것 또한 잠재적인 취약점을 유발할 수 있다. V2V 네트워크의 DSRC(Dedicated Short Range Communication)라고 하는 전용 단거리 통신 프로토콜은 75MHz의 대역폭으로 5.9GHz에서 동작하는 자동차용으로 특히 사용되는 이중 통신 프로토콜 채널이며, V2X 통신의 경우, WAVE(Wireless Access in Vehicular Environments)와 IEEE 802.11 p를 일반적으로 사용한다. DSRC, WAVE 및 IEEE 802.11 p는 공격자가 이용할 수 있는 알려진 취약점이 존재한다 [11].

자율 주행 자동차는 주행 중 추월, 차선 변경을 위해 호스트 차량과 근처 차량 간의 통신을 통해 데이터를 교환하며, 이때 V2V 네트워크를 통해 통신한다. 공격자는 V2V 네트워크의 알려진 취약점을 이용하여 위장 공격을 수행할 수 있으며 스푸핑을 통해 악의적인 차량을 위장 식별할 수 있도록 한다. 이를 통해 호스트 차량은 악의적인 차량과 연결되어 민감한 데이터를 송신하게 되며 공격자는 호스트 차량의 민감한 데이터를 수신하고 악용할 수 있다. V2V 네트워크의 치명적인 단점은 공격자가 호스트 차량과 근처 차량간의 트래픽과 데이터를 도청하여 인증 키와 같은 민감한 정보를 가져와 인증 공격으로 이끄는 취약한 프로토콜을 사용하는 것이다 [11].

### 3.1.6. OBD 포트 기반 공격

OBD는 온보드 진단을 나타내는 용어로서 OBD 포트의 경우, 2008년부터 제조된 모든 차량에 존재한다. OBD 포트는 차량 결함 및 성능 등 차량의 진단을 위한 데이터를 수집하는데 사용된다. OBD 포트의 경우, CAN 버스를 통해 ECU의 통신과 상호작용한다. USB 포트를 사용한 유선 연결 또는 블루투스를 사용한 무선 연결을 통해 컴퓨터에 연결이 가능하다. OBD 포트를 PC와 연결하였다면, 공격자는 데이터 패킷을 조작할 수 있으며, 악성 패킷을 차량 네트워크에 주입함으로써 적절한 차량 진단을 수행하지 못하도록 할 수 있다 [11]. OBD 포트 취약점으로 인한 공격 사례가 지속적으로 발표됨에 따라 2017년 EENews Automotive에서는 독일 자동차 산업이 OBD 인터페이스를 폐쇄할 것이라는 보도 또한 알려진 상태이다 [12].

### 3.1.7. ECU 펌웨어 변조 공격 및 Rogue 업데이트

일반적인 차량의 경우 100개 이상의 ECU로 구성되

어 있다. ECU(Engine Control Unit)는 엔진 제어 장치로서 하위 시스템의 센서 및 액추에이터를 위한 전자 제어 모듈이다. ECU 코드는 안전하고 보안성이 뛰어나지만 공격자는 사용자 지정 펌웨어로 ECU를 플래시하여 상태를 변화시켜 악의적이고 의도하지 않은 동작을 유발함으로써 공격을 성공시킬 수 있다. 공격자는 외부 인터페이스를 통해 ECU 펌웨어를 업데이트하여 ECU의 기능을 변경함으로써 공격자가 타겟으로 선정하고 있는 ECU 펌웨어 버전을 유지시킨다. 또한, 공격자는 ECU 메모리를 변경하여 보안 키를 변조하고 공격자가 의도한 소프트웨어 업데이트를 위해 해싱 기술과 인증을 사용하여 ECU 펌웨어 코드 및 업데이트 무결성을 유지시킨다 [11]. 자율 주행 자동차의 펌웨어 업데이트는 공격자로 하여금 Rogue 업데이트의 진입점이 된다. 자율 주행 자동차의 펌웨어 업데이트는 자동차 제조업체에서 별도로 제공해주지 않으며 안전 및 보안에 대한 적절한 업데이트가 없어 민감한 정보를 유출시키는 사이버 공격에 취약하다. 공격자는 물리 계층과 ECU가 통합되어 있다는 특징을 이용하여 센서 데이터, 제어 및 통신 모듈을 직접 이용하여 공격을 수행한다. 와이파이, 블루투스, 4G등을 이용한 차량과의 연결은 공격자로 하여금 원격 액세스를 수행할 수 있도록 한다. 공격자는 ECU를 의도하지 않은 CAN 버스에 연결되도록 하며 이를 통해 인터넷에 연결될 경우 펌웨어에 악성 코드나 바이러스 파일을 주입할 수 있다 [11].

#### 3.1.8. 의도적인 오작동(Adversarial attack)

자율 주행 자동차에 있어 DNN(Deep Neural Networks)과 같은 딥러닝 알고리즘은 주행을 위한 인식 단계에서 사용된다. 그러나 DNN과 같은 딥러닝 알고리즘은 공격자로 하여금 심각한 물리적 피해 및 인명 피해 또한 발생시킬 수 있다. 공격자는 원본 데이터가 저장되어 있는 곳에 교란을 일으킬 수 있는 악의적인 데이터를 추가함으로써 DNN 알고리즘이 올바른 의사 결정을 하지 못하도록 한다. Evtimov는 공격자가 교통 신호 감지 알고리즘에 악의적인 데이터를 삽입함으로써 교통 신호를 정확히 판단하지 못하는 것을 확인하였다 [13]. 이 취약점의 경우, 심각한 사회적 문제를 초래할 수 있으므로 자율 주행 자동차의 상용화 및 대중화있어 필수적으로 해결되어야할 문제이다.

〔표 3〕 자율 주행 자동차 관련 보안 기술 표준화[10]

| Standard | Description |
|---|---|
| IEEE 1609.2 | 자동차-자동차 및 자동차-기지국과의 WAVE 통신을 위한 보안 통신 규격 |
| IEEE 1616 | 자동차 Event Data Recorder 표준 |
| CAMP VSC3 | 프라이버시를 보존하는 자동차 PKI 표준 |
| EVITA | HSM 기반의 ECU 보안 플랫폼 규격 |
| AUTOSAR | 자동차 전용 임베디드 소프트웨어 표준(4.1버전 이후 보안 규격 포함) |
| ISO 14229 | 자동차 통합 진단 표준<br>- 14229-1: ECU에 대한 통합 진단<br>- 14229-2: 세션 레이어 서비스<br>- 14229-3: CAN 네트워크 통합 진단<br>- 14229-4: FlexRay 네트워크 통합 진단 |
| ISO TC22 SC31 WG2 | - 자동차 진단 프로토콜 표준 |
| ISO TC22 SC31 WG6 | 확장된 자동차, 차량 클라우드 서비스를 위한 인터페이스 표준, 보안규격 포함 |
| ITU-T X.1373 | 보안 제어 기능을 갖춘 자동차 소프트웨어 업데이트 절차 |
| ITU-T itssec-2 | 차량 V2X 통신 시스템에 대한 보안 권고사항 |
| ITU-T itssec-3 | 차량 접속 디바이스에 대한 보안 요구 사항 |
| ITU-T itssec-4 | 차량 침입 탐지 시스템 구성 방법 |
| ITU-T itssec-5 | 차량 클라우드 엣지 컴퓨팅 보안 권고사항 |
| ETSI TS 102 | ITS를 위한 보안 표준<br>- 731: ITS 보안 구조 및 서비스<br>- 893: ITS 보안 취약점 및 위협 분석<br>- 941: ITS 프라이버시 보호 기술<br>- 942: ITS 접근제어 기술<br>- 943: ITS 보안 구조 및 서비스 |

### 3.2. 자율 주행 자동차 보안 기술 동향

3.1절을 통해 확인할 수 있듯이 자율 주행 자동차에 탑재되어 있는 센서 및 통신을 위한 외부 네트워크는 공격자에게 보안 위협을 위한 진입점을 제공하는 것을 확인할 수 있었다. 자율 주행 자동차의 발전에 따라 ECU의 성능 또한 고도화되고 있는 추세이다. 현재 ECU를 보안하기 위한 기술로는 ECU의 비휘발성 메모리에 저장되는 펌웨어의 플래시 과정에서 신뢰할 수 있는 주체인지에 대한 인증 과정을 거치는 보안 옵션인 시큐어 부트, 소프트웨어를 업데이트할 경우 해당

소프트웨어가 제조사에 의해 인가된 소프트웨어 인지 확인하는 시큐어 플래싱, 접근 제어 등이 있다. 이러한 기술들은 ECU의 보안뿐 아니라 원격 업데이트를 위해서도 사용되고 있다. 또한 국내외적으로 보안 기술 표준화가 활발하게 이루어지고 있다. 다음 [표 3]을 통해 자율 주행 자동차 관련 보안 기술 표준화 내용을 확인할 수 있다 [10].

## Ⅳ. 결 론

자율 주행 자동차 시장은 매년 증가하고 있는 교통사고의 감소, 운전에 대한 접근성, 차량 운행 중 다양한 업무 가능 등의 장점으로 인해 매년 확대되고 있는 추세이며, 자동차 제조 회사뿐만 아니라 ICT 기업 또한, 자율주행 자동차를 상용화 및 대중화하기 위한 연구 및 개발을 진행 중에 있다. 본 논문에서는 지속적으로 개발되고 있는 자율 주행 자동차의 기술 동향을 파악하고, 자율주행 자동차에서 발생하고 있는 보안 위협과 보안 위협으로부터 안전한 자율 주행을 위해 연구/개발되고 있는 보안 기술 동향에 확인하였다. 논문에서 살펴본 바와 같이 자율 주행 자동차에 대한 보안 위협은 지속적으로 나타나고 있으며 보안 위협에 대한 보안 기술 또한 지속적으로 연구되고 있는 추세이다. 자율 주행 자동차의 경우, 사소한 오류로 인해 물리적인 피해뿐만 아니라 인간에게 심각한 피해를 입힐 수 있기 때문에 상용화 및 대중화를 위해서는 지속적인 보안 기술 연구/적용과 실증적인 테스트가 이루어져야 한다.

## 참 고 문 헌


[1] Gatner Forecasts More than 740,000 autonomous vehicles to be added to global market in 2023, https://www.gartner.com/en/newsroom/press-releases/2019-11-14-gartner-forecasts-more-than-740000-autonomous-ready-vehicles-to-be-added-to-global-market-in-2023, 2020년 3월 접속.

[2] 서화정, 권용빈, 권혁동, & 안규황. (2018). 자율주행자동차 보안 동향. 정보보호학회지, 28(5), 9-14.

[3] 자율 주행 자동차 상용화 및 지원에 관한 법률, http://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=208588&efYd=20200501#0000, 2020년 3월 접속.

[4] Audi, BMW, other frustrated by hurdles slowing launch of self-driving car, https://europe.autonews.com/automakers/audi-bmw-others-frustrated-hurdles-slowing-launch-self-driving-cars, 2020년 3월 접속.

[5] 서은비; 김휘강. 자율 주행 차량의 In-Vehicle 시스템 관점에서의 공격 시나리오 도출 및 대응 방안 연구. 한국자동차공학회논문집, 2018, 26.2: 240-253.

[6] 자율 주행 기술의 6단계, https://news.hmgjournal.com/Tech/%EC%9E%90%EC%9C%A8%EC%A3%BC%ED%96%89-%EA%B8%B0%EC%88%A0-%EB%A0%88%EB%B2%A8-6%EB%8B%A8%EA%B3%84, 2020년 3월 접속.

[7] 자율 주행의 핵심: 정밀지도, https://www.ktb.co.kr/common/download.jspx?cmd=viewPDF&path=/attach_file/RESEARCH/61685/1/20170410_B2510_ykmoon_106.pdf, 2020년 3월 접속.

[8] 정호기; 서재규. 센서 융합 기반 자동차용 정밀 측위시스템. 오토저널, 2015, 37.6: 29-34.

[9] MUJICA, Fernando. Scalable electronics driving autonomous vehicle technologies. Texas Instrument, 2014.

[10] 권혁찬, 이석준, 최중용, 정병호, 이상우, 나중찬. (2018). 자율주행 자동차 보안기술 동향. [ETRI] 전자통신동향분석, 33(1), 78-88.

[11] KUMAR, Amara Dinesh, et al. A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities. arXiv preprint arXiv:1810.04144, 2018.

[12] German car industry plans to close OBD interface, https://www.eenewsautomotive.com/news/german-car-industry-plans-close-obd-interface, 2020년 3월 접속.

[13] EYKHOLT, Kevin, et al. Robust physical-world attacks on deep learning visual classification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018. p. 1625-1634.

## 〈저 자 소 개〉


**권 순 홍 (Soonhong Kwon)**

학생회원

2016년 3월~2020년 2월 : 상명대학교 컴퓨터공학과

2020년 3월~현재 : 세종대학교 정보보호학과 재학

<관심분야> 네트워크 보안, 시스템 보안

**이 종 혁 (Jong-Hyouk Lee)**

정회원

2010년 2월 : 성균관대학교 공학박사

2009년 6월~2012년 2월 : 프랑스 INRIA 연구원

2012년 3월~2013년 8월 : 프랑스 그랑제꼴 TELECOM Bretagne 조교수

2013년 9월~2020년 2월 : 상명대학교 소프트웨어학과 부교수

2020년 3월~현재 : 세종대학교 정보보호학과 부교수

<관심분야> 프로토콜 엔지니어링 및 정보보호