자율주행 자동차 보안 취약성 및 솔루션 조사

박재경[O], 강승윤[*], Chat-GPT[*]
[O]한국폴리텍대학교 강서캠퍼스 사이버보안과,
[*]한국폴리텍대학교 강서캠퍼스 사이버보안과
e-mail: wildcur@gmail.com[O], 2320110215@office.kopo.ac.kr[*]

A Survey about Vulnerabilities and Solutions of Autonomous vehicle security

JaeKyung Park[O], SeungYoon Kang[*], Chat-GPT[*]
[O]Dept. Professor of Cyber Security, Korea Polytechnics University,
[*]Dept. Student of Cyber Security, Korea Polytechnics University

● 요 약 ●

본 논문은 자율주행 자동차의 보안 취약성과 이를 해결하기 위한 솔루션에 대한 조사를 다루고 있다. 자동차의 자율주행 및 초연결성이 대두됨에 따라 보안 위협이 점점 중요해지는 현실을 직면하고 있다. 본 논문은 다양한 취약성을 카테고리 별로 다루고, 해당 취약성에 대응하기 위한 보안 솔루션과 현재 연구 개발 중인 솔루션들을 소개하고 있다. 그러나 아직 해결되지 않은 과제들이 산적해 있으며, 연구와 개발이 계속되어야 안전하고 신뢰성 있는 초연결 자율주행 자동차를 구현할 수 있을 것으로 기대한다.

키워드: Autonomous Mobility(자율주행 자동차), Hyper-Connectivity(초연결성), Network(네트워크), V2X(Vehicle to Everything), Vulnerability(취약성), Solution(솔루션)

I. Introduction

자동차 및 교통 환경이 점차 자율주행, 지능형 교통 시스템으로 발전하면서 자동차 및 주행 환경은 복잡해지고, 지능화 되어 가고 있다. 또한 도로/교통 인프라와 자동차 간의 연결성도 대폭 확대되어 가고 있다. 현재 센서와 소프트웨어에 의한 자율주행 서비스는 결국 V2V, V2I를 통한 협력 자율주행 환경으로 변화가 예측되며 초연결 시대를 도래할 것으로 예상된다. 이러한 자율주행 환경으로 변화됨에 따라 인류는 편리성과 안전성을 가질 수 있지만, 보안 사고로 인한 심각한 문제를 야기할 수 있다. 물론 자동차 보안을 위한 지구촌 곳곳에서 다양한 보안 솔루션들이 개발·적용되고 있으나 지속해서 피해 사례 및 가능성이 보고 되고 있고, 지능화되고 고도화되는 자동차 사이버 공격에 대한 대응책이 필요한 상황이다. 일례로 3월 중순 캐나다 밴쿠버에서 개최된 '폰투온(Pwn2Own) 2023'에서 프랑스의 보안 회사인 시낵티브(Synacktiv)가 단 2분 만에 T사의 모델을 해킹해 주행 중 차량의 도어와 트렁크 개폐를 할 수 있었다. 이에, 본 논문에서는 자율주행 보안 취약점을 살펴보고, 이에 대응하기 위한 보안 솔루션 현황을 살펴보고자 한다.

II. Preliminaries

1. Related works

1.1 초연결 자율주행 자동차의 네트워크 개요

센서와 소프트웨어에 의한 자율주행 서비스는 결국 V2X(V2V, V2I 등)를 통한 협력 자율주행 환경으로 진화가 예측되며 초연결 자동차 시대를 도래할 것으로 예상된다. 다음 <그림 1>은 조만간 다가올 자율주행 자동차의 네트워크에 대한 개요를 도식화한 자료이다.

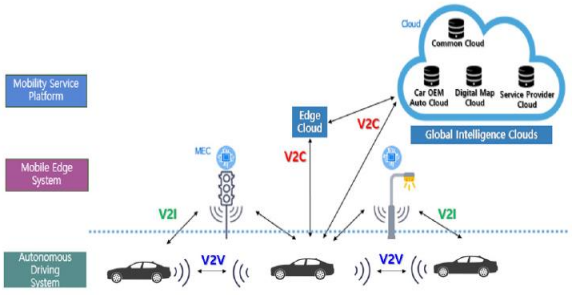

Fig. 1. Network Overview for Autonomous Vehicles

1.2 초연결 자율주행 자동차의 보안 취약성

다음은 자율주행 자동차에 대한 보안 취약성을 소개한다. 자동차에 대한 다양한 취약성은 아래의 <표 1>과 같다. <표 1>은 자율주행 자동차에 대한 보안 위협을 플랫폼, 내/외부 네트워크, 관리/진단 측면에서 구분하여 정리하였으며, 표에서 알 수 있듯이 자동차에 있어서 제일 심각한 취약성은 인가되지 않은 데이터의 내부 네트워크 침입과 DoS 공격으로 인한 데이터 가용성이 침해되는 것이다.

Table 1. Vulnerabilities by Category

Category	Vulnerability
Vehicle length Platform	● ECU Software fault, ECU Reverse engineering ● ECU Firmware hacking and Forgery ● Mounting a Camouflage ECU ● Infotainment system hacking, Malware infection ● Sensor physical attack(Blinding, Spoofing, Jamming)
Internal Network	● Injecting malicious control messages into Internal network ● Disrupting normal internal networks (Packet Insertion, Deletion, Tampering, Delay), Sniffing ● DoS, Replay, Spoofing, Discarding packets ● Hacking using Bluetooth network
External Network	● Wireless network hacking, DoS Attack ● Camouflage OBU(Onboard Unit), RSU(Road Side Unit) ● Misbehavior Vehicle ● Injecting Fake messages ● Hacking into Vehicle access devices
Management Diagnosis	● Invasion of privacy ● Remote update and Diagnostic protocol ● Deletion of Incident cause data by hacking

1.3 초연결 자율주행 자동차의 보안 솔루션

위에서 기술한 다양한 보안 위협과 이에 대응하기 위한 보안 솔루션들에는 아래의 <표 3>이 있다. 이러한 솔루션들은 적용 및 연구개발되고 있다. <표 3>은 플랫폼, 내/외부 네트워크, 관리/진단 측면에서 구분하여 정리하였다.

Table 2. Solutions by Category

Category	Solution
Vehicle length Platform	● Secure Boot, Secure Flashing, Access Control ● Application Sandbox, Platform Virtualization ● HSM(Hardware Security Module) ● Prevention Dechanneling ● Autosar CSM(Cryptographic Security Manager) ● SecOC(Secure Onboard Communication)
Internal Network	● F/W, IDS, IPS ● ECU Authentication, Key Management, Encryption ● Threat Detection(Rule-Based, Machine Learning-Based)
External Network	● V2X Message Authentication, Encryption ● High-speed Validation of Vehicle PKI, V2X Message signing ● Security for WAVE Communication with Cars and Base Stations(IEEE 1609.2)
Management Diagnosis	● Security Monitoring, Vulnerability Analysis ● Analyze anomalies and anomalous behavior ● Remote SW/FW Security Updates ● Forensics and Incident cause analysis techniques

III. Conclusions

자율주행 자동차의 급격한 발전과 함께 보안 취약성 문제가 점점 더 중요해지는 현실을 직면하고 있다. 본 논문을 통해 자율주행 자동차 시스템에 대한 다양한 취약점을 확인하고, 이를 해결하기 위한 솔루션을 조사했다. 그러나 아직 해결되지 않은 과제들이 남아있고, 이를 해결하려는 연구가 곳곳에서 진행되고 있다. 이로써 안전하고 신뢰성 있는 초연결 자율주행 차량을 통해 삶의 질이 향상되고 안전한 주행 시스템을 갖춘 미래가 올 것이라 믿어 의심치 않는다.

REFERENCES

[1] ETRI "Zero Accident, Connected Autonomous Driving Vehicle"

[2] ETRI "Security Trends for Autonomous Driving Vehicle“