정 보 보 호 학 회 지
제28권 제5호, 2018. 10

자율주행자동차 보안 동향

서 화 정*, 권 용 빈*, 권 혁 동*, 안 규 황*

요 약

운전자의 도움 없이 자동으로 운행하는 자율주행자동차는 차세대 IT 플랫폼으로써 그 중요도가 증가하고 있다. 현재 자동차 회사는 물론이거니와 대표적인 IT 기업들에서도 자율주행차량을 상용화하기 위한 노력을 기울이고 있다. 자율주행자동차는 주행과 관련된 기술적인 완성도도 중요하지만 이와 더불어 사소한 보안 취약점이 차량 탑승자의 생명을 위협할 수 있는 만큼 단 한차례의 사이버 공격도 허용할 수 없는 기술적 특징을 가진다. 본 논문에서는 자율주행자동차의 기술 발전 동향과 더불어 보안 취약점에 관련된 내용을 함께 확인해 보도록 한다.

Ⅰ. 서 론

자동차 관리법 제2조 제1호의3에 따르면 자율주행자동차란 운전자 또는 승객의 조작없이 자동차 스스로 운행이 가능한 자동차를 말한다. 자율주행자동차가 실용화되게 될 경우 자동차 안에서의 운전자의 역할이 축소되고 운전자는 차량 운행동안 또 다른 업무에 몰두할 수 있는 환경이 조성될 수 있다. 이는 지금까지 설계된 자동차와는 전혀 다른 개념으로 자동차와 운전자를 바라보게 된다. 따라서 앞으로의 자동차 설계와 주행에도 크나큰 변화가 올 것으로 기대되고 있다. 먼저 자동차 내에서 큰 부분을 차지했던 운전석의 기능이 축소되게 될 것이다. 이를 통해 확보된 공간은 또 다른 역할을 하는 공간으로 재탄생되게 될 것이다. 도로 상에 모든 차량이 컴퓨터 인공지능에 의해 동작하게 된다면 인간의 판단 착오로 발생했던 사고의 위험이 대폭 줄어들게 될 것이며 이를 통해 인류의 생활에도 막대한 영향을 미칠 것으로 생각된다.

자율주행차량은 모든 판단이 자율주행자동차가 외부를 인식하는 방법인 센싱 정보와 이를 해석하는 인공지능에 의해 결정되는 특징을 가지고 있다. 하지만 단 하나의 정보와 시스템이 악의적인 해커에 의해 조작되는 상황에 처하게 될 경우 이를 통해 도출되는 잘못된 판단은 큰 사고로 이어질 수 있는 문제점을 가지고 있다. 기존의 IT 시스템의 경우 해킹을 당하더라도 생명과는 거리가 먼 정보 혹은 재원이 탈취되는 경우가 대부분이었지만 자율주행자동차의 경우 한 번의 해킹으로 인해 탑승자의 생명이 위협받을 수 있다는 특징을 가지고 있다. 따라서 기존의 IT 시스템과는 차별화되고 강인한 보안 시스템 구축이 요구되고 있다. 본 논문에서는 최근 가속화되고 있는 자율주행자동차의 개발 동향에 대해 확인해 보고 이와 관련된 자율주행자동차 보안 이슈에 대해 확인해 보도록 한다.

본 논문의 구성은 다음과 같다. 2장에서는 자율주행차량의 최신 기술 동향에 대해 확인해 보도록 한다. 3장에서는 자율주행차량에서 발생할 수 있는 최신 보안 취약성에 대해 확인해 보도록 한다. 마지막으로 4장에서는 본 논문의 결론을 내린다.

Ⅱ. 자율주행자동차

2004년 DARPA에서는 자율주행자동차의 기술적 완성도를 테스트하기 위해 150마일에 대한 운행 대회를 개최하였다. 150마일 중에서 최고의 성적을 거둔 팀은 오직 7마일만을 성공적으로 운행하였다. 1년이 지난 대회에서는 5대의 자율주행자동차가 대회를 완전히 주행하였다. 2007년에는 6개의 팀이 교통 법규를 지키면서 운행하는 것을 성공적으로 완수하였다. 이는 매우 현실적이고 실제 생활에 적용이 가능한 시나리오를 적용한 경우라고 할 수 있다. 2014년에는 구글이 개발한 자율

이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5075742)
* 한성대학교 IT융합공학부 (hwajeong84@gmail.com, dove3333@naver.com, hdgwon@naver.com, tigerk9212@gmail.com)

주행자동차가 캘리포니아의 공공도로를 700,000마일 운행하였다[1]. 해당 결과에 고무된 다양한 자동차 제조회사들 (Audi, BMW, Cadillac, Ford, GM, Mercedes-Benz, Nissan, Toyota, Volkswagen, 그리고 Volvo)에서는 자율주행자동차 시스템을 테스트하기 시작하였다. 부분적으로 자동화된 시스템은 현재 판매중인 자동차에서 쉽게 확인가능하다. 대표적인 기술로는 Adaptive Cruise Control (ACC), land departure warnings, collision avoidance, 그리고 parking assist system으로 볼 수 있다. 유럽에서는 CityMobil2라는 프로젝트를 통해 저속 자율주행자동차를 5개 도시에서 시범 운영 중에 있다. 자율주행자동차 기술은 군대, 광업, 그리고 농업과 같은 분야에서 점차 확산되어 활용되고 있다[2]. 앞에서 살펴본 도시 상에서의 테스트를 통해 많은 문제를 확인하게 될 것이며 이는 자율주행자동차의 혁신에 이바지할 수 있을 것으로 기대된다. 자율주행자동차의 상용화가 가속화됨에 따라 미국의 주에서는 자율주행자동차를 합법화하고 있다. 현재 합법화하고 있는 주는 California, Florida, Nevada, Michigan 그리고 Washington, D.C가 있다. 현재 자율주행자동차는 운전자가 주행에 개입하는 정도에 따라 자동화단계를 나누어 설명하고 있다. 미국자동차공학회 SAE (Society of Automotive Engineering)에서 제시하는 가이드라인은 [표 1]과 같다. 최신 자동차의 경우 특정한 조건에 대해서는 자동화된 주행을 제공하게 된다. 완전한 자율주행은 레벨 5와 같이 사람의 도움 없이 주행하는 것을 의미한다. 이처럼 완전한 자율주행자동차는 운전자에 의해 주행되는 현재의 주행과 전혀 다른 형식으로 동작하게 되며 이는 사람들의 생활에 큰 영향을 미치게 될 것이다[3]. 자율주행자동차는 교통질서를 지키도록 프로그램 될 것이며 음주운전을 하는 경우도 없게 될 것이다. 자율주행자동차는 컴퓨터가 판단하기 때문에 인간보다 빠른 판단이 가능하며 이는 전체 차량 트래픽을 줄이고 매연연기의 방출을 줄일 수 있는 등 다양한 이점을 가지고 있다.

가장 먼저 살펴볼 이점은 안전성이다. 자율주행자동차를 활용하게 될 경우 교통사고의 확률을 획기적으로 낮출 수 있다. 미국의 교통사고 통계에 따르면 약 40%에 달하는 교통사고는 다양한 요건 (음주, 마약, 그리고 피로)들의 조합을 통해 도출되게 된다. 이러한 사고의 원인들은 사람에 의존적인 요인으로써 자율주행 자동차

〔표 1〕 운전자 주행 개입 정도에 따른 자율주행자동차 기준 상세 (SAE 기준)

Level	Name	Detail
1	Driver Assistance	- Single advanced driver assistant system Cruise control Lane keeping assistant Full-time performance by human driver
2	Partial Automation	Multi advanced driver assistant system - Lane keeping assistant - Adaptive cruise control Human driver perform all remaining aspects
3	Conditional Automation	Specific road condition, conditional automation Highway automation With response of human driver appropriately
4	High Automation	Automation in all road condition Human driver
5	Full Automation	Automation in all road condition Manless

상에서는 충분히 개선될 수 있는 사항이다.

두 번째 장점으로는 자율주행자동차를 사용함으로써 오는 경제적인 이득이다. 자율주행자동차는 주위환경을 센싱하여 자신의 주행을 예측하게 된다. 속도와 감속이 예측에 의해 조절되기 때문에 가장 효율적으로 속도를 조절하고 이는 교통혼잡을 줄이고 연료 사용량을 감소시키는데 이바지할 수 있을 것으로 예상된다.

세 번째로 생각해 볼 수 있는 부분은 지금까지는 자동차를 주행할 수 없었던 사용자들이 자율주행자동차를 활용하여 자신의 목적지에 보다 쉽게 접근 가능하다. 나이가 너무 어리거나 연세가 있으신 경우에는 차량 주행에 어려움을 겪을 수 있다. 하지만 자율주행자동차는 이러한 사용자에게 편안하고 자동화된 주행을 제공하기 때문에 새로운 사용자를 양산할 수 있는 장점을 가진다. 이와 더불어 자율주행자동차는 스스로 주차를 하게 될 것이며 이는 자동차 주차 문제를 효과적으로 해결할 수 있다.

위에서 살펴본 바와 같이 긴 역사는 아니지만 자동차

주행에 있어 새로운 패러다임을 제공하고 있는 자율주행자동차는 앞으로 다가올 제 4차 산업혁명 시대의 핵심 기술로 자리매김할 것으로 보인다. 하지만 기술이 발전함에 따라 사용자들이 얻어가는 이점이 커짐과 동시에 반대로 증가하는 부분이 있다. 그것은 바로 자율주행자동차의 보안취약성이다. 모든 정보가 센서를 통해 수집되고 수집된 정보는 인공지능을 통해 판단하는 완전한 시스템으로 보이지만 해커가 중간 과정에 개입하여 정보를 조작하게 될 경우 지금까지의 사이버 보안 사고와는 비교도 안 될 정도로 큰 파장을 일으키게 될 것으로 보인다. 따라서 다음 장에서는 자율주행자동차가 가지는 원천적인 보안 취약성에 대해 확인해 보도록 한다.

Ⅲ. 자율주행자동차 보안

완전한 자율주행을 위해서는 주변환경을 완전히 인지하는 것이 가장 중요하다. 이러한 인지 기술은 크게 ADAS (Advance Driver Assistance System), V2X (Vehicle to Everything), 그리고 정밀지도를 종합하여 확인하게 된다. ADAS는 카메라, 레이더, 라이다 등과 같은 장비를 이용하여 주변 환경을 판단하는 것을 의미한다. V2X는 각각의 자동차마다 가지고 있는 OBU (On Board Unit)과 RSU (Road Side Unit)들 간의 통신을 통해 주변 교통환경을 넓은 시야로 확인하는 기술을 의미한다. 마지막으로는 GPS와 그에 일치되는 정밀지도가 있다. 이러한 정보가 수집되게 되면 이를 인공지능 알고리즘을 활용하여 판단하게 되고 판단된 결과는 자율주행자동차의 각 장치들에 전달되어 제어하게 된다. 상황에 대한 인지와 판단, 그리고 제어는 유기적으로 작동해야 하며 만약 해커에 의해 한 부분이 잘못되게 될 경우 주행은 위협받게 된다.

2015년도 Black Hat Europe에서는 자동차에 설치된 카메라와 라이다 시스템에 대한 공격을 성공적으로 실시하였다 [4]. 공격이 가능한 시나리오로는 크게 세 가지로 나누어 볼 수 있다. 첫 번째는 자율주행자동차 근처의 자동차에서 공격을 하는 것이다. 근처의 자동차를 활용하게 될 경우 일정한 거리를 두고 지속적으로 공격이 가능한 장점을 가진다. 두 번째는 도로변에서 공격을 하는 것이다. 다중의 위치에 설치된 해킹 기기를 통해 지속적인 가능이 가능하다. 마지막으로 세 번째는 Evil Mechanic 공격 예시로써 짧은 시간 동안 목표로 하는 자동차에 접근하여 공격하는 것을 의미한다[5]. 사용자가 주차를 하는 순간 접근하여 공격하는 것이 하나의 예시이다.

이러한 시나리오를 기반으로 카메라에 대한 공격을 시도가 가능하다. 카메라는 자율주행자동차의 눈과 같은 역할을 하게 되고 만약 해킹을 당하게 되면 교통신호를 분간할 수 없게 되거나 차선을 확인하는 것이 어렵게 된다. 이와 더불어 이미지 프로세싱에 사용되는 딥러닝 기술을 해킹하여 사용자는 알 수 없는 정보를 컴퓨터가 인지하도록 하여 잘못된 결과를 도출할 수 있는 기술도 보고되고 있다 [6]. 카메라에 대한 첫 번째 공격 방법은 레이저를 카메라에 주입하여 카메라의 기능을 상실시키는 공격이다. 해당 공격 수행 시에는 주변 환경의 빛세기에 맞추어 공격에 적합한 빛세기를 찾은 이후 공격을 수행하여야 한다. 두 번째 공격 방법은 자동 조정 기능을 공격하여 시스템 안정화를 방해하는 공격이다. 주기적으로 레이저를 주입하기 때문에 카메라는 해커의 공격을 탐지하기 어렵다는 문제점을 가지고 있다. 카메라에 대한 레이저 공격을 효과적으로 대응하기 위해서는 첫 번째로 여러 대의 카메라를 설치하여 공격자가 모든 카메라를 공격하는 것을 어렵게 하는 방법이다. 두 번째는 공격자의 레이저를 걸러내는 필터를 카메라에 설치하여 공격자의 공격을 방어하는 기법이 있을 수 있다.

라이다 시스템 또한 자율주행차량에서 매우 중요한 인지능력을 담당하고 있기 때문에 이에 대한 공격이 가능하다. 라이다 시스템은 신호가 반사되어 돌아오는 시간에 의존하여 주변환경을 확인하게 된다. 이러한 라이다 시스템의 특성을 악용한 다양한 해킹기법들이 제안되고 있다. 첫 번째로는 replay attack을 응용한 relay attack이다. 진짜 신호를 다른 위치에서 발생시켜서 실제로는 존재하지 않는 가짜 물체를 만들어 내는 것이다. 두 번째는 spoofing 공격으로써 실제로는 존재하지 않는 물체에 대한 정보를 생산하여 라이다 시스템에 주입하는 것이다. 주입된 신호는 가짜 물체를 생성하게 되고 자율주행차량은 해당 신호로 인해 올바른 판단을 할 수 없게 된다. CHES'17에서는 spoofing 공격이 기존에는 불가능했던 가까운 위치 상에도 가짜 물체를 발생시킬 수 있는 기법이 소개되었다[7]. 이러한 공격을 막기 위해서는 카메라와 마찬가지로 다중 라이다 시스템을 적용하는 것이 하나의 해결책이 될 수 있다. 특히 각각의

라이다 시스템이 상이한 wavelength를 인식하도록 설계된다면 공격이 보다 어려워지게 된다 [8,9]. 두 번째 대안책은 정보를 읽어오는 주기를 변경해가며 동작시키는 것이다. 공격자는 신호의 주기를 알지 못하면 정확한 정보를 주입할 수 없기 때문에 공격이 어렵다. 하지만 회전하는 라이다 시스템의 경우 일정한 속도를 유지해야 하기 때문에 신호의 주기를 임의로 변경하는 것은 어렵다. 마지막 대응 기법은 신호의 주기를 짧게 하여 공격자가 악의적인 신호를 주어진 주기 안에 주입하는 것을 봉쇄하는 것이다.

USENIX'10에서는 현재 자동차 시스템이 가지는 보안 취약점에 대해서 발표하였다 [10]. 지금까지 자동차는 컴퓨터 보다는 기계에 가까웠다. 하지만 자율주행자동차는 제어자동화에 따라 기계보다는 컴퓨터 시스템에 가까워지고 있다. 따라서 기존의 자동차 시스템에서 자동차의 상태를 판단하는 용도로 활용되었던 TPMS (Tire Pressure Monitoring System)는 컴퓨터 시스템에 연결됨에 따라 정보가 유출될 수 있는 문제를 가지고 있다. 해당 논문이 발표되던 시점에는 TPMS에 대한 보안이 적용되지 않아 TPMS에 접근이 가능한 해커라면 spoofing 공격 혹은 battery drain 공격 그리고 원거리에서 자동차의 정보를 캡처하여 추적이 가능하다는 것을 보였다. 이러한 공격을 방지하는 가장 기본적이면서도 원초적인 방법은 프로토콜을 암호화하여 해커가 해당 정보를 변조하는 것을 막는 것이다.

USENIX'11에서는 해커 입장에서 자율주행자동차를 해킹할 수 있는 방면에 대해 확인하는 방안에 대하여 연구하였다 [11]. 근거리 통신으로는 블루투스, RF 기반의 RKE (Remote Keyless Entry), TPMS, RFID 자동차키, 그리고 802.11 WiFi 채널이 있다. 원거리 통신으로는 GPS, 위성 라디오, 그리고 원거리 telematics 시스템이 있다. 만약 이중에서 하나의 시스템이라도 해커에 의해 해킹당하게 된다면 사용자의 자동차는 원거리에서 큰 위험에 빠질 수 있다.

최근의 연구 결과에 따르면 상용화된 자동차 또한 해킹에 무방비 상태임을 확인할 수 있다 [12, 13]. 주행 중인 Jeep Cherokee 차량으로 원격으로 해킹하였을 뿐 아니라 Tesla Model S를 해킹한 사례까지 보고되고 있다. 해킹에 성공하게 될 경우 차량에 대한 모든 권한은 해커가 가지게 되기 때문에 탑승자는 큰 위험에 처하게 된다는 문제점을 가지고 있다.

이처럼 위에서 살펴본 바와 같이 현재 다양한 공격이 자율주행차량에서 행해지고 있다. 이를 방지하기 위해서는 다양한 기술과 보안이 융합되어 함께 해결해 나가야 할 것으로 보인다. 이러한 중요성으로 인해 각 나라

〔표 2〕 자동차 보안 관련 표준화〔14,15〕

Standard	Description
IEEE 1609.2	WAVE communication protocol to vehicle and base station(encryption, authentication, digital signature)
IEEE 1616	Vehicle EDR (event data Recorder) standard
CAMP VSC3	Vehicle PKI standard with privacy
EVITA	ECU security platform standard based on HSM
AUTOSAR	Automotive embedded software standard including security standard
ISO 14229	Automotive integrated diagnostic standard 14229-1: ECU diagnostic 14229-2: session layer service 14229-3: CAN network diagnostic 14229-4: FlexRay network diagnostic
ISO TC22 SC31 WG2	Automotive diagnostic protocol standard
ITU-T X.1373	Safety update procedure of vehicle software with security control function
ITU-T itssec-2	Security guideline for V2X communication system
ITU-T itssec-3	Security requirements for device connected to vehicle
ITU-T itssec-4	IDS (Invasion Detecting System) configuration
ITU-T itssec-5	Vehicle cloud edge computing security guideline
ETSI TS 102	Security standard for ITS (Intelligent transport system) 731:ITS security structure and service 893:ITS analysis security vulnerability and threats 941:ITS privacy protection technology 942:ITS access control 943:ITS structure and service
SAE J3061	Cybersecurity guidebook for cyber-physical vehicle systems
CAMP	Vehicle safety communication

와 단체들에서는 자동차 보안과 관련하여 표준화 작업을 진행 중에 있다. 자세한 사항은 [표 2]와 같다.

Ⅳ. 결 론

본 논문에서는 자율주행자동차의 최신 발전 동향에 대해 확인해 보았으며 이와 더불어 대두되고 있는 보안 이슈를 확인해 보았다. 논문에서 확인해 본 바와 같이 차세대 IT 플랫폼인 자율주행자동차에 대한 기술 개발과 이에 따른 보안 이슈가 매우 활발히 논의되고 있음을 확인할 수 있다. 특히 자율주행자동차와 같이 생명과 연관된 플랫폼 상에서의 정보보호에 대한 연구가 보다 활발히 진행되어 누구나 믿고 안전하게 사용할 수 있는 자율주행자동차의 개발이 빠르게 이루어져야 할 것으로 보인다.

참 고 문 헌

[1] S. Anthony, “Google’s self-driving car passes 700,000 accident-free miles, can now avoid cyclists, stop at railroad crossings,” Extreme Tech, 2014.

[2] “Inside Story: Look, No Hands,” Economist Technology Quarterly, September, pp. 17-19, 2012.

[3] D. J. Fagnant, K. Kockelman, “Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations,” Transportation Research Part A: Policy and Practice, vol. 77, pp. 167-181, 2015.

[4] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: Experiments on camera and lidar,” Black Hat Europe, 2015.

[5] J. Petit, M. Feiri, and F. Kargl, “Revisiting attacker model for smart vehicles,” In WiVeC, pp. 1-5, 2014.

[6] A. Nguyen, J. Yosinski, J. Clune, “Deep neural networks are easily fooled: High confidence predictions for unrecognizable images,” In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 427-436.

[7] H. Shin, D. Kim, Y. Kwon, Y. Kim, “Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications,” In International Conference on Cryptographic Hardware and Embedded Systems, pp. 445-467, 2017.

[8] X. Mao, D. Inoue, H. Matsubara, and M. Kagami, “Demonstration of In-Car Doppler Laser Radar at 1.55 for Range and Speed Measurement,” IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 2, pp. 599-607, 2013.

[9] A. Samman, L. Rimai, J. McBride, R., Carter, W. H. Weber, C. Gmachl, and A. Y. Cho, “Potential use of near, mid and far infrared laser diodes in automotive LIDAR applications,” In Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. vol. 5, pp. 2084-2089, 2000.

[10] 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,” In 19th USENIX Security Symposium, pp. 11-13, 2010.

[11] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, and T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces,” In USENIX Security Symposium, pp. 77-92, 2011.

[12] A. Greenberg, “Hackers remotely kill a jeep on the highway－with me in it,” Wired, 2015.

[13] J. Golson, “Car Hackers Demonstrate Wireless Attack on Tesla Model S,” The Verge, 2016.

[14] 권혁찬, 이석준, 최중용, 정병호, 이상우, 그리고 나중찬, “자율주행 자동차 보안기술 동향”, 2018.

[15] 이유식. “자동차 보안 기술 동향”, 한국통신학회지(정보와통신), vol. 35, no. 7, pp. 3-10, 2018.

〈저 자 소 개〉

서 화 정 (Hwajeong Seo)
종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2016년 2월 : 부산대학교 컴퓨터공학과 박사
2015년 4월~5월 : 난양공대 인턴쉽
2016년 1월~2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 IT융합공학부 조교수
관심분야 : 정보보호, 암호구현, 사물인터넷

권 용 빈 (YongBeen Kwon)
학생회원

2018년 8월 : 한성대학교 IT응용정보시스템공학과 졸업
2108년 8월~현재 : 한성대학교 정보시스템공학과 석사 재학
관심분야 : 머신러닝, 정보보호, 부채널분석

권 혁 동 (HyeokDong Kwon)
학생회원

2018년 2월 : 한성대학교 정보시스템공학과 졸업
2018년 3월~현재 : 한성대학교 정보시스템공학과 석사 재학
관심분야 : 정보보호, 암호구현, 부채널분석

안 규 황 (Kyuhwang An)
학생회원

2018년 2월 : 한성대학교 IT융합공학부 졸업
2018년 3월~현재 : 한성대학교 정보시스템공학과 석사 재학
관심분야 : 정보보호, 암호구현