미래모빌리티 자율주행 차량의 원격운전 안전성 기술에 대한 연구

탈레*, 윤철희**
*경찰대학교 공공안전학과 박사과정
**경찰대학교 치안정책연구소
taleh.korea@police.ac.kr,bertter@police.ac..kr

A study on remote driving safety technology for future mobility autonomous vehicles

Taleh Bill*, Cheol-Hee Yoon**
* Korea National Police University
**Police Science Institute, Korea National Police University

요 약

본 논문은 .미래 모빌리티 긴급상황에서의 원격운전에 대한 안전성 보장과 자율주행 인프라 시설 요소기술에 대한 정보보호관점의 안전성 검토를 고찰하였다. 자율주행 원격운전의 기본적인 기술 플랫폼을 검토 후 핵심 요소인 V2X 통신과 자율주행 원격운전과 협력주행을 위한 전방위적인 취약점을 방지방안을 제시하였다. 자율주행차량 제조에서부터, ROS, 센서 프로세싱에 이루기까지 보안성 개발 프로세스를 통해 체계적이고 지속적인 안전 위험성 평가 수행 그리고 유관기관의 지침, 모범 사례, 설계 원칙 방안 등을 제시하였다.

1. 서론

현재 도로에서 운행중인 일반차량과 달리 멀지 않은 미래에 도로를 다니게 될 자율주행 차량은 자율주행을 위한 전용 도로시설, 전용 교통안전시설, 전용 통신시설 인프라를 통해 운행되고, 관리되며, 관제센터를 통해 도입기와 생성기 그리고 안정화가 될 것이다. 이를 안정적으로 밑받쳐주는 기술은 자율차량의 사고 데이터 분석을 보장 및 방지해주는 플랫폼이라 생각된다. 미래 모빌리티 환경에서의 긴급상황에서의 원격운전에 대한 이슈와 자율주행 인프라 시설에 대한 치안안전은 매우 중요하다. 인프라 위해서 작동하는 자율주행 차량 원격운전은 사회 안전과 치안 안전의 형평성 유지를 위해 더욱 중요하기 때문에 미래 모빌리티에 대한 자율차 원격운전 안전성과 무결성 보장을 위한 플랫폼에 대한 연구는 반드시 필요하다.

현재 경찰은 교통안전과 치안안전을 위해 신호제어, 정보제공, 사고예방, 사고방지 등 일반 차량의 교통과 안전 방향 운영을 주도하고 있다. 그리고 자율차의 안전운행과 사고 예방을 위한 원격운전에 대한 연구, 자율주행 차량 교통체계를 구축하고 운영하며 자율주행 차량의 사고 데이터에 대해 기술적 판단과 분석을 위한 관련 기술을 개발을 위해 노력하고 있다.[1] 본 논문은 자율주행 차량의 치안 안전을 위한 자율주행 원격운전에 대한 차 사고 안전성 보장을 위한 방법을 제시하였고, 자율주행시대의 교통안전을 확보하기 위한 기술적인 검토를 제시하였다.

2. 본론

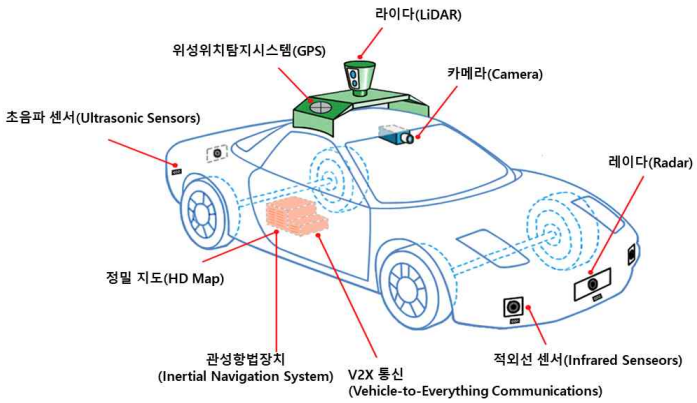
2.1 자울주행 원격주행 환경분석

현재 자율주행차는 각국의 정부기관들이 제도를 반영하기 어려울 정도로 급격한 속도로 발전하고 있기 때문에 향후 자율주행 차량에서 생성되는 데이터의 무결성 보장과 안전을 위한 원격운전 지원 플랫폼 구성은 매우 중요한 역할을 할 것이다. 또한, 자율주행과 관련하여 차량 운행에 필요한 기반기술로는 V2X(Vehicle to Everything) 통신기술의 안정성 확보인데, 고신뢰성·저지연 차량-인프라간 통신연결이 요구되고 연결체계의 고도화와 보급의 활성화가 필요하다. 특히 V2X통신의 인프라 협조형 자율주행 및 커넥티드 기술 기반의 서비스 구현을 위해서는 필수적이라 할 수 있다. 고정밀지도 역시 필수 기반기술인데,

자율주행 레벨3 이상은 클라우드 기반의 고정밀지도와 주행상황인식 기반 동적맵 기술이 중요하며 생성 데이터 역시 자율차 사고 분석에 큰 영향을 미친다. 이러한 기반기술과 연계되는 경찰의 교통시스템 또는 경찰의 업무와 관련된 응용 기술로 정보보호에 대한 안전성이 보장되어야 한다. 또한, 자율주행 차량의 사고에 직접적인 연관되어 있는 자율주행 신호제어 시스템 역시 AI기반 자율주행 신호제어 시스템 개발, 자율주행 교통정보의 실시간 수집 및 제공기술 개발, 자율주행자동차의 교통운영 및 관제 플랫폼 개발 등이 이루어져야 하며, 자율주행 차량에서의 일어난 교통사고 조사 동안 안전운행을 위한 자율주행 인프라는 IoT 기반 자율주행 교통안전시설물, 교통안전 인프라 통합관리 시스템, 교통안전시설물, 교통정보센터와 자율주행차량 간 V2I 정보교환 기술 등 신규기술의 개발이 같이 수반되어야 원활한 자율주행 원격 운전 준비가 이루어 질 것이다.

2.2. 자율주행 원격주행 원격운전 환경

자율주행 기술을 실현하기 위해 다양한 센서와 통신 모듈이 필요하기 때문에, 역으로 센서의 교란, 통신 해킹 등을 통해 사회 혼란을 야기시키고자 하는 범죄의 도구로 자율주행차가 사용되어질 수도 있는 위험성이 높아지고 있는 것도 사실이다. [그림1]]의 경우 자율주행차를 위해 주행환경을 수집하고 주행시 위치를 보정하기 위해 필요한 요소기술들을 설명하고 있는데, 카메라는 자율주행기술의 기본이 되는 센서로써 차량 인식, 보행자 인식, 차선 인식, 신호등 인식, 도로표지 및 표시 인식 등 자율주행에 영향을 끼칠 수 있는 환경 요소들을 인식하는데 사용된다. 이미지센서의 특성상 안개, 역광, 폭우 등 악조건 상에서는 인식률이 떨어질 수 밖에 없기 때문에 단독으로 사용하기는 힘들고 레이다와 다른 센서와 혼돈하여 사용하는 것이 일반적이다. 레이다는 객체와의 거리, 이동 방향, 속도 등을 인식하는데 사용되어지며, 환경에 강건하고 비교적 저렴하다. 근거리 레이다(80m 이하), 중거리 레이다(160m 근방), 원거리 레이다(200m 이상) 등을 복합적으로 사용하여 다양한 거리의 객체를 인식할 수 있다. 또한, 라이다는 정밀한 3D 형상 인식이 가능한 센서로 높은 해상도로 정확한 거리 값을 얻어낼 수 있는 것이 특징이다. 다만, 카메라나 레이다 보다 상대적으로 가격이 비싸며 짙은 안개와 같은 악조건 상에서는 센싱 능력이 떨어질 수 있다. 적외선 센서는 저조도 환경에서 차선, 보행자, 자전거등을 인식하는데 사용되어지고 초음파 센서는 주차보조시스템이나 근거리 장애물 인식 보조 시스템에 사용된다. 자율주행차가 출발지부터 목적지까지 차선을 바꾸어가며 주행하기 위해서는 정밀맵이 필요하며 자율주행차의 정확한 위치 추종을 위해서 GPS 수신기와 관성항법장치(INS)가 함께 사용된다.



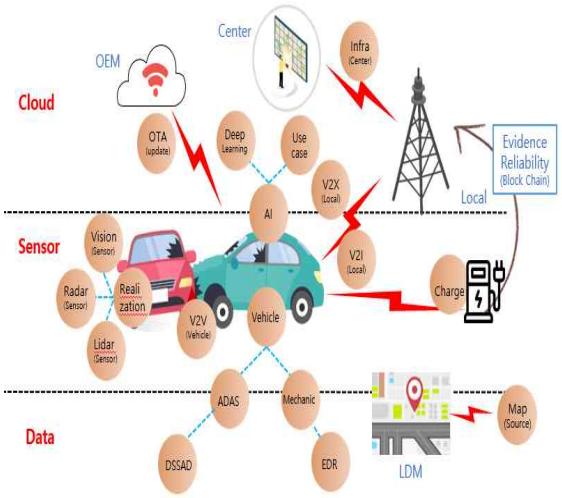
[그림 1] 자율주행차 요소기술

※ 출처: Center for Sustainable Systems, Autonomous Vehicles Factsheets Mobility (Ann Arbor, MI: University of Michigan, 2018)

여기서 주목할 것은 자율주행차의 원격운전 역시 V2X 통신을 기반으로 안전한 자율주행 기능을 수행할 수 있는 것 뿐만 아니라, 차량내 편리하고 다양한 모빌리티 서비스를 제공하기 위해 연결을 하고 있다. 차량간의 통신인 V2V(Vehicle-to-Vehicle)과 자율주행을 위해 중앙정부나 지자체에서 운영하는 도로 및 인프라와의 통신인 V2I(Vehicle-to-Infrastructure), 스마트폰을 이용하여 차량의 접근성과 편의성을 제공하기 위한 V2D(Vehicle-to-Nomadic Device)과 안전한 주행을 위한 자전거, 이륜차, 퍼스널 모빌리티 수단 등과 통신하는 V2P(Vehicle-to-Pedestrian) 그리고 집안의 다양한 가전과 차량이 연결되어 차량 원격 호출, 콘텐츠 공유, 스마트홈 원격제어 등 편리한 서비스를 제공하기 위한 V2H(Vehicle-to-Home), 차량과 전력망 사이의 통신인 V2G(Vehicle-to-Grid), 그리고 제조사에서 OTA(Over the Air)로 차량내 소프트웨어를 업데이트, 원격으로 차량상태를 모니터링 및 관리, V2N(Vehicle-to-Network), V2S(Vehicle-to-Service),

V2C(Vehicle-to-Cloud) 등의 방식들을 사용한다. [1] 이와 같이 자율주행차를 위한 원격운전의 기본적인 기술 플랫폼은 현재 고도화가 이루어지고 있는 상태이며 그 요소에는 V2X 통신은 필수 요소가 되고, 이를 통해 이용자에게 편의성을 제공하고 있으며 자율주행차의 핵심 기술로 사용되게 된다. [1]

앞에서 언급한 통신의 취약점을 악용해 악용해 사이버 해킹을 시도하게 되는데 자율주행 원격운전과 협력주행을 위한 전방위적인 통신 취약점을 악용하게 된다. 이런한 취약점을 방지하기 위해서는 자율주행 차량 제조에서부터, ROS, 센서 프로세싱에 이루기까지 보안성 개발 프로세스를 따라야 한다.[2] 자율주행 시스템에 대한 체계적이고 지속적인 안전 위험성 평가를 통해 유관 기관의 지침, 모범 사례 및 설계 원칙 등을 고려 후 자율주행 원격운전 차량에 대한 정보보안 활동에 대한 준비를 해야 한다.[2]-[4]



[그림 2] 자율주행 원격운전 위협 요소

※ 출처: 치안정책연구소, 자율주행 위협요소, 조민제

3. 결론

자율주행 차량은 레벨 3을 넘어 지속적으로 발전하고 있으며 원격운전, 자율주행 차량의 사고처리를 대비하기 위한 준비를 해나가고 있다. 자율주행 차량에서서 생성되는 데이터의 종류와 크기, 형태, 유통, 통신방식, 저장형태 등을 분석하기 위한 표준화 등 여러가지 준비 또한 중요하다. 그리고 제조사, 설계자, 통신업체, 운영자, 운전자 등 다양한 자율주행 교통사고 발생원인에 대해 분야별 전문가를 양성해야 한다. vision, radar, ridar 등 각 센서 인식 오류와 차량자체 결함의심, LDM 등 정밀지도 오류, V2X 동 통신업체 외 오류, OTA 등 SW 업데이트 오류, 혹은 사이버공격 까지도 자율차 원격운전에 대한 취약점이 될 수 있기 때문이다. 이런 다양한 원인을 종합적으로 분석하고 대응하는 전문가는 현재 양성되지 않고 있으며, 각 자율주행 교통사고 원인 별 분석 기반 데이터 수집 근거 뿐만 아니라 이를 분석할 수 있는 전문가 양성에 최선을 다해야 한다.

1) 심상규.(2018).자동차의 변화와 보안.한국멀티미디어학회지,22(2),25-35.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No.2021-0-01352, 자율주행 관련 법규 및 규제 대응 서비스 시나리오 실효성 검증 기술 개발)

참고문헌

[1] 김남선, 자율주행 기술동향 및 테러위협에 관한 고찰, 대테러연구, 경찰청

[2] 이만종, “지능형정보화 시대의 테러유형과 대응방안: 인공지능에 기반한 테러중점”, 국방연구 pp93-130, 2017

[3] 장승연 (2015). 안전소프트웨어를 위한 소프트웨어 테스팅 관점에서의 차량기능안전 표준(ISO26262) 적용 방안 논의. 정보과학회지, 33(7), 27-32

[4] 강성훈(2018), AUTOSAR 플랫폼 기반 ECU에서의 CAN메시지 처리S/W구조 최적화 연구, 한국자동차공학회, 추계학술대회, 512-516