자율주행 자동차 전망과 취약점

지도교수 : 이 강 호
연 구 자 : 윤 호 근

< 목 차 >

1. 서론

2. 자율주행 자동차 기술단계와 전망
2.1 자율주행 자동차 기술단계
2.2 자율주행 자동차 전망

3. 자율주행 자동차 취약점 및 분석
3.1 자율주행 자동차 취약점
3.2 자율주행 자동차 보안 위협

4. 결 론

요 약

자율주행 자동차는 운전자의 별다른 조작 없이 차량이 스스로 목적지에 도착하는 기술을 도입한 자동차로 점점 고도화된 기술이 포함된 자동차가 상용화되어 판매가 되고 있는 만큼 소비자들도 점차 관심을 가지고 있으며 편리함으로 인해 자율주행이 탑재된 차량을 구매하는 소비자 비중도 늘고 있는 추세이다. 현재의 자율주행 자동차는 생산 및 개발이 진행 중이나 사람이 조작하지 않는 완전한 자율주행이므로 보안이라는 문제가 남아있다. 이러한 자동차의 전망과 취약점 및 보안적 문제들이 무엇인지 조사하게 되었다.

주요어 : 자율주행 자동차, 보안위협, 취약점

1. 서론

자율주행 자동차는 운전자가 차량을 운전하지 않아도 스스로 움직이는 자동차를 말한다.

자율주행의 개념은 1960년대에 벤츠를 중심으로 제안되었고, 1970년대 중후반부터 초보적인 수준의 연구가 시작되었다. 초기에는 아무런 장애 요소가 없는 시험 주행장에서 중앙선이나 차선을 넘지 않는 수준이었으나, 1990년대 들어 컴퓨터의 판단 기술 분야가 크게 발전하면서 장애물이 개입되는 자율주행 분야가 본격적으로 연구되기 시작했다.

한국에서도 1990년대 후반부터 국책 교통연구기관과 고려대학교 연구팀을 중심으로 본격적인 연구에 돌입했으며, 잘 알려져 있지 않지만 2000년대 초반 이미 자유로에서의 자율주행 기술을 상당 수준으로 완성하는 데 성공했다

첨단 자동차 기술이 발전하면서 이제 자율 주행 자동차를 향한 꿈은 현실이 되어가고 그리고 자율주행 자동차는 최근 자동차 시장의 큰 화두로 떠올랐다. 자율주행 자동차 개발을 위하여 많은 단체들이 나서고 자동차 기업은 물론, IT 기업, 운송 기업, 컴퓨터 부품 제조 기업들도 자율주행 기술 개발에 뛰어들어 경쟁 또한 치열하다. 또한 자동차가 스스로 움직이기 위해서는 다양한 기술이 필요하다. 특히 주변 사물을 인식할 수 있는 첨단 센서와 성능 높은 그래픽 처리 장치의 도움이 필요하다. 첨단 센서는 사람처럼 사물과 사물의 거리를 측정하고 위험을 감지하여 사각지대(보이지 않는 곳) 없이 모든 지역을 볼 수 있도록 도와주며 그래픽 처리 장치는 여러 대의 카메라를 통해 자동차의 주변 환경을 파악하고 그 이미지를 분석해서 자동차가 안전하게 갈 수 있도록 도와준다. 여러 안전 표지판의 의미를 파악한다거나, 앞의 자동차가 급정거를 하지 않는지, 갑자기 사람이나 동물이 도로에 뛰어드는 것은 아닌지 등을 파악할 수 있게 만들어 준다.

2. 자율자동차의 기술단계와 전망

2.1 자율주행 자동차 기술단계

도로교통안전국(NHTSA)은 자율주행자동차를 운전자의 개입의 여부와 정도에 따라서 총 5단계로 나누었다. 먼저 0단계는 자율주행기술을 전혀 갖추고 있지 않은 단계로 우리가 주위에서 많이 볼 수 있는 대다수의 자동차가 이 단계에 속해있다. 그러므로 운전자는 운전의 모든 권한을 가져야 한다.

1단계는 자율주행기술이 일부 적용된 자동차가 포함된 단계로서 운전을 보조하는 기술이 들어가 있다. 차선 유지 시스템이나 크루즈컨트롤 같은 운전자 보조 시스템을 갖추고 있어서 운전자가 일반적으로 운전하거나 다른 차량과의 충돌하기 바로 전 상황에서의 일부 기능을 제외한 자동차 제어권을 가진다.

2단계에서는 그 전 단계인 1단계의 기술이 탑재된 상태에서 제어기능이 결합하여 운전자를 보조하는 역할을 한다. 대표적인 것으로는 차선유지 기능과 결합한 적응형 순항제어(ACC: Adaptive Cruise Control)를 꼽을 수 있다. 2단계에서는 운전자가 핸들과 페달을 자유롭게 다룰 수 있지만, 1단계와 마찬가지로 운전자는 주변을 주시해야 한다.

3단계는 제한된 자율주행 단계로 운전자가 운행주도권을 자동차에게 완전히 넘겨줄 수 있는 단계로, 이 때는 운전자가 조작 및 감시를 하지 않아도 된다. 하지만 자동차는 자율주행이 불가능한

상황이 오면 스스로 이를 판단하여 운전자에게 운행권을 넘겨준다. 즉 3단계는 자동차와 운전자가 서로 운전할 수 있는 상황을 변환시킬 수 있는 단계라고 말할 수 있다.

마지막으로 4단계는 완전 자율주행 단계라고도 불리며, 운전자의 개입이 없어도 되는 단계이다. 운전자가 정해준 목적지까지 스스로 갈 수 있으며 자동차가 전적으로 모든 상황을 책임지게 된다. <표1>은 자율주행의 기술단계에 따른 변화를 보여준다.

단계	운전자 개입	제어주체	책임주체
Level 0	필요	운전자	운전자
Level 1	필요	운전자 또는 자동차	운전자
Level 2	필요	자동차	운전자
Level 3	필요	자동차	운전자 또는 자동차
Level 4	필요없음	자동차	자동차

<표1> 자율주행의 기술단계에 따른 변화

2.2 자율주행 자동차 전망

글로벌 시장조사기관 IHS와 컨설팅 전문 업체 맥킨지(Mckinsey)에 의하면 자율주행자동차는 2030년에 1,720만대로 전 세계 신차 수요의 15%를 차지할 전망이다. 3만 5천 달러의 자율주행 자동차가 가능해지면 3만 달러 이상의 중 대형차 및 고급차의 저가사양 모델의 경우 레벨3 이상의 부분자율주행 기능은 기본사양이 될 가능성이 높다. 3만 5천 달러의 차량가격은 대중적인 차량가격 수준인 2만 5천 달러에 비해서는 여전히 비싸고 신흥국의 경우 인프라 문제로 기존 내연기관 자동차는 2025년 이후에도 시장의 상당부분을 차지할 것으로 예상된다.

그러나 레벨2의 자동차는 대중차와 신흥국에서도 기본사량으로 자리 잡을 것이다. 반면, 자율 주행 기술이 없는 내연기관 자동차의 수요는 2020년 이후 매년 3% 정도의 수요 감소가 예측된다. IHS는 레벨4의 완전자율주행자동차는 2025년에 23만 대에서 2035년에 98.5만대까지 보급될 것으로 전망하였다.

<표2>는 자율주행 자동차(레벨4) 의 세계시장 전망을 보여준다. 자율주행 자동차(레벨4)의 수요가 증가함 에 따라 기존에 일반 내연기관 차량 대수가 감소하는 것을 <표3>을 통해 볼 수 있다.

25년	26년	27년	28년	29년	30년	31년	32년	33년	34년	35년
23.0	27.1	32.0	36.5	43.0	50.8	59.9	70.7	83.5	83.5	98.5

<표2> 완전 자율주행 자동차(레벨4) 세계시장 전망 (단위 : 만대)

구분	2015	2020	2030
일반 내연기관차 대수	86,000	92,888	71,300
전체 대비 비중	98.9	92.9	62.0
연평균 성장률		1.6	-2.6
자율주행자동차 대수	0	230	17,250
전체 대비 비중	0.0	0.2	15.0
연평균 성장률			54.0
공유자동차 대수	100	500	10,000
전체 대비 비중	0.1	0.5	8.7
연평균 성장률		38.0	34.9
전체	87,000	100,000	115,000

<표3> 글로벌 자율주행 자동차 대수 추정 (단위 : 천대, %)

출처 : 한국자동차산업협회, 주요업체별 자율주행차 개발동향, KAMA 자동차산업 ISSUE PAPER, 2016.

대부분의 자율주행자동차 개발업체들은 레벨3의 자율주행자동차의 상용화는 2020년, 레벨4의 완전 자율 주행 자동차의 상용화는 2030년을 목표로 하고 있다. 레벨4의 구현을 2050년 이후로 예상하는 보수적인 전망도 다수 존재한다.

한편, 국내에서의 자율주행 대중화는 2050년경에 가능할 것으로 예측하고 있다. 글로벌 제조사들이 수년 내에 상용화를 자신하고 있으나 2020년경에는 시속 30~40km 정도로 한산한 지역에서 일부 운영될 것으로 보고, 실제 도심지의 혼잡한 도로의 경우 보행자, 자전거, 일반 자동차 등 다양하고 복잡한 조건에서는 운행이 어려울 것으로 보고 상당한 시간이 요구된다는 관측도 있다.

2020년경부터 자율주행자동차가 일부 운행되기 시작하는데 완전 자율 주행 자동차가 대중화 되기 전까지 상당 기간 동안 부분 자율주행자동차의 시대가 지속되고 부분 자율주행자동차와 일반 자동차의 공존하는 셈이다. 이후 완전자율주행자동차와 부분 자율주행자동차가 공존하는 기간도 상당할 것이다.

부분 자율주행자동차의 경우 완전 자율주행자동차에 비해 보다 복잡한 사고책임 부담 문제를 해결해야 할 것으로 보이므로 자율주행자동차의 발전단계별로 구분하여 방향성을 모색할 필요가 있다.

다양한 기관에서 자율주행 기술이 도입되는 시기를 예측한 자료에 따르면, 완벽한 자율주행 자동차의 기술이 적용 후 성숙되고 보편화 되는 시점은 2030년 이후로 예측되고 있다. 그러나 이러한 예측은 추정치이며, 매년 기술도입의 예측시점이 앞당겨지고 있는 추세이다. 한국산업기술평가관리원은 자율주행 자동차의 판매량 비율은 2030년 50% 미만에서 2035년 75%로 급 증가할 것으로 예측했다. 또한 2013년 글로벌 시장조사기관 Navigant Research는 같이 자동차 세계 3대 시장(북미, 서유럽, 아시아태평양)에서의 성장속도가 2020년 8,000대에서 2035년 9540만대로 연평균 성장률 85%를 기록할 것으로 전망하였으며, 2035년에는 자동차 판매량의 75%가 자율주행 자동차 일 것으로 예측했다.

3. 자율주행자동차 취약점 및 분석

3.1 자율주행자동차 취약점

자율주행자동차는 하나의 스마트폰이 차량에 탑재되었다고 볼 수 있을 만큼 지능적이고 다양한 ICT 기술들이 적용 되어있다. 그러므로 자동차에 대한 사이버 공격을 받을 수 있는 가능성이 존재한다. 자동차를 세 가지로 분류해보면 물리적인 움직임을 담당하는 구동부와 자동차의 엔진이나 변속기를 제어하는 전자제어장치(Electronic Control Unit, ECU), 차 안에서 외부를 연결시켜주는 인포테인먼트(infotainment)시스템으로 구분된다. ECU는 CAN(Controller AreaNetwork)를 통해서 제어가 가능하다. 이로 인해서 공격자는 CAN을 이용하여 ECU 영역을 침범해 자동차를 급제동을 가능케 하거나 브레이크 페달을 무력화 시킬 수 있다. 인포테인먼트(Infotainment) 부분에서는 자동차 내부의 네비게이션에 스마트폰 화면을 그대로 비춰주는 '미러 링크' 기술이 취약점으로 발견되었다. AVN(Audio, Video, Navigation) 시스템에서도 CD 등을 통해 취약점 공격이 가능하고 GPS를 통한 해킹에도 취약하다. 또한 블루투스를 이용하여 외부로부터 전송된 파일들을 통해서 악성코드가 감염 될 수 있다. <표4> 는 자율주행자동차를 이용하는데 있어 발생할 수 있는 취약점을 보여준다.

취약점	설명
ECU	• TPMS(타이어 공압 모니터 시스템) 해킹으로 ECU에 전달 그로 인한 무선 통신 가능 • 자동차 접근 시스템 • 회전 및 브레이크 접근 • 조명 시스템 접근 • 차량자가진단장치(OBD-Ⅱ)로 ECU에 접근 가능
인포테인먼트	• 미러링크 활성화하여 접근 통제 가능 • V2X를 통한 차량의 내부 시스템에 접근
AVN 시스템	• CD 등을 통한 펌웨어 취약점 공격 가능
블루투스	• 블루투스를 통해 다운받는 파일들로 인한 악성코드 설치

<표4> 자율주행자동차의 취약점

3.2 자율주행 자동차 보안 위협

자율주행자동차의 보안 취약점이 증가하면서, 취약점을 이용한 다양한 보안 위협이 발생 한다. 자동차에 대한 다양한 보안 위협과 이에 대응하기 위한 다양한 보안솔루션들이 연구 개발되고 있으나, 결국 자동차에 있어서 가장 큰 보안 문제는 인가되지 않은 데이터가 차량 내부 네트워크로 주입되는 것과 Dos등의 공격을 통해 자동차의 가용성이 침해되는 것이다. 이러한 목적을 위해 다양한 공격방법 및 위협이 존재한다. <표5> 는 자율주행 자동차에 대한 보안 위협을 플랫폼, 네트워크, 관리/진단 측면에서 구분하여 정리하였다.

분류	보안 위협
전장 플랫폼	• ECU 소프트웨어 결함, ECU 리버스 엔지니어링 • ECU 펌웨어 해킹 및 위/변조 • 위장 ECU장착 • IVI (In-Vehicle Infotainment) 해킹, 악성 감염 스마트 센서 물리 공격 (블라인딩, 스푸핑, 재밍)
내부 네트워크	• 차량 내부네트워크에 악의적인 제어 메시지 주입 • 정상적인 내부네트워크 방해(패킷 삽입, 삭제, 임의조작, 지연 등), 도청 • DoS, 리플레이, 스푸핑, 패킷 폐기 공격
외부 네트워크	• 무선 통신망 해킹, DoS공격 • 위장 OBU(Onboard Unit), RSU(Road Side Unit) • 거짓정보(Fake message) 제공 • 차량 접속 기기 해킹
관리, 진단	• 프라이버시 침해, OBD-Ⅱ 해킹 • 원격 업데이트 및 진단 프로토콜 해킹 • 해킹에 의한 사고원인 분석/증거 보존의 어려움

<표 5> 자율주행 자동차에 대한 보안위협

4. 결론

자율주행자동차 시장규모는 향후2030년 에는 2020년 보다 10배에 가까운 규모로 성장 할 것이라고 전망했다. 또한 신차판매량 중 자율주행자동차의 비중이 급격히 증가할 것 이라고 예측하고 있다. 자율주행 자동차는 운전자의 별 다른 조작 없이 스스로 목적지에 도착하는 자동차이다. 자율주행자동차 판매가 증가하는 만큼 보안은 아주 중요한 요소가 될 것이다. 자율주행 기술이 포함하고 있는 보안 취약점으로 인해 인명사고나 개인정보유출 사생활 유출 등 더 많은 위험이 생길 것으로 예측되고 있다. 그러므로 자율주행기술의 취약점 분석을 알아두고 그에 관련된 보안고려사항을 꼭 지켜 주어야 한다.

참고문헌

김예지, 이영숙(2017.7) 자율주행자동차의 취약점 및 보안 고려사항에 대한 연구 | 한국컴퓨터정보학회 학술발표논문집 25(2)

권혁찬, 이석준, 최중용, 정병호, 이상우, 나중찬(2018) 자율주행 자동차 보안기술 동향 | No. B0717-16-0097, 자율주행차량을 위한 V2X 서비스 통합 보안 기술 개발

자율주행자동차(무인자동차)의 장단점, 동향 및 자율주행자동차의 전망 분석 (2017.12)