기업가정신,국민대학교
Entrepreneurship, The KOOKMIN

2024학년도 2학기 문헌연구보고서

(자율주행 4단계 앞에 닥친 보안 위협: 우리는 어떠한 자세를 취해야 하는가)

이름	신채원
전공	소프트웨어학부
학번	20213021

자율주행 4단계 앞에 닥친 보안 위협: 우리는 어떠한 자세를 취해야 하는가

소프트웨어학부 20213021 신채원

<목차>

Ⅰ. 자율주행 기술의 현재 동향

자율주행은 가장 대표적인 IoT(Internet of Things) 기술이라고 할 수 있다. 사용자는 탑승 후 목적지만을 입력하며, 주행에 대한 모든 과정은 시스템이 담당하는 것이 자율주행이 궁극적으로 추구하고 있는 목표이다.

자율주행이 적용되는 가장 대표적이고, 널리 알려진 사례가 바로 자동차이다. 자동차관리법 제2조 제1호 3에 따르면 자율주행 자동차는 “운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차를 말한다.”라고 정의되어 있다. 그렇다면 ‘운전자 또는 승객의 조작’의 범위는 어디까지로 정해져야 하는가? 이를 위해 미국자동차공학회(SAE: Society of Automotive Engineers)는 자율 주행 단계를 6단계로 구분하였다.

단계	기능	설명
Level 0	비자동화	운전자가 모든 것을 통제한다.
Level 1	단일 주행 보조 기능	운전자가 대부분 통제하며, 차선 유지 등에 대해서만 시스템의 통제가 이루어진다.
Level 2	복수 주행 기능 융합 보조	시스템의 일정 시간 동안 보조 주행이 가능하며, 운전자는 주행상황을 주시해야 한다.
Level 3	제한된 자율주행	특정 조건에서 제한된 자율주행이 가능하며, 위급 상황에는 운전자의 개입이 필요하다.
Level 4	완전 자율주행	시스템이 모든 것을 제어하나 운전자의 탑승은 필요하다.
Level 5	무인 완전 자율주행	시스템이 모든 것을 제어하며, 무인 주행이 가능하다.

<표 1> 자율 주행 단계 (SAE)

테슬라 등 상용 자율주행 자동차의 수준은 2~3단계 정도(권혁찬 외, 2018)이나, 사회에서 흔히 통용되는

‘자율주행’의 의미는 SAE의 4단계 이상인 경우가 대부분이다. 즉 현재까지는 운전자의 개입이 필수적인 상황이며, 시스템의 완전 자동화를 목표로 개발이 진행되고 있다고 할 수 있다. 시스템에 모든 제어를 넘기기 위해서는 우선 자율주행을 구성하는 인지, 판단, 제어의 세 단계에서의 기술적인 상향이 먼저 전제되어야만 한다.

이 글에서는 자율주행의 기본 원리와 각 단계가 안전성의 면에서 갖는 중요성, 자율주행 자동차의 중심이 되는 소프트웨어를 겨냥하는 보안 위협과 해결책을 살핀다. 그 후 자율주행 자동차에 대해 사회가 가져야 할 시각에 대해 논의해보겠다.

Ⅱ. 자율주행의 원리와 각 단계의 중요성

자율주행의 기본 원리는 인지, 판단, 제어의 세 단계로 설명할 수 있다. 자율주행 4단계 이상의 개발을 위해서는 이 모든 단계의 기능 상향과 함께, 일어날 수 있는 문제점에 대한 보완이 이루어져야 한다.

인지는 시스템이 도로의 시설물을 인식하는 등, 적절한 대응을 위해 주변의 환경을 파악하는 단계이다. 자율주행을 위한 첫 번째 단계인 인지는 사람의 눈과 같은 역할을 한다. 홍윤석(2015)에 따르면 이전에는 센서가 주로 자동차 내부의 작동상태나 주행상황을 모니터링하는 용도로 사용되었으나, 최근 첨단운전자지원시스템(ADAS: Advanced Driver Assistance Systems)의 적용이 확대되면서 자동차의 내부뿐만 아니라, 외부 주변 환경을 인지하는 수준으로 진화하고 있다고 한다.

이러한 인지 단계는 오류가 발생할 시, 사람에게 가장 직접적으로 해를 가하는 방향으로 영향을 끼치게 되는 단계이기도 하다. 2018년 3월, 미국 애리조나에서 우버 자율주행 자동차로 인한 사망 사고가 발생하는 일이 있었다. 보행자를 발견했음에도 불구하고, 이를 물체 혹은 다른 차량으로 인식하며 발생한 사고였다. 자율주행 자동차가 상용화되기 위해서는 주변 환경에 대한 명확한 인지가 필수 불가결한데, 카메라 등과 같은 ADAS 센서는 사각지대 등의 기술적인 한계로 인해 환경에 대한 명확한 구분이 어렵다. 우버 자율주행 자동차 사고는 이러한 점을 명확하게 드러낸 사고이기도 하다.

이를 극복하기 위해 위성 정보를 통해 차량의 현재 위치를 파악하는 GPS 방법, V2X(Vehicle to Everything) 통신 기술을 활용하여 환경을 인지하는 방법 등을 사용하고 있다. V2X 통신 기술은 차량과 대상이 되는 모든 물체가 서로 정보를 주고받을 수 있도록 하는 기술을 의미한다. V2I(Vehicle to Infrastructure), V2N(Vehicle to Network), V2V(Vehicle to Vehicle) 등이 V2X에 포함되는 대표적인 것들이라고 볼 수 있다.

자율주행 자동차의 위치가 파악되고, 주변 환경에 대한 인식까지 끝났다면 상황을 분석하고, 주행을 위한 가장 적절한 전략을 선택해야 한다. 이것이 판단 단계이다. 판단 단계에서 내려지는 결정은 주행 경로, 속도 및 추월 여부 등의 주행 전략 등이 해당할 수 있다. 인지 단계가 인간의 눈에 해당하였다면, 판단 단계는 인간의 두뇌와 비슷한 역할을 수행한다. 운전자의 개입이 필요한 현재의 자율주행 단계에서는 고려할 사항이 적어 판단에 오랜 시간이 소요되지 않는다. 그러나 시스템에 모든 제어를 넘기는, 4단계 이상의 완전 자율주행 단계에서는 현재보다 고려해야 할 사항들이 많아지기에, 소프트웨어의 상향이 필수적으로 요구된다.

마지막으로 제어 단계는 앞선 단계들에서의 판단을 통해 브레이크 제어, 조향 등 운전 시스템을 제어하는 단계이다. 제어 단계의 가장 큰 목표는 사고를 예방하고 안전 운전을 하는 것으로, 이 단계에 와서야 실질적인 주행이 이루어지는 것이라고 볼 수 있다. 제어 기능은 이미 성숙 단계에 접어들어 현재의 기술 수준으로 자율주행이 가능한 상태이며, 자율주행 기능을 구현하는 과정에서도 판단 단계에서 정확한 판단만 수행된다면 제어 단계에서는 주어진 목표값에 따라 적절하게 제어하면 된다(홍윤석, 2015).

판단 단계와 제어 단계는 굉장히 밀접한 관계에 놓여 있다. 두 단계는 ‘결정 및 수행’으로 요약이 가능하며, 이를 통해 소프트웨어가 이들의 핵심임을 알 수 있다. 주행 지원 시스템, 자동차 제어를 위한 횡 방향

및 종 방향 제어 알고리즘, 전장 장치 구동을 위한 소프트웨어와 경로 계획을 위한 지도 작성(장승주, 2016) 등은 판단과 제어 단계에서 요구되는 소프트웨어 기술이다. 점차 센서의 기술이 다양화되고 발전됨에 따라 판단/제어 소프트웨어는 자율주행 자동차의 핵심 소프트웨어가 될 것(권순홍·이종혁, 2020)이다.

자율주행의 기본이 되는 각 단계에서의 기술이 점차 상향화됨에 따라, 자율주행 자동차의 시스템 보안은 안전성을 결정하는 대표적인 요소가 될 것이다. 그러나 앞서 소개했던 GPS 기술의 경우 신호를 왜곡하는 것에 복잡한 기술이 필요하지는 않으며, V2X 통신 기술은 보안 취약점이 이미 뚜렷하게 알려진 상황이다. 판단 및 제어 단계에서 사용되는 다양한 소프트웨어들은 모든 프로그램이 그렇듯이 해킹이 발생할 수 있는 잠재적인 가능성이 존재한다. 이러한 기술들이 갖는 취약점을 포함하여, 자율주행 자동차의 시스템에서 발생 가능한 보안 위협에 대해 자세히 알아보겠다.

Ⅲ. 자율주행 4단계에서 발생 가능한 보안 위협

자율주행 자동차는 다양한 센서와 프로그램으로 구성되어 있다. 또한 자율주행 시스템의 핵심인 ITS(Intelligent Transport System)를 통해 원활한 자율주행을 선보인다. 그러나 이는 제삼자가 악의적인 의도를 갖고 공격을 수행할 수 있는 경로가 다양함을 의미하기도 한다. 자율주행 시스템에 대한 공격은 인지, 판단, 제어의 세 단계 모두에서 발생할 수 있다.

인지 단계에서 발생할 수 있는 가장 대표적인 공격인 GPS 스푸핑과 재밍 공격이다. GPS는 인지 단계에서 차량의 위치 추정에 사용되며, 이렇게 얻은 위치를 통해 자율주행 자동차는 이동 경로를 설정한다. 그러나 GPS 기술의 기반이 되는 지구의 위성항법시스템(GNNS: Global Navigation Satellite System)은 근본적인 약점이 존재한다. 태양 활동에 의한 자연적 간섭현상에서부터 우발적인 발신 장치 오작동이나 신호 반사, 악의적인 신호 교란에 이르기까지 다양한 형태로 발생된 교란에 취약하다(허노정, 2011)는 것이다.

GPS 재밍 공격은 GNNS의 이러한 특성을 이용하여 의도적으로 전파를 교란시키는 것이다. GPS 재머의 사용은 법으로 금지되어 있음에도 불구하고, 인터넷에서는 기기를 저렴한 값에 구매할 수 있으며, 심지어 재머의 회로도 또한 공개되어 있다. GPS 재밍 공격은 예전부터 다양한 분야에서 발생하고는 했던 공격이다. 비슷하게 GPS 스푸핑은 공격자가 자신이 의도적으로 발생시킨 신호를 GPS 수신기로 보냄으로써 수신기가 올바르지 않은 정보를 인식하게끔 하는 것이다. 이 방법은 신호의 크기가 굉장히 약하다는 GNNS의 특징을 이용하여 공격자의 신호가 GNNS의 신호를 압도하게끔 한 것이다. 이러한 공격들은 차량의 위치가 공격자가 설정한 위치로 파악되게끔 함으로써 물리적 사고가 발생하도록 한다.

ITS를 구현하기 위해 사용되는 V2X 네트워크를 공격하는 방법 또한 존재한다. 한국인터넷진흥원의 스마트교통 사이버보안 가이드에서는 V2X 통신을 통해 “블루투스, Wifi, USB 등을 통해 차량 내에서 외부 기기와 연결이 가능”하다고 이야기하였다. 그러나 이러한 통신 채널의 경우 본질적으로 취약하고 공격자가 악용할 수 있는 알려진 버그 및 취약점을 포함하고 있다(권순홍·이종혁, 2020).

가장 대표적인 통신 기기인 스마트폰은 다른 장치와 상호작용하기 위한 인증 절차가 별개로 필요하지 않다. 이는 즉 인증되지 않은 장치이더라도 스마트폰과 상호작용이 가능하다는 이야기이며, 이로부터 스마트폰은 항상 공격 위험에 처해 있음을 알 수 있다. 이러한 스마트폰과의 연결은 자율주행 자동차로 하여금 잠재적인 취약점을 가지게 한다.

V2X 통신 중 한 종류인 V2V(Vehicle to Vehicle) 네트워크를 대상으로 한 스푸핑도 발생할 수 있다. V2V 네트워크는 추월, 차선 변경 등을 근처 차량에 알리기 위해 사용된다. 그러나 이 네트워크는 제삼자가 데이터를 도청하여 중요한 정보를 가져오는 것이 가능하다는 것이다. 이를 통해 공격자는 자율주행 차량이 자신의 차량과 연결하여 데이터를 송신할 수 있게끔 한다. 또한 이러한 연결로 인해 공격자가 대상이 된 차량의 데이터를 수신하고 악용할 수 있다는 가능성이 존재한다.

이러한 수많은 보안 위협은 단순히 물리적 사고 발생에서 그치지 않는다. 현재 전 세계의 자율주행은 도로인프라 등과의 협력주행을 통해 자율협력주행으로 나아가(윤성현, 2016)는 방향으로 목표를 설정하고 있다. 이를 위해서는 도로인프라에서 자동차에 많은 정보를 제공해주어야 하며, 이렇게 쌓이는 수많은 정보는 모여 누군가의 개인정보가 될 수 있다. <표 2>는 자동차가 요구하는 정보, 도로인프라가 제공하는 정보 중 대표적인 몇 가지를 안내하고 있다.

자동차가 요구하는 도로인프라 정보	- 실시간 교통정보 (사고 차량, 비상 차량 운행 등) - 교통운영 시스템 (속도제한 장치 등) - 물리적 인프라 (차선, 도로 파손 등)
도로인프라가 자동차에 제공하는 정보	- 도로 표지판, 안전 표지판, 가변 표지판 내용 - 신호 주기, 잔여 녹색 시간 - 자율주행 구간 및 차로 지정 여부

<표 2> 자율주행 자동차 운행을 위해 요구되는 정보

실제로 윤성현(2016)은 “온타리오주 자동차협회의 보고서에서도, ‘차량 안에는 지나가는 이들을 스캔하는 레이저는 없겠지만. 필요를 인식하고 또 이에 반응하는 향상된 시스템은 분명 존재할 것이다. 이를 통해 자동차 회사들은 지나가는 이들의 목소리, 이름, 나이 및 기타 특성들, 그들의 특정한 주소, 직장, 학교, 별장, 일상적으로 걷는 길 등과 각각의 가족 구성원들이 차량을 이용하는 특정 시간대 등의 정보를 포함한 개인정보를 이용할 수 있다.’고 하여 개인정보에 대한 각별한 주의를 당부한 바 있다.”라고 말하였다.

자율주행 자동차가 수집하는 정보들은 모두 V2X 통신을 통해 외부로 전달된다. 그러나 보안에 취약한 V2X 통신을 대상으로 한 해킹으로 인해 정보가 도청되면 개인정보 유출의 피해가 발생하게 될 것이다. 수집되는 정보의 범위에 대해서도 각별한 주의가 필요하지만, 수집 이후에도 오·남용되거나 외부로 유출되지 않도록 주의를 기울일 필요가 있다.

Ⅳ. 보안 위협에 대한 해결 방안

1. 기술을 통한 해결

자동차에 대한 다양한 보안 위협과 이에 대응하기 위한 다양한 보안 솔루션들이 연구 개발되고 있으나, 결국 자동차에 있어서 가장 큰 보안 문제는 인가되지 않은 데이터가 차량 내부 네트워크로 주입되는 것과 DoS 등의 공격을 통해 자동차의 가용성이 침해되는 것이다(권혁찬 외, 2018).

V2X 통신의 경우 이미 취약점이 널리 알려져 있기 때문에, 이에 대한 연구도 다양하게 진행되고 있는 상황이다. V2X 통신을 통해 수신 및 송신되는 데이터가 유출되는 것은 막을 수 없기에, 두 객체 사이에 오가는 데이터를 암호화하는 것을 목표로 두고 연구를 진행하고 있다. 이러한 목표를 달성하기 위해서 PKI(Public Key Infrastructure)가 사용된다.

일반적으로 사용되는 PKI는 인증서를 발급하고 검증하는 인증 기관(CA), 인증서 발급 대행 기관(RA), 인증서들을 보관하는 하나 이상의 디렉터리(LDA) 및 인증서 관리 서버로 구성된다(이유식 외, 2014). PKI가 주로 사용되던 기존의 시스템에서는 인증서의 소유자를 확인하는 과정이 중요했지만, V2X는 ‘차량’이 아닌, ‘신뢰할 수 있는가’의 여부에 주목한다. 차량 식별이 가능하게 된다면 이는 차량의 소유자를 알 수 있다는 의미로, 개인정보 보호에 대한 문제에 직면하는 것이기 때문이다.

이 때문에 V2X를 위한 PKI는 신뢰할 수 있는 CA로부터 인증서를 발급받은 정당한 개체인지만을 확인하게 하고, 인증서의 DN(Distinguished Name)를 통하여 차량을 식별할 수 없도록 익명성을 부여하는 것(이유식 외, 2014)에 주목한다. 그러나 현재까지 익명성을 부여하는 방식에 대해 정의된 표준은 없으며, 미국과

유럽이 각자의 방식을 따르고 있는 상황이다.

자율주행 시스템에 가해지는 공격에 대응하기 위한 방식으로는 분석 기술이 연구되고 있는 상황이다. 권혁찬 외(2018)에 따르면, 인텔은 미래 자동차 안전을 위한 보안 기술을 4가지로 분류하였으며, 파나소닉은 자동차 보안을 위한 라이프 사이클을 3단계로 정의하였다고 한다. 이들의 공통점은 모두 '지능형 분석'에 주목하고 있다는 것이다. 소프트웨어에 가해지는 대표적인 공격은 앞서 살펴보았던 것처럼 몇 가지로 축약할 수 있지만, 해커와 화이트 해커의 싸움은 결국 '시간 싸움'으로 정의될 수 있다. '얼마나 빨리 해결책을 찾느냐'가 승패를 좌우하기에, 사실상 시스템에 가해질 수 있는 공격은 무궁무진하다. 그러한 의미에서 딥러닝 학습을 통한 해결책 마련은 해킹으로 인한 피해를 예방하기 위한 가장 근본적인 해결책이라고 볼 수 있다.

해외에서는 이러한 인공지능을 기반으로 한 연구가 매우 활발하게 이루어지고 있다. 시만텍은 딥러닝을 기반으로 차량 내부네트워크의 트래픽을 학습하여 차량의 정상, 비정상 행위를 탐지하는 솔루션을 출시하였다(Symantec, 2016; 권혁찬 외, 2018).

이러한 분석 기술은 보안 위협을 해결하는 것 외에도 다양한 방면에서 활용될 수 있다는 점에서 또한 의미가 있다. 인공지능을 활용하여 차량을 분석하는 방식이기 때문에, 단순한 시스템 오작동에 대한 원인을 분석하는 일 등에도 사용될 수 있다. 우리나라는 아직 딥러닝을 기반으로 한 분석에 관한 연구가 많이 이루어지지 않은 상황이지만, 이에 관한 연구가 충분히 진행된다면 자율주행 4단계의 상용화 역시 기대해 볼 수 있으리라 생각된다.

2. 제도적 차원에서의 해결

2014년 11월, 자동차 제조업체 연합체와 글로벌 자동차 협회는 자발적으로 고객의 개인정보를 보호할 수 있는 원칙을 제정하였다. 그들이 발표한 Consumer Privacy Protection Principles는 총 7가지 원칙으로 이루어져 있으며, 원칙 수립에 동의한 글로벌 자동차 제조업체들은 각자의 방식으로 이를 이행해야만 한다.

Transparency (투명성)	수집 및 사용하는 개인정보는 투명하게 공개한다.
Choice (선택)	수집하는 정보의 자기정보결정권은 사용자에게 있다.
Respect for Context (수집 목적에 맞는 이용)	정보의 이용 방식은 수집 목적에 맞아야 한다.
Data Minimization, De-Identification & Retention (합법적인, 최소한의 데이터 수집)	정보는 목적에 맞게 최소한으로, 또한 합법적으로 수집하고 저장해야 한다.
Data Security (데이터 보호)	데이터에 대한 보호 조치가 취해져야 한다.
Integrity & Access (정보의 무결성 보장)	정보의 무결성을 유지하기 위해 합리적인 보호 조치를 취해야 한다.
Accountability (책임감)	해당 원칙을 준수하고 있음을 보증할 방안이 마련되어야 한다.

<표 3> Consumer Privacy Protection Principles

이러한 원칙은 업체들로 하여금 소비자의 개인정보 보호를 위해 노력할 수 있는 기준이 되어주었지만, 어디까지나 '자율적인' 참여를 요구하고 있다는 점에서 그 한계를 가진다. 이러한 원칙이 조금 더 넓은 범위에서 영향력을 발휘하기 위해서는 정부 차원에서의 법률 또는 가이드라인 제정이 이루어져야 할 필요가 있다.

이후 2016년 9월, 미국의 도로교통안전국(NHTSA)은 자율주행법(Self Drive Act)을 제정하며 자율주행의 안전 기준에 대한 가이드라인을 발표하였다. 가이드라인은 총 15개의 섹션으로 구성되어 있으며, 개인의 사생활을 보호하는 내용이 주요 사항으로 포함되었다.

전용일·유요한(2017)에 따르면 12번째 섹션의 Privacy Plan Required for Highly Automated Vehicles에서는 "제조사가 개인 정보 계획을 개발하지 않으면, 제조사는 고성능 자동화 차량 또는 부분적으로 자동운전이 가능한 자동차 또는 자동화 주행 시스템을 판매, 판매를 위한 제안, 주간(interstate) 상업거래에서의 소개나 배송할 수 없다."라고 정하였다고 한다. 개인정보계획은 자율주행 차량에 의해 "수집된 차량 소유자 또는 탑승자에 관한 정보의 수집, 사용, 공유 및 저장과 관련된 서면 개인 정보 보호 계획"을 의미한다고 한다.

이러한 국가 차원에서의 가이드라인 제정은 개인정보 위반에 대한 확실한 처벌의 근거를 지정해주며, 소비자로 하여금 자율주행 시장에 뛰어들게 한다. 이는 다시 자율주행 자동차의 활성화 및 상용화로 이어질 수 있다.

Ⅴ. 남은 과제들

앞서 보안 위협에 대한 몇 가지의 해결책들을 다루어 보았지만, 그것만으로 자율주행 자동차 4단계의 상용화가 이루어질 수 있다고 생각해서는 안 된다. 자율주행 4단계가 마주할 보안 위협은 언급된 것만이 전부가 아니며, 앞으로도 보안의 취약점이 발견되는 족족 그것은 다시 위협으로 돌아올 것이다. 보안 업계에서 '무엇이든 뚫는 창'이나 '무엇이든 막아내는 방패'는 존재하지 않는다. 할 수 있는 것은 공격자를 향한 '새로운 창'을 만들기 전까지 '최대한 버텨내는 방패'에 최선을 다하는 것뿐이다. 공격자가 계속해서 새로운 보안 취약점을 찾아 공략하듯이, 기술자들 또한 끝없이 새로운 해결책을 강구해내어야만 한다. 영원하다는 수식어는 승패 앞에 붙을 수 없다.

사실 자율주행 자동차의 상용화를 위해 가장 필요한 것은 '긴장을 놓지 않는 것'일지도 모른다. 보안 위협을 해결하는 것이 기술자들의 몫이라면, 우리는 자율주행 시스템을 현실에 들여놓고, 적용할 수 있도록 끊임없이 사회를 갈고 닦아야만 한다. 자율주행 4단계의 도입 여부는 자율주행의 첫 등장으로부터 몇 년이 지난 지금까지도 여전히 뜨거운 감자이다.

시스템에 제어권을 모두 넘긴 상태에서 인명 사고가 발생한다면, 그 책임은 누구에게 물어야 하는가? 열차가 선로 위를 달리고 있을 때, 현재의 선로 위에는 노동자 5명이 서 있고, 다른 쪽 선로 위에는 노동자 1명이 서 있다면, 열차는 어디로 향하는 것이 옳은가? 이때의 열차의 방향을 사람이 아닌 시스템이 결정해도 되는가? 이들은 자율주행 4단계의 상용화를 가정하고 던져지는 가장 대표적인 법적, 윤리적 문제이다.

보안 위협에 대한 해결책이 강구되는 동안 남은 사람들에게는 또 다른 과제가 주어졌다. 이러한 사회적 문제에 대한 끝없는 토의가 이루어지는 것이다. 해결해야 할 과제를 한가득 가지고 있는 자율주행 시스템에 대해, 우리는 가만히 앉아 상용화를 기다릴 것이 아니라, 적극적으로 질문하고 고민하는 자세를 갖춰야만 한다.

[참고 문헌]

- 권순홍·이종혁, 2020, 「자율 주행 자동차 보안 위협 및 기술 동향」, 『정보보호학회지』 30-2, 한국정보보호학회.
- 권용주, 2018. 5. 31., 「우버 자율주행 사고, 원인은 '인식 오류'」, 《오토타임즈》, http://autotimes.hankyung.com/apps/news.sub_view?nkey=201805310802331.
- 권혁찬 외, 2018, 「자율주행 자동차 보안기술 동향」, 『전자통신동향분석』 33-1, 한국전자통신연구원.

- 윤성현, 2016, 「자율주행자동차 시대 개인정보 보호의 공법적 과제」, 『법과 사회』 53, 법과사회이론학회.
- 이유식 외, 2014, 「V2X 통신을 위한 보안기술」, 『정보보호학회지』 24-2, 한국정보보호학회.
- 「자동차관리법」, https://www.law.go.kr/법령/자동차관리법, 2021년 6월 방문.
- 장승주, 2016, 「자율 주행 자동차 관련 SW기술 동향」, 『정보와 토신 : 한국통신학회지』 33-4, 한국통신학회.
- 전용일·유요한, 2017, 「미국 자율주행법(Self Drive Act)의 주요내용 및 시사점」, 『법학연구』 54, 전북대학교 법학연구소.
- 한국인터넷진흥원, 2019, 『스마트교통 사이버보안 가이드』, 호정씨엔피.
- 허노정, 2011, 「GPS 재밍 공격 대응 방안 비교 연구」, 『제어로봇시스템학회 합동학술대회 논문집』 1-1, 제어로봇시스템학회.
- 홍윤석, 2015, 「자율주행자동차의 기능 및 안전성 평가 방안」, 『월간교통』 2015-11, 한국교통연구원.
- https://itlaw.wikia.org/wiki/Consumer_Privacy_Protection_Principles:_Privacy_Principles_for_Vehicle_Technologies_and_Services