정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

# 커넥티드 카에서의 보안기술동향

박 현 경*, 안 효 범**

요 약

현재 자동차들은 차량 내부와 외부가 서로 유기적으로 연결된 장치들과 정보를 주고 받는 형태로 발전되고 있다. 이런 자동차들을 커넥티드 카(connected car)라고 한다. 커넥티드 카들은 인명과 관련되어 있어 보안에 대한 중요성이 강조되고 있다. 이 논문에서는 커넥티드 카의 시장 동향과 기술을 조사하고 분류한다. 또한, 커넥티드 카에서 발생하는 공격유형과 보안 취약점을 소개한다.

## Ⅰ. 서 론

현대의 자동차는 내부와 외부에 여러 종류의 연결 장치를 갖추고 있다. 따라서 커넥티드 카를 차량 자체와 차량 내 네트워크 및 ECU, 자동차 회사의 포털, 그들 사이의 통신 연결로 구성되어있다고 정의할 수 있다. 즉, 현대의 자동차가 차에 장착된 다른 모든 연결부를 포함하는 것을 커넥티드 카라고 할 수 있다.

미국 교통부에 따르면 커넥티드 차량 어플리케이션은 모든 시스템 사용자에게 지속적인 실시간 연결을 제공하기 위해 차량과 인프라 사이에 충돌을 방지하도록 하고, 안전성과 이동성 및 환경적 편의를 위해 차량 간 연결을 제공한다. 이 경우 인터넷의 연결을 필수적으로 보지 않고 일반적인 네트워킹 기능만이 고려되었다.

그러나 가장 최근의 문헌은 인터넷과의 지속적인 연결, 차내 대시보드에 인터넷 관련 서비스의 존재를 커넥티드 카의 필수 요소로 간주하고 있다. 스마트폰을 포함한 스마트 기기의 보급이 확대되면서 이들과의 연결성도 중요해졌다. 따라서 커넥티드 카는 “운전자와 탑승자가 사용하는 모든 모바일 기기에 인터넷 접속을 제공하는 차량”으로 볼 수 있다.

[1]에서는 커넥티드 카에 대해 앞서 언급한 정의들을 포함하여 다음과 같이 정의했다.

- 내장된 장치 또는 가져온 사용자 장치를 사용하여 언제든지 인터넷에 액세스할 수 있는 차량
- 현대적 어플리케이션과 상황별 동적 맞춤 기능을 갖추고 운전자와 탑승자에게 고급 인포테인먼트(infotainment) 기능을 제공하는 차량
- 도로 위 또는 기계와 관련된 샵에서 차량 간 인프라 통신 기술을 사용하여 다른 스마트 기기와 상호 작용할 수 있는 차량
- 차량 간 통신 기술을 활용하여 다른 차량과 상호 작용할 수 있는 차량

커넥티드 카 기술에서는 자동차의 통신 및 컴퓨팅 기능이 강화되고 스마트폰과 V2X와 함께 연결성이 강조될 것으로 예상된다. 특히 자율주행 자동차 자체를 하나의 새로운 모바일 플랫폼으로 인식하게 될 것으로 예상하고 있으며, 향후 커넥티드 자율주행자동차 기술로 많은 파생사업이 발생될 수 있을 것으로 기대된다.

IHS 등 자율주행 자동차 관련 시장조사기관의 발표에 따르면, 자율주행자동차는 관련 규제가 적은 북미와 유럽 지역을 중심으로 초기 시장을 형성한 뒤 2025년부터 2035년에 급성장 할 것으로 기대하고 있다. 자율주행자동차의 세계 판매량은 2025년 60만 대에서 2035년에는 2,100만 대로 대폭 증가할 것으로 전망된다[2].

하지만 보안은 취약하여 보안 취약점을 분석하고 예측되는 공격에 대해 대비해야한다.

* 공주대학교 정보통신공학부(대학생, 201701341@smail.kongju.ac.kr
** 공주대학교 정보통신공학부(교수, hbahn@kongju.ac.kr)

## Ⅱ. 커넥티드 카 시장

### 2.1. 커넥티드 카 서비스

커넥티드 카가 제공하는, 또는 제공해야할 서비스에는 교통 안전 서비스, 인포테인먼트 서비스, 교통 효율 서비스, 비용 효율 서비스, 편리성을 위한 유틸리티 서비스 등이 있다. [표 1]은 각 서비스 분야에 해당하는 서비스 별로 정리한 것이다[1].

〔표 1〕 Services of Connected Car

| 서비스 측면 | 종류 |
|---|---|
| 교통 안전 | • 운전자의 피로, 분노, 스트레스 감지<br>• 사고 방지 및 지원<br>• NVA(Night Vision Assistant) 및 HUD(Head Up Display)<br>• 원격 유지보수, 길가(roadside) 및 도난 차량 지원 |
| 인포테인먼트 | • 음악 스트리밍<br>• 비디오 스트리밍, 게임, 인터넷 검색<br>• 차내 와이파이(Wi-fi) 네트워크<br>• 소셜 네트워크 |
| 교통 효율 | • 네비게이션, 온라인 경로 계획<br>• 교통, 날씨, 도로 상태 모니터링<br>• 보조 주행 및 자율 차량 |
| 비용 효율 | • 보험 프로파일링<br>• 알고리즘 기반 차량 가격<br>• 에너지 최적화<br>• 상황별 광고<br>• 차량 테스트 |
| 편리성, 상호작용 및 기타 서비스 | • 스마트 홈 통합<br>• 웨어러블 장치와 통합<br>• 카셰어링(car sharing)<br>• 핸즈프리(hand-free) 컨트롤<br>• 운전자 프로파일(profile) 설정 |

### 2.2. 커넥티드 카 시장 동향

최근 자율주행 기술은 융합 연구개발 위주에서 응용 상용화 개발 위주로 개발은 고도화 되고 이에 따른 개발 속도는 가속화 되고 있다. 미국, 유럽, 일본, 중국 등의 선진국의 자동차 및 ICT 기업은 국적과 상관없이 여러 사업영역의 기업들과 인수합병 및 기술 제휴 추진이 급격히 증가하고 있다.

자율주행차 선두 자동차기업 중 GM은 자율주행 스타트업 Cruise Automation을 인수하고 차량 공유업체인 Lyft에 5억 달러를 투자하였다. 포드는 자율주행차 제조혁신센터 건립을 위하여 5.4조원을 투자할 예정이다. 다임러는 보쉬와 기술제휴를 통해 자율주행 레벨 5 기술개발을 추진중이다. 도요타는 우버의 전략적 투자자로 참여하고 앤비디아와 파트너쉽을 체결하는 등 사용화 기술개발을 추진 중이다.

ICT 업계로는 구글에서 자율주행 프로젝트 독립회사로 스핀아웃한 웨이모가 있으며 현재까지 가장 긴 자율주행 기록을 보유하고 있다. 차량공유 기업인 우버는 자율주행 트럭을 개발한 오토를 인수하였다.

국내 자동차 기업으로는 현대자동차그룹에서 자율주행 전문 기업인 오로라와 상용화 공동개발을 추진중이다. 자동차 부품기업으로는 만도가 자율주행용으로 자체 개발한 레이더를 기반으로 기술개발을 추진중이며, 인도 방갈로에 연구소를 설립하여 기술 개발을 추진하고 있다.

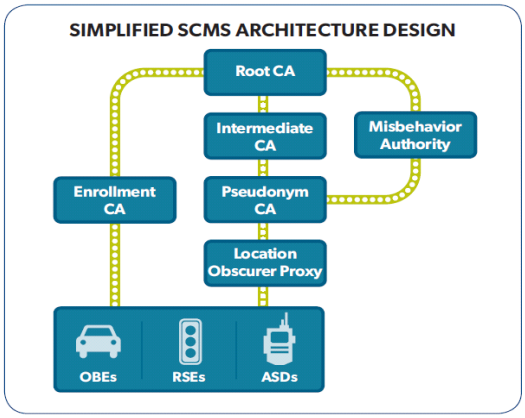
국내 ICT 기업으로는 삼성전자가 하만 인터내셔널 인수와 더불어 오스트리아 자율주행 스타트업 티티텍에 지분 인수 투자를 하였고, 자율주행 운영체제 스타트업 레노버 오토와 기술협력을 추진하고 있다. 엘지전자는 퀄컴과 5G V2X 개발을 위한 공동연구소 설립과 투자를 진행하고 있다. 네이버는 자율주행 관련 네이버랩스를 설립하여 추진하고 있으며, 이스라엘 자율주행 라이다 업체 이노비즈 테크놀로지에 공동 투자하고 있다.

자율주행을 위한 핵심부품인 반도체 기업은 엔비디아와 인텔 모빌아이가 선도하고 있으며 퀄컴과 엔엑스피에서도 관련 반도체 솔루션을 개발하고 있다. 인피이언과 르네사스에서는 자율주행 핵심부품에 탑재되는 반도체 부품 개발에 집중하고 있다[2].

## Ⅲ. 커넥티드 카 기술

### 3.1. VANET (Vehicular Ad-hoc Network)

VANET은 차량 도메인에서 작동하는 애드혹 네트워크의 서브셋이다. VANET은 ITS(Intelligent Transportation System)의 핵심요소다. 교통 효율을 개선하고 도로 안전을 개선한다는 ITS의 목표를 달성하기 위해 VANET은 도로 안전 정보, 교통 분석 관련 정보, 무정전 인터넷 연결을 이용한 일반 데이터(파일, 오디오, 비디오 등)를 공유한다[3].




〔그림 1〕 SCMS Architecture design

VANET에는 기본적으로 차량 간 순수 무선 통신인 V2V, 모바일 노드와 인프라 장치 RSU(Road Side Unit) 간의 통신인 V2I가 있으며, 최근에는 V2V와 V2I를 통칭하여 V2X(Vehicle-to-everything)라고 한다.

### 3.1.1. V2V (Vehicle-to-Vehicle)

V2V는 두 차량 간에 직접 정보를 교환할 수 있는 통신이다. 자율주행 자동차의 경우 이러한 통신수단의 확장은 자연스럽다. 실제로 자율주행 자동차는 두 사람의 운전자보다 더 많은 정보를 교환하고 분석할 수 있을 것이다. 따라서 V2V는 계획 및 제어 시스템의 신뢰성을 향상시키면서도 센서의 인식 한계를 감소시킬 것이다.

V2V 통신에는 무선 프로토콜과 라우팅 프로토콜이 사용되며 차이가 있다.

V2V 통신 전용 무선 시스템은 무선 LAN이라고도 하는 IEEE 802.11 표준에서 파생된 것으로, 두 대 이상의 차량이 동일한 무선 통신 범위에서 이동하면 자동으로 연결하여 애드혹 네트워크를 만들 수 있으며, 각 차량은 라우터 역할을 할 수 있고, 여러 번 점프하여 메시지를 보낼 수 있다는 것이 원칙이며, 원거리 차량, 그중 단일 무선 LAN 연결의 범위는 수백 미터로 제한 된다.

V2V 통신에 사용되는 무선 프로토콜에는 블루투스(IEEE 802.15.1), UWB(Ultra Wide Band, IEEE 802.15.3a), 와이파이(Wi-Fi, Wireless fidelity)가 있으며 세 프로토콜 모두 암호화 및 인증 메커니즘을 가지고 있다.

반면에 라우팅 프로토콜은 IoV(Internet of Vehicles) 수준에서 V2V 통신에 사용되는 프로토콜이다. V2V 통신은 IoV의 구성요소로, IoV가 제공하는 서비스는 송신기, 중계기, 수신기 등 해당 차량에 크게 의존하며, 차량은 자체 통신을 처리할 뿐 아니라 다른 차량 간의 통신을 위한 정보 릴레이 역할을 한다.

V2V 통신에 사용되는 라우팅 프로토콜에는 AODV(Ad hoc On demand Distance Vector), VADD(Vehicle-Assisted Data Delivery), RBVT-R(Road Based Vehicular Traffic Reactive), GPSR(Greedy Perimeter Stateless Routing), MA-DSDV(Multi-Agent Destination-Sequenced Distance Vector), GVGrid가 있다[4].

### 3.1.2. V2I(Vehicle-to-Infrastrucutre)

V2I는 차량과 인프라 간 연결 통신에서 실시간 데이터 교환을 가능하게 하는 솔루션이다. V2I 환경에서는 차량 온보드 장치(OBU)가 도로 측면 장치(RSU)와 통신하여 도로 상태에 대한 정보를 전달한다. RSU는 OBU를 인증하고 그들에게 인터넷 접속을 허가할 수 있다. VANET 내에서 OBU와 RSU는 모두 악의적인 활동에 대해 억제력이 있다.

### 3.1.3. V2X(Vehicle-to-everything)

V2X는 차량-사물 통신을 나타내는 용어로 차량으로부터 차량에 영향을 주는 물체로 정보를 전달하는 또는 그 반대로 정보를 전달하는 과정을 말한다. V2X는 V2V와 V2I를 통칭하여 사용하는 용어로 차량과 RSU 간 무선 통신을 가능하게 하여 자율주행과 주행 보조 솔루션을 제공한다. V2X의 주된 동기는 도로 안전, 교통효율성, 에너지 절약을 위하여 사용되는 기술로 WLAN과 셀(cell) 기반 즉 5G를 기반으로 한 통신 기술을 사용한다[5].

V2X는 차량과 RSU간 신뢰할 수 있는 양방향 인증 메시지를 기반으로 하여 통신을 하는데, 미국 교통국에서는 SCMS(Security Credential Management System)인 보안 인증서 관리 시스템을 표준화하는 작

업을 수행하고 있다[6]. SCMS는 보안 인증서를 관리하고 발급하기 위한 보안 기반구조를 제공하며 [그림 1]은 SCMS 아키텍처를 보여준다[7].

### 3.2. CAN (Controller Area Network)

CAN은 가장 대표적인 차내 네트워크로서, 요구되는 통신 회선 수를 대폭 감소시키고 데이터 전송 신뢰도를 높이기 때문에 사실상 차내 네트워크의 표준이 되었다[8]. 하지만 안타깝게도 CAN 설계에서 보안은 고려되지 않았다. 예를 들어, 버스 네트워크를 사용하여 데이터를 브로드캐스팅할 때 CAN은 CAN 데이터 프레임의 기밀성 및 인증을 보장하지 않으므로 악의적으로 공격자가 데이터를 쉽게 도청하거나 재생(replay) 공격을 할 수 있다. 차량이 진단 툴에 연결되면 차량의 정보를 탈취할 수 있게 된다. 진단 프로세스 중에 전자제어장치(ECU, Electronic Control Unit)의 기능을 점검하기 위해 툴은 암호화 및 인증 없이 CAN 데이터 프레임을 브로드캐스팅하여 ECU를 강제로 제어한다. 즉, 공격자가 ECU를 제어할 수 있는 CAN 데이터 프레임을 쉽게 얻기 위해 자동차 진단 툴을 사용할 수 있다[9].

## Ⅳ. 커넥티드 카 보안 문제

기존의 차내 소프트웨어(ECU에 설치된 소프트웨어)는 신뢰성, 보안, 기능 안전, 실시간 행동, 자원 소비 및 건전성 측면에서 항상 다른 소프트웨어 영역과 관련하여 다른 요구사항을 가지고 있다. 또한 ECU는 각각 다른 카테고리로 분할되며, 특정 요구 사항을 가진다. 따라서 자동차 영역의 독특한 측면도 고려해야 했던 소프트웨어공학의 규율에 대해 일련의 도전들이 생겨났다. 그중에서 보안 관련 문제는 커넥티드 카의 여러 요소에서 발생할 수 있으며 이를 [표 2]에 보여준다[1].

### 4.1. 커넥티드 카 보안 요소

지능형 차량 시스템의 안전한 구현은 넓은 보안 프레임워크의 설계와 개발에 달려 있다. 따라서 차량 시스템은 엄격한 보안 요건을 준수해야 한다. 개념 설계 및 개발의 초기 단계에서 적절한 보안 요건을 식별하는 것은 차량과 탑승자가 항상 안전하고 안전하게 유지되도록 하는 데 중요한 역할을 한다. 인증, 신뢰성,

〔표 2〕 Security Challenge of Connected car

| 커넥티드 카 요소 | 보안 문제 |
|---|---|
| ECU | • 인증 시스템이 제공되지 않거나 취약하기 때문에 악성 소프트웨어로 다시 프로그래밍될 수 있다. |
| 모바일 앱 | • 차량 내 대시보드에 통합된 모바일 기기에서 실행되는 앱은 적절히 보호되지 않는다. 앱은 차량 데이터를 노출시키는 악성 라이브러리를 포함할 수도 있으며, 앱이 차에 명령을 내리도록 허용될 때 문제는 더 심각해질 수 있다. |
| 임베디드 앱 | • 차량 내 대시보드에 설치된 오픈소스 애플리케이션의 취약성은 악성 소프트웨어를 주입하는 데 악용될 수 있다. |
| OBD-Ⅱ포트 | • 의무 OBD-Ⅱ포트는 자동차 버스 시스템 전체에 접근할 수 있게 해준다. 손상된 타사 장치가 연결되어 있으면 진단 데이터를 수집하거나 차량 내부에 멀웨어를 설치할 수 있다. 공격자가 동글을 차량에 꽂아두면 차량과 운전자에 대한 민감한 정보를 지속적으로 얻을 수 있다. |
| CD 플레이어 및 USB 포트 | • 자동차 CD 플레이어의 외부 디지털 멀티미디어 포트는 악성 소프트웨어가 삽입될 위험이 있다. 엔터테인먼트 시스템은 CAN 버스에 연결되어 있기 때문에 다른 구성 요소를 공격하는 인터페이스 역할을 할 수 있다. |
| CAN | • 자동차의 내부 네트워크는 전송된 데이터의 기밀성 등 정보보안의 주요 속성을 보증하는 프로토콜이 갖추어져 있지 않기 때문에 가장 큰 취약점이다. CAN 버스는 차량의 모든 중요 구동 구성 요소와 통신하는 데 사용되며, MAC 또는 디지털 서명에 의해 보호되지 않기 때문에 다른 노드에서 메시지를 읽을 수 있다. |
| 무선 네트워크 | • 휴대전화와 차내 기기를 연결하는 데 사용되는 와이파이나 블루투스 네트워크도 해킹이 가능하다. GSM 연결도 유사한 유형의 취약성을 갖기 때문에 차량이 통합 SIM 카드를 가지고 있고 3G/4G 네트워크에 직접 연결되어 있을 때 심각한 위험이 발생할 수 있다. |

무결성, 익명성(프라이버시), 가용성, 지연 처리, 기밀성은 보안 시스템이 제공해야 하는 가장 중요한 전제 조건들 중 하나이다. 따라서 커넥티드 카가 갖춰야 할 보안 요소는 다음과 같다[3, 10].

- **인증(Authentication)**: 인증은 우리에게 정보나 메시지 생성에 대한 확신을 준다. VANET 노드에서 다른 쪽 끝에서 수신한 정보에 따라 응답하므로, 시스템에서 전파되는 정보가 참이고 합법적인 사용자에 의해 생성되는 것이 필수적이다. 인증요건을 이행하기 위해서는 키 관리 및 배포가 효율적이고 정확해야 한다.
- **신뢰성(Reliability)**: 통신에서의 데이터 수신은 정확하고 사실적이어야 한다. 시스템의 정기적인 검증은 실제로 잘못된 정보를 제거하기 위해 이루어진다.
- **무결성(Integrity)**: 통신 시스템의 무결성은 송신자와 수신자 사이의 데이터 유효성을 가리킨다. 수신된 정보는 허가되지 않은 사용자에 의해 변경되지 않아야 한다. 그러한 변화는 시스템을 손상시킬 수 있고 심각한 인명 피해를 초래할 수 있다. 차량용 네트워크에서는 의도적으로 공격자에 의해, 또는 노이즈, 페이딩 등의 저하 요인에 의해 전송 중에 메시지가 손상되지 않았는지 검증할 수 있어야하며 이를 위해서는 오류 감지 및 수정 코드를 구현해야 한다.
- **익명성(Anonymity) 및 프라이버시(Privacy)**: 대부분의 운전자들은 익명성이 보장되는 환경에서 차량을 운전하고 있다. 따라서 보안 조치는 프라이버시를 보장해야 한다.
- **가용성(Availability)**: VANET은 매우 역동적이며 네트워크는 실시간으로 대응할 수 있어야한다. 따라서 콘텐츠 가용성을 높이고 제공 비용을 절감하기 위해 설계의 초기 단계에서 복제를 고려하는 것이 중요하다. 네트워크의 한 부분에 고장이나 일시적인 정전이 있을 때, 네트워크 운용이 계속되고 차량이 어떠한 문제도 인식하지 못하는 것이 중요하다. 항상 서비스를 이용할 수 있어야 한다. 따라서 이러한 목적에 필요한 중복성을 적절하게 구현해야 한다. 또한, 이러한 시스템은 긴급한 데이터를 처리하므로 모든 인증된 사용자가 쉽고 효율적으로 데이터를 이용할 수 있어야 한다.
- **지연 처리(Delay handling)**: 안전 정보는 시간에 민감하므로 지연 시간을 피하고 처리해야 한다.
- **기밀성(Confidentiality)**: 중요한 데이터는 권한이 없는 사용자가 접근해서는 안 된다.

### 4.2. 커넥티드 카 공격 및 보안 과제

#### 4.2.1. VANET에서의 공격

커넥티드 카에 영향을 미치는 공격에는 서비스 거부 공격(DoS), 분산 서비스 거부(DDoS) 공격, 블랙홀(Black-Hole) 공격, 재생(Replay) 공격, Sybil 공격, 위장(Impersonation) 공격, 멀웨어(Malware), 정보 위조(Falsified-Information) 공격, 타이밍(Timing) 공격이 있다[10].

- **서비스 거부 공격(DoS)**: 서비스 거부 공격(DoS)은 잘 알려져 있으며 수년 동안 네트워크 운영을 방해하는 데 광범위하게 사용되어 왔다. 서비스 거부 공격은 호스트에 엄청난 양의 정보를 보내 합법적인 사용자로부터 들어오는 정보를 수신하거나 처리하는 것을 방해하는 것이다. 서비스 거부 공격은 네트워크 운영을 방해하는 데 매우 효과적이지만 실행 비용이 계산적으로 많이 든다. DoS 공격은 수년간 발전해 왔다. DoS 공격은 네트워크의 핵심 요소로 보이는 특정 노드를 대상으로 하여 최적화되었다. 또 공통 제어 채널도 주요 대상으로 파악됐다. VANET에서, 공격자의 주된 목표는 도로변 유닛(RSU)이 될 것이다. RSU는 사용자와 사용자 정보를 인증, 관리 및 업데이트할 때 VANET의 핵심 구성 요소다. 그러므로 RSU에 대한 공격이 성공하면 네트워크 운영에 해로운 영향을 미칠 수 있다. 서비스 거부 공격에 대항하는 가장 간단한 방법은 공격자의 IP 주소를 차단하는 것이다.
- **분산 서비스 거부(DDos) 공격**: 기존의 서비스 거부 공격(DoS)에서, 단일 공격자는 대개 단일 컴퓨터에서 단일 IP 주소를 사용하여 노드나 채널을 공격한다. 이것은 공격자의 자원에 큰 부담을 줄 수 있다. 그 결과, 공격자는 분산 공격에서 복수의

IP 주소를 사용하는 경우가 많아 자원부담이 줄어든다. 종종 공격자는 의심하지 않는 사용자에게 트로이 목마를 심고 그들의 자원을 사용하여 디도스 공격을 할 것이다. DoS 공격과 유사하게 DDoS 공격은 RSU와 네트워크의 다른 차량 모두에서 수행될 수 있다[10]. 또한 도로변 장치(RSU) 소프트웨어가 기능할 수 없도록 정보의 불필요한 전송을 통해 DDoS 공격을 수행할 수도 있다[5].

- **블랙홀(Black-Hole) 공격**: 블랙홀 공격은 통신 시스템에서 흔히 발생한다. 블랙홀 공격에서는 패킷을 목적지로 전달하는 대신 공격자가 패킷을 떨어뜨려 패킷이 네트워크를 통해 이동할 수 없는 구멍을 만든다. 이러한 유형의 공격은 네트워크 성능과 라우팅에 심각한 영향을 미칠 수 있다.
- **재생(Replay) 공격**: 재생 공격은 블랙홀 공격과 관련이 있다. 차이점은 블랙홀 공격에서는 송신자가 의도적으로 공격자를 통해 패킷을 송신하고, 패킷을 목적지에 전달하지만 재생 공격에서 송신자는 중간 가로채기 팩에 노드가 있다는 것을 알지 못한다는 것이다. VANET에서 재생 공격은 대부분 차량과 도로변 장치(RSU) 간의 통신을 대상으로 한다. 공격자가 RSU와 암호화 키 또는 암호를 포함하는 차량 사이의 메시지를 가로채면 그들은 나중에 그들 자신을 인증할 수 있을 것이다. 중간자(man-in-the-middle) 공격과 재생(replay) 공격은 공격을 받았을 때 아는 것이 거의 불가능하기 때문에 효과적으로 막기는 어렵다.
- **Sybil 공격**: Sybil공격 또는 pseudo-spoofing공격은 사용자가 많은 수의 익명 신원을 만드는 것을 포함한다. VANET에서, GPS 스푸핑 공격의 도움을 받아 Sybil 공격이 수행될 때 공격자는 혼잡하지 않은 경로를 확보하도록 할 수 있다. 다른 모든 차량들이 혼잡한 지역을 돌아다니려고 하기 때문에 혼잡하지 않는 경로가 만들어질 것이다. 개인 간 통신(peer-to-peer) 네트워크는 사용자의 익명성에 크게 의존하기 때문에 이러한 유형의 공격은 완화하기 어렵다. 가장 효과적인 경감 방법은 암호나 공개 암호화를 사용한 식별 및 인증 기반 방법이다.
- **위장(Impersonation) 공격**: 위장 공격은 많은 실제 시나리오에서 흔하다. 가장 간단한 사칭의 예는 한 사람이 다른 사람인 척하여 이득(금전이나 물질)를 보거나 자신의 진짜 정체를 숨기는 것이다. 통신 시스템에서 사용자들은 비슷한 이유로 동기 부여를 받는다. 침해 공격은 접근이 제한된 자원이나 기밀 정보에 대한 접근을 얻기 위해 사용될 수 있다. VANET에서는 사용자들이 인증 세부 정보를 누설하도록 하기 위해 악의적인 노드가 도로변 유닛(RSU)을 가장할 것이다. 인증 정보를 획득한 후에는 기밀 정보에 접근하거나 다른 당사자와의 인증으로도 사용할 수 있다. 공격자들은 또한 이득을 얻기 위해 다른 차량들을 가장할 수 있다. 통신 시스템의 위장 공격으로부터 완화하기 위해 여러 가지 방법이 제안되었다. 암호화, 지역화, 클러스터링에 기초한 방법을 사용하여 가장 공격의 영향을 완화할 수 있다.
- **멀웨어(Malware)**: 악성 소프트웨어와 스파이웨어는 인터넷 초기부터 설계되었다. 악성 노드는 합법적인 소프트웨어 내에 특수화된 악성 소프트웨어(맬웨어)를 삽입한다. 실제로 악성코드는 VANET에 매우 해로운 영향을 미친다. VANET 네트워크는 매우 동적이며 자주 변경되고 업데이트되기 때문에 차량은 신뢰할 수 있는 소스로부터 정보를 수신받고 제공 받아야 한다. 그렇지 않고 감염되면 개인정보가 손실될 위험이 있으며, 경우에 따라 심각한 오작동이 발생할 수 있다. 맬웨어 공격의 완화를 위한 가장 간단한 방법은 합법적인 것에서 악의적인 메시지를 필터링할 수 있는 방화벽의 도입이다. 그러나 공격이 방화벽 주변에서 방법을 찾는 것으로 알려져 있으므로 추가적인 방법이 필요할 수 있다. 방화벽 보호 외에도, 신뢰받는 당사자의 메시지만 허용되도록 평판 기반 계획이 도입되는 경우가 많다.
- **정보 위조(Falsified-Information) 공격**: 가짜 정보의 확산은 통신 시스템에서 흔히 다시 사용된다. Sybil은 허위 정보 공격의 예라고 볼 수 있다. 이와 유사한 방법으로, 공격자들은 도로 정체와 관련된 허위 정보를 퍼뜨려 다른 운전자들이 다른 경로로 분산하도록 효과적으로 강요할 수 있다. 또 도로의 정체나 사고 신고를 소홀히 함으로써 정체를 유발할 수 있다. 이러한 형태의 공격은 VANET에서 흔히 사용된다. 만약 공격자가 한 대

의 차량을 설득할 수 있다면, 그 차량은 가짜 정보를 다음 차량으로 전파하기 때문에 자신도 모르게 공격자가 될 것이다. 이러한 형태의 공격은 종종 정당한 정보를 보내는 운전자에게 보상을 하고 허위 정보를 보내는 운전자를 처벌하는 평판 기반 계획을 사용하여 해결된다.

- **타이밍(Timing) 공격**: 시간 동기화는 VANET의 주요 측면이다. 차량은 RSU와 차량 사이의 실시간 업데이트와 정보 교환의 필요성을 소개하는 네트워크를 매우 빠르게 드나든다. 중요한 메시지 교환은 중요하므로, 메시지의 지연은 심각한 문제를 일으킬 수 있다. 타이밍 공격은 많은 면에서 블랙홀 공격과 그레이홀 공격과 유사하다. 그러나 악의적인 노드는 패킷의 전부 또는 일부를 삭제하는 대신 의도적인 지연을 도입하기 위해 시간 슬롯을 추가한다. 이는 특히 시간에 민감한 정보의 지연이 대형 사고를 유발할 수 있는 자율주행차의 주요 문제를 야기한다.

#### 4.2.2. VANET에서의 보안 과제

커넥티드 카의 보안 요소들이 VANET 구축에 장애를 일으킬 때도 있다. 기술적 문제(네트워크의 동태성 관리, 지연 시간 관리, 정체 및 충돌 분석, 대기 영향 및 보안 당면 과제)와 사회적 및 경제적 문제(VANET의 비용 영향 및 사회적 수용)로 분류된다.

VANET의 보안 시스템에 의해 극복되어야 하는 주요 과제는 다음과 같다.

- **데이터 일관성**: 중요 정보의 악의적인 변경은 사고로 이어질 수 있으며, 인증된 노드와 인증되지 않은 노드의 악의적인 활동으로 인한 데이터의 불일치를 피하기 위해, 다양한 노드에서 수신된 정보를 교차 확인하여 그러한 활동을 방지하는 메커니즘을 설계해야 한다.
- **높은 이동성**: VANET은 높은 처리능력 및 저장능력에도 불구하고 높은 수준의 보안 알고리즘을 필요로 하지 않는다.
- **오류 허용**: VANET에서 수신 및 대응 조치는 매우 빠르기 때문에 프로토콜이나 알고리즘의 오류는 시스템을 심하게 손상시킬 수 있다. 따라서 프로토콜은 이 문제를 고려하여 설계되어야 한다.
- **지연 시간 제어**: VANET에서 공유되는 정보는 시간에 민감하다. 실시간 정보 공유 특성을 보장하기 위해서는 보안에 사용되는 암호 및 기타 알고리즘이 신속하고 효율적이어야 한다.
- **키 관리**: VANET 보안에 사용되는 모든 알고리즘은 키에 의존한다. 따라서 키의 생성, 유지 및 배포는 특별히 다루어져야 한다.

애드혹 환경, 특히 차량 영역에서는 다양한 유형의 공격이 가능하다. 시스템에 대한 이러한 공격의 영향은 주로 뒤에 있는 공격자의 의도에 달려 있다. 공격자는 자신이 합법적인 사용자가 아닌 시스템 시설을 이용하거나 시스템의 기밀 데이터를 얻거나 네트워크의 효율적인 기능을 방해하는 목적 등의 여러 가지 이유로 악의적인 행동을 할 수 있다.

VANET에 가할 수 있는 공격은 네트워크 공격(NN, Network Attack), 애플리케이션 공격(AA, Application Attack), 타이밍 공격(TA, Timing Attack), 사회적 공격(SA, Social Attack), 모니터링 공격(MA, Monitoring Attack) 이렇게 5가지로 분류할 수 있다.

네트워크 공격은 가장 심각한 공격이며 네트워크와 노드의 기능에 대한 직접적인 공격을 의미한다. 여기에는 Dos, Sybil 등의 공격이 속한다.

애플리케이션 공격은 주로 공유되는 정보와 제공되고 있는 애플리케이션과 관련이 있다. BI(Bogus information)나 도청이 여기에 속한다.

타이밍 공격은 메시지 시간 간격에 따라 약간의 지연을 추가하기 위해 하는 공격이다.

사회적 공격은 다른 운전자들에게 정서적 불균형을 초래하는 모든 메시지나 공격을 말한다. 이 등급의 공격에서는 비윤리적인 메시지가 운전자를 방해하는 차량으로 전송되어 운전 중단, 보안 시스템의 다른 필수 조건의 상실로 이어진다.

모니터링 공격에서는 공격자가 조용히 전체 시스템을 감시하고 추적하며, 그러한 관찰을 바탕으로 악의적인 활동을 수행할 수 있다. 모든 소극적인 공격은 이 범주에 속하며, 위장공격(impersonation)이나 세션 하이재킹(session hijacking) 공격도 여기에 속한다[3].

## Ⅴ. 결 론

본 논문에서는 커넥티드 카의 시장동향 및 서비스, 기술 등을 정리하고 커넥티드 카에서 필요로 하는 보안 요소와 보안 과제, 공격 및 위협에 대해 정리했다. 커넥티드 카의 통신 기술은 빠르게 발전하고 있지만 보안이 취약하여 사이버 공격을 받을 위험이 매우 크다. 커넥티드 카는 차체내의 센서들간의 통신, 운영시스템, 외부와 통신을 위한 프로토콜과 인증 등에 대하여 많은 취약점을 보이고 있다. 이러한 보안 취약점에 대한 공격과 대안을 위한 연구들이 진행되고 있지만 5G와 같은 초소속 통신망을 사용함에 따라 더 많은 디바이스들과 연결되고 복잡해지는 경향을 보이고 있어 커넥티드 카에서의 보안 과제들에 대한 연구가 더 활발히 진행되어야 할 것으로 보인다.

## 참 고 문 헌


[1] R. Coppola, M. Morisio, “Connected Car: technologies, issues, future trends”, *ACM Computing Survey*, vol. 49, pp. 1-37, 2016

[2] 연규봉, “5G 커넥티드 자율주행차와 센서기술 동향”, 첨단센서 2025 포럼, June 2019, https://sensor2025.or.kr/bbs/board.php?bo_table=trend&wr_id=87

[3] R. Mishra, A. Singh, R. Kumar, “VANET Security: Issues, Challenges and Solutions”, *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016*, pp. 1050-1055, 2016

[4] J. Kawtar, M. Tomader, “Study of connectivity aspect of connected car”, *IEEE/ICCSRE2019*, July 2019

[5] Z.E. Rewini, K. Sadatsharan, D.F. Selvaraj, S.J. Plathottam, P. Ranganathan, “Cybersecurity challenges in vehicular communications”, ScienceDirect Vehicular Communications 23 (2020) 100214, 2020

[6] J. Walker, “Security Credential Management System (SCMS)”, United States Department of Transportation, Office of the Assistant Secretary for Research and Technology, Intelligent Transportation Systems Joint Program Office, https://www.its.dot.gov/resources/scms.htm

[7] B. Kreeb, K. Gay, “Security Credential Management System (SCMS) Proof Of Concept(POC)”, U.S. Department of Transportation

[8] K.H. Johansson, M. Torngren and L. Nielsen, “Vehicle Applications of Controller Area Network,” January 2005

[9] Samuel Woo, Hyo-jin Jo and Dong-hoon Lee, “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, No. 2, April 2015

[10] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang, Y. Xiang, S. Yu, “An Overview of Attacks and Defences on Intelligent Connected Vehicles”, *arXiv:1907.07455v1*, July 2019


## 〈저 자 소 개〉


**박 현 경 (Hyunkyung Park)**

학생회원

2017년 2월 : 공주대학교 정보통신공학부 정보통신공학전공 학사

<관심분야> 디지털포렌식, 네크워크 보안

**안 효 범 (Hyobeom Ahn)**

1992년 : 단국대학교 전자계산학과 (이학사)
1994년 : 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 : 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년 9월~2005년 3월 : 천안공업대학 정보통신과 부교수
2005년 3월~현재 : 공주대학교 정보통신학부 교수
<관심분야> 네트워크 보안, 디지털 포렌식, IoT보안