정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

5G 네트워크 환경의 자동차 보안

심 상 규*, 김 의 석*, 김 덕 수*

요 약

5G 네트워크의 출현으로 다양한 분야의 새로운 도약이 기대되고 있으며, 특히 자동차 분야에서의 적용에 대한 기대가 크다. 자동차는 커넥티드카(connected car)를 넘어 스마트카(smart car)로의 진화를 이어가고 있으며, 이 과정에서 5G 네트워크의 기여가 클 것으로 기대된다. 본 연구에서는 5G 네트워크의 적용에 따른 자동차의 변화상과 이에 따른 자동차의 보안 문제를 살펴본다.

Ⅰ. 서 론

내연기관 자동차가 생활필수품으로 자리 잡은 이래로 자동차는 엔진이 장착되어 있고 사람이나 화물을 실어 나르는 이동 수단으로만 인식되어 왔다. 그러나, 근래에는 자동차가 다양한 모습으로 변화하고 있으며 자율주행 자동차, 커넥티드카, 전기차 등의 어휘가 점점 익숙해지고 있다. 우리는 자동차가 새로운 모습으로 진화하는 시대를 살고 있는 것이다. 자동차의 미래 모습으로 자율주행 자동차를 먼저 떠올리는 이들도 많겠지만, 이는 자동차가 갖는 하나의 기능적 측면일 뿐이다. 다양한 연결성을 갖는 커넥티드카, 스스로 판단하고 운전하는 자율주행 자동차, 내연기관을 사용하지 않는 전기 자동차 등의 모습은 미래의 자동차가 갖게 될 하나의 측면이며 미래의 자동차를 정의하는 어휘는 마땅히 스마트카일 것이다. 개인이 갖게 된 최초의 스마트 기기가 스마트폰이라면, 스마트카는 개인이 일상에서 함께 이동할 수 있는 가장 큰 스마트 기기가 될 전망이다.

자동차의 이러한 진화를 가속화하는 것은 네트워크 기술이며, 자동차의 다양한 네트워크 기술들 중에서 가장 주목받고 있는 것이 5G 통신이 있다. 5G 통신을 통해서 자동차는 주변과 소통하며 더욱 지능적인 스마트 기기로 거듭날 수 있다.

한편, 자동차의 진화와 발전에서 우리가 우려하는 주요 측면 중의 하나는 보안이다. 기존의 자동차에서 중요한 측면은 안전(Safety)이었다. 안전은 사람의 생명에 위험을 초래할 수 있는 위해 요소(Hazard)가 발생하더라도 이를 극복하여 강건(Robustness)하게 동작하여 사람의 생명을 보호할 수 있도록 하는 것이다. 그러나, 자동차가 진화하면서 안전 뿐만 아니라 보안(Security)이 함께 필요하게 되었다. 보안은 위협(Threat)에 대해서 시스템을 신뢰(Trust)를 확보하여 자동차의 시스템 강건성을 보장하고 안전을 유지할 수 있도록 하는 핵심 요소로 받아들여지고 있다.

5G 통신을 비롯한 네트워크의 발전으로 가속되고 있는 자동차의 변화상을 살펴보고, 이에 따른 보안의 고려점을 함께 살펴본다.

Ⅱ. 자동차 진화의 기술 요인

자동차의 변화를 이끄는 주요 기술 요인을 5가지 요로 정의할 수 있다.

- 보안 (**S**ecurity)
- 서비스 플랫폼 (Service **P**latform)
- 자율주행 (**A**utonomous Driving)
- 연결성 (**C**onnectivity)
- 전력화 (**E**lectrification)

자동차 부품사 및 제조사, 그리고 MaaS (Mobility-as-a-Service) 업체들은 위의 기술들을 결합함으로써 새로운 자동차를 개발하거나 자동차 기반의 새로운 서비스들을 창출하고 있다.

* 펜타시큐리티시스템(주) (sgsim@pentasecurity.com, esskim@pentasecurity.com, dskim@pentasecurity.com)

2.1. 전력화(Electrification)

기존의 자동차들은 내연기관을 동력원으로 사용하는데 반해서 전기와 모터를 동력원으로 사용하는 전기차의 시장 점유율이 증가하고 있다. 내연기관 엔진을 사용하는 자동차는 엔진의 회전력을 바퀴까지 전달하기 위한 구동계(Powertrain)를 중심으로 많은 기계 부속들이 요구되는데 반해서, 전기차는 배터리와 모터의 조합으로 더욱 단순하고 가벼운 구조로 동작할 수 있는 장점을 갖는다. 그러나, 전기를 충전하는데 비교적 긴 시간이 필요하고 배터리의 재활용성과 관련된 문제점들도 대두되고 있다.

내연기관 자동차가 주유소를 필요로 하듯이 전기차는 충전기를 필요로 하고, 전기차의 충전을 제공하는 것이 하나의 산업으로 성장하고 있다. 충전기 사업자(CPO, Charge Point Operator), 충전 서비스 사업자(MSP, Mobility Service Provider) 등이 전기차의 충전 때문에 새롭게 생겨난 기업들이다.

전기차의 충전에 사용되는 충전 케이블은 충전기로부터 배터리로 전하를 이동시키는 역할도 하지만, 데이터 송수신도 함께 제공할 수 있다. 우리가 사용하는 스마트폰을 컴퓨터에 연결하면 충전과 데이터 동기화가 함께 이루어지는 것과 같은 이치이다. ISO15118 표준[1]은 자동차의 충전 과정에서 과금과 결제를 자동차와 충전기 사이의 통신을 통해 자율적으로 이루어질 수 있도록 하는 PnC (Plug&Charge) 서비스를 제공할 수 있다. 이 기술은 충전 시간 동안 차량의 진단, 차량의 소프트웨어 갱신 등의 서비스까지 확장될 수 있기도 하다. 특히, 자동차가 무선 충전을 통해서 충전하게 되면 ISO15118 기술에 기반한 PnC 서비스는 더욱 중요해질 것으로 예상된다.

ISO15118 표준에서 자동차, 충전기, 충전기 사업자, 충전 서비스 사업자 등은 인증서 기반의 보안 기술을 사용하여 인증을 비롯하여 과금과 결제가 안전하게 이루어지기 때문에, PnC 서비스에서도 보안은 핵심 기술로 자리잡고 있다.

5G 통신 기술은 PnC와 직접적인 연관이 적으나, 자동차의 진단과 소프트웨어 갱신 서비스가 PnC의 무선 충전 채널을 통해서 제공될 수도 있고 5G 통신을 통해서 제공될 수도 있다. 두 가지 통신 방법은 상호 보완적인 방법으로 활용되는 것이 바람직할 것으로 생각된다.

2.2. 연결성(Connectivity)의 확대

자동차가 스마트카로 진화하는데 가장 큰 기여를 하는 것은 연결성이다. 우리 사용하는 컴퓨터의 성능이 아무리 뛰어 나더라도 인터넷이라는 연결성이 없으면 효용성이 거의 사라져 버리는 것과 유사하게 생각할 수 있다. 자동차는 주변과 연결하고 원격의 시스템들과 연결됨으로써 더 많은 정보와 데이터를 활용할 수 있고 더 스마트한 기기로 거듭날 수 있다.

자동차에 적용되고 있는 연결성은 다음과 같은 다양한 형태가 있다.

- V2V (Vehicle-to-Vehicle) : 자동차의 추돌 방지를 위한 자동차 간의 연결
- V2I (Vehicle-to-Infrastructure) : 자동차와 도로 간의 연결
- V2P (Vehicle-to-Pedestrian) : 자동차와 보행자의 스마트 기기 간의 연결
- V2D (Vehicle-to-Device) : 자동차의 제어와 조작을 위한 자동차와 운전자의 스마트 기기 간의 연결
- V2H (Vehicle-to-Home) : 가정 내의 IoT 기기와 자동차 간의 연결
- V2C (Vehicle-to-Cloud) : 자동차와 온라인 서비스 클라우드 간의 연결

V2V, V2I, V2P 등은 교통 사고로 인한 피해와 손실을 줄이기 위해 정부 주도하에 이루어지고 있으며, 국내의 C-ITS (Cooperative Intelligent Transportation System; 차세대 지능형 교통체계) 사업이 대표적인 예라 할 수 있다. V2D, V2H, V2C는 높은 부가가치를 창출할 수 있는 영역으로서 주로 제조사를 비롯한 민간 기업들에 의해서 주도되고 있다.

5G 통신이 적용된다면, 5G의 저지연성(Low Latency)와 고속 통신의 성능적 특성을 기반으로 더욱 효율적인 연결성을 확보할 수 있을 것으로 기대된다. 각각의 연결성 형태에서 임의의 개체들을 연결하기 위해서는 당연히 보안이 고려되어야 한다. 가장 먼저 적용되어야할 보안은 인증(authentication)이다. C-ITS의 경우, 정보를 제공하는 발신자에 대한 신뢰를 확보하는 것이 무엇보다 중요하기 때문에 인증에 기반한 보안 통신을 적용하고 있다. 원격 제어나 결제 정보 등과 같

은 기밀성 데이터가 송수신된다면 암호화 채널을 적용하는 것이 필요하며, 원격제어의 경우에는 자동차에 대한 권한관리가 반드시 필요하다. C-ITS의 인증 기반 보안 통신에 5G를 적용할 때 고려되어야 할 문제에 대해서는 다음의 장에서 상세하게 살펴보도록 한다.

2.3. 자율주행(Autonomous Driving)의 발전

대중에서 자동차의 변화 상을 가장 직접적으로 체감할 수 있는 영역 중의 하나가 자율주행 기능이다. 자동차가 스스로 판단하고, 스스로 주행할 수 있는 것은 자동차의 지능화에 중요한 측도로 여겨지고 있다. SAE J3016 표준에서는 자동차의 자율주행 기술 수준을 0~5단계로 분류하고 3단계 이상을 자율주행 자동차로 정의하고 있다.

자율주행은 자동차가 데이터와 정보를 수집함으로써 상황을 판단하고 스스로를 제어함으로써 이루어진다. 자동차가 데이터와 정보를 수집하는 방법은 크게 3가지로 분류할 수 있다.

(1) 내장 센서를 활용한 수집 : 카메라, LiDar, Radar 등의 센서를 통해 주변 환경을 감지
(2) 주변 환경과의 통신에 의한 수집 : V2V나 V2I 통신을 통해 주변의 자동차나 시설물로부터 정보를 수집
(3) 원격 서버 통신에 의한 수집 : 원격의 온라인 서버로부터 제어 메시지를 수신

5G 네트워크를 비롯한 모바일 네트워크의 발전으로 주변 환경과의 통신 및 원격 서버 통신에서 발생할 수 있는 지연성(latency)를 해소하고 초고속 통신을 확보할 수 있게 되었다. 이로써 자동차는 원활하게 데이터와 정보를 수집할 수 있게 되었고 자동차가 자율주행을 하는데 필요한 기본 환경을 갖추게 되었다.

보안 위협은 자동차가 자율주행을 위해 수집하는 3가지 방법에서 모두 존재한다. 해커는 내장 센서의 올바른 센서 동작을 방해할 수 있고, 주변 통신을 방해하거나 위변조할 수 있다. 원격 서버와의 통신에서도 위변조, 세션 정보의 탈취, 신분의 위장 등이 가능하다. 이러한 보안 위협들은 자동차가 올바른 데이터와 정보를 확보하는 것을 방해하여 자동차가 정확한 상황 인식을 하지 못하도록 하고 나아가서는 사고를 유발시킬 수도 있다. 보안은 자동차가 올바른 데이터와 정보를 획득할 수 있도록 해주어야 한다.

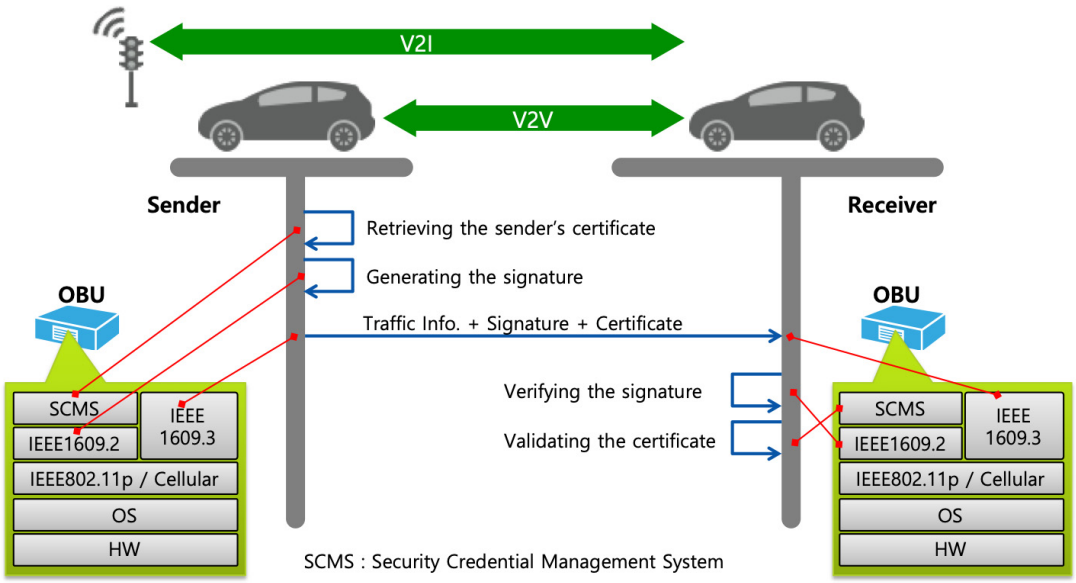
2.4. 서비스 플랫폼의 출현

무선 전화기가 피처폰(feature phone)의 형태에서 스마트폰(smart phone)으로 발전하면서 가장 두드러진 특징 중의 하나는 모바일 서비스의 발전이라 할 수 있다. 피처폰이 전화기의 하드웨어와 고정된 소프트웨어 기능의 결합이었다면, 스마트폰은 하드웨어와 사용자의 선택에 의한 소프트웨어들과 모바일 서비스들의 융합에 의해서 완성된다.

자동차도 이와 유사한 변화에 직면하고 있다. 현재의 자동차는 하드웨어와 고정된 내장 소프트웨어의 결합이라면, 향후의 자동차에서 소프트웨어는 사용자의 선택으로 구성되고 다양한 온라인 서비스들과 연결될 것이다. 온라인 서비스를 중심으로 본다면 자동차가 온라인 서비스를 사용자에게 제공하는 말단의 기기들 중의 하나가 되는 것이다.

현재에도 자동차에 온라인 서비스를 결합하여 텔레매틱스 서비스로 제공되고 있으나, 자동차의 도어락을 제어하거나 시동을 켜고 끄는 등의 단순한 기능만을 제공하고 있다. 이것은 편의 서비스이기는 하지만 가치 서비스(Value-Added Service)라고 보기는 어렵다. 사용자가 원하는 것은 가치와 만족감을 느낄 수 있는 서비스이고 이것이 가치 서비스이다. Google의 Android Auto와 Apple의 CarPlay는 스마트폰의 가치 서비스들을 자동차로 확장하기 위한 첫 번째 시도라 할 수 있다.

자동차에 서비스를 제공하기 위한 서비스 플랫폼을 구축하는 예도 있다. 독일 제조사 BMW는 Open Mobility Cloud을 발표하였고 자동차 뿐만 아니라 IoT 기기들까지 포용할 수 있도록 하고 있다. 지도 회사 Here는 Open Location Platform을 구축하여 지도의 지리 정보 위에 다양한 컨텐츠와 정보를 결합할 수 있도록 한다. 플랫폼 계의 공룡에 해당하는 Amazon은 음성인식 인공지능 비서인 Alexa가 자동차나 IoT 기기에 쉽게 적용될 수 있도록 기업들을 지원함으로써 자동차와 IoT 기기들이 서로 연결될 수 있는 거대 플랫폼을 단숨에 이루어내었다.



〔그림 1〕 C-ITS의 V2V 및 V2I의 인증 기법

앞으로 자동차 분야에서 서비스 플랫폼의 중요성은 더욱 높아질 것으로 보여 진다. 이런 측면에서 5G의 발전은 자동차가 서비스 플랫폼과 긴밀하게 연결될 수 있도록 해주고, 광대역의 데이터 통신을 제공함으로써 사용자에게 서비스 몰입도와 만족감을 높여줄 수 있는 핵심 기반이라 할 수 있다.

서비스 플랫폼의 발전을 위해 꼭 필요한 것은 신뢰(trust)이기 때문에 보안은 반드시 선결되어야 하는 문제이다. 그 중에서도 기기나 사용자의 인증은 무엇보다 중요하다. 최근 DID(Decentralized ID)의 부상은 이러한 흐름과 잘 부합한다. 사용자나 기기의 신원을 확인할 수 있는 검증값을 관리하는 체계를 구성함으로써 사용자나 기기의 인증을 제공할 수 있고 개방적인 구조에서 다양한 서비스로의 확장성을 제공해 줄 수 있기 때문이다.

Ⅲ. C-ITS의 통신 보안과 5G

국내와 미국, 유럽, 중국 등의 해외에서 다양한 C-ITS 사업들이 추진되고 있다. 이미 완료된 프로젝트들의 다수는 IEEE802.11p 표준〔2〕의 WAVE (Wireless Access in Vehicular Environments) 통신 규격을 채용하고 있다. 5G 통신의 실용화에 따라 5G 통신 규격을 채용한 C-ITS 사업들도 추진되고 있는 상황이다. 물리 통신 계층을 WAVE 혹은 5G를 사용하더라도 데이터 통신 규격과 보안 규격은 IEEE1609 표준을 준용하는 것으로 진행되고 있다. 특히, 보안은 IEEE1609.2 표준[3]에 따라 타원곡선 암호알고리즘 기반의 공개키 인증서를 사용한 인증과 암호화를 적용하고 있다.

3.1. IEEE1609.2와 SCMS 기술 규격

IEEE1609.2 표준은 IEEE1609 표준들 중에서 보안을 정의하고 있으며, 다음과 같은 특징을 가지고 있다.

(1) X.509와는 별개의 인증서 규격을 정의
(2) 전자서명의 검증과 인증서의 공개키 검증의 고속 처리를 위해 Implicit Certificate 방식의 인증서를 제공 가능
(3) 하나의 자동차가 임의의 시점에 복수 개의 유효한 인증서를 동시에 소유하고, 이를 무작위로 선택하여 사용
(4) 차량의 위치 정보의 보호를 위해 익명 인증서를 제공
(5) 하나의 자동차에게 대량의 인증서를 발급하기 위한 대량 발급 체계를 요구

V2V 혹은 V2I 통신으로 자동차는 {교통 정보, 전자서명, 인증서}의 조합으로 구성되는 정보를 불특정 다수에게 브로드캐스팅(broadcasting)하게 되고, 송신 차량의 인증서는 암호화되지 않은 상태에서 소유자 정보가 노출된다. 소유자 정보의 노출은 차량의 위치 정보와 이동 경로를 파악할 수 있어서 개인정보의 심각한 침해로 이어질 수 있다. IEEE1609.2는 자동차의 위치 정보를 보호할 수 있도록 소유자의 정보를 익명화하여 인증서를 생성하고, 차량은 임의의 시점에 복수 개의 유효한 익명인증서를 갖는다. 이러한 인증서 관리 방식은 기존의 일반적인 PKI(Public Key Infrastructure)와는 다르며 인증서를 발급하는 인프라 시스템이 복잡한 구조를 가지게 된다. 미국의 DoT (Department of Transportation)와 CAMP(Crash Avoidance Metrics Partnership) 컨소시엄은 IEEE1609.2의 활용을 위한 PKI의 규격을 SCMS(Security Credential Management System)[4]으로 정의했다.

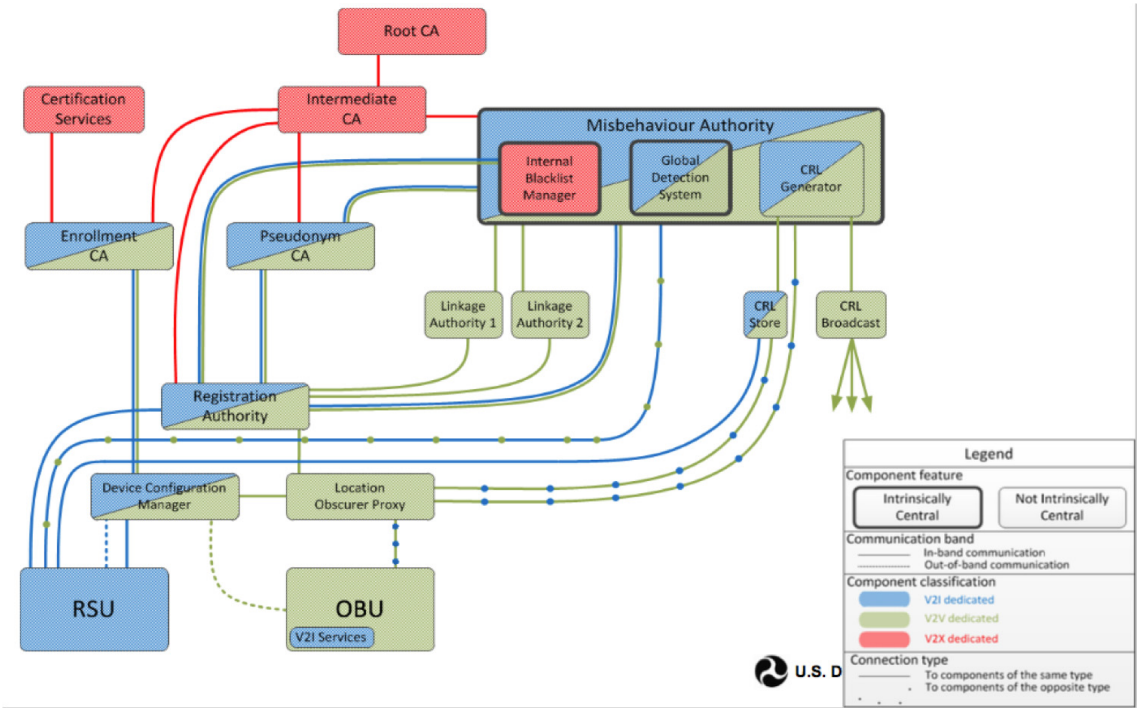
3.2. C-ITS의 개인정보 보호

IEEE1609.2와 SCMS는 자동차의 개인정보(위치정보)의 보호를 핵심 가치로 정의하고 이를 위해 여러 가지 기법들을 적용하고 있다.

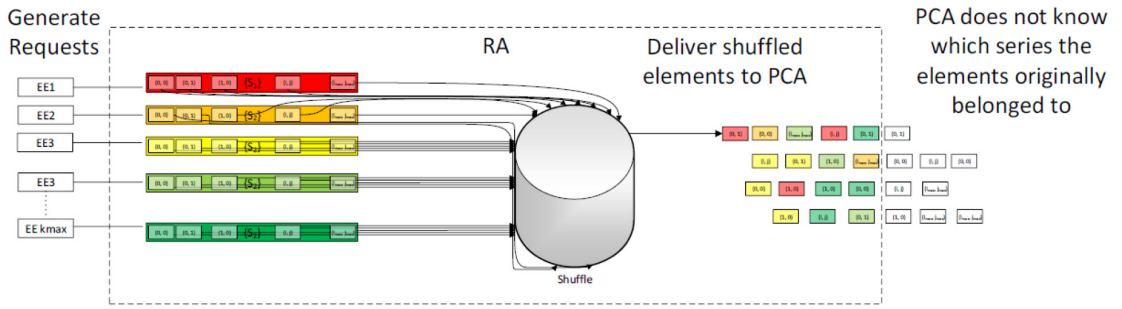
(1) 차량은 익명인증서를 사용하여 V2V 및 V2I 통신을 한다.
(2) 차량은 임의의 시점에 복수 개의 유효한 익명인증서를 복수 개로 가진다.
(3) 차량은 복수 개의 유효한 익명인증서를 무작위로 선택하여 V2V 및 V2I 통신에 사용한다.

차량이 복수 개의 익명인증서를 주기적으로 변경해서 사용하기 때문에, 브로드캐스팅되는 무선 통신 데이터를 모두 수집하더라도 특정 자동차가 어떤 위치에서 어떤 경로로 이동하는지를 분석하는 것은 불가능하다.

그러나, 위의 방식은 서비스 계층에서만 유효한 방식이다. 5G 통신이 도입되면 무선통신 모뎀의 식별자를 가지고 통신을 위한 MAC 주소 및 IP 주소를 가질 수 밖에 없다. 특정 자동차가 통신 시에 사용하는 인증



〔그림 2〕 SCMS의 PKI 구조



〔그림 3〕 SCMS의 LOP 개념

서는 익명인증서이고, 익명인증서도 매번 일정한 간격으로 변경된다고 하더라도 자동차가 갖는 IP 주소가 매번 동일하다거나 MAC 주소가 동일하다면 자동차의 위치와 이동 경로를 특정하고 추적할 수 있게 된다. 이를 막기 위해서는 자동차가 갖는 모뎀의 식별값, MAC 주소, IP 주소, 인증서가 일정한 간격으로 동시에 변경되어야만 한다.

5G 네트워크에서는 SUPI (SUbscription Permanant Identifier), SUCI (SUbscription Concealed Identifier), SUTI (SUbscription Temporary Identifier) 등의 기술을 통해서 가입자의 신원이 노출되는 것을 방지하는 기법을 제공하고 있다. 이 기술을 활용하여 자동차에 탑재되는 5G 통신 장치가 갖는 식별자의 노출을 최소화하고 IEEE1609.2의 익명인증서 이용 체계와 결합하여 자동차의 위치 정보를 보호하는 것이 필요하다.

자동차가 교통정보를 송수신할 때에는 익명인증서를 사용하여 개인정보를 보호할 수 있으나, 인증서의 발급 요청 등을 할 때에는 자동차의 신원을 확인하여야 하기 때문에 익명인증서를 사용할 수 없고, 자동차의 위치 정보가 노출될 수 밖에 없다. 이를 위해서 SCMS에서는 LOP(Location Obscurer Proxy)를 정의하고 있다.

LOP는 RA(Registration Authority)로 유입되는 자동차의 인증서 발급 요청(request)를 일정 시간 동안 보유하고 다른 다른 자동차의 요청과 함께 뒤섞어 CA(Certificate Authority)에 전송함으로써 CA가 자동차의 신원과 위치를 알 수 없도록 하는 방식이다. 5G에서는 네트워크 슬라이싱(Network Slicing)을 통해 특정 응용이나 서비스를 위해 네트워크를 가상화할 수 있다. SCMS의 LOP 기능을 5G 네트워크 구조에서 적용하기 위해서는 자동차의 V2I 통신을 네트워크 슬라이싱으로 네트워크 가상화 환경에서 제공할 필요가 있다. 네트워크 가상화를 통해서 CA는 수신한 요청이 물리적으로 어느 위치에서 어느 차량이 보낸 요청에 의한 것인지를 식별하지 못하도록 하여야 한다.

Ⅳ. 결 론

자동차 분야에서 모바일 네트워크의 도입과 연결성의 확대는 자동차의 변화와 진화에서 가장 중요한 요소라 할 수 있다. 연결성의 적용을 통해 자동차는 주변의 자동차 및 IoT와 정보를 주고 받을 수 있을 뿐만 아니라 원격의 온라인 서버와의 통신을 통해 자율주행을 완성할 수 있다. 또한 온라인 클라우드와 연결함으로써 사용자들에게 다양한 가치서비스를 제공할 수 있기도 하다. 5G 네트워크는 자동차의 연결성 확대에 큰 기여를 할 것으로 예상되며 자동차의 변화와 혁신을 이끄는 핵심 기술이라 할 수 있다.

자동차의 연결성을 확대함에 있어서 보안을 먼저 확보하여야 하고, 보안의 여러 기술들 중에서 인증 기술의 필요성은 필수적이다. 인증을 통해 자동차와 자동차, 자동차와 다른 개체 간의 통신 연결을 제공할 수 있으나 자동차의 신원과 위치 정보, 이동 경로 등의 개인정보가 유출될 수 있는 우려가 있다. 5G 네트워크는 LTE 등의 이전 기술에 비해 높은 보안성과 개인정보 보호 기술 등을 제공하고 있으나 자동차 분야에 적용하기 위해서는 서비스와 응용 계층의 자동차 보안 기술과의 결합하여 관리 및 운영 정책을 만들어 나가야 할 것이다.

참 고 문 헌

[1] *ISO 15118-1:2019 Road vehicles – Vehicle to grid Communication interface – Part 1: General information and use-case definition,* April 2019.

[2] IEEE, *802.11p-2010 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, July 2010.

[3] IEEE, *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages*, March 2016.

[4] https://wiki.campllc.org

〈저 자 소 개〉

심 상 규 (SangGyoo SIM)

1996년 2월 : POSTECH 전자전기공학과 학사
1998년 2월 : POSTECH 전자전기공학과 석사
2004년 2월 : POSTECH 전자전기공학과 박사
2005년 2월~2008년 4월 : 삼성전자 SW연구소
2014년 1월~2015년 12월 : 순천향대학교 융합서비스보안학과 겸직교수
2016년 1월~2016년 12월 : 동덕여자대학교 컴퓨터학과 겸직교수
2012년 2월~현재 : 펜타시큐리티시스템(주)
2019년 1월~현재 : 펜타시큐리티시스템(주) CTO
2018년 4월~현재 : AMO Labs, CEO
2019년 9월~현재 : POSTECH 가치융합창출학부 겸직교수
<관심분야> 자동차보안, IoT보안, 블록체인

김 의 석 (Eui-seok KIM)

1996년 : POSTECH 물리학과 학사
1999년 : NAS연구소 기획실장
2007년 : 펜타시큐리티시스템(주) 개발부장
2012년 : 펜타시큐리티시스템(주) 엔지니어링본부장
2016년 : 펜타시큐리티시스템(주) CTO
2018년 : 펜타시큐리티시스템 AutoCrypt사업본부장
2019년 : AutoCrypt, CEO
<관심분야> 자동차 V2X 보안, 전기차 충전 보안, 차량 내부 네트워크 보안

김 덕 수 (Duk Soo KIM)

1997년 2월 : POSTECH 전자전기공학과 학사
1999년 2월 : POSTECH 전자전기공학과 석사
1999년 1월~2019년 8월 : 펜타시큐리티시스템(주) CSO
2014년 9월~2018년 12월 : POSTECH 스타트업 인큐베이터 APGC-Lab Chief Director
2017년12월~현재 : Cloudbric, CTO
2019년 9월~현재 : Mobiligent, CEO
<관심분야> 클라우드보안, 자동차보안, 데이터분석