지능형 자율자동차 통신 보안 표준화 동향

이상우 한국전자통신연구원 정보보호연구본부 책임연구원, 응용보안평가인증(PG504) 의장

1. 머리말

최근 자율주행차량에 대한 연구가 급속도로 진행되는 가운데, 자율주행차량의 주행 안정성을 향상시킬 필수 요소 기술로서 차량통신기술의 상용화가 진행 중이다. 차량과 차량, 차량과 주변 환경과의 차량통신기술은 지능형 자율 자동차를 대상으로 하기 전부터 차량의 주행 안정성과 편의성을 향상시키기 위하여 꾸준히 연구되어져 왔다[1].

최근 차량통신기술은 지능형 자율자동차에서 그 중요성이 더욱 부각되고 있다. 지능형 자율자동차에서 센서를 통해 수집되는 차량 주변 환경정보의 한계를 극복하기 위하여 차량통신기술의 활용성이 강조되기 때문이다. 그러나 차량통신기술을 활용하기 위해서는 반드시 보안 기술의 확보가 선행되어야 한다. 차량통신 환경은 인터넷 등의 기존 네트워크 환경과 달리 네트워크의 보안성 확보 여부에 따라 운전자 및 보행자의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 따라서 차량 통신 환경에서의 사이버 보안사고 방지를 위한 연구 개발 및 다양한 표준화활동이 진행되고 있다[2,3].

ITU-T SG17은 통신 분야 표준화를 다루는 국제 기구인 ITU-T 산하의 사이버 보안기술에 대한 전문 표준화 그룹이다. SG17의 ITS(Intelligent Transport System) 보안 연구반(Question 13)은 차량통신보안기술의 표준화 필요성이 대두됨에 따라, 2017년 3월 설립되어 차량내부망 보안, 차량외부망 보안 및 ITS 응용보안 분야에서 표준화를 활발히 추진하는 중이다. 본 논문에서는 SG17의 ITS 보안연구반에서 추진 중인 표준화 동향과 TTA PG504가 추진하는 국내 차량통신 보안 표준화 현황을 소개한다.

2. 차량통신보안 표준화

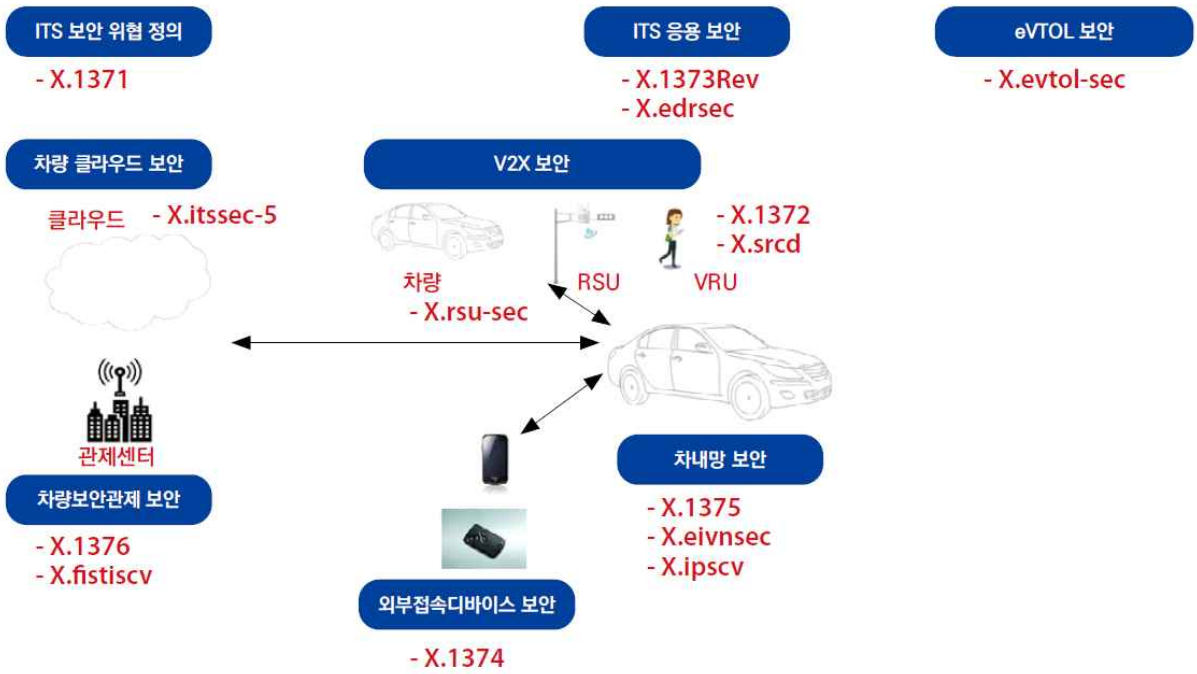
2.1 ITU-T SG17에서의 차량통신보안 표준화 동향

ITU-T SG17의 ITS 보안연구반(Question 13)의 표준화 범위는 차내망 보안, 차외망 보안, 차량 응용 서비스 보안, 차량외부접속디바이스 보안, 차량보안관제 보안, 차량 클라우드 보안 및 ITS 생태계의 기초적인 보안 위협 정의 등이다. [그림 1]은 SG17 ITS 보안연구반의 표준화 영역과 표준 아이템을 도시한 것이다.

<표 1>은 ITU-T SG17 ITS 보안연구반이 제정완료한 표준 목록을 나타낸 것이다[4~9].

X.1371(커넥티드 차량 보안 위협)은 커넥티드 차량 및 에코시스템에서의 보안 위협을 정의하는 것이다. UNECE(United Nations Economic Commission for Europe) WP29에서 제정한 '차

량 사이버보안 권고안(UN R155)[19]'의 보안 위협을 기반으로 하여, 커넥티드 차량에 대한 상위 레벨의 위협을 정의하고 있다.



[그림 1] ITU-T SG17 Q13 표준화 범위

<표 1> ITU-T SG17 Q13 차량통신보안 표준화 완료 목록>

약어	제목	승인시기
X.1371	Security threats in connected vehicles	2020
X.1372	Security guidelines for V2X communication system	2020
X.1373	Software update capability for ITS communications devices	2017
X.1374	Security requirements for external interfaces and devices with vehicle access capability	2021
X.1375	Guidelines for intrusion detection system for in- vehicle networks	2021
X.1376	Security-related misbehavior detection mechanism based on big data analysis for connected vehicles	2021

X.1371에서 정의된 보안 위협은 SG17 ITS 보안연구반에서 제정 중인 표준화 과제에서 참조하여 표준화가 진행 중이다.

X .1372(V2 X 통신 보안가이드라인)은 차량외부 통 신에서의 보안위협, 보안요구사항을 정의하고 있으며, ETRI 및 현대차가 주도적으로 표준화를 추진하였다. 차량외부통신망은 V2X (Vechicle-to-Everything) 통신이라고도 한다. 차량과 차량(V2V, Vehicleto-Vehicle), 차량과 인프라(V2I, Vehicle-to-Infrastructure), 차량과 노매딕 디바이스(V2D, Vehicle-to-Nomadic Device), 차량과 네트워크(V2N, Vehicle-to-Network)를 통칭한다.

X.1372에서는 V2X 환경의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증서비스 모델 등의 유스 케이스를 정의하고 있다. 특히 본 표준에서는 V2V/V2I 통신 환경을 차량

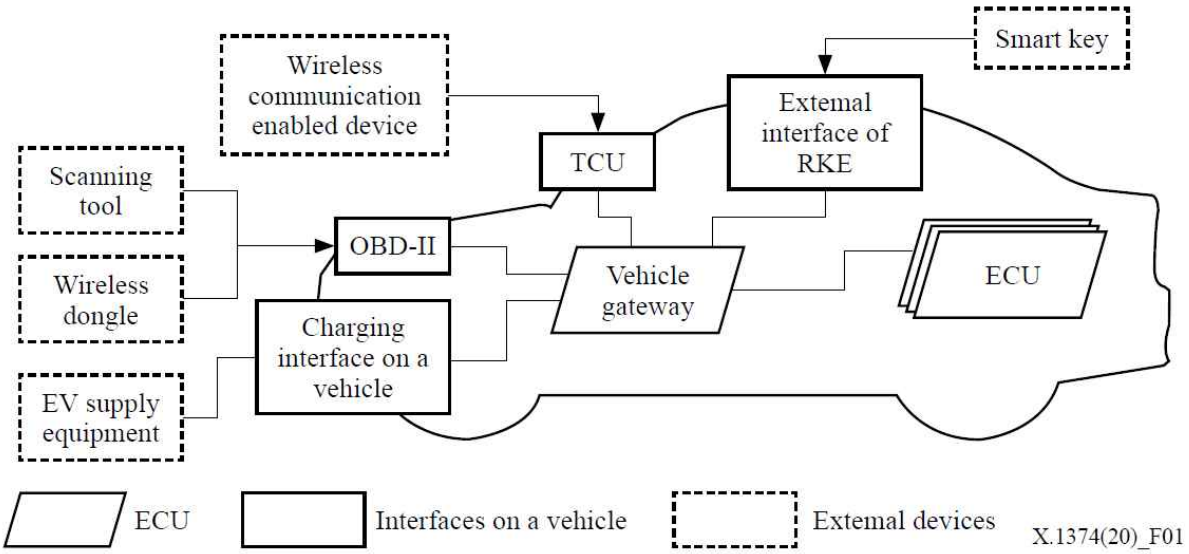
간 경고 전파, 차량 그룹 통신, 차량 경계, 차량과 인프라 간 경고 전파 형태로 구분하고, 상기 형태에 따른 보안 요구사항을 정의하고 있다. 또한 차량용 PKI(Public Key Infrastructure)의 참조 예로서, 유럽 ETSI의 예 및 미국 CAMP(Crash Avoidance Metrics Partnership)의 참조 모델에 대한 설명이 부록에 기술되어 있다. 차량통신에서의 메시지 암호화 방법 및 메시지 서명 방법도 소개되어 있다. 즉, 현재 차량통신환경에서 많이 쓰이는 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDSA(Elliptic Cureve Digital Signature Algorithm)의 규격을 정의하고 있다. 특히 X.1372에서는 차량군집주행서비스를 제공하기 위한 차량 인증 방법도 정의하고 있다.

X.1373(ITS 통신장비의 소프트웨어 업데이트)는 안전한 차량 소프트웨어 업데이트 절차를 정의한다. 차량에 다수의 ECU(Electronic Control Unit)가 쓰이고, 리콜 차량의 약 30%가 ECU 소프트웨어 업데이트 문제 때문으로 보고되는 현상을 반영, SG17의 ITS 보안 표준안 중 가장 먼저 표준으로 승인되었다. X.1373에서는 차량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다. 특히, 2017년 표준안 최종 승인 과정에서 차내망과 연관된 메시지는 부가적인 메시지로 지정되었으나, 완성차 업계의 차내망 연관 규격을 포함하여야 한다는 의견이 반영되어 현재 개정 작업이 진행중이다. 본 표준은 차량 소프트웨어 업데이트 세부 절차의 메시지 포맷과 XML 예제도 포함하여 기술하고 있다.

X.1374(차량 접속 외부 인터페이스 및 디바이스의 보안요구사항)은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것으로, 현대차 및 ETRI가 주도적으로 표준화를 추진하였다. X.1374는 차량 내부 진단 도구가 많이 활용하는 OBD-II(On-Board-Diagnostic II) 포트 및 블루투스 등을 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항을 정의하고 있다. 차량에 접속하는 디바이스의 일반적인 보안요구사항으로 하드웨어가 지원하는 보안 기능을 구비할것을 명시하고 있으며, 세부적인 요구사항으로는 보안 CPU, 보안 저장장치, 하드웨어 암호 가속 기능을 제시하고 있다. 차량 외부 접속 장치의 통신 기능 보안요구사항으로는 블루투스, 이동통신, Wi-Fi 등을 사용할 때 준수해야 하는 보안 요구사항을 기술하고 있다. 스마트 키의 경우, 키 추출방지 기능 및 one time programmable 기능 등의 역공학방지요구사항, 상호인증, 재생공격방지 및 무선신호전력제어 등의 통신보안요구 사항과 안전한 키 등록 기능 요구사항을 제시하고 있다. 또 외부접속장치로서, 스마트 키나 전기차충전시스템, Wi-Fi 또는 블루투스를 이용하는 접속장치에 적용될 수 있는 보안 제어 방법을 유스 케이스로 제시하고 있다. 부록에는 블루투스 및 이동통신망에 대한 기술 규격을 기술하고 있다. 본 표준은 완성차 업계의 요구사항을 반영하여 진행된 표준으로서, 향후 차량에 접속하는 디바이스 제작 및 관련 서비스 업계에서 참고할 필요가 있다. [그림 2]는 X.1374에서 다루는 차량 접속디바이스 및 인터페이스를 도시한 것이다.

X.1375(차내망 침입탐지시스템 가이드라인)은 차내망 침입탐지시스템 구성 방법을 정의하는 것으로, 고려대와 현대차, ETRI가 주도적으로 표준화를 추진하였다. X.1375는 차내망으로 많이 활용되는 CAN(Controller Area Network) 환경에 적합한 침입탐지시스템의 기능 및 규격을 정의하고 있다. 또 차내망 침입탐지시스템 구현을 위한 탐지 방법인 정적탐지(Static detection),

오용탐지(Misuse detection) 및 비정상탐지(Anomaly detection)의 특징을 기술하고 있다. 부록에는 차내망 침입탐지시스템의 기본 구조와 차내망 트래픽의 특징을 기술하고 있다.



[그림 2] 차량 접속 디바이스 및 인터페이스 환경

X.1376(커넥티드 차량의 보안이상행위탐지 메커니즘)에서는 차량의 사이버 보안 관련 비정상 행위 탐지 메커니즘을 정의하고 있다. 본 표준은 차량의 비정상행위를 수집하고 다양한 탐지 방법을 제공하며, 각 탐지 방법에 대한 사용 예를 부록에 담고 있다. 이 표준은 중국의 보안 업체 Qihoo 360 Technology이 주도한 표준으로, 차량용 안티바이러스 제품에 활용될 가능성이 높다.

ITU-T SG17 ITS 보안연구반에서는 <표 2>와 같이 현재 9개의 표준화 과제가 진행 중이다[10~18]. 그중에서 한국이 주도적으로 추진하고 있고, 2022년 사전채택 또는 사전승인을 목표로 추진하고 있는 표준화 과제의 주요 내용은 다음과 같다.

<표 2> ITU-T SG17 Q13 차량통신보안 표준화 진행 현황

약어	제목	추진일정
X.srcd	Security requirements for categorized data in V2X communication	2022.4Q
X.eivnsec	Security guideline for Ethernet-based In-Vehicle networks	2022.4Q
X.edrsec	Security guidelines for cloud-based data recorders in automotive environment	2022.4Q
X.fstiscv	Framework of security threat information sharing for connected vehicles	2022.4Q
X.ipscv	Methodologies for intrusion prevention system in connected vehicles	2022.4Q
X.rsu-sec	Security requirements for road-side units in intelligent transportation systems	2022.1Q
X.itssec-5	Security guidelines for vehicular edge computing	2023.4Q
X.1373Rev	Software update capability for ITS communications devices	2023.4Q
X.evtol-sec	Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment	2024.4Q

- X.ipscv(차량 침입방지스템 구현방법론)은 차량의 침입방지시스템의 구현방법론을 정의하는 것이다. 차량 침입탐지시스템의 보안 기능을 정의하는 X.1375와 연계하여 차내망 침입탐지기능을 이용한 차량 보안 침입 방지 시스템 구현 가이드라인을 표준화 내용으로 담고 있다. 즉, 차내에는 최소한의 침입탐지기능만 탑재하고, 수집된 침입 탐지 결과를 활용하여 차량 외부 서버에서 탐지 결과를 분석하여 최종적으로 차량이 외부의 비정상적 공격에 대응하도록 하는 프레임워크를 제공하는 것이 목적이다.
- X.eivnsec(이더넷 기반 차내망 보안가이드라인)은 이더넷 기반 차량 내부 네트워크의 보안위협, 보안요구사항 및 사용 예를 정의하는 것이다. 차량에 탑재된 카메라 및 센서 등으로인하여 차량 내부망에서 송수신되는 데이터 양이 증가함에 따라 현재 완성차 업계에서는 차량용 이더넷의 도입을 추진하고 있다. 이러한 업계 현황을 반영하여 한국 ETRI 및 차량 보안업체 Escrypt가 주도적으로 표준화를 추진하고 있다. 독일의 차량부품업체 Bosch도 관심을 가지고 적극적으로 표준화를 추진하는 중이다. X.eivnsec은 차내망 이더넷 보안게이트웨이의 기능요구사항을 정의하고. 부록에는 차량용 이더넷을 지원하는 AUTOSAR(AUTomotive Open System ARchitecture) 규격과 차량 게이트웨이에 대한 정보를 포함하고 있다.
- X.edrsec(클라우드 기반 차량 데이터 기록 장치 보안가이드라인)은 클라우드 기반의 차량 사고기록장치 시스템의 보안위협, 보안요구사항 및 사용 예를 정의한다. 자율주행차 운행에 있어서 사고 당시의 차량운행주체정보의 안전한 전송 및 관리 방법에 대한 보안요구사항도 정의해 나가고 있다. 한국의 ETRI 및 현대차가 주도적으로 표준화를 추진하는 중이다.

또한 ITU-T SG17 ITS 보안연구반에서는 V2X 통신환경에서 데이터 속성에 따른 보안 등급 분류를 X.srcd에서 다루고 있으며, 차량통신환경에서 인프라 및 차량과의 통신을 담당하는 노변기지국(RSU, Road-Side Unit)의 보안요구사항은 X.rsu-sec에서 다루고 있다. 본 표준은 중국 차이나모바일이 주도적으로 추진하고 있으며, 향후 셀룰러 V2X 환경을 고려한 보안요구사항도 정의해 나갈 계획이다.

ITU-T SG17 ITS 보안연구반에서의 최근 표준화 현황 중 주목해야 할 사항은 도심항공모빌리티 보안에 대한 표준화를 시작했다는 점이다. 2020년 8월 X.evtol-sec(도심항공모빌리티 환경에서의 eVTOL 보안가이드라인)이 신규 표준화 과제로 채택되었다. eVTOL은 전기동력 수직이착륙 항공기를 의미하는 것으로 도심용 항공모빌리티(UAM, Urban Air Mobility)의 대표적 교통 수단이다. 활주로가 필요 없는 교통수단으로서 에어 택시라고도 불린다. eVTOL은 사람을 탑승객으로 하는 교통수단이라는 점에서 기존 드론과 차별화되며, 한국의 현대차 및 ETRI가 표준화를 주도적으로 추진하고 있다.

2.2. TTA PG504의 차량통신보안 표준화 현황

국내에서는 TTA의 PG504(응용보안 및 평가인증)에서 ITS 산업계에서 참고할 수 있는 차량보

안 표준화를 추진하고 있다. TTA PG504는 차량 간 통신 보안요구사항(TTAK.KO-12.0208, 2012년)의 표준화를 시작으로, 2022년 현재까지 차량외부망 및 차량내부망 환경에서 다수의 차량통신보안 표준 제정을 추진하였다. 현재 무선통신기반 열차제어시스템의 보안요구사항 및 도로교통인프라 통합보안센서 보안요구사항 등의 표준화가 진행 중이다. <표 3>에 표준으로 제정된 목록 및 주요 내용을 요약하였다.

<표 3> PG504 차량보안 관련 제정 표준

제목	주요내용	표준번호	제정년도
차량용 이더넷 보안요구사항	차량내부망으로서 차량용 이더넷이 활용될 때의 보안 위협 및 보안요구사항을 정의	TTAK.KO-12.0363	2020
자동차 내부 계측 제어기 통신망을 위한 능동적 사이버 방어 체계 보안 요구 사항	자동차 내부 계측 제어기 통신망에서 보호 대상의 주요 속성(IP Address, Port, Protocol, Platform, OS 등)을 이동(Moving)시키면서 공격자의 공격 또는 분석 행위를 무력화시키는 능동적인 방어 전략인 능동적 사이버 방어 체계 보안 요구 사항을 정의	TTAK.KO-12.0364	2020
차량·사물 통신용 하드웨어 보안 모듈(HSM) 보안 요구 사항	전자서명키 등의 비밀정보를 안전하게 저장하고, 전자서명 및 암호화 등을 수행하는 하드웨어 모듈인 HSM을 차량통신환경에 적용할 때의 기능 및 보안요구사항을 정의	TTAK.KO-12.0365	2020
오토사(AUTOSAR) 기반의 차량 보안 기능 개발 지침	오토사(AUTOSAR) 기반의 차량 제어기를 개발할 때 적용 될 수 있는 보안 기능을 설명하고, 이를 적용하는 방법과 유의해야 할 사항을 기술	TTAK.KO-12.0357	2019
차량 내부 네트워크 보안 요구사항	자동차 내부 네트워크를 안전하게 보호하기 위하여 자동차 내부 네트워크 구성 요소들의 운용 및 관리 시 발생 가능한 사이버 보안 위협을 분석하고, 이에 대응하기 위한 보안 요구 사항을 정의	TTAK.KO-12.0346	2019
클라우드 커넥티드 자동차 보안요구사항	자동차와 클라우드 연계 방식 및 구조, 보안위협 및 보안 요구사항 정의	TTAK.KO-12.0342	2018
차량의 군집 주행 서비스를 위한 차량 등록 절차	차량의 군집 주행 서비스를 위한 차량 등록 절차 및 군집 형성을 위한 군집리더 차량의 인증서 발급 절차를 정의	TTAK.KO-12.0318	2017
자동차 전자제어장치(ECU) 펌웨어 보안 요구사항	자동차 내부에 탑재된 전자제어장치 펌웨어의 운용 및 관리 시 발생 가능한 보안 위협 분석 및 보안 요구사항 정의	TTAK.KO-12.0300	2016
차량 내부 통신을 위한 전자제어장치(ECU) 보안 구조	차량에 탑재되는 전자제어장치의 사이버 보안 안전성을 강화하기 위한 구조를 정의	TTAK.KO-12.0299	2016
차량의 군집 주행 서비스 보안 요구 사항	다수의 차량이 하나의 그룹을 형성하여 그룹의 리더 차량 및 다수의 멤버 차량으로 구성되어, 차량 간 통신을 이용하여 차량의 주행 정보(위치, 속도 등)을 교환하며, 멤버 차량이 차간 거리를 유지하며 선두 차량을 따라가는 주행 방법인 군집 주행 서비스에서의 보안요구사항을 정의	TTAK.KO-12.0290	2015
자동차 전자 제어 장치 간의 통신 보안 요구 사항	자동차 내부에 탑재된 전자 제어 장치 간의 통신 환경에서의 위협 분석 및 보안 요구 사항 도출	TTAK.KO-12.0286	2015
차량간 통신환경에서의 메시지 암호화 규격	차량 간 통신에서의 메시지를 암호화할 때 사용되는 암호 알고리즘의 차량 통신 환경에 특화된 제약 사항을 기술	TTAK.KO-12.0260	2015
차량 간 통신 인증 서비스 구조	차량간 통신환경에서 인증기관의 구조 및 인증서의 내용 및 기능을 정의	TTAK.KO-12.0238	2013
차량 간 통신 보안 요구사항	차량 간 통신을 서비스 형태로 구분하고, 각 서비스 형태에 따른 보안요구사항을 정의	TTAK.KO-12.0208	2012

3. 맺음말

지능형 자율자동차는 자율주행의 실현을 위하여 정확한 주변 환경 인식이 필수적이다. 센서로 수집되는 데이터를 보완하기 위하여 차량통신기술이 적극 활용되는 상황이나, 차량통신은 보안성이 선행되어야 운전자 및 탑승자, 주변 차량의 안전을 보장할 수 있다. 이에 차량통신보안 표준화를 활발히 추진하고 있는 ITU-T SG17 ITS보안연구반의 표준화 활동과 국내 TTA PG504의 표준화 현황을 살펴보았다.

사이버보안 공격으로부터 안전한 차량통신 환경을 구축하고 이를 자율주행차량에 활용하기 위해서는 지속적인 차량통신보안 연구가 필요하다. 이와 동시에 표준화 역시 적극적으로 추진할 필요가 있다. 급변하는 차량통신보안 표준화 분야의 주도권을 선점하기 위하여 학계, 산업계, 연구기관 등의 적극적인 표준화 참여가 필요하다.

※ 본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉채널 위험성 검증 연구)

[참고문헌]

[1] 이상우 외, "차량 통신 보안 기술 동향," 주간기술동향, vol. 1556, 2012.
[2] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, 2010.
[3] IEEE Std 1609.2, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages, 2016.
[4] ITU-T SG17 Recommendation, X.1373, Secure software update capability for ITS communications devices. 2018
[5] ITU-T SG17 Recommendation, X.1371, Security threats to connected vehicles, 2020.
[6] ITU-T SG17 Recommendation, X.1372, Security guidelines for Vehicle-to-Everything(V2X) communication. 2020.
[7] ITU-T SG17 Recommendation, X.1374, Security requirements for external interfaces and devices with vehicle access capability, 2021.
[8] ITU-T SG17 Recommendation, X.1375, Guidelines for intrusion detection system for in-vehicle networks, 2021.
[9] ITU-T SG17 Recommendation, X.1376, Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles, 2021.
[10] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelines for vehicular edge computing, 2021.
[11] ITU-T SG17 draft Recommendation, X.srcd, Security requirements for categorized data in V2X communication, 2021.
[12] ITU-T SG17 draft Recommendation, X.eivnsec, Security guidelines for Ethernet-based In-Vehicle networks, 2021.
[13] ITU-T SG17 draft Recommendation, X.edrsec, Security guidelines for Ethernet-based

In-Vehicle networks, 2021.
[14] ITU-T SG17 draft Recommendation, X.fstiscv, Framework of security threat information sharing for connected vehicles, 2021.
[15] ITU-T SG17 draft Recommendation, X.1373rev, Software update capability for ITS communications devices, 2021.
[16] ITU-T SG17 draft Recommendation, X.rsu-sec, Security requirements for road-side units in intelligent transportation systems, 2021.
[17] ITU-T SG17 draft Recommendation, X.ipscv, Methodologies for intrusion prevention system in connected vehicles, 2021.
[18] ITU-T SG17 draft Recommendation, Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment. 2021.
[19] UN R155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.04

※ 출처: TTA 저널 제199호