논문 2022-2-10 http://dx.doi.org/10.29056/jsav.2022.12.10

C-ITS 보안 기술 분석에 관한 연구

서대희*†

A Study on C-ITS Security Technology Analysis

Daehee Seo*†

요 약

스마트시티의 교통인프라 및 관제 체계가 디지털화되어감에 따라 통신상의 데이터 유출 및 원격해킹으로 인한 자동차 제어, 교통시스템 마비 등의 다수의 보안위협이 발생될 수 있다. 특히 보안위협으로 인해 인명사고부터 크게는 교통인프라 마비 등과 같은 대형사고가 발생할 수 있다. 이는 사용자의 안전과 밀접한 관계이기 때문에 보안에 대한 이슈는 더욱 중요해졌다. 따라서, 차세대 교통시스템(C-ITS; Cooperative Intelligent Transport Systems)의 특성을 파악하는게 우선이다. C-ITS에서 발생할 수 있는 사이버 공격과 침해사고를 분석하고, 이에 대한 해결책 및 보안 관련 기술들에 대한 연구가 필요하다. 본 논문에서는 C-ITS 환경에서 발생할 수 있는 보안 이슈 및 요구사항 등에 대해 분석한다. 또한 각 주요국의 C-ITS 관련 보안 기술들과 표준화 기술 내용을 분석하여 정리하고, 이를 기반으로 국내에서 안전한 C-ITS 환경을 위해 연구해야할 방향을 제언한다.

Abstract

As the smart city's traffic infrastructure and control system become digitized, several security threats, such as data leakage in communication and vehicle control due to remote hacking and traffic system paralysis may occur. In particular, due to security threats, major accidents such as human casualties and paralysis, of transportation infrastructure can occur. Since these are closely related to user safety, security issues have become more important. Therefore, it is a priority to understand the characteristics of the C-ITS(Cooperative Intelligent Transport Systems). It is necessary to analyze cyber attacks and intrusions that may occur in C-ITS, and to study solutions and security-related technologies. In this paper, we analyze security issues and requirements that may occur in the C-ITS environment. It analyzes and organizes each major country's C-ITS-related security technologies and standardization technologies. Based on this, we suggest the research direction for a safe C-ITS environment in Korea.

한글키워드 : 차세대 지능형 교통 시스템, 스마트시티, ITS 보안위협, ITS보안기술, ITS 보안 표준

keywords : C-ITS, Smart City, ITS Security Threat, ITS security technology, ITS Security Standards

1. 서 론

기존의 주요 도시인구 과밀 현상 및 해결을 위해 정보통신, 빅데이터, 인공지능, 5G/6G 기술 등을 기존 교통체계에 접목시킨 차세대 교통시스템(C-ITS; Cooperative Intelligent Transport Systems)의 도입이 요구된다. 해당 기술은 스마

* 상명대학교 지능데이터융합학부
† 교신저자: 서대희(email: daehseo@smu.ac.kr)
접수일자: 2022.09.15. 심사완료: 2022.11.08.
게재확정: 2022.12.20..

트시티 미래 신교통수단 프레임워크를 구축하기 위한 핵심적인 과제로 대두되고 있다. 또한 스마트시티환경에서 더욱 상용화 될 전기차, 수소차, 자율주행차량의 활성화를 위한 필요한 인프라 구축이 될수 있다. 차량-인프라 간 (V2X) 양방향 정보수집 및 제공 체계 기반 시스템이 수립되는 과정에서 발생되는 문제점을 파악하고, 기존 시스템과의 호환성과 비용을 고려하여 신규 서비스 개발과 서비스 고도화가 요구되고 있다.

스마트시티의 교통인프라 및 관제/통제 체계가 디지털화되어감에 따라 다수의 보안위협이 발생될 수 있기 때문에, 이에 맞는 보안 기술 및 고도화는 필수적인 요소가 되었다. 도시 내 주요 교통 관리를 전담하는 기반시설의 파괴 및 침해는 사회 경제적 손실을 비롯해 개인의 자유 및 권리를 위협하는 결과를 초래한다. 특히 교통신호제어시설이 보안위협에 노출되었을 경우에는 교통사고 등 사회 혼란을 유발시킬 뿐아니라, 시민들의 생활도 불편해진다. 최근 사람들의 인식은 구축된 제어시스템들이 폐쇄망으로 운영하고 있기 때문에 안전하다고 생각한다. 이에 정보보안 시스템이 구축되지 않거나 바이러스 백신 업데이트 및 보안 패치 등이 올바르게 이루어지지 않았다면, 이를 공격자가 이용하여 사이버 보안 공격에 노출될 수 있다. 따라서, 지능형교통시스템의 특성을 파악하는게 우선이며, 발생할 수 있는 사이버 공격 및 침해사고에 대안을 마련해야 한다[1].

현재 세계적으로, 자동차 보안시장 및 스마트시티 교통의 수요와 그 규모는 증가하고 있기 때문에, 우리나라 또한 자동차 보안 및 스마트 시티 교통 관련 기술 R&D(Research and Develop) 및 실증 사업을 계획하고 수행해야 할 필요가 있다[2]. C-ITS의 완전한 구현을 위해 실시간으로 교통 정보의 공유가 이루어져야 한다. 하지만, 현재 기술로는 C-ITS를 구축하기 위해 몇몇 한계점이 존재한다. 추가적으로 차량, 보행자, 센터 등을 포함한 도로 위 모든 객체가 자유롭게 통신하기 위해 교통 정보를 개방할 시 다수의 보안 이슈가 발생할 수 있기 때문에, 보안 이슈에 대한 우려 또한 커지고 있다. 따라서 통신, 지도 구축, 보안 등 지속적으로 관련 기술 연구에 대해 관심가져야 할 필요가 있다.

본 논문에서는 차세대 교통시스템(C-ITS; Cooperative Intelligent Transport Systems) 환경에서 발생할 수 있는 보안 이슈 및 기술을 분석하고, C-ITS에 대한 내용과 발생되는 문제점에 대한 연구방향을 제안하였다.

2. C-ITS와 보안 이슈

2.1 C-ITS

차세대 지능형 교통시스템은 사물 인터넷을 통해 차량-인프라 혹은 차량-차량 간에 양방향으로 데이터를 교환하며, 신속하게 도시에서 발생하는 문제들에 대응하고 예방한다. 세부적으로, 네트워크 기반의 C-ITS는 V2V, V2I, V2X, 등 정보를 실시간으로 주고받으며 협력하고, 정보공유 체계를 구축할 수 있다. 그리고 인프라와

표 1. C-ITS 용어설명
Table 1. C-ITS notation

모빌리티용어	설명
V2X (Vehicle-to-Everything)	차량과 다른 차량, 도로, 스마트콘 등 사물과 통신으로 정보를 주고받는 기술
V2V (Vehicle-to-Vehicle)	차량과 차량 간 통신 (차량끼리 정보를 주고받으며, 앞차와의 간격등을 제어 하는 기술)
V2I (Vehicle-to-Infrastructure)	차량과 인프라 통신 (신호등과 기지국 등 인프라와 소통하며, 교통현황과 사고 상황등을 파악하는 기술)

차량이 통신하여 실시간 교통 상황 또는 도로 위 돌발 상황을 빠르게 전달한다. 그리고 차량의 정밀한 위치 파악이 가능하다[3]. 추가적으로, 차량이 서로 통신 시 가속 또는 급정거, 접근, 추돌 등의 정보도 알 수 있으며, 이를 통해 차량 정체 및 사전에 2차 사고를 예방할 수 있다. 이를 기반으로 국토교통부는 안전 서비스 제공 시 운전자가 사고 위협에 대응할 수 있는 능력을 48.9% 가량 높이고, 사고를 최대 40.5% 가량 줄이는 것으로 예측하였다. 그림 1은 C-ITS 시스템 구조를 나타낸 그림이다.

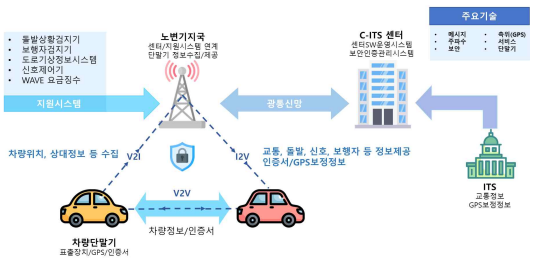

그림 1. C-ITS 시스템 구조
Figure 1. C-ITS system structure

2025년까지 국토교통부는 지자체에 ITS 구간 1만7483㎞, C-ITS 구간 1만2995㎞를 구축하고자 한다. 국토교통부의 서비스 분류에 대한 내용은 표 2와 같다.

2.2 스마트 차량

정보통신기술을 차량에 적용하였을 때, 더 편리하고 안전한 차량의 서비스를 제공받을 수 있는 스마트 차량(Smart Car)이 될 수 있고, 이와 관련된 다양한 기술들은 많은 관심을 받고 있다.

스마트 차량은 차세대 정보통신, 전기전자, 기능제어 기술을 차량 기술에 접목하여 차량의 내부 및 외부 상황을 실시간 인식하고, 고편의 고안전, 기능을 제공할 수 있는 차량을 의미한다

표 2. C-ITS 서비스 분류
Table 2. C-ITS Service Classification

A. 위치 기반 데이터 수집
B. 위치 기반 교통정보 제공
C. 요금징수 시스템
D. 도로위험구간 정보제공
E. 노면 기상정보 제공
F. 도록작업구간 주행지원
G, 교차로신호위반 위험경고
H. 우회전 안전운행 지원
I. 버스 운행관리
J. 엘로우버스 운행안내
K. 스쿨존 속도제어
L. 보행자 충돌방지 경고
M. 차량 추돌방지 지원
N. 긴급차량 접근 경고
O. 차량 긴급 상황 경고

[4]. 스마트 차량은 각 기능과 센서를 제어하는 ECU를 차량 내부망으로 연결한다. 그리고 이에 발생하는 정보를 기반으로 차량의 구동 및 제동, 조향, 각종 센서로부터 발생하는 정보를 전자장비가 제어한다. 이로써, 안전하고 편리한 차량 서비스를 제공받을 수 있기 때문에, 많은 관심을 받고 있다[5-6]. 추가적으로, 기존의 차량 제조사 외에 구글, 애플, 마이크로소프트 등 세계적인 IT 기업과 국내의 삼성전자 LG전자 등도 스마트 차량 개발연구에 참여하고 있다.

2.3 C-ITS 보안 이슈

양방향으로 실시간 통신을 기반으로 구성된 C-ITS 환경에서 스마트 차량이 V2V 또는 V2I의 정보 공유가 가능한 차세대 지능형 교통 시스템 시대로 도래했다. 이에 따라 다수의 보안 이슈가 발생 되고 있다. 특히 C-ITS 보안 중 차량 내부통신 및 처리에서 서비스의 정보유출, 데이터 위조 및 변조 등의 위협이 주요 보안 이슈이다. 또한 해킹을 통해 오작동 사고는 사람의 생명도 위협할 수 있으므로 보안 기술에 대한 개발

연구가 필수적이다. C-ITS 환경에서 발생할 수 있는 보안위협은 다음과 같이 크게 4가지로 구분된다[4].

- **스마트 차량 내부 전자 제어 장치 해킹으로 인한 보안 이슈**: 스마트 차량 내부 네트워크에서 전달되는 데이터들은 통신시 암호화되지 않은 형태로 사용된다. 따라서, 스마트 차량 내부 전자 제어 장치를 해킹하게 되면, 차량 운행에 필요한 많은 정보를 조작할 수 있다. 외부와 연결되지 않은 환경은 해킹에 대한 문제가 고려하지 않지만, 만약 네트워크를 통해 외부망과 연결이 된다면, 이는 보안위협 관점에서 큰 문제가 될 수 있다. 해당 문제는 내부 네트워크에 전송되는 데이터들을 암호화 하여 전송함으로써 해결할 수 있으나, 차량의 특성상 실시간으로 전달되는 데이터의 암·복호화에 적지 않게 많은 연산 및 시간을 소요한다면 차량제어에 영향을 줄 수 있다. 이를 해결하기 위해서는 차량을 운행 및 제어하는데 문제가 되지 않는 수준의 최적화된(경량화된) 암호기법을 연구개발하고, 이를 C-ITS 환경에 잘 적용해야 한다.
- **스마트 차량의 플랫폼이 가지고 있는 취약점을 활용한 원격 해킹으로 인한 보안 이슈**: 공격자가 스마트 차량 플랫폼이 가지고 있는 취약점 등을 이용하여 원격 해킹을 수행하고, 이로 인해 사고를 유발한다. 취약점을 해결하기 위해 시큐어 코딩 등의 기법을 잘 적용하여 플랫폼과 서비스를 설계 및 구현해야 하며, 최대한 보안 위협이 존재하지 않는 플랫폼이 되기 위해 수많은 테스트를 해봐야 한다. 또한, 완성된 플랫폼의 취약점 검색기법에 대한 정보보안 연구도 필요하다.
- **스마트 차량과 C-ITS간의 통신에서 잘못된 교통 정보를 전송함으로써, 안전주행 방해 등의 보안 이슈**: 스마트 차량과 C-ITS는 실시간 상황 정보를 주고받는데 있어, 대상 간의 상호 인증을 통해 신뢰할 수 있어야 한다. 기존 공개키를 기반으로 여러 상호 인증 기법들이 연구되었으나, 빠르게 이동 중인 V2I, V2V 사이의 통신을 위해서는 좀더 효과적인 인증 기법이 필요하다. 또한, 교차로 정보 지원 및 자율주행을 수신하고 있는 차량에 대해서 분산 서비스 거부와 같은 공격이 수행될 경우 이를 신속하데 인지하고 대응 가능한 보안기술이 필요하다.
- **스마트 차량 통신 내역을 바탕으로 개인의 프라이버시를 침해하는 보안 이슈**: 기본적으로 스마트 차량의 통신 내역을 통해 차량의 이동 경로를 알 수 있다. 이를 통해 차량이 방문한 곳이 어디인지 유추할 수 있으며, 이이 같이 스마트 차량 운전자의 프라이버시를 침해할 수 있다. 이를 해결하기 위해 수집된 정보를 가공하고, 상황에 따라 다른 차량이나 인프라에 제공해야 할지에 대한 여부, 즉 사용자 프라이버시에 대한 정책적인 결정이 필요하다.

3. C-ITS 보안 기술 및 표준화

3.1 물리적 보안 기술

스마트 교통시스템에 공격자가 물리적으로 직접 접근하여 데이터 유출 및 불법 펌웨어 업데이트 등의 위협이 발생시킬 수 있다[7]. 이와 같이 물리적으로 접근이 가능한 입력 및 출력 포트를 차단 후 불법적인 접근을 차단할 수 있다. 그 외에 물리적으로 접근하는 것을 해결하기 위해 스마트교통 시스템 및 서비스에 따라 다음과 같은 보안 대안을 선별하고, 적용해야 한다[표 3 참고].

- **외부 입출력 포트 비활성화**: USB와 같이 외부에 노출된 포트를 이용하여 펌웨어 및 주요

데이터에 접근할 수 없도록 해야 한다. 필요한 경우 인증 절차 기능을 제공하여, 비인가된 접속을 방지해야 한다.

- **내부 입출력 포트 비활성화**: UART을 제품 소스 코드에서 비활성화를 설정해야한다. 또한 JTAG에서 IC업체에 제공하는 메모리 관련 보호 도구로써, 비활성화로 설정해야 한다. 즉, 비식별을 위해 포트 식별 난독화을 적용하고, 비인가된 접속을 방지하기 위한 사용자 인증을 제공해야 한다.
- **외부 조작 검증 및 탐지 방지 메커니즘**: 조작 방지 솔루션을 활용하여, 비인가 조작을 탐지한다. 비인가 조작 탐지 시 민감한 데이터 및 주요한 키의 초기화를 수행해야 한다. 만약 초기화가 어려울 경우, 제품을 비활성화 해야 한다.
- **OBD-Ⅱ 포트 악용 방지 메커니즘 추가**: 진단 및 유지보수를 위하여 OBD-Ⅱ 포트를 통해 차량에 접속할 때, 악의적 메시지 전송 및 펌웨어 변조 등의 방지를 위한 네트워크 세분화 및 인증 메커니즘을 통한 메인 시스템 보호 등의 방지 대안을 제공해야 한다.

3.2 소프트웨어 보안 기술

스마트 교통 시스템은 소프트웨어를 기반으로 사용자와 차량에게 다양한 서비스를 제공한다. 소프트웨어 설계 관리시 보안을 중점적으로 고려해야 하며, 체계적인 사후관리를 진행하고 소프트웨어를 안전하게 개발해야 한다. 이를 해결하기 위해 C-ITS 및 서비스에 따라 다음 주요 보안 대책을 선별하여 적용해야 한다[표 4 참고].

- **시큐어 코딩**: 차량 내 소프트웨어 및 펌웨어 개발 시 보안 취약점을 최소화하기 위해 소

표 3. 물리적 보안 적용범위
Table 3. Physical Security Coverage

적용되는 보안 권고사항	인포테인먼트	통신	진단유지보수	기본·차체	V2V	V2I	V2N
1. 외부 입출력 포트 비활성화	○	○		○	○	○	○
2. 내부 입출력 포트 비활성화	○	○		○	○	○	○
3. 외부 조작 확인 및 분해방지 매커니즘	○	○		○	○	○	○
4. OBD-Ⅱ 포트 악용 방지 메커니즘 추가			○				

표 4. 소프트웨어 보안 적용범위
Table 4. Software Security Coverage

적용되는 보안 권고사항	인포테인먼트	통신	진단유지보수	기본·차체	V2V	V2I	V2N
1. 시큐어 코딩	○	○	○	○	○	○	○
2. 불필요한 서비스 비활성화	○	○	○	○	○	○	○
3. 배포 전 소프트웨어 검증	○	○	○	○	○	○	○
4. 펌웨어 관리	○	○	○	○	○	○	○

프트웨어 개발 생명주기(SDLC)의 단계별 보안을 고려 후 안전하게 개발해야 하며, MISRA C, CERT C 등의 시큐어 코딩 가이드를 참고한다. 소프트웨어 개발 단계별 보안 요구사항으로 먼저 요구사항 분석 설계 구현 테스트 유지보수, 두번째는 요구사항 중 보안 항목 식별, 세번째는 요구사항 명세서, 네번째는 위협원 도출을 위한 위협모델링, 다섯번째는 보안설계 검토 및 보안 설계서 작성, 여섯번째는 보안통제 수립, 일곱번째는 표준 코딩 정의서 및 SW 개발 보안가이드를 준수하여 개발, 마지막 여덟번째로 소스코드 보안 취약점 진단 및 개선 등 존재한다. 시큐어 코딩 관련 표준은 소프트웨어 라이프 사이클 프로세스와 관련된 ISO 12207, 정보보안 관리와 관련된 ISO 27001, 정보보안 기술와 관련된 ISO 27002, 소프트웨어 테스팅 표준와 관련된 ISO 29119 등이 존재하며, 이에 대한 세부적인 사항은 소프트웨어 개발 보안 가이드를 참고하면 된다[8].

표 5. 보안 테스트에 사용되는 도구 툴
Table 5. Tools used for security testing

1) Static Code Analyzer
2) Dynamic Code Analyzer
3) Fuzzer
4) Hardware Debugger
5) Known Answer Tester
6) Application Tester
7) Vulnerability Scanner
8) Exploit Tester

- **불필요한 서비스 비활성화**: 소프트웨어 알고리즘이 복잡할수록 버그가 발생할 확률은 높다. 이에, 불필요한 서비스는 비활성화 설정을 해야 한다. 만약 소프트웨어 버그가 존재할시, 보안 패치 적용 전 외부 접속 포트과 같은 서비스 비활성화를 디폴트 값으로 설정해야 한다. 외부 접속 포트 사용이 필요 시 비밀번호 설정·적용 등과 같은 인증 절차를 수행해야 한다.
- **펌웨어 관리**: 소프트웨어 버그를 탐지 시 최신 보안 패치를 신속하게 적용하고 체계적 업데이트를 진행해야 한다. 그리고 펌웨어의 위조, 변조 및 무결성 보장을 위해 안전한 디지털 전자서명을 적용해야 한다. 또한, 펌웨어 업데이트를 위해서 서버와 통신 시 서버 인증서의 진위를 검증하여 통신해야 한다. 이때 펌웨어 파일의 중요정보를 선별 후 암호화 및 난독화를 적용해야 한다.
- **보안 테스트 도구의 툴**: 보안 테스트에 사용되는 소프트웨어 기반의 도구들을 사용하여, 보안 위협에 노출되었는지를 테스트를 통해 확인할 수 있다. 보안 테스트에 사용되는 도구의 툴은 다음과 같다.

3.3 주요 표준화 동향

다양한 IoT 기반 융합 서비스들 가운데 스마트 카를 중심으로 한 C-ITS 관련 분야가 많은 관심을 받고 있다. 이에 이동통신사, 자동차 제조사 등 산업체 및 통신 분야의 표준을 책정하는 기구들은 대표적으로 ITU-T(International Telecommunication Union Telecommunication Standardization Sector), ISO(International Organization for Standardization), ETSI (European Telecommunications Standards Institute) 등이 존재한다[9]. 표 6은 자율주행차 국가표준활용 가이드라인에 표기된 자율주행 표준화 항목 및 기구를 나타낸 표이다[10].

표 6. 자율주행 표준화 항목 및 기구
Table 6. Autonomous driving standardization items and organizations

표준항목	기술위원회 및 작업반
고속도로 자율주행, 자율주행 자동차 서비스, 자율주행 셔틀 서비스 등	ISO TC204 WG14 ISO TC204 WG19
자율주행 지도 데이터베이스 동적데이터 저장소(LDM)	ISO TC204 WG3
차량용 이더넷, Extended Vehicle 센서 시맨틱 인터페이스	ISO TC22 SC31 WG3, WG6, WG9
V2X 통신 협력형 ITS 서비스	IEEE, 3GPP ISO TC204 WG16, WG18
운전자제어권 전환	ISO TC22 SC39
기능안전, SOTIF 사이버보안	ISO TC22 SC32
시나리오 기반 시험 방법	ISO TC22 SC33
강화학습, AI, 클라우드 및 엣지 컴퓨팅	ITU-T, ISO/IEC JTC1 SC38

이 외에도 다양한 기구에서도 C-ITS 관련기술에 대한 표준화 제정 또한 무수히 진행되고 있다. 각 개체 간의 상호인증 기술, 보안 통신 기술, 해킹 방지 기술 등이 포함된다[11].

만일, 보안이 제대로 보장되지 않으면 보안 사고 및 도로 안전정보 위조 및 변조를, 신호제어 등을 통하여 도로 안전 사고로 확산이 될 가능성이 있다. 따라서, 차세대 지능형 교통 시스템에 표준화 및 보안 관련 기술에 대한 연구가 필요하다.

- **X.itssec**: ECU, 네비게이션 시스템과 전기 요금 징수 ETC 시스템 같은 차량 내부의 발전으로 지능형 교통 시스템 환경에서 V2I, V2V로 다른 개체와 통신하는 것이 일반적이다. 그러나, 기기(디바이스)는 인터넷을 통해 소프트웨어 모듈을 자동 업데이트하는 방식이다. 이에, 공격자가 업데이트 서버로 가장하고 공격하는 방식 등의 업데이트 서버 및 장치에 대한 사이버 공격의 위험성이 높다. 위와 같은 위협으로 차량 오작동이 사고를 일으킬 수 있으며, 차량 소프트웨어 보안이 필수적으로 요구된다. 만일 V2X 통신 Ad-Hoc 네트워크에서 특성상 취약점을 발견한다면 다른 차량으로 전달되어 영향이 미치므로 이에 대한 대안이 필요하다. 2015년 4월 ITU-T 정보보호연구반에서는 ITS 통신 장비를 위한 보안 소프트웨어 업데이트 기능인 X.itssec-1와 V2X 통신 시스템에 대한 보안 지침인 X.itssec-2를 신규 표준화 과제로 채택하여 개발하였다. 2020년 8월 Q13 표준화 과제 현황에서 X.itssec-3에서 블루투스 및 차량진단 포트를 통하여 차량에 접속하는 다바이스에 대한 보안이 다루어진다. 특히 차량 내부망 보안을 위해서 X.itssec-4에서 차량용 침입탐지 시스템 방법론이 개발되고 있다. 그리고 보안관리 서버, 교통관제 서버 등 인프라 및 클라우드에 연관된 보안 표준화는 X.itssec-5, X.mdcv, X.fstiscv 등에서 다루고 있다[12].
- **ETSI TC ITSETSI TC ITS(Technical Committee Intelligent Transport Systems)**: ETSI TC는 미래 스마트 교통 시스템 환경에서 정보통신 기술을 사용하기 위한 표준화 기준 생성과 유지보수하는 기관이다. 그리고 대기오염 물질 배출 감소 및 교통사고, 교통의 효율성을 우선순위로 C-ITS 무선 통신 표준화를 진행 중이다. 또한, 차량, 도로, 센터 등의 ITS 장비 간의 상호호환성 확보를 기반으로 하는 C-ITS 표준화가 추진되고 있다. 추가적으로, C-ITS 관련 표준 개발 기구(CEN, IEEE, SAE 등)에서도 적극적인 참여로 인하여 글로벌 ITS 서비스 제공을 위한 연구가 진행 중이다. 표 7은 ETSI ITS 보안 표준을 나타낸 표이다.

표 7. ETSI ITS 보안 표준
Table 7. C-ITS ETSI ITS Security Standard

표준번호	표준명
ETSI TR 102 893 V1.1.1	Threat, Vulnerability and Risk Analysis (TVRA)
ETSI TS 102 867 V1.1.1	Stage 3 mapping for IEEE 1609.2
ETSI TS 102 943 V1.1.1	Confidentiality services
ETSI TS 102 941 V1.1.1	Trust and Privacy Management
ETSI TS 102 942 V1.1.1	Access Control
ETSI TS 102 940 V1.1.1	ITS communications security architecture and security management
ETSI TS 103 097 V1.1.1	Security header and certificate formats
ETSI TS 103 096-1 V1.1.1	Test requirements and Protocol Implementation Conformance Statement
ETSI TS 103 096-2 V1.1.1	Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 103 096-3 V1.1.1	Abstract Test Suite (ATS) and Protocal Implementation on eXtra Information for testing
ETSI TS 103 096-4 V1.1.1	Validation report

4. 국내 · 외 C-ITS 보안 기술 동향

4.1 국외 C-ITS 보안 관련 동향

- **미국**: 미국 교통부가 세운 ITS 관련 전략 주제는 5개 ITS 전략 주제 (ITS Strategic Plan, US DoT)이다. 첫 번째로 도로 및 차량 안전성 향상을 위해 자율주행 기술 개발 및 커넥티드 카(Connected Car), 돌발 상황 관리 시스템 기술 개발, 두 번째는 이동성 향상을 위해 돌발 상황, 도로 기상 및 대중교통 관리 등 관리하는 시스템 기술을 개발, 세 번째는 정체구간 우회, 교통 개선 등과 같은 환경적 요인을 최소화하는 기술 개발, 네 번째는 ITS의 혁신 촉진을 위해 새로운 시스템의 교통 기술을 개발, 마지막으로 교통 시스템의 정보 공유를 지원함으로써 차량과 인프라, 차량과 차량 및 차량과 디바이스 사이의 정보 공유 활동을 지원한다.

  미국은 지속적으로 이동성, 안전성 및 환경적 측면에서의 교통 문제를 해결하기 위한 연구 개발 및 실사용 프로젝트를 추진해왔다. 미국 교통부는 'ITS Strategic Plan 2020-2025' 발표를 통해 향후 5년동안 ITS 관련 연구 우선순위, 프로그램 종류, 전략주제, 연구방향 및 목표 등을 공개하였다. 이러한 전략 주제에 따른 프로그램을 다음과 같이 구성하였다. 먼저 커넥티드 카 차량 및 도로에 따라서 스스로 상황에 맞게 제어하는 기술인 자동화(Automation), 두 번째, C-ITS 기술 발전에 따라 생산될 잠재력 있는 신흥 기술(Emerging Capabilities), 세 번째, 데이터 수집 및 저장, 네 번째, 데이터 공유를 활용하는 대규모 데이터(Enterprise Data), 다섯 번째, 인프라와 시스템 및 장치와의 연결 강화 향상을 위한 상호운용성(Interoperability), 마지막으로 여섯 번째, 새로운 기술 도입에 따른 보급 문제를 해결할 수 있는 보급 가속화(Accelerating Deployment)로 프로그램을

구성하였다[13].

- **유럽**: 유럽에서 기존 C-ITS 구현을 위한 기술들과 관련해 많은 연구 및 개발되었지만 도로 인프라와 자동차에 통신 인프라가 설치돼야 하는 특징으로 실제 서비스가 제공되기 어려웠다. 유럽의 C-ITS Corridor 프로젝트는 이를 해결하기 위해 유럽의 C-ITS 암스테르담 그룹은 단계적 C-ITS 구축 방안을 제시했다. 먼저 차량 단말기 보급률을 기준으로 보급률이 낮은 상황에서도 특정 위험지역 경고 등과 같이 실현 가능한 단순한 서비스들을 정의하였다. 두 번째로, 도로 인프라 구축 및 차량 단말기 보급률을 통한 충돌 위험 경고 등과 같이 실현 가능한 서비스들을 구축하였다. 세 번째로, 모든 도로와 차량에 C-ITS 인프라를 구축하여 최적의 C-ITS 서비스를 개발하는 것을 정의하였다.

  현재 독일, 오스트리아 및 네덜란드는 각각 프랑크푸르트, 로테르담 및 비엔나를 연결하는 도로에 3개국 자동차 회사들 및 교통부가 협업하여 'C-ITS Corridor' 프로젝트를 수행하고 있다. 유럽에서 진행되는 'C-ITS Corridor' 프로젝트는 C-ITS 사업 중 하나로 대규모의 실구축 C-ITS에 대한 테스트 및 평가 등 측면에서 중요성을 가진다. 추가적으로, 독일은 자동차 회사를 중심으로 SIM-TD, DRIVE C2X 등의 프로젝트를 추진 중이다.
- **일본**: 일본은 과거 IT 전략본부 그룹인 국토교통성, 총무성, 경찰청, 경제 산업성이 'ITS SPOT' 프로젝트를 추진하여, 2020년까지 전국 주요 도로 교통 정체를 10년 대비 절반으로 줄이고자 하였다. 'ITS SPOT' 서비스는 도로와 차량 인프라에 설치된 'ITS SPOT'가 통신하여 실시간으로 교통정보 등과 같은 서비스를 제공받는 것을 의미한다. 현재 일본 지역 간 도시고속도로 및 고속도로에 약 1,600개의 노변장치를 설치하여 통행료 징수, 안전 운전지원, 경로안내 서비스를 제공한다. 그리고 일본은 차량 간의 서비스보다 인프라 측면을 중점적으로 연구하고 있으며, 운전의 편리성과 차량의 안전성을 높이는 방향으로 추진하고 있다[14].

4.2 국내 C-ITS 보안 관련 동향

한국도로공사에서는 지난 2007년 첨단도로기술의 도입을 위해 스마트하이웨이 R&D사업을 시작하였다. 그리고, 차세대 ITS 시범사업을 진행하였고 자율 협력 주행 도로 시스템 개발 및 시범사업을 추진하고 있다. 스마트하이웨이 사업은 2006년 건설교통 R&D 혁신로드맵 수립에 따라 세계적 수준의 지능형 고속도로 구현을 목표로 미래 유망 기술 중점추진 10개 프로젝트(VC-10) 중 하나를 추진한 사업이다[15]. 이를 위해 한국도로공사에서는 2007년 '스마트하이웨이사업단'을 출범하였으며, 주로 도로, 자동차, 통신 분야와 이를 통합해 결과를 검증하는 테스트베드를 설계 및 구축, 운영하는 과제로 구성하였다. '스마트하이웨이' 사업의 목적은 국토교통부가 2020년까지 '지속가능한 지능형 교통체계의 성장으로 생활형에서의 스마트 도로교통 구현'을 목표하였다. 즉, 고속도로에서의 사고 발생률을 줄이며 편리한 고속도로 이용을 위한 자동차 기술 및 첨단 IT를 융·복합하여 도로의 문제점 해결한다. 대표적인 기술은 다음과 같다. 먼저 고속주행 환경에서 정차하지 않고 자동 요금 정산이 가능한 '스마트 톨링 시스템', 두 번째로, 결빙, 낙하물 등 돌발 상황 발생 시 이를 탐지해 운전자에게 알려주는 '도로정보검지 레이더 시스템' 등이 존재한다. 스마트하이웨이사업의 성공적 마무리로 기술을 개발한 연구기관에서 현재 활발한 상용화가 이루어 지고 있다. 2015년 개최된 서울

세계도로대회에서는 현장 시찰(Technical Visit) 장소로 선정돼 36개국 약 100명을 대상으로 스마트하이웨이 기술을 선보였다. 이와 동시에 자율협력주행 스마트하이웨이 확산과 더불어 기반이 되는 기술들, 또는 관련된 C-ITS 시범사업을 추진 중이다. 2021년에는 과기부와 KISA에서 자율자행차 보안요구사항 및 보안모델에 대한 내용이 포함된 보고서가 제시되었으며[16], 2022년에는 ISO/TC 204(지능형 교통 시스템) 분야의 국가 11종을 중심으로 한 자율주행차 국가표준활용 가이드라인이 제시되었다. 향후 C-ITS 관련된 사업 추진을 위해 기술 표준화, 인증기준 마련 및 법·제도 정비를 추진해야 한다.

5. 결 론

최근 도로시설문과 차량 간의 양방향 통신을 이용하여 사고를 예방하고자 하는 연구가 진행되고 있으며, 이를 차세대 지능형 교통 체계(C-ITS)라 말한다. C-ITS는 차량, 도로, 보행자, 그리고 운전자 간의 통신 연결되어 차량이 주행하면서 다른 차량(V2V) 및 도로 인프라(V2I)와 끊임없이 통신하며 다양한 교통서비스에 관한 정보를 전달 및 공유가 가능하다.

그러나, C-ITS를 완벽하게 구현하기 위해서는 교통 정보의 공유가 실시간으로 이루어져야 한다. 그러나, 현재 기술로는 다양한 한계점이 존재한다. 국내 C-ITS 통신, 자동차, 교통 분야 및 관련 분야 산업체 등의 관련 종사자들은 우선적으로, 전 세계적으로 개발 중인 다양한 표준 및 서비스, 보안 모델 및 가이드라인 등을 분석해야한다. 그리고 분석된 자료를 기반으로, 국내 C-ITS 환경에 특화된 보안 모델 도출 및 가이드라인을 제시해야한다. C-ITS 관련 종사자들은 이를 참고하여, C-ITS 환경에서 발생할 수 있는 보안위협을 해결할 수 있는 보안 기술(SW/HW)들에 대한 연구를 수행해야 한다. 추가적으로, 연구한 C-ITS 모델을 실증 도시지역이나 스마트시티에 안정적으로 도입하기 위해서는 기존 시스템과의 연계 구축 방안 마련 및 단말기 보급과 더불어 사업지역의 특성에 맞는 서비스 구축 개발이 필요하다.

C-ITS의 발전은 사회비용 감소 및 고질적인 교통 문제들이 해결될수 있기에 전세계적으로 C-ITS에 대한 내용(관련 기술 및 표준) 등에 관심을 가지고 있다. 하지만 관련 기술과 더불어 중요한 것은 보안 기술이다. C-ITS 보안에 대한 기술 연구 및 발전·투자로 C-ITS 보안분야에 대한 기술의 우위를 선점하는 것이 중요하다.

본 연구 논문은 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음 [20ZR1300, TDC 원천기술개발 데이터 커넥팅 기술연구]

참 고 문 헌

[1] INNOPOLIS. Global Automotive Cyber Security Market Forecast. (2018). Frost & Sullivan, Global Automotive. Cybersecurity Market, Forecast to 2025. https://www.innopolis.or.kr

[2] T. H. Kim. et al. A Study on Smart City Transportation System Establishment Strategy and Implementation Project. (2018). KOTI. https://www.koti.re.kr

[3] C. M. Na. et al. Cooperative-Intelligent Transportation System (C-ITS) Technology Trends. (2022). ITFIND. https://www.koita.or.kr

[4] J. H. Jeong. et al. Major Security Issues in Smart Car and Cooperative-Intelligent

Transportation System (C-ITS) Environment. Korea Multimedia Society, 19(2), 35-40. (2015). pISSN : 1229-778X
[5] D. Y. Kim. et al. Threat Analysis and Security Reinforcement Schemes for Automotive Security Systems. The Magazine of the IEIE, 40(5), 68-79. (2013). ISSN : 1016-9288
[6] G. J. Yun., et al. Security Technology Status and Development Direction of Automotive Convergence Information and Communication Devices. Review of KIISC, 24(4), 21-27. (2014). pISSN : 1598-3978
[7] KISA. Smart Transportation Cyber Security Guide. IoT Security Alliance. (2018). https://www.kisa.or.kr
[8] KISA. Software Development Security Guide. (2021). https://www.kisa.or.kr/
[9] S. W. Ahn, The Realization of Connected Cars and Intelligent Transportation System. (2017). Software Policy & Research Institute. https://spri.kr/
[10] KSAE. Guidelines for the use of national standards for autonomous vehicles. (2022). The Korean Society Automotive Engineers. https://www.ksae.org
[11] S. M. Park. et al. Current status of Coorperative Intelligent Transportation System (C-ITS) at Domestic and Foreign and Major Security Standardization Trends. Review of KIISC, 25(5), 53-59. (2015). pISSN : 1598-3978
[12] ITU-T SG17 draft Recommendation. X.itssec-3, Security requirements for vehicle accessible external devices. (2020). https://www.itu.int/
[13] J. H. Jang. Roadmap between Automotive Industry and Infrastructure Organisations on Initial Deployment of Cooperative ITS in Europe. (2015). Korea Agency for Infrastructure Technology Advancement, Global Report. https://www.kaia.re.kr
[14] ITS Japan. Mobile and ITS Spot cooperative Service. (2013). https://www.its-jp.org/
[15] K. P. Kang. et al. C-ITS-based Smart Roads. (2020). Autonomous Cooperative Driving, and Local Win-Win Projects, KOTI. https://www.dbpia.co.kr/
[16] Convergence Security Policy Team. Autonomous car service security model. (2021). KISA and Ministry of science and ICT. https://www.kisa.or.kr/

저 자 소 개

서대희(Daehee Seo)

2006.2 순천향대학교 전산학과 박사
2015.3 한국전자통신연구원 선임연구원
2020.5 Kennesaw State University 연구원
2020.9-현재 : 상명대학교 조교수
<주관심분야> 정보보호, 암호 프로토콜, 유무선 네트워크, 클라우드 보안