Journal of KIIT. Vol. 23, No. 5, pp. 129-137, May 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.5.129

차세대 전기차 통신 프로토콜 ISO 15118-20의 추가 기능 및 한계점에 대한 연구

김종훈*, 김동완**

Study on Additional Feature and Limitations for the Next-Generation Electric Vehicle Communication Protocol ISO 15118-20

JongHoon Kim*, Dongwan Kim**

이 연구는 2024년도 산업통상자원부 및 산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임(RS-2024-00409722)

요 약

EV 시장의 성장과 함께 EV와 충전소 간 효율적인 충전을 위한 통신 프로토콜 표준에 대한 수요가 증가하고 있다. ISO 15118-1은 EV와 충전 인프라 간의 통신을 표준화한 ISO 15118 파트의 첫 번째 표준이며, 이를 기반으로 HomePlug GreenPHY 기반 유선 통신, Plug & Charge(PnC) 기능 및 TLS 1.2 보안을 지원하는 ISO 15118-2로 확장되었다. 그러나 ISO 15118-2는 단방향 통신만 지원하여 충전 속도 향상 및 효율적인 에너지 관리에 한계가 있다. 이러한 문제를 해결하기 위해 EV와 충전소 간의 양방향 통신을 지원하는 ISO 15118-20이 제정되었다. 본 논문에서는 EV 충전 표준인 ISO 15118-20을 다룬다. 먼저 ISO 15118-2에서 지원하는 기본 기능을 살펴보고, 이후 ISO 15118-20의 추가 기능과 한계를 분석하며, 이를 개선하기 위한 연구 방향을 제시한다.

Abstract

With the growth of the EV market, demand is rising for protocols that enable efficient charging between EVs and charging stations. ISO 15118-1 standardizes the communication between EVs and the charging infrastructure, and ISO 15118-2 builds on it by supporting HomePlug GreenPHY-based wired communication, Plug & Charge (PnC), and TLS 1.2 security. However, its unidirectional communication limits charging speed and energy management. To overcome these issues, ISO 15118-20 was introduced to support bidirectional communication. This paper reviews the basic functions of ISO 15118-2, examines the new features and limitations of ISO 15118-20, and suggests future research directions.

Keywords
ISO 15118-20, TLS, handshake, wireless attack

* 동아대학교 전자공학과 석사과정
- ORCID: https://orcid.org/0009-0006-8122-5595
** 동아대학교 전자공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-2779-9858

· Received: Apr. 03, 2025, Revised: Apr. 28, 2025, Accepted: May 01, 2025
· Corresponding Author: Dongwan Kim
Dept. of Electronic Engineering, Dong-A University, Busan, Korea
Tel.: +82-51-200-7708, Email: dongwankim@dau.ac.kr

Ⅰ. 서 론

자동차 배출가스에 대한 국제적인 환경 규제 강화, 석유 자원의 고갈 가능성 증가, 고유가 지속 등의 원인으로 내연기관 자동차에서 전기자동차(EV, Electric Vehicle)로 세계 자동차 시장이 전환되고 있다. EV는 온실가스 감소에 효과적이며, 미래에 환경을 보호하고 자원을 효율적으로 사용하는 지속 가능한 환경을 구축하기 위한 핵심 방안으로 자리 잡고 있다. 또한, 주요국은 EV 구매 보조금 지원, 세제 혜택, 주차 및 충전 편의성 확충 등 다양한 지원책을 시행함으로써 EV 시장이 지속적으로 성장하고 있다. EV 판매량은 약 3,000만 대를 넘어서고, 2040년에는 연간 7,300만 대에 이를 것으로 예상된다[1]-[3].

자동차 시장이 EV 시장으로 전환됨에 따라 충전 인프라에 대한 기술 연구도 급속히 발전하고 있다. 다양한 충전 인프라 간의 상호 운용성과 유연성을 고려하여 충전 인프라 표준이 제정되고 있다. EV와 충전소(EVSE, Electric Vehicle Supply Equipment) 간의 안정적이고 효율적인 통신을 위해 개발된 국제 표준으로 ISO 15118-1 표준이 제정되었다. ISO 15118-1은 EV와 EVSE 간의 각종 통신 프로토콜을 정의하고 있으며, 이를 기반으로 확장된 ISO 15118-2는 유선망을 통한 단방향 통신 프로토콜을 정의한다. 그러나, ISO 15118-2는 유선 통신에만 한정되어 있어, EV와 EVSE 간의 실시간 양방향 데이터 전송에 제약이 발생한다. 또한, ISO 15118-2에서 채택된 TLS 1.2 보안 프로토콜은 복잡한 핸드셰이크 과정으로 통신 지연이 발생한다. 게다가, RC4와 같이 취약한 암호화 알고리즘의 사용으로 인해 다양한 공격에 노출될 위험이 있다. 더불어, 유선망 기반 통신으로 무선 및 자동 연결이 불가능하다는 한계를 가진다.

이러한 문제를 해결하기 위해 2022년에 ISO 15118‐20이 발표되었다. ISO 15118‐20은 기존 단방향 통신의 한계를 보완하여 양방향 통신을 지원하고, TLS 1.3 기반 인증으로 보안을 강화하며, 동적 충전 제어를 가능하게 하였다. 이를 통해 무선 충전(WPT, Wireless Power Transfer), 양방향 에너지 전송(BPT, Bidirectional Power Transfer) 및 자동 연결 장치(ACD, Automatic Connection Device) 등을 지원하는 개선된 기능을 제공한다.

그러나 개선된 ISO 15118‐20도 한계점을 가지고 있다. 다중 사용자 환경에서의 문제, 다양한 인증 및 보안상의 취약점으로 인한 외부 공격 위험, 무선 인증의 한계 등이 존재한다. 이를 개선하기 위해 TPM 2.0 기반 KAP(Key Authorization Policy) 도입, Attestation 메시지 추가 등의 방안이 제안되고 있다. 본 논문에서는 ISO 15118‐20의 개선된 기능을 다루고, 나아가 현재 ISO 15118‐20의 한계점을 해결하기 위해 제안된 기술들을 분석한다.

Ⅱ. ISO 15118‐2

ISO 15118‐2는 EV와 EVSE 간의 통신을 위한 ISO 15118-1에서 확장된 표준으로서, EV와 EVSE 간에 필요한 Open Systems Interconnection(OSI) 모델의 3 계층(네트워크 계층)부터 7 계층(애플리케이션 계층)까지의 프로토콜을 정의한다. 이는 EV 통신 컨트롤러(EVCC, EV Communication Controller)와 충전소 통신 컨트롤러(SECC, Supply Equipment Communication Controller) 간의 IP 기반 통신을 전제로 하며, EV와 EVSE 간 충전 과정에서 발생하는 다양한 데이터를 주고받을 수 있도록 정의되었다[4].

ISO 15118‐2는 다음과 같은 기능을 정의한다.

·보안 기능 지원: TLS, 인증서 및 키 관리 등의 방법으로 EV와 EVSE 간 전송되는 데이터를 보호한다. ISO 15118‐2는 TLS 1.2를 기반으로 보안을 수행하며, TLS 핸드셰이크 과정에서 인증서와 키 교환을 통해 신뢰성을 확보하고 암호화된 데이터를 인증한다. 또한, 인증서를 사용하여 EV와 EVSE 간 상호 인증을 수행하고, 암호화 키를 사용하여 데이터를 암호화한다. 그러나 TLS 1.2 기반 보안 방식은 여러 RTT(Round Trip Time)이 필요하여 통신 지연이 발생하며, 단일 바이트 편향이 많아 공격자가 쉽게 공격할 수 있는 RC4와 같은 취약한 암호화 알고리즘으로 외부 공격에 취약하다는 한계가 있다.

·HomePlug GreenPHY 지원: HomePlug GreenPHY는 스마트 그리드와 전기차 충전 인프라를 위한 전력선 통신(PLC, Power Line Communication) 프로토콜이다.

ISO 15118-2에서 Home- Plug GreenPHY를 지원함으로써, 별도의 통신 케이블 없이 데이터 전송이 가능해졌다. 이 기술은 OFDM(Orthogonal Frequency Division Multi-plexting)을 활용해 2~30MHz의 낮은 대역에서 통신이 가능하다. 이를 통해 빠른 응답 속도를 특징으로 원활한 데이터 교환 및 충전제어가 가능했다. 그러나, 케이블 길이 제한, 노이즈에 대한 취약성, 단방향 충전 제한 등의 한계점이 존재한다.

·EXI(Efficient XML Interchange) 지원: EXI 방식은 XML 데이터를 이진 형식으로 압축하는 기술로, 네트워크 대역폭 활용과 전송 속도를 개선한다. 이 기술은 W3C 표준에 따라 라이센스 부담 없이 사용 가능하며, 기존 XML의 텍스트 기반 포맷과 문서 구조를 유지하여 높은 호환성을 제공한다. 또한, XML 메시지를 바이너리 수준에서 처리함으로써 데이터 처리 속도를 향상시키고 메모리 사용량을 감소시킨다. 단순한 문법 기반의 인코딩 방식을 적용하여 동등한 XML 문서 대비 최대 100배까지 데이터 크기를 줄일 수 있다.

·PnC(Plug and Charge) 지원: PnC는 EV와 EVSE 간의 자동화된 인증 및 결제 시스템을 제공하는 기능이다. 이는 EV와 EVSE가 직접 통신하여 사용자 개입 없이 충전 절차를 진행할 수 있다. 이 기능은 차량에 저장된 인증서를 통해 인증이 이루어지며, 이를 기반으로 사용자의 신원을 확인하고 결제를 처리한다. 이 방식은 PKI(Public Key Infrastructure)를 사용하여 안전하고 자동화된 상호작용을 구축하여 데이터 무결성을 보장하고 사기를 방지한다.

ISO 15118‐2는 EV와 EVSE 간 통신을 위한 필수적인 프로토콜을 제공하여 효율적인 EV 충전에 기여했지만, TLS 1.2 기반 보안의 취약성, 유선망 기반 통신의 한계점 등 여러 문제점을 내재하고 있다. 이러한 문제점을 해결하기 위해 ISO 15118‐20의 제정이 추진되었다.

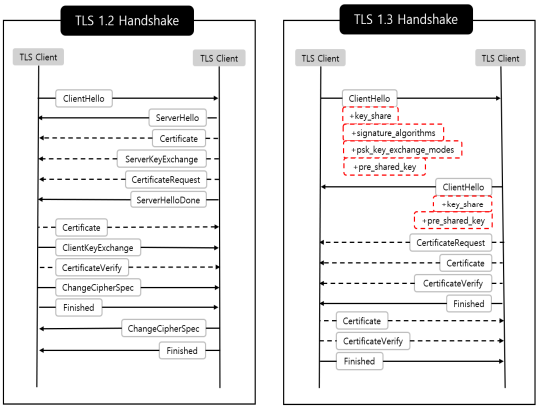
III. ISO 15118-20

ISO 15118‐20은 ISO 15118‐2의 업데이트 버전으로서, 기존 버전의 한계점을 극복하고 다음과 같은 개선된 기능들을 정의한다[5][6].

3.1 기존 보안에서 강화하기 위해 개선된 기능

·강화된 보안 기능 지원: ISO 15118‐20은 TLS 1.3을 도입하여 보안을 강화하였다. 이를 통해 핸드셰이크 과정을 단축시켜 RTT를 2회에서 1회(접속 이력이 있는 경우 0회)로 줄임으로써 통신 지연을 최소화하였고, 취약한 알고리즘을 제거하고, AEAD 암호화를 도입하여 보안을 강화하였다[7]. 또한, 인증서 발급 및 갱신 과정을 자동화하여 인증서를 체계적으로 관리할 수 있게 되어, 인증서의 신뢰성을 지속적으로 보장할 수 있다.

그림 1의 (a)는 TLS 1.2 핸드셰이크 과정을 보여주고, (b)는 TLS 1.3 핸드셰이크 과정을 보여준다. TLS 1.2는 키 교환이 바로 이루어지지 않고 순차적으로 이루어져 RTT가 2회가 소요된다. 그러나, TLS 1.3은 Key_share를 추가하여 즉시 응답을 가능하게 키 교환을 병렬화하였고, 이로 인해 RTT가 1회로 줄어 통신 지연을 최소화할 수 있다.



(a) TLS 1.2 핸드셰이크 (a) TLS 1.2 handshake

(b) TLS 1.3 핸드셰이크 (b) TLS 1.3 handshake

그림 1. TLS 1.2 와 TLS 1.3의 핸드셰이크[8]
Fig. 1. Handshake of TLS 1.2 and TLS 1.3[8]

·강화된 보안 메시지 포맷 지원: ISO 15118‐2의 메시지 포맷은 IP, UDP 및 TCP, V2GTP, EXI, V2G Message 순으로 구성되며, TLS는 필수가 아니어서 인증 모드에 따라 보안 수준이 달라진다. 반면, ISO 15118‐20은 TLS 포맷을 추가하여 TLS 1.3 암호화를 의무적으로 사용함으로써 보안 취약점을 보완하였다.

그림 2는 ISO 15118-20에서 TLS를 의무적으로 사용하기 위해 메시지 포맷에 추가된 TLS 헤더를 보여준다. Content Type은 데이터의 유형을 나타내고, Protocol Version은 TLS의 버전을 의미하며, 0x0303은 TLS 1.2, 0x0304는 TLS 1.3을 나타낸다. Length는 데이터의 길이를 나타내며, TLS 1.3의 경우 암호화된 데이터 기준 최대 16,640바이트로 제한된다.

그림 2. 추가된 TLS 헤더
Fig. 2. Added TLS header

표 1은 TLS 헤더에서 사용되는 Content Type 값에 대해 보여준다.

표 1. 콘텐츠 유형
Table 1. Content type

Value	Description
0x00-0x13	unassigned
0x14	change_cipher_spec
0x15	alert
0x16	handshake
0x17	application_data
0x18	heartbeat
0x19	tls12_cid
0x1A	ACK
0x1B	return_routability_check
0x1C-0x1F	unassigned
0x20-0x3F	reserved
0x40-0xFF	unassigned

0x00-0x13, 0x1C-0x1F, 0x20- 0x3F 및 0x40-0xFF는 할당되지 않은 값으로, 이 값이 전송되는 TLS 1.3은 fatal_unexpected_message를 전송하며, 연결을 즉시 종료한다. change_cipher_ spec은 TLS 1.2 버전에서 암호화 전환 신호로 사용되었지만, TLS 1.3에서는 하위 호환성 목적으로만 사용된다. alert는 warning 및 fatal 메시지를 전달하는 데 사용되며, TLS 1.3에서는 모든 alert 메시지를 암호화하여 전송한다. handshake는 TLS 연결 과정에서 협상 메시지를 전송할 때 사용되며, application_data는 암호화된 실제 애플리케이션 데이터 전송에 사용된다. heartbeat는 연결 상태 확인 프로토콜이지만, TLS 1.3에서는 취약성 때문에 비활성화되어 있다. tls12_cid는 TLS 1.2에서 CID(Connection ID)를 지원하기 위한 값으로 TLS 1.3에서는 사용되지 않는다. ACK은 Acknowledgement를 위해 사용되며, return_routability_check은 라우팅 가능성을 확인하는 데 사용된다.

3.2 ISO 15118-20에 추가된 기능

ISO 15118-20은 ISO 15118‐2에서 지원하지 않았던 새로운 기술들을 정의함으로써 충전 프로세스의 효율을 높였다.

ISO 15118‐20은 다음과 같은 새로운 기술을 정의한다.

·무선 통신 지원: ISO 15118‐2는 유선망 기반 통신만 지원하여 케이블 길이 제한, 노이즈 문제, 단방향 충전 등의 한계가 있었지만, ISO 15118‐20은 WLAN(IEEE 802.11n)을 적용하여 유선 통신뿐만 아니라 BPT, WPT, ACD 등 다양한 에너지 전송 방식을 확장하였다.

·ACD 지원: ACD는 운전자 개입 없이 자동으로 충전 연결 및 연결 해제 프로세스를 지원하는 기능으로, EV와 EVSE 간 물리적 연결을 자동으로 수행한다. ACD의 유형으로는 전기 버스와 같은 대중교통 차량에 팬터그래프를 통해 상부에서 정류장이나 차고지에서 자동으로 충전되는 ACDP(ACD Pantograph)가 있다. 또한, 차량 하부에서 연결되는 자동 연결 장치로 ACD-U(ACD-Underneath)가 있다. 이를 통해 대중교통, 상업용 및 자율주행 환경에서 충전 인프라의 효율성과 편의성을 크게 향상시킬 수 있다.

·WPT 지원: WPT는 자기 유도 및 자기 공명 방식으로 충전이 진행되며, ISO 15118-20은 이를 지원함으로써 EV와 EVSE 간의 물리적 충전 과정을 생략할 수 있다. 무선 충전 패드 위에 EV를 주차하면 자동으로 충전이 시작되며, ISO 15118- 20을 통해 차량의 위치 조정, 충전 전력 협상, 보안을 동시에 수행한다.

이 기술은 BPT와 결합하여 무선으로 V2G를 수행할 수 있고, 주행 중 무선 충전(Dynamic WPT)이 연구되고 있다. Dynamic WPT가 개발되면, 운전자의 편의성을 증가시키고, EV의 주행 거리 한계를 개선할 수 있을 것으로 보인다.

·BPT 지원: BPT는 EV와 전력망 간에 전력이 양방향으로 흐를 수 있게 하는 기능으로, EV의 배터리에 남는 에너지를 저장하거나, 전력망으로 반환하여 스마트 그리드와 통합을 지원한다. BPT는 V2G(Vehicle-to-Grid), V2H(Vehicle-to-Home), V2B (Vehicle-to-Building) 등 다양한 전력 흐름을 가능하게 함으로써, EV를 이동식 저장 시스템으로 활용할 수 있다. 이를 통해 전력 요금이 낮은 시간대에 충전하여 비용을 절감하고, 높은 시간대에 EV 배터리를 사용하여 피크 부하 절감 등을 가능하게 한다.

·효율적인 충전 제어 모드 지원: 기존 충전 제어 모드는 스케줄 모드로, EV와 EVSE는 ChargeParameterDiscoveryReq/Res 메시지와 교환된 정보를 기반으로 충전 전력을 협상한다. 이 모드에서는 전력, 전류 및 전압 각각의 최댓값, 에너지 요구사항, 출발 예정 시간 등을 통해 협상하여 충전한다. 이는 사전 협상으로 충전 과정이 고정되어 실시간 변화에 대응하기 어려웠다. 이를 해결하기 위해 ISO 15118-20은 동적 모드를 추가하여, 유동적으로 충전이 가능해졌다. 이 모드는 차량 자체가 아닌 외부 시스템에 의존하며, 추가된 DynamicParameter DiscoveryReq/Res 메시지를 통해 100ms 단위로 실시간 재협상을 한다. 이 메시지는 BPT Channel, EV 최대 방전 전력 및 그리드 제어 방식 등의 파라미터를 통해 협상한다.

ISO 15118‑20은 위와 같은 개선 기능과 추가 기능을 통해 EV 충전에 보안, 에너지, 운전자의 편의성 등의 다양한 이점을 가져왔다.

Ⅳ. ISO 15118‑20 한계점 및 제안된 기술

ISO 15118‑20은 ISO 15118‑2에 비해 WPT, BPT, ACD 등 다양한 추가 기능과 TLS 1.3을 도입하여 EV 충전에 효율성과 안정성을 크게 개선하였지만, 여전히 다음과 같은 한계점을 가지고 있으며, 이를 해결하기 위해 여러 기술이 제안되고 있다.

4.1 무선 통신 보안에 대한 제약

ISO 15118‑20은 WPT를 지원함으로써 유선망 기반 통신의 길이 및 노이즈 한계를 극복하고, WLAN 기반으로 빠른 데이터 전송과 실시간 데이터 교환이 가능하지만, Spoofing Messages나 DoS(Denial-of- Service) Attack 등 다음과 같은 외부 공격에 취약할 수 있다.

·Spoofing Messages: ISO 15118‑20은 암호화 프로토콜이 구현될 때까지, WLAN을 통한 모든 데이터는 일반 텍스트로 되어있다. 이는 공격자가 EV나 EVSE를 속이고 충전 종료나 EV가 실제로 필요한 전력보다 적게 공급하도록 메시지를 속여 통신을 방해할 수 있다.

·DoS 공격: 공격자가 Deauthentication 프레임을 위조하여 충전 세션을 강제로 끊는 Deauthentication 공격이나, 공격자가 노이즈를 이용하여 SNR(Signal-to-Noise Ratio)을 감소시켜 통신을 물리적으로 방해하는 Physical-Layer Jamming 등의 공격에 취약할 수 있다.

위 공격에 대응하기 위해 부족한 보안을 보완하기 위해 IEEE 802.11w 버전을 적용하는 방법이 제안되고 있다. 기존 IEEE 802.11n은 전송 속도에 집중되어 있기 때문에, 관리 프레임이 암호화나 인증 없이 전송되어 공격에 취약하였다. IEEE 802.11w는 WLAN의 보안을 강화하기 위해 개발된 보호 관리 프레임 표준으로, Deauthentication 프레임을 암호화 및 인증하여 공격자가 이를 조작하거나, 변조하지 못하도록 방지할 수 있다[9][10].

그림 3은 IEEE 802.11w의 Management MIC Information Element(MMIE)로 관리 프레임을 보호하기 위한 구조이다. Element ID는 MMIE를 식별하는 고윳값이 포함되어 있고, 0x4c로 정의된다. Length는 MMIE의 길이를 나타내며, Key ID는 무결성 검증에 사용되는 IGTK(Integrity Group Temporal Key)의 식별 값을 나타낸다. IPN은 Integrity Packet Number를 뜻하며, 재전송 공격 방지를 위한 카운터 값이다. MIC는 Message Integrity Code로, 이 값으로 수신자가 프레임의 무결성을 검증할 수 있다.

Element ID (1-Byte)	Length (1-Byte)	Key ID (2-Bytes)	IPN (6-Bytes)	MIC (8-Bytes)

그림 3. IEEE 802.11w MMIE 구조
Fig. 3. IEEE 802.11w MMIE structure

4.2 Downgrade 공격에 대한 한계

Downgrade 공격은 통신 과정에서 사용되는 보안 프로토콜이나 기능을 공격자가 낮은 버전으로 전환시켜, 보안 수준이 낮은 상태로 통신을 수행하게 하는 공격이다. 이로 인해 통신 데이터가 노출될 수 있으며, 공격자가 추가 공격을 할 가능성이 높아진다. 이를 해결하기 위해 TPM(Trusted Platform Module)을 활용하여 보안 데이터를 안정하게 저장하는 방식을 제안한다. TPM은 보안을 강화하기 위해 설계된 하드웨어 기반 암호화 프로세서로, 암호화 키 생성, 저장, 인증 및 데이터 검증과 같은 보안 기능을 제공한다. 이 방법은 부팅 시, TPM 내부에 서명 키를 생성하고, TPM2_NV_DefineSpace를 사용하여 시스템 기능을 저장한 후, TPM2_NV_WriteLock을 사용하여 시스템이 재부팅될 때까지 변경을 차단하여 보안을 강화한다. 또한, Challenge 메시지를 추가하여 보안이 문제없이 진행되고 있음을 검증할 수 있게 하는 방법을 제안하고 있다[11].

4.3 다중 사용자 계약 인증에 대한 한계

현재 ISO 15118‐20의 PnC는 단일 차량 소유주를 중심으로 설계되어 있어, 차량 공유나 법인 차량 같은 다중 사용자 환경에서는 사용에 한계가 있다. 이를 해결하기 위해 TPM 2.0 기반 사용자 계약 인증서 관리 시스템을 도입하는 기술이 연구되었다. 이 시스템은 E-Mobility Service Provider(EMSP), 차량 내 TPM 2.0 모듈, 충전 인프라의 3 계층 구조로 설계되어 있으며, 다음과 같은 관리 과정을 통해 수행된다.

1. 사용자는 EMSP에 PIN, 지문 같은 인증 데이터를 제출하여 등록하며, EMSP는 각 사용자마다 고유한 계약 인증서를 발급한다.
2. 발급된 인증서는 차량 내부의 TPM에 저장된다.
3. Key Authorization Policy(KAP)이라는 정책을 적용한다.

KAP은 조건을 설정해 사용자의 인증 데이터가 조건과 일치하면 인증서를 사용하게 허용하는 정책이다. TPM2_PolicySigned 명령어를 활용하여 다중 사용자 인증을 가능하게 한다[12].

4.4 원격 인증 지원 제약

ISO 15118‐20은 EVSE의 무결성을 확인하는 방법은 제공하고 있지 않기 때문에, 공격자가 장치에 접근할 경우 모든 키에 대한 접근 권한을 얻을 수 있다. 이를 해결하기 위해 EV가 신뢰할 수 있는 EVSE에서만 충전을 진행하도록 하기 위해 Remote Attestation을 도입하여 해결할 수 있다. 기존 SessionSetupReq/Res 이후에 AttestationReq/Res 메시지를 추가하여 장치의 소프트웨어 무결성을 검증한다. AttestationReq에는 Nonce, Attestation Type (Boot-time, Runtime, Periodic), Timestamp, EV Identifier로 구성되어 있고, AttestationRes에는 Integr- ity Hash, Nonce, TPM Signature, Timestamp, Public Key로 구성되어 있다. 이 메시지의 Boot-time, Runtime, 및 Periodic 검증으로 무결성을 검증할 수 있다[13].

표 2는 [13]에서 제안한 방식과 기존 ISO 15118-20 프로토콜을 비교하여, 개선된 기능 및 세션 셋업 시간을 나타낸다. Ross Porter et al.[13]은 프로토콜에 Attestation 메시지를 추가하여 무결성 검증 및 공격 탐지 기능을 확보하였다. 이로 인해 세션 셋업 시간은 791.8ms에서 1,238ms로 약 450ms가 추가되었다. 그러나, ISO 15118-20 표준에서는 V2G_EVCC_Msg_Timeout(SessionSetupReq)을 2s, V-2G_SECC_Msg_Performance_Time(SessionSetupRes)을 1.5s로 규정하고 있기 때문에, 추가된 시간은 수용 가능한 범위 내에 있다.

표 2. 기존 방식과 개선된 방식 비교
Table 2. Comparison between the existing and enhanced method

Classification	ISO 15118-20	R. Porter et al.[13]	Remarks
Session step time	791.8ms	1,238.0ms	+446.2ms
Integrity Verification	X	O	Verifiable
Attack detection	X	O	Detectable

그림 4는 EV, EVCC, OSM(Original Software Manu-facturer) 간의 메시지 교환 흐름 예시를 보여준다. 빨간색 네모 표시된 부분이 새롭게 추가된 메시지이며, 대괄호 안의 메시지는 선택적으로 사용되는 메시지를 나타낸다.

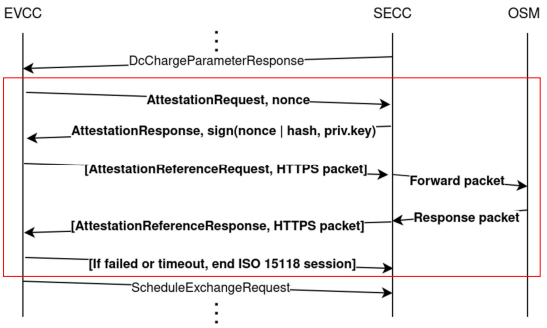


그림 4. R. Porter et al.[13] 방식 메시지 흐름
Fig. 4. R. Porter et al.[13] method message flow

AReq(AttestationRequest)는 EV가 SECC의 무결성 검증을 요청하기 위해 전송하는 메시지이며, ARes(AttestationResponse)는 AReq 메시지를 SECC가 받고 난 후에 보내는 응답 메시지이다. 이 메시지의 자세한 패킷은 그림 5에서 설명한다. 이 과정에서 EVCC에 무결성을 검증할 기준값이 없을 경우, OSM에게 ARReq (AttestationReference Request) 메시지를 전송하여 요청한다. EVCC는 ARRes(AttestationReferenceResponse) 메시지를 수신함으로써, 기준값을 얻을 수 있으며, ARReq 및 ARRes 메시지는 SECC가 확인할 수 없도록 암호화되어 전송된다. 이 메시지 흐름에서 Timeout 또는 Failed 경우에는 세션을 종료하고, 충전을 거부한다. 이는 무결성 검증에 실패했음을 의미하며, SECC를 이용한 공격을 방지하기 위한 필수적인 절차이다. R. Porter et al.[13]은 다음과 같은 시나리오를 통해 검증하였다.

1. EVCC는 Nonce를 생성하여 원하는 Attestation Type으로 SECC에 AReq를 전송한다.

2. SECC는 수신한 Nonce와 Integrity Hash를 결합하여 생성한 Signature와 Public Key를 ARes를 통해 EVCC로 전송한다.

3. EVCC가 기준값을 보유하지 않은 경우, ARReq/ARRes 메시지를 통해 OSM으로부터 기준값을 전송받는다.

4. EVCC는 전송받은 기준값과 ARes의 Signature를 비교하여 무결성을 검증하고, Timeout 규정을 초과하지 않았는지 확인한다.

5. 검증이 성공하면 다음 충전 세션을 수행하고, 실패하거나 Timeout일 경우, 세션을 종료한다.

그림 5는 추가된 AttestationResponse 메시지의 패킷을 보여준다. Evidence, Signature lengths는 각각 Evidence와 Signature의 길이를 나타내는 필드이다. Nonce는 EV에서 임의로 생성하여 EVSE에 전송하는 값을 나타내며, EVSE가 이를 반환함으로써 공격을 방지하고, 유효한 응답임을 보장한다. Evid- ence는 Boot-time, Runtime, Periodic을 표현하며, 이를 통해 무결성을 확인할 수 있다. Signature of (Nonce | Evidence)는 Nonce와 Evidence를 결합한 서명 값으로, EVCC에서 검증한다.

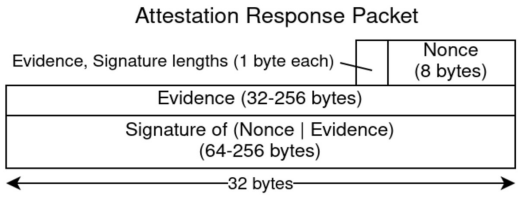


그림 5. AttestationResponse 패킷[13]
Fig. 5. AttestationResponse packet[13]

V. 결 론

본 논문은 ISO 15118-20이 기존 ISO 15118-2의 한계를 극복하기 위해 개선된 기능과 그 한계점을 분석하고, 이를 보완하기 위해 제안된 기술을 분석하였다. ISO 15118-20은 TLS 1.3을 채택함으로써, 핸드셰이크 RTT를 단축하고, AEAD 암호화 알고리즘 사용으로 보안성을 강화하였다. 또한, TLS 포맷을 추가하여 TLS 암호화를 의무적으로 사용함으로써, 보안 취약점을 보완하였다. 더불어, WLAN 기반 무선 통신을 통해 유선망 기반 통신의 한계를 극복하고, 실시간 동적 충전 제어를 가능하게 하여 EV와 EVSE 간의 효율적인 데이터 교환 및 충전 스케줄 관리가 이루어질 수 있도록 하였다. 게다가, WPT, BPT, ACD와 같은 새로운 충전 방식을 추가하여 충전 프로세스의 효율을 높였다.

그러나, ISO 15118-20도 다중 사용자 환경 및 무선 인증의 한계, 무선 환경에서의 Downgrade 및 DoS 공격과 같은 각종 외부 공격에 대한 취약성 등 여러 한계점을 가지고 있다. 이로 인해 TPM 2.0 기반 KAP 정책을 통한 다중 사용자 인증 지원, IEEE 802.11w를 통한 보호 관리 프레임 적용 및

Attestation 메시지를 통한 EVSE 무결성 검증 방식이 연구되었다. 이러한 기술은 향후 확장된 ISO 15118‐20의 기반이 될 것이며, 충전 인프라에 중요한 역할을 할 것으로 기대된다. 또한, 향후 연구에서는 제안된 개선 방안뿐만 아니라 물리적 및 다른 측면에 대한 추가적인 연구가 필요하다.

References

[1] H. Shin and M. Jung, "Global green vehicle adoption trends and implications of major environmental regulatory policies", Energy Economics Institute, Energy Focus, Vol. 85, No. 82, pp. 82-102, Oct. 2022.

[2] BloombergNEF, "Electric Vehicle Outlook 2024", https://about.bnef.com/electric-vehicle-outlook/. [accessed: Feb. 28, 2025]

[3] International Energy Agency, "Global EV Outlook 2024", https://www.iea.org/reports/global-ev-outlook-2024. [accessed: Feb. 25, 2025]

[4] International Organization for Standardization, "ISO 15118-2: Road Vehicles—Vehicle-to-Grid Communication Interface—Part 2: Network and Application Protocol Requirements", https://www.iso.org/standard/55366.html. [accessed: Feb. 09, 2025]

[5] International Organization for Standardization, "ISO 15118-20: Road Vehicles—Vehicle-to-Grid Communication Interface—Part 20: 2nd Network and Application Protocol Requirements", https://www.iso.org/standard/77845.html. [accessed: Feb. 09, 2025]

[6] U. Willrett, "Innovative Charging Functions using ISO 15118-20", Antriebe und Energiesysteme von morgen 2023(ATZLive23 2023), pp. 241-251, Jul. 2023. https://doi.org/10.1007/978-3-658-46551-3_19.

[7] C. M. Steffen and K. Buchler, "SSL/TLS Certificate Security-Management and Expiration Challenges", https://www.appviewx.com/ema-eport-ssl-tls-certificates-security-management-and-expiration-challenges/. [accessed: Mar. 24, 2025]

[8] H. Lee and M. Shin, "TestShark: A Passive Conformance Testing System for ISO 15118 Using Wireshark", MDPI, Energies 2024, Vol. 17, No. 23, pp. 5833, Nov. 2024. https://doi.org/10.3390/en17235833.

[9] S. Kohler, S. Birnbach, R. Baker, and I. Martinovic, "On the Security of the Wireless Electric Vehicle Charging Communication", IEEE International Conference on Com- munications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, Singapore, pp. 393-398, Oct. 2022. https://doi.org/10.1109/SmartGridComm52983.2022.9961000.

[10] I. S. Bandurova, I. Kotsiuba, and T. Biloborodova, "Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations", IEEE International Conference on Big Data (Big Data), Osaka, Japan, pp. 3099-3106, Dec. 2022. https://doi.org/10.1109/BigData55660.2022.10020644.

[11] R. Porter, M. B. Abhari, B. Tan, and D. Thrimawithana, "Extending ISO 15118-20 EV Charging: Preventing Downgrade Attacks and Enabling New Security Capabilities", 21st Annual International Conference on Privacy, Security and Trust (PST), Sydney, Australia, pp. 1-9, Aug. 2024. https://doi.org/10.1109/PST62714.2024.10788058.

[12] C. Plappert, L. Jager, A. Irrgang, and C. Potluri, "Secure Multi-User Contract Certificate Management for ISO 15118-20 Using HardWare Identities", Association for Computing Machinery, 18th International Conference on Availability, Reliability and Security, Benevento, Italy, No. 54, pp. 1-11, Aug. 2023, https://doi.org/10.1145/3600160.3605165.

[13] R. Porter, M. B. Abhari, B. Tan, and D. Thrimawithana, "Enhancing Security in the ISO 15118-20 EV Charging System", Elsevier, Green Energy and Intelligent Transportation, pp. 100262, Jan. 2025. https://doi.org/10.1016/j.geits.2025.100262.

저자소개

김 종 훈 (JongHoon Kim)

2025년 2월 : 동아대학교 전자공학과(공학사)
2025년 3월 ~ 현재 : 동아대학교 전자공학과 석사과정
관심 분야 : 전기자동차 표준, Edge 컴퓨팅

김 동 완 (Dongwan Kim)

2003년 8월 : 고려대학교 전자공학과(공학사)
2006년 2월 : 포항공과대학교 정보통신공학과(공학석사)
2015년 2월 : 고려대학교 전기전자공학과(공학박사)
2006년 2월 ~ 2017년 2월 : 삼성전자 네트워크사업부 책임연구원
2017년 3월 ~ 현재 : 동아대학교 전자공학과 부교수
관심 분야 : 전기자동차 표준, Edge 컴퓨팅