

V2G 충전 통신 SLAC 프로토콜의 NMK 노출 취약점 분석 및 채널 임펄스 응답 기반 키 합의 방안

정소연*, 박병석*, 최인지*, 강수경*, 이진영*, 최지원*, 원유재*
한국전력공사*, 충남대학교*

Analysis of NMK Exposure Vulnerabilities in V2G Charging Communication SLAC Protocol and Channel Impulse Response-Based Key Consensus Method

So-Yeon JUNG*, Byeong-Seok Park*, In-Ji Choi*, Soo-Jyung Kang*, Jin-Young Lee*, Ji-Won Choi*, Yu-Jae Won*
KEPCO*, Chungnam National University*

Abstract - ISO 15118-3 표준은 SLAC 프로토콜의 NMK를 평문으로 전송하는 구조적 취약점을 가진다. HPGP 표준 13.8.2 절은 보안이 강화된 SecureSLAC을 제시하지만 PKI 인프라 구축이 필수적이므로 ISO 15118-3은 이를 채택하지 않는다. 선행 연구들은 CM_SLAC_MATCH.CNF 메시지에서 NMK가 평문으로 전송되는 취약점을 공통적으로 악용하고 있으나, 상위계층인 ISO 15118-20과 달리 물리계층 표준인 ISO 15118-3은 개정 없이 유지되고 있다. 이를 보완하기 위해 본 논문은 전력선의 특성을 사용하여 별도의 정보 교환 없이 로그 중심화와 양자화를 이용하여 EV와 EVSE가 키를 직접 교환하지 않고도 동일한 NMK를 독립적으로 도출하는 방법을 제안한다.

1. 서 론

탄소중립 정책과 배터리 기술 발전에 따라 EV(Electric Vehicle) 보급이 빠르게 증가하고 있다. 산업통상자원부(現기후 에너지환경부) 등 관계부처는 2030년까지 EV 420만대 보급에 대비해 EVSE(Electric Vehicle Supply Equipment) 123만 기 구축 계획을 발표하였다.[1] 단순 전력 공급에 머물렀던 충전 인프라는 V2G(Vehicle to Grid) 기술 도입으로 차량과 전력망 간 양방향 충방전을 지원하는 지능형 충전기로 발전하고 있다. V2G 충전기는 EV와 EVSE 간 통신에 ISO 15118 표준을 적용하며 인증, 충전제어, 결제 기능을 제공한다. 이러한 연결성 확대는 새로운 보안 위협을 수반한다.

Miller and Valasek의 차량 원격 해킹 사례[2]가 이를 잘 보여준다. 과거 CAN(Controller Area Network)통신은 외부와 분리된 폐쇄망 환경을 전제로 설계되어 별도의 인증 및 암호화 기능이 포함되지 않았다. 그러나 차량의 스마트화 및 외부 네트워크 연결 기능이 확대되면서 다양한 사이버 공격에 실제 악용될 수 있음이 확인되었다. 이는 설계 당시 위협으로 여겨지지 않았던 취약점이 환경의 변화에 따라 심각한 보안 문제로 부상할 수 있음을 보여주는 사례이다.

V2G 충전 통신의 물리계층에서도 이와 유사한 상황이 전개된다. ISO 15118-3의 SLAC(Signal Level Attenuation Characterization) 절차에서 HPGP(HomePlug Green PHY) 네트워크 형성에 사용되는 128비트 NMK(Network Membership Key)는 현재 암호화 없이 평문으로 전송된다. 충전기와 차량이 전력선으로 직접 연결되어 외부 도청이 어려워 이 취약점은 그간 크게 주목받지 못하였으나, 다수의 국제 보안 연구를 통해 NMK 노출이 네트워크 도청, 세션중단, 프로토콜 조작 등으로 이어질 수 있음이 이미 실증되고 있다.[3][4][5][6]

본 논문은 인프라 확산 이전에 NMK 평문 노출 취약점에 대응하고자, SLAC 프로토콜의 구조적 취약점을 분석하고 이를 악용한 공격 사례를 정리한 뒤 채널 임펄스 응답 기반 로그 중심화 양자화 키 합의 방법을 현실적 대안으로 제안한다. 이는 전력선 채널의 상호성에 기반한 물리계층 키 생성 연구[9]를 V2G SLAC 환경에 최초로 적용한 것이다.

2. 본 론

2.1 현행 SLAC 프로토콜 취약점과 공격 방식

SLAC 프로토콜은 EV가 충전 포트에 연결될 때 CP(Control Pilot) 신호 변화를 트리거로 자동 시작된다. 그림 1과 같이 CM_SLAC_MATCH.CNF 메시지의 NMK 128비트가 전력선으로 유니캐스트 되어 평문으로 전송된다.

NME	필드	옥텟 번호	필드 크기 (옥텟)	값	정의
CM_SLAC_MATCH.CNF Unicast	EVSE MAC	44~49	6	MAC Address of the EVSE Host	EVSE MAC 주소
	RunID	50~57	8	variable	전기자동차 측의 CM_SLAC_PARAM.REQ 전송한 값과 같음.
	RSVD	58~65	8	0x00	향후 이용을 위해 예비됨.
	NID	66~72	7	variable	[HPGP]의 4.4.3.1에 따라 EVSE의 NMK에서 파생된 네트워크 ID
	RSVD	73	1	0x00	향후 이용을 위해 예비됨.
	NMK	74~89	16	variable	EVSE의 사실 NMK(평문 값)

〈그림 1〉 CM_SLAC_MATCH.CNF 메시지 프레임 구조

선행 연구에서 제시된 다양한 공격 시나리오를 2가지 방식으로 나누어 볼 수 있다.

① 도청 : 공격자가 전력선에 물리적으로 접근하거나 누설된 전기신호를 도청하여 CM_SLAC_MATCH.CNF 메시지에서 NMK를 획득한다.[3]

② 중간자 공격: 공격자가 NMK를 획득한 뒤 AVLN에 무단 합류한다.[4] 이후 PIB 필드 규칙 변조를 통한 충전 세션을 강제 중단하거나 상위 계층 메시지 위변조로 피해 차량 요금 전가 등 다양한 후속 공격으로 이어질 수 있다.[5][6] 따라서 위 시나리오들의 공통 전제인 NMK 평문 노출을 원천 차단하는 것이 핵심 목표이다.

EV와 EVSE가 NMK키를 독립적으로 도출하기 위해 전력선의 물리적 고유성을 사용할 것이다. 이전 연구[9]는 전력선의 상호성을 이용한 물리계층 키 생성 가능성을 실증하였으나, 임피던스 비대칭 문제를 해결하기 위해 공개 채널로 정보를 교환하는 과정이 필요했다. 본 논문은 로그 중심화를 적용하여 임피던스 스케일링 인자를 별도의 정보 교환 없이 제거함으로써, EV와 EVSE가 완전히 독립적으로 동일한 채널 지문을 도출하고 이를 NMK로 변환할 수 있는 방법을 제안한다.

2.2 전력선 채널 특성 기반 NMK 도출 원리

HPGP 전력선 채널의 주파수 응답은 다중 경로 전파 모델로 표현된다.

$$H(f) = \sum_{k=1}^k a_k \cdot e^{-j2\pi f \tau_k} \quad (1)$$

여기서 a_k 는 k번째 경로의 감쇠 계수, τ_k 는 전파 지연, k는 유효 경로 수이다. EV와 EVSE는 동일한 전력선 케이블로 연결되어 공통 채널 $H_{common}(f)$ 를 공유한다. 그러나 각 측의 입력

임피던스 차이로 인해 실수 스케일링 인자 α 가 적용된 형태로 나타난다.

$$H_{EV}(f) = \alpha_{EV} \cdot H_{common}(f) \quad (2)$$

$$H_{EVSE}(f) = \alpha_{EVSE} \cdot H_{common}(f) \quad (3)$$

α 의 존재로 단순 양자화 적용 시 양측 NMK가 불일치한다. 이를 해결하기 위해 로그 중심화 변환을 적용한다. 각 측 채널 응답에 로그 변환 후 주파수 평균 μ 를 차감하면 식 (2),(3)의 $\log|\alpha|$ 항이 상수이므로 평균 차감 시 완전히 상쇄된다.

$$\tilde{H}_{EV}(f_i) = L_{EV}(f_i) - \mu_{EV} = \log|H_{common}(f_i)| - \mu_{common} \quad (4)$$

$$\tilde{H}_{EVSE}(f_i) = L_{EVSE}(f_i) - \mu_{EVSE} = \log|H_{common}(f_i)| - \mu_{common} \quad (5)$$

따라서 다음이 성립한다.

$$\tilde{H}_{EV}(f_i) = \tilde{H}_{EVSE}(f_i) \quad (6)$$

식(6)에 의해 양측이 동일한 정규화 채널 벡터를 독립적으로 획득한다. 이후 1비트 양자화하여 128비트 양자화 비트열에 HKDF_SHA256을 적용하여 동일한 NMK를 도출 할 수 있다.

2.3 SLAC 프로토콜 적용 및 방어 메커니즘

채널 임펄스 측정은 기존 CM_MNBC_SOUND 단계에서 추가 메시지 없이 수행되며, CM_SLAC_MATCH.CNF의 SECURITY_TYPE 필드를 0x01로 설정하여 NMK 필드를 더미값으로 대체한다. 수신 측은 이 필드를 인식하여 채널 임펄스 응답에서 독립 도출한 NMK를 사용하며, 레거시 장치(SECURITY_TYPE=0x00)와의 하위 호환도 유지된다.

제안 방식 적용 후 CM_SLAC_MATCH.CNF에 NMK가 포함되지 않으므로 2.2절에서 확인한 공격 시나리오의 공통 전제인 NMK 평문 획득이 불가능해진다. 공격자가 물리적으로 채널 중간에 삽입될 경우 채널 특성이 변화하여 NMK를 재현할 수 없다. 차량 신원 인증은 ISO 15118-20 TLS기반 상호 인증이 담당한다. 또한 ISO 15118-3의 메시지 구조 자체를 변경하지 않기에 HPGP표준의 SecureSLAC보다 장점이 많다.

〈표 1〉 채널 임펄스 응답 기법의 장단점

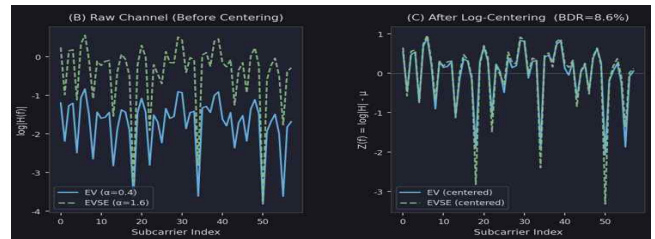
항목	채널 임펄스 응답 기법	SecureSLAC
외부인프라	[장점] 불필요 물리적 채널만으로 키 도출	SLAC전용 PKI 필요 V2G PKI 재활용 불가
인증서관리	[장점] 없음 발급, 갱신, 폐기 불필요	인증서 수명 관리 필요 만료, 폐기 시 충전 불가
프레임 구조	[장점] 재활용 가능 기존 M-Sound 재활용 및 추가 페이로드 최소한 추가	새 프레임 정의 필요 SLAC프로토콜 새로 설계
레거시 충전기 호환성	[장점] 높음 Reserved필드 활용 기존 장비와 공존 가능	없음 미지원 장비와 충전 불가
표준 개정 범위	[장점] ISO15118-3 부분수정 SLAC프로시저+필드추가	대규모 개정 필요 표준 + 신규 PKI 전면 개정
배포 현실성	[장점] 높음 펌웨어 업데이트만으로 적용 가능	낮음 PKI구축 인프라 동시 업그레이드
신원 인증	[단점] 없음 채널인증만 수행 ISO 15118-20에서 수행가능	있음 인증서로 EVSE신원 검증

2.4 제안 방식 검증

제안 방식의 핵심 원리를 검증하기 위해 Python 시뮬레이션을 수행하였다. 임피던스 스케일링 인자 α 가 0.4(EV)와 1.6(EVSE)으로 4배 차이나는 조건에서, 그림 2(a)와 같이 로그 중심화 변환 적용 전에는 양측 채널 응답이 수직으로 어긋나 있으나, 그

림 2(b)와 같이 로그 중심화 변환 적용 후 양측의 정규화 채널 벡터가 수렴함을 확인하였다. 이는 수식 (4)~(6)에서 증명한 α 항 상쇄 원리가 시뮬레이션을 통해 실험적으로 확인됨을 보여준다.

채널 벡터의 수렴이 확인되면 동일한 비트열에 HKDF-SHA256을 적용하므로 EV와 EVSE가 동일한 NMK를 독립 도출하는 것은 수학적으로 따라온다. 단, 실환경에서는 전력선 노이즈에 의해 비트 불일치가 발생할 수 있으므로 실측 검증 후 향후 연구로 수행할 예정이다.



〈그림 2〉 로그 중심화 원리 시각화 : (a) 변환 전, (b) 변환 후

3. 결 론

본 논문은 ISO 15118-3 SLAC 프로토콜의 NMK 평문 전송 취약점을 사용한 공격을 분석하고 전력선 채널 임펄스 응답 기반 NMK 키 합의 방안을 제안하였다. 로그 중심화와 양자화 기법을 통해 임피던스 스케일링 인자를 수직적으로 상쇄함으로써 EV와 EVSE가 사전 공유 없이 동일한 NMK를 독립 도출할 수 있음을 증명하였다. Python 시뮬레이션을 통해 α 가 4배 차이나는 조건에서도 로그 중심화 적용 후 채널 벡터가 수렴함을 검증하였다. HPGP SecureSLAC 비교를 통해 제안 방식이 추가 인프라 및 별도 메시지 교환 없이 기존 SLAC 메시지를 재활용하여 NMK 탈취를 원천 차단함을 보였다.

추후 연구에서는 SECURITY_TYPE 필드를 활용하여 채널 임펄스 응답 기반 NMK 도출 방식을 기존 SLAC 프로토콜에 삽입하는 구체적인 구현 방안을 제시할 예정이다. 또한 KEPCO V2G 테스트베드를 활용한 실측 실험을 통해 실환경에서의 채널 안정성 및 NMK 일치율을 검증할 계획이다.

〔참 고 문 헌〕

- [1] 산업통상자원부, "전기차 충전인프라 구축·운영 지침", 2023.
- [2] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," IOActive Technical White Paper, Aug. 2015.
- [3] R. Baker and I. Martinovic, "Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging," 28th USENIX Security Symposium, pp. 407 - 424, Aug. 2019.
- [4] B. Szakaly, et al., "Current Affairs: A Security Measurement Study of CCS EV Charging Deployments," Workshop on Automotive and Autonomous Vehicle Security (VehicleSec), 2025.
- [5] J. Loew, et al., "Security Analysis of ISO 15118 V2G Communication," arXiv:2512.15966, Dec. 2024.
- [6] M. Dudek, et al., "V2Ginjector: Exploiting Electric Vehicle Charging Networks," SSTIC, 2019.
- [7] ISO 15118-3:2015, "Vehicle to Grid Communication Interface - Part 3," ISO, 2015.
- [8] HomePlug Powerline Alliance, "HomePlug Green PHY Specification v1.1," Section 13.8.2, Jan. 2012.
- [9] F. Passerini and A. M. Tonello, "Physical Layer Key Generation for Secure Power Line Communications," MDPI Electronics, 2020.