V2G 네트워크에서의 인증 취약점 및 완화 기법 분석

가드가 나무라타[1], 레리사 아데바 질차[2], 김득훈[3], 곽진[4]
[1]아주대학교 사이버보안학과, 정보보호응용및보증연구실(대학원생)
[2]아주대학교 AI융합네트워크학과, 정보보호응용및보증연구실(대학원생)
[3]아주대학교 소프트웨어융합연구소(박사후연구원)
[4]아주대학교 사이버보안학과(교수)
khadka.isaa@gmail.com, lelisa.isaa@gmail.com, dhkim.isaa@gmail.com, security@ajou.ac.kr

Analysis of Authentication Vulnerabilities and Mitigating Methods in V2G Networks

Khadka Namrata[1], Lelisa Adeba Jilcha[2], Deuk-Hun Kim[3] and Jin Kwak[4]
[1]ISAA Lab., Dep of Cyber Security, Ajou University (Graduate student)
[2]ISAA Lab., Dep of AI Convergence Network, Ajou University (Graduate student)
[3]Inst. for Computing and Informatics Research, Ajou University (Post Doctor)
[4]Department of Cyber Security, Ajou University (Professor)

Abstract

The Vehicle-to-Grid (V2G) paradigm facilitates bi-directional energy and data exchange between Electric Vehicles (EVs) and the Smart Grid, enhancing power distribution efficiency and dynamic grid interaction. However, this open communication framework presents authentication-related security risks, particularly impersonation, Man-in-the-Middle (MITM), and replay attacks.

This paper offers a focused analysis of these vulnerabilities by reviewing typical attack models and evaluating how current authentication protocols respond to them. Special attention is given to lightweight, certificate-based mutual authentication mechanisms employing Transport Layer Security (TLS) and Public Key Infrastructure (PKI). Through step-wise examination, the paper assesses the strength and limitations of these strategies in practical V2G environments, highlighting deployment challenges and security considerations.

1. Introduction

The Vehicle-to-Grid (V2G) concept is central to modern smart grids, enabling Electric Vehicles (EVs) to both consume and supply energy [1]. V2G integration enhances power system reliability, security, and efficiency by leveraging advanced communication and control technologies. As a core component, it facilitates bidirectional energy flow between EVs and the grid [1].

However, increasing use of IT in EV charging has exposed protocol vulnerabilities, leading to communication security issues. Users may tamper with charging data to lower billing, causing financial losses [2]. Hackers may also steal sensitive information like passwords, locations, or account credentials, compromising user privacy [2].

This paper explores the root causes of such attacks and their real-world impact. By analyzing threat models and protocol weaknesses, we aim to support secure, scalable, and efficient V2G authentication design. The V2G authentication process typically involves four stages:

Stage 1. Pre-Authentication

The EV and Electric Vehicle Supply Equipment (EVSE) exchange capability information and negotiate the communication protocol (e.g., ISO 15118 or CCS) [3].

Stage 2. Physical Connection and Link Setup

A secure communication link is physically established between the EV and the EVSE.

Stage 3. Mutual Authentication

Contract-based credentials or digital certificates are exchanged and verified for identity assurance.

Stage 4. Authorization

The Charging Station Management System

(CSMS) verifies user permissions and approves the charging session.

While this structured flow enhances trust, real-world deployments remain vulnerable to attacks if verification and message integrity are not rigorously enforced [4].

2. Analysis of Authentication-Relate Problems in V2G Systems

Authentication weaknesses in V2G systems expose security threats that affect the integrity, confidentiality, and availability of grid communications. Below, we examine three common attack scenarios and their impact on EV charging systems.

2.1 Man-in-the-Middle (MITM) Attacks

MITM attacks occur when an adversary intercepts and possibly alters communication between two parties without their knowledge [5]. In a V2G scenario, a malicious node may position itself between the EV and EVSE to eavesdrop or inject false data [5], compromising both confidentiality and integrity. For example, attackers can alter charging commands or meter readings, leading to incorrect energy transactions, privacy breaches, or disruptions in grid operations [6]. This may cause manipulated charging behaviors or mislead the grid about EV status, resulting in overcharging or financial discrepancies [6].

2.2 Replay Attacks

In a replay attack, an adversary captures legitimate communication messages and later reuses them to deceive the system [4]. The attacker retransmits valid messages to create unauthorized effects or confusion in the network [4]. In V2G, replaying stale messages can duplicate control instructions, causing the system to act on an old charging request again or register a completed transaction twice [5]. This disrupts synchronization, leading to energy imbalances and operational errors [5]. For an EV, it could falsely re-initiate or terminate charging, causing improper cycles or billing issues. The grid could also be tricked into believing an EV is supplying or drawing power when it is not, undermining trust in system state [6].

2.3 Impersonation Attacks

Impersonation attacks involve attackers using stolen or forged credentials to masquerade as a legitimate EV or EVSE. By posing as an authorized entity, the attacker gains illicit access to services, steals electricity, or disrupts energy flows [1]. For example, they might steal a certificate or token from a real EV and use it to impersonate that vehicle on the network [1]. This could let them initiate charging for their own device without permission or send false data to the grid [1]. Such intrusions may cause financial losses and threaten grid stability if a rogue device manipulates energy feed timing or volume. Without robust authentication, the system may grant access to impostors, risking overall V2G security and reliability [7].

3. Analysis of Mitigation Approaches for Authentication Problems in V2G Networks

To address the above threats, we analyze existing lightweight certificate-based mutual authentication approaches that leverages TLS/PKI security features. The following subsections discuss how the proposed measures mitigate each type of attacks.

3.1 Mitigation of MITM Attacks

MITM attacks exploit weak TLS or certificate validation during session initiation [7], but mutual authentication with certificates and cryptographic challenges helps ensure only trusted entities communicate between EV and EVSE.

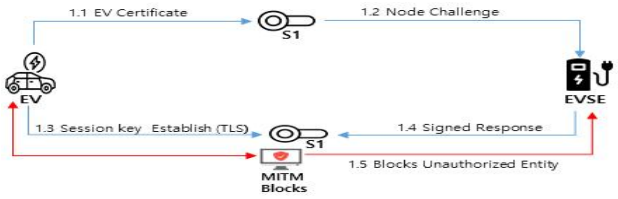
Step 1. The EV and EVSE exchange digital certificates issued by a trusted Certificate Authority establishing initial trust.

Step 2. A challenge response protocol is performed, where a unique nonce is signed and returned by each party using their respective private keys.

Step 3. Mutual verification is carried out. Each entity confirms the validity of the signature and

the nonce, ensuring the communicating party possesses the corresponding private key.

Step 4. Upon successful verification, a secure TLS session is established using session keys negotiated during the handshake.



(Fig 1) Mitigation Process Of MITM Attacks

These steps ensure mutual trust and session confidentiality between EV and EVSE [8]. Figure 1 shows a secure flow where a MITM attacker fails due to cryptographic protections like PKI validation and encryption [1]. However, V2G deployments may face challenges in certificate management due to mobility and connectivity limits [3].

3.2 Mitigation of Replay Attacks

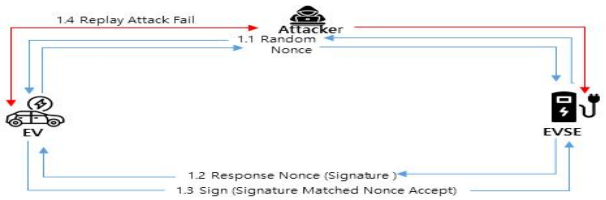
Replay attacks exploit the retransmission of previously valid messages to trigger unintended actions [5]. To counter this, message freshness is ensured using nonces or time stamps within the authentication process [3, 8].

Step 1. The EVSE generates a random nonce and transmits it to the EV as a freshness challenge.

Step 2. The EV signs the nonce using its private key and sends the signature, along with its digital certificate, to the EVSE.

Step 3. The EVSE validates the signature using the EV's certificate and checks that the received nonce matches the issued challenge.

Step 4. Any replay attempt using a previously signed message fails, as the nonce will not align with the current challenge, and the EVSE rejects the session.



(Fig 2) Mitigation Process Of Replay Attacks

The inclusion of session-specific nonces ensures that only fresh, context aware messages are accepted, effectively mitigating replay threats [1, 7]. Figure 2 demonstrates this process. While lightweight and effective, nonce-based verification depends on secure random number generation and proper handling [8]. Systems with limited entropy or poor synchronization may face nonce reuse or predictability, weakening the defense [8].

3.3 Mitigation of Impersonation Attacks

Impersonation attacks exploit weak identity verification to access grid services [1]. Mitigation involves mutual TLS and PKI-based credential validation between EV and EVSE [1], ensuring only legitimate participants engage in V2G.

Step 1. The EV initiate a secure session with the charging station, requesting a TLS handshake.

<Table 1> Comparative Summary of Attack Types and Mitigation Strategies in V2G Systems

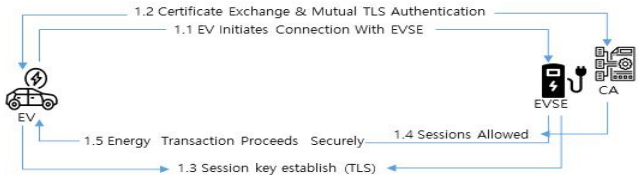
Attack Types	Attack Mechanism	Mitigation Techniques	Security Focus
MITM Attack	Intercepts and modifies real-time messages between EV and EVSE	Mutual TLS authentication with signed challenge response exchanges	Verifies both parties identities to prevent session hijacking
Replay Attack	Reuses previously valid protocol messages to trigger unauthorized actions	Session specific nonce-based challenges to ensure message freshness	Ensures all authentication responses are unique and not reusable
Impersonation Attack	Uses stolen credentials to pose as a legitimate EV or charger	Certificate-based TLS handshake and challenge - response validation	Blocks unauthorized entities lacking valid certificates and keys

Step 2. Both parties exchange digital certificates issued by a trusted CA.

Step 3. Mutual authentication is performed, including certificate chain validation and challenge-response exchanges. Invalid or revoked certificates result in session termination.

Step 4. A session key is negotiated and used to encrypt subsequent communications.

Step 5. Only after successful authentication, energy exchange is authorized. All transactions are logged and tied to the verified identities.



(Fig 3) Mitigation Process Of Impersonation Attacks

While Mutual TLS provides strong security but require effective certificate life cycle management [5]. Figure 3 shows a framework where only authenticated EVs and EVSEs can access the V2G system, ensuring identity assurance and blocking unauthorized access [1]. In constrained environments, delayed revocation checks can be mitigated using PKI with short-lived tokens or trusted hardware [5]. Table 1 shows that although a challenge response method is common, each attack demands a distinct focus: real-time protection (MITM), freshness (Replay), and identity assurance (Impersonation) [1, 3, 5].

4. Conclusion

This paper analyzed authentication vulnerabilities in V2G systems, focusing on replay, MITM, and impersonation attacks. Evaluation of TLS and PKI-based approaches revealed both strength and limitations. While current mechanisms provide a strong foundation, deployment must consider scalability and device constraints. The findings support ongoing refinement of V2G authentication strategies.

Acknowledgment

This work was supported by the Technology Innovation Program(RS-2024-00443436) funded By the Ministry of Trade, Industry Energy(MOTIE, Korea).

References

[1] Xiao Nan, Zhaoshun Wang and Xiaoxue Sun, "A secure and efficient authentication Scheme for vehicle to grid in smart grid," Frontiers in Physics, Vol. 13, p. 1529638, Mar. 2025.

[2] Li Yafei, Yong Wang, Min Wu and Haiming Li, "Replay Attack and Defense of Electric Vehicle Charging on GB/T27930-2015 Communication Protocol", Journal of Information Security, Vol. 7, no. 12, p. 20, Dec. 2019.

[3] Chen Yunwang, Yanmin Zhao and Siuming Yiu "Cyber-Physical Authentication Scheme for Secure V2G Transactions", preprint arXiv:2409.14008, Sep. 2024.

[4] Marc Multin "How ISO 15118 Supports Vehicle-to-Grid (V2G)", Switch EVBlog, Apr. 2024.

[5] Conti Mauro, Denis Donadel, Radha Poovendran and Federico Turrin, "EVExchange: A Relay Attack on Electric Vehicle Charging System", Springer, Vol. 13555, pp. 519 - 538, Sep. 2022.

[6] Saxena Neetesh, Santiago Grijalva, Victor Chukwuka and Athanasios Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid", IEEE Wireless Communications, Vol. 24, no. 4, pp. 88 - 98, Mar. 2017.

[7] Kave Masoud, Diego Martín, and Mohammad Re za Mosavi, "A Lightweight Authentication Sch eme for V2G Communications: A PUF-Based Approach Ensuring Cyber/P hysical Security a nd Identity/Location Privacy," Electronics, Vol. 9, no. 9, p. 1479, Sep. 2020.

[8] Mekkaoui Kheireddine, Mansour Mekour and Hamza Teggar "Securing Vehicle-to-Grid Networks: A Bio-Inspired Intrusion Detection System", Scientia Iranica, Aug. 2024.