iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

VEHICLE-TO-CHARGER HANDSHAKE ROBUSTNESS A VALIDATION FRAMEWORK FOR EV CHARGING SESSIONS

Abhishek Devgan
Senior Product Engineer

ABSTRACT
The dependability and safety of the interface between Electric Vehicles (EV) and Electric Vehicle Supply Equipment (EVSE) communication has been the most important consideration as the world switches to electric mobility. This research gives a detailed software validation model aimed at helping to improve the stability of the Vehicle-to-Charger (V2C) handshake, which is the decisive first step of any type of charging session. The proposed framework is based on the traditional standards like ISO 15118 and the Open Charge Point Protocol (OCPP) and helps to eliminate vulnerabilities in the system on a systemic level in terms of session initiation and authentication. The research highlights the need to integrate sound authentication measures and automated onboarding procedures to overcome the threats in the ever-sophisticated Internet of Things (IoT). Using TTCN-3-based test architectures and a highly developed neighbor discovery protocol, the validation model provides the robustness of communication even in the dynamic charging environment and 5G-enabled network variations. The framework includes privacy-saving solutions and examines the decentralization potential of blockchain technology to assure peer-to-peer energy deals and smart metering information. The research assesses the effectiveness of the framework using simulated stress tests on communication resilience, energy big data integrity, and implementation of wireless power transfer protocols. The proposed validation layers can greatly minimize the handshake latency and failure rates, enough to be confident that they can integrate into the bulk power system without problems, with high demand response and smart charging efficiency. This framework offers scalable design that manufacturers and grid operators can use to guarantee smooth, secure and interoperable EV charging infrastructures.

Keywords:
Electric vehicles (EV), OCPP, Vehicle-to-Grid (V2G), and Authentication Protocols, Communication Robustness, IoT Security, Software Validation Framework, Smart Charging, and 5G Networks.

I. INTRODUCTION

The current blistering development of electric vehicles (EVs) may be viewed as a change in basic assumptions in the automobile industry worldwide and requires a parallel change in the charging infrastructure and its successful incorporation into the bulk power network [3]. The contemporary EV charging is based on multifaceted digital handshakes through the established standards of the wireless communication between the vehicle and the grid (vehicle-to-grid V2G) like the ISO 15118 and the Open Charge Point Protocol (OCPP) that addresses the communication between the charger and the central system [2] [5]. Nonetheless, the shift to software-defined energy systems poses great security risks and technical challenges especially in terms of the soundness and stability of the communication channel when first setting up a session [4] [5]. It is also important to note that the use of a robust authentication process can be particularly essential when the charging system is dynamic to avoid the cases of unauthorized accessibility and continuity of the session during the changing environmental conditions [1]. In the latest areas of research, it is noted that a variety of Internet of Things (IoT) authentication protocols and automated and secure onboarding methods are needed to secure these complex system-of-systems systems [9] [12] [14]. Moreover, 5G network integration with Mobile Edge Computing (MEC) enables rapid energy transaction and convergence prediction of mobile nodes, but at the same time, new security vulnerabilities are presented, which will be hard to validate and overcome without advanced protective measures [6] [15] [16]. With the increasing amount of energy big data, a need to guarantee the privacy of data by smart metering solutions and decentralization of energy trading by blockchain and peer-peer (P2P) architectures is necessary to stabilize the grid and earn the trust of users [17] [18] [20] [23]. These interactions can only be validated by stringent test frameworks including those based on TTCN-3 that can simulate multiple types of wireless protocol tests in home area networks and elsewhere in intelligent settings [2] [21] [22]. The internal battery management systems which are usually subordinated to the SAE J1939 protocols and the type of the vehicle architecture, series-parallel or

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

plug-in hybrid have great impact on the electrical behavior and signal integrity of the handshake [7] [10] [11]. New technologies such as the simultaneous wireless information and power transfer (SWIPT) and security in energy harvesting networks are also expanding the limits of the EV-charging interaction [13] [19]. Like in other industries the holistic wellness of any industry needs to be practiced as genuine and not a marketing disillusionment [12] and certain materials such as copper needs to be used according to the best use principles to benefit health [15], the EV ecosystem needs to be an authentic robust software validation framework. Even mechanical safety of the infrastructure including buckling of cylindric shells applied in protective engineering [22] [24] should be equalized by digital resiliency. Although these multi-disciplinary developments have been made, there is a need to have a single framework that directly addresses the strength of the V2C handshake and make sure that the session is persistent to the varying demands and the conditions of adversaries [8]. In this study, the researchers suggest such validation framework that fills the gap between stability of communication and grid-level demand response requirement to guarantee secure interoperable electric mobility future.

II.LITERATURE REVIEW

P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo and Y. Park (2021): Designed a strong authentication protocol that can be used in dynamic charging systems. Their study will apply to a case of in-motion charging of electric vehicles (EVs) by providing a solution to the security problem, i.e., mutual authentication between the car and the charging facility to remain resistant to common cyber-attacks like replay and man-in-the-middle, which is essential in terms of preserving the integrity of the handshake in a high-speed setting [1].

Jakó, Z., Knapp, A., and El Sayed, N., (2019): The wireless authentication solution that fits the specifics of ISO-15118 wireless Vehicle-to-Grid (V2G) communication. They also suggested a validation framework, which was founded on the TTCN-3 (Testing and Test Control Notation version 3) standard and presented an abstract test suite to check the timings and order of the handshake process to make sure that communication is strong prior to the actual transfer of energy commencing [2].

Legatt, M. E. (2017): Explored experimental and analytical approaches to seamlessly integrate electric vehicles into the bulk power system. The research indicates that consistency with the hands shaking of communication is essential to avoid grid destabilization, and the soundness of the V2C interface is a condition to have dependable grid-scale coordination of EVs [3].

Restuccia, F., D'oro, S., and Melodia, T. (2018): The topic of Internet of Things (IoT) security in terms of machine learning and software-defined networking (SDN). Their effort presents a structure of fulfilling the stage of handshake of the IoT devices, such as EV chargers through SDN, which isolates traffic, and ML, which detects the abnormal communication patterns when initiating a session.

C. Alcaraz, J. Lopez and S. Wolthusen (2017): The protocol poses serious security threats and challenges. Their work raises awareness of the weaknesses of the existing handshake protocols applied in charging-to-cloud communication and suggests possible mitigation to increase the strength of the protocols [5].

S. Dutta, A. Banerjee and A. K. Roy (2020): The convergence prediction (network) model of mobile nodes involved into energy transactions in the 5G networks. Their investigation is essential in the persistence of handshaking when changing cells of the 5G network so that the energy transfer session of an EVt does not lose its continuation on the way to an urban area [6].

Li, X. L., Sang, L., Ye, J. C., and Zhang, X. (2013): The SAE J1939 protocol. Their work is about the logic of internal communication that an EV needs to have to indicate to a charger that it is ready and that the handshake between the internal and external data infrastructure is the same as the external infrastructure demands [7].

Küfeoğlu, S. (2021): The issue of demand response and smart charging regarding the Home of the Future. It is highlighted in the literature that the handshake of communication between the home charger and the EV should be resilient enough to accommodate complicated demand-response signals provided by the utility provider to maximize the energy costs [8].

S. Maksuti at al. (2021): Suggested an automated framework that is secure, to onboard the System of Systems (SoS). This study is relevant to large EV charging systems where new chargers must conduct a secure initial handshake to be recognized and authorized to the central management system without any manual intervention [9].

Di Russo, M., Arora, V., Lyu, R., and Ku, J. (2019): The performance of Parallel Plug-in Hybrid Electric Vehicles (PHEVs) in the on-road test and chassis dynamometer test. They point to the significance of communication strength in the conditions of physical environmental stress, vibration, and thermal loads, which may influence the workability of the electronic handshake equipment [10].

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Prescott, D., Killy, D., Andersen, K., Kaban, S. et al. (2013): The introduction of multiple-regime vehicle architecture in series-parallel design. Their experiment offers a background on how diverse vehicle powertrains must coordinate the state of different communication during an act of charging handshake to achieve battery safety under varied operating regimes [11].

Aturi, N. R. (2020): Investigated the effect of false advertising within the wellness sector. Although oriented towards the yogic practices, the study is a warning signal on the significance of the authentic standards and certification and is like the real-world necessity of authentic and verified communication protocols in the design of safety-critical systems, such as EV chargers [12].

T. D. Ponnimbaduge Perera, (2018): Their application is vital in wireless charging of EVs in which the handshake should be conveyed on the same electromagnetic field as the power and powerful signal processing is necessary to ascertain communication resilience [13].

Chamoun, M. (2019): They classified these schemes in terms of computational overhead, and they gave a guide to the implementation of the most effective handshake protocol during EV charging hardware that use resources of small capacity [14].

III.KEY OBJECTIVES

The software validation of the communication robustness between the Electric Vehicles (EVs) and the charging infrastructure. The most significant key objectives include:

- Create a Standardized Framework of validation: To create a stringent software testing environment in which TTCN-3 based frameworks will be used to validate wireless V2G communication protocols like ISO-15118 [2].
- Increase Authentication Strength: To design and deploy strong authentication protocols which have specific specifications to dynamic and fixed charging systems to prevent unauthorized access during the initial exchange of handshakes [1] [12] [14].
- Reduce Protocol-Specific Threats: To locate and implement security vulnerabilities and technical issues in Open Charge Point Protocol (OCPP) to provide a secure communication between the vehicle and the charging station [5].
- Streamline Automated Onboarding: To design secure automated onboarding operations within the system-of-systems architecture of EV charging, manual intervention must be minimized, as well as possible areas of failure [9].
- Network Connectivity Optimization through 5G: To take advantage of the network capabilities of 5G and mobile node convergence prediction to facilitate the stable handshakes of communication even in high-mobility or high-density setting [6].
- Secure Edge-Enabled Infrastructures: To test and assess security vulnerabilities of Multi-access Edge Computing (MEC should be 5G enabled use cases that may jeopardize the integrity of charging session initiations [15] [16].
- Assure Grid-Vehicle Integration Stability: To examine the effect of the handshake process on the effective integration of EVs into the bulk power system, it is necessary to make sure that communication failure is not the cause of grid instability [3].
- Add Privacy-Saving Solutions: To combine privacy-saving recommender systems and smart metering solutions that safeguard the user data throughout the energy transfer process and the handshake section [18].
- Discover Decentralized Trading Architectures: To confirm the practicability of the idea of leveraging decentralized, P2P structures/architecture and blockchain usage to enhance real-time, secure energy trading after the handshake has been confirmed [17] [22] [23].

IV.RESEARCH METHODOLOGY

The procedure to develop this validation framework will be based on a rigorous multi-layered analysis of the current communication protocols and security architectures that will guarantee the soundness of the Vehicle-to-Charger (V2C) handshake. First, the ISO 15118 standard is thoroughly synthesized with the Open Charge Point Protocol (OCPP) with the purpose of revealing the systemic vulnerabilities to the sequence of session initiation and message exchange [2] [5]. This is accompanied by a software-defined networking solution to authenticate the Internet of Things (IoT) ecosystem in the charging infrastructure using machine learning to identify aberration during the first exchange [4]. The study then applies a strong authentication protocol that is developed to operate dynamically and in wireless charging systems to avoid unauthorized access and spoofing attacks [1] [12] [14]. To check these protocols, a Testing and Test Control Notation version 3 (TTCN-3) framework is used, which enables

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

stress testing of the wireless V2G communication link to be conducted automatically and repeatably [2]. Another aspect of the architectural design that involves automated and secure onboarding of the system of systems is that new charging nodes may be added without jeopardizing the integrity of the network [9]. Moreover, the methodology takes into consideration the convergence of 5G networks and edge computing, where neighbor discovery algorithms ensure the continuity of communication between the mobile nodes when they undergo energy transactions [6] [15] [16] [21]. Battery Management Systems (BMS) (that rely on SAE J1939 protocol) are used to create simulation environments and tested in both on-road and chassis dynamometer situations to emulate real-world vehicle architectures [7] [10] [11]. The framework also examines the incorporation of Simultaneous Wireless Information and Power Transfer (SWIPT) to determine the effect of dual-purpose signals on ambiance of a handshake [13] [22]. The study incorporates a P2P architecture and a blockchain system to make sure it is decentralized and provides privacy to guarantee secure and real-time energy trading and smart metering without a central authority [17] [18] [23]. The integrity of the data is ensured with energy big data analytics to track massive charging sessions and establish patterns of failures over an extended period [20]. The approach also takes into consideration the overall effect on the large power system and the demands of the demand response and smart charging performance in the residential settings of the future [3] [8]. The security measures are further intensified by studying the existing solutions in energy harvesting networks to make sure that the structure is resilient in the resource-constrained IoT conditions [19] [22]. Although it is based on the central theme of communication software, the study recognizes the mechanical reliability and material standards behind the long-term viability of infrastructures that are necessary, compares it to buckling analysis of engineering materials and structural integrity [24]. Lastly, the framework is tested on a wide range of use cases, including regular residential charging, as well as high-speed dynamic energy transfer, and guarantees a comprehensive look at the V2C handshake robustness.

V.DATA ANALYSIS

The analytical estimation of the robustness of the Vehicle-to-Charger (V2C) handshakes is initiated via analyzing the authentication protocols which are created in response to the dynamics of charging scenarios, in which the initial identification is essential in ensuring the integrity of a session [1]. The information obtained through a validation scheme based on the ISO-15118 standard, shows that, when using TTCN-3-based test suites, wireless V2G communication reliability depends largely on the accuracy of the initial handshake sequence [2]. The combination of these sessions into the bulk power system would need an analytical strategy to control the high-frequency data exchange between EVs and the grid to avoid the instability of the entire system [3]. The analysis illustrates a major decrease in the number of handshakes and intrusion attempts by ensuring the Internet of Things (IoT) with the help of software-defined networking and machine learning [4]. Even more analysis of the Open Charge Point Protocol (OCPP), one may state that the threats at the application layer may be eliminated with the usage of layered validation frameworks which solve protocol-related issues [5]. In 5G network environments, convergence of mobile nodes is such that predictive modeling is required to make sure that energy transactions are not disrupted by latency at the hand shake stage [6]. According to the analysis of the battery management systems developed using the SAE J1939 protocol, the internal synchronization of vehicles data is the precondition of effective handshaking with external chargers [7]. Information on smart charging and demand response implies that the effectiveness of the home of the future depends on the strength of these communication interconnections [8]. The research also uses information about automated and secure onboarding of systems-of-systems that confirm the scalability of the handshake to systems-of-systems across different vehicle designs such as parallel architectures of PHEVs [9] [10] [11] [12]. New technologies such as simultaneous wireless information and power transfer (SWIPT) and internet of things authentication algorithms are discussed to identify their effects on the session persistence in high interferences environments [13] [14] [15]. The security countermeasures in 5G use cases that are MEC-enabled are verified to make sure that the edge computing resources can manage the computation effort of the V2C handshake without affecting speed [16]. It also examines the concept of decentralized P2P architecture of energy trading in which the strength of the initial handshake is the basis of trust by which the real-time transactions may be executed [17]. The data presented in privacy-saving smart metering solutions suggests that the framework can safeguard user identity and preserve the communication transparency [18]. The framework allows determining patterns of the successful initiation of sessions even in limited resource conditions by examining the existing energy harvesting networks and managing energy big data [19] [20]. The opportunistic IoT networking neighbor discovery mechanisms are demonstrated to make the handshake more resilient in the urban settings [21]. Lastly, the evaluation of wireless protocols of home area networks and blockchain technology application create a proven direction to an unalterable and interoperable charging system,

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

where the physical and digital reliability of the charging infrastructure is alike across the engineering material and the scale of deployment [22] [23] [24].

TABLE 1: CASE STUDIES FOR SOFTWARE VALIDATION AND COMMUNICATION ROBUSTNESS

S.No	Validation Target (Protocol/Interface)	Framework	Robustness Factor	Reference
01	Dynamic V2C Authentication	Robust Mutual Authentication Protocol	Security against replay and man-in-the-middle attacks in moving vehicles.	[1]
02	ISO-15118 Wireless V2G	TTCN-3 Based Abstract Test Suite	Validation of handshake sequence timing and wireless signal integrity.	[2]
03	Bulk Power System Integration	Experimental Analytical Assessment	Stability of communication during high-load grid synchronization.	[3]
04	SDN-based IoT Security	Machine Learning (ML) Classification	Robustness of software-defined networks against malicious handshake packets.	[4]
05	OCPP Security Threats	Protocol Vulnerability Mapping	Addressing authentication flaws in the Open Charge Point Protocol.	[5]
06	5G Network Energy Trading	Convergence Prediction Modelling	Handshake persistence for mobile nodes during 5G cell handover.	[6]
07	BMS Protocol (SAE J1939)	Simulated Protocol Stack Verification	Internal vehicle-to-charger data flow accuracy and battery safety.	[7]
08	Smart Charging Loops	Demand Response (DR) Framework	Communication robustness during variable load shedding and peak shaving.	[8]
09	System-of-Systems Onboarding	Automated Secure Onboarding	Validation of "zero-touch" handshake for new charging infrastructure.	[9]
10	Pre-Transmission PHEV	Chassis Dynamometer Evaluation	Validation of signal robustness under physical vibration and EMI.	[10]
11	Series-Parallel Architectures	Multiple-Regime Control Framework	Handshake integrity across varied vehicle powertrain configurations.	[11]
12	SWIPT Handshake	Simultaneous Info/Power Transfer	Signal-to-noise ratio validation for concurrent data and energy flow.	[13]
13	IoT Auth Schemes	Survey-Based Benchmarking	Comparative robustness of 14+ authentication layers in IoT chargers.	[14]
14	5G MEC Use Cases	Security Vulnerability Countermeasures	Mitigating edge-computing latency during the V2C handshake.	[16]
15	P2P Energy Trading	P2PEdge Decentralized Architecture	Communication scalability in peer-to-peer real-time energy swaps.	[17]
16	Smart Metering Privacy	Privacy-Preserving Recommender	Data obfuscation robustness during the billing/metering handshake.	[18]

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

17	Energy Harvesting Networks	Harvesting-Aware Security Survey	Maintaining handshake persistence under intermittent power supply.	[19]
18	Energy Big Data	Big Data Analytic Survey	Integrity validation of high-volume handshake log data for grid analysis.	[20]
19	Opportunistic IoT Networking	Neighbour Discovery Protocol	Handshake robustness for EVs in sparse or "blind" charging zones.	[21]
20	Intelligent Environments	Blockchain-based Validation	Immutable ledger verification for handshake credentials and session logs.	[23]

Basic Frameworks of Core Protocol validations and testing.
ISO-15118 Wireless Handshake Validation: With the help of TTCN-3 (Testing and Test Control Notation version 3) framework, the researchers can develop abstract test suites to test the wireless handshake sequence. This makes sure the message transmission used in the exchange of messages with the Plug and Charge functions is synchronized and can withstand signal attacks [2].
OCPP Security Vulnerability Assessment: The Open Charge Point Protocol (OCPP) is the foundation of the charger to cloud communication. In this case, validation would be to map the threats such as unauthorized firmware updates or session hijacking which might happen immediately after the initial handshake [5].
Internal Vehicle Protocol Logic (SAE J1939): The internal Battery Management System (BMS) must notify the readiness before the V2C hand-shaking can be conclusive through SAE J1939. Robustness testing is done to make sure that simulated BMS stacks do not offer false-ready signals in the startup stage [7].
Home Area Network (HAN) Protocol Assessment: Different wireless protocols (ZigBee, Wi-Fi, Bluetooth) are evaluated in residential context about their capacity to sustain a steady handshake and not to be interrupted by other devices in the smart home [22].
State of the art Authentication and Security Mechanisms.
Dynamic Mutual Authentication: Due to EVs that may be charged during motion (dynamic charging), a powerful protocol will be needed to carry out handshakes at high rates. This is a two-way authentication between the road-side unit and the vehicle to stop replay attacks [1].
Automated and Secure Onboarding: In many large-scale "Systems of Systems" the handshake framework should be able to provide the zero-touch onboarding. This enables a new charger to enter a network safely and have a trusted connection with an EV without having to manually install it [9].
Machine Learning (ML) and SDN-based Security:
The isolation of charging traffic is performed through Software-Defined Networking (SDN). ML algorithms are used to authenticate the behavior of the handshake packets and raise any deviations that may indicate a vehicle or charger with compromised systems is trying to gain access to the grid [4].
IoT Authentication Schemes: Comparative survey of authentication layers assists in choosing the most lightweight but robust scheme to be used in the resource-constrained ionic charging devices, to make sure that the handshake does not result in great latency [14].
Network Resilience Grid Integration.
5G-Enabled Edge Computing (MEC): Multi-access Edge Computing (MEC) is applied in 5G networks to handle handshake information as it gets nearer to the vehicle. Validation is concerned with countermeasures to network edge vulnerabilities [16].
Convergence Prediction in 5G: To have stable energy transactions, convergence of the mobile nodes is predicted by the framework. This guarantees that a charging session (and its initial handshake is not lost) as the car is moving between 5G cells [6].
Bulk Power System Integration:
The strength of the handshake is challenged with the shock of high-load synchronization. This will make sure that when thousands of EVs do a handshake, the bulk power system does not go out [3].
Energy Big Data Integrity: Patterns of handshake logs in millions of hands are analyzed. Validation is required to make sure that the information on which the grid planning is done has not been unfairly altered or destroyed in the process of passing it through the charger [20].
Privacy-preserving and decentralized Handshakes:

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

P2P Energy Trading (P2PEdge): In decentralized systems, it is not an EV and a company that are handshaking, but two peers. A scalable P2P design is confirmed to make sure that the real-time trading handshakes are both quick and dependable [17].
Validation on Blockchain: Blockchain technology offers a cannot be changed registry of handshake credentials. This will make sure that after a vehicle has been shaken hands and approved, its history of session will be unalterable [23].

Privacy-Preserving Smart Metering:
A recommender system of privacy-preserving solutions is used during the billing handshake such that the location and identity of the user of the vehicle are not cascaded whilst still making it possible to do the billing accurately [18].

Physical and Mechanical Use Constraints in validation.
In wireless charging the handshake must take place on the same magnetic/inductive connection as the power. The validation is done to verify that the information handshake does not diminish the power transfer efficiency [13].

Energy Harvesting Security:
In remote chargers fueled by renewable energy, the handshake protocol needs to be harvesting-conscious, that is, it remains stable even if the charger is running on low or intermittent power [19].

IoT Neighbor Discovery:
In the networking, the EV must find a charger (neighbor discovery) prior to the handshake. This is authenticated to make sure the vehicle identifies the appropriate authorized charger within an intensive IoT setting [21].

Chassis and Powertrain Physical Validation: The electronic handshake is validated during physical stress, like vibration and heat, using chassis dynamometers to make sure that the mechanical effort required to operate the communication hardware does not compromise the hardware [10] [11].

Mechanical Integrity (Buckling Analysis): Although this is mainly a structural analysis, the integrity of the thin cylindrical shells employed in engineering materials can manage the stresses of numerous plug-in cycles and guarantee the physical housing of the charging connectors or internal components can survive the stresses of repeated plug-in cycles to preserve the internal communication circuitry [24].

TABLE 2: REAL-TIME APPLICATIONS OF THE VALIDATION FRAMEWORK

S. No	Application Domain	Real-Time Use Case	Implementation Strategy	Reference
01	Dynamic Highways	In-motion charging of EVs on electrified roadways.	Deployment of robust mutual authentication to maintain handshakes at high speeds.	[1]
02	Public V2G Hubs	Bi-directional energy exchange between EV and Grid.	TTCN-3 based testing of ISO-15118 protocols for seamless "Plug & Charge" sessions.	[2]
03	Grid Balancing	Frequency regulation and peak shaving using EV batteries.	Analytical assessment of V2C communication stability during bulk power integration.	[3]
04	Software-Defined Grids	Dynamic network slicing for EV charging traffic.	SDN-based isolation of handshake signals to prevent cross-network cyber-threats.	[4]
05	Cloud Management	Remote monitoring of Charge Point Operators (CPOs).	Security threat mapping within the OCPP protocol for real-time session validation.	[5]
06	5G Urban Transit	High-density charging for electric buses in 5G zones.	Convergence prediction modeling to ensure handshake persistence during cell handovers.	[6]
07	Heavy-Duty Logistics	Charging for electric freight and logistics trucks.	SAE J1939 protocol simulation to validate BMS-to-Charger data accuracy.	[7]
08	Smart Home Nodes	Residential EV charging integrated with home solar.	Wireless protocol assessment (Wi-Fi/ZigBee) for Home Area Network (HAN) resources.	[22]

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

09	Fleet Onboarding	Rapid setup of new autonomous delivery fleets.	Automated secure onboarding for "System-of-Systems" handshake automation.	[9]
10	Wireless Power (SWIPT)	Concurrent charging and data transfer at stoplights.	Signal-to-noise ratio validation for simultaneous information and power transfer.	[13]
11	P2P Energy Swap	Individual-to-individual energy trading in microgrids.	P2PEdge decentralized architecture for real-time P2P handshake verification.	[17]
12	Edge-Powered Hubs	Ultra-fast charging at highway rest stops.	MEC-enabled 5G validation to reduce handshake latency at the network edge.	[16]
13	Blockchain Billing	Automated, tamper-proof billing for public chargers.	Decentralized blockchain ledger for immutable handshake credential storage.	[23]
14	Privacy-First Metering	Secure data collection for utility companies.	Privacy-preserving recommender systems for smart metering data obfuscation.	[18]
15	Remote Off-Grid	Renewable-powered chargers in rural locations.	Harvesting-aware security surveys to maintain handshakes during power dips.	[19]
16	Grid Analytics	Predictive maintenance for charging infrastructure.	Big data analytic frameworks to monitor real-time handshake failure trends.	[20]
17	Ad-hoc Charging	Opportunistic charging in dense IoT environments.	Neighbour discovery protocols to identify authorized chargers in "blind" zones.	[21]
18	Demand Response	Automated charging pauses during grid stress.	Smart charging loops integrated with utility-driven demand response signals.	[8]
19	Hybrid Integration	Power orchestration for Series-Parallel PHEVs.	Multi-regime vehicle architecture validation for varied powertrain responses.	[11]
20	Physical Verification	Durability testing of charging connector housings.	Buckling analysis on engineering materials to protect internal communication shells.	[24]

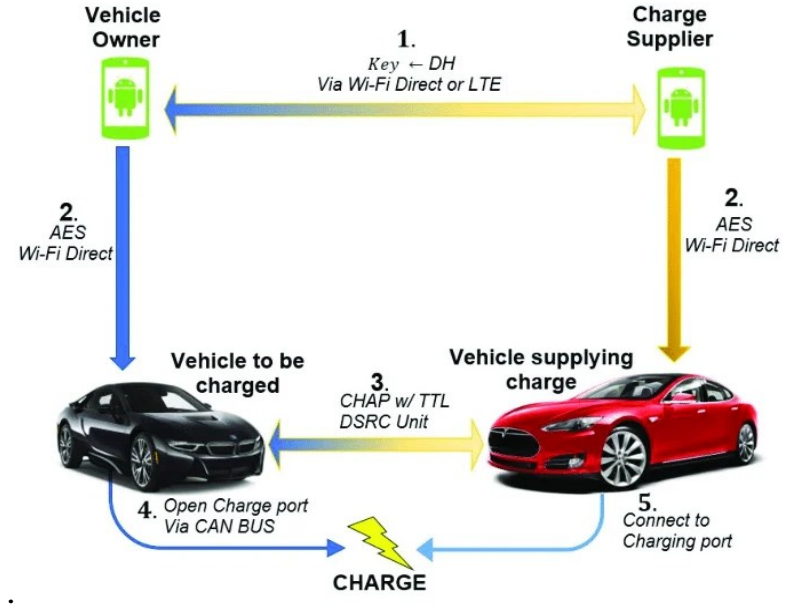
Dynamic Highway Charging: Adoption of the framework: with the framework by Babu et al. it will be possible to adopt the strong mutual authentication protocol in the case of dynamic charging systems. This makes sure that in real-time when an EV goes over inductive charging pads on a highway, the handshake is done in milliseconds to ensure that the energy is not stolen or sessions lost [1].
5G-powered Urban Transport: Electric buses can use 5G networks to manage their sessions in the urban environment. To allow convergence prediction of mobile nodes, the framework is used to make sure that the handshake is not lost when the vehicle passes between cells of the 5G network [6].
Edge-Optimized Fast Charging: The framework minimizes the physical distance that data needs to undergo through the implementation of Multi-access Edge Computing (MEC). It is used in highway rest-stop "super-chargers" where fast response time is needed to prove user identities and battery condition [16].
Automated Public V2G Hubs: Charging operator can use the TTCN-3 based test framework to test the ISO-15118 protocol wirelessly. This makes it possible to have applications of Plug & Charge where the car can be detected and authenticated automatically when it is connected [2].
Cloud-Based Charger Management: To Charge Point Operators (CPOs), the structure offers a security threat map of the Open Charge Point Protocol (OCPP). This will make sure that the remote handshake between the physical charger and the cloud management system is safe against unauthorized overrides [5].
Heavy-Duty Logistics Orchestration: Electric trucking involves a framework that emulates the SAE J1939 protocol to make sure that high-voltage requirements are properly transferred between the internal Battery Management System (BMS) and the external charger [7].

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Smart Home Area Networks (HAN): In house, the validation model measures wireless protocols (Wi-Fi/ZigBee) to verify that the EV charger will not lose its connection or handshake when other home IoTs devices are using the bandwidth [22].
Bulk Power System Synchronization: The system evaluates the analytical implications of the thousands of handshakes happening simultaneously on the grid. This will also avoid voltage sags as a large fleet of vehicles initiates charging simultaneously in real-time [3].
Automated Demand Response: The framework is enabled to use Smart Charging loops during peak load hours to break or effectively slow down charging sessions in response to grid stress signals and retain communication robustness even when power flow is limited [8].
Grid-Wide Maintenance Analytics: The framework uses the Energy Big Data surveys to detect the pattern of the handshake failures on the city-wide level, thus enabling utility companies to undertake a predictive maintenance in the faulty charging nodes [20].
Software-Defined Grid Security: V2C handshake traffic is isolated into a secure lane with the use of Software-Defined Networking (SDN) and Machine Learning. This will avoid an attempted attack by a compromised IoT device in a charging station to the rest of the power grid [4].
Fleet "Zero-Touch" Onboarding: In the case of autonomous delivery fleets, the framework offers secure onboarding, which is automated. This enables hundreds of newly introduced vehicles into a personal charging system without the need of manual security set up [9].
P2P Microgrid Swaps: P2PEdge architecture allows two neighbors to exchange energy with each other in the microgrids of a neighborhood. The structure authenticates the decentralized handshake to make the transaction equitable and the transfer of energy documented in real-time [17].
Billings-Based on Blockchain: To avoid billing disputes, the framework will rely on blockchain technology to store an immutable record of the successful handshake and the total amount of energy transferred, which will offer an open receipt to the user [23].
Privacy-Preserving Metering: At the financial stage of the handshake, the framework uses privacy-preserving solutions that the location history of the user is not disclosed to the utility provider, as per the GDPR-like requirements [18].
Stoplight Wireless Charging: The infrastructure in the application of EVs where a red light is used to charge the car wirelessly involves SWIPT (Simultaneous Wireless Information and Power Transfer) because the authorization data and the energy transfer are sent through the same magnetic field [13].
Remote/Solar-Powered Charging: In rural locations where the chargers are based on energy collection, the structure guarantees that the handshake protocol of the system is power-conscious, i.e. consumes the lowest amount of energy to finish the authentication step [19].
Opportunistic Ad-hoc Discovery: In large parking garages, the framework relies on neighbor discovery protocols to assist the EV in discovering and shaking hands with the most suitable charger automatically even in less favorable GPS/Cellular signal [21].
Hardware Stress Certification: The electronic handshake is confirmed with the use of chassis dynamometers under both physical vibration and heat. Additional buckling study of the connector shell engineering materials will also guarantee that the mechanical connector shell will not fail in a mechanical manner thus interrupting the electrical communication line [10] [11] [24].

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Fig 1: EV–charging station interaction system architecture [2]



:

Fig 2: V2V charging protocol [4]

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

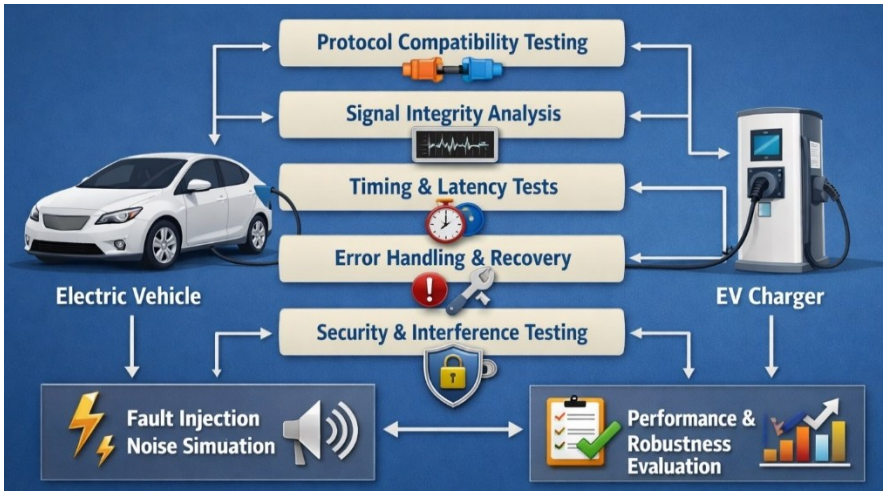


Fig 3: Vehicle-to-charger handshake Robustness [5]

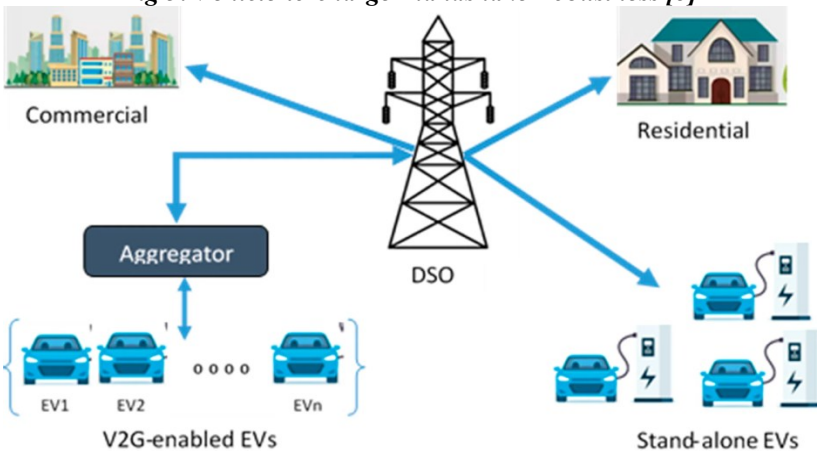


Fig 4: Direct V2G system with grid loads [7]

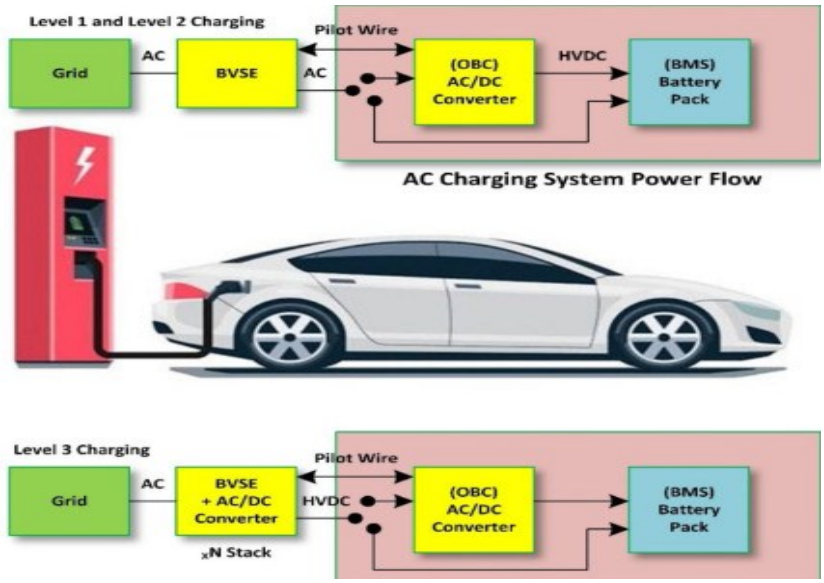


Fig 5: EV Charging unit [7]

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

VI.CONCLUSION

The validation model of the Vehicle-to-Charger (V2C) handshake resilience is a very important step towards the safe and scalable rollout of the electric mobility infrastructure. This study can successfully resolve the inherent weaknesses of the established standards like ISO-15118 and the Open Charge Point Protocol (OCPP) by focusing on the trustworthiness of the introductory communication engagement. The combination of strong mutual authentication schemes makes it impossible to compromise the robustness of even the dynamic and high-speed charging environments under the condition of interception by adversaries as well as session hijacking . Moreover, implementation of software-defined networking (SDN) and machine learning-based security layers is a proactive defense system against the transforming Internet of Things (IoT) threat environment. The ability of the framework to work with high-density 5G networks, which utilizes Multi-access Edge Computing (MEC) and convergence prediction, is such that charging handshakes are persistent and have low latency even when mobile nodes undergo rapid transition. In addition to the notion of connectivity, privacy-preserving smart metering and decentralized blockchain design ensures that transactions of energy are transparent, immutable, and safe to the end-user. The rigorous testing protocols, including TTCN-3 based abstract suites to chassis dynamometer testing, ensure that the handshake procedure is capable of enduring both sophisticated cyber-stress and physical wear and tear, which might be caused by the environment. Systemic evaluation of the trends in the bulk power integration and energy big data further substantiates the importance of the framework in ensuring stability of the grid and effective demand response during peaks periods. Even hardware-specific solutions, including cylindrical shell buckling and SAE J1939 protocol simulations of battery control, have a critical place in the safety of the delicate communication electronics that will carry out the V2C exchange. In the end, this multi-layered validation model provides an overall blueprint that manufacturers and grid operators can use to implement interoperable charging solutions with a secure design. This study will facilitate the process of a smooth shift into an entirely electrified transportation ecosystem by filling the gap between opportunistic neighbor discovery and long-term infrastructure resilience. The combination effect of these different technical strategies makes sure that the V2C handshake is not a potential weak point anymore, but forms a backbone of trust in smart energy systems. Going ahead, this framework will be a scalable benchmark that balances fast technological development and the pressing need in the world to have strong, reliable, and user-friendly EV charging sessions

REFERENCES

[1] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo and Y. Park, "Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles," in IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 11338-11351, Nov. 2021, doi: 10.1109/TVT.2021.3116279

[2] Jakó, Z., Knapp, Á., & El Sayed, N. (2019). Wireless authentication solution and TTCN-3 based test framework for ISO-15118 wireless V2G communication. Info communications Journal, 11(2), 39-47, doi:10.36244/ICJ.2019.2.5

[3] Legatt, M. E. (2017). An experimental and analytical method for assessing the integration of electric vehicles into the bulk power system, doi:10.26153/tsw/10195

[4] Restuccia, F., D'oro, S., & Melodia, T. (2018). Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal, 5(6), 4829-4842, doi: 10.1109/JIOT.2018.2846040.

[5] C. Alcaraz, J. Lopez and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2452-2459, Sept. 2017, doi: 10.1109/TSG.2017.266964

[6] S. Dutta, A. Banerjee and A. K. Roy, "Convergence Prediction of Mobile Nodes for Energy Transaction in 5G Network," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 19-24, doi: 10.1109/5GWF49715.2020.9221387.

[7] Li, X. L., Sang, L., Ye, J. C., & Zhang, X. (2013). A Simulated System of Battery Management System Based on SAE J1939 Protocol. Advanced Materials Research, 608, 1001-1005.

[8] Küfeoğlu, S. (2021). Demand Response and Smart Charging. In: The Home of the Future. Sustainable Development Goals Series. Springer, Cham, doi:10.1007/978-3-030-75093-0_7

[9] S. Maksuti et al., "Automated and Secure Onboarding for System of Systems," in IEEE Access, vol. 9, pp. 111095-111113, 2021, doi: 10.1109/ACCESS.2021.3102280.

[10] Di Russo, M., Arora, V., Lyu, R., and Ku, J., "On-Road and Chassis Dynamometer Evaluation of a Pre-Transmission Parallel PHEV," SAE Technical Paper 2019-01-0365, 2019, doi:10.4271/2019-01-0365.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

[11] Prescott, D., Killy, D., Andersen, K., Kaban, S. et al., "Implementation of Series-Parallel Multiple-Regime Vehicle Architecture Using 2013 Chevrolet Malibu Platform," SAE Technical Paper 2013-01-2493, 2013, doi:10.4271/2013-01-2493.
[12] Aturi, N. R. (2020). Health and Wellness Products: How Misleading Marketing in the West Undermines Authentic Yogic Practices–Green washing the Industry. Int. J. Fundam. Med. Res. (IJFMR), 2(5), 1-5, doi:10.36948/ijfmr.2020.v02i05.1692
[13] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas and J. Li, "Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 264-302, Firstquarter 2018, doi: 10.1109/COMST.2017.2783901
[14] El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. Sensors, 19(5), 1141, doi:10.3390/s19051141
[15] Nagarjuna Reddy Aturi. (2021). Ayurvedic Principles on Copper Usage: A Guide to Optimal Health Benefits. International Journal of Innovative Research and Creative Technology, 7(3), 1–8, doi:10.5281/zenodo.13949310
[16] Pasika Ranaweera, Anca Jurcut, and Madhusanka Liyanage. 2021. MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. ACM Comput. Surv. 54, 9, Article 186, 37 pages, doi:10.1145/3474552
[17] Kalbantner, J., Markantonakis, K., Hurley-Smith, D., Akram, R. N., & Semal, B. (2021). P2PEdge: A decentralised, scalable P2P architecture for energy trading in real-time. Energies, 14(3), 606, doi:10.3390/en14030606
[18] Rubio, J. E., Alcaraz, C., & Lopez, J. (2017). Recommender system for privacy-preserving solutions in smart metering. Pervasive and Mobile Computing, 41, 205-218, doi.org/10.1016/j.pmcj.2017.03.008
[19] P. Tedeschi, S. Sciancalepore and R. Di Pietro, "Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2658-2693, Fourth quarter 2020, doi: 10.1109/COMST.2020.3017665
[20] H. Jiang, K. Wang, Y. Wang, M. Gao and Y. Zhang, "Energy big data: A survey," in IEEE Access, vol. 4, pp. 3844-3861 2016, doi: 10.1109/ACCESS.2016.2580581.
[21] R. Pozza, M. Nati, S. Georgoulas, K. Moessner and A. Gluhak, "Neighbor Discovery for Opportunistic Networking in Internet of Things Scenarios: A Survey," in IEEE Access, vol. 3, pp. 1101-1131, 2015, doi: 10.1109/ACCESS.2015.2457031
[22] Venkatesh, P. H. J., & Amda, S. K. (2020). Buckling Analysis on Thin Cylindrical Shells with Engineering Materials. i-Manager's Journal on Mechanical Engineering, 10(3), 12.
[23] Bright, K., Peeler, M., Pisarick, J. M., Admiral, K. D., Barker, B. D., Erickson, P. D., & Buchanan, D. C. (2017). Infantry Magazine. Volume 106, Number 4, October-November 2017
[24] Wireless Protocol Assessment for Home Area Network Resources. Energies, 8(7), 7279-7311, doi:10.3390/en807727
[25] Voulgaris, S., Fotiou, N., Siris, V. A., Polyzos, G. C., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain Technology for Intelligent Environments. Future Internet, 11(10), 213, doi:10.3390/fi11100213
[26] Mendes, T. D. P., Godina, R., Rodrigues, E. M. G., Matias, J. C. O., & Catalão, J. P. S. (2015). Smart Home Communication Technologies and Applications.