Cybersecurity Challenges in the EV Charging Ecosystem

AMANJOT KAUR[*], NIMA VALIZADEH[*], DEVKI NANDAN JHA[†], TOMASZ SZYDLO[†], JAMES R. K. RAJASEKARAN[‡], VIJAY KUMAR[*], MUTAZ BARIKA[†], JUN LIANG[*], RAJIV RANJAN[†], and OMER RANA[*], Cardiff University, UK, Newcastle University, UK, and Northumbria University, UK

The growing adoption of intelligent Electric Vehicles (EVs) has also created an opportunity for malicious actors to initiate attacks on the EV infrastructure, which can include a number of data exchange protocols across the various entities that are part of the EV charging ecosystem. These protocols possess a range of underlying vulnerabilities that attackers can exploit to disrupt the regular flow of information and energy. While researchers have considered vulnerabilities of particular components within an EV charging ecosystem, there is still a notable gap in vulnerability analysis of charging protocols and the potential threats to these. We investigate threat vectors within the most widely adopted protocols used in EV infrastructure, explore the potential impact of cyberattacks and suggest various mitigation techniques investigated in literature. Potential future research directions are also identified.

CCS Concepts: • **Computer systems organization → Embedded and cyber-physical systems**; **Cloud computing**; • **Security and privacy → Network security**; **Security in hardware**; • **Networks → Network protocols**.

Additional Key Words and Phrases: Cybersecurity, Charging Station, Electric Vehicle, Power Grid

ACM Reference Format:
Amanjot Kaur, Nima Valizadeh, Devki Nandan Jha, Tomasz Szydlo, James R. K. Rajasekaran, Vijay Kumar, Mutaz Barika, Jun Liang, Rajiv Ranjan, and Omer Rana. 2023. Cybersecurity Challenges in the EV Charging Ecosystem. *J. ACM* 37, 4, Article 111 (December 2023), 32 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

In recent years, the global transportation landscape has undergone a transformative shift towards electric vehicles (EVs), driven by environmental concerns and a desire to reduce dependence on conventional fossil fuels. There have also been significant global investments in charging infrastructure to support this transition to EVs, with all major vehicle vendors now including EVs in their portfolio. This transition, however, brings forth a myriad of challenges, particularly in the realms of security and infrastructure. This paper surveys existing protocols employed in EV charging infrastructure, covering key features and vulnerabilities in the most widely used protocols. Various cyberthreats and attacks on EVs have been reported [4, 46], raising questions about the robustness of the protocols in place.

Authors' address: Amanjot Kaur, KaurA7@cardiff.ac.uk; Nima Valizadeh, ValizadehN@cardiff.ac.uk; Devki Nandan Jha, dev.jha@ncl.ac.uk; Tomasz Szydlo, tomasz.szydlo@ncl.ac.uk; James R. K. Rajasekaran, james.rajasekaran@northumbria.ac.uk; Vijay Kumar, kumarv14@cardiff.ac.uk; Mutaz Barika, mutazb999@gmail.com; Jun Liang, liangj1@cardiff.ac.uk; Rajiv Ranjan, raj.ranjan@ncl.ac.uk; Omer Rana, RanaOF@cardiff.ac.uk, Cardiff University, Cardiff, UK and Newcastle University, Newcastle upon Tyne, UK and Northumbria University, Newcastle upon Tyne, UK.

The research methodology included searching various databases, including the ACM Digital Library, ScienceDirect, IEEEXplore, Web of Sciences, Elsevier and Google Scholar. Keywords and phrases employed in the search process comprised terms such as "Protocols," "ISO 15118," "OCPP," "OSCP," "OpenADR," "OCPI," "Vulnerabilities," "Cyberattacks in protocols," "Charging Infrastructure," and "Charging Ecosystem." The phrase "Electric Vehicle (EV)" was added to all previous keyword searches. We analysed research papers focusing on communication protocols and cyberattacks within the EV charging ecosystem. These papers were organized based on communication protocols, functionalities, types of cyberattacks, detection and mitigation strategies and interoperability between diverse protocols. While some research papers did not explicitly specify the vulnerabilities of the identified protocols, the majority were focusing on one protocol only. In this survey we focus on the most widely used protocols, associated vulnerabilities within an EV charging ecosystem, and emphasise how an attack on one protocol can propagate/ cascade towards other components and sub-systems of the EV charging ecosystem.

This paper makes the following contributions: (i) survey of existing communications protocols within the EV charging ecosystem; (ii) review of cyberattacks on EV charging infrastructure; (iii) mechanisms to enhance the security of protocols and connectivity between components in an EV charging infrastructure; (iv) a comparison of currently available simulators for EV charging infrastructure, highlighting their characteristics, capabilities, and limitations in testing communication protocols identified in (i)–(iii). The remainder of the paper is structured as follows: Section 2 provides the background and context of the EV charging infrastructure. In Section 3, a description of EV charging protocols is presented, describing their key functions and their associated vulnerabilities. Section 4 extends this discussion with additional attack vectors associated with these protocols. Section 5 identifies simulators available for these communication protocols. Section 6 provides a summary of key findings and outlines future research directions. The paper concludes with final remarks in Section 7.

1.1 Comparison with Existing Surveys

While numerous research papers have investigated vulnerabilities within EV charging infrastructure, understanding vulnerabilities within communication protocols associated with charging infrastructure remains a gap. This article focuses on the most widely used communication protocols employed across different components of the EV charging infrastructure. By consolidating scenarios previously dispersed across research papers, this paper aims to serve as a valuable resource for individuals seeking an expansive understanding of cyber threats across the EV charging ecosystem (EV to power grid). Table 1 is included to illustrate the information gathered from prior survey papers and highlights key differences in our approach.

2 EV CHARGING INFRASTRUCTURE

Charging electric vehicles (EV) is a complex process that involves several key entities, including the EV itself, charging stations, charge point operators, aggregators, e-Mobility Service Providers (eMSPs), and distribution system operators (DSO)/transmission system operators (TSO). The complex interaction among these entities is governed by specific protocols tailored to the unique requirements of EV charging. A schematic diagram showing the complex interactions among the entities is illustrated in Fig. 1. Table 2 provides a list of acronyms used throughout the paper.

EV may be fully electric or hybrid that use an electric propulsion system and an internal combustion engine. Some hybrid vehicles, called plug-in Hybrid EV (PHEV), may include a charging socket for the internal battery. EVs are charged through the charging Station (CS) that allows electricity to be pulled from the hardwired power grid and delivered to directly connected EVs to recharge their batteries. Depending on the type of the charging station, they might provide different charging

Table 1. Comparison of survey papers focusing on communication protocols in the EV charging ecosystem

Paper	Protocol					Focus
	ISO-15118	OCPP	OCPI	Open ADR	OSCP	
[10]		✓				Focused only on OCPP
[38]		✓		✓		Specified only OCPP-OpenADR compatibility
[69]	✓	✓		✓		Did not cover security aspects
[47]	✓	✓	✓	✓	✓	Detailed analysis lacking
[5]	✓	✓		✓		Surveyed from grid perspective
[85]	✓	✓	✓	✓	✓	Brief overview of EV protocols
[31]	✓	✓	✓			Overview on EV charging ecosystem
[72]	✓	✓		✓		Security vulnerabilities overview
[89]	✓	✓	✓	✓		Explored Roaming Protocols
[66]	✓	✓		✓		Overview of privacy and security challenges
Proposed	✓	✓	✓	✓	✓	Coverage of EV charging protocol

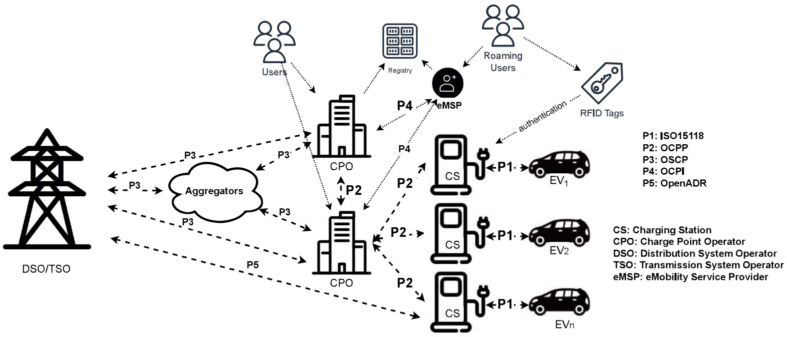

Fig. 1. Collaboration diagram for the entities in the end-to-end EV charging infrastructure

characteristics. An AC charging station uses AC voltage to charge EVs over several hours, while a DC charging station provides fast charging capability to charge EVs during a short time period. EV communicates with the CS via the charging cable using power line communication (PLC) and high-level protocol denoted as P1 in Fig. 1.

Charging points are managed and operated by Charging Point Operators (CPO), responsible for setting up and maintaining physical chargers. This includes selecting suitable locations, installing the necessary equipment, and ensuring that charging stations work properly. Management of the charging stations is performed using the Open Charge Point Protocol (OCPP) denoted as P2 in Fig. 1. In cases where the same CPO operates multiple charging stations, they often manage a network of charging stations. Users can interact with CPOs directly using dedicated mobile applications.

The e-MSP is a company an electric vehicle (EV) driver contacts for all services related to electric charging. The e-MSP issues charging passes or RFID cards that allow EV drivers to access and use charging stations within the e-MSP's network. The e-MSP is responsible for billing and invoicing EV drivers for charging sessions. They may offer different pricing models, such as pay-as-you-go or subscription-based plans. Many e-MSPs have agreements with charging station operators to create a roaming network. The cooperation between eMSP and the CPO is achieved by the Open Charge Point Interface (OCPI) protocol denoted as P4 in Fig. 1. This allows EV drivers to use a single provider's services across multiple charging networks, making it more convenient to charge

Table 2. Nomenclature

Acronym	Meaning	Acronym	Meaning
BEV	Battery Electric Vehicles	CHAdeMO	CHArge de MOve
CPO	Charge Point Operator	CS	Charging Station
CSO	Charging Point Operator	DERs	Distributed Energy Resources
DR	Demand Response	DSO	Distribution System Operator
e-MSP	E-mobility service provider	EMS	Energy Management System
EPs	Energy Providers	EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller	EVSE	Electric Vehicle Supply Equipment
ISO	International Standards Organization		
OCA	Open Charge Alliance	OCPI	Open Charge Point Interface
OCPP	Open Charge Point Protocol	OCSP	Online Certificate Status Protocol
OpenADR	Open Automated Demand Response	OSCP	Open Smart Charging Protocol
PII	Personally Identifiable Information	PHEV	Plug-In Hybrid Electric Vehicles
PKI	Public Key Infrastructure	RFID	Radio Frequency Identification
SECC	Supply Equipment Communication Controller	V2G	Vehicle-to-Grid

their vehicles. This simplifies the usage and payments by EV drivers for chargers from different operators, e.g. by using a single RFID card [1].

To establish and maintain seamless operation during roaming services, the identity of an e-MSP and CPOs are maintained by external registries, usually national ones, e.g. EV Roam (UK), AFIREV (France), EIPA (Poland). Some e-MSPs also provide services aggregating cross-network data (e.g., Zap-Map and Open Charge Map) to provide static and real-time data on charge points. They use OCPI protocol for real-time charge point information, including availability, charging status and maintenance information (e.g. out-of-order stations and planned unavailability). In the OCPI protocol, provider and operator names are used to extract this information. An issuing authority maintains a centralized repository of recognized providers and operators.

Transmission System Operator (TSO) and Distribution System Operator (DSO) are the power grid operators responsible for the distribution of electric power from the generation source to the consumer. This can occur at both high and low voltage levels, depending on types of consumers involved. Energy aggregators are entities responsible for combining demand information from various charging stations, to request energy from the power grid. In this case, these aggregators cooperating in the distributed charging process through V2G, controlling the charging of each EV, and take part in the demand-response of the power grid [23, 78]. They play a crucial role as intermediaries connecting the Distribution System Operator (DSO) with electric vehicles (EVs). Usually, the Open Smart Charging Protocol (OSCP) denoted as P3 in Fig. 1 is used for enabling cooperation. Energy aggregation is commonly used by large commercial and industrial customers with significant energy consumption needs, to enable a mechanism to negotiate a better tariff with an energy provider, reduce risk and make more effective use of green energy.

3 PROTOCOLS

In this section we describe the most widely used protocols in the EV charging ecosystem. Fig. 2 provides an overview of the taxonomy of protocols and vulnerabilities within EV Charging Infrastructure.

3.1 International Organization for Standardization 15118 (ISO 15118)

ISO 15118 ("Road Vehicles – Vehicle to Grid Communication Interface") is an international communications protocol for an EV and a charging station – depicted as *P1* in Figure 1. It defines bidirectional digital communication between EVs, involving Battery Electric Vehicles (BEV) and Plug-In Hybrid Electric Vehicles (PHEV), and Electric Vehicle Supply Equipment (EVSE). ISO 15118

[1] (Competition & Markets Authority. Electric Vehicle Charging Market Study—Final Report 2021)

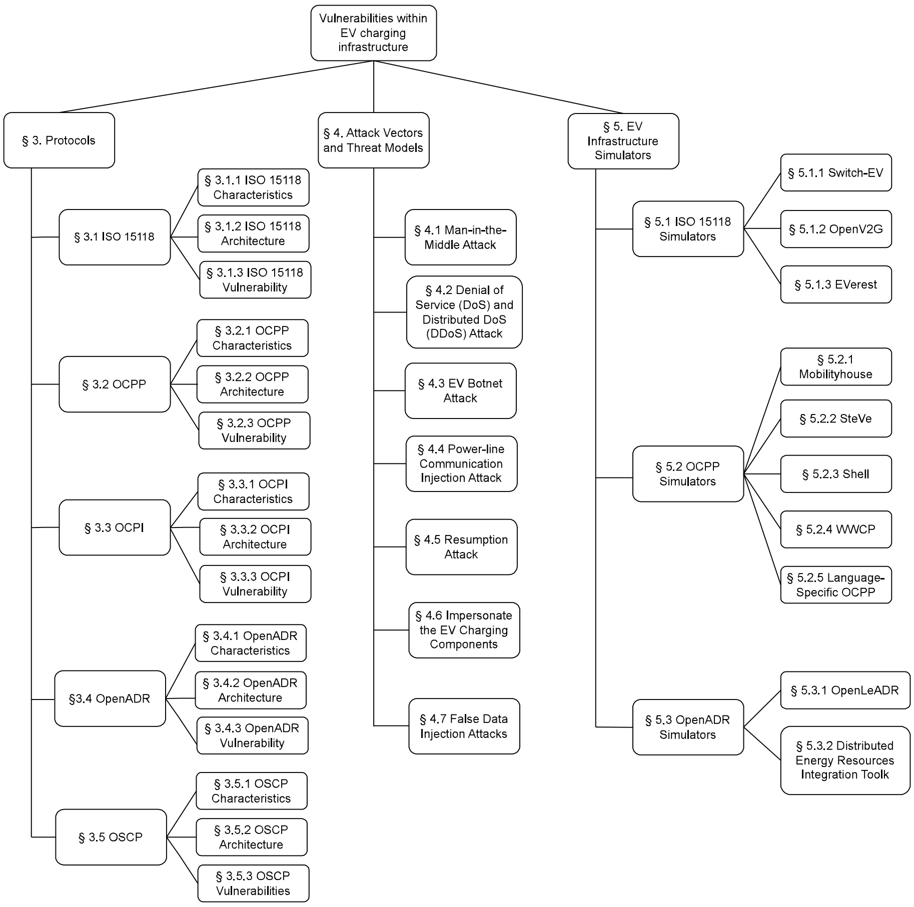
Vulnerabilities within EV charging infrastructure
§ 3. Protocols
§ 4. Attack Vectors and Threat Models
§ 5. EV Infrastructure Simulators
§ 3.1 ISO 15118
§ 3.1.1 ISO 15118 Characteristics
§ 3.1.2 ISO 15118 Architecture
§ 3.1.3 ISO 15118 Vulnerability
§ 3.2 OCPP
§ 3.2.1 OCPP Characteristics
§ 3.2.2 OCPP Architecture
§ 3.2.3 OCPP Vulnerability
§ 3.3 OCPI
§ 3.3.1 OCPI Characteristics
§ 3.3.2 OCPI Architecture
§ 3.3.3 OCPI Vulnerability
§3.4 OpenADR
§ 3.4.1 OpenADR Characteristics
§ 3.4.2 OpenADR Architecture
§ 3.4.3 OpenADR Vulnerability
§ 3.5 OSCP
§ 3.5.1 OSCP Characteristics
§ 3.5.2 OSCP Architecture
§ 3.5.3 OSCP Vulnerabilities
§ 4.1 Man-in-the-Middle Attack
§ 4.2 Denial of Service (DoS) and Distributed DoS (DDoS) Attack
§ 4.3 EV Botnet Attack
§ 4.4 Power-line Communication Injection Attack
§ 4.5 Resumption Attack
§ 4.6 Impersonate the EV Charging Components
§ 4.7 False Data Injection Attacks
§ 5.1 ISO 15118 Simulators
§ 5.1.1 Switch-EV
§ 5.1.2 OpenV2G
§ 5.1.3 EVerest
§ 5.2 OCPP Simulators
§ 5.2.1 Mobilityhouse
§ 5.2.2 SteVe
§ 5.2.3 Shell
§ 5.2.4 WWCP
§ 5.2.5 Language-Specific OCPP
§ 5.3 OpenADR Simulators
§ 5.3.1 OpenLeADR
§ 5.3.2 Distributed Energy Resources Integration Toolk

Fig. 2. Structure of the paper

is created with an interoperability feature, ensuring that EVs and EVSEs from various manufacturers can communicate seamlessly. Moreover, this standard is designed to be adaptable, catering to the needs of both residential and public charging stations. The ISO 15118 protocol functions as a client-server system, with the EV serving as the client and the EVSE as the server. Each of these entities is equipped with its communication controller, the EV utilizing an Electric Vehicle Communication Controller (EVCC) and the EVSE employing a Supply Equipment Communication Controller (SECC). The most commonly embraced versions of the protocol are ISO 15118-2 and ISO 15118-20. Hence, this survey paper concentrates on vulnerabilities within these widely adopted ISO 15118 versions.

3.1.1 ISO 15118 Characteristics. The ISO 15118 protocol exhibits several characteristics that contribute to its effectiveness in standardizing communication within Electric Vehicle (EV) charging systems. The ISO 15118 standard concentrates on the application layer, specifying the messages and procedures essential for secure and efficient communication throughout the charging process.

It does not prescribe the specific transport or internet layer protocols to be used. The characteristics of ISO 15118 include: (i) **Automated authentication & authorization:** offers two authentication methods: the External Identification Mechanism (EIM) and the more user-friendly Plug and Charge (PnC). With EIM, users are required to authenticate using RFID tags, QR code scanning, debit/credit cards, or charging applications. In contrast, PnC simplifies authentication by employing digital certificates, supporting billing processes between the EV and the EVSE (charging station), eliminating the need for external identification methods like RFID tags. (ii) **Wireless Power Transfer (WPT):** enables automatic and contactless charging, eliminating the need for physical cables and connectors. (iii) **Bidirectional Power Transfer (BPT):** encompasses bidirectional power capabilities, also known as Vehicle-to-Grid (V2G) functionality, enabling EVs to both receive from and feed back power into the grid (or supply power to a home/ building). (iv) **Automated Connection Device (ACD):** provides components supporting the automatic connection and disconnection process for conductive energy transfer between an EV and an EVSE, e.g. use of an ACD device to charge an electric bus through a pantograph.

ISO 15118-2 introduced the concept of Plug & Charge, facilitating seamless authentication and payment without user intervention [36]. ISO 15118-20 builds upon this foundation by incorporating advanced functionalities such as bidirectional charging (vehicle-to-grid, V2G), faster communication protocols, and enhanced security measures [44].

3.1.2 ISO 15118 Architecture. The ISO 15118 protocol defines a robust and standard (interoperable) architecture for communication within EVSE. There are two key components within this architecture, the Electric Vehicle Communication Controller (EVCC) and the SECC (Supply Equipment Communication Controller). The EVCC, embedded within the EV, acts as the communication hub, facilitating secure and standardized data exchange with a charging station. On the other hand, the SECC manages the power supply and communication with the EV. EVCC and SECC adhere to a client-server protocol, with EVCC functioning as the client and SECC serving as the server. These components enable EVCC and EVSE to engage in secure, automated communication to initiate and authorize the charging process without requiring additional user input. They exchange mutual charging limits and a charging schedule via message request-response pairs. There are different message sequences involved between both entities Both EVCC and SECC transmit various charging technical parameters to SECC, including $departure\_time$, $maximum\_current\_limit$, $maximum\_voltage\_limit$, $full\_soc$, $energy\_request$, and more [29]. Using these exchanged parameters, a charging schedule is established, which can be renegotiated.

3.1.3 ISO 15118 vulnerability. This segment raises concerns regarding conceptual flaws inherent in the formulation and structure of the ISO 15118 standard.

Trusted environments. ISO-15118-2/20 suggests mandatory use of Transport Layer Security (TLS) for all communication between the charging station and the vehicle, except in trusted environments [47]. The standard defines a trusted environment as a 'closed user group' possessing pre-issued tokens for accessing the SECC charging service. This could encompass scenarios like home garages with physical keys or RFID tokens for car sharing. Consequently, TLS is not obligatory when the charger serves a limited group of EVs with external authentication methods. This exemption exposes communication in safe environments to tampering or manipulation, allowing malicious activities. Another concern arises from the possibility of incorrect implementations or errors leading to the use of vulnerable versions of TLS. Exploitation of weaknesses present in older TLS versions could compromise communication security. Bao et al. suggest fully eradicating the concept of trusted environments [19]. They argue that optional security solutions tend to trigger implementation errors and misconfigurations. Instead, they advocate making TLS mandatory in all circumstances.

Unimodal authorization. The authorization mechanisms outlined in the ISO 15118 standard operate in a unimodal manner. For example, within the PnC mode, the authentication process exclusively validates the authenticity of the legitimate EV itself. The modes for EIM are– smartphone app, credit card, RFID card or a license plate scanning at a charging station. For PnC– the method works with an asymmetric key algorithm supported by a public key infrastructure (PKI) and certificates stored in the EV and EVSE. Conversely, the EIM focuses solely on authenticating the genuine EV user. Consequently, situations can arise where an illegitimate EV could misuse a valid EV user's smart card to initiate charging, or an EV possessing a valid digital certificate might gain charging privileges even in cases where the driver is not authorized. Current approaches to authentication and authorization in current EV charging networks prominently depend on RFID smart cards. Given that these authentication methods are unimodal and single-channel in nature, their level of security remains comparatively limited, leaving them exposed to a range of potential malicious attacks.

Session hijacking. During the communication setup sequence, a SessionID is generated for the new session. In the event of paused charging and subsequently resumed after a period, the same SessionID is retained for the ongoing charging session. During the resuming process, the only thing necessary is to transmit the SessionID from the previously authenticated session [64]. The utilization of TLS is not mandatory, which means this information could be intercepted by malicious entities. They could then exploit it as a form of authentication token to mimic the original EV owner. This could allow them to interrupt or recommence charging, adjust charging profiles, or even perform charging using the victim's credentials. Consequently, this scenario presents a potential vulnerability for session hijacking.

Lack of end-to-end guarantees. While ISO 15118 primarily addresses communication between EVs and charge points, numerous charging processes encompass backend systems, such as CPO, DSO, and so on. Because the data's protection extends only until it reaches the charge point, and there's no assurance of end-to-end integrity and confidentiality between the EV and the final recipient, the charger could potentially manipulate the backend communication with ease.

Requirement for verifying the validity of an EV certificate using OCSP is absent. ISO 15118 employs PKI for authentication and authorization by issuing digital certificates. The usage of the Online Certificate Status Protocol (OCSP) by the supply equipment to verify the electric vehicle certificate's validity is discretionary. In this context, adversaries might choose to employ expired or revoked certificates rather than obtaining a currently valid one.

Revealing Personally Identifiable Information (PII). At the start of a charging session, there is a significant exchange of data between EVs and charging station (CSs), which potentially includes a substantial amount of PII. When the vehicle authenticates with the CS, it becomes directly identifiable Given the information exchange between the EV and the charging station, such as the EVCC ID, which includes the MAC address of the EVCC used during session setup with the CS, it becomes an identifiable piece of information. This can result in situations where an energy provider could potentially acquire the home location of an EV [42].

Insecure Power Line Communication. The incorporation of HomePlug Green PHY (HPGP) into ISO 15118 does not provide encryption and is susceptible to eavesdropping and potential MitM attacks [37] [96]. Thus, it is possible for the attacker to gain access to the network. If the adversary manages to infiltrate the HPGP/PLC network at both the MAC and IP levels, they could execute an attack on the ISO 15118 service discovery.

Version downgrade. ISO 15118-20 mandates the use of mTLS (mutual authentication between client and server) with encryption protocols and key lengths designed to remain secure in the future. However, one can use a less secure ISO 15118-2 during the session setup process. This can permit unencrypted communication in scenarios involving EIM [96]. In [18], an attack is described by enforcing a security downgrade, thereby gaining the ability to eavesdrop on all the data being exchanged.

3.2 Open Charge Point Protocol (OCPP)

OCPP is an open-source communication protocol between charging stations and EVs [38] and used to: (a) establish communication with the EVSE; (b) set specific characteristics of the charging service, considering the user's preferences, condition of the EV, and the status of the power grid. (c) gather and save data related to the charger; (d) keep a record of scheduled charging appointments. In Figure 1, this protocol is referred to as *P2*. This protocol is established and managed by Open Charge Alliance (OCA) which aims to foster global development, adoption, and compliance of communication protocols in the EV charging infrastructure and related standards through collaboration, education, testing, and certification [1]. Due to a free and open source access, OCPP has quickly become a defacto protocol for EV charging infrastructure across multiple vendor platforms. This popularity and wide usage also causes an increase in potential security vulnerabilities.

3.2.1 OCPP Characteristics. OCPP is an IP-based protocol, using Transport Layer Security (TLS) for authentication and encrypted communication. For the Physical and Data link layer, OCPP is entirely based on Ethernet communication. The main characteristics of OCPP 2.0 are as follows:

- **Device Management:** It includes features to get and set configurations and monitor a Charging Station – important for Charging Station Operators managing multi-vendor charging stations.
- **Added Security:** OCPP 2.0 introduces secure firmware updates, security logging and event notification, and security profiles for authentication and secure communication.
- **Smart Charging Functionalities:** These are added for scenarios with an Energy Management System (EMS), a local controller, and for integrated smart charging of the EV, charging station, and Charging Station Management System.
- **Display and Messaging Support:** This feature provides the EV driver with information on the display, for instance regarding rates and tariffs.

3.2.2 OCPP Architecture. The architecture of the Open Charge Point Protocol (OCPP) is designed to facilitate seamless communication between Electric Vehicle Service Equipment (EVSE) and CPO. At its core, OCPP defines three main components: the Charging Station (CS), which represents the physical infrastructure where EVs connect for charging, equipped with an embedded controller that communicates with the CPO. The CPO, the software application at the core of the EV charging ecosystem, acts as a backend infrastructure to manage and monitor the entire charging network, coordinating interactions between the CPs and EVSEs. It handles tasks like assigning charging slots, monitoring charge sessions, billing customers, and facilitating communication with external systems, such as payment gateways and energy management platforms. The interaction between the CS, EVSE, and CPO occurs through standardized OCPP messages. These messages, exchanged over a secure communication channel, convey essential information about the charging process, station status, and energy consumption. The CPO responds with corresponding messages, ensuring bidirectional communication.

3.2.3 OCPP vulnerability. According to OCA and the official documentation of OCPP [1], there are three major security profiles in OCPP 2.0.1: (i) UTBA (Unsecured Transport with Basic Authentication) profile lacks fundamental security measures and does not incorporate authentication for the Charging Station Management System (CPO) or secure communication channel setup. It relies solely on HTTP Basic Authentication, making it suitable only for trusted networks. (ii) TLS-BA (TLS with Basic Authentication) profile enhances security by employing TLS to encrypt communication between the charging station and CPO. While it improves authentication compared to UTBA, it still relies on username and password, which may not suffice for robust security. (iii) TLS-CSC (TLS with Client-Side Certification) stands as the highest security profile, using TLS for encryption and requiring both charging station and CPO to authenticate using certificates. This model offers a superior level of security but must be carefully managed to address potential vulnerabilities in TLS or certificate systems. Additionally, avoiding TLS compression methods is recommended to prevent compression side-channel attacks and ensure interoperability.

High Exposure to External Networks. Charging station infrastructures are highly exposed to external networks, where the central system commonly contacts external links over the Internet. This exposure increases the risk of cyberattacks, as malicious actors could potentially gain access to the system [10]. Despite the launch of new security measures at the device and communication level in the most recent version of OCPP (v2.0.1), potential security risks still remain [10]. One such risk is a server hijack, where a malicious server can hijack traffic from the charger. This vulnerability may arise by manipulating DNS entries in one of the DNS servers used by the charger, leading to exposure of confidential data and the attacker sending malicious commands to the charger, causing damage [32].

Subversion or Malicious Endpoints. Subversion of the protocol can occur if an attacker gains control over a charging point or the central management system and manipulates the communication between them. This could lead to destabilization of power networks. For instance, an attacker could interfere with resource reservation originating with the EV, which may also be initiated by a man in the middle, leading to energy theft or fraud [11]. Such attacks may also result in over- or under-shooting of power network provisioning, or the (total/partial) disintegration of the integrity and stability of power networks [11].

Interference with Resource Reservation. Interference with resource reservation in OCPP can be a significant vulnerability [11]. The OCPP specifies communication between charging points and energy management systems. An attacker could interfere with resource reservation originating with EV, which may also be initiated by a man in the middle. This could lead to unauthorized use of energy resources, resulting in energy theft or fraud [11].

Support for ISO/IEC 15118. While support for ISO/IEC 15118 in OCPP 2.0 allows for easy two-way communication between Electric Vehicles and the charging stations (Management System), it also introduces the risk of automatic identification, which could potentially be exploited by malicious actors. As an example, The ISO/IEC 15118 standard introduces the use of RFID tags for user identification and authorization during a charging session. However, insecure RFID cards can put both vehicles at risk to cyberattacks. Some mobility operators and Charging Station Operators (CPOs) use MIFARE Classic RFID cards, which have been proven to be insecure [2]. Hackers can access and manipulate charging station configuration data, and make counterfeit RFID cards to steal user account information.

3.3 Open Charge Point Interface (OCPI)

The OCPI protocol is a communication protocol deployed extensively within the EV charging infrastructure ecosystem [70]. Its primary function lies in fostering interoperability among diverse

[2] https://www.switch-ev.com/blog/iso15118-mitigates-hacking-charging-infrastructure

stakeholders within the EV charging landscape. These stakeholders encompass CPOs, CS Operators (CSOs) and eMSPs as shown in Fig. 1. OCPI empowers these entities to engage in seamless information exchange, enabling the provision of uninterrupted and user-friendly charging services to the community of EV users [73, 89]. OCPI is supported by 200+ international companies and organisations, including ElaadNL, BeCharged, GreenFlux, EV Box, New Motion, Last Mile Solutions, the EVRoaming foundation[3] endorsed by the Netherlands Knowledge Platform for Charging Infrastructure[4].

3.3.1 OCPI Characteristics. OCPI primarily operates at the application layer, focusing on defining messages and procedures for communication during the charging process [70]. It does not mandate the use of specific transport and network layer protocols, such as TCP/IP or Ethernet. This allows for flexibility in the choice of underlying protocols, enabling OCPI to work with various infrastructure configurations and deployment requirements, such as a wired Ethernet network or a wireless communication protocol like LoRaWAN. This flexibility ensures that OCPI can be adapted to the specific needs of different EV charging networks. The main characteristics of OCPI are as follows.

- **Efficient Roaming System:** OCPI provides an effective roaming system that can be used bilaterally (between two parties) or through a centralized hub. This means that charging networks can seamlessly collaborate, allowing EV drivers to use different charging networks.
- **Real-Time Information:** OCPI offers up-to-the-minute details about charging station locations, their current availability, and pricing.
- **Standarised Data Exchange:** OCPI establishes a consistent method for sharing data. This includes Notification Data Records and Charge Data Records, which cover information both before, during, and after a charging session. This standardization simplifies communication between different systems and stakeholders.
- **Remote Mobile Access (RMA):** RMA enables EV drivers to access and initiate charging sessions directly from their mobile devices. This eliminates the need for pre-registration or manual authentication at the charging station, providing a more streamlined and user-friendly charging experience. Through RMA, EV drivers can use their mobile applications to search for nearby charging stations, view their real-time availability, and initiate charging sessions without physically approaching the station. The mobile application communicates with the charging station through the OCPI protocol, sending charging instructions and receiving status updates. This remote access capability offers several benefits for EV drivers including convenient charging on the go, reduced wait times, improved charging efficiency and enhanced accessibility.

3.3.2 OCPI Architecture. The OCPI architecture involves orchestrating the interactions between two key entities namely CPOs and eMSPs with CSOs playing a more indirect role [70, 90]. CPOs are service providers that own, operate, and manage EV charging stations. They integrate OCPI into their CSMS to oversee the entire charging process. This includes managing charging sessions, setting and managing charging fees, and engaging in roaming agreements to expand their network's coverage. eMSPs act as intermediaries between EV drivers and CPOs, providing a comprehensive platform for managing charging services. eMSPs communicate with CPOs using OCPI messages to initiate charging sessions, manage charging accounts, and access charging station information. CPOs, in turn, relay these commands and data to the relevant CSOs to manage the physical charging process. This indirect interaction ensures centralized control over charging networks while maintaining compatibility with the standardized OCPI messaging framework. This offer EV

[3] https://evroaming.org/

[4] https://nklnederland.nl/the-netherlands-knowledge-platform-for-charging-infrastructure/

drivers a user-friendly interface to search for charging stations, initiate charging sessions, manage charging accounts, and leverage roaming agreements to access a wider network of charging options [74, 91]. While CSOs (Charging Station Operators) play a crucial role in maintaining and managing charging infrastructure, they operate outside the direct communication loop of the OCPI architecture.

3.3.3 OCPI Vulnerability. OCPI offer numerous features to facilitate EV charging for roaming users. However, these features may lead to security vulnerabilities [20, 70, 73]. The main features and security implications are given below.

Offline Behaviour. OCPI-compliant systems must handle offline scenarios effectively to ensure the reliability and continuity of EV charging services. By logging data, allowing local authorisation, queuing transaction data, and providing user feedback, the protocol ensures that EV drivers can continue to charge their vehicles even when there are temporary connectivity issues. This offline recording can be subject to data privacy violations.

Credentials. The Credential module in OCPI plays a pivotal role in maintaining the integrity and security of the charging infrastructure, enabling seamless and protected EV charging transactions between Charging Stations and EVs while adhering to the specifications outlined in the protocol. The Credential Module within OCPI supports: *Credential Exchange* for secure sharing of credentials between EVs and Charging Stations. This includes mechanisms for validating the authenticity of EVs and their authorization to use charging services [70]. In cases where tokens are used for authentication, the Credential Module manages the generation, distribution, and validation of tokens i.e., *Token Handling*. This process ensures that only authorized EVs can initiate charging sessions. The module also enforces *Access Control* policies, determining which EVs are allowed to connect to specific Charging Stations based on the credentials presented during the charging session initiation. It also includes an error-handling mechanism to effectively communicate and address any issues related to credential validation, ensuring a smooth and secure charging experience for EV users. However, it can be exploited by adversaries to attack the EV charging surface.

Location. The Location module in OCPI serves as a critical component for managing and providing location-related information in the EV charging ecosystem. It is responsible for handling data related to charging station locations, their availability, status, and other essential details. Each location can encompass multiple EVSEs, and each EVSE can have several Connectors, enabling a hierarchical structure. By offering a standardized and comprehensive way to exchange location information, the location module enhances the accessibility and convenience of EV charging services for users. Location data and status information can be shared with eMSPs. Location can be updated by CPOs and sent to/ queried by the eMSPs. It is important to note that complete deletion of Locations, EVSEs, and Connectors is not possible due to their dependencies with other modules. Charging locations intended exclusively for private use and not designated for public charging must not be disclosed or made available through OCPI. Security vulnerabilities in the Location module of the OCPI can have significant consequences for the integrity and privacy of EV charging services.

Session. The Session object in the OCPI protocol serves as a fundamental component for managing and tracking EV charging sessions. This object is designed to capture and convey information about each charging session, offering insights into the duration, energy consumption, associated costs, and the charging station used. It facilitates standardized data exchange between CPOs, eMSPs, and other stakeholders, enabling seamless tracking and billing of charging sessions. To ensure transparency, multiple charging periods are included in a Session. The frequency of Charging Period transmission should be balanced, considering factors like charging speed. However an adversary can manipulate the size of charging period for unauthorised usage.

Charge Detail records (CDR). serves as a description of each EV charging session, including information such as session start and stop times, energy consumption, associated costs, and various charging parameters. CDRs hold particular significance for billing purposes, acting as the sole billing-relevant object. Once a charging session is completed, CDRs are transmitted from the CPO to the eMSP. Importantly, CDRs, once dispatched to the eMSP, are immutable; they cannot be altered or replaced. However, if necessary, a Credit CDR can be issued to rectify any billing discrepancies or adjustments, ensuring the accuracy and integrity of the billing process. This inherent immutability in CDRs underpins the reliability and trustworthiness of billing operations within the EV charging ecosystem. However a CDR can be forged and the communication can be intercepted to get the charging information the later usage.

Token. The Token empowers CPOs with knowledge of token information issued by eMSPs, which can take the form of RFID cards or digital credentials. eMSPs proactively share token data with CPOs, enabling the establishment of a cache of recognized tokens. When authorization requests from Charge Points are received, CPOs can cross-reference them with this cache, ensuring that only authorized users access the charging infrastructure. Additionally, the cached token information equips CPOs with the knowledge of which eMSP to collaborate with for the eventual transmission of Charge Detail Records (CDRs) which can be mishandled or used illegally by the adversary.

3.4 Open Automated Demand Response (OpenADR)

OpenADR is a standardised communication protocol that was originally created to manage electricity demand. It has found a critical use in EV charging, providing smooth coordination between utilities, grid operators, and charging systems. The OpenADR protocol bridges the gap between EV charging infrastructure and the power grid. OpenADR adds intelligence to EV charging by enabling grid-optimized and demand-responsive charging schemes – providing convenience of charging to EV owners and promoting the stability of the electrical grid. This OpenADR protocol acts as the interface between the charge point operator and the electric grid through aggregators as shown in Fig. 1. OpenADR is intended to support a range of devices, including thermostats, building management systems, and industrial equipment, making it suitable for a wide range of applications. One of OpenADR's most notable advantages is its emphasis on interoperability. It establishes a common language and communication infrastructure that enables various systems, devices, and applications to share information and signals for demand response in real time. This connectivity is critical for successful and efficient energy resource management.

3.4.1 OpenADR characteristics. OpenADR improves grid reliability and energy efficiency with essential characteristics such as scalability for multiple applications, two-way communication enabling bidirectional information sharing, and support for various demand response signals such as event-based, price-based, and simple-level signals. The protocol's various entities can be combined in a variety of ways to meet the needs of various organisations. A utility, for example, may use a single entity to manage all of its disaster recovery programmes, or it may use multiple VTNs to manage different types of disaster recovery programmes (e.g., residential, commercial, and industrial). Similarly, a VEN can be managed by a single VTN or by a group of VTNs. The OpenADR protocol is meant to be interoperable as well. This means that devices from various vendors can be used together without any proprietary constraints. This is because the OpenADR protocol employs a standard communication format that all OpenADR-compliant devices understand. The protocol ensures compatibility by utilising conventional communication protocols such as HTTP, HTTPS, and WebSockets. Authentication, encryption, and access controls are all used to provide security. The flexibility, real-time capabilities, and extensive reporting capabilities of OpenADR contribute to its broad acceptance, making it a cornerstone in current energy management systems.

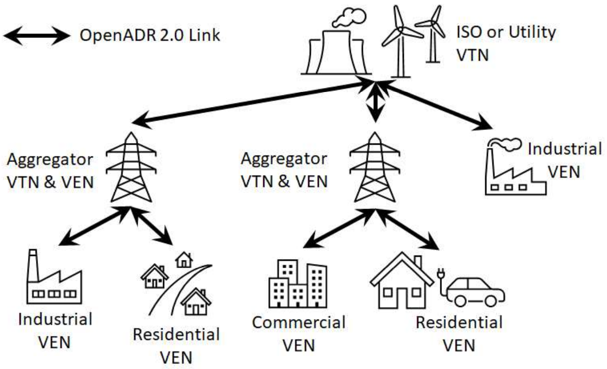

Fig. 3. Hierarchical Relationship in OpenADR 2.0 Entities

3.4.2 OpenADR Architecture. The OpenADR protocol is defined in terms of two entities that communicate with each other to exchange demand response signals. The OpenADR protocol's entities include VTN (Virtual Top Node) and VEN (Virtual End Node). Fig. 3 shows an example where the entities can communicate with OpenADR protocol in a hierarchical manner. These two entities can be combined in a variety of ways to meet the needs of various organisations. A VEN is a device or group of devices capable of responding to demand response signals. VENs are in charge of receiving and responding to events, generating reports, and managing demand-side resources. VENs can be found anywhere along the power grid, from individual homes and businesses to large industrial facilities. A VTN is a system that manages VENs and transmits demand response signals to them. VTNs play an important role in resource management, event creation and transmission, and report request. Whereas VTNs can be run by utilities, aggregators, or other entities.

To exchange data between VTNs and VENs, the OpenADR protocol employs web services. These web services function similarly to logical request-response services. OpenADR provides the following essential services:

(1) Event Service: Facilitates the transmission and acknowledgment of demand response events.
(2) Opt Service: Allows VENs to set temporary availability schedules.
(3) Report Service: Enables VTNs to request and receive reports from VENs.
(4) RegisterParty Service: Supports VEN registration and the exchange of device information.

These services use standard communication protocols such as HTTP/S and XMPP to exchange data. They use XML payloads and can communicate over broadband or dedicated internet connections. This ensures robust and flexible communication within the OpenADR framework. In simpler terms, OpenADR uses web services to send and receive messages between VTNs and VENs. These messages can be used to send demand response events, set availability schedules, request and receive reports, and register VENs. OpenADR uses standard communication protocols and XML payloads, which makes it easy for different systems to communicate with each other.

3.4.3 OpenADR vulnerability. The OpenADR protocol suffers from a number of reported vulnerabilities, as described below:

Authentication Mechanisms. To authenticate parties, OpenADR 2.0 uses public key cryptography methods such as ECC (Elliptic Curve Cryptography) and RSA (Rivest-Shamir-Adleman). Secure generation, retention, and administration of private keys is critical to the success of authentication. Any flaw in these methods can leadto unauthorised access.

Digital Certificates. VENs and VTNs employ digital certificates to validate their identities, boosting communication channel security. Expired or incorrectly handled certificates can cause authentication issues, potentially allowing hostile actors to compromise the system.

Secure Connections. Weaknesses or misconfigurations in TLS (Transport Layer Security) implementation can lead to vulnerabilities, e.g. eavesdropping or man-in-the-middle attacks.

Security Event Logging. OpenADR 2.0 offers facilities for security event logging, which aids in monitoring and incident response. However, insufficient or poorly managed logging may limit the discovery of security issues or the tracking of unauthorised actions.

3.5 Open Smart Charging Protocol (OSCP)

The OSCP serves as an open communication protocol that facilitates interaction between the CPO and the DSO. This protocol is responsible for transmitting a 24-hour forecast of the power grid's available capacity to the CPO. This protocol is depicted as *P4* in Figure 1. The developers of the Open Smart Charging Protocol have introduced a well-defined domain model that serves as the fundamental framework for the entire specification.

3.5.1 OSCP characteristics. The characteristics of OSCP converge to create a robust and user-friendly protocol. Specifically, OSCP supports: (i) **Remote Management:** The protocol allows for remote management of charging sessions, enabling users and service providers to monitor, control, and manage the charging process; (ii) **Dynamic Charging Control:** OSCP supports dynamic charging control, allowing adjustments to charging parameters based on factors such as grid conditions, energy demand, or user preferences; (iii) **Scalability:** The protocol is designed to be scalable, accommodating a variety of charging infrastructure sizes and types, from small home chargers to public fast-charging stations. (iv) **Interoperability:** OSCP promotes interoperability between different EVs and charging infrastructure, ensuring a seamless experience for users regardless of the equipment they are using.

3.5.2 OSCP Architecture. The *OSCP* specification employs various terms, including Capacity Provider, Capacity Optimizer, Flexibility Provider, and Flexibility Resource, as shown in Figure 4. A Flexibility Resource refers to a physical device with the ability to consume or generate energy in a controlled and flexible manner, such as EVs. Flexibility Resources have the potential to exhibit flexibility in terms of both the timing and the quantity of energy they consume or generate. The management of all Flexibility Resources is the responsibility of the Flexibility Provider. The Flexibility Provider, such as a CPO, gives instructions to Flexibility Resources for either generating or consuming energy. The Flexibility Providers are provided with upper and lower bounds for energy consumption or generation by the Capacity Provider. It is important to note that Capacity Providers do not directly interact with individual Flexibility Resources. In contrast, it is the duty of the Flexibility Provider to manage their Flexibility Resources, guaranteeing that they operate within the constraints defined by the Capacity Provider. For instance, a Capacity Provider, such as a DSO, ensures the proper functioning of a certain area, and a Flexibility Provider, such as a CPO, manages energy requests and demands while staying within the prescribed capacity limits of the grid connection. The Capacity Optimizer can assist the Flexibility Provider by offering an optimal approach to managing their Flexibility Resources. In practical terms, the Capacity Optimizer may leverage additional data sources, including weather forecasts and historical energy tariffs. These additional data sources can enhance the decision-making process for the Flexibility Provider.

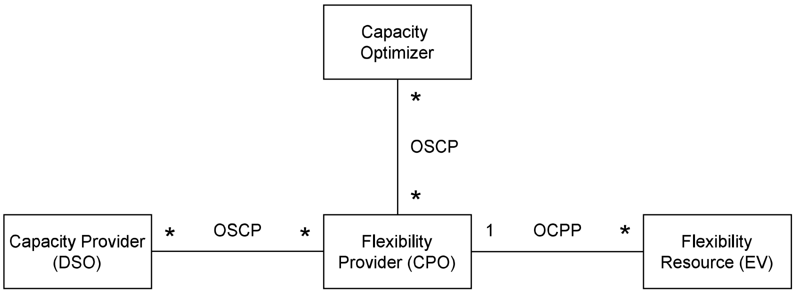

Fig. 4. OSCP components

In general, the entities mentioned in the above section can transmit five types of messages. Among these five messages, three of them, namely *UpdateGroupCapacityForecast*, *AdjustGroupCapacityForecast*, and *GroupCapacityComplianceError*, pertain to Capacity. The remaining two messages: *UpdateGroupMeasurements*, and *UpdateAssetMeasurements*, relate to Metering.

UpdateGroupCapacityForecast. This message contains a Capacity Forecast for a specific group or area, outlining the anticipated capacity for a particular time period. This forecast could, for instance, be derived from data collected from a transformer or statistical information about household energy consumption at a specific point in time. The message is relayed from the Capacity Provider to the Flexibility Provider and subsequently from the Flexibility Provider to the Capacity Optimizer. The goal is for the Capacity Optimizer to calculate the most suitable capacity forecast to be utilized within the specific group.

AdjustGroupCapacityForecast. In the event that the Flexibility Provider requires more capacity than originally allocated, they have the option to request additional capacity from the Capacity Provider. Conversely, if the Flexibility Provider requires less capacity than initially assigned, they can request a reduction in the allocated capacity from the Capacity Provider. The *OSCP* accommodates both scenarios through the use of an *AdjustGroupCapacityForecast* message. However, this message may not be accessible if the role of the Capacity Provider is assumed by a DSO or TSO, unless explicitly specified otherwise.

GroupCapacityComplianceError. When the Flexibility Provider cannot conform to the Capacity Forecast outlined in an UpdateGroupCapacityForecast message, this message allows them to notify the Capacity Provider of their inability to do so.

UpdateGroupMeasurements. This message is employed to send the aggregated energy usage data for each group or area from the Flexibility Provider to the Capacity Provider. By utilizing this information, the Capacity Provider can gain insight into the energy consumption of each Flexibility Provider in relation to the *UpdateGroupCapacityForecast* message.

UpdateAssetMeasurements. This message can encompass diverse metering values, including counts of active EV sessions and session start or end events, among others. It is relayed from the Flexibility Provider to the Capacity Optimizer. The Capacity Optimizer can utilize this data to create an optimized profile.

3.5.3 OSCP vulnerabilities. Security aspects of communication protocols pertaining to EV charging infrastructure is discussed in [88], especially in the context of OSCP. As specified in [88], the security shortcomings of those protocols are weak authentication and their reliance on secure tunnels which may not provide end to end security and lack non-repudiation. Possible Solutions were provided in

[88] to solve these flaws of secure tunnels such as data centric security approach were discussed. A detailed study on the technologies involved in grid integration of EV charging infrastructure was reported in [76]. The authors of [54] studied how various communication protocols related to EV charging infrastructure can inter-operate with each other. It specially discussed on the interoperability between OCPP and OSCP in a grid integrated EV charging infrastructure setup. Other more specific OSCP vulnerabilities include:

Lack of endpoint registration. In OSCP, the endpoints must be registered to verify the authenticity of incoming messages. This registration process is crucial for ensuring that messages originate from the correct source. For instance, a Flexibility Provider needs to verify the authenticity of the limits, confirming that they originate from a legitimate Capacity Provider. This implies that all the entities depicted in Fig. 4 must generate distinct tokens for authentication when registering with each other. Securing the transmission of this token between parties is a vital procedure, yet the protocol does not encompass specific measures for ensuring this security.

Heartbeat attack. In this protocol, a heartbeat message is transmitted from the Capacity Provider to the Flexibility Provider, as well as from the Capacity Optimizer to the Flexibility Provider. The purpose of a heartbeat message is to ensure that the involved entities are alive in the system. However, there is a possibility of a potential vulnerability or attack within the heartbeat messages. The sender heartbeat message comprises three components: a request for acknowledgment, a short, randomly selected message, and the character count of that message. The receiver is required to reply by acknowledging and echoing the same message. However, there is a potential risk where a malicious entity, posing as a Capacity Optimizer, could send a lengthy heartbeat message, where an actual message contains only 10 characters, but informing the Flexibility Provider that it contains 6400 characters. In the current scenario where entities are assumed to be secure, the Flexibility Provider may send the 10-character message along with sensitive information from the buffer, resulting in what is commonly referred to as a "buffer overflow." The malicious entity can repeatedly send messages, potentially causing the unintended exposure of the Flexibility Provider's private and confidential data. By exploiting this vulnerability, a malicious entity could potentially access departure times, electric vehicle (EV) credentials, or information about energy tariffs, thereby creating an opportunity for carrying out attacks.

4 ATTACK VECTORS AND THREAT MODELS

EV adoption can also lead to significant impact on the charging infrastructure, such as energy blackout caused by uncoordinated charging activities in urban areas, causing the power grid to fail [41, 81]. Threat models in this context may be characterised as: (i) **Attacks on public transport.** A long-term goal is to ensure access to charging points regardless of their brand and EV operator. Attacks targeting the payment mechanism (for roaming users) and thus restricting access to charging stations; (ii) **Attacks on navigation systems.** Integration of navigation systems with the location and availability of EV charging points may be used for route planning – as the range of an EV is limited. Attacks on the availability and status of charging stations may lead to the inability to charge and inaccurate route calculation. This section describes the common attacks that can be initiated on EVs and the associated charging infrastructure – in the context of the protocols described in Section 3. Table 3 summarizes the overview of attacks discussed in this section with the various protocols. Specific attack vectors on EV protocols (and existing solutions) are described utilising widely used threat models – such as Man-in-the-middle attacks, Denial of Service,and Botnets.

Table 3. Attack overview with respect to EV charging protocols

Attack Type	ISO 15118	OCPP	OCPI	Open ADR	OSCP
1. Man in the Middle Attack	Yes	Yes	Yes	Yes	Yes
2. DoS/DDoS	Yes	Yes	Yes	Yes	Yes
3. EV Botnet Attack	Yes	Yes	Yes	Yes	Yes
4. Power-line Communication Attack	Yes	No	No	No	No
5. Resumption Attack	Yes	Yes	No	No	Yes
6. EV Charging Impersonation	Yes	Yes	Yes	Yes	Yes
7. False Data Injection Attack	Yes	Yes	Yes	Yes	Yes

4.1 Man-in-the-middle attack

A man-in-the-middle (MitM) attack involves an attacker intercepting or manipulating communication between two groups without their consent, especially when data is unencrypted (permissible in ISO 15118). In the context of EVs, a MitM attack could lead to overcharging of an EV battery, causing damage to the vehicle[22]. Transmission of unencrypted data can lead to potential for eavesdropping or data manipulation [40]. These attacks could compromise the security of data transmission and enable malicious actors to intercept traffic at a charging station. Certain forms of attacks become feasible when an attacker gains physical access to the vehicle. In such scenarios, the attacker could exploit their close physical proximity to the target, enabling them to eavesdrop on and tamper with data between the supplied equipment and the vehicle [19]. A MitM attack could be accomplished either through a modified charging cable or by strategically placing a counterfeit charging point between the EV and the supply equipment. If the attacker's focus is solely on intercepting the communication[33, 34]. The ISO 15118-3[36] protocol for matching lacks authentication, allowing a potential adversary to assert themselves as the supply equipment possessing the strongest signal strength [37]. The attack can also happen between the CPO and the CS where a potential attacker intercepts the communication in the interface between the charging point and the central system, secretly relaying and possibly altering the information exchanged between these two parties [10, 11]. This may expose sensitive data of special interest to the various stakeholders involved in this context. MitM can also be caused by the potential risk of unauthorized interception or manipulation of tokens for OCSP during their transfer between entities. Upon successful token manipulation, an attacker can execute a MitM attack. Following the initiation of this attack, the attacker gains the capability to exploit metering values or elevate the consumption capacity of the Flexibility Provider. This increased capacity has the potential to yield detrimental consequences for the broader *EV* ecosystem. For instance, it can lead to local grid overload and disrupt the balance between energy supply and demand. Another way through which a MitM attack can be initiated is by exploiting vulnerabilities in the Handshake mechanism – which serves as the starting point for every communication between any two entities within *OSCP*.

Existing solutions. Numerous solutions are presented to handle MitM in the EV charging ecosystem. A Multimodal and Multipass Authentication using the Contract Certificate (MMA-CC) scheme was introduced by Vaidya et al. [87]. Similar solutions for safeguarding within the framework of the EV power trading decentralized architecture are presented by Li et al. which operates on the foundation of a consortium blockchain [62, 63]. To counteract potential MitM threats in the communication between the EVCC and the SECC, the solution introduces the Direct Anonymous Attestation (DAA) protocol and the in-vehicle Trusted Platform Module (TPM) [95]. The blockchain-based framework aims to establish secure charging services and reliable reservation capabilities for

EVs. This framework operates by executing smart contracts, which ensures the integrity and trustworthiness of the processes involved [26]. Additionally, to mitigate against a MitM attack between EV and EVSE, a temporary Elliptic-Curve key pair can be utilized until both parties generate and share their session ID key [18]. A machine learning-based system that can differentiate between malicious and normal traffic, ensuring the authenticity of station traffic is proposed by Moroson et al. [67]. However, the system was not able to detect real-time malicious traffic at charging stations, which is necessary when such stations are in operation. Addressing this issue, Al-Maksousy et al. [9] proposed a real-time system to detect and classify malware based on network behaviour using deep neural networks. To handle MitM attack between CP and CS, a counter-measure against these MitM attacks, Rubio et al. [77] presents a feasible solution and assesses its behaviour in a simulator. Wang et al. presented a certificate pinning [93] solution for MitM attacks caused by OCSP certificates. An OCSP stapling method [71] is proposed to ensure secure authentication and prevent unauthorized interception or manipulation of tokens. However, these proposed mitigation methods against MiTM attacks have challenges such as scalability, performance overhead, complex certificate management, legacy system compatibility and energy constraints which make their implementation difficult in large, distributed and resource-constrained EV ecosystems.

4.2 Denial-of-service (DoS) and Distributed DoS (DDoS) attack

Electric vehicles (EVs) are vulnerable to DoS attacks, where an attacker disrupts communication to hinder the proper functioning of the charging infrastructure [19]. For instance, an attacker could target the EVSE, making it unusable and potentially causing damage to the vehicle. One common vulnerability arises when multiple users share a single SECC, which manages the status of EVSE. If an attacker manipulates the EVSEStatusType by indicating *EVSE not in service*, it could make the charging station inaccessible to legitimate users [58]. Furthermore, a DoS attack can exploit the physical layer by jamming Power Line Communication (PLC) channels in ISO 15118 or by overwhelming the SECC with session requests, exhausting system resources and denying services to others. A fuzzification attack, as highlighted in OCPPStorm, can exacerbate these vulnerabilities by injecting malformed or unexpected inputs into the communication protocol, causing unintended behavior, system crashes, or resource exhaustion. This type of attack can be used to disrupt OCPP-based charging infrastructures, leading to denial of service and operational instability [13]. Manipulating time synchronization for validating TLS certificates is another vector that attackers could exploit, potentially invalidating certificates and preventing secure communication between devices.

DDoS attacks further extend these threats by using multiple compromised systems to overwhelm the EV charging infrastructure. Attackers can generate a high volume of fake charging requests, consuming bandwidth, processing power, and session resources, making the infrastructure more susceptible to outages and service denial [79]. By flooding communication protocols like ISO 15118, attackers can block or degrade the transmission of critical data, causing timeouts, delays, or even system crashes. Additionally, exploiting the load-balancing mechanisms in OCPP or OCPI enables attackers to focus the malicious traffic on specific charging points, forcing a shutdown and denying access to multiple users [38, 80]. A targeted DDoS attack on the SECC could artificially inflate session requests, consuming all available session resources, and preventing legitimate users from accessing charging services.

Existing solutions. Existing solutions to mitigate DoS and DDoS attacks in the EV charging ecosystem focus on securing communication channels and improving resource management within the infrastructure. The simplest approach is the use of enhanced encryption protocols such as Transport Layer Security (TLS) within ISO 15118 [52], which ensures secure data exchange between

EVs and EVSE. Load-balancing mechanisms in protocols like OCPP/OCPI can be optimized to detect unusual traffic patterns, thus preventing attackers from overwhelming specific charging points [49]. Rate-limiting techniques are also employed to restrict the number of requests that any single entity can generate, protecting SECC from session exhaustion attacks [80]. Additionally, protocol fuzzing tools can be leveraged defensively to detect vulnerabilities exploited by fuzzification attacks, helping to identify weaknesses before attackers can exploit them. Anomaly detection systems, which monitor real-time traffic for irregularities, can identify potential DDoS attacks early. Various ML-based anomaly detection methods are available which help detect DoS/DDoS attacks before it cause significant disruptions [15, 28, 43].

However, these solutions face several challenges. Encryption methods such as TLS may introduce latency and require robust key management, making it resource-intensive for large-scale deployments. Load-balancing and rate-limiting mechanisms may be uncovered by more sophisticated attackers who can mimic legitimate traffic patterns. Anomaly detection requires advanced algorithms that can distinguish between normal fluctuations in traffic and actual attacks. Moreover, maintaining effective security in distributed networks like EV charging infrastructure requires continuous updates and integration across different standards, which can be costly and time-consuming for operators.

4.3 EV Botnet attack

A botnet attack in the EV charging ecosystem involves a network of compromised devices, such as hacked IoT devices, charging stations or other connected infrastructure being remotely controlled by an attacker to launch a coordinated cyber attack [8, 80, 83]. The attacker uses this botnet to execute malicious activities, such as overwhelming the EVSE or SECC with a flood of traffic, leading to system overload and service disruption. Unlike a DDoS attack, which typically relies on traffic volume, a botnet attack could be more sophisticated by introducing specific, targeted disruptions at multiple layers of the charging infrastructure. For example, compromised EVSE units in various locations could simultaneously send erroneous data to manipulate charging sessions or hijack PLC communication channels [94]. The result could be large-scale service outages that affect not only charging availability but also the system's integrity, making it difficult to detect the root cause of the failure. The attacker could also use compromised charging stations to spread malware across the EV ecosystem, infecting connected vehicles or other infrastructure elements [50]. A well-coordinated botnet attack could lead to both financial losses for operators and potential safety risks for EV users, particularly if vehicles are denied charging or are sent erroneous information about charging status.

Existing solutions. Mitigating botnet attacks involves securing individual devices, strengthening communication channels and implementing real-time monitoring systems. Monitoring the EVSE and other connected infrastructure devices for regular patching with the latest firmware and security updates reduces their vulnerability to exploitation [68]. Deploying network segmentation techniques isolates critical systems such as SECC and EVSEs from compromised devices, preventing malware from spreading throughout the network [46]. Moreover, an IDS can monitor traffic between CS and EVs to detect abnormal behaviour indicative of botnet activity [15, 43]. Anomaly detection algorithms combined with network firewalls, provide an additional layer of defense by flagging suspicious traffic from infected devices [59].

However, botnets are becoming increasingly sophisticated and are using evasive techniques to mimic legitimate traffic and avoid detection by traditional IDS or firewalls. Detecting the spread of botnet/ malware in real-time is also difficult as botnet attacks often operate quietly over an extended period before launching a full-scale attack. Further, the decentralised nature of the charging infrastructure means that each operator must implement and maintain consistent security measures, which may not always be feasible due to cost or technical limitations.

4.4 Power-line communication injection attack

Power-line communication plays a crucial role in the global charging of electric vehicles and is a vital component in the EV industry. The ISO 15118 link layer does not have built-in defenses against eavesdropping and tampering, creating an opening for potential adversaries to use readily available tools like the CCS Listener [92] or develop custom PLC [30] devices. These tools can be connected to the same grid, often through means like a grounded socket on the charger or within the parking lot. This setup allows attackers to intercept, inject, and alter Vehicle-to-Grid (V2G) messages as needed. As TLS in ISO 15118-2 remains an optional feature, all communication remains susceptible to eavesdropping. This vulnerability allows malicious actors to potentially access sensitive information, including the EVCCID (Electric Vehicle Communication Controller's ID, essentially the vehicle's MAC address), the sessionID for the ongoing charging session, charging schedules, and tariff information. Such data can be valuable for planning an attack. With access to the captured sessionID, an adversary can craft and insert arbitrary messages conforming to the ISO 15118 format, effectively taking control of the charging session to align with their chosen attack strategy. By implanting malicious code into EVSE or the electric vehicle itself, an attacker can potentially breach sensitive information. In [55] [56], the authors have illustrated a comprehensive approach to the Brokenwire attack, showcasing how an adversary can interrupt a charging session. In order to thwart PLC injection attacks, it was possible to disrupt an ongoing communication session and halt the charging process [30], by employing V2GInjector to transmit a SessionStop message from a malicious PLC device.

Existing Solutions. Existing defense mechanisms against these attacks include encryption protocols to secure transmitted data, such as advanced cryptographic techniques, secure key exchange protocols (Elliptic Curve Diffie-Hellman (ECDH)) and secure symmetric encryption like AES-256 can protect against unauthorized data modification or injection tailored for PLC environments [53]. A signal cancellation system is proposed in [84] which handles the PLC-based attacks using a signal cancellation system that restores benign charging sessions by annihilating the attack signal. Robust anomaly detection systems leveraging ML algorithms can also help identify patterns indicative of PLC-based attacks [65]. These systems monitor traffic for abnormal signal modulation or deviations in expected communication patterns. Techniques like frequency hopping and noise filtering are also applied to reduce the feasibility of successful interference in the PLC medium.

Despite these advances, the inherent noise and variability in PLC environments can complicate the accurate detection of anomalies. Additionally, implementing robust encryption and authentication protocols can increase computational and energy overheads, which are critical constraints in EV ecosystems.

4.5 Resumption attack

After successful authentication, the vehicle has the capability to initiate and halt ISO 15118 sessions by presenting the sessionID. However, to save time and resources, session resumption allows a charging session to restart without undergoing the full authentication and handshake process if the same vehicle returns to the EVSE within a certain period [10]. The session resumption process can be attacked to exploit the vulnerabilities in ISO 15118. In a resumption attack, an attacker can intercept or manipulate the session resumption process, exploiting weaknesses in session management, encryption, or session identifiers to impersonate a legitimate EV or EVSE [96]. By doing so, they can bypass security mechanisms and gain unauthorized access to the system. For example, an attacker might capture and replay session resumption tokens or session IDs to manipulate the SECC into resuming a previously established session. This allows the attacker to engage in fraudulent activities such as gaining free charging or disrupting legitimate charging sessions. If an attacker manipulates the resumption process, they could also alter billing details, interfere with the charging status, or even initiate fake sessions. Moreover, attackers could use the resumption attack to gather sensitive data, such as vehicle identification or user account information, potentially leading to data breaches or identity theft.

Existing solutions. Addressing resumption attacks in the EV charging ecosystem also focuses on improving session management and enhancing encryption standards. Extending the use of stronger encryption protocols for securing session resumption tokens ensures that attackers cannot easily intercept or manipulate the sessionID [52]. Additionally, implementing more robust session timeout mechanisms or requiring partial re-authentication even for resumed sessions reduces the attack window, making it harder for attackers to replay or hijack session tokens [12, 17]. Token expiration and verification checks are also critical to ensure that session resumption tokens expire after a short duration or are invalidated after one-time use. A blockchain-based token verification model is presented in [7].

More frequent authentication processes can introduce delays and negatively impact user experience. Updating session management techniques across a distributed network of charging stations also requires a coordinated effort among various stakeholders, which could be hindered by technical and operational differences across these stakeholders.

4.6 Impersonate the EV charging components

In the EV charging ecosystem, particularly with ISO 15118, identity information for the charging session is stored directly in the EV, creating a vulnerability that attackers can exploit through impersonation. A malicious EV could substitute its own identification details with those of a victim's EV, effectively impersonating the target. In this scenario, the attacker manipulates the charging infrastructure, convincing the supply equipment that the communication is occurring with an authenticated and legitimate vehicle, even though it is not. This allows the attacker to "freeload," charging their own EV at the victim's expense by hijacking their credentials. There are three primary methods through which this impersonation attack can be carried out [36]. (i) Intercepting and continuing an authenticated charging session, in which the attacker intercepts a legitimate charging session, pausing it before the victim disconnects and then resuming it to charge their own vehicle using the victim's credentials. (ii) Obtaining a valid contract certificate, in which the attacker acquires a contract certificate, either by compromising the OEM's key management system or by collaborating with a "Contract-Sharer" who shares their certificate and private key. (iii) Using an expired contract certificate, in which the attacker uses an expired contract certificate to initiate a charging session by exploiting the optional revocation checks and lack of time synchronization in the charging infrastructure, allowing them to bypass security measures.

Supply Equipment can also be impersonated. The concern revolves around the potential for an attacker to impersonate supply equipment during a charging session. To engage in impersonation during a TLS-based charging session, a hacker needs either stolen certificates or the installation of a fraudulent root certificate. A hacker, while pretending to be supply equipment, can exploit the vehicle-to-grid support feature to withdraw energy from the battery of a legitimate EV owner's vehicle. In another scenario, the attacker can also eavesdrop on an ongoing charging session. The use of TLS is mandatory in trusted environments, making it essential for safeguarding identifying details like the E-Mobility Account Identifier and the MAC address of the EVCC. This information can be eavesdropped only when a malicious actor manages to acquire authentic supply equipment certificates. On the contrary, each vehicle can be recognized by utilizing the MAC address of the PLC (Power Line Communication) interface at the data link layer [37]. Furthermore, at the network layer, it is possible to infer the MAC address from the IP address. It is feasible for an eavesdropping attacker to recognize charging electric vehicles connected to the same SECC, as these layers lack encryption [42] as mentioned in section 4.2.7.

Existing solutions. The most common existing defense mechanisms for such attacks include mutual authentication protocols, such as Public Key Infrastructure (PKI), where the EV and EVSE verify each other's credentials before initiating a session [51]. A more advanced multimodal and multi-pass authentication mechanism is presented in [87]. A sophisticated federated Byzantine agreement model utilising certificates is presented in [35] which can also be used for offline EVSE. Moreover, session-based authentication mechanisms can also be employed where unique session identifiers are used and validated for each interaction, reducing the likelihood of unauthorized impersonation attempts [24].

As the security implementation is protocol-specific, challenges remain in terms of interoperability across diverse EV and EVSE manufacturers, ensuring global standardisation and managing the computational overhead introduced by complex cryptographic techniques. Additionally, vulnerabilities in legacy systems or improper implementation of secure protocols could still leave infrastructure susceptible to impersonation attacks.

4.7 False Data Injection attacks

A false data injection attack involves an attacker injecting compromised data into the communication between an EV, EVSE or the central system that manages the charging infrastructure [6, 16]. This false data could involve altering critical information such as the vehicle's state of charge, charging status, energy consumption, or billing details [75]. These fabricated messages are designed to influence consumer decisions and actions, leading to detrimental consequences for system reliability. For example, an attacker could falsify data to indicate that an EV is fully charged when it is not, or alter energy consumption records to reduce the cost of charging or overcharging. Attackers may manipulate DR signals in an undetected way, leading to line overloads that can have cascading effects on the energy grid [86]. In more severe cases, the attacker can manipulate the grid demand signals to mislead the energy management system, causing load imbalances. In extreme cases, the attack could lead to system-wide blackouts, disrupting electrical power service to a large number of customers [27, 97]. The concept of Dynamic Load Altering Attacks (D-LAAs) is introduced in [14] as a new category of cyber-physical attacks specifically targeting smart grid demand response programs – manipulating the behaviour of flexible loads within the smart grid, leading to adverse consequences such as frequency instability.

Existing solutions. To counteract False Data Injection Attacks (FDIAs), a range of solutions have been proposed across various domains. A notable approach is the use of optimization-based protection systems [14], which employ a non-convex pole-placement optimization framework to enhance grid stability while addressing sensor uncertainty to detect and mitigate attacks on demand-side systems. Similarly, [60] introduces a Fog Computing-enabled Secure Demand Response (FSDR) mechanism, leveraging fog nodes as sanitisers to encrypt and randomize energy states and demand-response (DR) strategies through homomorphic operations, thus thwarting data manipulation and collusion attacks. Addressing the risks of FDIAs in real-time pricing (RTP) systems, [39] proposes a network reconfiguration method that optimizes the switch states within the distribution network, enhancing resilience and minimizing power losses induced by manipulated RTP signals. Additional techniques include machine learning-based anomaly detection frameworks that identify irregularities in transmitted data [28] and blockchain-based systems that ensure data integrity

Table 4. Comparison of Existing simulators

Simulator	Main Protocol	Additional Protocols	Language	Target Community	Attack/Fault Handling	Open source/ Proprietary
OpenV2G	ISO 15118	-	C	Researchers	-	Open-source
Switch EV	ISO 15118	OCPP 2.0 (planned)	Python	Researchers, Industry	-	Open-source
Everest	ISO15118, OCPP 2.0 (limited)	OpenADR	Dockerfile	Researchers, Industry	Faults	Open-source
Mobilityhouse	OCPP 1.6, OCPP 2.0	-	Python	Researchers, Industry	-	Open-source
Steve	OCPP 1.6	-	Java	Researchers	-	Open-source
ShellRecharge	OCPP 1.6, OCPP 2.0	-	Scala	Researchers, Industry	Partial	Open-source
WWCP_OCPP	OCPP 1.6, OCPP 2.0, OCPP 2.1	WWCP	C#	Researchers, Industry	Partial	Open-source
Java-OCA-OCPP	OCPP 1.6, OCPP 2.0	-	Java	Researchers, Industry	-	Open-source
OCPP-go	OCPP 1.6, OCPP 2.0	-	Go	Researchers, Industry	-	Open-source
OCPP.Core	OCPP 1.6, OCPP 2.0	-	.Net	Researchers, Industry	-	Open-source
OCPP-js	OCPP 1.6, OCPP 2.0	-	JS	Researchers, Industry	-	Open-source
OpenLeADR	OpenADR	-	Python	Researchers, Industry	-	Open-source
DERIT	OpenADR	-	-	Researchers	-	-

and transparency by recording immutable energy transaction records [7, 65]. Secure multiparty computation (SMC) techniques can also play a critical role by allowing collaborative operations on encrypted data without exposing sensitive information [24]. These solutions rely on precise grid models – which in practice may not be able to handle real-world dynamics effectively. The increased computational overhead of data encryption may also limit benefit. More generally, machine learning-based detection methods can suffer from high false positives, adaptability issues against evolving attacks, and scalability to larger data sets.

5 EV INFRASTRUCTURE SIMULATORS

EV infrastructure simulators are critical tools for designing, analysing and optimizing EV charging ecosystems. These simulators enable researchers and practitioners to model complex interactions within EV charging networks, including energy demand, charging station placement, load balancing, communication protocols and attack scenarios. By simulating real-world cases, they facilitate the evaluation of algorithms and defense mechanisms against cyberattacks explained in Section 4, under controlled conditions. Additionally, simulators assist in evaluating grid resilience, integration of renewable energy sources, and the scalability of charging networks, providing insights into cost efficiency and environmental impact. They play a pivotal role in advancing secure and efficient EV infrastructure development. In this section, we discuss existing simulators for various EV charging protocols, describing their features and shortcomings. Table 4 presents a summary of simulators explained.

5.1 ISO 15118 Simulators

This section provides information about various simulators that support the integration of EVCC and SECC for ISO 15118. The most well-known ISO 15118 simulators are as follows:

5.1.1 Switch-EV. [5] Switch EV offers tools and platforms designed to implement and test V2G communication standards, with a strong focus on ISO 15118. One of its offerings, RISE V2G[6], serves as a reference implementation for ISO 15118, providing features like Plug and Charge (PnC) for authentication and billing. However, this project is being replaced by a newer initiative, Josev Community[7], which supports updates to the latest versions of ISO 15118-20, emphasising easy integration with charging infrastructure.

5.1.2 OpenV2G. [8] This is an open-source implementation of the ISO 15118 communication protocol, focusing on PnC capabilities and basic interoperability testing. It supports extensions and custom testing scenarios for research and development environments.

5.1.3 Everest. [9] This is an open-source framework for EV charging software stack currently supporting ISO 15118 with limited OCPP support. Available as Docker containers and provided with a user interface, it is easy to use and evaluate.

5.2 OCPP Simulators

In this subsection, we focus on simulators that implement the OCPP protocols.

5.2.1 Mobilityhouse OCPP Simulator. [10] This is a Python implementation of OCPP with support for versions 1.6 and 2.0 and uses the JSON version of the protocol. It also provides examples of how to implement a charging station and client. It is available open source for researchers and industry to explore the features of OCPP.

5.2.2 SteVe. [11] Steve offers an open-source implementation of OCPP 1.6 in Java. The implementation focuses on the SOAP version of the OCPP protocol and includes compatibility with charging stations.

5.2.3 ShellRechargeSolutionsEU/ocpp (Scala). [12] This is an open-source simulator which allows defining data types for the OCPP messages, RPC and error reporting. No real message handling is provided. This is implemented in Scala and is available for researchers and industry personals.

5.2.4 OpenChargingCloud/WWCP. [13] WWCP_OCPP offers an implementation of OCPP and provides gateways between OCPP and WWCP (World Wide Charging Protocol). It also offers extensions and workarounds to address flaws and security issues in the OCPP specification. It aims to simplify daily operations, enhance high availability, and support additional concepts such as GDPR and the German Calibration Law (GCL).

[5] https://github.com/SwitchEV
[6] https://github.com/SwitchEV/RISE-V2G
[7] https://github.com/EcoG-io/josev
[8] https://github.com/Ecognize/openv2g
[9] https://github.com/EVerest/EVerest
[10] https://github.com/mobilityhouse/ocpp
[11] https://github.com/steve-community/steve
[12] https://github.com/ShellRechargeSolutionsEU/ocpp
[13] https://github.com/OpenChargingCloud/WWCP_OCPP/

5.2.5 Language-specific OCPP implementation. Java-OCA-OCPP[14] provides a Java implementation of OCPP.OCPP-go[15]: is implemented in Go, and also supports the JSON version of the OCPP protocol. OCPP.Core[16] is the server implementation written in .NET 6. OCPP-js[17]: offers an OCPP implementation in JavaScript.

5.3 OpenADR Simulators

This subsection provides the details of the popular tools available to simulate the OpenADR protocol.

5.3.1 OpenLeADR. OpenLeADR[18] is a user-friendly and compatible Python library for the OpenADR protocol. As an open-source project, OpenLEADR allows developers and organisations wishing to adopt demand response systems with transparency and freedom. This provides compatibility and interoperability with other OpenADR-compliant systems and devices.

5.3.2 Distributed Energy Resources Integration Toolkit (DERIT). [19] DERIT is a sophisticated collection of tools aimed at bridging the gap between utilities and distributed energy resource (DER) owners. This toolkit includes reference implementations of OpenADR servers, VEN emulators, and data management tools that are OpenADR-compliant. The toolbox extends beyond standard OpenADR tools. It has capabilities built expressly for DER integration. DER simulation tools enable developers and utilities to virtualize and test DR methods, reducing risk and ensuring DERs respond correctly to OpenADR signals.

Existing simulators for EV charging infrastructure, while valuable for testing specific protocols like ISO 15118, OCPP and OpenADR, do not provide a detailed view of the entire charging scenario, particularly in terms of attack and fault analysis at each protocol level. Most simulators focus on the technical functionality of communication protocols without integrating a comprehensive security framework that accounts for threats and vulnerabilities across the system. There is a clear gap in simulators that combine protocol-level security testing across the various layers of the EV charging infrastructure, particularly when considering real-time attack simulations and fault management. This results in limited testing environments where the full spectrum of vulnerabilities, from physical to application layers, remains unaddressed. Thus, a more integrated, multi-protocol simulator is needed to accurately assess the resilience of EV charging systems in the face of complex cyber threats.

6 DISCUSSION AND FUTURE RESEARCH DIRECTIONS

Previous sections of this survey have focused on features and vulnerabilities in EV charging communication protocols and infrastructure. Several critical insights have emerged, paving the way for promising future research directions. As evidenced by the vulnerabilities outlined in Section 4, establishing robust cybersecurity measures for the EV industry remains a challenge. One notable area of inquiry revolves around the evaluation of EV security without relying on cloud-based assessments. Additionally, there is a need to focus on more application layer protocols versus transport layer protocols, taking account of specific features introduced in the EV charging application. The impact of new encryption technologies, such as post-quantum or homomorphic encryption, also looms large, prompting a reassessment of security measures. Exploring open application layer protocols, post-quantum transport, and the implications of using proprietary protocols by vendors

[14] https://github.com/ChargeTimeEU/Java-OCA-OCPP
[15] https://github.com/lorenzodonini/ocpp-go
[16] https://github.com/dallmann-consulting/OCPP.Core
[17] https://github.com/aymen-mouelhi/ocpp-js
[18] https://github.com/openleadr
[19] https://www.epri.com/research/products/000000003002013623

are key facets in understanding the evolving threat landscape. Moreover, delving into well-defined attacks and examining how additional layers may augment attack scenarios, such as altering feeder loads, can add to our understanding of potential vulnerabilities. Finally, the environmental and economic consequences of attacks carried out on the EV ecosystem, and their impact on other smart city services, provides a compelling avenue for further investigation. Such dependencies have the potential to impact critical infrastructure systems and user safety significantly. Table 5 provides an exploration of key topics that surfaced during our research, highlighting critical research aspects in the EV ecosystem.

Table 5. Future research needs for EV charging ecosystem

Topic	Research Areas
Technological Evolution	(i) Smart charging, Dynamic pricing; (ii) AI-driven continuous risk assessment; (iii) Autonomous charging, Crucial authentication for seamless integration
End-to-end Simulation Validator	(i) Fragmented Simulators, Protocol-specific; (ii) A unified protocol simulator for comprehensive security
Application Layer	(i) Seamless EV Communication; (ii) Standardized Protocols for user-friendly EV ecosystem; (iii) Zero-trust model; (iv) Potocols with security measures
Cryptography	(i) Computationally efficient Homomorphic encryption; (ii) Post-quantum algorithms
Gaps in Security	(i) Blockchain integration for charging infrastructure security; (ii) Multi-party computation in smart grid scenarios involving EV interactions; (iii) Zero-trust model and adaptive security framework for EV infrastructure; (iv) Biometric Authentication, Multi-factor authentication
Environmental and economic impacts of attacks	(i) Minimise disruption on smart city services; (ii) Secure operation of smart city
Carbon Footprint	(i) Edge Computing for EV; (ii) Monitoring and reporting in energy and carbon for EV infrastructure; (iii) Install EV charging stations powered by renewable energy; (iv) Off-peak charging

Protocol Evaluation. This survey focuses on key protocols and standards, including ISO 15118, OCPP, OCPI, OCSP and OpenADR, given their widespread adoption and critical role in the current EV charging ecosystem. However, the scope of this work does not encompass other standards like SAE J2931, CHAdeMO, and IEC 61851, which are also part of EV communication and charging. These protocols also lead to additional interoperability challenges, including a variation in their implementation in different regions and updates to these standards that can take place at different times.

Technological Evolution provides new opportunities to improve the security of EV infrastructure. Advancements in AI and Machine Learning (ML) can lead to smart charging patterns and dynamic pricing models. AI/ML algorithms can also be used for threat detection to strengthen security. AI/ML-driven risk assessment frameworks can be used to identify and address emerging vulnerabilities in the complex EV ecosystem through proactive analysis of newly introduced technologies. Integrating current and prospective innovations in charging solutions, such as autonomous charging, becomes paramount. Addressing challenges such as authentication is crucial in ensuring the seamless integration of these technologies into the broader EV charging infrastructure.

End-to-end Simulation Validator. Current simulators are designed specifically for individual protocols, leading to a fragmented approach with separate simulators dedicated to ISO, OCPP, and various other protocols. To address this open issue, a unified simulator capable of operating seamlessly across the entire EV ecosystem is needed. Such a simulator could be used to identify additional potential attack vectors, extending from EVs, to charging points to the power grid, whilst also identifying mitigation strategies to protect against such attacks.

Application layer. Protocols at this layer are integral for facilitating communication across EVs and charging infrastructure. Future work could focus on advanced security mechanisms such as continuous authentication in EV applications so that user identity can be verified based on behavioral patterns during system communications without disrupting the user experience. Also, there is a growing push for the development and adoption of standardized protocols to enhance the cohesion and user-friendliness of the EV ecosystem. Future application layer protocols should include security measures and more efficient data exchange mechanisms. Establishing a zero-trust security framework in which there is no inherent trust granted to any entity, whether it is part of the internal network or external to it is also important. It requires continual authentication of each device, user, and application attempting to access or connect to the system.

Cryptography. As the EV charging landscape evolves, new cryptographic methods such as computationally efficient homomorphic encryption [3] and post-quantum algorithms [48] are becoming increasingly relevant to ensuring the security and resilience of the system. Traditional encryption mechanisms, such as symmetric or public-key encryption, provide data confidentiality but often require data decryption for processing, which creates vulnerabilities during the operational phase and increases exposure to attacks like data leakage or tampering. Once decrypted, sensitive data is exposed and may be susceptible to unauthorized access or manipulation, making it essential to consider solutions that minimize the need for decryption. Given the evolving landscape of EV charging, where sensitive user and operational data are frequently processed and shared between multiple stakeholders, homomorphic encryption offers an added layer of security, ensuring end-to-end privacy without compromising functionality. Moreover, cryptographic methods such as secure multi-party computation (SMPC) [25] and confidential computing environments (CCEs) [61] offer promising alternatives. SMPC enables computations on encrypted data without decryption, maintaining data confidentiality even during processing. CCEs, on the other hand, allow sensitive data to be processed in a secure, hardware-protected environment, reducing the risk of exposure or tampering. Additionally, format-preserving encryption (FPE) [21] can provide encryption while retaining the format of the data, facilitating secure processing in real-time environments where maintaining data format is crucial. Furthermore, the integration of post-quantum algorithms becomes imperative, considering the potential threats posed by the rise of quantum computing, which could compromise traditional cryptographic methods [48]. Adopting these advanced cryptographic methods in EV charging infrastructure not only enhances data protection but also secures communication channels and fortifies transaction integrity. As the EV charging landscape continues to evolve, the implementation of advanced cryptography measures becomes a crucial pillar in building a resilient, secure, and future-proof charging ecosystem.

Gaps in security. Additional research is needed to investigate the viability of integrating cutting-edge security technologies, such as blockchain technologies (including parachains – such as Cosmos [57], PolkaDot.Network [2] and IoTA [82]) and zero-trust security model [45], as potential improvements and/or replacements for current security methodologies to further enhance the security posture of EV infrastructure. The charging infrastructure, including charging stations and their communication networks, may be susceptible to cyber-attacks, leading to disruptions and potential unauthorized access. Implementing blockchain in the charging infrastructure can enhance security by creating a transparent and secure transaction history, reducing the risk of fraudulent activities. Another future research direction is to utilise multi-party computation in smart grid situations involving EV interactions, allowing secure computations for load prediction, responding to electricity demand, or enhancing charging schedules – without exposing private user information or compromising grid safety. On top of the aforementioned open gaps, the most interesting future work is to integrate adaptive security architectures in EV infrastructure. By developing an integrated and adaptive security framework tailored to the needs of EV system. this framework can dynamically adjust security protocols and measures in response to real-time threat assessments.

Environmental and economic impacts of EV system attacks. The EV ecosystem involves different communication protocols that connect various EV entities, thus attackers can exploit vulnerabilities across different layers of the EV system to manipulate the EV charging system to cause environmental and economic disruptions to smart city services. With this in mind, the security of EV system impacts the secure operation of smart city services that co-exist alongside such charging infrastructure. Investigation of the potential environmental and economic implications of exploiting the EV system vulnerabilities on smart city, aiming to minimise disruption on smart city services and ensuring user safety is also an important area for future research.

Carbon footprint. Edge computing and renewable energy in EV infrastructure can also be used to reduce the overall carbon footprint. Additional research is needed in edge-based systems for efficient energy management and carbon footprint reporting by relocating computational tasks to the edge of the EV charging ecosystem (with the goal of reducing the overall carbon footprint linked to centralized data processing and storage). This will allow for real-time monitoring and optimization of energy usage in EV charging as well as providing real-time reporting of EV charging-related carbon footprint to make informed decisions when opting charging stations in proximity to renewable generation.

7 CONCLUSION

The rising demand for EVs underscores the necessity for an in-depth examination of the security and privacy challenges inherent in EV charging infrastructure – a key component which differs from other vehicular systems. The existence of diverse protocols connecting each entity within the EV charging infrastructure contributes to a highly complex (and interdependent) system. Additionally, this heightened complexity and connectivity exposes vehicles to the risk of cyberattacks. This paper examines the cyber-physical vulnerabilities associated with protocols from EVs to the power grid. Our goal is to offer a comprehensive overview of the protocols, including their underlying vulnerabilities and potential mitigation strategies against these.

We examine the collaborating entities engaged in EV charging, the operational protocols governing their interactions, and the inherent vulnerabilities within these protocols. Subsequently, we delve into the discussion of potential attack vectors associated with each of these protocols. We also explore conceivable countermeasures and propose future directions to enhance the overall security and privacy of protocols within the EV ecosystem. The present landscape of EV charging protocols is characterized by a patchwork of proprietary standards, hindering interoperability and introducing security vulnerabilities. While consolidating these protocols under a single organization could streamline compliance validation and foster standardization, it also raises the specter of honeypot attacks. By pooling vulnerabilities under a single umbrella, attackers could potentially exploit a centralized system with greater efficiency. In conclusion, the evolving nature of EV technology exposes a vast attack surface, leaving it vulnerable to exploitation by malicious actors. Protecting the integrity and safety of the EV ecosystem demands a unified approach that encompasses advanced countermeasures specifically designed for the protocols and communication channels employed in this dynamic environment.

REFERENCES

[1] 2020. *Open Charge Alliance - Global Platform For Open Protocols.* https://www.openchargealliance.org/ Online; accessed 2023-10-13.

[2] Hanaa Abbas, Maurantonio Caprolu, and Roberto Di Pietro. 2022. Analysis of polkadot: Architecture, internals, and contradictions. In *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 61–70.

[3] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. 2018. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)* 51, 4 (2018), 1–35.

[4] Samrat Acharya, Yury Dvorkin, and Ramesh Karri. 2020. Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable? *IEEE Transactions on Smart Grid* 11, 6 (2020), 5099–5113.

[5] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. 2020. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access* 8 (2020), 214434–214453.

[6] Samrat Acharya, Robert Mieth, Ramesh Karri, and Yury Dvorkin. 2022. False data injection attacks on data markets for electric vehicle charging stations. *Advances in Applied Energy* 7 (2022), 100098.

[7] Vladislav Aistov, Benedikt Kirpes, and Micha Roon. 2020. A blockchain token economy model for financing a decentralized electric vehicle charging platform. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1737–1742.

[8] Amirhossein Akbarian, Mahdi Bahrami, Mehdi Ahmadi, Mehdi Vakilian, and Matti Lehtonen. 2024. Detection of Cyber Attacks to Mitigate Their Impacts on the Manipulated EV Charging Prices. *IEEE Transactions on Transportation Electrification* (2024).

[9] Hassan Hadi Al-Maksousy, Michele C Weigle, and Cong Wang. 2018. NIDS: Neural network based intrusion detection system. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 1–6.

[10] Cristina Alcaraz, Jesus Cumplido, and Alicia Trivino. 2023. OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security* (2023), 1–27.

[11] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. 2017. OCPP protocol: Security threats and challenges. , 2452–2459 pages.

[12] Abdullah M Almuhaideb and Sammar S Algothami. 2022. ECQV-based lightweight revocable authentication protocol for electric vehicle charging. *Big Data and Cognitive Computing* 6, 4 (2022), 102.

[13] Omer Rana Rigel Gjomemo V.N. VenkatakrishnanGaetano Coppoletta Amanjot Kaur, Nima Valizadeh. 2024. OCPPStorm: A Comprehensive Fuzzing Tool for OCPP Implementations. *Network and Distributed System Security Symposium (NDSS 2024), San Diego, USA* (2024).

[14] Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. 2018. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Transactions on Smart Grid* 9, 4 (2018), 2862–2872.

[15] Yagiz Alp Anli, Zeki Ciplak, Murat Sakaliuzun, Seniz Zekiye Izgu, and Kazim Yildiz. 2024. DDoS detection in electric vehicle charging stations: A deep learning perspective via CICEV2023 dataset. *Internet of Things* 28 (2024), 101343.

[16] Ugonna R. Anuebunwa, Haile-Selassie Rajamani, Raed Abd-Alhameed, and Prashant Pillai. 2018. Investigating the Impacts of Cyber-Attacks on Pricing Data of Home Energy Management Systems in Demand Response Programs. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*. 1–5.

[17] Ponnuru Raveendra Babu, Alavalapati Goutham Reddy, Basker Palaniswamy, and Suneel Kumar Kommuri. 2022. EV-Auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover. *IEEE Transactions on Intelligent Vehicles* 7, 3 (2022), 734–747.

[18] Richard Baker and Ivan Martinovic. 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA, 407–424.

[19] Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. 2018. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. , 3–12 pages.

[20] Robert Basmadjian. 2021. Communication vulnerabilities in electric mobility hcp systems: a semi-quantitative analysis. *Smart Cities* 4, 1 (2021), 405–428.

[21] Mihir Bellare, Phillip Rogaway, and Terence Spies. 2010. The FFX mode of operation for format-preserving encryption. *NIST submission* 20, 19 (2010), 1–18.

[22] Narayan Bhusal, Mukesh Gautam, and Mohammed Benidris. 2021. Cybersecurity of Electric Vehicle Smart Charging Management Systems. In *2020 52nd North American Power Symposium (NAPS)*. 1–6.

[23] Sinan Cai and Ryuji Matsuhashi. 2022. Optimal dispatching control of EV aggregators for load frequency control with high efficiency of EV utilization. *Applied Energy* 319 (2022), 119233.

[24] Ashwin Chandwani, Saikat Dey, and Ayan Mallik. 2020. Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and countermeasures. *IEEE access* 8 (2020), 226982–226998.

[25] Ronald Cramer, Ivan Bjerre Damgård, et al. 2015. *Secure multiparty computation.* Cambridge University Press.

[26] Syed Muhammad Danish, Kaiwen Zhang, Hans-Arno Jacobsen, Nouman Ashraf, and Hassaan Khaliq Qureshi. 2021. BlockEV: Efficient and Secure Charging Station Selection for Electric Vehicles. *IEEE Transactions on Intelligent Transportation Systems* 22, 7 (2021), 4194–4211.

[27] Thusitha Thilina Dayaratne, Carsten Rudolph, Ariel Liebman, and Mahsa Salehi. 2022. 15 - False data injection attacks on distributed demand response: I'm paying less: A targeted false data injection attack against distributed device scheduling. In *Decentralized Frameworks for Future Power Systems*, Mohsen Parsa Moghaddam, Reza Zamani, Hassan Haes Alhelou, and Pierluigi Siano (Eds.). Academic Press, 391–421.

[28] Palak Dixit, Pronaya Bhattacharya, Sudeep Tanwar, and Rajesh Gupta. 2022. Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey. *Expert Systems* 39, 5 (2022), e12754.

[29] Typhoon HIL Documentation. 2023. https://www.typhoon-hil.com/documentation/typhoon-hil-software-manual/References/iso15118_protocol.html Online; accessed 07-Nov-2023.

[30] Sébastien Dudek, Jean-Christophe Delaunay, and Vincent Fargues. 2019. V2G Injector: Whispering to cars and charging units through the Power-Line. (2019), 5–7.

[31] Hossam ElHussini, Chadi Assi, Bassam Moussa, Ribal Atallah, and Ali Ghrayeb. 2021. A Tale of Two Entities: Contextualizing the Security of Electric Vehicle Charging Stations on the Power Grid. *ACM Trans. Internet Things* 2, 2, Article 8 (mar 2021), 21 pages.

[32] David Elmo, George Fragkos, Jay Johnson, Kenneth Rohde, Sean Salinas, and Junjie Zhang. 2023. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6. In *2023 Resilience Week (RWS)*. 1–8.

[33] Rainer Falk and Steffen Fries. 2012. Electric vehicle charging infrastructure security considerations and approaches. *Proc. of INTERNET* (2012), 58–64.

[34] Rainer Falk and Steffen Fries. 2013. Securely connecting electric vehicles to the smart grid. *Int. Journal on Advances in Internet Technology* 6, 1 (2013).

[35] Javad Fattahi. 2024. A Federated Byzantine Agreement Model to Operate Offline Electric Vehicle Supply Equipment. *IEEE Transactions on Smart Grid* 15, 2 (2024), 2004–2016.

[36] International Organization for Standardization. 2014. ISO 15118-2 Road vehicles–vehicle-to-grid communication interface–part 2: network and application protocol requirements.

[37] International Organization for Standardization. 2015. ISO 15118-3 Road vehicles–vehicle-to-grid communication interface–part 2: network and application protocol requirements.

[38] Zacharenia Garofalaki, Dimitrios Kosmanos, Sotiris Moschoyiannis, Dimitrios Kallergis, and Christos Douligeris. 2022. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP). *IEEE Communications Surveys Tutorials* 24, 3 (2022), 1504–1533.

[39] Peyman Amirpour Giglou and Sajad Najafi Ravadanegh. 2021. Defending against false data injection attack on demand response program: A bi-level strategy. *Sustainable Energy, Grids and Networks* 27 (2021), 100506.

[40] Raju Gottumukkala, Rizwan Merchant, Adam Tauzin, Kaleb Leon, Andrew Roche, and Paul Darby. 2019. Cyber-physical System Security of Vehicle Charging Stations. In *2019 IEEE Green Technologies Conference(GreenTech)*. 1–5.

[41] Erdem Gumrukcu, Ali Arsalan, Grace Muriithi, Charukeshi Joglekar, Ahmed Aboulebdeh, Mustafa Alparslan Zehir, Behnaz Papari, and Antonello Monti. 2022. Impact of cyber-attacks on EV charging coordination: The case of single point of failure. In *2022 4th Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 506–511.

[42] Christina Höfer, Jonathan Petit, Robert Schmidt, and Frank Kargl. 2013. POPCORN: privacy-preserving charging for eMobility. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. 37–48.

[43] Arif Hussain, Ankit Yadav, and Gelli Ravikumar. 2024. Anomaly Detection Using Bi-Directional Long Short-Term Memory Networks for Cyber-Physical Electric Vehicle Charging Stations. *IEEE Transactions on Industrial Cyber-Physical Systems* 2 (2024), 508–518.

[44] International Organization for Standardization. 2022. ISO 15118-20: Road Vehicles – Vehicle to Grid Communication Interface – Part 20: 2nd Generation Network and Application Protocol Requirements.

[45] Devki Nandan Jha, Graham Lenton, James Asker, David Blundell, Martin Higgins, and David CH Wallom. 2024. A Run-Time Framework for Ensuring Zero-Trust State of Client's Machines in Cloud Environment. *IEEE Transactions on Cloud Computing* (2024).

[46] Jay Johnson, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, Kandy Phan, Michael Kunz, Rick Pratt, et al. 2022. *Cybersecurity for electric vehicle charging infrastructure.* Technical Report. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[47] Jay Johnson, Timothy Berg, Benjamin Anderson, and Brian Wright. 2022. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. *Energies* 15, 11 (2022), 3931.

[48] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning organizations to post-quantum cryptography. *Nature* 605, 7909 (2022), 237–243.

[49] Dustin Kern, Christoph Krauß, and Matthias Hollick. 2024. Attack Analysis and Detection for the Combined Electric Vehicle Charging and Power Grid Domains. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*. 1–12.

[50] Omniyah Gul M Khan, Ehab El-Saadany, Amr Youssef, and Mostafa Shaaban. 2019. Impact of electric vehicles botnets on the power grid. In *2019 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 1–5.

[51] Ahmet Kilic. 2023. Plug and Charge solutions with vehicle-to-grid communication. *Electric Power Components and Systems* 51, 16 (2023), 1786–1814.

[52] Ahmet Kilic. 2024. TLS-handshake for Plug and Charge in vehicular communications. *Computer Networks* 243 (2024), 110281.

[53] Yoonjib Kim, Saqib Hakak, and Ali Ghorbani. 2023. Smart grid security: Attacks and defence techniques. *IET Smart Grid* 6, 2 (2023), 103–123.

[54] Silke Kirchner and Helen Ruiz. 2023. OCPP Interoperability: Democratized Future of Charging. In *36th International Electric Vehicle Symposium & Exposition (EVS36)*. 1–12. ISSN: 2166-9546.

[55] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. 2022. Brokenwire: Wireless disruption of ccs electric vehicle charging. (2022).

[56] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. 2022. End-to-End Wireless Disruption of CCS EV Charging. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 3515–3517.

[57] Jae Kwon and Ethan Buchman. 2019. Cosmos whitepaper. *A Netw. Distrib. Ledgers* 27 (2019), 1–32.

[58] Seokcheol Lee, Yongmin Park, Hyunwoo Lim, and Taeshik Shon. 2014. Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology. In *2014 International Conference on IT Convergence and Security (ICITCS)*. 1–4.

[59] Alexios Lekidis. 2024. Anomaly detection mechanisms for in-vehicle and V2X systems. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*. 1–8.

[60] Gaolei Li, Jun Wu, Jianhua Li, Zhitao Guan, and Longhua Guo. 2018. Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE. *IEEE Access* 6 (2018), 11278–11288.

[61] Xupeng Li, Xuheng Li, Christoffer Dall, Ronghui Gu, Jason Nieh, Yousuf Sait, and Gareth Stockwell. 2022. Design and verification of the arm confidential compute architecture. In *16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22)*. 465–484.

[62] Yuancheng Li and Baiji Hu. 2020. An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain. *IEEE Transactions on Smart Grid* 11, 3 (2020), 2627–2637.

[63] Yuancheng Li and Baiji Hu. 2021. A Consortium Blockchain-Enabled Secure and Privacy-Preserving Optimized Charging and Discharging Trading Scheme for Electric Vehicles. *IEEE Transactions on Industrial Informatics* 17, 3 (2021), 1968–1977.

[64] Hanna Lindwall. 2020. *A Concept for an Intrusion Detection System over Automotive Ethernet.*

[65] Tehseen Mazhar, Hafiz Muhammad Irfan, Sunawar Khan, Inayatul Haq, Inam Ullah, Muhammad Iqbal, and Habib Hamam. 2023. Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet* 15, 2 (2023), 83.

[66] Roberto Metere, Zoya Pourmirza, Sara Walker, and Myriam Neaimeh. 2022. An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure. arXiv:2209.07842

[67] Adrian Gabriel Morosan and Florin Pop. 2017. OCPP security - Neural network for detecting malicious traffic. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems* (Krakow Poland, 2017-09-20). ACM, 190–195.

[68] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi. 2022. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security* 112 (2022), 102511.

[69] Myriam Neaimeh and Peter Bach Andersen. 2020. Mind the gap-open communication protocols for vehicle grid integration. *Energy Informatics* 3 (2020), 1–17.

[70] OCPI 2.2 2020. *OCPI 2.2: Open Charge Point Interface.* Standard. EV Roaming Foundation.

[71] Michalis Pachilakis, Antonios A Chariton, Panagiotis Papadopoulos, Panagiotis Ilia, Eirini Degkleri, and Evangelos P Markatos. 2020. Design and implementation of a compressed certificate status protocol. *ACM Transactions on Internet Technology (TOIT)* 20, 4 (2020), 1–25.

[72] Zoya Pourmirza and Sara Walker. 2021. Electric Vehicle Charging Station: Cyber Security Challenges and Perspective. In *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*. 111–116.

[73] Dwidharma Priyasta, Hadiyanto Hadiyanto, and Reza Septiawan. 2022. An Overview of EV Roaming Protocols. In *E3S Web of Conferences*, Vol. 359. EDP Sciences, 05006.

[74] Dwidharma Priyasta, Reza Septiawan, et al. 2023. Enabling EV Roaming Through Cascading WebSockets in OCPP 1.6. *Journal Européen des Systèmes Automatisés* 56, 3 (2023).

[75] Gururaghav Raman, Jimmy Chih-Hsien Peng, and Talal Rahwan. 2019. Manipulating Residents' Behavior to Attack the Urban Power Distribution System. *IEEE Transactions on Industrial Informatics* 15, 10 (2019), 5575–5587.

[76] Zakir Rather, Rangan Banerjee, Angshu Nath, and Payal Dahiwale. 2021. Fundamentals of Electric Vehicle Charging Technology and its Grid Integration. *Nationally Determined Contributions-Transport Initiative for Asia (NDC-TIA)* (2021).

[77] Juan E. Rubio, Cristina Alcaraz, and Javier Lopez. 2018. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 1–5.

[78] Omid Sadeghian, Arman Oshnoei, Behnam Mohammadi-ivatloo, Vahid Vahidinasab, and Amjad Anvari-Moghaddam. 2022. A comprehensive review on electric vehicles smart charging: Solutions, strategies, technologies, and challenges. *Journal of Energy Storage* 54 (2022), 105241.

[79] Khaled Sarieddine, Mohammad Ali Sayed, Sadegh Torabi, Ribal Atallah, and Chadi Assi. 2023. Investigating the security of ev charging mobile applications as an attack surface. *ACM Transactions on Cyber-Physical Systems* 7, 4 (2023), 1–28.

[80] Khaled Sarieddine, Mohammad Ali Sayed, Sadegh Torabi, Ribal Attallah, Danial Jafarigiv, Chadi Assi, and Mourad Debbabi. 2024. Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. 977–989.

[81] Mohammad Ali Sayed, Ribal Atallah, Chadi Assi, and Mourad Debbabi. 2022. Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power & Energy Systems* 137 (2022), 107784.

[82] Wellington Fernandes Silvano and Roderval Marcelino. 2020. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future generation computer systems* 112 (2020), 307–319.

[83] Saleh Soltan, Prateek Mittal, and H Vincent Poor. 2018. {BlackIoT}:{IoT} botnet of high wattage devices can disrupt the power grid. In *27th USENIX Security Symposium (USENIX Security 18)*. 15–32.

[84] Soyeon Son, Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. 2024. Securing EV Charging System against Physical-layer Signal Injection Attack. In *2024 Symposium on Vehicles Security and Privacy (VehicleSec)*. 1–11.

[85] Vinay Simha Reddy Tappeta, Bhargav Appasani, Suprava Patnaik, and Taha Selim Ustun. 2022. A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles. *Energies* 15, 18 (2022).

[86] Mingjian Tuo, Arun Venkatesh Ramesh, and Xingpeng Li. 2020. Benefits and Cyber-Vulnerability of Demand Response System in Real-Time Grid Operations. In *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 1–6.

[87] Binod Vaidya and Hussein T Mouftah. 2020. Multimodal and multi-pass authentication mechanisms for electric vehicle charging networks. In *International Wireless Communications and Mobile Computing (IWCMC)*. 371–376.

[88] Fabian van den Broek, Erik Poll, and Bárbara Vieira. 2015. Securing the Information Infrastructure for EV Charging. In *Wireless and Satellite Systems*, Prashant Pillai, Yim Fun Hu, Ifiok Otung, and Giovanni Giambene (Eds.). Springer International Publishing, Cham, 61–74.

[89] Mart van der Kam and Rudi Bekkers. 2023. Mobility in the Smart Grid: Roaming Protocols for EV Charging. *IEEE Transactions on Smart Grid* 14, 1 (2023), 810–822.

[90] Mart van der Kam and Rudi NA Bekkers. 2020. Design principles for an 'ideal'EV roaming protocol: Report D6. 3 for the evRoaming4EU project. (2020).

[91] Mart van der Kam, Roland Ferweda, and Rudi NA Bekkers. 2020. Developing roaming protocols for EV charging: Insights from the field. *Proceedings of the 8th Transport Research Arena (TRA'20)* (2020).

[92] Vector 2022. CCS Listener. https://www.vector.com/int/en/products/products-a-z/hardware/vh5110a.

[93] Wenya Wang, Yakang Li, Chao Wang, Yuan Yan, Juanru Li, and Dawu Gu. 2021. Re-check your certificates! experiences and lessons learnt from real-world HTTPS certificate deployments. In *Network and System Security: 15th International Conference, NSS 2021, Tianjin, China, October 23, 2021, Proceedings 15*. Springer, 17–37.

[94] Fanrong Wei and Xiangning Lin. 2023. Cyber-physical attack launched from EVSE botnet. *IEEE Transactions on Power Systems* 39, 2 (2023), 3603–3614.

[95] Daniel Zelle, Markus Springer, Maria Zhdanova, and Christoph Krauß. 2018. Anonymous Charging and Billing of Electric Vehicles. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (Hamburg, Germany) *(ARES '18)*. Association for Computing Machinery, New York, NY, USA, Article 22, 10 pages.

[96] Maria Zhdanova, Julian Urbansky, Anne Hagemeier, Daniel Zelle, Isabelle Herrmann, and Dorian Höffner. 2022. Local power grids at risk–an experimental and simulation-based analysis of attacks on vehicle-to-grid communication. In *Proceedings of the 38th Annual Computer Security Applications Conference*. 42–55.

[97] Hongbo Zhu, Hui Yin, Xue Feng, Xinxin Zhang, and Zongyao Wang. 2023. Demand Response Management via Real-Time Pricing for Microgrid with Electric Vehicles under Cyber-Attack. *Electronics* 12, 6 (2023).

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009