A Detailed Security Assessment of the EV Charging Ecosystem

Joseph Antoun, Mohammad Ekramul Kabir, Bassam Moussa, Ribal Atallah, and Chadi Assi

Abstract

The drive for efficient, reliable, green, and connected smart cities has promoted the use of electric vehicles (EVs) as the main future means of transportation. This resulted in a breakthrough in the anticipated number of adopted EVs by the year 2020, and consequently an urge for an available and trustworthy EV charging infrastructure. The diversity of the involved players, the used technologies, the bulk data exchange, and the widespread nature of the charging network give rise to security concerns in the form of message tampering, spoofing, or delaying among others to disconcert the charging service along with the underlying power layer. Furthermore, confidentiality and privacy of user information (i.e. identity, location, payment information, etc.) is another major concern associated with the deployment and use of the charging infrastructure. Thus, there is a need to identify and classify such concerns, and devise suitable solutions for a secure charging infrastructure. In this paper, we present a security assessment of the EV charging infrastructure. We highlight and categorize cyber threats targeting different players in a charging system, along with the security solutions presented in the literature. Finally, we present a gap analysis and insights into future research directions for EV charging system security.

Introduction

The wide adoption of electric vehicles (EVs) is expected to accelerate especially with advancements in reforming the power grid to a smart grid. Due to their environmental benefits (i.e., reduced greenhouse emissions), their role in the grid's ancillary services, dynamic energy pricing, and governmental incentives, the number of EVs in use is expected to grow from 3 million to 125 million by 2030 [1].

To achieve this goal, countries around the globe set their own target in EV adoption; for example, the Quebec government in Canada targets to reach 1 million EVs by 2030, while it is expected to be 100 thousand by 2020 [2]. Unfortunately, the reality (24000 EV are active in Quebec as of 2018[1]) indicates that Quebec is still far away from its self imposed target. Actually, range anxiety among several challenges restrains most countries from achieving their specified EV adoption target, and an adequate charging infrastructure is required to mitigate such anxiety.

Hence, to facilitate the integration and use of EVs, and to address their associated challenges, an interconnected charging infrastructure is currently ought to be developed to manage the smart charging and discharging of electric vehicles [3]. Several stakeholders take part in this infrastructure and contribute differently to the provided services, including EV users, distribution network utilities providing charging stations (CS) and electric vehicles supply equipment (EVSE), electricity suppliers and communication companies. Indeed, two-way flow of energy and information between the EVs and the infrastructure is a key enabling technology for EV smart charging through public or private charging stations.

Nevertheless, advancements in the deployment and use of this infrastructure face concerns associated with the nature of the provided services and the used technologies. Indeed, along with the advantages introduced by information and communication technologies, the system acquires their associated security concerns and threats. Those threats escalate with the wide deployment of public charging stations, and the random mobility of EVs which augment the attack surface along with chances to spread infections across the system. Furthermore, critical data will be shared across the EV-charging system, including location information, charging duration, EV identity, state of charge (SoC), payment info, etc. This gives rise to cyber-attacks targeting user privacy and charging network availability [4].

For instance, public charging stations demand user data, currently stored on an RFID card, to complete a transaction. Based on the outcome of a recent report by Kaspersky Labs [5], the user data stored on those cards can be copied, replicated, and used for unauthorized charging transactions. Moreover, through a Man-in-the-Middle (MitM) attack exploiting the USB port on CSs, logs and critical data can be copied, and malicious firmware can be injected into those CSs [5]. Similar exploits exist in private home smart chargers; an intruder can gain control over the charging scheduler to change the EV charging power, terminate the charging process, or reschedule it to a later time [6].

On the other hand, vulnerabilities existing in the EVs can be exploited through cyber-attacks. Using the vehicle identification number (VIN) of a Nissan Leaf, an attacker managed to remotely connect to and gain control over the vehicle [7]. During this attack, the attacker could turn the EV

[1] According to FleetCarma's data.

Digital Object Identifier:
10.1109/MNET.001.1900348

J. Antoun, M.E. Kabir, and C. Assi are with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada; B. Moussa is with Thales Research and Technology, Montreal, QC, Canada; R. Atallah is with the Hydro-Quebec Research Institute, Varennes, QC, Canada.
B. Moussa is funded by a FRQNT postdoctoral research scholarship.

on and off, change the climate settings, download the logs stored at the vehicle, and collect data about the vehicle usage including ride distance, charging process times, SoC, etc.

The presence of the previously mentioned threats, along with the existence of multiple actors in the EV and charging infrastructure ecosystem, give rise to the need for a comprehensive security assessment to expose the security threats and gaps endangering advancements of the deployment of this technology. Indeed, the integration of electrical, communication, and transportation systems empowers attackers to exploit vulnerabilities, normally localized in one system, and disrupt the functionality of multiple sectors. In this paper, we aim at exploring the threat landscape that would breach EVs and their charging infrastructure in an attempt to provide a comprehensive survey of the challenges to secure this system.

We believe the literature lacks a similar study that covers security challenges and threats for EVs, and provides insights into future research directions.

The remainder of this manuscript is structured as follows. The next section presents related work. The EV charging system is covered in the following section, followed by our security assessment. Then we discuss countermeasures from the literature, followed by a gap analysis. Concluding remarks are given in the final section.

Related Work

The security of EVs and their charging infrastructure recently attracted much interest from the research community. Early in 2013, Mustafa *et al*. [8] provided a generic study of the security aspect of smart EV charging. The authors devised a model of smart EV charging and identified possible threats, in addition to proposing some security requirements for their model. However, their presented model and study was a generalized one and lacked details about security challenges in the charging infrastructure architecture. Privacy concerns associated with E-mobility were the target of Langer *et al*. in [9]. The authors of [9] presented four fundamental use cases and analyzed their implication on user's privacy. Moreover, they provided possible solutions to help obscure consumer's power consumption and location. Recently, Fariji *et al*. [10] identified the security threats and attacks targeting the PUVEC (Urban Platform for Connected Electric Vehicles) project and the Internet of Vehicles (IoV) communications technology. Their work was more focused on the threats, attacks and vulnerabilities related to the architecture and communication system under study. On the other hand, threats imposed by EV usage on the grid was described by Clyde *et al*. in [11]. The authors discussed the negative effects of EVs mass charging on the grid operations, and considered attacks initiated from EVs to target the grid. Through their analysis, they pointed out that such attacks are capable of affecting the grid's stability. The literature lacks a comprehensive security assessment of the electric vehicle intelligent charging infrastructure. In this paper, we aim at presenting an assessment that details threats associated with EVs and their charging infrastructure. Our assessment will cover the existing exploits along with solutions proposed in the literature, and the unaddressed security gaps.

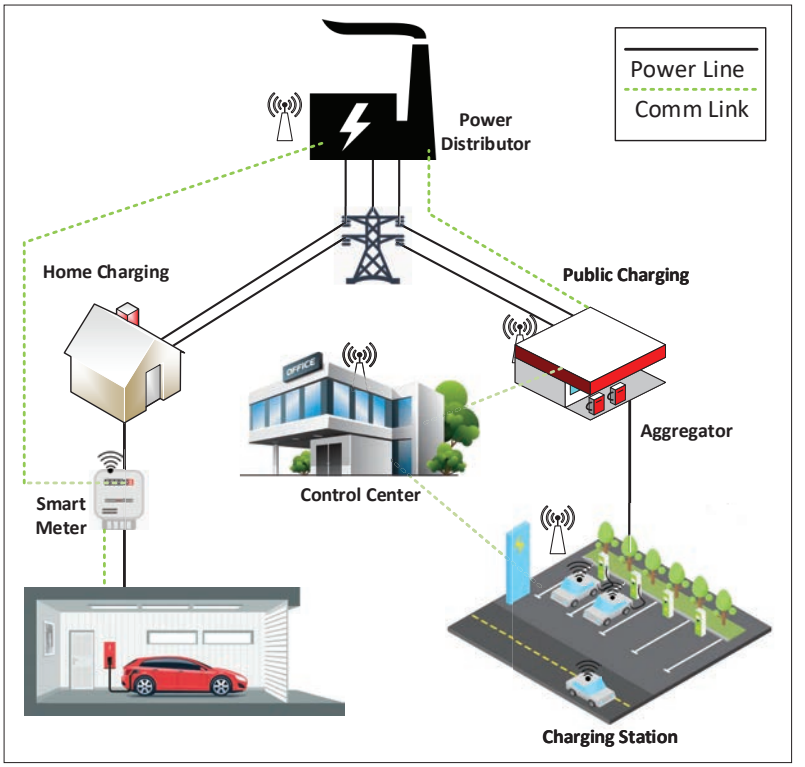

FIGURE 1. EV charging system module.

Charging System

In this section we present an overview of the EV charging system, presented in Fig. 1, including the charging scenarios, and the charging model used throughout this manuscript.

Charging Scenarios

The EV charging infrastructure is deployed at the customer premises, in office buildings, and at public stations. The widespread nature of this infrastructure facilitates the usability of EVs, and consequently involves different agents in the charging process depending on the charging location. EV charging at residential locations requires a connection to an EVSE available at the premises. This EVSE is normally connected to the user's smart meter to benefit from dynamic pricing policies issued by the utility. Currently, EVSEs deployed by users at home are labeled as smart chargers, connected to the Internet to manage the charging procedure, and automatically add the consumption to the customer's electric bill.

Parking lots at work spaces might be equipped with an EVSE to offer a charging service for employees. Employees usually spend approximately eight hours or more at their offices, during which an EV can be charged or discharged to offer ancillary services for the gird. A typical company might offer a flat rate price for its employees for charging, or bill them following their power consumption. In order to enable such services, the EVSE connects to a smart meter for the purpose of acquiring electricity prices from the distributor. Furthermore, the EVSE is capable of identifying users for billing purposes.

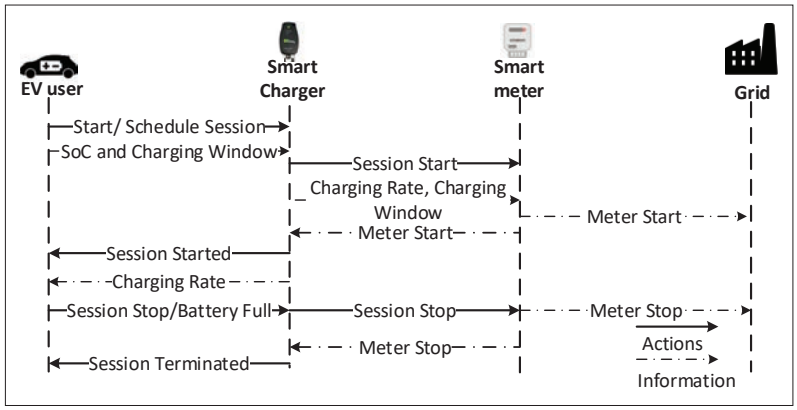

FIGURE 2. Home charging sequence diagram.

Alternative charging places for EVs are public charging stations available at shopping malls, highway rest areas, etc. Installed by commercial operators or the power distribution network utilities, EVSEs provide charging services at those locations. Similarly, dedicated charging stations, similar to gas stations, are built for the purpose of providing charging services for EVs. EV owners use these stations to recharge their vehicles and pay for the used services. On the other hand, some residential buildings might not be equipped with a dedicated EV parking area. In such cases, EVSEs can be located on the street to offer charging services to EV owners in such buildings. For public charging, EV users pay the operator of public EVSEs in return for the service. To ensure bill fairness, the operator communicates with the supplier to acquire the correct pricing, and forwards this price to EV users.

Charging Model

Based on the above mentioned scenarios, we elaborate a charging model composed of a set of entities and their interactions as follows.

Entities: Different actors are involved in the charging process depending on the used charging locations. We identify the following entities in the charging process:

- EV: an electric powered vehicle.
- User: an owner of an EV, or someone who uses an EV and pays for consumed power.
- Electric vehicle supply equipment (EVSE): a component that connects the EV to the Grid.
- Smart meter (SM): an advanced metering device that measures electricity usage, communicates with the grid utility, and controls and schedules the operations of residential electrical appliances including EVs.
- Smart charger: a device that regulates the charging procedure, scheduling, and charging power.
- Charging station: a public place equipped with EVSEs for EV charging.
- Aggregator: an entity that manages the two-way electrical demand and supply between the power distribution utility and its associated charging stations.
- Control center: the central management unit for the power grid operations, including the supervision of charging requests issued by roaming EVs and EVSEs present in charging stations.
- Power distributor: an electricity provider for residential premises and public charging stations.

Communications and Data Shared Between Entities: The EV charging ecosystem requires the exchange of various messages over different communication links while using public charging stations as well as private ones. However, the communicated data differs from one charging scenario to another as we highlight in this section.

Home charging includes the following communication:

- Physical connection between EV and EVSE to charge/discharge the EV's battery where SoC is shared.
- Secure connection between a user and deployed smart charger, mostly over wireless links to schedule and manage the EV charging process, where the SoC and charging parameter (i.e., current, rate, start and stop time, etc) are shared.
- Data communication between SM and smart charger to track the amount of power delivered from/to the charger. Meter start and stop commands as well as pricing data are shared over this link.
- Data communication between SM and power distributor for billing purposes and load consumption tracking, where the distributor shares the power price and availability and the SM sends power consumption parameters.

We represent the actions and communication taking place in a home charging paradigm as a sequence diagram in Fig. 2. Through this exchange, the EV shares its SoC with the smart charger, and schedules its charging window.

Public charging includes the following communication:

- Physical connection between EV and EVSE to ensure power delivery to the EV's battery and SoC sharing.
- Communication between users and control center (aggregator) or CS to reserve an EVSE, and negotiate the charging process parameters. Over this link, a multitude of data is shared, including EV-ID, EV location, SoC, charging parameters, payment info, availability, and price.
- Communication between control center and the CS where the control center sends the EV data to the CS, and ensures the availability of the EVSE for the requesting EV. The exchanged data includes EV ID, SoC, along with the CS-ID, and IDs of available outlets.
- Data communication between the control center and the power distributor to negotiate dynamic power pricing, and the amount of power that can be drawn at a specific time. This includes the communication of the power price and availability, in addition to power consumed.
- Communication between aggregator and control center to provide and manage EVs participation in ancillary services. In this case, EVs IDs, payment info, and power needed are exchanged.

Figure 3(a) depicts actions and information sequence implied in a public charging scenario, where data is being shared between all the

entities taking part in this process. In addition, in figure 3(b) we see the OCPP commands sent and received between CS and CC during such a process.

The described charging scenarios include the transfer of private and confidential information such as the participating EVs location, ID, SoC, and payment info. Moreover, the management of the charging process is made possible through the successful delivery of various control messages. The availability, confidentiality and integrity of such messages is essential to ensure the physical integrity of the grid, the EV battery, and the availability of EV charging outlets.

Protocols and Standards

The management of charging and billing actions in the EV charging ecosystem is made possible through different protocols. Some of those protocols are standardized such as the ISO 15118[2], and others are widely deployed and used such as OCPP[3]. To start with, the ISO 15118 is an international standard that outlines the digital communication protocol that an EV and CS should use to recharge EV's high-voltage battery. The smart charging mechanism built into ISO 15118 makes it possible to match the grid's capacity with the energy demand for the growing number of EVs that connect to the electrical grid. ISO 15118 allows EVs and CS to dynamically exchange information based on which a proper charging schedule can be negotiated. Without secure communication between EVs and CS, malicious third parties can intercept and modify messages and tamper with billing information. For that purpose, ISO 15118 introduced the Plug & Charge feature. Through this feature, the EV and CS are required to establish and share a secure communication link. This implies that both the EV and CS must be able to encrypt and decrypt messages, and consequently ensure the confidentiality and integrity of the established communication, along with mutual authentication.

On the other hand, different protocols are used to manage communication in EV charging paradigms. J1772 and CHAdeMO exist as standard protocols to govern the communication of fast charging between CS and EVSE, while the Open Charge Point Protocol (OCPP) developed in The Netherlands is used to govern all information communication between CS and control center. OCPP is an initiative led by the Open Charge Alliance (OCA). It is an open communication protocol that allows electric vehicles charging stations and central management software to communicate with each other. The protocol has been adopted by dozens of leading charging station providers and auto manufacturers around the world. OCPP exists in different versions (1.2, 1.5, 1.6, 2.0). The wide usage of version 1.5 and 1.6 of OCPP made it a global standard. OCPP makes use of SOAP and JSON frameworks, which makes it possible to send messages between components over the Internet. Within OCPP 1.5 and 1.6, 25 operations are described, 10 are initiated by the charge point and 15 by the control center. According to ChargeHub[4], public charging networks in Quebec are operated by Chargepoint, FLO, and Electric Circuit. Those three networks use OCPP as their main communication protocol in order to manage the flow of information between their stations and control center, as well as communications between networks themselves.[5]

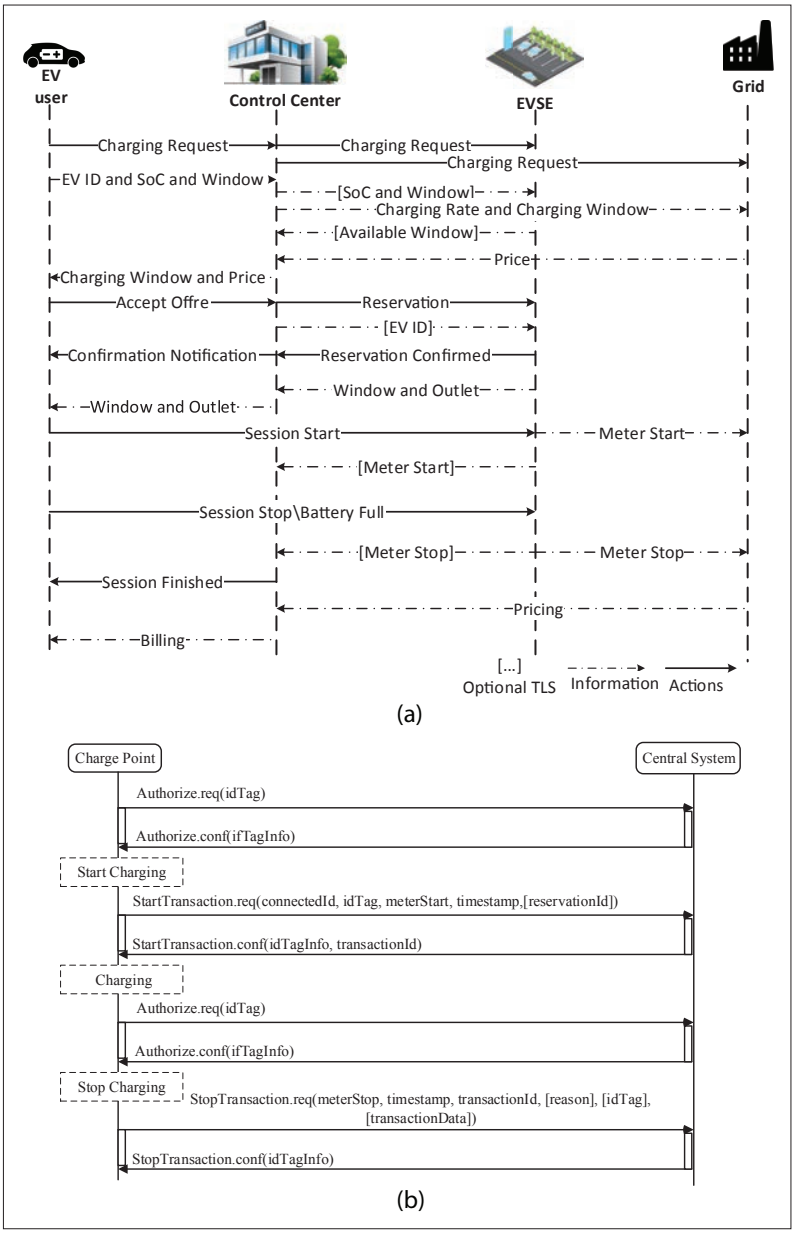

FIGURE 3. Public charging sequence diagram.

Threats and Vulnerabilities

The EV smart charging paradigm inherits a multitude of security concerns and vulnerabilities from all the participating actors. Those vulnerabilities are associated with the actors themselves, the exchanged messages, and the communication medium used. We depict the threats associated with the different security requirements, and present the vulnerabilities targeting the EV charging system. We can summarize those entities into three levels: EV, communication medium, and charging station or smart charger.

Threat Model

We consider an adversary interested in attacking the EVs and the charging infrastructure through exploiting vulnerabilities at the different entities

[2] https://www.iso.org/standard/69113.html

[3] https://www.openchargealliance.org/

[4] https://chargehub.com

[5] https://addenergietechnologies.com

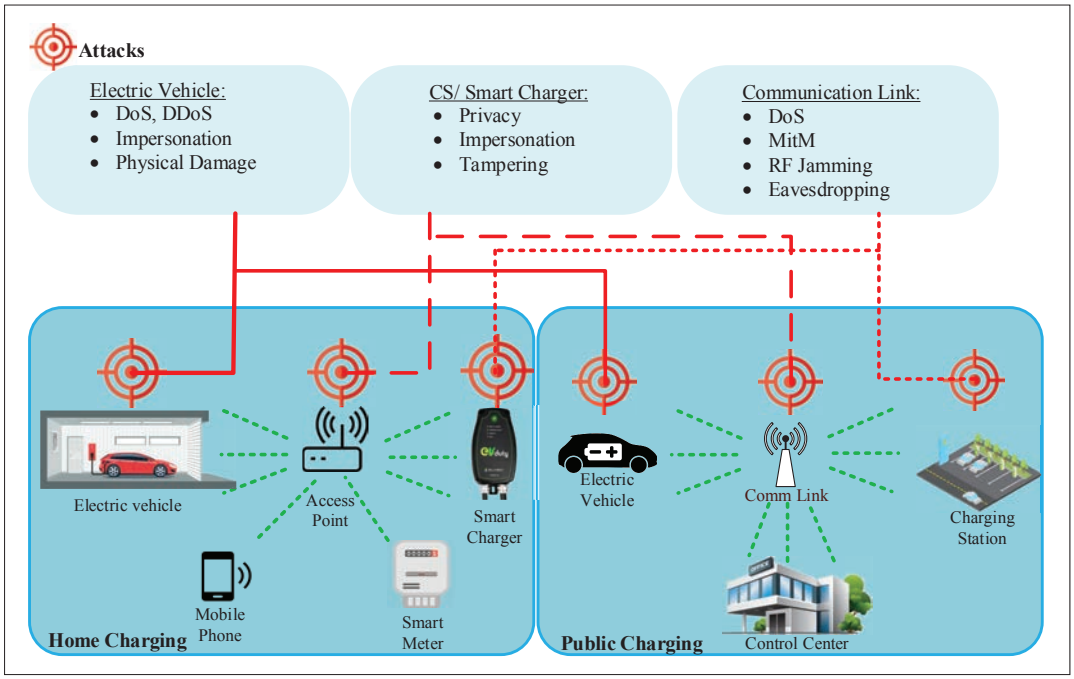

FIGURE 4. Electrical charging system potential threats.

participating in the charging scenarios. The attacker has the capability to perform reconnaissance activities to learn the environment, and prepare the necessary steps to execute his attack. Our attacker can sniff messages exchanged by the communicating parties, and get hand on the information exchanged in plain text. Moreover, the attacker can fake, intercept, inject, and modify similar messages.

Next, we discuss vulnerabilities in the home charging and public charging infrastructures. Those vulnerabilities are sum.marized in Fig. 4.

Home Charging Vulnerabilities

EV: EVs serve as IoT devices at residences, which makes them susceptible to various attacks. The communication between the battery management system at the EV and the charging station is subject to a message modification attack [12]. An attacker can intercept and modify, or fabricate the voltage and current parameters communicated by the battery management system to force a higher charging rate. This modification can degrade the battery life or even cause a burn out [12]. This attack can take place in the public charging scenario as well.

Communication Medium: An attacker breaking into the unsecured communication between the smart charger and the smart meter can collect messages to analyze the users charging habits, intercept and/or fabricate messages to start/stop the charging procedure, and thus impact the availability of the EV. Moreover, the attacker may target the scheduler at the smart charger through tampering with the charging requests sent to the charger. This can incur additional costs to the user if charging is re-scheduled to take place at peak times, and thus deny the user the advantages of dynamic pricing policies issued by utilities.

Smart Charger: The software component of the smart charger is subject to message injection attacks. Those attacks target the configuration of the SC, remote connectivity to the charger, and the scheduling of charging activities to result in denial of service at the smart charger level.

Public Charging Vulnerabilities

In the public charging scenario, we have a wider interconnected charging system with a large number of stakeholders. Some of the vulnerabilities identified for home charging scenarios can be found in public charging as well; nevertheless, those vulnerabilities have a higher impact on public charging due to the large number of EVs and their mobility.

EV: With the lack of appropriate security measures, EVs are a favorable attack surface used by adversaries to launch attacks against the public charging network [13]. Through a successful compromise of an EV, a malicious actor can compromise other EVs and the charging infrastructure as well [13]. The multiple compromised EVs can be used by the attacker to initiate a Denial of Service (DoS) or Distributed DoS (DDoS) attack by flooding the network with fake/unnecessary charging requests to reserve charging times. This attack overloads the charging schedules of public charging stations, and prevents them from serving benign EVs. Moreover, the same attack would affect the EV to control center communication, and prevents or delays prompt responses from the control center to non compromised EVs. On the other hand, the identity of an EV is subject to theft and later use by an attacker through EV impersonation for public charging billing purposes.

Communication Medium: The use of wireless communication in the public EVs charging ecosystem gives rise to a multitude of attacks such as jamming, eavesdropping, and Man-in-the-Middle (MitM). Jamming attacks are another form of DoS attacks. They affect system availability as messages may be dropped or delayed due to added noise on the wireless channel, and thus prevent the involved parties from communicating over the

wireless channel. On the other hand, a malicious user can eavesdrop messages sent on the wireless channel. This attack is a major concern associated with users private and confidential information. In fact, the communicated messages may carry payment information, identity, SoC, and location among others, which is considered confidential and private for the EV user. This concern escalates with the ability of a MitM to modify the communicated messages and affect the ongoing EV charging process.

On the other hand, public EV charging is enabled through the Open Charge Point Protocol (OCPP). OCPP coordinates communication and power flow between charging points, control center, the EVs and the grid. OCCP, by design, introduces several threats to the EV public charging system [14]. Those threats arise from the fact that OCCP communicates information in clear text, and can be categorized as follows:

- Disclosure: copying or reading private information.
- Distortion: fake data injection or spoofing.
- Disruption: Deleting or dropping messages.

To account for security, OCPP can be used with transport layer security (TLS) to provide confidentiality over the communication links. However, manufacturers ignore this practice as it introduces unwanted overhead and additional costs when using cellular networks for communication. However, in the presence of TLS, OCPP is subject to impersonation attacks where an attacker pretends to be a CS or the control center, to request or acquire private data regarding the charging transactions performed by the different EVs.

Charging Station: The majority of CSs are being deployed without proper physical security, and hence can be accessed by anyone. This makes them an accessible attack point that adversaries can use to target the charging network infrastructure. Further, once infected, a CS can help propagate malicious software to other CSs in the same network, as well as to connected EVs [13]. Moreover, an infected CS can be used to initiate an impersonation attack to send fake messages carrying erroneous information, for example CS location, to affect the integrity of the system.

On the other hand, CSs can be targeted through a MitM attacker that leverages vulnerabilities in OCPP. For instance, a MitM attacker can change the CS clock to delay communication with EVs, alter the connection status to reject legitimate connection requests, and produce a DoS through fake data [14]. Another impersonation attack, through OCPP, can target CS and result in a fake local authorization list (LAL) at the CS. The LAL allows a CS to operate in standalone manner in offline mode. An attacker impersonating the control center can delay the connection between the targeted CS and the benign control center, thus forcing the CS to go into offline mode, and rely on the fake LAL. This will later force the control center to accept any queued transactions produced by the offline mode operation. As an indirect consequence, this attack results in energy fraud and theft.

Furthermore, more serious threats arise when CSs are exploited to target the power grid. For instance, a MitM attack can affect the amount of power delivered during the transaction to a CS or a cluster of CSs. The attacker can perturb the rate of charging delivered by the CS, and reverse the power flow during peak hours, potentially overloading the grid. Moreover, if an attacker successfully injects a false message to indicate low power prices during peak time, he could initiate large scale EV charging processes, and eventually drive the grid into unstable conditions.

Mitigation and Proposed Solutions

With the increased adoption of EVs worldwide, securing smart EV charging systems becomes a pressing matter. In this section we review relevant security solutions previously proposed in the literature to secure the EV charging infrastructure. The authors of [15] tackled data privacy when using OCPP. The authors proposed a solution to prevent MitM attacks, and ensure a secure flow of data between a CS and the control center. A light modification of the original charging operation was designed that included additional steps after the stop transaction request. In this solution, the meter stop request is divided into shares sent separately and associated with a threshold value that defined the minimum number of error free shares needed to recover the message. However, this technique is faced by several challenges. For example, if the CS is forced into offline mode, according to OCPP, the CS should accept all transactions and queue them. In this case, the CS's storage system might get saturated since it has to store all the shares from all the queued transactions. This might lead to a loss of shares, and open a window for a buffer overflow attack [15]. This vulnerability can be exploited by an attacker to perform unrecorded charging sessions. To counteract those challenges, they propose a multi-step protocol composed of (i) charging request, (ii) authorization, (iii) charging response, and (iv) pay.ment, secured using public and private key cryptography.

A threat analysis and model for the propagation of cyber infections in the EV smart charging system is presented by Mousavian *et al.* in [13]. The authors devised a solution to counteract the propagation of cyber infections across the charging infrastructure while maintaining the EV charging services. Their solution was based on the disconnection of the infected EVSEs and was formulated as a linear program. The presented model is a good starting point to understand the severity of the threats facing the EV charging system. However, there is a need to detail those threats, and prepare the suitable countermeasures to handle such threats. OCPP was recently updated to include additional security features through OCPP 2.0. Those features include a secure communication channel, mutual authentication, secure firmware update process, logging of security events, and the addition of new messages, data types, and configuration keys. However, the threats targeting OCPP still prevail in deployments using earlier versions of the protocol. Furthermore, vehicular technology is in constant development either in industry or research.

The V2X or Vehicle to Everything communication paradigm is on the rise recently and has recently attracted significant attention from the research community. V2X can be leveraged in

Reference	Targeted area	Outcomes
[11]	Attacks and vulnerabilities	Identifying physical and cyber threats affecting the grid caused by attacks initiated from EVs.
[13]	Attacks, vulnerabilities and mitigation	Identifying the severity of an attack on EV network by studying the spread of malware over this network.
[14]	Attacks and vulnerabilities	Identifying existing vulnerabilities in the OCPP 1.6 protocol.
[15]	Mitigation and solutions	Suggesting a security measurement to secure data shared using OCPP in EV charging infrastructure.

TABLE 1. Summary of related work.

Threat level	Attacks	Affected properties
EV	DoS, DDoS, impersonation	Availability, privacy, confidentiality, authenticity
Communication medium	DoS, eavesdropping, MitM, jamming	Availability, privacy, confidentiality, integrity, authenticity
CS and smart charging	Impersonation, tampering	Integrity, privacy, authenticity

TABLE 2. EV Charging infrastructure security concerns.

EV charging infrastructure in order to help either secure the communication or enhance quality of service. V2X can help create a blockchain environment to enable security and privacy in EV charging infrastructure communications. However, increasing the number of connected entities in a system augments its attack surface, and consequently makes it more susceptible to attacks. In addition to V2X, an electric vehicle is expected to have its own digital signature and identifier (PKI, electronic licences plates, etc.). These technologies can help harden the data exchange security among vehicles and the charging infrastructure. In the case of EV, such features will add more encryption opportunities for the data shared within the charging infrastructure. However, integrating these new technologies in an existing system might be costly and hard to achieve. Those approaches are summed up in Table 1.

Gap Analysis

An EV smart charging ecosystem is shown to be vulnerable to various cyber-attacks as summarized in Table 2, and Fig. 4. The participating entities in the EV charging infrastructure share different types of data with a varying level of sensitivity. As a ramification, various attacks can be initiated on different entities at different stages of current EV charging practices and protocols. In this section, we highlight the security gaps that persist despite the existing efforts in the literature. We will categorize those gaps based on the requirements of the EV charging infrastructure.

Availability

Availability comes on top of the requirements of a secure EV charging infrastructure. However, the current infrastruc.ture's availability can be targeted by a multitude of attacks as highlighted in the previous section. DoS and DDoS are still a threat, especially for the public charging facilities. In addition, as OCPP is designed without security concerns, hijacking OCPP sessions and denying services through OCPP is a major threat to public charging as well. Even with OCPP 2.0, several specifications of the protocol can be exploited to target availability of the charging infrastructure. Thus, there is a need for a charging protocol that considers security as a major component of the charging process.

Confidentiality and Privacy

The confidentiality and privacy of the communicated data under different charging scenarios is another major challenge that needs to be overcome to facilitate the adoption of EVs. As most of the data is communicated in clear text form, this data is a candidate to be compromised by attackers. The challenge of ensuring the confidentiality and privacy of this data escalates with the diversity in the communicating entities. This gives rise to the need to deploy cryptographic and privacy preserving approaches to secure the communicated and collected data while taking into consideration the computational capabilities of the involved parties. ISO 15118 addresses confidentiality through symmetric-key cryptography. However, this requires that the EV and CS agree upon a symmetric key at the beginning of each charging session. This adds an overhead in the charging process as the charging station has to establish a different key with each EV.

Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its life cycle. The integrity of the communicated information is of extreme importance for the proper functioning of the charging infrastructure. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. In addition, integrity violation schemes need to be deployed to detect and prevent unauthorized data modifications before affecting the network on a wide scale. Using asymmetric cryptography in ISO 15118, data integrity verification can be realized. However, this still faces the same issues as highlighted in the previous section.

Authenticity and Nonrepudiation

Enforced authenticity of messages guarantees the communicating entities are the ones they claim to be, and the communicated message and commands are truthfully generated by the entities as claimed. Ensuring message authenticity while preserving the user's privacy is challenging. In addition, through proper authentication schemes, malicious users are denied the chance to impersonate key system players, and entities develop a notion of trust in their interactions. Currently, the deployed infrastructure lacks such a scheme and this results in several attacks, as highlighted in the previous section.

Finally, the lack of robust security mechanisms in the charging infrastructure lures attackers to infiltrate the infrastructure, and launch large scale attacks, especially with the increased connectivity and the rise of the Internet of Things (IoT). Thus, securing this infrastructure is of paramount importance to a more secure, robust, and reliable power grid.

Conclusion

The mass adoption of EVs indicates a paradigm shift in the transportation sector with notable effects on the ecosystem, and the critical infrastructure represented by the power grid as well. The positive impact of EV adoption carries with it several challenges, including security associated concerns. Indeed, with the deployed smart charging infrastructure, a diverse set of actors exchange real time data and contribute to provide charging services. However, this interconnected infrastructure along with the communication protocols used and the data exchanged is vulnerable to a multitude of cyber attacks that target the infrastructure availability and the user privacy as well. In this paper, we presented the EV smart charging system followed by a security assessment that highlighted the security threats and vulnerabilities targeting this system. We analyzed the threats in the context of both public and private charging facilities, and we reviewed the security solutions proposed in the literature. Finally, we provided insights into future work in the form of a gap analysis of the system security.

References

[1] T. Bunsen *et al.*, *Global EV Outlook 2018: Towards Cross-Modal Electrification*, 2018.

[2] https://montrealgazette.com/news/local-news/the-shift-to-electric-cars-are-we-there-yet

[3] J. Dong, C. Liu, and Z. Lin, "Charging Infrastructure Planning for Promoting Battery Electric Vehicles: An Activity-based Approach Using Multiday Travel Data," *Transportation Research Part C: Emerging Technologies*, vol. 38, 2014, pp. 44–55.

[4] N. Karali *et al.*, *Vehicle-Grid Integration*, 2017.

[5] https://www.kaspersky.com/blog/electric-cars-charging-problems/20652/

[6] https://securelist.com/remotely-controlled-ev-home-chargers-the-threats\ \-and-vulnerabilities/89251/

[7] https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[8] M. A Mustafa *et al.*, "Smart Electric Vehicle Charging: Security Enalysis," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2013, pp. 1–6.

[9] L. Langer *et al.*, "Privacy Issues of Smart e-mobility," In IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, pages 6682–6687. IEEE, 2013.

[10] Y. Fraiji *et al.*, "Cyber Security Issues of Internet of Electric Vehicles," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2018, pp. 1–6.

[11] C. Carryl *et al.*, "The PEV Security Challenges to the Smart Grid: Analysis of Threats and Mitigation Strategies," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, IEEE, 2013, pp. 300–05.

[12] F. Sagstetter *et al.*, "Security Challenges in Automotive Hardware/Software Architecture Design," in *Proceedings of the Conference on Design, Automation and Test in Europe*, EDA Consortium, 2013, pp. 458–63.

[13] S. Mousavian et al., "A Risk-based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, 2017, pp. 6160–6169.

[14] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, 2017, pp. 2452–2459.

[15] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2018, pp. 1–5.

Biographies

Joseph Antoun received his B.E. degree in computer and communications engineering from the Notre-Dame University of Louaizeh, Zouk Mosbeh, Lebanon, in 2018. Currently, he is pursuing his M.A.Sc. degree in electrical engineering at Concordia University in Montreal, Canada. He has been an active member of the IEEE since 2017. His current research interests span the areas of electric vehicle charging systems, cyber security, machine learning, intelligent transportation systems and queuing theory.

Mohammad Ekramul Kabir is a Ph.D. candidate in information systems engineering at Concordia Univeristy, Montreal, Canada. He has received the B.Sc. and M.S. degree in applied physics, electronics and communication engineering from the University of Dhaka, Bangladesh. His research interests include green charging of electric vehicle, smart grid, renewable energy, applications to smart city and machine learning.

Bassam Moussa is currently a postdoctoral fellow at Thales Research & Technology in artificial intelligence eXpertise (cortAIx) where he holds the FRQNT Postdoctoral Award. He received the Ph.D. degree in information and systems engineering from Concordia University, Montreal, in 2018. His research interests include cybersecurity for the smart grid, security of cyber-physical systems, IoT security, security metrics and time synchronization systems.

Ribal Atallah received the B.E. degree in computer engineering from the Notre Dame University of Louaize, Lebanon, in 2009, the M.Sc.E. degree in computer engineering from Lebanese American University in 2012, and the Ph.D. degree in information and systems engineering from Concordia University, Montreal, Canada, in 2017. Currently he is a cybersecurity research scientist at Hydro-Québec working on various machine learning algorithms to protect the smart grid against cyber attacks. His research interests include deep learning, deep reinforcement learning, cyber security of the smart grid, intelligent transportation systems and queuing theory.

Chadi Assi received the Ph.D. degree from the City University of New York (CUNY) in 2003. He is currently a full professor at Concordia University and an IEEE fellow. He was a recipient of the Prestigious Mina Rees Dissertation Award from CUNY in 2002 for his research on wavelength-division multiplexing optical networks. He is on the Editorial Board of *IEEE Communications Surveys and Tutorials*, *IEEE Transactions on Communications*, and *IEEE Transactions on Vehicular Technologies*. His current research interests are in the areas of network design and optimization, network modelling, and network reliability. Dr Assi is a fellow of the IEEE.