Electric Vehicle Charging Infrastructure: Review, Cyber Security Considerations, Potential Impacts, Countermeasures, and Future Trends

Deepak Ronanki, *Senior Member, IEEE*, and Harish Karneddi, *Graduate Student Member, IEEE*

***Abstract*— With the continual development of intellectualization and vehicle onboard communication networks, the cyber-physical security of modern electric vehicles (EVs) has captured paramount importance. Particularly, the powertrain and battery charging infrastructure are becoming more vulnerable to cyber-attacks owing to interconnectedness among the EVs in the intelligent traffic environment. Therefore, it urges the development of monitoring and diagnosis strategies to ensure secure and reliable power electronics systems for networked EVs. However, there is a lack of overview of the ramifications, detection, and mitigation approaches of cyber-attacks on battery charging infrastructure. This article aims to provide an overview of the latest research contributions regarding the evolution of battery charger architectures, control methods, EV supply equipment (EVSE), charging protocols, communication channels, and their compliance from the perspective of cyber security. Furthermore, the potential impacts of sabotage cyber-attacks on various popular battery chargers are explored through case studies. In addition, the latest hardware and software-intensive cyber-attack detection and countermeasure techniques are discussed and analyzed through case studies. Finally, distinct challenges and prospective research opportunities for establishing cyber-resilient EV battery charging systems are presented.**

***Index Terms*— Battery chargers, cyber-physical security, electric vehicles (EVs), power conversion harmonics.**

I. Introduction

ELECTRIC vehicles (EVs) have gained popularity owing to minimal maintenance, high well-to-wheel efficiency, and zero emissions [1]. However, the major limitation in the wide adoption of EVs is the lack of charging infrastructure. Over the past few years, significant research has been conducted in developing battery charging infrastructure, charging techniques, and several interfacing devices to enable faster power transfer with global compatibilities [2]. Recently, connected and automated EVs have captured significant attention with increasing communication technologies, including vehicle-to-grid (V2G), vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) [3]. The exponential growth of EVs is overloading the power system network. To overcome these concerns, the power system is interconnected, and their power allocation is monitored using cloud-based control [4]. Moreover, charging stations and EVs are connected through the EV supply equipment (EVSE) and interconnect with the cloud through communication channels for power monitoring, authorized access, and payments [5]. In addition, EVs communicate with other vehicles, infrastructure, auxiliary devices, Bluetooth keys, etc., as depicted in Fig. 1.

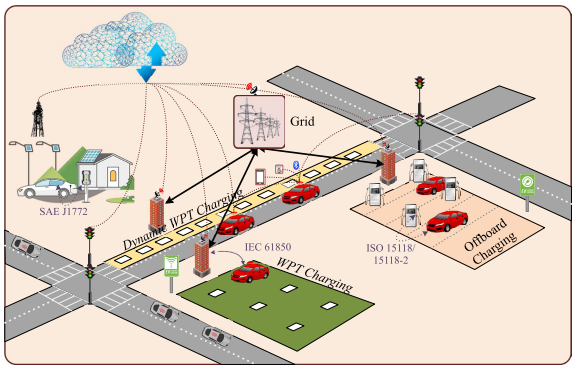

Fig. 1. Systematic architecture of the EVs and its charging infrastructure communication network.

This interconnection of EVs in the intelligent traffic environment, infrastructure for the powertrain, and battery charging is particularly becoming more susceptible to cyber-attacks. In addition, battery charging systems are more vulnerable to cyber threats with the growing penetration of Internet-of-Things (IoT)-enabled solutions in EVs and the grid [6]. Furthermore, the involvement of inadequately encrypted communication channels, networked electronic unit controls, outdated firmware, unsecured local access, weak passwords, and vulnerable customized hardware is directly exposed to cyber threats. Consequently, attackers can access sophisticated data, like the converter's sensor signals, battery management system (BMS), switching pulses, main control unit (MCU) of the EVSE, and communication channels [7]. Therefore, data integrity attacks (DIAs), denial of service (DoS) attacks, and other cyber threats are becoming more and more likely to affect power electronics systems. Consequently, these attacks may disrupt the charging infrastructure control and power converters, cause lasting damage to the battery, and influence the grid [8]. As a result, significant financial losses to the charging station organizations diminish user's trust and reputational damage [9]. Table I summarizes a few recent cyber-attacks on battery charging infrastructure and EVs [10], [11], [12], [13].

Manuscript received 3 May 2023; revised 30 August 2023; accepted 20 November 2023. Date of publication 27 November 2023; date of current version 5 February 2024. This work was supported in part by the Science and Engineering Research Board (SERB), Government of India, under Startup Research Grant (SRG) with Grant No: SRG/2021/000184; and in part by the IHUB NTIHAC Foundation, IIT Kanpur, with Grant No: IHUBNTIHAC/2021/01/05/1050. Recommended for publication by Associate Editor Sheldon Williamson. *(Corresponding author: Deepak Ronanki.)*

The authors are with the Department of Engineering Design, IIT Madras, Chennai 600036, India (e-mail: dronanki@ieee.org; ed20d016@smail.iitm.ac.in).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JESTPE.2023.3336997.

Digital Object Identifier 10.1109/JESTPE.2023.3336997

2168-6777 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

TABLE I
RECENT CYBER-PHYSICAL ATTACKS ON BATTERY CHARGING INFRASTRUCTURE

Time	Attack Description
Nov. 2021	A bug in the vehicle charging app provider in the UK resulted in the exposure of customer data and charge history.
Jan. 2022	Several charging stations had seven vulnerabilities that allowed remote attackers to impersonate admin users and undertake actions on their behalf.
Feb. 2022	A hacker in Ukraine disrupted EV charging stations on a 450-mile route between Moscow and St. Petersburg.
April 2022	An EV charging station on the Isle of Wight was hacked to display illegal information, and some EV owners were also getting high-voltage failure codes, leaving them stuck.
April 2022	A new attack on combined charging systems EVSE was found, with the potential to disrupt the charging ability.
July 2022	Researchers discovered security flaws that enabled them to remotely switch chargers on and off, lock and unlock cords, and revoke charging authorization.

Therefore, the cyber-physical security of contemporary EVs has essential relevance with the ongoing development of intellectualization and vehicle onboard communication networks. Thus, a thoughtful study is desirable to emphasize the potential impacts of cyber-physical attacks on the EV onboard components and battery charging infrastructure. In addition, developing accurate and reliable cyber-attack detection and mitigation techniques is indispensable for networked EVs. To meet the escalating demand, several initiatives such as the Society of Automotive Engineers (SAE) J3061 [14], the International Organization for Standardization (ISO) 26262 [15], IEEE Power Electronics Security Workshop (2019) [16], and a committee draft of the standard "ISO-SAE 21434 road vehicles—cyber security Engineering" [17] are imposed. In the past decade, many efforts have been made by researchers to realize the impact of cyber threats on power electronic systems for networked EVs [18], [19], [20], [21], [22], [23], [24]. Cyber threats and related studies on EV powertrain components [18], onboard chargers (OBCs) [19], offboard chargers [20], power converters [21], motor drives [22], [23], and cooperate charging systems [24] are discussed. Even though various cyber-physical security implementation methods are developed for modern EVs, they lack the summarizing of these studies and approaches. Furthermore, comprehensive cyber-attack consequence assessments, detection, and mitigation techniques on commercially available and impending battery charging infrastructures such as OBCs, offboard chargers, wireless power transfer (WPT), and hybrid conductive–inductive charging infrastructure along with grid side impacts are deficient in the literature. Most importantly, the existing studies on the battery charging infrastructure do not specifically address the impacts and security aspects against cyber threats on modern battery charging infrastructure. Therefore, analyzing the cyber threats and reviewing mitigation strategies for EV charging infrastructure is crucial for the following purposes.

1) Identify susceptible nodes and analyze the potential impacts of cyber threats on various types of battery charging infrastructure.
2) Summarize the existing cyber-attack detection and mitigation techniques and provide a reference for the researchers in this field.
3) Analyze the current problems and look at potential future research areas in establishing cyber resilience of battery charging infrastructure.

This article elucidates the state-of-the-art battery charging technologies, challenges, and future prospects of cyber-physical security in various kinds of battery charging infrastructure along with case studies on them against sabotage cyber threats, which is the first comprehensive study to the best of the author's knowledge. The key contributions of this article are given as follows.

1) A comprehensive review of the latest research advances in EV battery charging technologies, including system architectures, battery charger configurations, power converter topologies, control schemes, EVSE, and communication protocols, is presented.
2) Summarizes the possible sabotage cyber-attacks by the state actors and their vulnerabilities on battery charging infrastructure as well as secondary distribution networks in a step-by-step manner. Furthermore, it analyzes cyberattack implications on the commercially available wired (onboard and offboard) and wireless battery chargers through case studies under a variety of sabotage cyberattacks.
3) A detailed discussion of the latest methods, such as software, hardware, and signal conditioning-based solutions to detect and mitigate cyberattacks, is presented. In addition, a generalized approach to these methods is formulated, and some important approaches are investigated through simulation and experimental studies.
4) Challenges and opportunities in creating next-generation cyber secure battery charging technologies are discussed to assist readers with recommendations for future research on this topic.

II. OVERVIEW OF BATTERY CHARGING INFRASTRUCTURE

Typically, the nominal battery voltages of EVs are not always the same, and this is changing with the proliferation of EVs. Currently, EVs have a battery pack voltage ranging from 120 to 450 V [25]. Alternatively, next-generation EVs come with high-voltage (HV) battery pack voltages ranging from 600 to 800 V, being advantageous in terms of achieving substantial EV weight savings and a significant reduction in charging time [26], [27]. The battery chargers convert the input power supply according to battery requirements and deliver the desired power to the battery pack. These chargers are categorized into level-1, level-2, and level-3 chargers with typical power rating of 1.9, 19.2, and $>$ 240 kW, respectively [28], [29]. Typically, level-1 and level-2 chargers are ac chargers, while level-3 chargers are dc chargers. These chargers maintain unity power factor (UPF), extract sinusoidal input current, and maintain the input current total harmonic distortion (THD) within the limits of IEEE 519 [30]. In addition, galvanic isolation is provided to circumvent the leakage current as per the standards of IEC 62752 and IEC 62955 [31].

The energy can be replenished into EV batteries through conductive (wired) chargers, WPT-based chargers, and battery swapping [28]. Wired chargers connect the EV and charging unit using a charging cord and EVSE. While in wireless charging, the charging unit and EV are connected through loosely

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

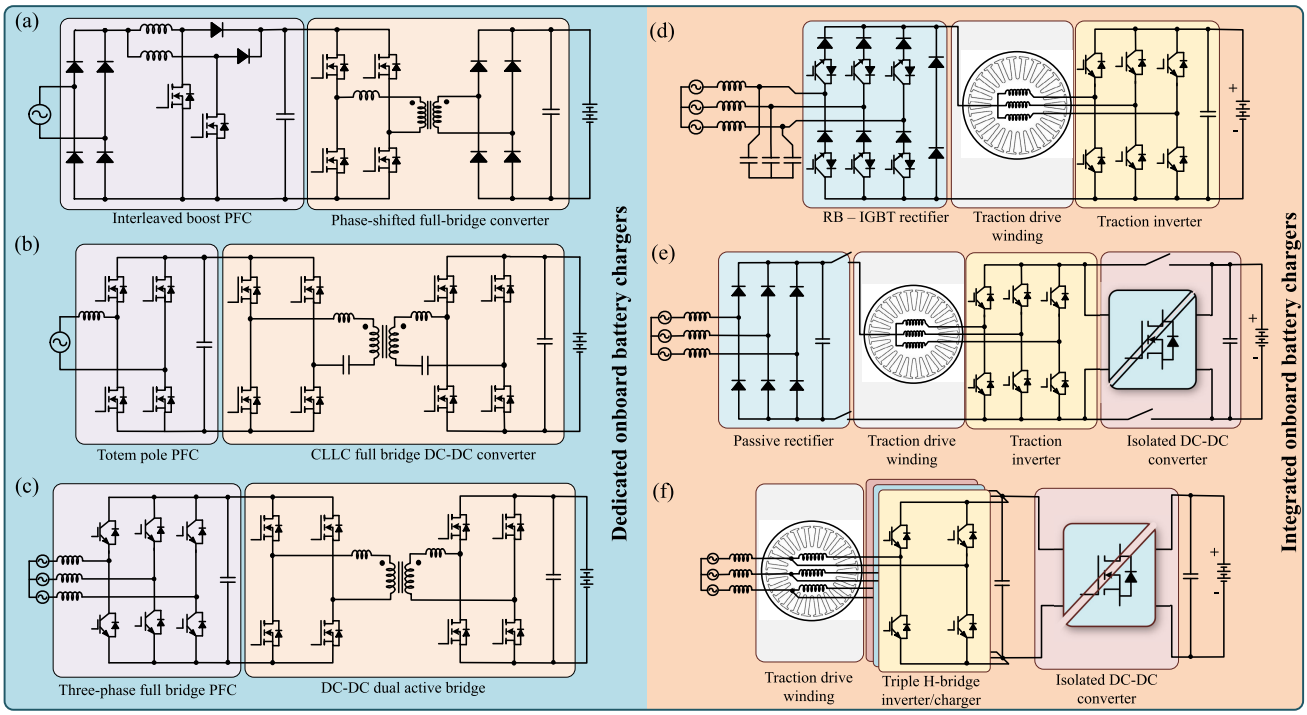

Fig. 2. Onboard battery charging infrastructure. DOBCs. (a) 3.3-kW second-gen Chevy Volt OBC. (b) 6.6-kW Delta-Q OBC. (c) 6.6-kW Current Ways OBC. IOBCs. (d) 43-kW Renault Chameleon IOBC. (e) 22-kW Continental IOBC. (f) 90-kW galvanically isolated IOBC [45].

coupled inductor coils/capacitor plates, transferring power through electromagnetic (EM) or electrostatic fields [32]. In case of battery swapping, depleted batteries will be replaced with fully charged ones [33]. Thus, it reduces the idle time for energy refilling; however, these are expensive owing to spare batteries, robotic machinery for swapping, and infrastructural requirements for storing the charged batteries. In addition, the EV batteries can also charge from opportunity charging and flash charging [34]. However, these charging techniques are currently in the research and development stage.

A. Conductive Battery Chargers

Conductive chargers are classified into OBC and offboard chargers based on the charger's location. OBCs are equipped in the vehicle, while the offboard chargers are placed outside the vehicle [28]. Based on the number of conversion stages from the source to the battery, chargers are classed into two-stage chargers (ac–dc–dc) and single-stage (ac–dc) chargers. The two-stage chargers comprise a front-end power factor correction (PFC) converter and a dc–dc conversion. The PFC converter maintains the desired dc voltage at the dc link along with the UPF at the source and maintains the input current THD [35], [36]. While the dc–dc battery interface provides the galvanic isolation and preserves the desired voltage/current corresponding to the charging technique. Two-stage OBCs are more popular due to their ease of design and their control. In contrast, the single-stage OBCs involve one conversion stage with fewer components; however, its control is complex [37].

OBCs are further classified into dedicated OBCs (DOBCs) and integrated OBCs (IOBCs). DOBCs are further categorized into $1-\phi$ and $3-\phi$ chargers based on the type of input supply. The $3-\phi$ OBCs are similar to $1-\phi$ OBCs; however, only the PFC configuration is different [35]. The most significant commercially accessible DOBCs are depicted in Fig. 2(a)–(c). A second-gen Chevy-volt DOBC shown in Fig. 2(a) comprises interleaved boost PFC followed by the phase-shifted full-bridge (PSFB) converter [38]. Owing to the front-end diode bridge rectifier, the charger power rating is limited to 3.3 kW. Fig. 2(b) shows a 6.6-kW Delta-Q DOBC with a totem-pole PFC configuration, which has greater efficiency due to the absence of a front-end diode rectifier [39]. Therefore, this charger is suitable for a higher power rating along with bidirectional power flow [40]. Moreover, $1-\phi$ OBC's maximum power rating is limited to 6.6 kW owing to the $1-\phi$ residential outlet. A 6.6-kW Current Ways DOBC shown in Fig. 2(c) comprises a $3-\phi$ active front-end (AFE) rectifier followed by a dual active bridge (DAB) [41]. Due to the absence of unidirectional components, this charger is also feasible for bidirectional power transfer, i.e., grid-to-vehicle (G2V) and V2G. Nevertheless, due to the space and weight constraints, the DOBCs' power rating is limited, typically in the range of 1.3–19.2 kW [28].

Thus, IOBCs are intended to enhance the charger power rating without adding additional weight to the vehicle using the traction converter/drive for charging purposes [42]. Several prominent IOBCs, including the Renault Chameleon 43 kW, Continental 22 kW, and a 90-kW galvanically isolated IOBC, are featured in Fig. 2(d)–(f) [43], [44], [45]. Renault Chameleon [see Fig. 2(d)] and Continental IOBC [see Fig. 2(e)] use traction drive windings and the traction converter to realize three-leg interleaved boost converter. Similarly, IOBC in Fig. 2(f) is realized with a triple H-bridge PFC converter followed by an isolated dc–dc converter. Traction drive windings are used as PFC-stage boost inductors, and this charger is also compatible with bidirectional power transfer. Due to the utilization of the traction drive/converter for charging purposes, the utilization factor and charger power

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

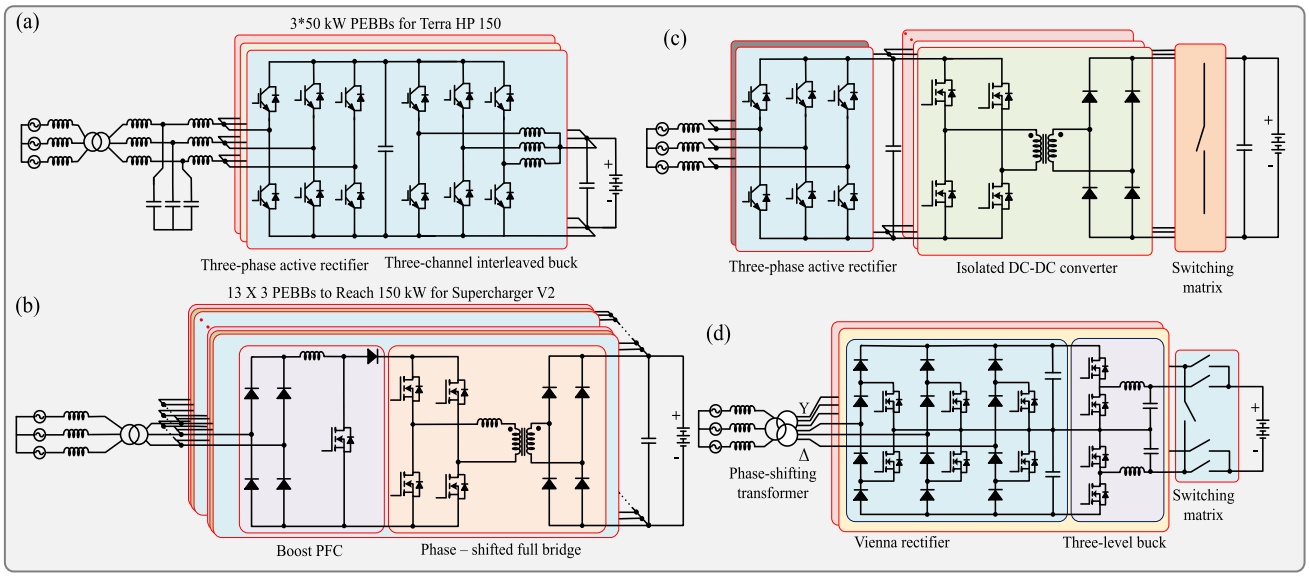

Fig. 3. Offboard battery charging infrastructures. (a) 150-kW ABB Terra HP offboard charger. (b) 150-kW Tesla supercharger V2. (c) 600-kW ENERCON E-charger. (d) 350-kW Porsche modular fast charger.

ratings are increased. However, it is limited to the traction converter/drive power rating. In addition, these chargers are nonisolated chargers, which leads to leakage currents. Furthermore, using a traction drive as a charger will diminish its life owing to mechanical vibrations and generate torque production during charging fed from the three-phase grid.

To overcome the aforementioned concerns with the OBCs, offboard chargers are proposed with higher power ratings to minimize the charging time. The power ratings of these chargers typically range from a few kW to MW [46]. These chargers are categorized into ac and dc distributed chargers based on the local distribution between charging units [47]. Generally, these chargers are similar to OBC; however, the number of OBC modules will be cascaded to enhance the power rating. The most prominent commercially available offboard charger topologies are depicted in Fig. 3. A 150-kW ABB Terra HP charger depicted in Fig. 3(a) is realized with three 50-kW modules, which comprise a $3-\phi$ AFE rectifier followed by a three-leg interleaved buck converter [48]. The galvanic isolation is provided with a low-frequency transformer (LFT). A 150-kW Tesla supercharger V2 shown in Fig. 3(b) is realized with 13×3 OBC modules, which is composed of a boost PFC followed by a PSFB converter [28]. The module's inputs are connected in Δ form, whereas the outputs are connected in parallel. The number of modules in operation depends on the power requirement.

Similarly, the 600-kW Enecorn E-charger and Porche 350-kW modular chargers are depicted in Fig. 3(c) and (d), respectively [49], [50]. A switching matrix at the battery end is used to reconfigure the charger for LV or HV battery pack EV charging. The existing 50-kW chargers are around 93% efficient, with an LFT efficiency of 98.5%. A viable method to overcome the aforementioned challenges is the use of solid-state transformer (SST) technology [4], [47], which allows for direct connection to the medium voltage (MV) line by eliminating the need for an LFT. Most importantly, this architecture enables a standard dc bus configuration and the ability to include renewable energy sources and energy storage with reduced conversion stages. With the increased power rating, these chargers shorten the charging period; however, handling high-power charging cords during adverse weather conditions is a risk of electrical shock, and these chargers are expensive.

B. WPT Chargers

The configuration of the WPT chargers is similar to that of the conductive chargers; loosely coupled coils/plates are placed in place of the high-frequency transformer (HFTF). In addition, compensation circuits are used on the transmitter and receiver sides to minimize the VA rating of the charger. WPT chargers are categorized into inductive power transfer (IPT) and capacitive power transfer (CPT) chargers [32], [51], [52]. IPT chargers operate at 85 kHz (SAE J2954) and have more power density, whereas CPT chargers operate at a 1-MHz frequency and have better misalignment tolerance [53]. A two-stage IPT charger [54], single-stage direct ac–ac IPT charger [55], and single-stage active clamped half-bridge IPT charger [56] and a CPT [57] charger are depicted in Fig. 4(a)–(d), respectively. To accomplish the advantages of both IPT and CPT, researchers have proposed hybrid IPT–CPT chargers as depicted in Fig. 4(e) and (f) [58], [59], [60]. These chargers are categorized into series hybrid [see Fig. 4(e)] and parallel hybrid [see Fig. 4(f)] WPT chargers. On the other hand, dynamic WPT (DWPT) is a new and prominent technology that minimizes the battery requirement, improves the range, and diminishes the vehicle's cost. On the flip side, DWPT charging is less efficient and expensive.

C. Hybrid Conductive–Inductive Battery Chargers

The conductive chargers are efficient; however, handling the charging cords during adverse weather conditions is a risk of electric shock. On the other hand, WPT chargers provide safe charging in all weather conditions; however,

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

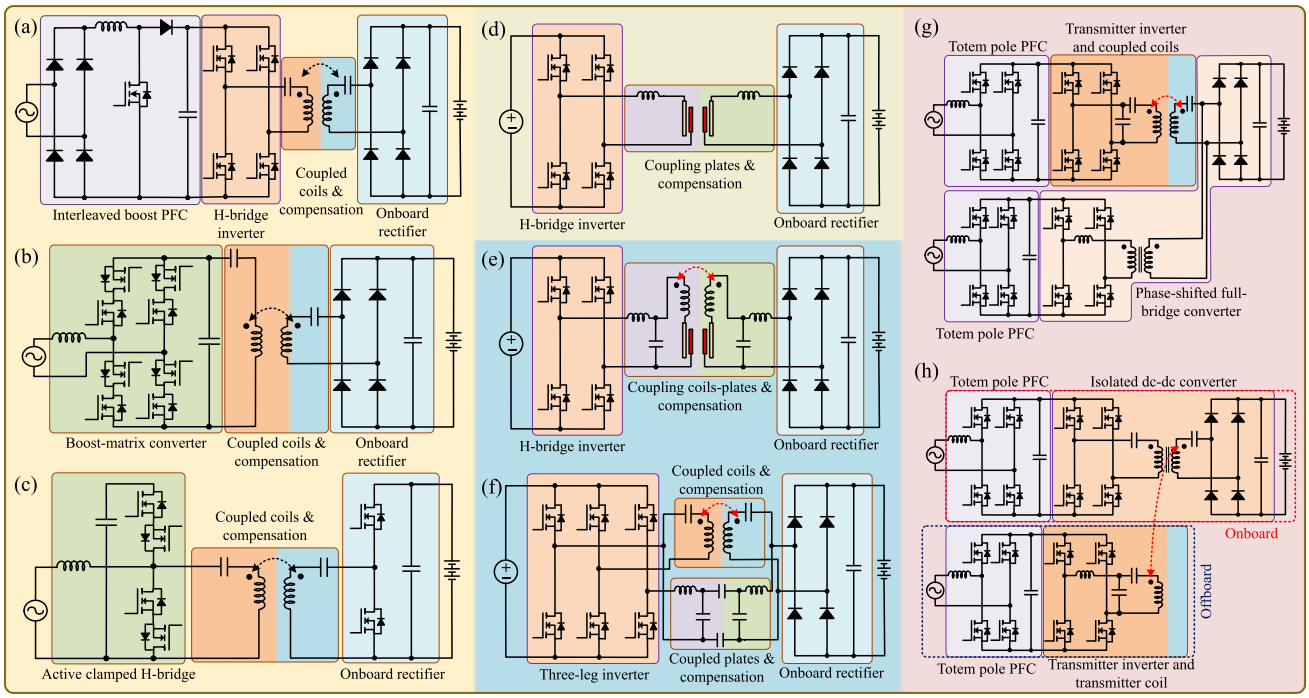

Fig. 4. WPT and hybrid battery charging infrastructure. (a) Two-stage inductive WPT [54]. (b) Single-stage direct ac–ac inductive WPT [55]. (c) Active clamped half-bridge direct ac–ac inductive WPT [56]. (d) DC–dc CPT [57]. (e) Series hybrid IPT–CPT [59]. (f) Parallel hybrid CPT–IPT [60]. (g) Parallel hybrid inductive–conductive battery charger [62]. (h) Hybrid battery charger with common receiver coil [63].

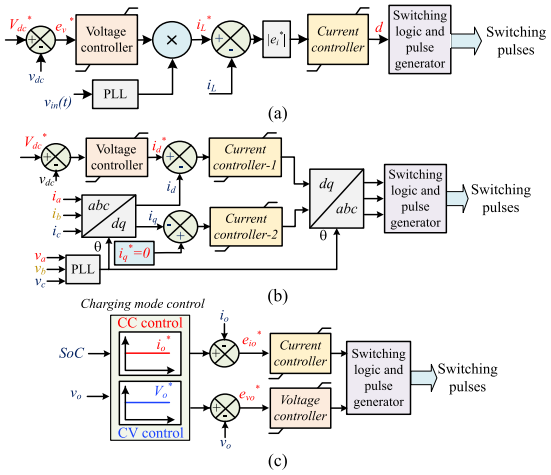

Fig. 5. Generic control architectures for the battery charger power conversion stages. (a) 1-ϕ PFC. (b) 3-ϕ PFC. (c) DC–dc battery interface.

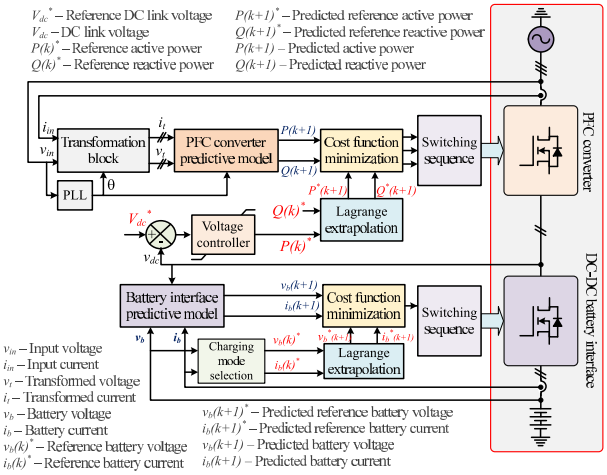

Fig. 6. Block diagram of a battery charger with an MPC.

these charger's efficiency is comparatively lesser than the conductive chargers. Thus, researchers have proposed numerous hybrid conductive–inductive battery chargers to accomplish the advantages of the conductive and inductive chargers [61], [62], [63]. These chargers charge the battery efficiently during normal weather conditions with conductive charging and safely during adverse weather conditions with WPT charging. Fig. 4(g) illustrates the parallel hybrid battery charger with a mutual onboard rectifier. Similarly, the hybrid battery charger with a mutual receiver coil and onboard rectifier configuration is shown in Fig. 4(h) [62], [63]. However, the design of the mutual receiver coupler and the charger's control are complex.

D. Battery Charger Control Architectures

The battery chargers typically consist of $1-\phi/3-\phi$ PFC converter and dc–dc battery interface stages. The PFC converters are controlled to draw a sinusoidal input current and regulate dc link voltage. In general, these converters are controlled with dual-loop controllers, which consist of a faster inner current loop followed by a slower outer voltage loop [28]. The current loop regulates the extraction of a sinusoidal input current along with the UPF, and the outer voltage loop regulates the dc-link voltage. The generalized control architectures of the $1-\phi$ and $3-\phi$ PFC converters are shown in Fig. 5(a) and (b), respectively. On the other hand, the dc–dc converters are controlled to maintain the desired voltage/current at the battery terminals according to the charging technique [36]. The generalized control architecture for the dc–dc converter is shown in Fig. 5(c), which involves voltage and current loops. These control loops are generally slower, whereas the current loop should be a faster loop for sinusoidal ripple charging (SRC) [56]. These controllers are realized with linear proportional–integral (PI) controllers in

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

the synchronous dq-reference frame. The PI controllers are connected in a cascaded manner. However, the tuning of the PI controllers to obtain the gains is complex. In addition, the dynamic behavior of the PI controller is limited by the gains, bandwidth, and switching frequency [64]. To overcome these concerns, the model predictive control (MPC) methods have been adopted for inner loops owing to their fast dynamic response, ability to handle multiple objectives, and ease of implementation [65], [66]. The generalized MPC-based control architecture for a two-stage battery charger is illustrated in Fig. 6. In this control, the outer loop remains the same, whereas the inner loops are realized with a converter predictive model and cost function minimization to generate switching pulses. However, the real-time implementation of MPC imposes some disadvantages, such as variable switching frequency, high computational burden, and dependence on weighting factor selection.

E. EVSE, Communication Channels, and Protocols

Conductive chargers are connected to the vehicle from the input supply or the charging unit through the charging cord and EVSE. The configuration of EVSE depends on the type of input supply and charging protocol. Various countries follow numerous connector configurations based on charging power requirements and local–global standards. The power flow is monitored by following various communication protocols for safe charging, as depicted in Fig. 7. Some of the commercially available dc, ac, and dc–ac connectors are shown in Fig. 7(a) [29], [67], [68], [69], [70], [71], [72]. These connectors involve several numbers of pins, which are broadly grouped into power, ground, and control pins. The power pins depend on the type of input supply, and the control pins depend on the communication protocol. A $1-\phi$ OBC realized with an SAEJ1772 EVSE is shown in Fig. 8, comprising two power pins (L and N), one ground pin (G), and two communication pins [control pilot (CP) and proximity pilot (PP)]. These communication channels are present between the EVSE controller and the EV to exchange the battery parameters, grid condition, vehicle connectivity, and available power for safe charging.

The communication protocols of battery chargers and EVs are generally categorized into low-level communication (LLC) and high-level communication (HLC). The LLC follows the SAE J1772 protocol, in which the power availability is communicated to the EV with a duty cycle of a 1-kHz pulsewidth modulation (PWM) signal as shown in Fig. 8 [29]. The HLC follows ISO 15118 protocol to monitor and control the power flow and communicate with broadcast messages through an internet protocol (IP)/control area network (CAN)/power line communication (PLC) [73]. The ISO15118 protocol architecture along with the success and failure end conditions are shown in Fig. 7(b) [74]. ISO 15118-2 standard represents a transparent hypertext transfer protocol (secure) [HTTP(s)]/file transfer protocol (FTP) connection to control the vehicle remotely from the charging infrastructure during the charging. On the other hand, the offboard and bidirectional chargers follow the ISO 15118/ISO 15118-2 and ISO 15118-20 protocols, respectively [75]. GB/T and CHAdeMO communicate through the CAN bus, whereas WPT chargers communicate through Bluetooth/Wi-Fi/5G. The most popular commercially available EV battery charging infrastructure and their features are summarized in Table II.

III. Introduction to Cyber-Attacks and Impacts on Battery Charging Infrastructure

A cyber-attack is an attempt by threat actors to gain unauthorized access to systems, steal data, or harm the charging infrastructure and powertrain components [86]. Cyber-attacks are categorized as local and remote attacks based on the distance between the attack point and the attacker [18]. Local attacks are based on Faraday's EM induction, which modifies or injects noise to the sensor/relay data by placing an energized coil nearby [21]. While the remote attacks target the cloud or communication channels to steal sensible data, modify switching pulses, etc. [8].

The OBCs are monitored with the MCU presented in EVSE [29]. On the other hand, offboard and WPT battery charging infrastructures are cloud-connected for power monitoring, payment gateways, user access control, etc. [22]. In addition, EVs with bidirectional chargers [39], [41], [45], [48] communicate with other vehicles and the infrastructure for the V2V and V2I power transfer [87]. The cloud, EVSE, MCU, and communication channels are the gateways for cyber-attacks against charging infrastructure. Therefore, the offboard and WPT chargers are highly vulnerable to cyber-attacks due to the extensive communication network. The generalized wireless charging infrastructure with susceptible attack points is depicted in Fig. 9. The broad classification of cyber-attacks is given as follows.

1) *Modification Attack:* Modification attacks on charging infrastructure entail modifying the charger's predefined variables (increasing/decreasing), such as reference voltage/current, sensor data, and feedback/controller gains. During normal operation, the voltage controller operates to maintain zero error voltage ($e_v = 0$), resulting in the desired voltage at the output

$$e_v = V_o^* - V_o = 0 \tag{1}$$

where e_v, V_o^*, and V_o are the error, reference, and actual battery voltages, respectively. For instance, consider a modification attack on a feedback gain, the voltage controller tries to operate with zero error, which can be expressed as follows:

$$\begin{aligned} e_v = V_o^* - (V_o \times k) = 0 \Rightarrow V_o = \frac{V_o^*}{k} \\ I_c' = \frac{V_o^*}{R_{\text{eq}} \times k} = \frac{V_o^*}{R_{\text{eq}}} \times \frac{1}{k} = \frac{I_c}{k} \end{aligned} \tag{2}$$

where k, R_{eq}, I_c, and I_c' are the modification factor, battery equivalent resistance, charging current, and modified charging current, respectively. As a result, the modification attack on feedback gain leads to a deviation of the charger's operating voltage (2). Substantially, it increases/decreases the charging current, which delays charging or damages the battery pack.

2) *Interference Attack:* This attack involves interference with sensor/feedback data paths or communication channels and injecting white noise into it, which results in

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

TABLE II
MOST POPULAR COMMERCIALLY AVAILABLE EV BATTERY CHARGING INFRASTRUCTURE

Charger type	Charger manufacturer	Charger configuration	Power rating	EVSE connector	Communication
Dedicated onboard chargers	Chevy Volt [38]	Interleaved boost PFC - PSFB	3.3 kW	SAE J1772	PLC
	Delta-Q [39]	Totem pole – C-L-L-C full bridge	6.6 kW	IEC 62196 type – 1/2	PLC
	Current Ways [41]	3-phase full-bridge PFC - Dual active bridge (DAB)	6.6 kW	SAE J1772, GB/T 20234.2 CHAdeMO	PLC, CAN
	Nissan Leaf [76]	Interleaved boost PFC - PSFB	6.6 kW	IEC 62196 type – 2, CHAdeMO	CAN
Integrated onboard chargers	Renault Chameleon [43]	3-phase unidirectional controlled rectifier-PMSM traction drive- 3-leg traction inverter	44 kW	CCS-2	High-level IP
	Valeo dual-inverter [77]	PMSM traction drive – 3×H-bridge inverter – Isolated dc-dc converter	22 kW	CCS-2	CAN
	Continental [44]	Uncontrolled rectifier – Traction drive – Traction converter – Isolated dc-dc converter	22 kW	CCS-2	Near field communication
Offboard chargers	ABB Terra 53/54 [78]	3 module (uncontrolled rectifier - LLC Resonant Half Bridge)	50 kW	CCS 2/JEVS G105, CHAdeMO	CAN
	ABB Terra HP 150-kW [48]	3×50 kW modules (3-phase active rectifier – 3-leg interleaved buck)	150 kW	CCS-1 and CHAdeMO	Open charge point protocol - 1.5, & 1.6
	Tesla Supercharger V2 [71]	13×3 (Boost PFC-PSFB)	150 kW	Supercharger	J1772-dc
	Porsche Modular Fast Charging Park A [50]	2-module (Vienna rectifier – Three-level buck)	350 kW	CCS-2	Unknown
	Enercon E-charger [79]	3-phase active rectifier – Modular isolated dc-dc converter – Switching matrix	600 kW	CCS-2	Ethernet
Static WPT chargers	WiTricity [80]	Two-stage (Air gap: 100-200 mm)	3.4 kW	Inductive coupled	Wi-Fi
	HEVO [81]	Two-stage (Air gap: 300 mm)	10 kW	Inductive coupled	5G
	KAIST [82]	Two-stage (Air gap: 120-200 mm)	15 kW	Inductive coupled	B5G/6G
Dynamic WPT chargers	Bombardier [83]	Two-stage (Air gap: 60 mm)	200 kW	Inductive coupled	Wi-Fi
	ORNL [84]	Two-stage (Air gap: 162 mm)	30 kW	Inductive coupled	Radio
	WAVE [85]	Two-stage (Air gap: 152-254 mm)	50 kW	Inductive coupled	Unknown

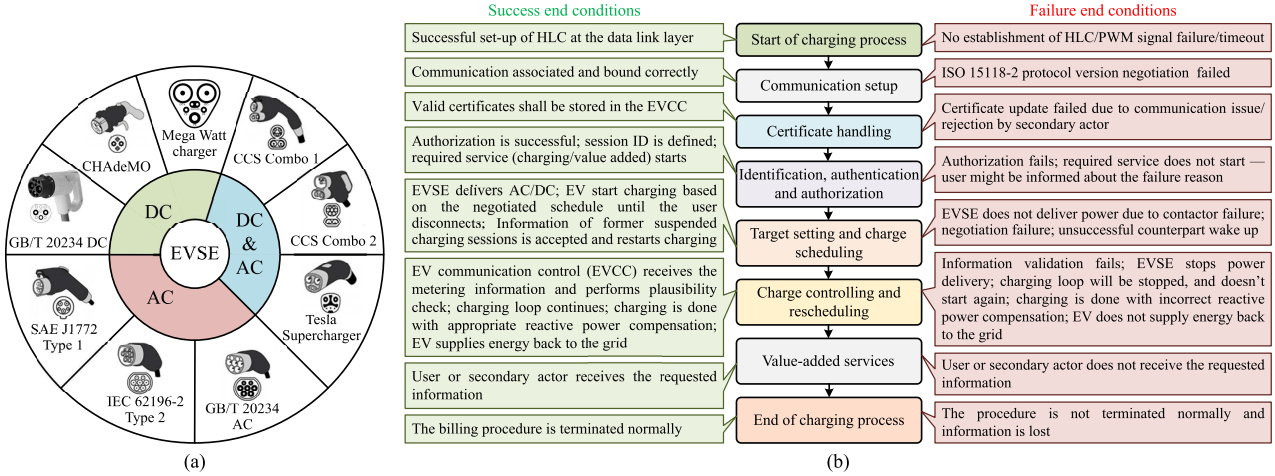

Fig. 7. EVSE. (a) Standardized dc and ac EVSE connectors. (b) ISO 15118 communication protocol.

deviation in the charger's operation. Interference attack on the sensed voltage signal is considered, and it is expressed as follows:

$$I_c' = \frac{V_o^* \mp m(t)}{R_{\text{int}}} = \frac{V_o^*}{R_{\text{int}}} \mp \frac{m(t)}{R_{\text{int}}} = I_c \mp i_{\text{additional}}(t) \tag{3}$$

where $m(t)$, and R_{int} are the interference signal and internal resistance, respectively. Therefore, an interference attack causes a significant increase/decrease in charging current, which degrades life or causes permanent damage to the battery.

3) *Interruption Attack:* This attack involves interrupting communication channels, sensor data, switching pulses, etc. It also involves interrupting the input-output relay signals, causing a DoS, and increasing the charging period.

4) *Interception Attack:* Interception entails an assault on the cloud and accessing sophisticated data to gain unauthorized access to the charging station database. As a result, the attacker can attain complete control of the charging station.

The manipulation of the reference signal on the battery charger increases/decreases the reference signal, damages the power converters, degrades the battery performance, or causes permanent damage. Interruption and DoS attacks on OBCs and WPT are moderate. However, the same attack on offboard chargers creates a voltage swell and frequency distortion at the distribution grid and damages the grid-end filter capacitors. On the other hand, battery swapping stations are monitored by the local controllers. However, these are interfaced with

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

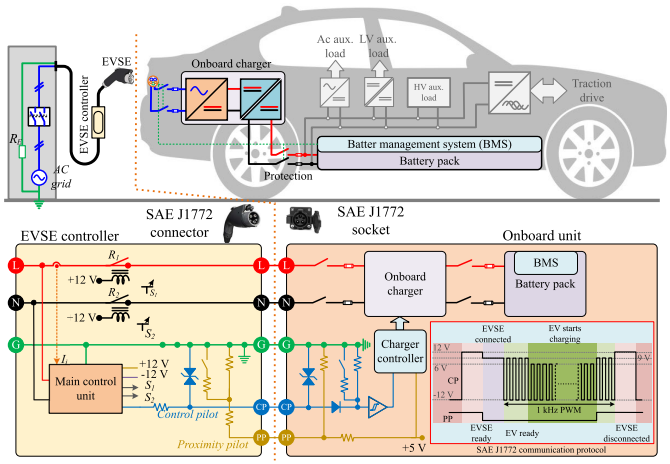

Fig. 8. Block diagram of 1-ϕ OBC with SAE J1772 EVSE.

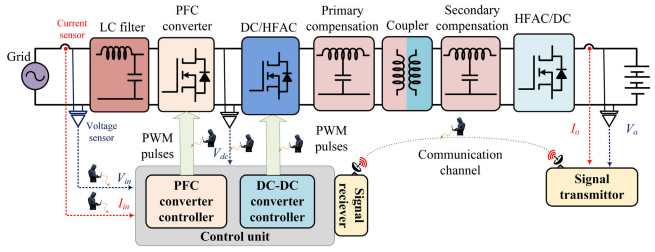

Fig. 9. Inductive charging system with potential cyber-attack points.

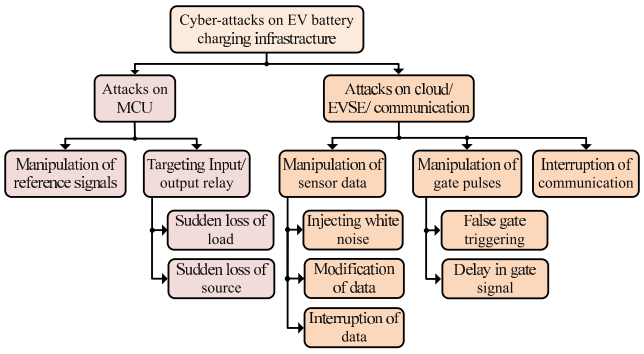

Fig. 10. Classification of cyber-attacks on battery charging infrastructure.

cloud-based control for grid support. Thereby, attackers can attain complete control of the charging station and cloud data with interception attacks which are more common in cloud-based control. Furthermore, swapping stations may overcharge/DoS/explode the batteries due to cyber-attacks. Fig. 10 depicts the classification of some of the possible cyber-attacks on the charging infrastructure. Table III summarizes the prominent cyber-attacks on battery chargers, their severity, and potential impacts.

IV. Case Study: Impacts of Cyber-Attacks on Battery Charging Infrastructure

Cyber-attack vulnerabilities on battery chargers are performed on the MATLAB/Simulink platform to assess the possible implications. The aforementioned cyber-attack has significant potential impacts on all the battery chargers. However, for the simulation studies, an interruption attack on a 3.3-kW Second-gen Chevy-volt OBC, interference and modification attacks on a 150-kW ABB Terra HP bidirectional offboard charger, modification and interruption attacks on a 3.3-kW IPT charger, and a DoS attack on a parallel hybrid conductive–inductive battery charger are considered.

TABLE III
Cyber-Attacks, Risk, and Their Impacts of EV Battery Charging Infrastructure

Attack	Risk	Potential impact
Increase in sensor data	Moderate	Enhances the charging period
Decrease in the reference signal	Moderate	Enhances the charging period
Turn on delay in switching pulse	Moderate	Converter operates in discontinuous conduction mode. If delay is high, the EV disconnects from the charger
Injecting white noise into sensor data	Moderate	Battery temperature rise, life degradation. Consequently, permanent damage to the battery
Decrease in sensor data	Extensive	Damages power converters and battery
Increase in the reference signal	Extensive	Overcharges the battery, degrade the battery life or permanently damages
False gate triggering	Extensive	Damages the battery charger
Turn off delay in switching signal	Extensive	Extracts over current from grid, and damages the charger
Short circuit on the load side	Extensive	Battery damages due to huge current extraction
Dc-link short circuit	Extensive	Damage the power converters, and disturbance in grid

A. Interruption Attack on OBC

A 3.3-kW second-gen Chevy-volt OBC [see Fig. 2(a)] [38] is modeled and controlled using the constant current–constant voltage (CC-CV) charging technique. A 1-ms delay in switching pulses due to interruption and interception cyber-attacks is considered to assess the impact on the OBC at 1.5 s. Switching pulse delay keeps switches in their prior state. Thus, the turn-on delay causes the switches to remain in the off position, and the source is directly connected to the load. In contrast, the turn-off delay short-circuits the source via the front-end inductor. The potential impacts of interrupting the gate signals of an OBC are depicted in Fig. 11(a). It is noted that the current drawn from the source has dropped to zero during the turn-on delay owing to the fully charged capacitor, which extends the charging time and injects harmonics into the grid. On the other hand, a turn-off delay results in a huge current drawn from the grid, which substantially impacts the grid and damages the semiconductor devices and filter components.

B. Interference and Modification Attacks on Offboard Charger

A 150-kW ABB Terra HP bidirectional offboard battery charger [see Fig. 3(a)] [48] is considered for assessing the potential impacts of data modification and interference attacks. Interference of the switching pulse causes false triggering of the semiconductor device, which results in a short-circuit/open-circuit. The interference attack is created for one module at 4 s in the G2V power transfer mode, and the corresponding impacts are shown in Fig. 11(b). It was noted that the modules operated with rated power with negligible reactive power prior to the attack. Whereas an attack at 4 s

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

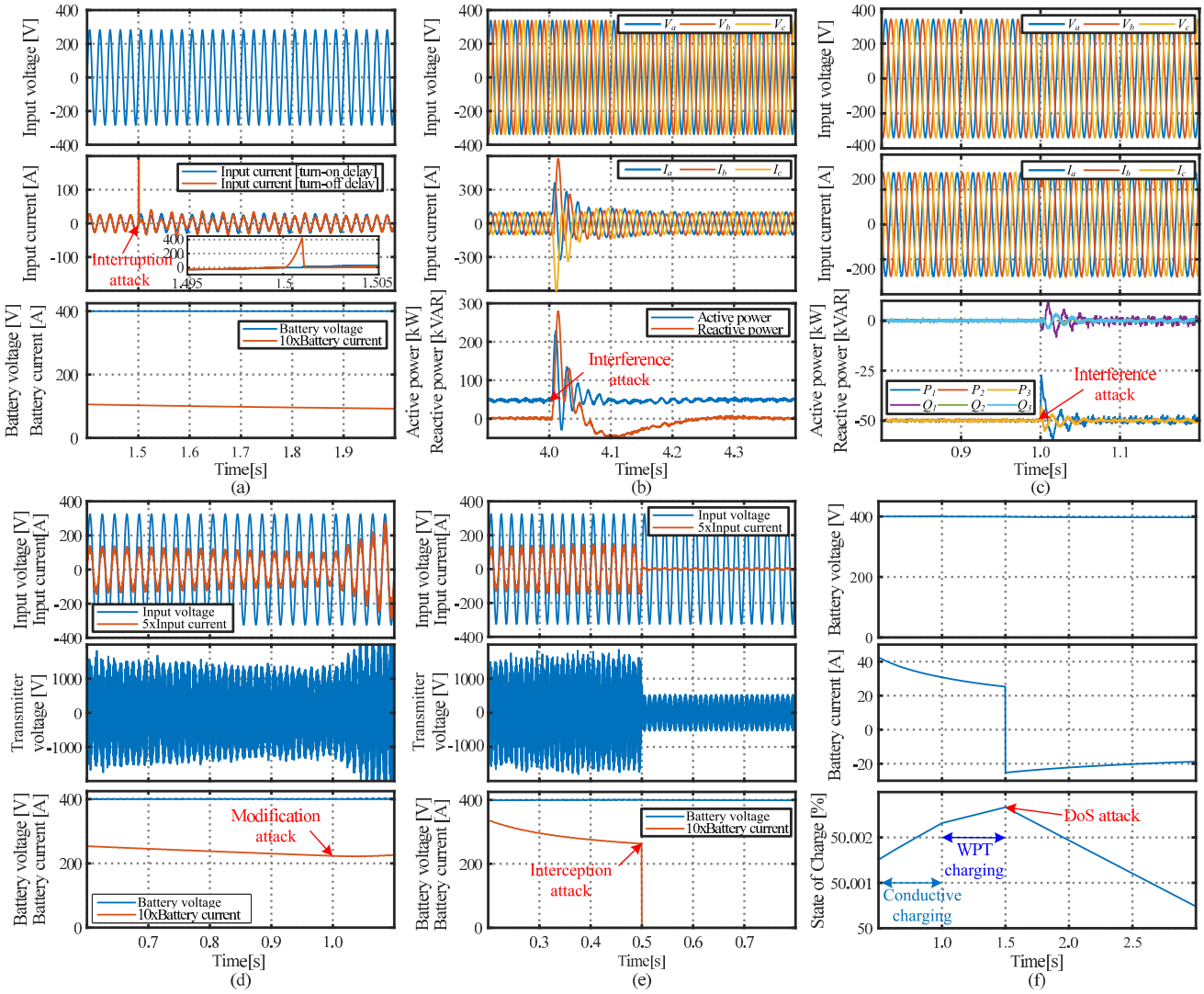

Fig. 11. Impacts of cyber-attacks. (a) Interference and interruption attacks on OBC—delay in switching pulse. (b) Interference attack on offboard charger—false triggering. (c) Modification and interference attacks on offboard charger during V2G operation—white noise injection. (d) Modification attack on IPT—modification of reference voltage. (e) Interruption attack on IPT—communication interruption. (f) DoS attack on hybrid conductive–inductive charger.

causes an enormous increase in active and reactive power, module current, and unbalanced loading, which results in disturbance in the grid, damages the module, and reduces the charger power rating.

The same charger operated in the V2G mode to identify the impacts of modification and interference attacks on bidirectional battery chargers. An interference attack is created by injecting white noise into module-1 sensor data, and the modification attack is created by a decrease in voltage reference signal by 1 V. These attack impacts are depicted in Fig. 11(c). It is observed that these attacks create a different loading on the modules, thereby generating a circulating current between modules and resulting in a decrease in charger efficiency and power rating. It is to be noted that an ac V2V charging with the aforementioned attacks will also have similar kinds of impacts.

C. Modification and Interruption Attacks on IPT

A 3.3-kW single-stage IPT charger [see Fig. 4(d)] [55] is modeled on the simulation platform to analyze the modification and interruption attack impacts on the WPT chargers. The modification attack is created by increasing the predefined reference battery voltage by 1 V at 1 s, and the corresponding implications are shown in Fig. 11(d). A small change in reference voltage causes a significant increase in the charging current owing to the negligible battery's internal resistance (in the order of mΩ). Consequently, it leads to an increase in battery temperature and performance deterioration or permanent damage.

The interruption attack is created on the IPT charger by interrupting the communication channel between the transmitter and the receiver. Typically, BMS data are transferred to the charging infrastructure through the communication channel to monitor the power flow. However, the roadside charging unit may not receive the vehicle's state due to this attack. Thus, the vehicle is disconnected from the transmitter and interrupts the charging; the corresponding effects are depicted in Fig. 11(e). A high-frequency (85 kHz) voltage appears across the transmitter due to the resonance circuit formed by the compensation network and transmitter. In addition, it draws a negligible current owing to the semiconductor device parasitics.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

D. DoS Attack on Hybrid Conductive–Inductive Charger

To evaluate the impacts of a DoS attack, a 3.3-kW parallel hybrid charger [see Fig. 4(d)] [62] is modeled. Initially, the EV is charged from the conductive charging; at 1 s, the charging mode transitions to inductive charging, and a DoS attack is created at 1.5 s. The corresponding results are depicted in Fig. 11(f). It is observed that the DoS attack ceases charging the EV, and the battery's state of charge (SoC) starts decreasing due to the presence of auxiliary loads.

V. Detection and Mitigation Opportunities, Challenges, and Future Visions

A. Detection and Mitigation Approaches

The case studies presented in Section IV conclude that cyber-attacks significantly impair and impact the EV charging infrastructure, EVSE, battery, and the grid. Therefore, cyber-attacks must be detected and mitigated early. On the other hand, the transient behavior of the charger resembles the cyber-attack behavior. Thus, it is challenging to distinguish between transient and cyber-attack behavior and detect the type of cyber-attack to counterattack. Researchers proposed numerous cyber-attack detection and mitigation techniques, which are broadly categorized as follows.

1) Software-Based Detection and Mitigation Techniques: The battery charging infrastructure can be protected from cyber-attacks using software-based detection and mitigation techniques. These techniques are developed in digital signal processors (DSPs), field-programmable gate array (FPGA)-based controllers, etc. These techniques are further categorized into model-based and data-driven mitigation techniques.

a) Model-based cyber-attack detection and mitigation techniques: In this method, the future state of the charging infrastructure is anticipated from the plant's modeling equations, input parameters, and sensor data [88]. The controller identifies the cyber-attack by comparing the anticipated data with the actual data, which can be expressed as follows:

$$e^* = |V_o(k) - \hat{V}_o(k)| \geq \tau \tag{4}$$

where $V_o(k)$, $\hat{V}_o(k)$, e^*, and τ are the measured output, anticipated output, error, and threshold voltages, respectively. If the error surpasses the threshold, it is deemed a cyber-attack [see (4)]. The controller protects the charging infrastructure and detects cyber-attack from cloud data and counter-attacks accordingly [89]. The generalized flowchart for the model-based cyber-attack detection and mitigation techniques is depicted in Fig. 12(a). This method is easier for small and medium systems owing to minimal data and time requirements; however, it is composite for larger systems owing to the complexity of identifying the model equations.

b) Data-driven cyber-attack detection and mitigation techniques: Data-driven algorithms are model-free and identify the abnormal behavior of the charger from the past collected data and counter-attack accordingly [18], [90]. In the absence of a counter-attack, protect the charger, and the new attack data will be stored in the database to train the controller toward new cyber-attacks. The generalized data-driven algorithm's flowchart is depicted in Fig. 12(b). Large systems prefer data-driven algorithms over the model-based algorithms.

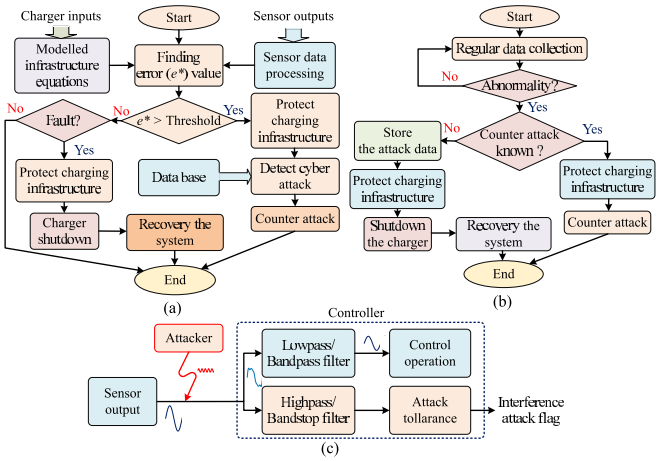

Fig. 12. Generalized flowchart of cyber-attack detection and mitigation approaches. (a) Model-based, (b) data-driven, and (c) filtering-based techniques.

TABLE IV
Cyber-Attack Detection and Mitigation Techniques for Battery Charging Infrastructure

Cyber-physical attack	Model-based detection and mitigation technique	Data-driven detection and mitigation technique
Modification attack	χ^2 attack detection [96], Kalman filter based state estimation [97], autoregressive model [98]	Singular value decomposition [99], stochastic coding [100], varying frequency-based signature [101]
Interference attack	State estimation [102], proactive defence [103], automatic generation control [104].	SVM technique [91], Artificial neural network [94], Gaussian mixture model [105]
Interruption attack	Observer-based detection technique [106]	Dynamic state estimation [107]
Interception attack	Robust Kalman filter technique [108]	Spare-matrix approximation [109], Reinforced learning [110]

These methods are realized with machine learning (ML), data mining techniques, and statistical models. Numerous data-driven methods such as ML [91], signal-analytic-based [92], leverage score [93], support vector machine (SVM) [91], neural networks [94], and deep learning [95] are proposed to detect the attacks. Various model-based and data-driven techniques for cyber-attack detection and mitigation are listed in Table IV.

c) Signal-processing-based mitigation techniques: In this technique, an additional signal processing circuitry is implemented in the controller to attenuate the injected white noise [21]. The generalized block diagram of this technique is illustrated in Fig. 12(c), and it can be realized with software or hardware filters. However, hardware-based realization increases circuit complexity and cost.

2) Hardware-Based Detection and Mitigation Techniques: The battery chargers can also protect from various cyber-attacks, such as DoS attacks, interference attacks on switching pulses, and sensor/feedback data, using additional hardware circuitry. Apart from signal processing circuitry, interference attacks can also be overcome using radio frequency (RF) shielding and magnetic shielding. Furthermore, interception attacks in WPT charging, i.e., sudden loss of load, can be attenuated using higher order inductor–capacitor–capacitor (LCC) primary and secondary compensation. Subsequently,

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

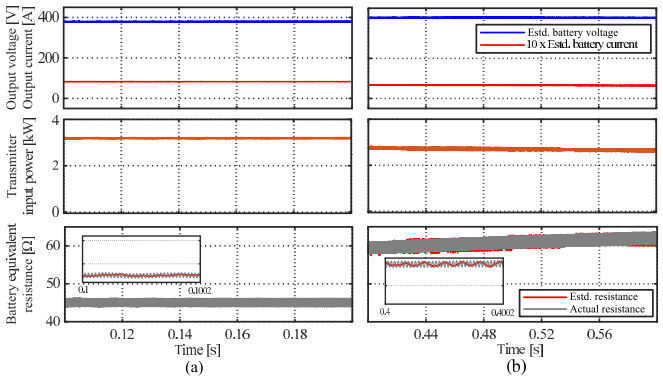

Fig. 13. Performance of the WPT charger with model-based detection and mitigation technique. (a) CC mode. (b) CV mode.

the transmitter operated as a current source, minimizing the effect of a sudden load loss. During larger attack mitigation periods and in the absence of mitigation techniques, the hardware protection circuit isolates the battery charging infrastructure from the source and vehicle to minimize the attack's impact.

B. Case Studies

Case studies are performed on software-based and hardware-based mitigation techniques. A model-based software mitigation technique is implemented to overcome the interruption of the communication channel. In contrast, a hardware-based mitigation technique is implemented to mitigate interference attacks on the switching pulses.

1) Software-Based Cyber-Attack Detection and Mitigation Technique: A 3.3-kW IPT charger with a model-based control and mitigation technique is implemented to estimate the battery equivalent resistance using the charger's transmitter voltage, current, and system parameters [111]. Furthermore, the battery's SoC will be identified using the equivalent resistance. A CC–CV charging technique is adopted and delivers a corresponding voltage/current. The performance of the charger with the model-based control technique in both the CC and CV modes is illustrated in Fig. 13(a) and (b), respectively. It is noted that the model-based controller's estimated resistance is quite close to the actual equivalent resistance of the battery. In addition, it maintained the desired voltage/current according to the charging technique. Thus, this technique avoids the communication channel requirement and minimizes the gateways for cyber-attacks.

2) Hardware-Based Cyber-Attack Mitigation Technique: Typically, most of the power converters in charging infrastructures involve complementary switches as half-bridge configurations. The controller ensures nonoverlap switching of these switches to avoid shoot-through faults. However, an interference attack or an error in the controller may turn on the complementary switches together, which damages the switches. A hardware-based circuitry depicted in Fig. 14(a) is implemented to protect from these concerns. The operating flowchart and the truth table of the hardware logic circuitry are illustrated in Fig. 14(b) and (c), respectively. Complementary switching signals (S_{HS} and S_{LS}) of a SiC-MOSFETS are considered, which are operated with a 0.5 duty cycle at 50-kHz

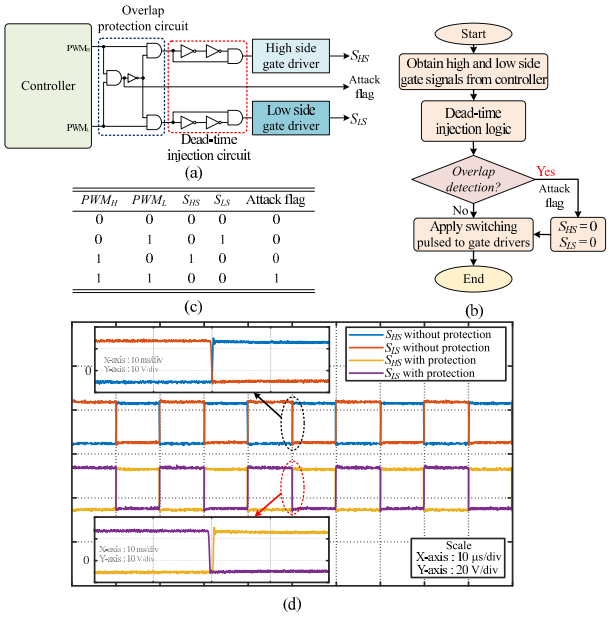

Fig. 14. Hardware-based interference attack mitigation technique. (a) Mitigation circuit. (b) Flowchart. (c) Truth table. (d) Experimental results.

switching frequency. The experimental results of complementary switching signals with and without hardware circuitry are depicted n Fig. 14(d). It is noted that the hardware circuitry turns off both the switches during attack/error conditions. In addition, it provides a dead band of approximately 250 ns, which is negligible compared with the switching period. Therefore, this circuitry can attenuate the interference attack on the switching pulses and operate up to 50-kHz switching frequency satisfactorily.

C. Challenges and Future Prospects

Industrial control system cyber-security involves the never-ending process of identifying and improving system flaws. A cyber-physical attack vulnerability study is essential in demonstrating the cutting-edge and profoundly needed for battery charging infrastructure security. Despite the fact that this article provides a foundation for a cyber-physical attack study, detection, and countermeasure techniques on charging infrastructure, there are still several problems concerning the cyber security aspects of the battery charging infrastructure and power electronic systems.

1) Over the past decade, there have been significant contributions regarding charging infrastructure, including power converter topologies, control schemes, and EVSEs. However, there is a lot of scope to improve the efficiency, power density, and availability of these systems. Furthermore, an increase in demand for 800-V battery systems can open up more opportunities for research in reconfigurable power converters that are suitable for both the 400- and 800-V systems. Therefore, these systems require further investigation of the power converter topologies with advanced control schemes that comply with present and future charging as well as cyber-security standards.
2) Another research area that would be required in the future is the development of battery chargers with

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

reduced power conversion systems with fault tolerance capabilities that must comply with the charging, EM interference/EM compatibility, and cyber-security standards. This improvement would enhance the efficiency and reliability of the battery chargers. This necessitates high-performance and advanced control schemes such as MPC methods for fault identification, localization, and reconfiguration. However, MPC methods have high computational complexity and require proper selection of weighting factors in the cost function optimization. Hence, new MPC techniques that are independent of weighting factors, faster dynamic response, and computationally efficient are crucial areas for research.

3) The online health monitoring of life-limited capacitors is done by measuring or estimating their equivalent series resistance and impedance using noninvasive methods to detect and replace failing components before a fault occurs. Therefore, further investigation is required to develop noninvasive health monitoring schemes for active switches and capacitors used in wired and wireless battery chargers. In addition incorporating active decoupling circuits along with long-life capacitors should be considered through new topologies and control schemes, offering an alternative path for double-line frequency ripple power on the battery side. As a result, battery temperature can be reduced, improving its cycle life. One important consideration while developing active decoupling circuits and their control in view of cyber security is the minimization of susceptible nodes for cyber threats and the utilization of noninvasive control methods.
4) Another important issue is that the existing algorithms developed for the control of charging infrastructure demand a large number of voltage sensors, current sensors, and communication channels for control and monitoring. As a result, sensorless control methods and parameter estimation approaches must be developed to reduce costs and nodes susceptible to cyber-attacks. Communication channels are the gateway for cyber-physical attacks. As a result, communication channels with end-to-end confidentiality, integrity, authentication, authorization, nonrepudiation, auditing, and side-channel attack-free are needed. Therefore, developing advanced cloud-based intrusion detection and malware detection systems using deep learning approaches is necessary.
5) Cyber-attacks disrupt the charging infrastructure in short periods and show significant impacts, leading to permanent damage. Note that the battery charging infrastructure has multiple interconnected subsystems. However, the representation of the charger with state equations and dynamics of the operating conditions makes it complex. As a result, distinguishing between cyber-attacks and physical faults is difficult. Therefore, early attack detection and fault identification techniques are emerging areas for future research.
6) Several methods for cyber-attack or physical attack detection are developed. However, new and advanced ML-based approaches can evolve to extend their availability. Furthermore, the majority of the literature currently in existence is focused on either physical fault detection or cyber-attack detection. Thus, advanced root diagnosis and detection techniques must be developed to distinguish between cyber-attacks and physical failures. In addition emulation of these faults without building physical hardware is to be considered through controller or power hardware-in-the-loop approaches as it saves time and money spent on actual infrastructure.
7) The majority of recent research on cyber-physical control systems does not take computational needs into account. In general, power electronic systems in the EV charging infrastructure operate faster than other processing control systems. It is necessary to develop a quick detection methodology so that the cyber-attack can be stopped in its tracks. Therefore, sampling rate, computational load, and detection time must be considered in addition to the detection accuracy.
8) Although data-driven methods for cyber-physical control systems provide an alternative way to detect and mitigate cyber-attacks, there are still limitations and challenges, particularly for charging infrastructure cyber security in terms of charging profile and data scarcity. However, real charging profile data can be difficult to obtain and is frequently kept confidential. Furthermore, training data may not be available for every attack scenario in various charging infrastructures. As a result, more novel solutions to reduce data dependence, improve computation efficiency, and enhance model fidelity must be investigated.

Overall, EV charging infrastructures are affected by various cyber-attacks. As a result, a comprehensive study on the cyber-attack-free battery charging infrastructure is still an emerging research topic.

VI. Conclusion

This article presents a systematic overview of prominent EV battery charging infrastructures, including charger configurations, power converter topologies, control methods, EVSEs, and their communication protocols for autonomous e-mobility applications. Furthermore, the potential impacts and mitigation approaches on battery charging infrastructure and their components against sabotage cyber-attacks have been comprehensively studied. In this article, the potential cyber-attack-prone points/nodes are identified and classified mainly based on the manipulation of the reference signals, sensor data, interruption of communication channels, and protection systems. For providing practical guidance to the researchers, the potential impacts of data-integrity-based cyber-attacks on commercially available conductive, inductive, and hybrid conductive-inductive battery chargers are analyzed in detail through case studies.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

The presented studies reveal that OBCs have a minimum entry point for cyber-attacks due to smaller communication networks. In contrast, the offboard and wireless chargers have numerous gateways for cyber threats, which are highly susceptible and risky in view of cyber security. Cyber-attacks, especially sophisticated DIAs on charging infrastructure, cause a massive rise in charger current/voltage, causing catastrophic implications for the power converter's operation, the safety of the batteries, and grid disruption. The results concluded that interruption and DoS attacks on low-powered conductive and WPT chargers significantly impact EV battery charger's performance, disrupting the charging infrastructure and batteries. On the other hand, the same attack on offboard chargers shows severe impacts on the grid side, such as voltage swell/sag, frequency distortion at the distribution grid, and damage to the grid-end filter capacitors, along with the aforementioned effects.

The state-of-the-art approaches, including software-intensive, hardware-based, and signal conditioning-based detection and mitigation techniques, are comprehensively discussed with detailed case studies. These studies concluded that software detection and mitigation techniques are more feasible solutions to protect the system against cyber-attacks than hardware-based techniques. In software-intensive techniques, model-based techniques are viable for smaller systems, and data-driven techniques are worthwhile for larger systems. Hardware-based mitigation techniques incorporate additional circuitry, which makes the complex and incurs costs at the system level. Signal-processing-based techniques can be implemented in hardware and in software. However, implementation in higher order filtering circuitry in hardware is complex and expensive. The case studies concluded that the model-based control technique reduces the gateways for cyber-attacks by eliminating the communication link in the case of wireless charging systems. The designed circuitry in the hardware at the device or component level ensures the nonoverlap of switching pulses of complementary switches, which protects from interference and modification attacks on switching pulses. Finally, unique challenges and future trends in battery charging infrastructure toward achieving cyber-resilience are also discussed.

REFERENCES

[1] G. Correa, P. Muñoz, T. Falaguerra, and C. R. Rodriguez, "Performance comparison of conventional, hybrid, hydrogen and electric urban buses using well to wheel analysis," *Energy*, vol. 141, pp. 537–549, Dec. 2017.

[2] D. Ronanki, A. Kelkar, and S. S. Williamson, "Extreme fast charging technology—Prospects to enhance sustainable electric transportation," *Energies*, vol. 12, no. 19, p. 3721, Sep. 2019.

[3] S. Chakraborty, M. A. Al Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, "Automotive cyber–physical systems: A tutorial introduction," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 33, no. 4, pp. 92–108, Aug. 2016.

[4] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018.

[5] D. Reeh, F. Cruz Tapia, Y.-W. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2019, pp. 1–6.

[6] *Cybersecurity for Electric Vehicle Charging Infrastructure*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.osti.gov/servlets/purl/1877784

[7] *Automotive Cybersecurity*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.ul.com/services/solutions/cybersecurity

[8] S. Acharya, Y. Dvorkin, H. Pandžic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[9] *10 Types of Cyber Attacks You Should Be Aware in 2023*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

[10] *Why Hackers Are Now Targetting Electric Car Charging Stations*. Accessed: Feb. 24, 2023. [Online]. Available: https://nocamels.com/2022/08/why-hackers-are-now-targeting-electric-car-charging-stations/

[11] *EV Charging, API Cyberthreats Emerge in Auto Industry*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.eetimes.com/ev-charging-api-cyberthreats-emerge-in-auto-industry/

[12] *Hacked Electric Car Charging Stations in Russia Display Putin is a D*ckhead and Glory to Ukraine*. Accessed: Feb. 24, 2023. [Online]. Available: https://electrek.co/2022/02/28/hacked-electric-car-charging-stations-russia-displays-putin-dckhead-glory-to-ukraine/

[13] Daily Echo. *Porn Displayed on Isle of Wight Electric Vehicle Charging Points*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.dailyecho.co.uk/news/20046990.electric-car-owners-shock-pornographic-photos-hacked-website/

[14] *Vehicle Electrical System Security Committee: SAEJ3061 Cybersecurity Guidebook for Cyberphysical Automotive Systems*, document SAEJ3061, Society of Automotive Engineers (SAE), Warrendale, PA, USA, 2016. [Online]. Available: https://saemobilus.sae.org/content/j3061_201601

[15] *Road Vehicles—Functional Safety—Part 1–10*, ISO Standard 26262, Geneva, Switzerland, 2011.

[16] IEEE Power Electronics Society. *Cyber-Physical Security Initiative*. Accessed: Dec. 20, 2021. [Online]. Available: https://www.ieee-pels.org/technical-activities/tc-10- design-methodologies

[17] C. Schmittner and G. Macher, "Automotive cybersecurity standards—Relation and overview," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Cham, Switzerland: Springer, 2019, pp. 153–165.

[18] J. Ye et al., "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[19] S. Dey, A. Chandwani, and A. Mallik, "Real time intelligent data processing algorithm for cyber resilient electric vehicle onboard chargers," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2021, pp. 1–6.

[20] Y. Park, O. C. Onar, and B. Ozpineci, "Potential cybersecurity issues of fast charging stations with quantitative severity analysis," in *Proc. IEEE CyberPELS (CyberPELS)*, Apr. 2019, pp. 1–7.

[21] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2020, pp. 98–103.

[22] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2019, pp. 1–6.

[23] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020.

[24] F. Jiang et al., "A false data injection attack detection method for cooperative charging systems," *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 3946–3956, May 2022.

[25] *EV Specifications*. USA. Accessed: Apr. 1, 2023. [Online]. Available: https://www.evspecifications.com/

[26] I. Aghabali, J. Bauman, P. J. Kollmeyer, Y. Wang, B. Bilgin, and A. Emadi, "800-V electric vehicle powertrains: Review and analysis of benefits, challenges, and future trends," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 3, pp. 927–948, Sep. 2021.

[27] H. Karneddi and D. Ronanki, "Reconfigurable battery charger with a wide voltage range for universal electric vehicle charging applications," *IEEE Trans. Power Electron.*, vol. 38, no. 9, pp. 10606–10610, Sep. 2023.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

[28] S. Rivera, S. Kouro, S. Vazquez, S. M. Goetz, R. Lizana, and E. Romero-Cadaval, "Electric vehicle charging infrastructure: From grid to battery," *IEEE Ind. Electron. Mag.*, vol. 15, no. 2, pp. 37–51, Jun. 2021.

[29] *SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler*. SAE, Warrendale, PA, USA. Accessed: Mar. 1, 2023. [Online]. Available: https://www.sae.org/standards/content/j1772

[30] *IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems*. IEEE, Geneva, Switzerland. Accessed: Mar. 1, 2023. [Online]. Available: https://standards.ieee.org/ieee/519/3710/

[31] *In-Cable Control and Protection Device for Mode 2 Charging of Electric Road Vehicles (IC-CPD)*, IEC Standard 62752:2016, Geneva, Switzerland, 2016. [Online]. Available: https://webstore.iec.ch/publication/24284.

[32] D. Ronanki, P. S. Huynh, and S. S. Williamson, "Power electronics for wireless charging of future electric vehicles," *Emerging Power Converters for Renewable Energy and Electric Vehicles: Modeling, Design, Control*. Boca Raton, FL, USA: CRC Press, 2021, pp. 73–110.

[33] M. R. Sarker, H. Pandžic, and M. A. Ortega-Vazquez, "Optimal operation and services scheduling for an electric vehicle battery swapping station," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 901–910, Mar. 2015.

[34] H. Karneddi and D. Ronanki, "Driving range extension of electric city buses using opportunity wireless charging," in *Proc. 47th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2021, pp. 1–5.

[35] M. Yilmaz and P. T. Krein, "Review of battery charger topologies, charging power levels, and infrastructure for plug-in electric and hybrid vehicles," *IEEE Trans. Power Electron.*, vol. 28, no. 5, pp. 2151–2169, May 2013.

[36] H. Karneddi, D. Ronanki, and R. L. Fuentes, "Technological overview of onboard chargers for electrified automotive transportation," in *Proc. 47th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2021, pp. 1–6.

[37] N. D. Weise, G. Castelino, K. Basu, and N. Mohan, "A single-stage dual-active-bridge-based soft switched AC–DC converter with open-loop power factor correction and other advanced features," *IEEE Trans. Power Electron.*, vol. 29, no. 8, pp. 4007–4016, Aug. 2014.

[38] D. Cesiel and C. Zhu, "A closer look at the on-board charger: The development of the second-generation module for the Chevrolet volt," *IEEE Electrific. Mag.*, vol. 5, no. 1, pp. 36–42, Mar. 2017.

[39] D. S. Gautam, F. Musavi, M. Edington, W. Eberle, and W. G. Dunford, "An automotive onboard 3.3-kW battery charger for PHEV application," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3466–3474, Oct. 2012.

[40] S. S. Williamson, A. K. Rathore, and F. Musavi, "Industrial electronics for electric transportation: Current state-of-the-art and future challenges," *IEEE Trans. Ind. Electron.*, vol. 62, no. 5, pp. 3021–3032, May 2015.

[41] *IP67 BC-Series 6.6kW EV Battery Charger*. Current Ways, Santee, CA, USA. Accessed: Mar. 16, 2023. [Online]. Available: https://currentways.com/ip67-bc-series-6-6kw-ev-battery-chargers/

[42] D. Ronanki and S. S. Williamson, "Modular multilevel converters for transportation electrification: Challenges and opportunities," *IEEE Trans. Transport. Electrific.*, vol. 4, no. 2, pp. 399–407, Jun. 2018.

[43] *Highly Integrated Electric Powertrain*, U.S. Patent 20 120 286 740 A1, 2013. [Online]. Available: https://patentimages.storage.googleapis.com/US20120286740A1.pdf

[44] *Fast Charging Device for an (30) Foreign Application Priority Data Electric Vehicle*. Accessed: Mar. 16, 2023. [Online]. Available: https://www.continental-automotive.com/getattachment/Highly-integrated-electric-powertrain.pdf

[45] S. Haghbin, S. Lundmark, M. Alakula, and O. Carlson, "An isolated high-power integrated charger in electrified-vehicle applications," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4115–4126, Nov. 2011.

[46] M. A. H. Rafi and J. Bauman, "A comprehensive review of DC fast-charging stations with energy storage: Architectures, power converters, and analysis," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 2, pp. 345–368, Jun. 2021.

[47] H. Tu, H. Feng, S. Srdic, and S. Lukic, "Extreme fast charging of electric vehicles: A technology overview," *IEEE Trans. Transport. Electrific.*, vol. 5, no. 4, pp. 861–878, Dec. 2019.

[48] *Electric Vehicle Infrastructure Terra HP high power charging UL*. Accessed: Mar. 16, 2023. [Online]. Available: https://search.abb.com/library/Download.aspx?DocumentID=4EVC700601-LFUS&LanguageCode=en&DocumentPartId=&Action=Launch

[49] *ENERCON E-CHARGER 600*. ENERCON, Aurich, Germany. Accessed: Mar. 16, 2023. [Online]. Available: https://www.enercon.de/fileadmin/Redakteur/Service/EC_E-Charger_600_en_web.pdf

[50] Porsche Engineering Charging Solutions, Weissach, Germany. *Excellent Performance Starts with Charging*. Accessed: Mar. 16, 2023. [Online]. Available: https://www.porscheengineering.com/filestore/download/Charging-Solutions-Flyer.pdf

[51] H. Feng, R. Tavakoli, O. C. Onar, and Z. Pantic, "Advances in high-power wireless charging systems: Overview and design considerations," *IEEE Trans. Transport. Electrific.*, vol. 6, no. 3, pp. 886–919, Sep. 2020.

[52] A. Ahmad, M. S. Alam, and R. Chabaan, "A comprehensive review of wireless charging technologies for electric vehicles," *IEEE Trans. Transport. Electrific.*, vol. 4, no. 1, pp. 38–63, Mar. 2018.

[53] *Wireless Power Transfer for Light-Duty Plug-in-Electric Vehicles and Alignment Methodology J2954_202010*. SAE, Warrendale, PA, USA. Accessed: Mar. 16, 2023. [Online]. Available: https://www.sae.org/standards/content/j2954_202010

[54] P. S. Huynh, D. Ronanki, D. Vincent, and S. S. Williamson, "Overview and comparative assessment of single-phase power converter topologies of inductive wireless charging systems," *Energies*, vol. 13, no. 9, p. 2150, May 2020.

[55] S. Samanta and A. K. Rathore, "A new inductive power transfer topology using direct AC–AC converter with active source current waveshaping," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 5565–5577, Jul. 2018.

[56] P. S. Huynh, D. Ronanki, D. Vincent, and S. S. Williamson, "Direct AC–AC active-clamped half-bridge converter for inductive charging applications," *IEEE Trans. Power Electron.*, vol. 36, no. 2, pp. 1356–1365, Feb. 2021.

[57] F. Lu, H. Zhang, and C. Mi, "A two-plate capacitive wireless power transfer system for electric vehicle charging applications," *IEEE Trans. Power Electron.*, vol. 33, no. 2, pp. 964–969, Feb. 2018.

[58] D. Vincent, P. S. Huynh, N. A. Azeez, L. Patnaik, and S. S. Williamson, "Evolution of hybrid inductive and capacitive AC links for wireless EV charging—A comparative overview," *IEEE Trans. Transport. Electrific.*, vol. 5, no. 4, pp. 1060–1077, Dec. 2019.

[59] F. Lu, H. Zhang, H. Hofmann, and C. C. Mi, "An inductive and capacitive combined wireless power transfer system with LC-compensated topology," *IEEE Trans. Power Electron.*, vol. 31, no. 12, pp. 8471–8482, Dec. 2016.

[60] D. Vincent, P. S. Huynh, and S. S. Williamson, "A link-independent hybrid inductive and capacitive wireless power transfer system for autonomous mobility," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 3, no. 2, pp. 211–218, Apr. 2022.

[61] H. Karneddi and D. Ronanki, "A new hybrid conductive-inductive battery charger with reduced component count for electric transportation applications," in *Proc. IEEE Energy Conver. Congr. Expo.*, Oct. 2022, pp. 1–6.

[62] T. A. Nergaard and J. B. Straubel, "Integrated inductive and conductive electrical charging system," U.S. Patent 8 933 661 B2, Jan. 13, 2015. [Online]. Available: https://patents.google.com/patent/US20130285602A1/en

[63] V.-B. Vu, J. M. González-González, V. Pickert, M. Dahidah, and A. Triviño, "A hybrid charger of conductive and inductive modes for electric vehicles," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12021–12033, Dec. 2021.

[64] P. Karamanakos, E. Liegmann, T. Geyer, and R. Kennel, "Model predictive control of power electronic systems: Methods, results, and challenges," *IEEE Open J. Ind. Appl.*, vol. 1, pp. 95–114, 2020.

[65] S. Kouro, M. A. Perez, J. Rodriguez, A. M. Llor, and H. A. Young, "Model predictive control: MPC's role in the evolution of power electronics," *IEEE Ind. Electron. Mag.*, vol. 9, no. 4, pp. 8–21, Dec. 2015.

[66] T. He, J. Zhu, D. D.-C. Lu, and L. Zheng, "Modified model predictive control for bidirectional four-quadrant EV chargers with extended set of voltage vectors," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 7, no. 1, pp. 274–281, Mar. 2019.

[67] *Electric Vehicle Conductive Charging System—Part 1: General Requirements*, IEC Standard 61851-1:2017, IEC, Geneva, Switzerland, 2017. [Online]. Available: https://webstore.iec.ch/publication/33644

[68] *Plugs, Socket-Outlets, Vehicle Connectors and Vehicle Inlets—Conductive Charging of Electric Vehicles—Part 1: General Requirements*, IEC Standard 62196-1:2022, IEC, Geneva, Switzerland, 2022. [Online]. Available: https://webstore.iec.ch/publication/59922

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.

[69] *GB/T 20234.1-2015 (GB/T20234.1-2015)*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.chinesestandard.net/PDF.aspx/GBT20234.1-2015

[70] *Electrway Connector*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.chademo.com/products/connectors/electway_c

[71] *Tesla Wall Connector*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.tesla.com/support/home-charging-installation/wall-connector-features

[72] *CharIN and the Megawatt Charging System (MCS)*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.chademo.com/products/products_type/connectors

[73] C. Lewandowski, S. Gröning, J. Schmutzler, and C. Wietfeld, "Interference analyses of electric vehicle charging using PLC on the control pilot," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2012, pp. 350–355.

[74] *Road Vehicles—Vehicle to Grid Communication Interface—Part 1: General Information and Use-Case Definition*, ISO 15118-1:2013, ISO, Geneva, Switzerland, 2013. [Online]. Available: https://www.iso.org/standard/55365.html

[75] *Road Vehicles—Vehicle to Grid Communication Interface—Part 20: 2nd Generation Network Layer and Application Layer Requirements*, ISO 15118-20:2022, ISO, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/77845.html

[76] *Nissan Leaf Charging Guide*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.zap-map.com/charge-points/nissan-leaf-charging-guide/:~:text=The%20Nissan%20Leaf%20is%20fitted,to%20charge%20at%206.6%20kW

[77] *Charger-Inverter*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.valeo.com/en/charger-inverter/

[78] *Terra 54/54HV Charger Installation Manual*. Accessed: Mar. 27, 2023. [Online]. Available: https://library.e.abb.com/public/5f58d25f8b944c848ca3d955df625775/Terra54_Installation_Manual.pdf

[79] *Electric Vehicle Fast Charging Station Powerful. Grid-Friendly. Reliable*. Accessed: Mar. 27, 2023. [Online]. Available: https://pdf.archiexpo.com/pdf/enercon/enercon-e-charger-600/88093-357197.html

[80] *Wireless Charging*. Accessed: Apr. 5, 2023. [Online]. Available: https://www.st.com/content/ccc/resource/sales_and_marketing/presentation/product_presentation/group0/5a/b1/8e/6c/2b/0d/46/3c/Apec/files/APEC_2016_SiC_%20Wtricity_Wireless_Charging.pdf/_jcr_content/translations/en.APEC_2016_SiC_%20Wtricity_Wireless_Charging.pdf

[81] *HEVO: Wireless Charging for Electric Vehicles*. Accessed: Apr. 5, 2023. [Online]. Available: https://hevo.com/index.html

[82] J. H. Kim et al., "Development of 1-MW inductive power transfer system for a high-speed train," *IEEE Trans. Ind. Electron.*, vol. 62, no. 10, pp. 6242–6250, Oct. 2015.

[83] *Bombardier's PRIMOVE Technology Enters Service on Scandinavia's First Inductively Charged Bus Line*. Accessed: Apr. 5, 2023. [Online]. Available: https://bombardier.com/en/media/news/bombardiers-primove-technology-enters-service-scandinavias-first-inductively-charged-bus

[84] I. Villar, A. Garcia-Bediaga, U. Iruretagoyena, R. Arregi, and P. Estevez, "Design and experimental validation of a 50 kW IPT for railway traction applications," in *Proc. IEEE Energy Conver. Congr. Expo.*, Sep. 2018, pp. 1177–1183.

[85] *Loading the Wireless WAVE*. New York, NY, USA. Accessed: Apr. 5, 2023. [Online]. Available: https://waveipt.com/

[86] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[87] S. M. S. Hussain, T. S. Ustun, P. Nsonga, and I. Ali, "IEEE 1609 WAVE and IEC 61850 standard communication based integrated EV charging management in smart grids," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7690–7697, Aug. 2018.

[88] J. Giraldo et al., "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2019.

[89] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[90] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proc. 50th IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 2195–2201.

[91] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[92] B. Yang, F. Li, J. Ye, and W. Song, "Condition monitoring and fault diagnosis of generators in power networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2019, pp. 1–5.

[93] F. Li et al., "Detection and identification of cyber and physical attacks on distribution power grids with PVs: An online high-dimensional data-driven approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1282–1291, Feb. 2022.

[94] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, "Real-time cyber-physical false data attack detection in smart grids using neural networks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2017, pp. 1–6.

[95] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced cyber-physical security in Internet of Things through energy auditing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5224–5231, Jun. 2019.

[96] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[97] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 49–59, Mar. 2017.

[98] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC: Semantic security monitoring for industrial processes," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 126–135.

[99] K. Chatterjee and S. A. Khaparde, "Data-driven online detection of replay attacks on wide-area measurement systems," in *Proc. 20th Nat. Power Syst. Conf. (NPSC)*, Dec. 2018, pp. 1–6.

[100] D. Ye, T.-Y. Zhang, and G. Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack," *Inf. Sci.*, vol. 481, pp. 432–444, May 2019.

[101] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Saludes, and J. Quevedo, "Detection of replay attacks in cyber-physical systems using a frequency-based signature," *J. Franklin Inst.*, vol. 356, no. 5, pp. 2798–2824, Mar. 2019.

[102] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[103] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 342–347.

[104] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[105] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 161–171, Dec. 2017.

[106] J. Gan, J. Wu, C. Long, and S. Li, "Secure control for networked control systems under denial-of-service attacks," in *Proc. 11th Asian Control Conf. (ASCC)*, Dec. 2017, pp. 31–45.

[107] M. A. Hasnat and M. Rahnamay-Naeini, "A data-driven dynamic state estimation for smart grids under DoS attack using state correlations," in *Proc. North Amer. Power Symp. (NAPS)*, Oct. 2019, pp. 1–6.

[108] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[109] A. Anwar, A. N. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Proc. Pacific–Asia Workshop Intell. Secur. Inform.*, Mar. 2016, pp. 180–192.

[110] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[111] P. Tiwari and D. Ronanki, "Cyber-resilient grid-interactive renewable powered wireless charging of electric vehicles," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Jaipur, India, Dec. 2022, pp. 1–6.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 07:21:13 UTC from IEEE Xplore. Restrictions apply.