This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3041074, IEEE Access

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.2017.DOI*

# Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective

**SAMRAT ACHARYA[1], (Student Member, IEEE), YURY DVORKIN[2], (Member, IEEE), HRVOJE PANDžIć [3], (SENIOR MEMBER, IEEE), AND RAMESH KARRI[1], (Fellow, IEEE)**

[1]Department of Electrical and Computer Engineering, Center for Cybersecurity, New York University, NY 11201, USA
[2]Department of Electrical and Computer Engineering, Center for Urban Science and Progress, New York University, NY 11201, USA
[3]University of Zagreb Faculty of Electrical Engineering and Computing, Zagreb 10000, Croatia

Corresponding author: Samrat Acharya (e-mail: samrat.acharya@nyu.edu).

The work of Y. Dvorkin and S. Acharya was supported by the U.S. NSF under Grants ECCS-2029158 and ECCS-1847285. The work of Y. Dvorkin and H. Pandžić was supported in part by the Croatian Science Foundation and the European Union through the European Social Fund under project Flexibility of Converter-based Microgrids – FLEXIBASE (PZS-2019-02-7747).

**ABSTRACT** With the roll-out of electric vehicles (EVs), the automobile industry is transitioning away from conventional gasoline-fueled vehicles. As a result, the EV charging demand is continuously growing and to meet this growing demand, various types of electric vehicle charging stations (EVCSs) are being deployed for commercial and residential use. This nexus of EVs, EVCSs, and power grids creates complex cyber-physical interdependencies that can be maliciously exploited to damage each of these components. This paper describes and analyzes cyber vulnerabilities that arise at this nexus and points to the current and emerging gaps in the security of the EV charging ecosystem. These vulnerabilities must be addressed as the number of EVs continue to grow worldwide and their impact on the power grid becomes more viable. The purpose of this paper is to list and characterize all backdoors that can be exploited to seriously harm either EV and EVCS equipments, or power grid, or both. The presented issues and challenges intend to ignite research efforts on cybersecurity of smart EV charging and enhancing power grid resiliency against such demand-side cyberattacks in general.

**INDEX TERMS** Cybersecurity, electric vehicles, electric vehicle charging stations, smart grids.

## GLOSSARY

| | |
|---|---|
| AC | Alternating Current |
| AMI | Advanced Metering Infrastructure |
| BEMS | Building Energy Management System |
| BEV | Battery Electric Vehicle |
| CAN | Controller Area Network |
| CCS | Combined Charging System |
| $CO_2$ | Carbon dioxide |
| CD | Compact Disc |
| CHAdeMo | CHArge de MOve |
| DC | Direct Current |
| DER | Distributed Energy Resource |
| DR | Demand Response |
| DoS | Denial-of-Service |
| DVD | Digital Versatile Disc |
| ECU | Electronic Control Unit |
| EV | Electric Vehicle |
| EVCS | Electric Vehicle Charging Station |
| FM | Frequency Modulation |
| GPS | Global Positioning System |
| G2V | Grid-to-Vehicle |
| HEV | Hybrid Electric Vehicle |
| HMI | Human-Machine Interface |
| HVAC | Heating, Ventilation, and Air Conditioning |
| ICE | Internal Combustion Engine |
| ID | Identity |
| IEC | International Electrotechnical Commission |
| ICE | Intelligent Electronic Device |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| IoT | Internet of Things |
| IVI | In-Vehicular Infotainment |
| LAN | Local Area Network |
| LIN | Local Interconnect Network |
| MOST | Media Oriented Systems Transport |
| NFC | Near-Field Communication |
| OpenADR | Open Automated Demand Response |
| OBD | On-Board Diagnostic |

| | |
|---|---|
| OCPP | Open Charge Point Protocol |
| OEM | Original Equipment Manufacturer |
| OVMS | Open Vehicle Monitoring System |
| PFC | Power Factor Corrector |
| PHEV | Plug-in Hybrid Electric Vehicle |
| PLC | Power Line Communication |
| PMU | Phasor Measurement Unit |
| PV | Photovoltaic |
| PWM | Pulse-Width Modulation |
| QR | Quick Response |
| RF | Radio Frequency |
| R&D | Research and Development |
| RFID | Radio Frequency Identification |
| ROM | Read Only Memory |
| RSU | Road-Side Unit |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SD | Secure Digital |
| SM | Smart Meter |
| SMS | Short Message Service |
| SQL | Structured Query Language |
| SW | Switch |
| TPMS | Tire Pressure Monitoring System |
| USB | Universal Serial Bus |
| VANET | Vehicular Ad-hoc Network |
| V2G | Vehicle-to-Grid |
| WAN | Wide Area Network |

## I. INTRODUCTION

OVER the past decade, electric vehicles (EVs) have become one of the primary technologies to assist society in achieving ambitious clean energy and decarbonization goals. The global EV industry has grown on average by 60% annually in 2014–2019, with China and the US leading the way in the number of EVs produced and adopted [1]. This growth is projected to continue with even greater adoption rates in the near future for three main reasons:

1) **Incentivizing clean fuel vehicles and decarbonization efforts:** Many countries have set policies incentivizing clean fuel vehicles. For instance, Netherlands and France are banning sales of fossil-fuel vehicles starting in 2025 and 2040, respectively [2].
2) **Overcoming range anxiety for EV drivers:** Range anxiety is often identified as the main barrier for the adoption of EVs [3]. Recent advances in battery and charging technologies are helping overcome this range anxiety. For instance, Tesla Model S features a 100 kWh battery, which is sufficient for a trip up to 402 miles. Similarly, the capacity and quantity of EV charging stations (EVCSs), and their support infrastructure has expanded considerably. Deployment of EVCSs increased by 60% in the year 2019, leading to the total of 7.3 million EVCS at the year end worldwide [1]. Moreover, the EVCSs have grown in charging power, thus offering faster charging services. Ionity [4] in Europe and Electrify America [5] in the US have deployed EVCSs with the rated charging power up to 350 kW, the greatest charging rate, which is commercially available now. These chargers can charge an EV in under 15 minutes.
3) **Seamless EV charging experience:** Smart EV charging features such as remote control via smartphone applications are not only making EV charging faster, but also user-friendly and, thus, more accessible to broader customer audiences.

Although smart EVCSs have not yet experienced large-scale and high-profile cyberattacks, threats and plausible attack vectors have been reported. Kaspersky Lab [6] revealed security flaws in the ChargePoint Home smartphone application for EV charging. This flaw would enable a remote attacker to intrude into the charger and tamper with EV charging via the WiFi connection to the charging device. Security flaws were also identified in EVlink chargers produced by Schneider Electric [7]. This flaw would allow a remote attacker to bypass hard-coded authentication credentials, inject malware, and disable the charger. Web applications of EVCSs (e.g., by Circontrol, an EVCS vendor with over 80,0000 EVCS across 60 countries [8]) were also vulnerable to cyberattacks. This vulnerability would exploit the weak login credentials for EV charging stored as plain text [9]. These known vulnerabilities, and more importantly a possibility of zero-day vulnerabilities, highlight the cyber risks of EVs and EVCSs.

In light of these vulnerabilities and their societal costs, efforts are underway towards standardizing cyber-physical interfaces for residential and commercial EV charging. The European Network of Cybersecurity [10] proposed security standards for several EV charging architectures. The requirements encompass security for the procurement of the EVCSs and for the communication between the EVCS operator and the power grid operator. The standard defines message encryption for secure communication, access control, future-security-compatible design of EVCS, and monitoring and controlling system security. While generally lagging behind European leaders, the US Department of Energy, Department of Homeland Security, and Department of Transportation outlined cybersecurity challenges of smart EV charging [11], [12]. The US Department of Transportation [13] and the US National Motor Freight Transportation [14] have added a few security features to the recommendations offered in [10]. For example, the EVCS cloud server security is added in [13], [14]. Despite these efforts, they remain as recommendations and are yet to be standardized and enforced. Furthermore, there is no established consensus among the stakeholders – manufacturers, third-party electricity and service providers, power utilities, and national and international authorities – involved in producing, operating, and regulating EVs and EVCSs. For instance, power utilities in New York (NY) proposed a unified cybersecurity protocol for distributed energy resources (DERs), which included EVs, and it was subsequently challenged and not implemented by the third-party providers due to its engineering complications, imple-

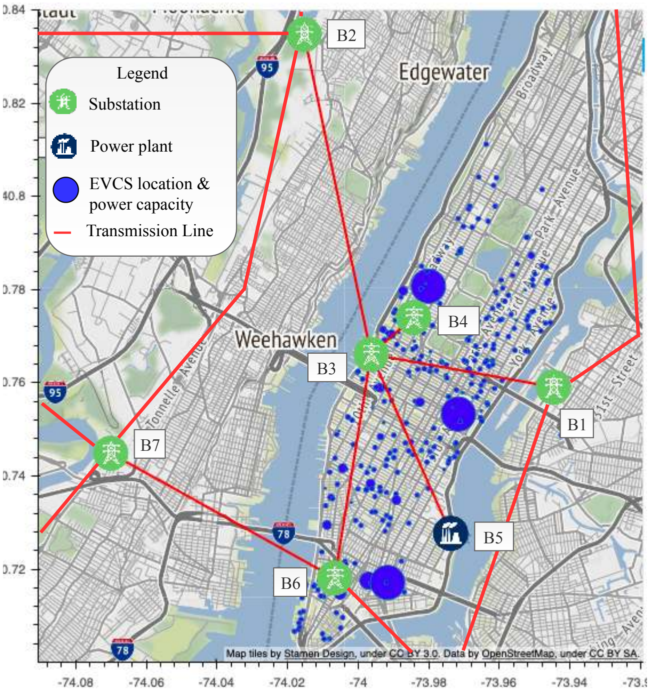

FIGURE 1. Reconstructed topology of the transmission-level power grid and locations of public EVCSs in Manhattan, NY as of March 2019. This data was acquired from public sources. The size of the blue circles is proportional to the EVCS demand. The largest and smallest circles are 100 kW and 6.6 kW, respectively. The figure is adopted from prior work in [16].

mentation barriers, and relatively high adoption costs [15]. Non-standard cyber-physical interfaces make EVs and EVCS susceptible to attacks that can damage the EV and EVCS equipments. Furthermore, vulnerabilities in these interfaces make it possible to weaponize EVs to launch large-scale, demand-side cyberattacks on the power grid [16].

Demand-side cyberattacks on power grids are launched by manipulating internet-connected, high-power and often behind-the-meter demand-side appliances such as EVs, DERs, and heating, ventilation, and air conditioning (HVAC) loads. Although power grids have not encountered such attacks in the past, there is mounting evidence to support that such attacks could be executed using already existing vulnerabilities. As a consequence of the attacks, power grid operators will not be able to cope with them without resorting to massive load shedding. For instance, previous work in [16] revealed a cyber threat using publicly available EV charging and power grid data. This can be exploited by an unsophisticated attacker with minimal capabilities (e.g., foreign and domestic non-state actors). This work demonstrated that this *dilettante* but realistic attack imposes minimal data requirements on the attacker, which can be fulfilled by exploring EVCS smartphone applications for a real-time operational status, charging prices, and historical usage profiles of the EVCSs. Adversarial actors can scrape power grid data from websites and technical documents of the local power utilities and the concerned regulatory authorities to design the most destructive attack strategy via impact-driven simulations. For example, Fig. 1 shows a electrical transmission network and EVCSs in Manhattan, NY, which was reconstructed using exclusively public sources [16].

Motivated by a possibility and fairly low sophistication of the demand-side attacks exploiting EV and EVCS cyber vulnerabilities, this paper provides an in-depth cyber-physical analysis of smart EV charging to increase cyber awareness among the stakeholders involved and to facilitate R&D and regulatory efforts to seek acceptable consensus for EV charging protocols. The main contributions of the paper are summarized below:

- This is the first paper providing a comprehensive review of the state-of-the-art EV charging security. It details the device- and network-level vulnerabilities that are common at the nexus of EVs, EVCSs, and power grids.
- It reviews the technical and financial risks faced by the power grids in light of realistic cyberattack scenarios on EV charging infrastructure and its network.
- Finally, the paper seeks to raise awareness of the simple, yet severe demand-side cyberattacks that can be launched via EV charging and facilitates the negotiation of a common cybersecurity consensus among the concerned parties- EV and EVCS manufacturers, EV drivers, power grids, and service providers for secure EV charging.

The rest of the paper is organized as follows. Section II presents an overview of smart grid cybersecurity and its gap to bridge EV charging security. Sections III and IV discuss a cyber-physical model of the EVs and EVCSs. Sections V and VI review the known vulnerabilities in EVs and EVCSs, respectively. Section VII presents a threat model to disrupt power grid operations via the known attack vectors in the EVs and EVCSs. Section VIII presents impacts of malicious smart EV charging on the power grid. Finally, Section IX concludes the paper.

## II. CYBERSECURITY OF SMART GRIDS

Fig. 2 presents a cyber-physical overview of the smart electric power grid. This *smartness* is facilitated by the roll-out of IoT-enabled grid-edge resources such as photovoltaic (PV) panels, storage units, controllable, schedulable and shiftable loads (e.g., EVs and HVACs) that can provide on-demand flexibility to the grid, as well as a vast communication infrastructure that makes it possible to coordinate these resources with the remaining power grid. Furthermore, the IoT-enabled resources continue to be deployed in all four power sectors: generation, transmission, distribution, and customers [17]. However, this proliferation also introduces additional cyber threats to the power grid exploiting IoT-enabled devices. Table 1 summarizes these threats based on their origin and attack class. Below is a comprehensive discussion of these threats in the context of smart grid cybersecurity.

### A. STRIDE THREAT MODEL

Cyberattacks can be categorized using the STRIDE threat model, a categorical risk assessment model for spoofing,

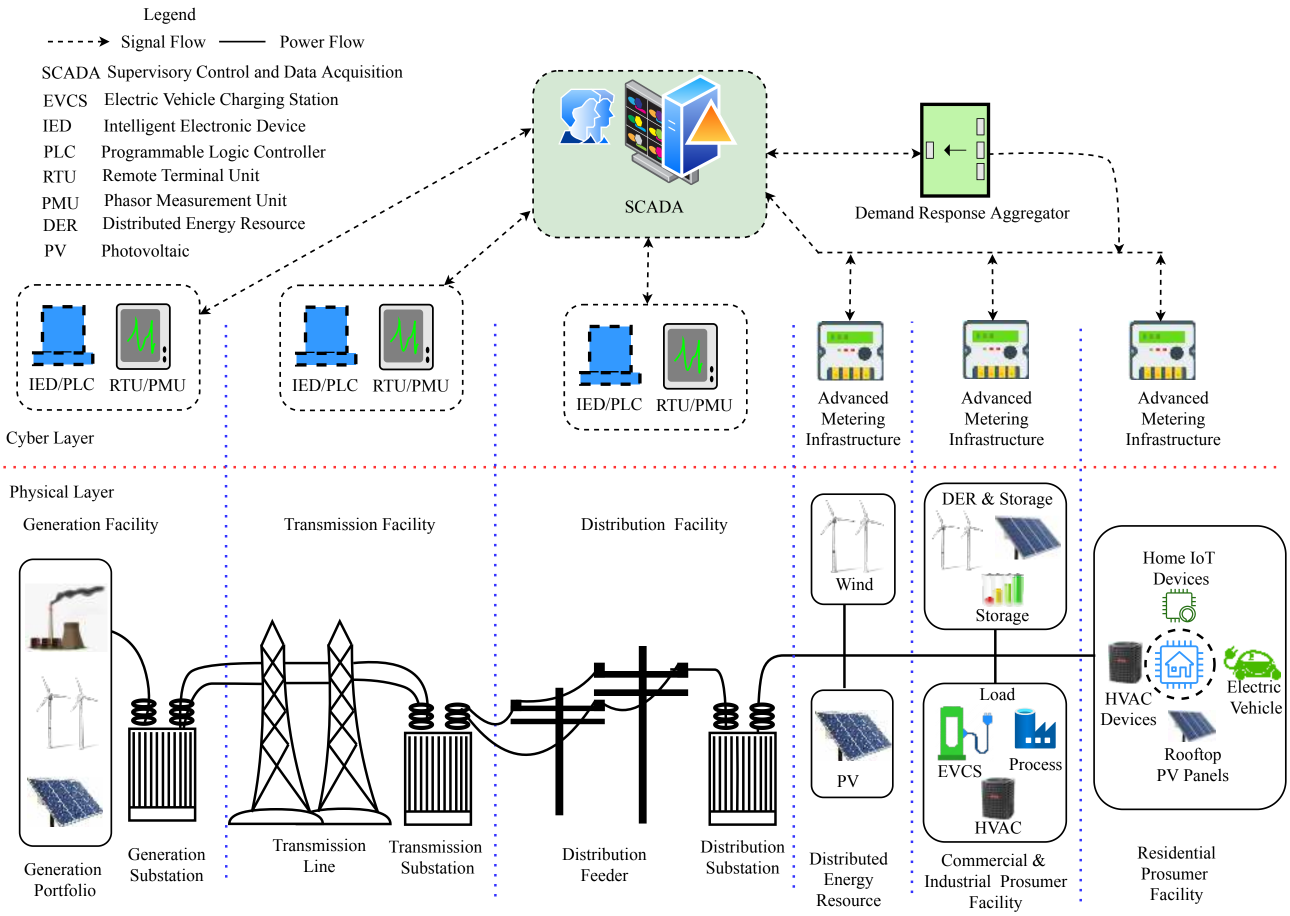

FIGURE 2. A cyber-physical overview of the smart electric power grid.

tampering, repudiation, integrity, denial-of-service (DoS), and elevation of privilege threats to a given cyber-physical system, originally developed by Microsoft to asses software threats [18]. This study uses the STRIDE threat model to discuss cyber threats to smart grids.

- **Spoofing** refers to disguising as a legitimate source or process. This common class of attacks has already been operationalized in real-world power grids (e.g., the infamous 2015 Ukraine power grid attack was initiated by sending spear phishing emails to the employees to access the supervisory control and data acquisition (SCADA) system [19]).
- **Tampering** means an unauthorized alteration or destruction of data or a process. This attack is widely studied as a false data injection attack, where attackers exploit vulnerabilities on devices and communication channels. For example, the data measured by the SCADA field units (e.g., phasor measurement unit (PMU) and remote terminal unit (RTU)) can be maliciously tampered with to create anomalous control signals and grid schedules [20].
- **Repudiation** denotes irresponsibility of actions performed. For example, demand response (DR) schedules and incentives exchanged among the power grid and DR provider using the OpenADR 2.0 protocol are digitally certified and acknowledged [21]. As a result of this certification, the likelihood of denying any malicious actions of the DR provider is reduced. It also implies that the concerned party is responsible or aware of the actions performed in its device or service.
- **Information Disclosure** is an unauthorized acquisition and dissemination of information. For instance, smart meters (SMs) measure granular electricity usage data and broadcast this data to the utility, which can be sniffed exploiting vulnerabilities in the measurement and communication [22].
- **DoS** refers to a state where any authorized entity is deprived of reliable and timely access to services and information (e.g. SMs or other metering/management units). This attack is also likely to be combined with information disclosure and tampering attacks.
- **Elevation of Privilege** implies that an attacker gains extra privileges circumventing standard authorization protocols. For instance, if an EVCS permits an user to inject malware through its universal serial bus (USB) port, the user privilege is elevated to an EVCS operator.

**TABLE 1.** Survey of Smart Grid Vulnerabilities: type of study (attack vs defense), threats considered, type of attack(s), and scope of the study.

| | Study | | Threat | | | | | | Attack Class | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Papers/Research | Attack | Defense | SCADA | SCADA Field Devices | AMI | Demand Response | IoT of HVAC Devices | EV Charging | Spoofing | Tampering | Repudiation | Info disclosure | Denial-of- Service | Elevation of Privilege |
| Lee et al. [23] | ✓ | ✓ | ✓ | | | | | | | ✓ | | ✓ | | |
| E-ISAC [19] | ✓ | | ✓ | | | | | | | | | ✓ | ✓ | |
| Sridhar et al. [20] | ✓ | | ✓ | ✓ | | | | | | ✓ | | | | |
| Shepard et al. [24] | ✓ | | | ✓ | | | | | ✓ | | | | | |
| Deng et al. [25] | ✓ | | | ✓ | | | | | | | ✓ | | | |
| Seijo et al. [26] | ✓ | | | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Tarlogic [22] | ✓ | | | | ✓ | | | | | ✓ | | | | |
| Wu et al. [22] | ✓ | | | | ✓ | | | | | ✓ | | ✓ | | |
| Greveler et al. [27] | ✓ | | | | ✓ | | | | | | | ✓ | | |
| Tabrizi et al. [28] | ✓ | | | | ✓ | | | | | ✓ | | | | |
| Kumar et al. [29] | ✓ | | | | ✓ | | | | | ✓ | | | | |
| Wu et al. [30] | ✓ | | | | ✓ | | | | | ✓ | | | | |
| AlMajali et al. [31] | ✓ | | | | ✓ | ✓ | | | | | | | ✓ | |
| Raman et al. [32] | ✓ | | | | | ✓ | | | ✓ | | | | ✓ | |
| Ustundag et al. [33] | ✓ | | | | | ✓ | | | ✓ | | | | | |
| Karimi et al. [34] | ✓ | | | | | ✓ | | | ✓ | ✓ | | | | |
| Soltan et al. [35] | ✓ | | | | | | ✓ | | | ✓ | | | | |
| Huang et al. [36] | ✓ | ✓ | | | | | ✓ | | | ✓ | | | | |
| Dvorkin et al. [37] | ✓ | | | | | | ✓ | | | ✓ | | | | |
| Amini et al. [38] | ✓ | | | | | | ✓ | | | ✓ | | | | |
| Acharya et al. [16] | ✓ | | | | | | | ✓ | | ✓ | | ✓ | ✓ | |
| Rohde [39] | ✓ | | | | | | | ✓ | | ✓ | | | ✓ | |
| Khan et al. [40] | ✓ | | | | | | | ✓ | | | | | ✓ | |
| Morrison [41] | ✓ | | | | | | | ✓ | | | | | ✓ | |

## B. SMART GRID THREATS

### 1) SCADA Threats

SCADA is a centralized monitoring and control system, which is commonly used in real-world power grids, and can be split into four main components: 1) a central master terminal unit assisted by various control subsystems such as an energy management system, a DER management system, a geographic information system, and a DR automation, 2) a human-machine interface (HMI) for assisting system operators to manage SCADA, 3) field units such as PLC and RTU, and 4) communication channels [42]. The central master terminal unit along with its subsystem controllers are networked by local area networks (LAN) such as TCP/IP and UDP. This SCADA network and corporate LANs used by the operators are separated with firewall, virtual private networks, and intrusion detection systems. However, this separation has been insufficient to prevent the 2015 Ukraine power grid attack [19]. Furthermore, the SCADA network remains vulnerable to insider's attacks (e.g., organized by a disgruntled or radicalized employee) despite the industry-grade defense mechanisms.

### 2) SCADA Field Unit Threats

SCADA field units include intelligent electronic device (IEDs), PLCs, RTUs, and PMUs. IEDs are microprocessor devices such as relays, sensors, and breakers. RTUs monitor IEDs and transmit measurements to PLCs, SCADA, or both. In turn the PLCs and SCADA send control signals to IEDs via RTUs. Due to this control ability of PLCs, some control actions can be taken without involving SCADA in a decentralized fashion. Unlike PLCs and SCADA, PMUs are relatively new to power grid monitoring and provide measurements on a microsecond-resolution compared to a seconds-resolution of RTUs. The field units communicate with each other using field-bus protocols, while communications with SCADA rely on the ModBUS and DNP3 protocols and communication technologies such as radio frequency (RF), optical fiber, telephone lines, and power line communication [42]. Notably, these protocols are vulnerable to cyber attacks. For instance, the DNP3 protocol allows for attackers to sniff and tamper with data via unauthenticated communication [23]. Furthermore, data from field units can be manipulated by attackers to force system operators to take anomalous or erroneous decisions. For instance, if global positioning system (GPS) signals used by PMUs are spoofed by even microseconds, it can cause PMU errors above a desirable error limit [24]. Similarly, injecting false data into an automatic governor controller [20] and a state estimator [25] can destabilize system operations.

### 3) Advanced Metering Infrastructure (AMI) Threats

Power grids increasingly deploy AMI such as SMs to enable two-way communications between the utility, consumers and DERs. Residential consumers or prosumers may have IoT-enabled devices such as smartphone connected to the same network as their SM, while commercial DER operators are expected to protect their SM connected network with VPN. With this attack surface, SMs and their communication channels are prone to all classes of cyberattacks [22], [26]. For instance, Kumar et al. [29] demonstrated feasibility of tampering attacks on a SM manufactured by General Electric in a controlled lab environment. The attack is based on ping flood attack, where the SM is pinged with continuous traffic and, in turn, the SM responds to the ping overloading SM traffic. This resulted in measuring a lower power consumption data, which incured financial losses to the utility. Similarly, Wu et al. [30] presented an integrity attack on SM data by switching behind-SM loads ON/OFF at the same sampling rate as the SM. Furthermore, AlMajali et al. [31] reported that as low as 5% of SMs, simultaneously sending low-bit rate traffic to the utility, will be sufficient to overload and disable their communication with the utility.

### 4) Demand Response Threats

DR resources exploit AMI and SMs and, therefore, are also vulnerable to the threats presented in Section II-B3. Additionally, there are threats which are specific to DR. For instance, Raman et al. [32] reported the manipulation of the behavior of residential high-wattage appliances as a result of sending a false DR alert or disrupting a real-time DR alert, which can lead to reduced power grid reserves, hampered voltage profiles, increased peak loads, and even forced power outages. Similarly, Ustundag et al. [33] spoofed a Short Messaging Service (SMS) alert sent to DR customers leading to voltage instability and system outages caused by anomalous DR responses. Furthermore, Karimi et al. [34] tampered with DR incentives broadcasted to DR customers, and reported their anomalous behavior to the DR calls, thus causing an erroneous evaluation of curtailed power.

#### 5) Threats from Devices with IoT

High-wattage devices and appliances with IoT interfaces can be infiltrated exploiting vulnerabilities in local networks with weak passwords and in connectivity with remote devices such as smartphone and smart television, which are prone to supply chain threats. In general, cyber manipulations with IoT-connected high-power devices that can be orchestrated to damage the power grid fall under the category of so-called demand-side or load altering cyberattacks [35]–[38]. Soltan et al. [35] and Huang et al. [36] demonstrated that such attack can cause regional and cascading power outages, as well as an increase in power grid operating costs. Amini et al. [38] presented a muti-period dynamic demand-side cyber attack causing frequency instability. Dvorkin and Garg [37] presented a model to analyze propagation of demand-side cyberattacks from the distribution networks to the transmission network under different attack strategies and in presence of relay protection means.

#### 6) EV Charging Threats

This class of smart grid threats is the interest of this paper. The paper provides an in-depth analysis of these threats in the following sections. Additionally, studies [16], [39]–[41] from Table 1, which operationalize EV attacks on the power grid, are also discussed in detail in Section VIII.

### C. SMART GRID SECURITY

There are several defense mechanisms described in the literature to enhance smart grid cybersecurity. These mechanisms include cryptographic solutions, firewalls, virtual private network, and strong authentication credentials. For example, [43]–[45] propose mechanisms for authenticating the interface between the SMs and an utility or a local energy management system. However, such schemes have a centralized authority to manage the authentication database, which incurs a system-wide failure upon a point of attack, i.e., an attack on a centralized database or server. Recently decentralized security techniques such as blockchain have surfaced as technically competitive options for smart grid security [46]–[50]. Using blockchains inherently increases security and privacy by means of: i) trustless decentralized network, ii) immutability, and iii) network consensus. Unlike the centralized security authority, each blockchain is managed by an anonymized decentralized node that verifies authenticity of new nodes and data using network consensus. For example, two smart grid resources can transact their energy with each other without involving a mediator (e.g., the utility [49]). Furthermore, blockchains maintain timestamped and hashed list of data (e.g., EV charging data [48], [50]) known as blocks, i.e., a current hash depends on previous blocks. This hashing increases the difficulty for an attacker to tamper with data. Although blockchains have more robust security features compared to centralized security mechanisms, it has been shown to be vulnerable to security threats arising from cryptojacking, where malicious actors access unauthorized computations across blockchain nodes thwarting genuine transactions. For example, compromising $51\%$ of blockchain nodes in a given network can enable deleting all nodes and rewriting consensus rules [51].

### D. RELATED WORK

There are several reviews and surveys on smart grid security, see [52]–[57]. Yan et al. [52] surveyed security of smart grid communication technologies and protocols. Otuoze et al. [53] classified smart grid cyber vulnerabilities across technical (e.g., device and network) and non-technical (managerial and regulatory) issues. Mehrdad et al. [54] surveyed cyber-physical security issues of smart grids across four dimensions of resiliency, including prevention and planning, detection, response, and recovery. Liu et al. [55], Gunduz et al. [56], and El Marabet et al. [57] surveyed smart grid attacks based on emerging privacy and security requirements of smart grids, i.e., an equivalent taxonomy of the STRIDE threats. However, these surveys [52]–[57] are focused on a holistic view of smart grid security as presented in this section and disregard the nuances and complexity associated with particular attack vectors. Hence, this paper builds on discussions in [52]–[57] to describe and analyze cyber vulnerabilities arising from EV charging. To our knowledge, this is the first survey paper discussing cybersecurity of EV charging and its implications on smart grids.

## III. ELECTRIC VEHICLES ARE CYBER-PHYSICAL SYSTEMS

This section provides a cyber-physical description of EVs. The physical layer discusses EV components from a power engineering perspective, while the cyber layer discusses communication assets and interfaces of the EV that allow for connecting it with external components. Fig. 3 shows cyber-physical details of the nexus of EVs, EVCSs, and power grid.

### A. PHYSICAL LAYER

EVs are classified based on the source of energy as battery electric vehicles (BEVs), plug-in hybrid electric vehicles (PHEVs) or hybrid electric vehicles (HEVs). BEVs are powered solely by an electrochemical battery charged from the power grid using either residential or commercial EVCSs. PHEVs are powered by both a fossil-fuel-based internal combustion engine (ICE) and an electrochemical battery [58], which can be alternated either by a battery management system, or by an automated trip planner, or manually by a driver using switches SW C and SW D (see Fig. 3). The HEVs are similar to the PHEVs, except that they plug into the grid for energy exchange. Notably, BEVs can also plug

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3041074, IEEE Access

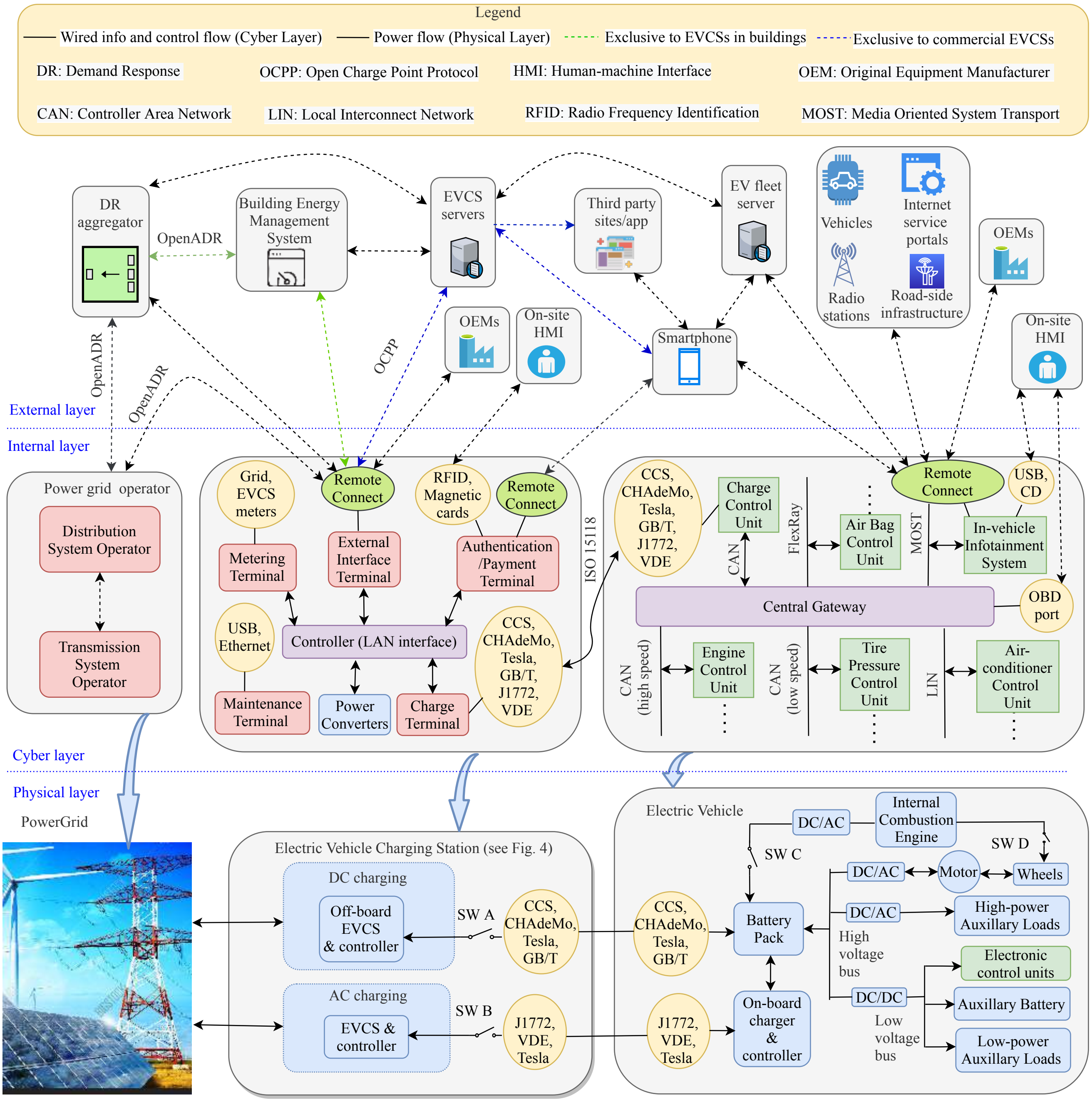
Legend
Wired info and control flow (Cyber Layer)
Power flow (Physical Layer)
Exclusive to EVCSs in buildings
Exclusive to commercial EVCSs
DR: Demand Response
OCPP: Open Charge Point Protocol
HMI: Human-machine Interface
OEM: Original Equipment Manufacturer
CAN: Controller Area Network
LIN: Local Interconnect Network
RFID: Radio Frequency Identification
MOST: Media Oriented System Transport
DR aggregator
OpenADR
Building Energy Management System
EVCS servers
Third party sites/app
EV fleet server
Vehicles
Internet service portals
Radio stations
Road-side infrastructure
OEMs
OEMs
On-site HMI
Smartphone
On-site HMI
OpenADR
OpenADR
OCPP
External layer
Internal layer
Power grid operator
Distribution System Operator
Transmission System Operator
Grid, EVCS meters
Remote Connect
RFID, Magnetic cards
Remote Connect
Metering Terminal
External Interface Terminal
Authentication /Payment Terminal
USB, Ethernet
Controller (LAN interface)
CCS, CHAdeMo, Tesla, GB/T, J1772, VDE
Maintenance Terminal
Power Converters
Charge Terminal
ISO 15118
CCS, CHAdeMo, Tesla, GB/T, J1772, VDE
Charge Control Unit
CAN
FlexRay
Air Bag Control Unit
MOST
Remote Connect
USB, CD
In-vehicle Infotainment System
Central Gateway
OBD port
CAN (high speed)
Engine Control Unit
CAN (low speed)
Tire Pressure Control Unit
LIN
Air-conditioner Control Unit
Cyber layer
Physical layer
PowerGrid
Electric Vehicle Charging Station (see Fig. 4)
DC charging
Off-board EVCS & controller
SW A
CCS, CHAdeMo, Tesla, GB/T
AC charging
EVCS & controller
SW B
J1772, VDE, Tesla
Electric Vehicle
DC/AC
Internal Combustion Engine
SW C
SW D
DC/AC
Motor
Wheels
CCS, CHAdeMo, Tesla, GB/T
Battery Pack
DC/AC
High-power Auxillary Loads
High voltage bus
Electronic control units
DC/DC
Auxillary Battery
J1772, VDE, Tesla
On-board charger & controller
Low voltage bus
Low-power Auxillary Loads

**FIGURE 3.** A schematic diagram of the multi-level, cyber-physical nexus of EVs, EVCSs and the power grid.

into the grid. From a power engineering perspective, the components of a generic EV are:

- *Battery units:* EV batteries are typically operated at ≈300–700 V [59] and can be charged from the power grid via an charger, an ICE, regenerative braking, or a combination of these methods [60]. The most common EV battery types use lithium-ion, lithium-ion polymer, nickel-metal-hydride, lead-acid, sodium-nickel-chloride, and nickel-cadmium electrochemistry [61], [62]. Notably, lithium-ion batteries are thus far the most wide-spread technology in EVs due to their higher energy density and specific-energy, and lower costs compared to other technologies. However, some HEVs use nickel-metal-hydride battries due to their mature abuse-tolerant technology and longer life cycles [61]–[64]. The EVs also have auxiliary batteries usually operated at 12 or 24 V to power auxiliary loads and controllers. Moreover, many EVs are equipped with supercapacitors in addition to the electrochemical batteries, which enable faster energy transfer mechanisms

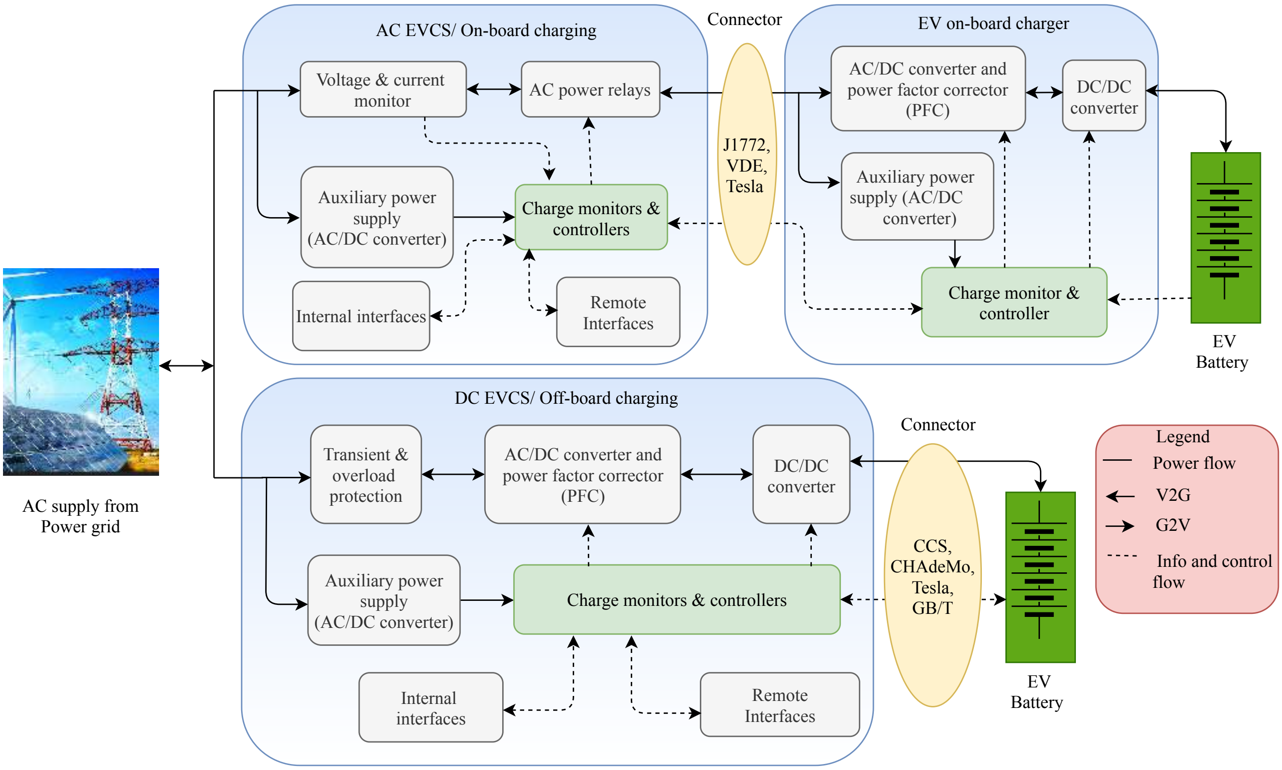
AC EVCS/ On-board charging
Voltage & current monitor
AC power relays
Auxiliary power supply (AC/DC converter)
Charge monitors & controllers
Internal interfaces
Remote Interfaces
Connector
J1772, VDE, Tesla
EV on-board charger
AC/DC converter and power factor corrector (PFC)
DC/DC converter
Auxiliary power supply (AC/DC converter)
Charge monitor & controller
EV Battery
AC supply from Power grid
DC EVCS/ Off-board charging
Transient & overload protection
AC/DC converter and power factor corrector (PFC)
DC/DC converter
Auxiliary power supply (AC/DC converter)
Charge monitors & controllers
Internal interfaces
Remote Interfaces
Connector
CCS, CHAdeMo, Tesla, GB/T
EV Battery
Legend
Power flow
V2G
G2V
Info and control flow

FIGURE 4. A schematic diagram of the cyber-physical layers within a typical EVCS.

during ignition and regenerative braking. However, supercapacitors have a lower energy density than batteries and, therefore, battries are used as the primary energy storage unit by EVs.

- *Power conditioning units:* EV batteries can be charged from the power grid either directly by means of external residential or commercial chargers or via the internal on-board charger [59]. The latter option typically requires more time for charging the same amount of energy. Fig. 3 illustrates both charging circuits with two mutually exclusive configuration switches SW A and SW B, which prevent the simultaneous use both chargers [59]. The on-board charger and off-board charger use an AC/DC power converter that transform AC power drawn from the power grid to DC power supplied to the battery, as shown in Fig. 4. Additionally, the chargers are equipped with a power factor corrector (PFC), a DC/DC converter, an auxiliary AC/DC converter, as well as a charging monitor and controller. The PFC is to used to ensure that the power charged to the battery satisfy safety requirements on the harmonics and distortions to avoid damage to the battery and its premature decay. As Fig. 3 shows, the the battery is also connected to four additional converters. The first DC/AC converter is 3-phase and bi-directional, which allows to supply power to the traction motor and, in the opposite direction, to charge power back to the battery during regenerative braking. The second DC/AC converted supplies power to high power auxiliary loads such as HVAC systems. The third DC/DC converter steps down voltage to 12 or 24 V and supplies low-power loads such as lights and an auxiliary battery. The fourth AC/DC converter transfers power generated by an ICE to the battery.
- *Motor and Loads:* The AC traction motor is operated at $\approx 240$ V [59], [65] and is typically a 3-phase permanent magnet synchronous motor (e.g., Nissan Leaf) or an induction motor (e.g., Tesla). The high-power auxiliary loads include a 3-phase compressor and fans of the air conditioner, while the low-power auxiliary loads (12 or 24 V) include headlights, cabin lights, radio, power steering, and USB chargers [66]. The auxiliary loads can reduce the range of an EV up to $35\%$, especially if the indoor and ambient temperatures are very different [67]. On the other hand, EV range can also be extended up to $22\%$ by tuning HVAC system settings [68].

## B. CYBER LAYER

This section describes the EV cyber layer, which includes the in-vehicle and external (EV-X) layers. Generally, external cyber interactions accessible by modern EVs include EVCSs, internet service portals, road infrastructure, other vehicles, radio stations, and original equipment manufacturer (OEMs) producing components used in EVs, as shown in Fig. 3. Advances in smart vehicular technologies have significantly enabled the in-vehicular networks to interact with the external networks and infrastructures systems. Although interconnected, these layers differ in the cyber threats they impose, and in the threat propagation patterns within and outside EVs.

### 1) In-Vehicle Layer

Modern vehicles have over 125 electronic control units (ECUs), and this number is constantly increasing [69], [70]. The ECUs enable control of the entire vehicle including critical functions such as brake control, battery management, and infotainment modules. The ECU market is projected to increase at the compound annual of 4.4% through 2025, leading to a total of 3.29 billion ECUs [71]. An ECU consists of a microprocessor, a memory, and input/output interfaces. The ECUs are interconnected via the controller area network (CAN) bus, local interconnect networks (LINs), media oriented systems transport (MOST), and FlexRay [72], [73] as shown in Fig. 3. The CAN bus network is dominant and its security has been discussed as it connects the critical ECUs and, if compromised, can be used to tamper with the EV charging process. The LIN is a cost-effective network used for ECUs such as air-conditioner control unit, which do not require a high-speed communication. MOST is, on the other hand, a costly network used in the in-vehicular infotainment (IVI) system, which requires a high bandwidth communication [74]. Finally, FlexRay is used in ECUs, which require a relative high fault tolerance, such as air bag control unit [75].

The CAN bus architecture is based on a peer-to-peer network, where each ECU and peripheral units are connected and can interact with one another directly as peers. Thus, the network behaves as a centralized communication channel. This bus standard is adopted in EVs due to four reasons. First, the CAN bus is capable of handling simultaneous commands from multiple ECUs in real-time and without significant communication delays. This is achieved through the centralized architecture of the CAN bus, where an ECU sends a message with an arbitration identity (ID) to all ECUs via the CAN bus and only the targeted ECU receives the message. Second, the CAN bus is splited into the high-speed and low-speed buses, which are connected together by the common gateway [76], [77]. The time-critical ECUs such as brake control and battery management units are connected to the high-speed CAN bus, while the less time-critical ECUs such as HVAC controller are hosted at the low-speed CAN bus. Third, the CAN bus enables centralized diagnostics of the ECUs via the on-board diagnostic (OBD) port. Using this port, EV mechanics and regulatory authorities monitor the operational status of the EV such as $CO_2$ emission and battery health. Fourth, the CAN bus is flexible; it is easy to add/remove ECUs, is cost-effective and robust against electric disturbances and electromagnetic interference [78], which may adversely affect the critical EV functions.

Some ECUs such as the tire pressure monitoring system (TPMS) have sub networks with their sensors. The TPMS sub network is formed between battery-powered sensors located on the EV tires and the tire pressure control unit via RF. The control unit processes the signals from the sensors and informs an EV driver of the tire pressure via the CAN bus. Such sub networks are unavoidable. For example, TPMS is legally mandated in the US and Europe to reduce road accidents caused by under-inflated tires [79].

### 2) EV-{X=EVCS}

EVs communicate with a chosen EVCS to coordinate the charging details and preferences via a wired channel as shown in Fig. 3. The L1 and L2 EVCSs use a pilot wire for this communication, while the L3 EVCS communicates using the CAN or PLC protocol. Note that the L1 and L2 EVCSs are defined in Section IV-A. The communication contains signals authenticating the EV and EVCS, control and protection commands, and software packages required for the charging process. The control and protection commands include readiness of the EV for charging (using pulse-width modulation (PWM) signals), requested charging current, current state-of-charge of the EV battery, and ground-fault detection [59]. Although this communication is generally wired, there are a few exceptions when EVs and EVCSs communicate wirelessly using the assigned IP addresses [80]. It is expected that the wireless communication will become more common in the future, however, current protocols for the wireless EV-EVCS communication are diverse. Yet, more recently, the ISO 15118 standard has been used to consolidate the wireless and wired protocols [39].

### 3) EV-{X=Physically Accessible Ports}

EVs have USB ports, compact disk (CD) slot, secure digital (SD) card slot, and OBD2 port for external communication. The OBD2 port is a standardized interface to the CAN bus used by EV mechanics, EV users, and EV regulatory authorities to monitor and obtain reports on the operational status of EVs (e.g., $CO_2$ emission), EV speed and traffic patterns, and battery status. The port is typically located under the EV dashboard, and thus, cannot be accessed directly by potential intruders without breaking into the vehicle. To secure this port, it is common for a proprietary OBD2 scanner to be connected to the port to read the OBD microcontroller data. However, the scanner is often paired to smartphone apps such as EML327 and PLX KiWi [81].

### 4) EV-{X=Internet Service Portals}

Internet service portals (e.g., smartphone applications) are generally enablers for remotely accessing the EV features. EVs use wireless communications to exchange information with web-based and smartphone applications (e.g., Tesla for Tesla EVs and NissanConnect® for Nissan EVs) for monitoring and controlling EV charging [81], [82]. Also, smartphones are often connected to the built-in EV IVI dashboard via bluetooth and USB ports for media playback and smartphone access. As mentioned in Section III-B3, the OBD2 scanner is often paired with a smartphone. Moreover, service portals such as key fobs also communicate wirelessly with EVs for a keyless door entry [83]. The web-based and smartphone applications use long and medium range wireless channels such as cellular networks and WiFi [81], [82], whereas key fobs use short-range RF or near-field communication (NFC) [79], [83].

#### 5) EV-{X=Radio Stations}

The GPS is an indispensable component of modern EVs used to receive the spatial information broadcasted from a space-based radio station. For example, the EVs use the GPS signals to find a path to the nearest/cost-effective EVCS, or other user-defined destinations. EV infotainment applications connect to the radio stations and navigation stations using cellular networks.

#### 6) EV-{X=OEM/Vendors}

The EVs communicate wirelessly with their manufacturer and OEMs for regular and ad-hoc software update and security patching using wide area network (WAN) such as cellular network and RF. The OEMs and vendors prefer wireless patching strategies rather than the conventional patching methods performed via on-site HMI (e.g., USB and ethernet ports) because of swift delivery and cost-effectiveness [84].

#### 7) EV-{X=Road-side Infrastructure and Vehicles}

Modern EVs have the capability of communication with the road infrastructure such as traffic signals and other vehicles via cellular networks for a safe, efficient, and comfort driving. Although not widely deployed yet, these communications are expected to become more common as self-driving and partially automated driving technologies are introduced.

## IV. ELECTRIC VEHICLE CHARGING STATIONS ARE CYBER-PHYSICAL SYSTEMS TOO

This section provides a cyber-physical description of an EVCS shown in Fig. 3. While the physical layer generally, does not change across different commercial-residential EVCS designs, the cyber layer varies for different use cases and is described below.

### *A. PHYSICAL LAYER*

An EVCS is a device that facilitates the power exchange between the power grid and the EVs, thus enabling EV charging. Although this power exchange can be bidirectional, the grid-to-vehicle (G2V) direction is more common and the vehicle-to-grid (V2G) direction is limited to relatively small-scale pilot projects and implementations, e.g., [85], [86]. However, it is projected that V2G services become more wide spread in the near future, especially in regions with near-term deep-decarbonization goals [2].

Depending on the voltage and power transfer ratings, EVCSs are categorized into three levels: Level 1 (L1), Level 2 (L2), and Level 3 (L3). The L1 EVCSs are the wall outlets with an AC supply system of single-phase 120 V and 12–16 A delivering the charging power rate of 1.44–1.92 kW. The L2 EVCSs supply power to EVs via a 1-phase 240 V AC or a 3-phase 400 V AC cable with the rated current of up to 80 A and the rated power power of up to 55 kW. The L1 and L2 EVCSs are mostly residential chargers. The L1 chargers dominate in the US and the L2 chargers are popular outside the US. The L3 EVCSs are commercial high-power chargers ensuring a fast turnaround of charging vehicles. L3 units supply DC power of up to 800 V, 500 A, and 350 kW. The L3 EVCSs include DC fast chargers and superchargers for medium and heavy duty EVs [14]. Since the L1 and L2 EVCSs output AC power, they are referred to as AC EVCSs and L3 EVCS are called DC EVCSs for the same reason, as shown in Fig. 4.

A DC EVCS is more complex by design and bulkier than its AC counterpart as the former contains hardware and software necessary to convert AC power from the grid to DC power and to control EV charging. On the other hand, an AC EVCS operates at lower voltages and currents than the DC EVCS, and utilize the EV on-board charger for power conversion. The AC EVCS monitors and controls the power flow to the EV on-board charger and controls the physical and cyber connection between the EV and the grid. A DC EVCS can be viewed as a combination of an AC EVCS and a high-power on-board charger. Generally, a DC EVCS hosts power converters, PFC, sensors and protection relays, controllers, and communication interfaces. The AC power drawn from the power grid is continuously monitored and checked against overload and voltage and current transients using the electromagnetic interference filters, protection relays, and circuit breakers. The two-stage AC/DC converters are deployed with the PFC to boost conversion efficiency, control flexibility of charging, and limit total harmonic distortions of current within the limits defined by IEEE 519 [87]. The PFC maintains the power factor close to 1 for reducing harmonics induced into the AC power grid, but it can be adjusted to follow a given power factor value if there is a proper communication and converter configuration. In practice, the AC/DC stage and PFC are integrated into a single unit (e.g., Vienna rectifiers, interleaved PFC or boost converters operating in the continuous current mode). The DC/DC stage regulates the DC output voltage level of the EVCS, which has several deployment topologies (e.g., multiple interleaved buck converters, full-bridge LLC resonant converters, phase-shift full-bridge converter [88]). An auxiliary AC/DC converter powers the sensor, controllers, and relays typically at 12 V.

The off-board charging scheme (e.g., the DC EVCSs) is advantageous over on-board charging scheme as it enables higher charging speeds. However, due to higher investment costs and power supply requirements of DC EVCSs, the AC EVCSs are predominantly used at commercial locations and exclusively at residential locations [89]. Thus, the EVs have charging receptacles for both on-board and off-board charging. There are various types of connectors or plugs between EVCSs and EVs, which tend to differ in their voltage and current ratings among different geographical locations, and EVCS and EV vendors. However, there are regional standards for the connector-receptacle configuration so that EVs are allowed to charge on EVCSs from different vendors. Among these standards, SAE J1722, VDE-AR-E 2623-2-2, and Tesla Destination are the dominant connectors for the L1 and L2 EVCSs. Similarly, the L3 EVCSs use CHAdeMo, combined charging system (CCS), GB/T DC, and Tesla Super Charger connectors. Despite the various connectors, EV manufacturers provide receptacles to allow their EV to charge at other EVCSs (e.g., Tesla EVs have receptacles to charge at non-Tesla EVCSs).

Across these EV charging configurations, the cost of charging infrastructure depends on various societal, environmental, and economic factors and policies, which are jurisdiction-specific. For instance, the adoption of EVs has been influenced by the affordability of EV and availability of residential and commercial charging, environmental awareness about EV advantages, and social justice considerations [90]. In general, the capital cost of a networked L3 EVCS is the greatest, while a non-networked L1 EVCS is the most affordable. For example, the hardware cost of the networked 350 kW L3 EVCS is ≈ $140,000, while the non-networked L1 EVCS costs ≈$813 in the US in 2019 [91]. Similarly, the EV charging price at public L3 EVCS varies between $0.1/kWh to >1/kWh with an average of $0.35/kWh [92].

Despite the EV charger levels (L1, L2, and L3) and types (AC and DC), customers may often pair these installations with distributed energy resources and energy storage units to enhance the EV charging resiliency and energy independence, as shown in the physical layer of Fig. 2. Furthermore, this configuration facilitates future adoption of hybrid AC/DC microgrids [93], [94] or DC grids [95].

### B. CYBER LAYER

The L2 and L3 EVCSs have on-site HMI, EV-EVCS interface, and remote interfaces for improving EV charging efficiency and controllability, as shown in Figs. 3 and 4. In addition to the EV-EVCS cyber interface described in Section III-B, EVCSs have remote interfaces that include communication with a building energy management system (BEMS), power grid, EVCS servers, and smartphones. Since the L1 EVCSs are simple, small-scale, residential, and stand-alone, they typically have restricted choices for on-site HMI and remote interfaces. Below is a discussion of the cyber interfaces in-detail, which helps in building their threat model.

#### 1) EVCS-{X=On-Site HMI}

EVCSs have a touchscreen display, a card reader, and an authentication and maintenance terminal as a part of their HMI. The touchscreen display allows for users to customize their charging session by selecting a desired charging level, connector type, payment method, and duration of the charging process. Moreover, it displays real-time information such as an EVCS operating status, charging price, and energy use. The card reader serves for authentication of the user and payment of the charging session. Proprietary radio frequency identification (RFID) cards and smartphone applications are widely used for the authentication, while charging is paid using these authentication methods, credit or debit cards, and/or cash. The EVCSs have USB, serial, and Ethernet ports for maintenance and software updates.

#### 2) EVCS-{X=BEMS-Power Grid Interface}

The electric power grid and distribution system operators, which are in charge of ensuring cost-efficiency and reliability of electric power delivery to end-users, have been encouraging high-power demand-side appliances such as EVCS to participate in their DR programs. From a cybersecurity angle, the primary goal of the DR programs is to minimize adversarial impacts of high-wattage loads such as EV charging on the power grid and other customers (e.g., avoiding additional losses, excessive demand peaks, current and voltage fluctuations). Some power grid operators use third-party aggregators of small-scale producers and demand-side resources, which works in-between the customers and the grid.

Similar to other small-scale electricity producers and demand-side resources, the DR participation of an EVCS involves a two-way communication, where the grid or aggregator acquires real-time energy use data and broadcasts DR scheduling and pricing signals. This communication of the grid or aggregator can be either directly with the EVCSs or, as in case of the integrated large real-estate EVCS developments, indirectly routed via a BEMS. The direct configuration is suitable for street EVCSs, while the indirect communications are more suitable for urban residential and commercial areas. The direct configuration is performed via the OpenADR 2.0 specification[1] via a WAN [21]. Alternatively, the grid or aggregator can communicate with the BEMS via WAN using the OpenADR 2.0, which controls the various smart appliances including EVCSs via WiFi and ZigBee. Communication between the BEMS and the EVCSs are non-standard. Smart appliances controlled by the BEMS include inverter-interfaced energy sources (e.g., rooftop solar panel), energy data loggers and managers (e.g., SMs), and infotainment systems (e.g., smartphones, smart televisions). These devices have supply chains and connectivity, which are unparalleled in complexity and make it possible to attack their supply chain and penetrate BEMS network premise.

#### 3) EVCS-{X=EVCS Servers-Smartphone Interface}

It is common for an EVCS, especially if in the same geographic area or owned by the same operator, to be networked via a centralized server to coordinate operations (e.g., ChargePoint, Blink, Tesla, and EVgo). Refer to Fig. 2 in [16] for the EVCS servers operating in Manhattan, NY as of March 2019. An EVCS communicate with a centralized server via a proprietary communication protocol. Currently such protocols are not standardized, but efforts are ongoing to devise such a specification, e.g., open charge point protocol (OCPP) [96]. There are four main functions of the centralized EVCS server.

[1] OpenADR 2.0 is a non-proprietary, open standard information exchange model for DR. The model is recognized as IEC standard 62746-10-1 for the interface between customers and the grid/aggregator.

1) Congregate and archive real-time measurements of each EVCS (e.g., operational status and energy usage).
2) Authorize EVs to charge. Each EV can be locally authenticated by the EVCS after receiving authentication request from a smartphone or a proprietary RFID card.
3) Broadcast to web-based and smartphone applications information about EVCS availability, charging levels available, and charging prices. Notably, this information is released by EVCS operators, cross-company third-party sites via smartphone and web-based applications as a part of their business model [16].
4) Communicate with the power grid operator or DR aggregators, either directly or via BEMS (see Fig. 3). While the adoption of indirect communication via BEMS is rare, it has been piloted by some utilities (e.g., Southern California Edison [97]).

In addition to these interfaces, one can envision that in the near future EVCS servers will be equipped to interact with EV fleets (platoons) for enhancing the EV charging experience. For example, this extension is vital to optimize fleet charging in the context of transportation management tasks. Thus, the New York City Taxi and Limousine Commission [98] and other transportation authorities foresee that such extensions are needed as fossil-fueled taxis and rideshare (e.g., Uber or Lyft) vehicles are gradually replaced with EVs.

#### 4) EVCS-{X=OEM/Vendors}

Similar to the interface of EV-OEMs discussed in Section III-B6, an EVCS communicate wirelessly with its manufacturer and other OEMs for regular and ad-hoc software updates and security patches using WAN such as cellular network and RF. Moreover, the EVCS OEMs and vendors also prefer wireless patching and update strategies rather than the conventional approach of physically-accessed patching for cost-effectiveness and swift delivery.

## V. ELECTRIC VEHICLES ARE VULNERABLE TO CYBERATTACKS

Consistent with the cyber-physical outlook of EVs in Section III-B, this section explores EV vulnerabilities arising from: i) in-vehicular networks of ECUs, sensors, and peripherals and ii) external networks of web-based and smartphone applications and their communication links.

### A. IN-VEHICULAR VULNERABILITIES

#### 1) CAN Bus Vulnerabilities

Since the CAN bus architecture is a peer-to-peer system, which is based on the isolated trust model (i.e., the CAN bus security design does not account for a possibility of intrusions from external networks, and hence, is not immune to malware injected externally into it [77]), an attacker that manages to tamper with the CAN bus or even certain individual ECU can fully control EV operations. Full control implies that an attacker can modify, eavesdrop, reverse engineer, spoof, or replay the CAN messages to pursue a desired malicious objective [77], [81], [99]–[102]. A message sent by a ECU or a peripheral device connected via the CAN bus is received by all of its peers. Moreover, the message transported via the CAN bus is neither encrypted nor authenticated to avoid memory overhead and assure its swift transfer [99], which is crucial for time-critical ECUs such as the brake control unit. A message transported via the CAN bus does not contain sending and receiving peer IDs. Rather it is delivered based on its arbitration ID indicating the message priority [81], [103], [104]. The CAN bus has a limited bandwidth inhibiting implementation of sophisticated and computationally expensive encryption without compromising the rate of message delivery [105].

From this perspective, the key challenge of the attacker is to compromise the CAN bus. The OBD2 port of the CAN bus has been widely investigated and marked as a crucial access point to the CAN bus [77], [81], [99], [100], which has a wide infiltration surface aided by physical and remote vulnerabilities. The OBD2 port can be physically accessed by outsiders at many points during the EV life time (e.g., a mechanic during EV maintenance, a valet during parking, and a charging station assistant). Additionally, the OBD2 port can be compromised using smartphone applications, e.g., open vehicle monitoring system (OVMS), connected via a wireless short-range network (e.g., bluetooth [81]) or a cellular network [99], [100]. Hence, the applications allow for remote monitoring and control of the EV components and processes that have cyber interfaces to the CAN bus, including battery charging and traction motor control. Furthermore, third-party- and OEM-distributed telematics, which also connect the OBD2 port to external devices, e.g., laptops, are vulnerable to remote attacks [101].

Similar vulnerabilities in FlexRay, LIN, and MOST have been studied in [74]. If compromised, the LIN and MOST would not lend aforementioned critical attack capabilities as compared to the risks of compromising the CAN and FlexRay. This is because the MOST network is confined to non-critical ECUs such as IVI system, and the LIN has a smaller exposure to external EV networks.

#### 2) TPMS Vulnerabilities

TPMS is another in-vehicular attack vector. The system is vulnerable to cyberattacks causing privacy and security issues of EVs. The signals sent by the tire pressure sensors are not encrypted, the sensors identifiers are 32-bit static, and the sensor messages are not authenticated. These security flaws allow attackers to eavesdrop, reverse engineer, and spoof the communication within 40-meter vicinity to an EV [79]. The attack results in remote tracking of the EV and false data injections into the EV IVI system.

### B. EV-X INTERFACE VULNERABILITIES

#### 1) X={Physically Accessible Ports} Vulnerabilities

Besides the OBD2 port, there are various physical interfaces that connect, and thus, can be used to manipulate the external cyber layer and ECUs. For example, USB ports, SD-card ports, CD-ROM/DVD-ROM drives, headphone jacks, touchscreens, and optical media readers are physical access points to IVI ECUs. These ports are often physically accessed for software updates in the IVI system, smartphone charging, media playback, and human interface. Malicious devices inserted into these ports enable an attacker to inject persistent malware in the IVI system, to launch DoS attack against the system, and even to provide a side-channel access point to hamper other ECUs [106]–[108]. Such malicious device can reach an EV at various points of its supply chain and maintenance. Furthermore, smartphone and Ethernet terminal further expand an attack surface for remote intrusions by enabling an indirect access to IVI ECU.

#### 2) X={EVCS} Vulnerabilities

An EV typically communicates with an EVCS via a wired communication layer of a CAN bus or PLC using communication protocol ISO 15118, which is vulnerable to cyberattacks [11], [109], [110]. The ISO 15118 regulates the communication between an EV and an EVCS, but lacks security measures such as certification of messages and end-to-end encryption in a trusted transport layer security [110], which can enable a remote attacker to eavesdrop, modify, and spoof the EV charging message. For example, Luo et al. [109] demonstrated a possibility of remote eavesdropping of EV charging messages in 54 EVCS with CCS connectors. This attack also successfully revealed private EV information, including its unique identifiers used for charging and payment. Besides these security and privacy issues, malware infected EVs can transmit the infection to the connected EVCS and vice-versa [11].

#### 3) X={Internet Service Portals} Vulnerabilities

In addition to USB ports, the IVI system can be interfaced with smartphones wirelessly (e.g., bluetooth). Although short-range, this pairing is also vulnerable to cyberattacks because a remote attacker can intrude the connection, reverse engineer the encryption of the pair, eavesdrop the encrypted messages, and spoof the messages [108], [111], [112]. This vulnerability enables an attacker to inject malware in the IVI system, deny the IVI service, and steal smartphone and IVI data. Furthermore, malicious smartphone apps mirrored in the IVI dashboard pose side-channel threats to the CAN bus and data integrity threats to the IVI system [113]. These vulnerabilities likely raise security concerns when EV drivers use various third-party smartphone applications for remote EV monitoring and control, and for EVCS finding. Furthermore, third-party applications installed in the IVI system can be malicious or can be attacked. For instance, software updates for the third-party applications can be sniffed and redirected to a malicious server, leading to malware injection in the IVI system [114].

The remote keyless entry system of an EV is triggered by pressing a key fob within a vicinity of EV ($\approx 5 - 20$ meters), which in turn transmits an encrypted dynamic or static signal from a key fob to the door control ECU via a RF wave. After authenticating the received signal, the ECU locks/unlocks the door and puts off the security alarm. Attackers can eavesdrop, record, reveres engineer, and jam the transmitted signals remotely, which allows the attacker physically access EVs and even launch DoS attack on door operations [83].

#### 4) X={Radio Stations} Vulnerabilities

The GPS signals are vulnerable to remote cyberattacks such as spoofing and jamming [115], [116], which allow attackers to feed false spatial information and even put off the navigation system in EVs. The GPS signals are relatively weak due to long travel distances, and hence, the attacker-generated stronger signals are preferred by the GPS receiver. Similarly, signals broadcasted by FM radio stations to an EV radio are vulnerable to remote spoofing and malware injection attacks [112], [117].

#### 5) X={Road-side Infrastructures and Vehicles} Vulnerabilities

Advances in intelligent and autonomous transportation requires wireless communication within an individual, among vehicle fleets and road-side infrastructure systems. This futuristic communication architecture is called vehicular ad-hoc network (VANET), where vehicles and road-side units (RSUs) are connected via LANs or cellular networks. Vehicles exchange information about vehicle position and speed, road, traffic, and accidents with RSUs and other vehicles for an increased safety, comfort, and efficiency in driving and routing [118], [119]. However, these interfaces increase the attack surface to external networks and devices causing privacy and data integrity issues of the vehicles [118], [120]. For example, an attacker can launch a Sybil-type attack in VANET, mimicking the presence of numerous virtual vehicles in the network. These fake vehicles can jam the network or spread misinformation to RSUs and connected vehicles.

#### 6) X={OEMs/Vendors} Vulnerabilities

The OEM and third-party vendors must access ECUs to deliver security patches and software updates. This is traditionally done using physical dongles and USB flash drives via the OBD2 and USB ports. As such, these traditional methods are vulnerable to supply chain and maintenance attacks. Presently, the OEM and third-party vendors are switching to wireless updates to avoid the barriers and costs associated with physical delivery [121]. The updates are sent as code or data images, as well as metadata containing information for authentication. The wireless software updates are thus vulnerable to man-in-the-middle cyberattacks where an attacker can remotely eavesdrop, deny, and alter the update [122].

## VI. ELECTRIC VEHICLE CHARGING STATIONS ARE VULNERABLE TO CYBERATTACKS TOO

Consistent with the EVCS cyber layer in Section IV-B, the vulnerabilities of an EVCS are categorized into two types: i) vulnerabilities in EVCS cyber components and internal communication networks and ii) vulnerabilities in the external EVCS communication networks.

TABLE 2. Survey of EV and EVCS Vulnerabilities: type of study (attack vs defense), threats considered, and type of attack(s).

| | Study | | Threat | | Attack Class | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Papers/Research | Attack | Defense | EVs | EVCSs | Spoofing | Tampering | Repudiation | Info Disclosure | Denial-of- Service | Elevation of Privilege |
| Koscher et al. [77] | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rouf et al. [79] | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | |
| Woo et al. [81] | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | |
| Garcia et al. [83] | ✓ | | ✓ | | ✓ | ✓ | | | | |
| Currie [99] | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Jafarnejad et al. [100] | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Waszecki et al. [102] | | ✓ | ✓ | | | ✓ | | | ✓ | |
| Checkoway et al. [108] | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | ✓ |
| Baker et al. [109] | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | | |
| Miller et al. [112] | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | |
| Mazloom et al. [113] | ✓ | | ✓ | | | ✓ | | | | ✓ |
| Luo et al. [114] | ✓ | ✓ | ✓ | | ✓ | ✓ | | | ✓ | |
| Zeng et al. [116] | ✓ | | ✓ | | ✓ | | | | | |
| Karthik et al. [122] | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | |
| Schneider [7] | ✓ | | | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| Circontrol [9] | ✓ | | | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Rohde [39] | ✓ | | | ✓ | | ✓ | | | ✓ | |
| Van Aubel et al. [123] | | ✓ | | ✓ | | | ✓ | ✓ | | |
| Rubio et al. [124] | | ✓ | | ✓ | | | ✓ | ✓ | | |
| Alcaraz et al. [125] | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| ChargePoint [126] | ✓ | | | ✓ | | ✓ | | ✓ | | ✓ |
| Kaspersky [127] | ✓ | | | ✓ | ✓ | ✓ | | ✓ | | |

## A. INTERNAL VULNERABILITIES

EVCS internal processors communicate via a LAN typically using the RS232 protocol. The vulnerability analysis and penetration testing carried out by the Idaho National Laboratory on L2 EVCSs has revealed several hardware and software flaws [128], [129]: (i) EVCS processors running under a legacy Linux-based kernel with weak passwords and hashing algorithms, ii) a weak access control with unnecessary processes gaining root user privileges, iii) an unsigned firmware update process, and iv) an easy extraction of the firmware using the Joint Test Action Group and USB sticks, and reloading the tampered firmware. Moreover, the OCPP makes it possible for an EVCS to authenticate and authorize EVs by itself when it loses communication with its server, which forces EVCS to store and process authentication database locally. These vulnerabilities let an attacker gain full control of the EVCS, thus acquiring information of locally charged EVs in the past. Similarly, the study carried out by Positive Technologies has revealed vulnerabilities in EVCSs manufactured by Schneider Electric caused by hard-coded login credentials, remote code injections, and SQL injections [7]. These vulnerabilities would also enable an attacker to gain unauthorized access privileges and launch cyberattacks on EVCSs including data tampering, information disclosure, and DoS. Notably, Schneider Electric has addressed these vulnerabilities by disseminating security updates and increasing user awareness about the need for strengthening login credentials. Similarly, vulnerabilities in web-based and smartphone EVCS applications (e.g., CirCarLife) have been reported, which would allow an attacker to acquire login credentials stored in plain text, and thus, bypass the EV authentication [9].

## B. EVCS-X VULNERABILITIES

### 1) X={On-Site HMI} Vulnerabilities

Public EVCSs naturally have lower resistance to physical tampering. Serial, USB and ethernet ports, as well as magnetic card readers and touchscreens are mounted outside of the EVCS casing, which make them accessible for physical intrusions. The USB ports are convenient access points for cyberattacks that make it possible to copy a current EVCS configuration, modify or erase the data stored in the EVCS, and even access the EVCS server authentication credentials and identifiers of the EVs that previously charged [11], [127], [128]. Moreover, attackers could modify copied data and re-upload it to the EVCS as an updated firmware. Attackers can remotely skim magnetic card readers used for payments, similar to attacks in gas stations [130].

RFID cards and QR codes are used in public EVCSs for authenticating the EV users. The cards are authenticated at the beginning and end of each EV charging session. Phishing a RFID card reader installed at the EVCS allows to eavesdrop and gather login credentials [12]. The attackers can duplicate the EV user login credentials stored in the RFID card, allowing the attackers to imitate EV charging [127]. Unauthorized charging may remain stealthy for a prolonged period as the EVCSs bill their users typically on a monthly cycle.

### 2) X={EVCS Servers} Vulnerabilities

Although communications between distributed EVCSs and the EVCS server are not standardized worldwide, the OCPP is recognized by many EVCS vendors. This protocol is based on a client/server architecture, where both parties can request a communication session. This protocol, however, is vulnerable to man-in-the-middle cyberattacks on data privacy, message authenticity, message integrity, and non-repudiation due to a lack of server/client certificates and end-to-end message encryption [123], [124]. The vulnerabilities allow for stealing, altering, and spoofing EV charging data, e.g., unique EV and EVCS identifiers and charging settings [125]. The most recent OCPP release (OCPP 2.0.1, April 2020) enhanced the security of this protocol with authentication, client-side certification, firmware updates, and security notifications. Although a much needed effort to improve EVCS cybersecurity, there is no detailed security assessment of this release reported in public sources.

### 3) X={Smartphone} Vulnerabilities

Smartphone and web-based applications are indispensable to EV charging at commercial EVCSs, and there is a growing number of such applications distributed by EVCS operators and third-party EVCS aggregators [16]. These applications are used for locating public EVCSs, authenticating EVs at EVCSs for charging, remotely controlling charging sessions, and paying for the charge. Malicious smartphone applications or unintended and undiscovered bugs can be hazardous to the EV charging, and hence, can be exploited as a portal to disseminate worms in EVs and EVCSs. For instance, Kaspersky Lab has revealed vulnerabilities in the smartphone application developed by ChargePoint Home [126], which allow for imitating a user, bypassing user authentication, and tampering with EV charging data and charge settings. Such attacks could potentially damage both the EVCSs and connected EVs.

### 4) X={BEMS-Power Grid Interface}Vulnerabilities

Direct communications between an EVCS and an utility is mostly standardized via protocols such as the OpenADR protocol, which uses data encryption and digital signature via a WAN. Similarly, the utilities and DR aggregators also use the OpenADR protocol to communicate with a BEMS via a WAN. However, the EVCS-BEMS and DR aggregator-{X= BEMS, EVCS} communication is proprietary. The BEMS coordinates EVCS operation with various in-building smart appliances and sensors such as television, HVAC appliances, and security cameras via WiFi, ZigBee, or WiMaX. Because of a lack of industry-grade cybersecurity practices at customer-end, the likelihood of an attacker infiltrating the BEMS via connected smart appliances increases. For instance, 2016 Mirai botnet exploited over 600,000 smart home appliances with factory-set default login credentials [131]. Remote control of smart home appliances via smartphone applications, and diverse supply chains of the appliances and applications can be used as attack access points to the BEMS.

### 5) X={OEMs/Vendors} Vulnerabilities

Delivering security patches and software updates to EVCSs wirelessly is subject to similar vulnerabilities as EVs as reported in [11], [12] and discussed in Section V-B6. EVCS supply chains, communication channels used for the software update, and internal networks of an EVCS can be exploited to compromise the software updates and security patches.

## VII. POWER GRID THREAT MODEL

Attackers can exploit physical and wireless vulnerabilities in EVs, EVCSs, or both to affect the EV charging process, with the intent of harming the power grid stability. Table 2 summarizes the literature on attack/defense exploiting vulnerabilities in EVs and EVCSs. The attack/defense literature is categorized based on a STRIDE threat model discussed in Section II-A. Benefited by these classes of threats, an attacker can find multiple vulnerable avenues to hit its target. Therefore, it is common in the cybersecurity community to use threat modeling to identify and analyze such attack paths, which helps in developing an appropriate defense. Exploiting the vulnerabilities reported in Sections V and VI, Fig. 5 presents an attack tree for a power grid threat due to two types of cyberattacks in EV charging at public EVCSs: i) DoS of EVCSs and ii) EVCSs data tampering. The root node of the tree, the goal of the attack, is to create an over/under -frequency or over/under-voltage instability event in the power grid that would trigger protection relays and potentially disconnect bulk generators or substation equipment, leading to a cascade of failures [132]. For example, over-frequency relays at the distribution substation trip, which may cause a regional blackout, if the resulting frequency excursion exceeds limits prescribed by the IEEE 1547 standard.

In case of the DoS attack, the goal of the attacker is to suddenly shut down the EVCS operation, i.e., to stop charging all connected EVs, thus significantly reducing the power grid demand and causing over frequency excursion. To do so, two intermediate nodes with a logical "OR" relationship (see Fig. 5) are realized: the attacker needs to form an EVCS botnet or compromise an EVCS server. In turn, the botnet is succeeded by two logical "OR" leaf nodes pertaining to a transmission of malware to EVCSs either by means of infected EVs or a direct malware injection into EVCSs. Since there are multiple EVCS operators and service providers, the attacker needs to identify appropriate EVCS networks and their peak operating time in order to compromise a sufficient number of EVCSs to create an over-frequency event after their shutdown. Notably, there are various EVCS networks, smartphone applications, and fleets in a presumably attacked power grid area. For a successful attack on the power grid, the attacker needs to find out EVCS network(s), smartphone application(s), and fleet(s) with enough coverage of EVCSs and EVs, termed as *impactful* EVCS and fleet networks and smartphone applications.

On the other hand, in case of the tampering attack, EVCS usage data disseminated to EVs via smartphone applications is modified. For instance, EVCSs are shown unavailable or a higher charging price is broadcasted during their peak occupancy hours so that EVs are routed to EVCSs where their demand would cause an additional stress to the power grid. By doing so, the attacker intends to overload equipment in a chosen part of the grid, with presumably reduced security margins, thus either causing additional power losses or violating voltage constraints. Such overloads may also trigger relay protection leading to cascading failures. Tampering with EVCS data can be accomplished by compromising EVCS servers, fleet servers, or EV charging smartphone applications. These three intermediate nodes are preceded by three "OR" leaf nodes, pertaining to their *impactful* networks or applications, in Fig. 5.

While the attacks are actionable and can be implemented in practice, e.g., [16], they are not unique. Potentially, attackers can explore a combination of known and unknown vulnerabilities to pursue the same attack goals. Regardless of the chosen attack strategy, the most impactful way of damaging

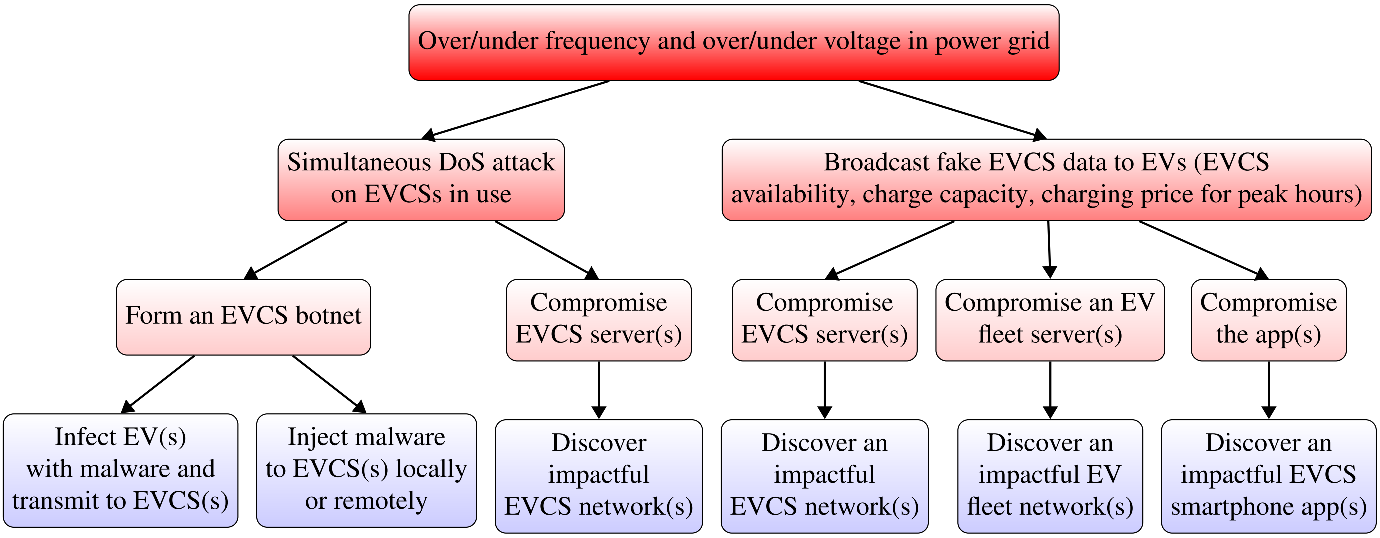
Over/under frequency and over/under voltage in power grid
Simultaneous DoS attack on EVCSs in use
Broadcast fake EVCS data to EVs (EVCS availability, charge capacity, charging price for peak hours)
Form an EVCS botnet
Compromise EVCS server(s)
Compromise EVCS server(s)
Compromise an EV fleet server(s)
Compromise the app(s)
Infect EV(s) with malware and transmit to EVCS(s)
Inject malware to EVCS(s) locally or remotely
Discover impactful EVCS network(s)
Discover an impactful EVCS network(s)
Discover an impactful EV fleet network(s)
Discover an impactful EVCS smartphone app(s)

**FIGURE 5.** An cyberattack tree for over/under-frequency and over/under-voltage events in the power grid by means of exploiting EV and EVCS vulnerabilities.

the power grid is to create an under/over frequency/voltage event, and trigger protection relays. Section VIII has an analysis of such attacks and their impacts on the power grid.

## VIII. POWER GRID IMPACTS OF CYBERATTACKS ON SMART EV CHARGING

Unlike the damage to individual EVs and EVCSs that the cyberattacks described above can cause, power grid implications of cyberattacks on EV charging are relatively underexplored and pose greater socioeconomic risks. As discussed in Section II-B5, cyber manipulations with IoT-connected high-power electric power loads to damage the power grid fall under the so-called demand-side cyberattacks [32]–[38]. However, these studies generalize demand-side cyberattacks on the power grid via high-power appliances without considering the nuances and complexity of the attack vectors such as EVs and EVCSs.

Table 3 summarizes the studies dedicated to impact-driven analysis of demand-side cyberattacks on the power grid that exploit vulnerabilities in EVs and EVCSs. Acharya et al. [16] developed a data-driven attack mechanism on the power grid that causes frequency instability by manipulating EVCS demand. Notably, the proposed attack design benefited from publicly accessible EVCS and power grid data that allowed for a prior evaluation of the worst-case attack impact on the power grid. As a proof-of-concept, [16] acquired public data on all commercial L2 and L3 EVCSs located in Manhattan, NY via smartphone applications and acquired public data on the power grid in Manhattan, NY by canvassing reports and technical documents released by the local electric power utility, authorities, as well as their affiliates. The impact-driven analysis of the attack on the power grid demonstrated that one needs to compromise at most the demand comparable to ∼1,000 EVs charging at 350 kW EVCSs to trigger over-frequency relay protection, leading to major power outages. Furthermore, it is noteworthy that suitability of compromising the calculated amount of EVCSs demand can be analyzed from publicly available EV charging profiles and power grid operational schedules (e.g., peak hours).

**TABLE 3.** Effects on the power grid due to cyberattacks on EV charging.

| Study | Threat | Effect |
|---|---|---|
| Acharya et al. [16] | Public data on EVCSs and power grid | Small signal instability, over-frequency causing cascading blackouts |
| Rohde [39] | EVCS control system | Low power factor, inoperable harmonic distortion, over-frequency |
| Khan et al. [40] | EV botnet | Under-voltage; line over load |
| Morrison [41] | EV botnet | Under-frequency events; power outages |

Rohde [39] demonstrated the impact on power quality due to a cyberattack on the EVCS control system. The cyberattack interrupted the coordination among power converters and power conditioning units of a 50kW DC EVCS. As a result, the EVCS suffered from an unacceptable total harmonic distortions in the EVCS current fed by the power grid ($> 20\%$) and a relatively low power factor ($< 0.8$). The incurred total harmonic distortion was far off from the limits prescribed by the IEEE-519 Standard [133], which restrict such distortions to be below $8\%$ for voltage levels up to 1 kV as measured at the coupling point between the EVCS and the power grid. Thus, if scaled to a sufficient number of EVCS, this attack could cause an over-frequency event in grid and lead to the same consequences as in [16].

Khan et al. [40] analyzed power grid impacts of the EV botnet cyberattacks seeking to stress voltage levels and power flows in the power grid, under the assumption of an omniscient attacker. Although the study was carried out 33- and 39-bus IEEE distribution and transmission networks, which are artificial test systems, it used real-life EV mobility and charging data obtained from the Toronto Parking Authority, Canada. Simulation results in [40] demonstrated that the EV botnet, when directed to certain L3 EVCSs, can create under-voltage events and power outages in some parts of these networks. Similarly, Morrison [41] conservatively analyzed parameters of the botnet, which consists of 7 kW residential L2 EVCSs, to create under-frequency outages in California region, which is a part of Western interconnection of the US power grid. The outcome of this study is that this botnet will need to simultaneously shutdown 12% EVs in California to cause a frequency drop of 0.5 Hz, which is sufficient for triggering under-frequency alarms in the western interconnection. An interconnection frequency response obligation [134], a statistical index for a minimum MW/0.1 Hz frequency response required to restore the normal operation during a loss of generator in a particular power grid, and an approximated population of EV users are used to calculate parameters of the EVCS botnet.

## IX. CONCLUSION

This paper reviews cyber-physical vulnerabilities arising at the nexus of the EVs, the EVCSs, and the power grid. While current cybersecurity protocols are diverse, often ad-hoc and with case- and location-specific nuances of operation, this study generalizes a cyber-physical outlook of this nexus. The paper presents vulnerabilities, both existing and emerging, in EV/EVCS cyber assets and components, and in communication interfaces demonstrating a demand-side attack vector on power grids. It describes a credible threat model (using an attack tree) that summarizes the attack strategies to cause voltage and frequency instability in the power grid leading to cascading failures. The analysis points to necessary R&D actions needed to secure this cyber-physical nexus:

- Standardizing and unifying protocols for EV charging is of foremost priority, while internalizing cybersecurity concerns on a par with physical security.
- Protocols must recognize the restrictions and peculiarities of the multi-party cyber environment of smart EV charging, which includes EV drivers, EVCS operators and aggregators, and power grid utility that have different cost, security, and privacy preferences.
- While the adoption of new EVs and the roll-out of new EVCSs, both with enhanced cybersecurity defense and capabilities, continues, it is important to upgrade and secure legacy vehicles and their components.
- Recognizing the risk of emerging and zero-day attacks, develop technological means of resiliency- and interoperability-by-design for future EVs and EVCSs to prevent wide-spread malware propagation and impacts on normal operations.
- Increase cybersecurity awareness among EV drivers and EVCS personnel to prepare for zero-day cyber accidents, with the primary focus on identifying, isolating, and recovering from cyberattacks.

## REFERENCES

[1] (2020) Global EV outlook 2020. [Online]. Available: https://webstore.iea.org/download/direct/3007?fileName=Global_EV_Outlook_2020.pdf

[2] (2019) Innovation outlook: Smart charging for electric vehicles. [Online]. Available: https://www.irena.org/publications/2019/May/Innovation-Outlook-Smart-Charging

[3] T. Capuder, D. M. Sprčić, D. Zoričić, and H. Pandžić, "Review of challenges and assessment of electric vehicles integration policy goals: Integrated risk analysis approach," International Journal of Electrical Power & Energy Systems, vol. 119, p. 105894, 2020.

[4] The power of 350 kw. [Online]. Available: https://ionity.eu/en/design-and-tech.html

[5] Find charging fast. [Online]. Available: https://www.electrifyamerica.com

[6] (2018) Remotely controlled EV home chargers-the threats and vulnerabilities. [Online]. Available: https://securelist.com/remotely-controlled-ev-home-chargers-the-threats-and-vulnerabilities/89251/

[7] (2018) Schneider electric EVLink parking. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSA-19-031-01

[8] EV charging solutions for every market segment. [Online]. Available: https://circontrol.com

[9] (2019) Circontrol CirCarLife. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSA-18-305-03

[10] ENCS, "EV charging systems security requirements," 2017. [Online]. Available: https://encs.eu/documents/

[11] K. Harnett, B. Harris, D. Chin, G. Watson et al., "DoE/DHS/DoT volpe technical meeting on electric vehicle and charging station cybersecurity report," John A. Volpe National Transportation Systems Center (US), Tech. Rep., 2018.

[12] S. Lightman and T. Brewer, "Symposium on federally funded research on cybersecurity of electric vehicle supply equipment (evse)," National Institute of Standards and Technology, Tech. Rep., 2020.

[13] U.S. Department of Transport, "Government fleet and public sector electric vehicle supply equipment (EVSE) cybersecurity best practices and procurement language report," 2019. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/43606

[14] (2019) Extreme fast charging (XFC) cybersecurity threats, use cases and requirements. [Online]. Available: https://github.com/nmfta-repo/nmfta-hvcs-xfc/find/master

[15] H. Mai, "Retail energy suppliers, others reject New York utilities' proposed cybersecurity protocols," 2019, May 1. [Online]. Available: https://www.utilitydive.com

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

[17] D. Kothari and I. Nagrath, Power System Engineering, 3e. McGraw-Hill Education, 2019.

[18] Uncover Security Design Flaws Using The STRIDE Approach. [Online]. Available: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[19] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, 2016.

[20] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on scada control system," in IEEE PES General Meeting, 2010, pp. 1–6.

[21] OpenADR. [Online]. Available: https://www.openadr.org

[22] (2020) Smart Meters – A proof of concept: hacking a smart meter. [Online]. Available: https://www.tarlogic.com/en/blog/smart-meters-a-proof-of-concept-hacking-a-smart-meter/

[23] D. Lee, H. Kim, K. Kim, and P. D. Yoo, "Simulated attack on dnp3 protocol in scada system," in Proceedings of the 31th Symposium on Cryptography and Information Security, Kagoshima, Japan, 2014, pp. 21–24.

[24] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," International Journal of Critical Infrastructure Protection, vol. 5, no. 3-4, pp. 146–153, 2012.

[25] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2871–2881, 2018.

[26] M. Seijo Simó et al., "Cybersecurity vulnerability analysis of the PLC PRIME standard," Security and Commun. Netw., vol. 2017, 2017.

[27] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in Proceedings of the International Conference on Information and Knowledge Engineering (IKE). The Steering Committee of The World Congress in Computer Science, Computer . . . , 2012, p. 1.

[28] F. M. Tabrizi and K. Pattabiraman, "A model for security analysis of smart meters," in IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012). IEEE, 2012, pp. 1–6.

[29] S. Kumar, H. Kumar, and G. R. Gunnam, "Security integrity of data collection from smart electric meter under a cyber attack," in 2019 2nd International Conference on Data Intelligence and Security (ICDIS). IEEE, 2019, pp. 9–13.

[30] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, "False load attack to smart meters by synchronously switching power circuits," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2641–2649, 2018.

[31] A. AlMajali, A. Viswanathan, and C. Neuman, "Analyzing resiliency of the smart grid communication architectures under cyber attack." in CSET, 2012.

[32] G. Raman, J. C.-H. Peng, and T. Rahwan, "Manipulating residents' behavior to attack the urban power distribution system," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5575–5587, 2019.

[33] E. Ustundag Soykan and M. Bagriyanik, "The effect of smishing attack on security of demand response programs," Energies, vol. 13, no. 17, p. 4542, 2020.

[34] H. S. Karimi, K. Jhala, and B. Natarajan, "Impact of real-time pricing attack on demand dynamics in smart distribution systems," in 2018 North American Power Symposium (NAPS). IEEE, 2018, pp. 1–6.

[35] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 15–32.

[36] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in 28th USENIX Security Symposium (USENIX Security 19), 2019, pp. 1115–1132.

[37] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in 2017 North American Power Symposium (NAPS). IEEE, 2017, pp. 1–6.

[38] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2862–2872, 2016.

[39] K. W. Rohde, "Cyber security of dc fast charging: Potential impacts to the electric grid," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2019.

[40] O. G. M. Khan, E. El-Saadany, A. Youssef, and M. Shaaban, "Impact of electric vehicles botnets on the power grid," in 2019 IEEE Electrical Power and Energy Conference (EPEC). IEEE, 2019, pp. 1–5.

[41] G. S. Morrison, "Threats and mitigation of ddos cyberattacks against the us power grid via EV charging," 2018.

[42] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "Scada security in the light of cyber-warfare," Computers & Security, vol. 31, no. 4, pp. 418–436, 2012.

[43] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in 2011 IEEE wireless communications and networking conference. IEEE, 2011, pp. 909–914.

[44] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," IEEE Transactions on Smart grid, vol. 2, no. 4, pp. 675–685, 2011.

[45] M. Nabeel, X. Ding, S.-H. Seo, and E. Bertino, "Scalable end-to-end security for advanced metering infrastructures," Information Systems, vol. 53, pp. 213–223, 2015.

[46] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," IEEE Internet of Things Journal, 2020.

[47] H. ElHusseini, C. Assi, B. Moussa, R. Attallah, and A. Ghrayeb, "Blockchain, ai and smart grids: The three musketeers to a decentralized EV charging infrastructure," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 24–29, 2020.

[48] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4601–4613, 2018.

[49] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in 2017 Resilience Week (RWS). IEEE, 2017, pp. 18–23.

[50] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in v2g environment," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2019, pp. 1–6.

[51] Top Five Blockchain Security Issues in 2019. [Online]. Available: https://ledgerops.com/blog/2019-03-28-top-five-blockchain-security-issues-in-2019/

[52] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

[53] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," Journal of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 468–483, 2018.

[54] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: A review," Current Sustainable/Renewable Energy Reports, vol. 5, no. 1, pp. 14–22, 2018.

[55] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981–997, 2012.

[56] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, p. 107094, 2020.

[57] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," Computers & Electrical Engineering, vol. 67, pp. 469–482, 2018.

[58] D. W. Gao, C. Mi, and A. Emadi, "Modeling and simulation of electric and hybrid vehicles," Proceedings of the IEEE, vol. 95, no. 4, pp. 729–745, 2007.

[59] Introduction to EV charging stations. [Online]. Available: https://training.ti.com/introduction-ev-charging-stations-piles

[60] Electric-drive vehicles. [Online]. Available: https://afdc.energy.gov/files/u/publication/electric_vehicles.pdf

[61] S. Manzetti and F. Mariasiu, "Electric vehicle battery technologies: From present state to future systems," Renewable and Sustainable Energy Reviews, vol. 51, pp. 1004–1012, 2015.

[62] K. Young, C. Wang, K. Strunz et al., "Electric vehicle battery technologies," in Electric vehicle integration into modern power networks. Springer, 2013, pp. 15–56.

[63] Batteries for hybrid and plug-in electric vehicles. [Online]. Available: https://afdc.energy.gov/vehicles/electric_batteries.html

[64] M. Ehsani, Y. Gao, S. Longo, and K. Ebrahimi, Modern electric, hybrid electric, and fuel cell vehicles. CRC press, 2018.

[65] Z.-G. Electrical, E. M. Association et al., "Voltage classes for electric mobility," Frankfurt am Main, Germany, 2013.

[66] J. A. Baxter, D. A. Merced, D. J. Costinett, L. M. Tolbert, and B. Ozpineci, "Review of electrical architectures and power requirements for automated vehicles," in 2018 IEEE Transportation Electrification Conference and Expo (ITEC). IEEE, 2018, pp. 944–949.

[67] EV auxiliary systems impacts. [Online]. Available: https://avt.inl.gov/sites/default/files/pdf/fsev/auxiliary.pdf

[68] J. J. Meyer, J. Lustbader, N. Agathocleous, A. Vespa, J. Rugh, and G. Titov, "Range extension opportunities while heating a battery electric vehicle," SAE Technical Paper, Tech. Rep., 2018.

[69] Benefits of ECU Consolidation. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/ecu-consolidation-white-paper.pdf

[70] Mercedes and Nvidia Announce the Advent of the Software-Defined Car. [Online]. Available: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/mercedes-and-nvidia-announce-the-advent-of-the-softwaredefined-car

[71] E. O. M. Size, "Share & trends analysis report by application (cleaning & home, medical, food & beverages, spa & relaxation), by product, by sales channel, and segment forecasts, 2019-2025," Report ID, pp. 978–1, 2019.

[72] J. Deng, L. Yu, Y. Fu, O. Hambolu, and R. R. Brooks, "Security and data privacy of modern automobiles," in Data Analytics for Intelligent Transportation Systems. Elsevier, 2017, pp. 131–163.

[73] H. Kitayama, S. Munetoh, K. Ohnishi, N. Uramoto, and Y. Watanabe, "Advanced security and privacy in connected vehicles," IBM Journal of Research and Development, vol. 58, no. 1, pp. 7–1, 2014.

[74] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in Workshop on Embedded Security in Cars. Bochum, 2004, pp. 1–13.

[75] W. Zeng, M. A. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1552–1571, 2016.

[76] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," IEEE Network, vol. 31, no. 5, pp. 50–58, 2017.

[77] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., "Experimental security analysis of a modern automobile," in 2010 IEEE Symposium on Security and Privacy. IEEE, 2010, pp. 447–462.

[78] CAN bus explained-a simplified intro. [Online]. Available: https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en#CAN-Bus-Intro-Dummies-Basics

[79] I. Rouf, R. D. Miller, H. A. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study." in USENIX Security Symposium, vol. 10, 2010.

[80] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019, pp. 1–5.

[81] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," IEEE Transactions on intelligent transportation systems, vol. 16, no. 2, pp. 993–1006, 2014.

[82] A. K. Mandal, F. Panarotto, A. Cortesi, P. Ferrara, and F. Spoto, "Static analysis of android auto infotainment and on-board diagnostics ii apps," Software: Practice and Experience, vol. 49, no. 7, pp. 1131–1161, 2019.

[83] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—on the (in) security of automotive remote keyless entry systems," in 25th USENIX Security Symposium (USENIX Security 16), 2016.

[84] (2019) Securing software updates for automobiles. [Online]. Available: https://uptane.github.io/attacks.html

[85] E.ON and Nissan are launching new V2G trial project in the UK. [Online]. Available: https://insideevs.com/news/437785/eon-nissan-v2g-trial-project-uk/

[86] Vehicle2Grid. [Online]. Available: https://amsterdamsmartcity.com/projects/vehicle2grid

[87] X. Gong and J. Rangaraju, "Taking charge of electric vehicles-both in the vehicle and on the grid," Texas Instruments, Dallas, TX, USA, pp. 1–13, 2018.

[88] S. Chakraborty, H.-N. Vu, M. M. Hasan, D.-D. Tran, M. E. Baghdadi, and O. Hegazy, "DC-DC converter topologies for electric vehicles, plug-in hybrid electric vehicles and fast charging stations: State of the art and future trends," Energies, vol. 12, no. 8, p. 1569, 2019.

[89] M. Smith and J. Castellano, "Costs associated with non-residential electric vehicle supply equipment: Factors to consider in the implementation of electric vehicle charging stations," Tech. Rep., 2015.

[90] A. Nordlund, J. Jansson, and K. Westin, "Acceptability of electric vehicle aimed measures: Effects of norm activation, perceived justice and effectiveness," Transportation Research Part A: Policy and Practice, vol. 117, pp. 205–213, 2018.

[91] M. Nicholas, "Estimating electric vehicle charging infrastructure costs across major US metropolitan areas," URL: https://theicct.org/sites/default/files/publications/ICCT_EV_Charging_Cost_20190813.pdf, 2019.

[92] M. Muratori, E. Kontou, E. M. Elgqvist, D. S. Cutler, and J. D. Eichman, "Electricity cost for electric vehicle fast charging," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.

[93] O. Khan, S. Acharya, M. Al Hosani, and M. S. El Moursi, "Hill climbing power flow algorithm for hybrid DC/AC microgrids," IEEE Transactions on Power Electronics, vol. 33, no. 7, pp. 5532–5537, 2017.

[94] M. S. Rahman, M. Hossain, F. Rafi, and J. Lu, "EV charging in a commercial hybrid AC/DC microgrid: Configuration, control and impact analysis," in 2016 Australasian Universities Power Engineering Conference (AUPEC). IEEE, 2016, pp. 1–6.

[95] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids—part ii: A review of power architectures, applications, and standardization issues," IEEE transactions on power electronics, vol. 31, no. 5, pp. 3528–3549, 2015.

[96] Open charge alliance global platform for open protocols. [Online]. Available: https://www.openchargealliance.org

[97] A. Hoekstra, R. Bienert, A. Wargers, H. Singh, and P. Voskuilen, "Using openadr with ocpp," Montréal, Canada, 2016.

[98] NYC Taxi and Limousine Commission, "Take charge: A roadmap to electric New York city taxis," 2013. [Online]. Available: https://www1.nyc.gov/assets/tlc/downloads/pdf/electric_taxi_task_force_report_20131231.pdf

[99] R. Currie, "Hacking the can bus: Basic manipulation of a modern automobile through CAN bus reverse engineering," SANS Institute, 2017.

[100] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, "A car hacking experiment: When connectivity meets vulnerability," in 2015 IEEE Globecom Workshops (GC Wkshps). IEEE, 2015, pp. 1–6.

[101] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable: A story of telematic failures," in 9th USENIX Workshop on Offensive Technologies (WOOT 15), 2015.

[102] P. Waszecki, P. Mundhenk, S. Steinhorst, M. Lukasiewycz, R. Karri, and S. Chakraborty, "Automotive electrical and electronic architecture security via distributed in-vehicle traffic monitoring," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 11, pp. 1790–1803, 2017.

[103] National Instruments, "Controller area network (CAN) overview," 2019. [Online]. Available: http://www.ni.com/en-us/innovations/white-papers/06/controller-area-network--can--overview.html

[104] O. Avatefipour and H. Malik, "State-of-the-art survey on in-vehicle network communication (can-bus) security and vulnerabilities," arXiv preprint arXiv:1802.01725, 2018.

[105] S. Hartzell and C. Stubel, "Automobile can bus network security and vulnerabilities (2018)."

[106] T. Lin and L. Chen, "Common attacks against car infotainment systems," 2019.

[107] C. Smith, The car hacker's handbook: a guide for the penetration tester. No Starch Press, 2016.

[108] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., "Comprehensive experimental analyses of automotive attack surfaces." in USENIX Security Symposium, vol. 4. San Francisco, 2011, pp. 447–462.

[109] R. Baker and I. Martinovic, "Losing the car keys: Wireless PHY-layer insecurity in EV charging," in 28th USENIX Security Symposium (USENIX Security 19), 2019, pp. 407–424.

[110] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol ISO 15118," Computer Science-Research and Development, vol. 33, no. 1-2, pp. 3–12, 2018.

[111] D. Antonioli, N. O. Tippenhauer, and K. B. Rasmussen, "The {KNOB} is broken: Exploiting low entropy in the encryption key negotiation of bluetooth br/edr," in 28th USENIX Security Symposium (USENIX Security 19), 2019, pp. 1047–1061.

[112] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, vol. 2015, p. 91, 2015.

[113] S. Mazloom, M. Rezaeirad, A. Hunter, and D. McCoy, "A security analysis of an in-vehicle infotainment and app platform," in 10th USENIX Workshop on Offensive Technologies (WOOT 16), 2016.

[114] Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions," IEEE Wireless Communications, vol. 25, no. 6, pp. 113–119, 2018.

[115] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," Proceedings of the IEEE, vol. 108, no. 2, pp. 357–372, 2019.

[116] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems," in 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 1527–1544.

[117] E. Fernandes, B. Crispo, and M. Conti, "Fm 99.9, radio virus: Exploiting fm radio broadcasts for malware deployment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 1027–1037, 2013.

[118] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," Computer Communications, vol. 44, pp. 1–13, 2014.

[119] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018, pp. 1–6.

[120] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in vanets: Communication, applications and challenges," Vehicular Communications, vol. 19, p. 100179, 2019.

[121] T. K. Kuppusamy, L. A. DeLong, and J. Cappos, "Uptane: Security and customizability of software updates for vehicles," ieee vehicular technology magazine, vol. 13, no. 1, pp. 66–73, 2018.

[122] T. Karthik, A. Brown, S. Awwad, D. McCoy, R. Bielawski, C. Mott, S. Lauzon, A. Weimerskirch, and J. Cappos, "Uptane: Securing software updates for automobiles," in International Conference on Embedded Security in Car, 2016, pp. 1–11.

[123] P. Van Aubel, E. Poll, and J. Rijneveld, "Non-repudiation and end-to-end security for electric-vehicle charging," in 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). IEEE, 2019, pp. 1–5.

[124] 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.

[125] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2452–2459, 2017.

[126] (2018) Chargepoint home security research. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/13084354/ChargePoint-Home-security-research_final.pdf

[127] (2018) Don't be sure charging your electric car is secure enough. [Online]. Available: https://www.kaspersky.com/blog/electric-cars-charging-problems/20652/

[128] (2018) Cyber assessment report of level 2 AC powered electric vehicle supply equipment. [Online]. Available: https://avt.inl.gov/sites/default/files/pdf/reports/Level2EVSECyberReport.pdf

[129] (2018) EV charging: Mapping out the cyber security threats and solutions for grids and charging infrastructure. [Online]. Available: https://www.smartgrid-forums.com/wp-content/uploads/2018/06/EV-Charging-Mapping-out-the-Cyber-security-threats-and-solutions-for-grids-and-charging-infrastructure-Chistian-Hill-.pdf

[130] N. Bhaskar, M. Bland, K. Levchenko, and A. Schulman, "Please pay inside: Evaluating bluetooth-based detection of gas pump skimmers," in 28th USENIX Security Symposium (USENIX Security 19), 2019, pp. 373–388.

[131] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, "Understanding the Mirai botnet," in 26th USENIX Security Symposium. USENIX Association, 2017, pp. 1093–1110.

[132] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, no. 2, p. 026103, 2007.

[133] "IEEE recommended practice and requirements for harmonic control in electric power systems," IEEE Std 519-2014 (Revision of IEEE Std 519-1992), pp. 1–29, 2014.

[134] (2019) 2019 Frequency Response Annual Analysis. [Online]. Available: https://www.nerc.com/comm/OC/Documents/2019%20FRAA%20Report%20Final.pdf

**Samrat Acharya** (Student Member, IEEE) received the B.E. degree in electrical and electronics engineering from Nepal Engineering College, Pokhara University, Nepal, in 2014, and the M.Sc. degree in electrical power engineering from the Masdar Institute of Science and Technology (collaborative program with MIT, USA), Abu Dhabi, UAE, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, New York University. His research interests include cyber–physical modeling and cybersecurity of smart grids, demand side management, and real-time simulation.

**Yury Dvorkin** (Member, IEEE) received the Ph.D. degree from the University of Washington, Seattle, WA, USA, in 2016. He is currently an Assistant Professor and the Goddard Faculty Fellow with the Department of Electrical and Computer Engineering, New York University, New York, NY, USA, with a joint appointment with the New York University's Center for Urban Science and Progress. His research interests include cyber–physical energy systems, environment, and economics. He was awarded the Scientific Achievement Award by Clean Energy Institute (University of Washington) for his doctoral dissertation in 2016, the NSF CAREER Award in 2019, and the Goddard Junior Faculty Award with New York University in 2019. He is an Associate Editor of the IEEE Transactions on Smart Grid.

**Hrvoje Pandžić** (Senior Member, IEEE) received the M.E.E. and Ph.D. degrees from the University of Zagreb Faculty of Electrical Engineering and Computing, Croatia, in 2007 and 2011, respectively. From 2012 to 2014, he was a Postdoctoral Researcher with the University of Washington, Seattle, WA, USA. He is currently an Associate Professor at the University of Zagreb Faculty of Electrical Engineering and Computing and Head of the Department of Energy and Power Systems. His research interests include planning, operation, control, and economics of power and energy systems. He has been an editor of the IEEE Transactions on Power Systems since 2019.

**Ramesh Karri** (Fellow, IEEE) received the B.E. degree in ECE from Andhra University and the Ph.D. degree in computer science and engineering from the University of California at San Diego, San Diego, CA, USA. He is a Professor of electrical and computer engineering with New York University, where he co-directs the Center for Cyber Security. He co-founded the Trust-Hub and organizes the Embedded Systems Challenge, the annual red team blue team event. He has published over 275 articles in leading journals and conference proceedings. His research and education activities in hardware cybersecurity include trustworthy integrated circuits, processors and cyber–physical systems, security-aware computer-aided design, test, verification, validation, and reliability, nano meets security, hardware security competitions, benchmarks and metrics, biochip security, and additive manufacturing security. His work in trustworthy hardware received best paper award nominations (ICCD 2015 and DFTS 2015), the Awards (ACM TODAES 2017, ITC 2014, CCS 2013, DFTS 2013, VLSI Design 2012, ACM Student Research Competition at DAC 2012, ICCAD 2013, DAC 2014, ACM Grand Finals 2013, and Kaspersky Challenge and Embedded Security Challenge). He received the Humboldt Fellowship and the National Science Foundation CAREER Award. He is a fellow of IEEE for his contributions to and leadership in Trustworthy Hardware. He is the Editor-in-Chief of the ACM Journal of Emerging Technologies in Computing. He served/s as an Associate Editor of the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, the ACM Journal of Emerging Computing Technologies, the ACM Transactions on Design Automation of Electronic Systems in 2014, IEEE Access, the IEEE Transactions on Emerging Technologies in Computing, IEEE Design and Test in 2015, and IEEE Embedded Systems Letters in 2016. He served as an IEEE Computer Society Distinguished Visitor from 2013 to 2015. He served on the Executive Committee of the IEEE/ACM Design Automation Conference leading the Security@DAC initiative from 2014 to 2017. He has given keynotes, talks, and tutorials on Hardware Security and Trust.