

# Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs

Alessandro Brighente, *Member, IEEE*, Mauro Conti, *Fellow, IEEE*, Denis Donadel,  
Raadha Poovendran, *Fellow, IEEE*, Federico Turrin, and Jianying Zhou, *Senior Member, IEEE*,

**Abstract**—Electric Vehicles (EVs) share common technologies with classical fossil-fueled cars, but they also employ novel technologies and components (e.g., Charging System and Battery Management System) that create an unexplored attack surface for malicious users. Although multiple contributions in the literature explored cybersecurity aspects of particular components of the EV ecosystem (e.g., charging infrastructure), there is still no contribution to the holistic cybersecurity of EVs and their related technologies from a cyber-physical system perspective.

In this paper, we provide the first in-depth study of the security and privacy threats associated with the EVs ecosystem. We analyze the threats associated with both the EV and the different charging solutions. Focusing on the Cyber-Physical Systems (CPS) paradigm, we provide a detailed analysis of all the processes that an attacker might exploit to affect the security and privacy of both drivers and the infrastructure. To address the highlighted threats, we present possible solutions that might be implemented. We also provide an overview of possible future directions to guarantee the security and privacy of the EVs ecosystem. Based on our analysis, we stress the need for EV-specific cybersecurity solutions.

**Index Terms**—Electric Vehicles, Cyber-Physical Systems, Security, Privacy

## I. INTRODUCTION

THE recent climate crisis demands green alternatives to replace technologies with high environmental impact. Among the others, fossil-fueled transportation is one of the significant causes of greenhouse gases. Electric Vehicles (EVs) have been proposed as a green alternative, where electric batteries are employed as a power source. During the last years, the number of people opting for the EV alternative increased up to the point where the market share of new EV sales reached more than 50% in countries such as Iceland (55.6%) and Norway (82.7%) [1]. The adoption of EVs is further expected to increase in the next years. In fact, governments are incentivizing the adoption of EVs thanks to the deployment of a large number of Electric Vehicle Supply Equipment (EVSE) in public charging infrastructures [2] and planning to ban sales of fossil-fueled vehicles [3]. Furthermore, technology advancements remove the current barriers against consumers’

A. Brighente, M. Conti, D. Donadel, and F. Turrin are with the Department of Mathematics and HIT Research Center, University of Padova, 35131 Padova, Italy (e-mail: alessandro.brighente@unipd.it; conti@math.unipd.it).

R. Poovendran is with the Department of Electrical and Computer Engineering, University of Washington, 98195 Seattle, USA.

J. Zhou is School of Information Systems Technology and Design, Singapore University of Technology and Design, 487372, Singapore. (email : jianying.zhou@sutd.edu.sg).

Manuscript received X X, 2022; revised X X, 2022.

adoption of EVs, providing extended driving range and seamless charging [4].

The increasing number of EVs demands a thorough analysis of the security of both vehicles and infrastructure operations. Like traditional vehicles, EVs are equipped with many Electronic Control Units (ECUs), sensors and actuators that measure, process, and control the different stimuli inside and outside the vehicle. However, EVs include additional components. Indeed, an EV integrates components to govern the hardware and software dedicated to managing electric energy smartly. These components are, for instance, the Battery Management System (BMS) and the charging system.

Different studies have already proven the impact of potential cybersecurity attacks on automotive systems. For instance, Miller and Valasek [5] proved the feasibility of hijacking a vehicle by remotely controlling it through the infotainment system. Furthermore, most existing vehicles exploit Controller Area Network (CAN) as in-vehicle network architecture, which has already been proved as non-secure [6] and, therefore, may be vulnerable to potential cyberattacks. Lastly, privacy shall also be guaranteed to prevent malicious users from obtaining sensitive information on the driver, such as her location or habits. It is essential to include security and privacy features by design to prevent these and other attacks. Researchers investigated vehicle security, focusing on the different aspects of in-car communications [7], [8]. However, EVs are equipped with specific components that provide fundamentally different attack surfaces and exploitation points. For instance, EVs are equipped with electric batteries to power the vehicle components ranging from the infotainment system to the acceleration pedal, together with systems to manage the electrical power as shown in Figure 1.

Therefore, analyzing the in-vehicle threats associated with these components is essential. Furthermore, the power supply must be regulated by dedicated hardware, not classical vehicles. Researchers discussed how the EV charging infrastructure could be exploited by attackers [9], however, neglecting the in-vehicle threats.

**Contribution.** In this paper, we examine the security and privacy issues of EVs from a Cyber-Physical System (CPS) point of view. Given the high demand for EVs and the increasing number of deployed charging facilities, it is fundamental to guarantee the security and privacy of both vehicles and users. Many literature contributions discuss solely technical aspects of the EV ecosystem without focusing on security issues. Other security-focused works study a single system component (e.g., the vehicle’s internal bus, the smart grid, or the

communication protocols) without comprehensively analyzing the whole environment. We provide a general overview of EV functioning, focusing on their core components to build the basic knowledge needed to analyze the possible threat vectors. We then discuss possible attacks and countermeasures specific for EV and underline the existing security solutions for fuel vehicles that are also effective in EVs. With the bird-eye on the CPS concept, we are not only able to discuss the issues related to the exchange of information between the different involved entities, but also the side channels that may leak sensitive information or that could lead to hazardous behavior impacting on users' safety. We hence shed light on the unresolved challenges of EVs ecosystems, providing interested researchers with possible directions worth investigating to guarantee the security and privacy of the overall EV ecosystem. We also consider future directions such as the Wireless Power Transfer (WPT) charging of EVs, which has only been developed on small-scale testbeds at the time of writing. We believe that delving into this emerging system's security and privacy issues will help future developers design and implement secure-by-design WPT solutions for EV.

We summarize the contribution of this work as follows.

- We examine the peculiar components that differentiate EVs from fossil-fueled vehicles and provide an overview of their role and how they exchange information.
- We provide an overview of the different technologies employed to charge electric vehicles, comprising both wired and wireless charging. We present the available standards for each of them and describe their basic functioning.
- We provide an in-depth discussion of the security and privacy issues of the EVs ecosystem. We analyze the threats related to the in-vehicle network and the threats related to the charging process. We particularly focus on their effects on the peculiar EV components and analyze them from a CPS point of view.
- We analyze and compare possible countermeasures proposed in the literature for each of the presented attacks, even grasping from other similar areas.
- We outline future directions for research in the EV cybersecurity domain.

**Organization.** The rest of the paper is organized as follows. In Section II, we review the related literature. In Section III, we describe the EV components the charging infrastructure. In Section IV, we then discuss the in-vehicle security and privacy threats, and those related to the charging infrastructure in Section V. Along with the threats, we also present possible countermeasures. Then, we discuss the possible future direction in Section VI, and lastly we conclude the paper in Section VII.

## II. RELATED LITERATURE ON EV SECURITY

Automotive cyber-security requires standardization to allow for security guarantees and interoperability. Schmittner et al. [7] reviewed the available standards, including designing and validation aspects. These standards, however, do not consider the peculiar features of EVs. Scalas et al. [8] provided

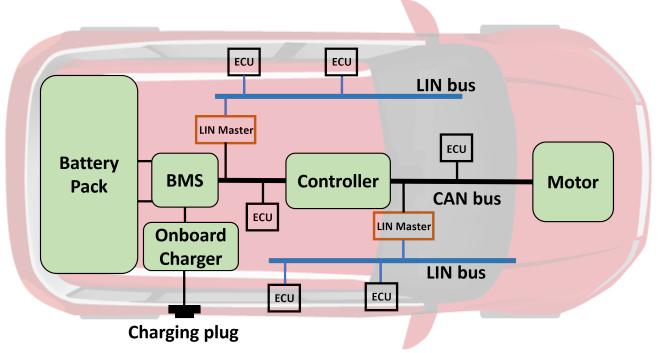


Fig. 1. Main components of an EV. Green components are EV specific.

an overview of the cybersecurity requirements for the future of the automotive industry, focusing on in-vehicle components. They discussed several technologies and attacks but were not specific for EVs. Furthermore, different works present technical reviews of the EV ecosystem [10], [11]. However, none of them consider the security aspects.

Some contributions in the literature focused on specific components of EVs. For instance, Khalid et al. [12] focus on the BMS, discussing the lack of a cybersecurity standard to guarantee its security and providing an overview of the possible standardization framework that could be adopted to achieve this goal. Chandwani et al. [13] presented an overview of the cybersecurity threats associated with the onboard charging system of EVs. Despite providing an accurate analysis of the security of this component, their contribution does not consider how these attacks can impact the other peculiar components of the EV. These contributions do not provide a general overview of the EV ecosystem. Furthermore, they do not discuss the threats associated with privacy. Acharya et al. [14] provide the first discussion on how EVs can be considered as CPS. The authors discuss how different attacks can be conducted inside the car and during communication with the power supplier. However, they do not consider the specific components of the EVs such as the BMS. Jin et al. [15] focus on the CPS system represented by the power electronics in EVs. However, they do not consider how these attacks may impact the other components of the EV and did not discuss the issues related to WPT. Most of the literature related to EVs' cybersecurity focus on the charging infrastructure and process. Gottumukkala et al. [9] provide an overview of the CPS threats associated with a wired EV charging infrastructure. Antoun et al. [16] discuss the security threats associated with the negotiation and actuation of a charging session investigating the communications between the multiple involved entities. They presented different charging scenarios, neglecting the WPT option.

Vehicles can be interconnected with one another to form the internet of vehicles. This is also feasible with EVs, which imposes additional security challenges. Frajji et al. [21] discuss the cybersecurity threats associated with the internet of electric vehicles, discussing the threats associated with the communication with the multiple involved entities being part

Reference	BMS	Onboard Charger	Battery Pack	Controller	Electric Motor	Wired Charging	Wireless Charging
Khalid et al. [12]	✓						
Chandwani et al. [13]		✓					
Acharya et al. [14]						✓	
Ye et al. [15]	✓			✓	✓	✓	
Sripad et al. [17]			✓				
Gottumukkala et al. [9]						✓	
Antoun et al. [16]						✓	
Garofalaki et al. [18]						✓	
Van Auben et al. [19]						✓	
Babu et al. [20]							✓
<b>Our paper</b>	✓	✓	✓	✓	✓	✓	✓

of the road infrastructure. The cybersecurity focus is on the communication links, therefore neglecting the impact of the peculiar EVs' components.

Garofalaki et al. [18] present a detailed survey on Open Charge Point Protocol (OCPP) and the corresponding threat and vulnerabilities on the Vehicle-to-Grid (V2G) ecosystem due to its adoption. Similarly [19] overview the main protocols for EV charging adopted in the Netherlands and analyze their security features, while Babu et al. [20] analyzed the security of the main protocols proposed for the EV environment with a particular focus on the payment methods and the authentication solutions. Differently from these works, instead of focusing on the protocols, we focus on the entire EV architecture, highlighting the main security and privacy challenges in this typology of CPS.

Table II compares the related works on EV security with our contribution. We can see that most of the contributions focus on vehicle-to-grid communications in the wired case. However, none of the available papers focus on intertwining the different cyber-physical aspects of EVs. Therefore, our paper provides a more complete analysis of the security and privacy challenges for EVs.

### III. ELECTRIC VEHICLES FROM A CYBER-PHYSICAL SYSTEM PERSPECTIVE

In this section, we analyze EVs from a CPS perspective. We emphasize those components that differentiate EVs from gas-fueled vehicles. In particular, we first describe the traditional vehicle architecture in Section III-A. Then, we present the main components of an EV in Section III-B, showing how it differs from traditional vehicles. Lastly, we provide an overview of the EV charging infrastructure in Section III-C.

#### A. Traditional Vehicle Architecture

Nowadays, vehicles contain dozens of different microcomputers, called Electronic Control Units (ECUs), running millions of lines of code [22]. Each ECU is responsible for controlling a mechanical (e.g., brakes) or electrical (e.g., light) component of a modern vehicle. Depending on the component it has to manage, an ECU generally employs a wide range of microcontrollers, from simple 8-bit RISC controllers to more complex 32-bit multicore processors. ECUs are typically implemented with ad-hoc firmware, even if complex ECUs may run complete operating systems: the infotainment system,

for instance, usually runs a Linux-based kernel. In order to provide more flexibility during updates, more advanced solutions envisage the implementation of multiple ECUs on a single FPGA board [23].

Communications among ECUs that reside in the vehicle pass through wires that connect multiple components. The two mostly implemented technologies are CAN and Local Interconnect Network (LIN). CAN represents the main network that allows for cost-effective wiring, self-diagnosis and error correction [24]. The CAN bus consists of two wires and implements a distributed architecture, where car modules (i.e., the ECUs) share messages upon winning a contention phase. However, CAN has been designed to be a reliable solution, neglecting possible security and privacy shortcomings.

The LIN bus is a supplement to CAN [25]. In particular, it connects a smaller number of ECUs (one master and up to 16 slave nodes) and offers a drastically cheaper implementation at the cost of lower performance and reliability. A LIN master node is typically a gateway to CAN, and multiple LIN buses can communicate via the CAN bus. The LIN bus can be used to control, among the others, sensors and actuators for steering wheels, comfort, powertrain, engine, air conditioning, doors, and seats.

Besides CAN and LIN, also other technologies such as FlexRay [26] and Media Oriented Systems Transport (MOST) [27] are currently used for automotive networks. To overcome some of these technologies' limitations and ease their interoperability, automotive Ethernet has recently been introduced as a possible solution [28]. Given the CPS nature of our investigation, we do not prefer one technology over another, as these all represent communication means for the exchange of information inside the EV. We refer the interested reader to [28] for a discussion on automotive Ethernet security.

Modern vehicles also include mechanisms to update the internal software. This service is generally implemented with the aid of external device plug (e.g., USB flash drive) or Over-the-Air (OTA) software update [29] (e.g., via Internet connection). Furthermore, many vehicles nowadays include complex entertainment systems, which may expand the vulnerable surface, exposing new connections (e.g., Bluetooth) and operating systems (e.g., Android).

### B. Electric Vehicle Specific Components

EVs share most of the architecture with fuel-based vehicles. However, they comprise a different set of hardware modules that manage how the vehicle generates power and how to generate motion. In particular, an EV comprises the following components [30], depicted in Figure 1.

**Battery.** The battery is where the charge is stored in the form of Direct Current (DC). It provides the power needed to operate the EV components. Batteries are usually combined in packs and connected in series or parallel to increase the voltage and Amper/hour they can deliver to the EV. Batteries suitably combined are enclosed into a metal casing to prevent damage. The case usually includes a cooling system to avoid damage due to batteries overheating.

**Battery Management System.** This module manages all operations regarding the battery. It manages the current output and the charging and discharging of the battery by keeping it in a safe operating area. Hence, it regulates the electricity flow through the battery. The BMS is unique for each EV model, and may be designed according to various topologies, i.e., modular, centralized or distributed [12]. The BMS monitors each battery in the pack and measures each cell's voltage, current, and temperature. It is instructed with a threshold limit for each of them and disconnects the load if values exceed the threshold value. Furthermore, the BMS measures the State of Charge (SoC) and state of health of the battery. The BMS communicates with the human-machine interface to report information on this information. All the information are exchanged via CAN or LIN bus.

**Battery Charger/Onboard Charger.** This component provides an interface between the charging system and the EV battery. As soon as an Alternate Current (AC) charging process begins, the charger converts the input voltage to DC and passes it to the battery for storage. For high power DC charging, the conversion phase is done on the charging column. Furthermore, it prevents possible damages to the battery or the supply system (e.g., overheating) by limiting the power flow [13].

**Controller.** The controller handles the flow of current from the battery to the EV associated with all operations, ranging from motors-related operations to powering the infotainment system. It receives the input from the driver to control the acceleration, brake pressure, and driving mode and converts the energy in the battery from DC to AC to control the EV accordingly. On the other hand, the EV may generate electricity due to, e.g., regenerative braking. In this case, the controller converts the generated AC to DC such that the energy can be stored in the battery.

**Electric Motor.** The motor is powered by the EV battery, which provides the electricity needed to turn it and move the EV. The electric motor communicates with sensors and actuators in the EV that control the amount of thrust required [31]. There exist many implementations of electric motors. The most commonly used for EVs are AC induction due to their lower cost implementation thanks to the absence of permanent magnets.

These components characterize an EV and differentiate it from other types of vehicles. In particular, the conventional

motor is replaced with an electric one, and a battery pack replaces the fuel tank. Notice that all the components mentioned above need to share messages inside and outside the vehicle to guarantee the correct functioning. An attacker might exploit some of these messages to create inconsistencies on the EV status or to cause damages to both the vehicle and driver. We provide a detailed security analysis based on these components in Section IV.

### C. Electric Vehicles Charging Infrastructure

The EV needs to charge its battery periodically to provide power to its components. To this aim, the EV shall be connected to a charging infrastructure with whom it negotiates a charging session. According to the negotiated session, the infrastructure then delivers the needed energy to the EV. Charging may happen either in public areas (e.g., shopping malls or offices) or at a private site (e.g., home). To prevent possible malfunctioning, the charging infrastructure must be carefully managed. This is particularly true when considering a scenario where handling a massive number of EVs may lead to blackout and other grid malfunctions [32].

Charging an EV differs from other devices, such as smartphones or laptops, as it requires dedicated hardware and a drastically larger energy supply. Indeed, if many EVs are concurrently charging, there can be grid overloading, leading to malfunctions and local blackouts. To avoid these issues, the grid must employ a communication channel with the EV to negotiate to charge parameters that respect the vehicle's battery requirements without overloading the grid. V2G refers to the technology enabling this communication type. There are two solutions to manage a charging session: wired and wireless. While the former is more diffused and widely implemented nowadays, the latter is still in the initial stage and under development. Unfortunately, there is no unique world standard to regulate this communication channel. Instead, different manufacturers implement different standards based on the technologies used for the charging process. For instance, CHAdeMO [33] (Japan) or GB/T [34] (China) can be used only with wired charging, while ISO 15118 (Europe, North America) also supports WPT [35], [36].

1) *Wired Charging:* With this setting, the EV is connected to an EVSE through a cable that transmits both the control signals ad the charging current. In turn, EVSEs negotiate with power grids for the energy needed to charge the vehicle, based on both EV and grid requirements. However, these basic functions are integrated by every charging standard, which employs different communication methods. Low current charging levels, such as AC Level 1 or AC Level 2, require a simple control channel which is generally provided by a Pulse-Width Modulation (PWM) communication. More advanced charging, such as DC charging, needs better management of the energy provided by a High-Level Communication (HLC) provided by protocols such as CAN or Power Line Communication (PLC). These technologies enable the development of additional services, such as the automatizing of the billing process [37], [38], or the download of firmware updates [39]. In case of a lack of automated authentication solutions, EVSE

may be equipped with RFID readers through which users can authenticate and pay for the service. EVSEs can be deployed at private or public premises: private charging columns are generally less advanced and support less charging level with respect to public EVSE.

There are mainly two protocols supporting the HLCs between EV and EVSE during DC charging sessions. The first one, employed by Combined Charging System (CCS), is the ISO 15118 [38], which modulates data over the control pilot pin using PLC. The second one, CHAdeMO [33] employs a CAN channel for the communication.

The physical connection between EV and EVSE may be implemented with different plugs according to different standards. In particular, we can classify EVSEs according to different levels. Figure 2 shows the different charger levels together with their lead characterization.

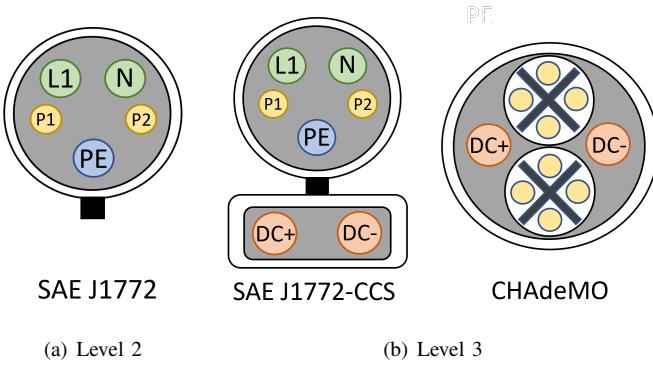


Fig. 2. Different types of EV chargers. L1 = AC line 1; N = AC line neutral, P1 and P2 = proximity lines, PE = ground.

Level 1 and Level 2 EVSEs exploit a five-leads connector implementing the SAE J1772 protocol [40], as shown in Figure 2(a). This connector exploits two leads to deliver the charging current, two leads for pilot signals, and one lead for ground (or protective earth). The two current leads plus the ground one are used by the EVSE for metering and computing the session cost. The two pilot lines have two different functions. The first one, the control pilot, is used to exchange information with the EV during the charging session. The signals exchanged through the control pilot either control the amount of current delivered to the EV [41] or are used to check the connection status and remove power from the adapter in case of disconnection to prevent the user injuries [9]. The second pilot line is the proximity pilot, used by the EV to check whether a proper physical connection has been established with the EVSE.

Level 3 EVSEs, i.e., those allowing for fast charging, are based on different implementations and are showed in Figure 2(b). The first is the CCS expansion of the SAE J1772, which allows for direct current exchange for fast charging. Furthermore, it implements PLC to exchange information between the EV, the EVSE, and the smart grid [40]. The second implementation is the Japanese CHAdeMO [42], which implements a fast charging protocol. Besides delivering power, this implementation allows for data exchange via the CAN bus protocol. Thanks to this type of connection, it is possible to

avoid applying power to the connector in case of a non-safe connection or to exchange information related to the battery SoC. Furthermore, CHAdeMO allows V2G communication, where the EV battery is later used as energy storage to provide service to the grid [33]. Other protocols exist, such as the proprietary protocol employed by Tesla vehicles and the Chinese GB/T, which will probably be replaced by Chaoji, an evolution of CHAdeMO [10].

The main differences between Level 3 and Level 2 chargers lie in the higher number of leads in Level 3, and in the implemented circuitry which converts AC to DC, which is inside the charging columns for Level 3, while it is onboard in the EV for Level 2. Furthermore, Level 3 charging includes richer communication capabilities thanks to the support of HLC.

**2) Wireless Power Transfer:** Charging via WPT allows charging an EV's battery without physically connecting the vehicle to the charging infrastructure. In WPT, a source (powered by the grid) generates a time-varying electromagnetic field that triggers the generation of a current at the receiver's (EV's) side. This current is generated thanks to a coil mounted on the EV's side that receives the transmitted electromagnetic field and, due to Faraday's law of induction, generates an AC [43].

Via WPT, it is possible to create multiple charging scenarios depending on the mobility of the EV [44]. In fact, thanks to the absence of a physical connection, EVs can be either charged while parked or while driving in a dynamic scenario [20]. The static scenario is similar to the one previously described in Section III-C1, where a user books a charging session and receives the power from the grid while parked at a charging facility. Instead, the dynamic case requires a suitably designed infrastructure composed of multiple sequential WPT transmitters. Figure 3 shows a pictorial representation of a dynamic WPT system for EVs. The street is equipped with multiple WPT transmitters deployed underneath the street. These transmitters are connected to the grid that provides the power needed to charge the EV.

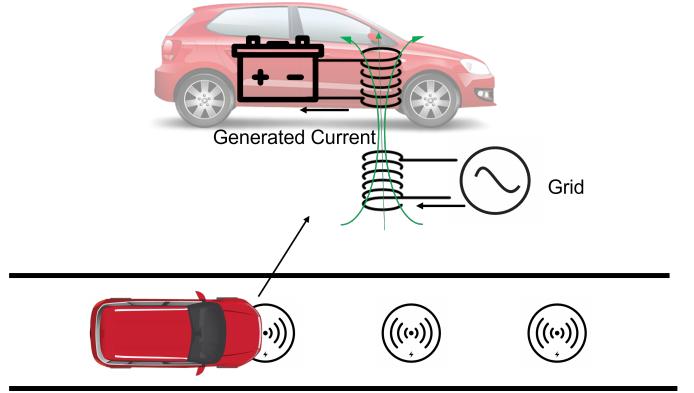


Fig. 3. Representation of a WPT system for EVs.

Dynamic WPT can be further divided into two categories: quasi-dynamic and fully-dynamic [45]. In the former case,

charging is limited to the cases where the EV is not moving, e.g., while waiting at stops or traffic lights. In fully-dynamic WPT, charging is continuously delivered to the EV as long as it drives near transmitting coils. In both dynamic scenarios, the challenge is to guarantee that transmitters are activated only when needed to avoid energy waste and that only legitimate users access the emitted power. In fact, due to the absence of a medium, users could steal power by driving close to an EV that paid for the charging session. We discuss all the security problems related to WPT in Section IV.

As specified in the ISO 15118 standard [35], the connection between the vehicle and the charging column during a static WPT scenario uses WiFi (IEEE 802.11). The vehicle can connect before being correctly parked or when it is already over the coil. If needed, the EVSE provides the EV with fine positioning messages to help the driver correctly place the vehicle to reduce energy dispersion. After establishing the connection, the two entities communicate similarly to wired cases. Some modifications are introduced to adapt to the wireless scenario, including the WPT charging mode and the fine positioning messages.

Due to their novelty, dynamic and quasi-dynamic charging are not yet covered by approved and widely adopted standards. Some research works [46] adopt Dedicated Short-Range Communications (DSRC) to create a channel between vehicles and the Road Side Units (RSUs), which are in charge of controlling a portion of the road coils.

Another possible solution can be to extend WPT to deliver also information along with power. In fact, Wireless Information and Power Transfer (WIPT) represents a technology that might be exploited for electric vehicle [47]. WIPT can be adopted to implement a system similar to that exploited in wired EV charging, where control signals are exchanged through the pilot line and the charging current. In WIPT, control signals can be coded into the time-varying electromagnetic field to deliver power and check the connection's status simultaneously. Furthermore, this solution can be exploited to authenticate EVs and solve part of the security challenges in WPT. Although not yet discussed in the literature, we believe that WIPT represents a suitable line of research for EV charging technologies.

#### IV. IN-VEHICLE SECURITY AND PRIVACY CHALLENGES

This section discusses the security and privacy challenges related to the components and protocols used inside EVs. First discuss in Section IV-A the challenges related to the battery and the BMS. Then, we discuss the challenges related to the controller and charger in Section IV-B. The security of CAN bus has been extensively studied in the literature, as it does not envision secure by design solutions [48]. However, how these attacks may impact EVs has never been studied. Since all in-vehicle messages are exchanged through CAN and LIN buses, we discuss how their vulnerabilities can be exploited to impact those components specific to the EVs. We summarize in Table IV the in-vehicle security and privacy challenges together with their effects, impact severeness, and possible countermeasures.

##### A. Battery and BMS

The battery pack is a sensitive component of an EV. In case of malfunctions, it may catch fire and even explode [49], [50]. Such situations can severely harm the passengers and create financial damage to the owner and a reputation loss to the manufacturer. Less severe cyberattacks can, however, create financial damage, for instance, by reducing the battery's lifespan, forcing the owner to a premature battery replacement [17].

The battery pack is managed by the BMS, which handles communication with the other ECUs via the vehicle bus. Again, this channel has been proven to be vulnerable to many cyberattacks [48], [24]. In the following, we discuss how cyberattacks impact EVs, extend their effects to the CPS domain, and highlight their effect on the battery and BMS.

*a) Denial of Service:* The BMS is responsible for reporting information on the battery status and managing the energy delivery. An attacker might flood the BMS controller by forging and sending a vast number of requests, in similar ways to what may happen with Denial of Service (DoS) attacks against websites [51]. An overload of the BMS may slow responses to legitimate requests or even prevent the BMS from sending response messages completely. This may lead to multiple effects depending on the information requested to the BMS and how the requester device reacts to the absence of a response. In fact, this might cause damage to the battery if power is not properly removed in case of abnormal behavior or physical tampering by the attacker. A DoS may target sensor measurements, such as temperature, and it may prevent the activation of cooling mechanisms, forcing the battery into critical temperatures, which may be irreversible [52]. Furthermore, this attack may also prevent the user from obtaining information on the amount of charge left, causing range anxiety and possibly jeopardizing the drivers' safety in case of a sudden EV stop.

Flow control might prevent the BMS from handling many fake requests. In this context, source authentication may provide information regarding the legitimacy of the sender [53]. A solution for flow control may be given by an adapted version of time-lock puzzles [54]. Furthermore, rate limiting can help mitigate against DoS attacks [55], while intrusion detection strategies can help in identifying the attack before it creates damage [56]. Redundancy on the controllers can also help in mitigating severe DoS attacks against the BMS [57].

*b) Tampering:* An attacker might physically tamper with the battery and the BMS. Depending on the specific tampered component, an attacker may be able to cause a short circuit that may lead to catastrophic events such as the start of a fire that might harm both the vehicle and the passenger. This consideration holds for battery and BMS, as they both manage high voltages. Tampering may also lead to less severe consequences, such as the BMS being unable to communicate with the battery or to deliver the full power to the battery during charging. These attacks may also include detaching or cutting cables.

As a possible countermeasure, the battery and BMS shall include an anomaly detection system to prevent applying a

TABLE I  
SUMMARY OF IN-VEHICLE CHALLENGES.

Component	Attack Type	Effect	Impact	Possible Solutions
Battery and BMS	DoS	Prevent energy delivery Prevent information reception Increase energy consumption Physically damage the battery	Medium	Flow control Time-lock puzzles Rate limiting Intrusion detection
	Tampering	Short circuit Prevent energy delivery	High	Anomaly detection Tamper-proof hardware
	Malicious Code Injection	Modify BMS response to command Collect sensitive information	Medium	Authentication Remote attestation Intrusion detection
	Spoofing, Replaying, and MitM	Report false information to the driver Report false information to the other ECUs Physically damage the battery Disrupt charging process Excessive discharging Overcharging	High	Identity management Authentication Intrusion detection Redundancy Timestamps Integrity protection
Controller and Charger	MitM	Report false information Isolate charger components Modify control signals Increase energy consumption	High	Anomaly detection Intrusion detection Intrusion prevention Integrity Protection
	DoS	Prevent the exchange of energy	Medium	Cookies Time-lock puzzles Rate limiting Intrusion detection
	Spoofing, and Replaying	Report false information Physical damage Increase energy consumption	High	Intrusion detection Identity management Timestamps
	Malicious Code Injection	Modify EV response to commands Collect sensitive information Remote control/hijack	High	Authentication Remote attestation Intrusion detection
	Tampering	Impair the charging process Power loss and overvoltage	High	Anomaly detection Tamper-proof hardware
	Eavesdropping, and Side Channels	Track the user Profile users' preferences	Low	Differential privacy Encryption

voltage to tampered components and causing the aforementioned damages [58]. Another solution may be the physical protection of these components with tamper-proof hardware. For instance, in case of physical tampering, the battery should be designed so that it cannot receive or deliver power [59]. The SAE J2464 standard contains safety measures that can also be effective against tampering [60].

c) *Malicious Code Injection:* The battery pack is managed by the BMS, which is a piece of hardware with firmware onboard. Attackers may try to reverse engineer the software to discover vulnerabilities and build exploit against them [61]. To patch bugs, EVs' software may be updated over the air or via the charging cable [39], thus easing the update process for manufacturers and users. However, this represents a security challenge, as software updates need to access the overall EV network [29]. A malicious user may inject malware via software update to gain control of the BMS [29]. By having partial or complete control over it, the attacker may thus impact the normal functioning of the vehicle. For instance,

the malware may prevent the BMS from requesting energy from the battery, causing a blackout in the EV. Contrarily, the BMS may be forced into requesting more energy than needed to speed up the discharging process. Furthermore, thanks to the malware, the attacker may measure other sensitive information of the driver, which may lead to privacy leakages.

To prevent code injection and its effects, access to the EV's internal network shall be strictly regulated. Possible solutions include the use of external source authentication. In case of a successful injection, it is fundamental to identify and mitigate its effect. To this aim, remote attestation and its collective extension may be used to validate the in-vehicle components [62]. Furthermore, anomaly and intrusion detection techniques may help identify attacks to the in-vehicle network [56]. Injection of malicious updates can be detected by integrity verification on the new software, possibly employing a blockchain [63].

d) *Spoofing, Replaying, and Man-in-the-Middle:* An attacker may spoof or modify messages to report to the driver

false information on the battery SoC, thus impairing a safe drive. The attacker may also report incorrect information to the charging infrastructure by impersonating the BMS or modifying information in the middle of the communication. This may cause the charging process to provoke damage to the battery or the EV circuitry. Furthermore, an attacker may report false information to prevent the correct exchange of energy from the battery to the BMS, for instance, by lowering the current demand and preventing the exchange of a sufficient amount of power from the battery to the EV. By requiring excessive power, an attacker can discharge the battery faster than expected in a battery exhaustion attack [64] or may force the battery to overcharge, leading to a massive shortening of the battery lifetime [17]. Finally, through Man-in-the-Middle (MitM), an attacker may modify the voltage values of the battery pack, leading to over-discharging and consequent battery degradation [65].

To prevent these attacks, the battery and BMS should be given an identity, and all messages shall provide source authentication and integrity protection. The cryptographic material shall be embedded in these devices, with examples in trusted platform modules [66] or physical unclonable functions [67], and shall not be disclosed during communications to prevent MitM attacks. An intrusion detection system can help in identifying ongoing attack [64]. Redundant controllers can be employed to enhance the resilience of the BMS against adversarial attacks during charging [57]. Kim et al. [68] proposed to employ blockchain to provide authentication and access control in the communication between the BMS and the other devices inside the EV. Strategies to mitigate the effect of an attacker who has gained direct access to the vehicle's bus have been proposed [48]. Some works have considered peculiar features of EV to detect spoofing attacks: Guo et al. [69] proposed a physically-guided machine learning method to detect replay and false data injection attacks on the bus. Their system, tested in a Hardware-In-the-Loop (HIL) simulation testbed, could identify the attacks with an accuracy of more than 98%. Finally, to prevent replaying attacks, designers can consider the addition of timestamps to packets and signals transmitted [70].

### B. Controller, Charger, and Electric Motors

The controller and charger are fundamental elements that communicate with the BMS to exchange power to recharge the battery and to feed the EV components with energy. The charger communicates with the EVSE to negotiate the parameters of the charge. Moreover, it manages the energy received and forward it to the battery pack according to the BMS requirements. If bidirectional charging is available to EV, the charger may also deliver energy from the EV battery to the charging column upon request [71]. The controller manages the energy delivered from the battery to the other components. Some of these components are powered by the battery also in petrol-based vehicles, such as the infotainment system or the lights. Others, such as the electric motors, are instead specific to EV. The controller sends energy to them following the driver's input, such as the torque pedal pressure.

This section discusses how an attacker may impair their correct functioning.

*a) Man-in-the-Middle:* Modifying the data in the bus may disrupt the regular operation of the charger since the control signals are usually transmitted through this channel. An attacker may isolate certain charger components (e.g., the load relay), leading to a surge in the DC voltage. These attacks can damage the battery causing degradation in the performance and shortening the lifetime of the battery [72]. An attacker may also modify the signals managing the electric motors by adding noise or other mutations to the original signal. This attack can damage the correct functionality of the motors and put the driver in dangerous situations [73].

Mitigation techniques can be applied using algorithms that can detect the attack in almost real-time by monitoring the physical properties of the vehicle, such as sensor data [13], [72]. To make the receiver aware of possible MitM attacks targeting certain packets, integrity protection mechanisms must be in place. Furthermore, intrusion detection and prevention systems that monitor the data exchanged on the bus can also be implemented to strengthen the defense mechanism [64], [74].

*b) Denial of Service:* The operations handled by the charger and controller heavily rely on the sensors reporting information on the charging status. A malicious user can generate a large number of requests to the sensors reporting data or overload the charger and control modules by flooding them with packets, thus preventing the receipt of legitimate messages. If not properly handled, this attack may cause the controller to stop receiving correct state information, impairing the overall state control.

Flow control may prevent controllers and motors from handling a large number of fake requests similarly to the BMS, for instance, by employing an adapted version of time-lock puzzles [54]. Source authentication might be employed to verify the sender's lawfulness [53], while rate limiting can help mitigate against DoS attacks [55]. Furthermore, intrusion detection can be adopted to identify ongoing DoS attacks [56].

*c) Spoofing, and Replaying:* An attacker may spoof sensor identities to create multiple packets with legitimate identifications. By exploiting the same concept, an attacker may also report false information to the charger and controller. Therefore, the controller may take actions based on false data. This may cause damage to the hardware, possibly impairing the whole charging system [13]. False data, if correctly crafted, may also impact the electric motors' functionality. For instance, they could force a stop of the motors by sending false control signals. Encryption can be a countermeasure to spoofing, preventing a malicious user from freely creating new packets. However, replay attacks can be employed to send correct sensor measurements or actuator updates previously recorded from the bus. An attacker may also spoof the information from the infotainment system, acceleration pedal, or other energy-hungry devices in the EV. The malicious entity may demand a power amount higher than the truly needed one, thus causing higher energy consumption and shortening the battery's lifespan causing the driver to charge the EV frequently. The controller also handles the

information regarding acceleration and breaking. An attacker may spoof the related sensors to report false state changes to the electricity supplier. For instance, an attacker may spoof the gas pedal and prevent the receipt of the amount of power needed by the driver to speed up. This may cause safety issues, for instance, when the driver needs to surpass another vehicle.

As already depicted, encryption can only prevent certain kinds of spoofing attacks, but it is insufficient to mitigate replay attacks. To prevent the latter, a combination of unique identifiers and timestamps can be adopted [70]. Identity management may be another fundamental countermeasure against these threats [53]. In fact, the controller and charger need to have, by design, access to the identities of all legitimate components. The identification of attacks is possible using intrusion and anomaly detection techniques [56].

*d) Malicious Code Injection:* Similarly to the BMS case, controllers, chargers, and motors also contain software, which may often require updates. However, software updates represent a security challenge since it needs access to the overall EV network [29]. A malicious user may force the installation of a malicious software update to gain control of some components of the EV's internal network [29]. The attacker may thus impact the safety of the driver. For instance, the malware may cause the EV to respond to the driver commands oppositely (e.g., decelerating while pushing on the gas pedal) and may also propagate to all the EV's components. Furthermore, thanks to the malware, the attacker may measure sensitive information on the driver (e.g., location) or profile the driver. A further threat is due to the implementation of controllers and ECUs via Field Programmable Gate Array (FPGA). In this case, an attacker may be able to inject malicious software into the central management system via communication lines by manipulating the FPGA controller [13].

Countermeasures are similar to the BMS case. The access to the EV's internal network shall be strictly regulated, for instance, using strong authentication mechanisms. Remote attestation and its collective extension may be used to validate the in-vehicle components [62], while blockchain can have a role in the verification of new software [63]. Finally, intrusion detection techniques may help the identification of ongoing attacks [56].

*e) Tampering:* An attacker might physically tamper one of the controllers, charger, or motor components. In this case, for instance, the attacker may prevent the charger from correctly detecting the presence of a power source (either wired or wireless), thus impairing the possibility of charging the vehicle. This is the case for proximity sensors. For instance, the attacker may attach a shield to the pin on the EV side such that it cannot correctly communicate with the proximity pilot line. Furthermore, an attacker may tamper with the power converter to degrade its quality, causing power losses or overvoltage.

To prevent physical tampering, controllers, chargers, and motors may implement anomaly detection frameworks to detect the application of a voltage in non-safe situations and react to the attack [58]. Furthermore, these devices can be designed as tamper-proof, so they will stop functioning in case of tampering [59]. Although this may impair the vehicle's

functioning, it allows for safeguarding the user's safety.

*f) Eavesdropping, and Side Channels:* The current exchanged during the charging process leaks features that can be exploited for user tracking and profiling [75], [76]. An attacker may attach a module to the charger and controller to collect the current exchanged during the charging process and extract those features, thanks to the absence of encryption methods. For the same reason, an attacker may also eavesdrop on the information exchanged between the controller, the charger, the motors, and the BMS to launch the attacks mentioned above. An adversary may also analyze the power exchanged between the controller and the infotainment system to obtain users' sensitive information, such as preferences, habits, and passwords. This attack has been shown in other scenarios [77], such as smartphone charging, where users' activities can also be detected in case of encrypted traffic [78]. Therefore, it is fundamental to include methods to prevent malicious users from accessing the communication among these entities.

To guarantee the user's privacy, the current exchanged may be altered via a noisy signal that hides the original signal's features similarly to differential privacy in other contexts [79]. On the receiver side, the components shall be able to guarantee that the input current does not cause any damage to the circuitry. These solutions may hold for all the involved sources of current. Cryptographic methods may not always represent a viable solution, as they would add computational overhead to a possibly safety-critical system. Furthermore, they do not represent a solution to side channels, which are challenging to mitigate [80].

## V. EV CHARGING SECURITY AND PRIVACY CHALLENGES

This section discusses the security and privacy issues related to the EV charging process. In particular, we discuss the challenges associated with wired charging in Section V-A. Then, we discuss the challenges associated with WPT and WIPT in Section V-B. For both technologies, we also discuss possible solutions and countermeasures. In Table V, we summarize all the security and privacy challenges associated with the charging process, their effects, impact severeness, and possible countermeasures.

### A. Wired Charging Challenges

In the following, we focus on attacks targeting a wired charging scenario, which is the most common way at the moment of writing. Some of the attacks are specific to cases where HLC is available (e.g., MitM, spoofing), while others are suitable for every type of wired charging, such as tampering or side channel analysis.

*a) Tampering Attacks:* In this attack, a malicious user physically tampers with the devices involved in the charging process. In particular, an attacker might manipulate the pilot lines and tamper with the proximity sensor to prevent an EV from deeming a secure connection and hence prevent charging. Furthermore, this can also impact users' safety, as it might be possible to detach the cable before removing the current. By observing electromagnetic leaks or operations in the chip components both in the EVSE and EV, an attacker might infer

TABLE II  
SUMMARY OF EV CHARGING CHALLENGES.

System	Attack	Effect	Impact	Possible Solutions
Wired Charging	Tampering	Prevent charging Cause a shock to the driver Get sensitive information	High	Tamper-proof hardware Inconsistencies handler
	Energy repudiation	Cheat on billing Steal energy from the system	Low	Aggregate signature schemes Blockchain for energy transactions
	DoS	Prevent EV charging Disruption of the charging service	Medium	Identity verification Authentication Intrusion detection
	MitM	Prevent proper charging Modify charging parameters	High	Integrity protection Encryption
	Spoofing, and Replaying	Create charging state inconsistencies Steal energy from another EV	Medium	Identity management Authentication Encryption Timestamps
	Relaying	Steal energy from another EV	Medium	Distance bounding Fingerprinting
	Eavesdropping	Steal sensitive EV information	Medium	Encryption
	Side Channels, and Information Leaking	Track user Profile user's preferences	Low	Differential privacy Secondary batteries
WPT	Overpower	Damage to EV battery	High	Energy-efficient overvoltage protection Anomaly detection
	Jammering, and DoS	Prevent EV charging	Medium	Channel hopping Identity verification Authentication Intrusion detection
	Freeride attack	Steal energy from the system	Low	Authentication Blockchain
	Energy repudiation	Cheat on billing Steal energy from the system	Low	Aggregate signature schemes Blockchain for energy transactions
	Spoofing, and Replaying	Create charging state inconsistencies Steal energy from another EV	Medium	Authentication Encryption Physical layer authentication Timestamps
	Relaying	Steal energy from another EV	High	Distance bounding
	MitM	Prevent proper charging Modify charging parameters	Medium	Integrity protection Encryption Physical layer authentication
	Eavesdropping	Steal sensitive EV information	Medium	Encryption
	Side Channels, and Information Leaking	Track user Profile users' preferences	Medium	Differential privacy Secondary batteries

sensitive information on the user, such as private keys used for billing purposes [9]. Furthermore, by tampering with the charging cable, an attacker might prevent the proper charging of the victim EV or steal energy from an EV in charge by connecting additional cables [81], [82].

As possible countermeasures, tamper-proof hardware may represent a viable solution [59], [83]. Thanks to these devices, the attack may be limited to the car functioning without impacting the users' safety. Lastly, proper inconsistency handling mechanisms may be implemented to check that all involved components report the same physical status.

b) *Energy Charging Repudiation:* A malicious user may report to the EVSE that the EV's battery did not receive any power by exploiting the behavior of the pilot line and the feedback associated with it. In this situation, the attacker may be able to charge a smaller amount compared to the amount of energy effectively used. If bidirectional charging is available,

an attacker may pretend to have sold more energy than it has actually sold, thus stealing money from the energy provider.

A possible countermeasure to energy repudiation is the use blockchain technology to handle transactions and guarantee traceability and non-repudiation [84], [85]. Aggregate signature schemes from different physical components can represent another possible mitigation to the problem [86].

c) *Denial of Charging:* A malicious actor may try to prevent a vehicle from charging. It may be done at the data level by modifying values on the packets exchanged during the handshake between the EV and EVSE [87]. In some cases, DoS can also be performed remotely, exploiting unshielded cables, which are often used for the recharge [88]. DoS may also be launched against more than one vehicle, trying to compromise a portion of the grid. A greedy attacker may falsify the information on the battery's SoC, such that s/he can demand an energy amount higher than needed, thus preventing

other users from benefiting from the service. The number of users that can simultaneously charge their EVs and the energy effectively delivered each moment depends on the grid's capacity. If the grid capacity is limited, the attacker can successfully launch this attack and prevent other users from charging.

Possible countermeasures to DoS attacks include low-complexity authentication services in all the packets exchanged such that the EVSE can rapidly decide whether to accept or discard a request. Identity-based traffic filtering may be combined with a physical state update related to the charge level of a certain user to prevent multiple malicious requests. Intrusion detection can be employed to detect ongoing DoS attacks which may generate strange communication patterns [56]. Furthermore, enforcing physical security by adopting shielded cables can prevent some kinds of DoS and eavesdropping attacks [88].

*d) Man-in-the-Middle:* When operating charging modes employing HLCs, such as CHAdeMo or ISO 15118, the EV and EVSE exchange data through network packets. A MitM attack can be employed to modify the content of this communication. It may be a consequence of tampering if the malicious actor can insert a device on the pilot line between the vehicle and the charging column. In some cases, MitM can be performed from other charging columns attacking the SECC Discovery Protocol [89]. A malicious actor may exploit this channel to manipulate the exchanged information and create inconsistencies in the recharging process. For instance, an attacker who can modify packets on the fly may prevent proper charging by modifying request and response parameters. Further attacks can be launched starting from MitM, such as malware injections or DoS [87].

To identify modified data, integrity protection can be added to packets [90]. Another possible countermeasure is encryption. Novel versions of ISO 15118 mandates the usage of Transport Layer Security (TLS) for all the communications between the vehicle and charging column, even if in real life, data are often exchanged in plaintext [81].

*e) Spoofing, and Replaying:* An attacker might interact in the communication link between the vehicle and the charging column by injecting packets spoofing other devices' identities. For instance, a malicious user can spoof the identity of an ECU and report false information on the battery SoC. Furthermore, an attacker may inject false information by spoofing the identity of an EVSE and stealing sensitive information from an EV. For example, in the case of automatic billing based on the EV features, a malicious user can extrapolate those features from an EV and store them for later use to bill the victim. The same concept can also be applied to other types of connectors, as long as billing is based on automatic feature recognition [37].

Possible countermeasures to these attacks include using a proper identity management scheme, authentication, and data encryption [91]. Authentication systems shall include information related to the charging status of the EV or the energy delivered by the EVSE to help guarantee the consistency between the reported information and the actual physical state. It is important to consider that encryption cannot prevent the

replaying of packets, which may instead be enforced with unique identifiers and timestamps [70].

*f) Relaying:* A relay attack is possible if an attacker has access to the network traffic and can relay it to a nearby charging column. By relaying information, a malicious user can manipulate the billing system. For instance, a malicious user can relay the data between two neighboring EVSEs to bill a closely-located victim user for a charging session [82]. If bidirectional charging is available, a malicious user can sell the energy of a victim's vehicle and get paid for it.

The location information of EV and EVSE may be exploited to prevent relay attacks, e.g., employing distance bounding protocols [92], [82]. Furthermore, the physical features of the EV may be exploited to design dedicated authentication protocols [93], [94].

*g) Eavesdropping:* An attacker may be able to read the information exchanged between the vehicle and charging columns in different ways, similarly to what was presented before for MitM attacks. With access to all the network traffic, a malicious entity can steal sensitive information from the user, from simple charging parameters to credit card numbers.

To protect against eavesdropping, encryption can be applied. As already explained, novel versions of ISO 15118 mandate the usage of TLS for all the communications between the vehicle and the charging column, even if real-life data are still often exchanged in plaintext [81]. It is important to recall that even if the exchanged data are encrypted, side channel analysis is possible to extract some users' preferences, as presented in the following section.

*h) Side Channels, and Information Leakages:* An attacker in control of an EVSE may be able to track and profile users who authenticate to the EVSE even if data are encrypted. It may rely on different information, such as the MAC address of the EV or the certificate employed by Plug and Charge [38]. However, in Level 1 and Level 2 charging, these kinds of data are unavailable since no HLC is generated between the two entities. In that case, an attacker may rely on other features, such as the exact voltage of the control pilot pin or the duration of the handshake at the beginning of the charging process [94]. Another side channel that may transfer information is the effective current exchange. This does not convey information in a network sense, i.e., it does not involve the creation of packets with the sender's and receiver's information. Therefore, no encryption method is applied to this signal, which is transmitted in plaintext. However, it has been shown that it is possible to profile users by extracting features from the charging current [75], [76]. In particular, the charging current contains features peculiar to each EV, allowing for EV tracking and user profiling based on the current demand. Therefore, it is fundamental to manipulate the current signal to prevent these attacks.

Countermeasures to privacy threats shall not undermine the efficiency of the charging process. Therefore, possible solutions must allow the involved parties to retrieve sufficient information, e.g., to the SoC. Differential privacy methods may represent a viable solution [95]. An alternative is represented by the use of secondary batteries to create a connection between the EV and EVSE, similarly to what was discussed

in [75], [76]. When HLC is available, MAC address randomization may represent a good mitigation technique to reduce the profiling power of an attacker.

### B. WPT Challenges

Due to the exposure of the wireless medium, WPT incurs in a large number of safety, security, and privacy issues. In fact, it is likely that WPT signals to impact more vehicles and that an attacker gets access to the signals or information wirelessly exchanged [96]. In this section, we review and extend the taxonomy of the possible attacks to WPT presented in [96] and adapted it to the EV case.

*a) Overpower attack:* The wireless medium's intrinsic vulnerability makes it possible that a single EV receives both its signal and the signal intended for another vehicle. For instance, if two cars are closely located, and both are charging their batteries via WPT, they will receive more power than expected. This is even more likely when considering fully-dynamic WPT, where vehicles move and cannot hence guarantee that a reasonable safety space is kept between them. The excessive received power might harm some components of the BMS or the battery if a proper overvoltage regulator is not deployed. Furthermore, an attacker might exploit this concept to launch an overvoltage attack to damage the EV's components.

Possible countermeasures include implementing overvoltage protection mechanisms at the EV's side. Such mechanisms shall, however, guarantee the efficiency of the charging process to avoid requiring excessive charging times. Anomaly detection methods can also be applied to detect the reception of abnormal power values or other anomalies in the charging process. Design choices can help mitigate overpower attacks. For instance, the distance between coils must be designed to make overpower attack unfeasible or, at least, more complicated.

*b) Jamming, and Denial of Service:* In the case of WIPT, the reception of multiple signals might cause excessive interference at the receiver's side, thus preventing the correct reception of messages. Due to the openness of the WPT medium, an attacker might be able to simultaneously jam multiple EVs by sending random WIPT messages and degrading the channel quality up to the point where messages are not correctly received. Furthermore, this concept can be exploited to prevent a successful charging negotiation phase, thus preventing a connection between the EV and the charging system. This represents a DoS attack. Similarly, an attacker may launch a jamming attack against the charging column's WiFi access point, preventing legitimate users from connecting and using the service. An attacker may also target a portion of the energy grid by continuously sending charging requests. If many users engage in this session, they might prevent other users from benefiting from the service availability. Although feedback mechanisms to report on the SoC of the receiver might be implemented to automatically detach an EV when fully charged, an expert attacker might be able to craft feedback packets to avoid showing full battery's SoC.

Possible solutions include frequency hopping mechanisms, where channels are selected according to different strategies to avoid using a channel under jamming attack [97].

Low-complexity authentication services in all the packets exchanged such that the EVSE can rapidly decide whether to accept or discard a request can help in preventing DoS attacks. To detect a DoS attack, intrusion detection systems can be deployed [56]. Identity-based traffic filtering may be combined with a physical state update related to the charge level of a specific user to prevent multiple malicious requests.

*c) Freeriding attack:* As previously mentioned, a user might connect to public infrastructure and pay for charging via WPT. Due to the openness of the WPT medium, a malicious user could exploit the proximity to a vehicle in charge to steal energy and charge his/her EV. A similar scenario envisions the collusion of multiple EV owners when a single one registers for the service and multiple users share the bill and benefit from the charging process. These attacks are feasible in all types of dynamic WPT models; the only requirement is a short inter-EV distance. This attack is challenging to detect, as it does not impact the legitimate channel. In fact, although a second EV might be connected to the charging channel, the main channel will not face any performance degradation, thus making it unfeasible to detect the attack.

WPT sessions need to be authenticated to prevent other users from benefiting from a charging session they are not paying for. Furthermore, authentication procedures might include the physical features of the involved devices and the amount of power transferred. The blockchain solutions proposed by Jiang et al. [98] may be adapted to the EV case to guarantee security against this attack.

*d) Energy repudiation:* WPT is less efficient compared to its wired counterpart, as the wireless medium is characterized by losses due to both attenuation and the relative position of the transmitter and receiver devices. Therefore, part of the transmitted energy may be lost during the charging process. A fair system requires that users pay for the actually received energy. Therefore the billing system needs to compare the transmitted power with the received one. However, this might create security issues. In fact, a malicious user might continuously report a received power value smaller than the true one or report zero received energy. This is commonly known as a repudiation attack, where the user denies benefiting from a service.

To guarantee the correctness of the reported power usage information, possible solutions might include the use of aggregate signature schemes from different physical components [86] or the blockchain technology [85], [98].

*e) Spoofing, and Replaying:* A malicious user who knows the standard employed or which is able to eavesdrop on the communication can easily craft malicious packets. Based on the crafted information, this class of attacks may have different impacts on the system. For instance, an attacker may use the identifier of another vehicle to negotiate a charging session that the victim will pay for. Furthermore, a malicious actor can craft packets declaring weird SoC and spoof other vehicles' identifiers to create inconsistencies in the charging process.

The use of authentication and integrity protection mechanisms can be effective countermeasures against spoofing. In this context, using physical layer authentication may help in

designing suitable protocols [99]. In the context of WPT, the transmission frequency can be regulated to encrypt information and guarantee that only the legitimate party can receive power [100]. This also represents a possible solution to the attacks aforementioned in this section. Finally, timestamps can be added to identify multiple sending of the same packet in a replaying attack [70].

*f) Eavesdropping:* Due to the exposure of the wireless medium, an attacker may easily intercept WPT packets. These packets may contain different types of information, such as the vehicle identifier, SoC information, or billing information.

Possible solutions include the use of cryptographic techniques to hide information. The newest release of ISO 15118 [36] mandates TLS on every communication.

*g) Relaying:* An attacker may relay information from a victim vehicle to the access point of the attacker's charging column to steal energy [82]. This kind of attack work even if the traffic is encrypted since the data is only relayed and not modified. With respect to the wired counterpart, where the attacker has to tamper in some way with the charging column, a wireless relay attack does not need any hardware modification.

To protect against relay attacks, a distance bounding protocol can be employed to assess if a malicious entity is relaying the network flow [82].

*h) Man-in-the-Middle attack:* With respect to wireless charging, when dealing with WPT, the interception and forwarding of communication flow are easier due to the openness of the medium [101]. At the same time, directional jamming can be employed in some cases to prevent the receiver from getting both the original and the modified data. If the communication flow is unencrypted or the cryptography is weak, an attacker can launch a MitM attack to modify on-the-fly packets. For instance, a malicious user might modify the information sent by the victim (i.e., report full SoC) after establishing a connection with the service provider. To perform such an attack, a malicious entity may set up a fake access point and use it to relay the communication to the legitimate one, gaining the ability to modify packets at will.

Partial solutions include the previously mentioned solutions, such as encryption, authentication, and integrity protection mechanisms. In the context of WPT, the transmission frequency can be regulated to encrypt information and guarantee that only the legitimate party can receive power [100]. Furthermore, physical layer authentication may enhance the security of the authentication process [102].

*i) Side Channels, and Information Leaking:* Although WPT signals might be encrypted or avoid sensitive reporting information on the user, the power signal can be exploited for profiling purposes. This attack has been proven feasible for smartphones, where the WPT signal analysis reveals information on the user's activity [103]. This might also be the case for EVs, where an attacker can infer different types of information. This attack is similar to the profiling performed in the wired case, where it might be possible to track a user and obtain information on her habits and power demands. Preventing this attack represents a challenging task, as it cannot be detected, and data encryption is not sufficient [104].

A possible solution is represented by differential privacy, where data is corrupted with a noisy pattern that might prevent inferring sensitive users' data [79]. Furthermore, as for the wired counterpart, secondary batteries may prevent the attacker from inferring sensitive users' information.

## VI. FUTURE DIRECTIONS

Looking at the impact of the different attacks in Tables IV and V, we can conclude that many security issues related to the cyber-physical nature of EVs may impact the safety of the driver. We notice that some of the attacks and countermeasures discussed can also be applied to other EV assets. However, due to space limitations and to avoid being repetitive, we only discussed those we considered to be the most interesting. Nevertheless, we summarize all the attacks and countermeasures in the comprehensive Table III. Although many threats concern the charging infrastructure, the most severe in terms of safety are related to the in-vehicle network. In fact, the electric component of EVs may be tampered with or impaired to electroshock the user. Furthermore, the increasing cyber nature of the EVs' components leads to challenges regarding the coherency of the information coming from the cyber and the physical worlds. Lastly, the increasing interest in the application of the WPT technology to EVs impose significant challenges that still need to be properly addressed from a CPS point of view.

Based on our analysis, we foresee the following future directions and needs in the field of EV CPS security.

- Denial of Service (DoS) represents one of the most challenging threats in EVs security. It is known as difficult to prevent, and almost every component of the EV can suffer from it. Compromised internal components can attack other ECU to compromise the in-vehicle network, but DoS attacks can be launched from charging columns to EV during charging, or vice-versa. In certain cases, DoS can have an impact not only on a single vehicle but can compromise EVSEs in a certain geographical area. To mitigate this risk, not only do all the vehicle entities need to be associated with an identity, but their allowed flow of information (and hence generated traffic) should depend on the vehicle's physical situation. In fact, it might be that a specific ECU needs to send messages at a higher rate when the vehicle is experiencing certain physical stimuli. At the same time, all ECUs shall be guaranteed a sufficient amount of resources. Therefore, future protections against DoS for in-vehicle networks should account for the physical factors and the possible impact on the whole electric grid.
- The potential tampering with the EV components might represent a significant threat to the user's safety and may also have repercussions on other elements of the vehicle system. All vehicle components shall be equipped with anomaly detection capabilities or should prevent the application of a voltage or current flow in case of tampering. Possible future solutions might include the collective verification of multiple components to make tampering with a single unit ineffective.

TABLE III

SUMMARY TABLE WITH ATTACKS AND COUNTERMEASURES FOR EACH ASSET. THE FIRST ROW INDICATE THE ASSETS INTERESTED BY EACH ATTACK, WHILE THE FOLLOWING ROWS POINT OUT WHICH COUNTERMEASURE IS EFFECTIVE AGAINST EACH ATTACK.

■ : BMS AND BATTERY; □ : CONTROLLERS, CHARGER AND MOTORS; ⚡ : WIRED CHARGING; AND ☎ : WPT.

Attack \ Countermeasure	DoS	Tampering	MitM	Replaying	Spoofing	Malware	Overpower	Freeride	Jamming	Repudiation	Eavesdropping	Side-Channels	Relaying
Affected assets	■ □ ⚡ ☎	■ □ ⚡ ☎	■ □ ⚡ ☎	■ □ ⚡ ☎	■ □ ⚡ ☎	■ □	☎	☎	☎	☎	■ □ ⚡ ☎	■ □ ⚡ ☎	☎
Aggregate signature										⚡ ☎			
Anomaly detection		■ □					☎						
Authentication	⚡ ☎		■ □ ⚡ ☎		■ □ ⚡ ☎	■ □	☎						
Blockchain							☎			⚡ ☎			
Channel hopping							☎						
Cookies	■ □												
Differential privacy								■ □		■ □ ⚡ ☎			
Distance bounding											⚡ ☎		
Encryption		■ □ ⚡ ☎			■ □ ⚡ ☎			■ □ ⚡ ☎					
Fingerprinting										⚡			
Flow control	■ □												
Intrusion detection/prevention	■ □ ⚡ ☎		■ □	■ □	■ □	■ □							
Identity management			■ □		■ □	■ □							
Identity verification	⚡ ☎			⚡ ☎			⚡ ☎						
Inconsistencies handler		⚡											
Integrity protection		■ □ ⚡ ☎											
Overvoltage protection							☎						
Physical layer security			☎		☎		☎						
Rate limiting	■ □												
Redundancy	■		■	■	■	■							
Remote Attestation						■ □						⚡ ☎	
Secondary battery													
Tamper-proof hardware		■ □ ⚡											
Time-lock puzzles	■ □				■ □ ⚡ ☎								
Timestamps													

- The increasing attackers' capabilities impose additional challenges in guaranteeing the cyber-security of EVs. In fact, an attacker might be able to combine multiple attacks to impair the EV functioning. To strengthen the defense mechanisms, it is essential to implement in EVs frameworks collecting information from multiple sources, combining the cyber and the physical world. For instance, verifying the message integrity might employ data from different sensors and actuators to increase the difficulty of information manipulation. Similarly, intrusion detection techniques might combine network data exchanged through the bus with physical signals from sensors to model better the state of the EV. This will also help prevent attacks related to malicious ECUs controlling actuators for mechanical operations (e.g., steering). Future work should consider the EV-specific components such as the battery or the charger as data sources regarding the vehicle's state. For instance, the charge and discharge curves of batteries can be modeled by computers with discrete confidence [105], [106], [107]. A simple application of these simulations is a reference to identify packets declaring modified SoC.
- One of the strengths of EVs compared to previous generations of vehicles relies on the software managing all their operations. However, this implies that vehicles are more subject to cybersecurity attacks. Some of these attacks may include malware injection into some of the EV's components. To this aim, collective remote attestation can be used to verify the integrity of all the EV's components

and prevent possible safety threats. Remote attestation measures should, however, account for the resource-limited nature of EVs' components and the time-critical nature of the exchanged information.

- WPT is one of the promising technological solutions to alleviate the range anxiety of drivers fearing not reaching their destination with the available charge. Thanks to the charging while driving paradigm, EVs can be charged during their operation. However, deploying the required public infrastructure poses many security challenges both to the operators and the users. Some examples include the billing process and the openness of the wireless medium. WPT related challenges heavily rely on the cyber-physical nature of the overall infrastructure. Therefore, security solutions in this area should account for the coherency of information from the cyber and the physical domains.

## VII. CONCLUSION

The increasing market for EVs demands an in-depth analysis of EV technology's security and privacy challenges. In this paper, we provided an overview of the components of an EV, focusing on their characteristic components. We provided the basic information needed to understand how in-vehicle communication networks work and which devices need to communicate with one another. We then discussed how an EV battery could be charged via wire and WPT. We provided the information needed to understand both technologies and discussed the different implementations. We also provided the

security and privacy issues of in-vehicle communications and those related to the charging infrastructure. Focusing on a CPS perspective, we discussed how different attacks might impact both the user and the system's security and privacy. We then discussed possible countermeasures and proposed some future direction to improve the overall EV ecosystem security and privacy. We conclude that the EV technology currently presents a large attack surface that users with malicious intents can exploit. Therefore, it is fundamental to develop technologies considering the CPS nature of EVs to provide full security.

## REFERENCES

- [1] Z. Shaham, “16 Countries Now Over 10% Plugin Vehicle Share, 6 Over 20%,” <https://cleantechnica.com/2021/09/05/16-countries-now-over-10-plugin-vehicle-share-6-over-20/>, 2021.
- [2] A. Madhani and T. Krisher, “Biden Pushes Electric Vehicle Chargers as Energy Costs Spike,” <https://www.usnews.com/news/business/articles/2021-11-17/biden-pushes-electric-vehicle-chargers-as-energy-costs-spike>, Nov. 2021.
- [3] P. Gordon, “Netherlands aims to ban conventionally-fueled vehicles by 2050,” <https://www.smart-energy.com/industry-sectors/electric-vehicles/netherlands-aims-to-ban-conventionally-fueled-vehicles-by-2050/>, Jan. 2019.
- [4] T. Capuder, D. M. Sprčić, D. Zorićić, 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.
- [5] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” *Black Hat USA*, vol. 2015, no. S 91, 2015.
- [6] C.-W. Lin and A. Sangiovanni-Vincentelli, “Cyber-security for the controller area network (CAN) communication protocol,” in *2012 International Conference on Cyber Security*. IEEE, 2012, pp. 1–7.
- [7] C. Schmittner and G. Macher, “Automotive cybersecurity standards—relation and overview,” in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2019, pp. 153–165.
- [8] M. Scalas and G. Giacinto, “Automotive cybersecurity: Foundations for next-generation vehicles,” in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*. IEEE, 2019, pp. 1–6.
- [9] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, “Cyber-physical system security of vehicle charging stations,” in *2019 IEEE Green Technologies Conference (GreenTech)*. IEEE, 2019, pp. 1–5.
- [10] A. Bahrami, “Ev charging definitions, modes, levels, communication protocols and applied standards,” *Changes*, vol. 1, pp. 10–01, 2020.
- [11] H. S. Das, M. M. Rahman, S. Li, and C. Tan, “Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review,” *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109618, 2020.
- [12] A. Khalid, A. Sundararajan, A. Hernandez, and A. I. Sarwat, “Facts approach to address cybersecurity issues in electric vehicle battery systems,” in *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*. IEEE, 2019, pp. 1–6.
- [13] A. Chandwani, S. Dey, and A. Mallik, “Cybersecurity of onboard charging systems for electric vehicles—review, challenges and countermeasures,” *IEEE Access*, vol. 8, pp. 226 982–226 998, 2020.
- [14] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, “Cybersecurity of smart electric vehicle charging: A power grid perspective,” *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.
- [15] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, “Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2020.
- [16] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, “A detailed security assessment of the ev charging ecosystem,” *IEEE Network*, vol. 34, no. 3, pp. 200–207, 2020.
- [17] S. Sripath, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, “Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks.”
- [18] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, “Electric vehicle charging: a survey on the security issues and challenges of the open charge point protocol (ocpp),” *IEEE Communications Surveys & Tutorials*, 2022.
- [19] P. Van Aubel and E. Poll, “Security of ev-charging protocols,” *arXiv preprint arXiv:2202.04631*, 2022.
- [20] P. R. Babu, B. Palaniswamy, A. G. Reddy, V. Odelu, and H. S. Kim, “A survey on security challenges and protocols of electric vehicle dynamic charging system,” *Security and Privacy*, vol. 5, no. 3, 2022.
- [21] Y. Frajji, 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.
- [22] Many cars have a hundred million lines of code. MIT Technology Review. [Online]. Available: <https://www.technologyreview.com/2012/12/03/181350/many-cars-have-a-hundred-million-lines-of-code/>
- [23] K. Cho, J. Kim, D. Y. Choi, Y. H. Yoon, J. H. Oh, and S. E. Lee, “An fpga-based ecu for remote reconfiguration in automotive systems,” *Micromachines*, vol. 12, no. 11, p. 1309, 2021.
- [24] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of can bus security challenges,” *Sensors*, vol. 20, no. 8, p. 2364, 2020.
- [25] “Road vehicles — Local Interconnect Network (LIN) — Part 8: Electrical physical layer (EPL) specification: LIN over DC powerline (DC-LIN),” International Organization for Standardization (ISO), Standard, Mar. 2019.
- [26] R. Makowitz and C. Temple, “Flexray—a communication network for automotive control systems,” in *2006 IEEE International Workshop on Factory Communication Systems*. IEEE, 2006, pp. 207–212.
- [27] B. Fijalkowski, “Media oriented system transport (most) networking,” in *Automotive Mechatronics: Operational and Practical Issues*. Springer, 2011, pp. 73–74.
- [28] C. Corbett, E. Schoch, F. Kargl, and F. Preussner, “Automotive ethernet: Security opportunity or challenge?” *Sicherheit 2016-Sicherheit, Schutz und Zuverlässigkeit*, 2016.
- [29] S. Halder, A. Ghosal, and M. Conti, “Secure over-the-air software updates in connected vehicles: A survey,” *Computer Networks*, vol. 178, p. 107343, 2020.
- [30] F. Un-Noor, S. Padmanaban, L. Mihet-Popa, M. N. Mollah, and E. Hossain, “A comprehensive study of key electric vehicle (EV) components, technologies, challenges, impacts, and future direction of development,” *Energies*, vol. 10, no. 8, p. 1217, 2017.
- [31] L. Guo and J. Ye, “Cyber-physical security of electric vehicles with four motor drives,” *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4463–4477, 2020.
- [32] S. S. Ravi and M. Aziz, “Utilization of electric vehicles for vehicle-to-grid services: progress and perspectives,” *Energies*, vol. 15, no. 2, p. 589, 2022.
- [33] T. Blech, “CHAdMO DC charging standard: evolution strategy and new challenges,” Tech. Rep., 2019.
- [34] Y. Li, Y. Wang, M. Wu, and H. Li, “Replay Attack and Defense of Electric Vehicle Charging on GB/T 27930-2015 Communication Protocol,” vol. 07, no. 12, pp. 20–30.
- [35] International Standard Organization, “ISO 15118-8:2020: Road vehicles — vehicle to grid communication interface — part 8: Physical layer and data link layer requirements for wireless communication,” Standard, Sep. 2022.
- [36] —, “ISO 15118-20:2022: Road vehicles — vehicle to grid communication interface — part 20: 2nd generation network layer and application layer requirements,” Standard, Apr. 2022.
- [37] What is Autocharge? Fastned FAQ. [Online]. Available: <https://support.fastned.nl/hc/en-gb/articles/115012747127-What-is-Autocharge>.
- [38] “ISO 15118-1:2019: Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition,” International Organization for Standardization (ISO), Standard, Apr. 2019.
- [39] L. Buschlinger, M. Springer, and M. Zhdanova, “Plug-and-patch: Secure value added services for electric vehicle charging,” in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–10.
- [40] “SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler,” Society of Automotive Engineers (SAE), Standard, Apr. 2019.
- [41] Z. J. Lee, G. Lee, T. Lee, C. Jin, R. Lee, Z. Low, D. Chang, C. Ortega, and S. H. Low, “Adaptive charging networks: A framework for smart electric vehicle charging,” *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4339–4350, 2021.
- [42] “IEEE Standard Technical Specifications of a DC Quick Charger for Use with Electric Vehicles,” *IEEE Std 2030.1.1-2015*, pp. 1–97, 2016.

- [43] Z. Zhang, H. Pang, A. Georgiadis, and C. Cecati, "Wireless power transfer—an overview," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1044–1058, 2018.
- [44] H. Wang and K. W. E. Cheng, "An improved and integrated design of segmented dynamic wireless power transfer for electric vehicles," *Energies*, vol. 14, no. 7, p. 1975, 2021.
- [45] P. Machura, V. De Santis, and Q. Li, "Driving range of electric vehicles charged by wireless power transfer," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5968–5982, 2020.
- [46] L. F. Roman and P. R. Gondim, "Authentication protocol in ctns for a cwd-wpt charging system in a cloud environment," *Ad Hoc Networks*, vol. 97, p. 102004, 2020.
- [47] F. Corti, A. Reatti, M. C. Piccirilli, F. Grasso, L. Paolucci, and M. K. Kazimierczuk, "Simultaneous wireless power and data transfer: Overview and application to electric vehicles," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2020, pp. 1–5.
- [48] H. J. Jo and W. Choi, "A survey of attacks on controller area networks and corresponding countermeasures," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
- [49] E. Sutcliffe, A look at electric car explosions. EV Fire Safe. [Online]. Available: <https://www.evfiresafe.com/post/electric-car-explosions>
- [50] A. F. Blum and R. T. Long Jr, "Fire hazard assessment of lithium ion battery energy storage systems," 2016.
- [51] T. Gunasekhar, K. T. Rao, P. Saikiran, and P. S. Lakshmi, "A survey on denial of service attacks," 2014.
- [52] M. Culler and H. Burroughs, "Cybersecurity considerations for grid-connected batteries with hardware demonstrations," *Energies*, vol. 14, no. 11, p. 3067, 2021.
- [53] B. Groza and P.-S. Murvay, "Security solutions for the controller area network: Bringing authentication to in-vehicle networks," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 40–47, 2018.
- [54] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," 1996.
- [55] M. Kuerban, Y. Tian, Q. Yang, Y. Jia, B. Huebert, and D. Poss, "Flowsec: Dos attack mitigation strategy on sdn controller," in *2016 IEEE International Conference on Networking, Architecture and Storage (NAS)*. IEEE, 2016, pp. 1–2.
- [56] C. Young, J. Zambrero, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design & Test*, vol. 36, no. 6, pp. 48–55, 2019.
- [57] S. Bogosyan and M. Gokasan, "Novel strategies for security-hardened bms for extremely fast charging of bevs," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2020, pp. 1–7.
- [58] Z. Sun, Y. Han, Z. Wang, Y. Chen, P. Liu, Z. Qin, Z. Zhang, Z. Wu, and C. Song, "Detection of voltage fault in the battery system of electric vehicles using statistical analysis," *Applied Energy*, vol. 307, p. 118172, 2022.
- [59] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin, "Algorithmic tamper-proof (atp) security: Theoretical foundations for security against hardware tampering," in *Theory of Cryptography Conference*. Springer, 2004, pp. 258–277.
- [60] "J2464: Electric and Hybrid Electric Vehicle Rechargeable Energy Storage System (RESS) Safety and Abuse Testing," Society of Automotive Engineers (SAE), Standard, Aug. 2021.
- [61] P. Kiley, "Reverse Engineering the Tesla Battery Management System to Increase Power Available," *Blackhat*, p. 28, 2020. [Online]. Available: <https://i.blackhat.com/USA-20/Wednesday/us-20-Kiley-Reverse-Engineering-The-Tesla-Battery-Management-System-To-Increase-Power-Available.pdf>
- [62] M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise, "Collective remote attestation at the internet of things scale: State-of-the-art and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2447–2461, 2020.
- [63] G. Bere, J. J. Ochoa, T. Kim, and I. R. Aenugu, "Blockchain-based firmware security check and recovery for battery management systems," in *2020 IEEE Transportation Electrification Conference & Expo (ITEC)*. IEEE, 2020, pp. 262–266.
- [64] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," in *Third IEEE international conference on pervasive computing and communications workshops*. IEEE, 2005, pp. 141–145.
- [65] R. Guo, L. Lu, M. Ouyang, and X. Feng, "Mechanism of the entire overdischarge process and overdischarge-induced internal short circuit in lithium-ion batteries," *Scientific reports*, vol. 6, no. 1, pp. 1–9, 2016.
- [66] S. L. Kinney, *Trusted platform module basics: using TPM in embedded systems*. Elsevier, 2006.
- [67] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.
- [68] T. Kim, J. Ochoa, T. Faika, A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.
- [69] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Transactions on Transportation Electrification*, vol. 7, no. 3, pp. 2010–2022, 2020.
- [70] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended iot devices designed for healthcare," in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)*. IEEE, 2017, pp. 811–817.
- [71] J. Pinto, V. Monteiro, H. Gonçalves, B. Exposto, D. Pedrosa, C. Couto, and J. L. Afonso, "Bidirectional battery charger with grid-to-vehicle, vehicle-to-grid and vehicle-to-home technologies," in *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2013, pp. 5934–5939.
- [72] S. Dey, A. Chandwani, and A. Mallik, "Real time intelligent data processing algorithm for cyber resilient electric vehicle onboard chargers," in *2021 IEEE Transportation Electrification Conference & Expo (ITEC)*. IEEE, 2021, pp. 1–6.
- [73] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3301–3310, 2019.
- [74] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, 2012.
- [75] A. Brighente, M. Conti, and I. Sadaf, "Tell me how you re-charge, i will tell you where you drove to: Electric vehicles profiling based on charging-current demand," in *European Symposium on Research in Computer Security*. Springer, 2021, pp. 651–667.
- [76] A. Brighente, M. Conti, D. Donadel, and F. Turrin, "Evscout2.0: Electric vehicle profiling through charging profile," *ACM Trans. Cyber-Phys. Syst.*, sep 2022.
- [77] H. Li, Y. He, L. Sun, X. Cheng, and J. Yu, "Side-channel information leakage of encrypted video stream in video surveillance systems," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.
- [78] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Can't you hear me knocking: Identification of user actions on android apps via traffic analysis," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 2015, pp. 297–304.
- [79] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.
- [80] A. K. Khan and H. J. Mahanta, "Side channel attacks and their mitigation techniques," in *2014 First International Conference on Automation, Control, Energy and Systems (ACES)*. IEEE, 2014, pp. 1–4.
- [81] R. Baker and I. Martinovic, "Losing the car keys: Wireless PHY-Layer insecurity in EV charging," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 407–424. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity19/presentation/baker>
- [82] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," in *Computer Security – ESORICS 2022*. Springer International Publishing, 2022, pp. 488–508.
- [83] A. Ahmad, S. Lee, and M. Peinado, "Hardlog: Practical tamper-proof system auditing using a novel audit device," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 1554–1554.
- [84] R. Jurdak, A. Dorri, and M. Vilathgamuwa, "A trusted and privacy-preserving internet of mobile energy," *IEEE Communications Magazine*, vol. 59, no. 6, pp. 89–95, 2021.
- [85] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE access*, vol. 6, pp. 13 565–13 574, 2018.
- [86] F. Zhang, L. Shen, and G. Wu, "Notes on the security of certificateless aggregate signature schemes," *Information Sciences*, vol. 287, pp. 32–37, 2014.

- [87] L. Attanasio, M. Conti, D. Donadel, and F. Turrin, “Miniv2g: An electric vehicle charging emulator,” in *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*, ser. CPSS ’21. New York, NY, USA: Association for Computing Machinery, 2021, p. 65–73. [Online]. Available: <https://doi.org/10.1145/3457339.3457980>
- [88] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, “Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging.” [Online]. Available: <http://arxiv.org/abs/2202.02104>
- [89] S. Dudek, J.-C. Delaunay, and V. Fargues, “V2G injector: Whispering to cars and charging units through the power-line,” 2019.
- [90] M. Ahmadvand, A. Pretschner, and F. Kelbert, “A taxonomy of software integrity protection techniques,” in *Advances in Computers*. Elsevier, 2019, vol. 112, pp. 413–486.
- [91] A. C.-F. Chan and J. Zhou, “A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 3367–3376, 2015.
- [92] ———, “On smart grid cybersecurity standardization: Issues of designing with nistir 7628,” *IEEE Communications Magazine*, vol. 51, no. 1, pp. 58–65, 2013.
- [93] ———, “Cyber–physical device authentication for the smart grid electric vehicle ecosystem,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.
- [94] R. L. Houser, W. Kempton, R. McGee, F. Kiamilev, and N. Waite, “Ev fingerprinting,” SAE Technical Paper, Tech. Rep., 2017.
- [95] M. U. Hassan, M. H. Rehmani, and J. Chen, “Differential privacy techniques for cyber physical systems: a survey,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.
- [96] Q. Liu, K. S. Yildirim, P. Pawelczak, and M. Warnier, “Safe and secure wireless power transfer networks: Challenges and opportunities in RF-based systems,” *IEEE Communications Magazine*, vol. 54, no. 9, pp. 74–79, 2016.
- [97] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.
- [98] L. Jiang, S. Xie, S. Maharanj, and Y. Zhang, “Blockchain empowered wireless power transfer for green and secure internet of things,” *IEEE Network*, vol. 33, no. 6, pp. 164–171, 2019.
- [99] N. Xie, Z. Li, and H. Tan, “A survey of physical-layer authentication in wireless communications,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2020.
- [100] Z. Zhang, K. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” *IEEE Transactions on Power Electronics*, vol. 30, no. 9, pp. 5237–5246, 2014.
- [101] H. Hwang, G. Jung, K. Sohn, and S. Park, “A study on mitm (man in the middle) vulnerability in wireless network using 802.1 x and eap,” in *2008 International Conference on Information Science and Security (ICISS 2008)*. IEEE, 2008, pp. 164–170.
- [102] L. Y. Paul, J. S. Baras, and B. M. Sadler, “Physical-layer authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.
- [103] A. La Cour, K. Afzadi, and G. E. Suh, “Wireless charging power side-channel attacks,” *arXiv preprint arXiv:2105.12266*, 2021.
- [104] B. Saltafornaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, and J. Qian, “Eavesdropping on fine-grained user activities within smartphone apps over encrypted network traffic,” in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.
- [105] R. C. Kroeze and P. T. Krein, “Electrical battery model for use in dynamic electric vehicle simulations,” in *2008 IEEE Power Electronics Specialists Conference*, 2008, pp. 1336–1342.
- [106] G. Saldaña, J. I. San Martín, I. Zamora, F. J. Asensio, and O. Oñederra, “Analysis of the current electric battery models for electric vehicle simulation,” *Energies*, vol. 12, no. 14, p. 2750, 2019.
- [107] M. Chen and G. Rincon-Mora, “Accurate electrical battery model capable of predicting runtime and i-v performance,” *IEEE Transactions on Energy Conversion*, vol. 21, no. 2, pp. 504–511, 2006.



systems.

**Alessandro Brighente** is assistant professor at the University of Padova. He was visiting researcher at Nokia Bell Labs, Stuttgart, Germany in 2019 and University of Washington, Seattle, USA, in 2022. He served as TPC for several conferences, including Globecom, VTC, and WWW. He is guest editor for IEEE Transactions on Industrial Informatics and program chair of DevSecOpsRA, co-located with EuroS&P. His current research interests include security and privacy in cyber-physical systems, vehicular networks, blockchain, and communication



**Mauro Conti** is Full Professor at the University of Padua, Italy. He is also affiliated with TU Delft and University of Washington, Seattle. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of Security and Privacy. In this area, he published more than 400 papers in topmost international peer-reviewed journals and conferences. He is Area Editor-in-Chief for IEEE Communications Surveys & Tutorials, and has been Associate Editor for several journals, including IEEE Communications Surveys & Tutorials, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, ACNS 2020, and General Chair for SecureComm 2012, SACMAT 2013, CANS 2021, and ACNS 2022. He is Senior Member of the IEEE and ACM. He is a member of the Blockchain Expert Panel of the Italian Government. He is Fellow of the Young Academy of Europe.



**Denis Donadel** received his MSc in Telecommunication Engineering from the University of Padua, Italy, in 2020. He is now a Ph.D. Student in Brain, Mind and Computer Science (BMCS) at the University of Padua where he joined the SPRITZ Security and Privacy Research Group under the supervision of Prof. Mauro Conti. Together with his academic course, Denis is also working with Omitech SRL as part of his high apprenticeship program. During the 2021 Summer, he was granted the New Generation Internet (NGI) Explorers grant to support a collaboration with the University of Washington (Seattle, USA). His research interests lie primarily in Cyber-Physical Systems security, focusing particularly on Vehicles Security and Critical Infrastructures Security.

- [108] ———, “A survey of physical-layer authentication in wireless communications,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2020.
- [109] Z. Zhang, K. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” *IEEE Transactions on Power Electronics*, vol. 30, no. 9, pp. 5237–5246, 2014.
- [110] H. Hwang, G. Jung, K. Sohn, and S. Park, “A study on mitm (man in the middle) vulnerability in wireless network using 802.1 x and eap,” in *2008 International Conference on Information Science and Security (ICISS 2008)*. IEEE, 2008, pp. 164–170.
- [111] L. Y. Paul, J. S. Baras, and B. M. Sadler, “Physical-layer authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.
- [112] A. La Cour, K. Afzadi, and G. E. Suh, “Wireless charging power side-channel attacks,” *arXiv preprint arXiv:2105.12266*, 2021.
- [113] B. Saltafornaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, and J. Qian, “Eavesdropping on fine-grained user activities within smartphone apps over encrypted network traffic,” in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.
- [114] R. C. Kroeze and P. T. Krein, “Electrical battery model for use in dynamic electric vehicle simulations,” in *2008 IEEE Power Electronics Specialists Conference*, 2008, pp. 1336–1342.
- [115] G. Saldaña, J. I. San Martín, I. Zamora, F. J. Asensio, and O. Oñederra, “Analysis of the current electric battery models for electric vehicle simulation,” *Energies*, vol. 12, no. 14, p. 2750, 2019.
- [116] M. Chen and G. Rincon-Mora, “Accurate electrical battery model capable of predicting runtime and i-v performance,” *IEEE Transactions on Energy Conversion*, vol. 21, no. 2, pp. 504–511, 2006.



**Radha Poovendran** is Professor of the Department of Electrical & Computer Engineering at the University of Washington. He is the founding director of the Network Security Lab and is a founding member and associate director of research for the UW's Center for Excellence in Information Assurance Research and Education. He has also been a member of the advisory boards for Information Security Education and Networking Education Outreach at UW.

In collaboration with NSF, he served as the chair and principal investigator for a Visioning Workshop on Smart and Connected Communities Research and Education in 2016. Poovendran's research focuses on wireless and sensor network security, adversarial modeling, privacy and anonymity in public wireless networks and cyber-physical systems security. He co-authored a book titled Submodularity in Dynamics and Control of Networked Systems and co-edited a book titled Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks. Poovendran is a Fellow of IEEE and has received various awards including Distinguished Alumni Award, ECE Department, University of Maryland, College Park, 2016; NSA LUCITE Rising Star 1999; NSF CAREER 2001; ARO YIP 2002; ONR YIP 2004; PECASE 2005; and Kavli Fellow of the National Academy of Sciences 2007.



**Federico Turrin** received the Master's Degree in Computer Engineering from the University of Padova, Italy, in 2019, where he is currently pursuing the interdisciplinary Ph.D. in Brain, Mind, and Computer science, since October 2019. He has been visiting researcher at SUTD Singapore in 2022. His research interests lie primarily in Cyber-Physical System Security with a particular focus on Industrial Control Systems Security, Vehicles Security, and Anomaly detection.



**Jianying Zhou** is a professor and co-center director for iTrust at Singapore University of Technology and Design (SUTD). He received PhD in Information Security from Royal Holloway, University of London. His research interests are in applied cryptography and network security, cyber-physical system security, mobile and wireless security. He has published 300 referred papers at international conferences and journals with 13,000 citations, and received ESORICS'15 best paper award. He has 2 technologies being standardized in ISO/IEC 29192-4

and ISO/IEC 20009-4, respectively. He is a co-founder & steering committee co-chair of ACNS. He is also steering committee chair of ACM AsiaCCS, and steering committee member of Asiacrypt. He has served 200 times in international cyber security conference committees (ACM CCS & AsiaCCS, IEEE CSF, ESORICS, RAID, ACNS, Asiacrypt, FC, PKC etc.) as general chair, program chair, and PC member. He has also been in the editorial board of top cyber security journals including IEEE Security & Privacy, IEEE TDSC, IEEE TIFS, Computers & Security. He is an ACM Distinguished Member. He received the ESORICS Outstanding Contribution Award in 2020, in recognition of contributions to the community.