Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges and Future Visions

Jin Ye, *Senior Member, IEEE,* Lulu Guo, Bowen Yang, Fangyu Li, *Member, IEEE,* Liang Du, *Senior Member, IEEE,* Le Guan, and Wenzhan Song, *Senior Member, IEEE,*

***Abstract*—Power electronics systems have become increasingly vulnerable to cyber-physical threats due to their growing penetration in Internet of Things (IoT) enabled applications, including connected electric vehicles (EVs). In response to this emerging need, a cyber-physical-security initiative was recently launched by the IEEE power electronics society (PELS). With increasing connectivity due to Vehicle-to-everything (V2X) and the number of electronic control units, connected electric vehicles are facing greater cyber-physical security challenges. However, existing research extensively focuses on the network security of internal combustion engine vehicles and fails to address the cyber-physical security of EVs specifically. In this paper, the challenges and future visions of cyber-physical security are discussed for connected electric vehicles from the perspective of firmware security, vehicle charging safety, and powertrain control security. The vulnerabilities of EVs are investigated under a variety of cyber-attacks, ranging from energy-efficiency-motivated attacks to safety-motivated attacks. Simulation results, including hardware-in-the-loop (HIL) results, are provided to further analyze the cyber-attack impacts on both converter (device) and vehicle (system) levels. More importantly, an architecture for the next-generation power electronics systems is proposed to address the cyber-physical security challenges of EVs. Finally, potential research opportunities are discussed in detail, including detection and migration for firmware security, model-based, and data-driven detection and mitigation. To the best of our knowledge, this is the first comprehensive study on cyber-physical security of powertrain systems in modern EVs.**

***Index Terms*—Cyber-physical security, Modern electric vehicles, Powertrain systems, Firmware security, Vehicle-to-grid security**

I. Introduction

WITH the growing penetration in IoT enabled applications, e.g., electric vehicles (EVs), power electronics systems are becoming more vulnerable to cyber-physical threats ranging from cyber-attacks to physical faults. Meanwhile, due to the lack of cyber awareness in the power electronics community, it becomes more urgent to develop monitoring and diagnosis strategies for networked power electronics systems. For many safety-critical applications, if these threats are not detected at the early stage, they can lead to a catastrophic failure and substantial economic loss. In response to this emerging need, a PELS cyber-physical-security initiative was recently launched by the IEEE power electronics society (PELS), and the first IEEE Power Electronics Security Workshop (Cyber PELS) was held in April 2019.

While cyber-physical security of power electronics systems is an emerging area, vehicle security has been actively studied from information/network security aspects over the past few years [1], because of the enormous number of electronics and software that rely on environmental sensors and networks. For example, the traffic, road, and environmental information has been widely used in both academia and industry, which can be obtained from radar, lidar, visual sensors, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-everything (V2X), and dedicated short-range communication [2], [3]. Some examples of cyber-attacks have been demonstrated in literature and reports [4]. In July 2015, two researchers exploited software vulnerabilities in a Cherokee Jeep to remotely take control of safety-critical systems, leading to severe consequences such as disabling brakes and losing control [5]. In [6], researchers were able to hack a Tesla via both Wi-Fi and cellular connection, and in [7], the potential cyber-attacks specific to automated vehicles and their vulnerabilities were investigated. The automotive industry has made significant efforts to design secure modern cars, and several security standards are established, for instance, Society of Automotive Engineers (SAE) J3061, International Organization for Standardization (ISO) 26262, and a committee draft of the “ISO-SAE Approved new Work Item 21434 Road Vehicles - Cybersecurity Engineering” standard. Overview of the recommendations provided by these guidebooks is given in [8]–[10].

Apart from the efforts of automotive industry, researchers in academia have published studies in the last few years, among which the security of in-vehicle networks, especially for the network in connected vehicles, is a well-researched topic [7], [11]. A typical in-vehicle network architecture of a modern vehicle is shown in Fig. 1, which illustrates multiple electronic subsystems. In this architecture, the safety-critical systems (braking system, engine control unit, steering control unit), powertrain control, body and comfort control, in-vehicle info-

Manuscript received XXX, 2020; revised XXX, 2020; accepted XXX, 2020; online XXX, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1946057. (*Corresponding author: Jin Ye.)*

Jin Ye, Lulu Guo, and Bowen Yang are with the Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602, USA (e-mail: jin.ye@uga.edu, lulu.guo@uga.edu, bowen.yang@uga.edu).

Fangyu Li is with the Department of Electrical and Computer Engineering, Kennesaw State University, Marietta, GA 30060, USA (e-mail: fli6@kennesaw.edu).

Liang Du is with the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA 19122, USA (e-mail:ldu@temple.edu).

Le Guan is with the Department of Computer Science, University of Georgia, Athens, GA 30602, USA (e-mail:leguan@uga.edu).

Wenzhan Song is with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602, USA (e-mail: wsong@uga.edu)

tainment, and telematics systems are considered [12]. Based on this architecture, several studies analyzed vehicle cybersecurity and discussed several approaches to defend vehicles against malware attacks. Further, [3], [12]–[15] presented mitigation techniques and solution frameworks to defend modern vehicles against cyber-attacks such as secure onboard diagnostics (OBD-II) port, better firewall, reliable hardware, secure software updates, penetration testing, and code reviews. In addition, some analytics and detection methodologies for in-vehicle network security [16]–[18] and control systems [19], [20] have been studied.

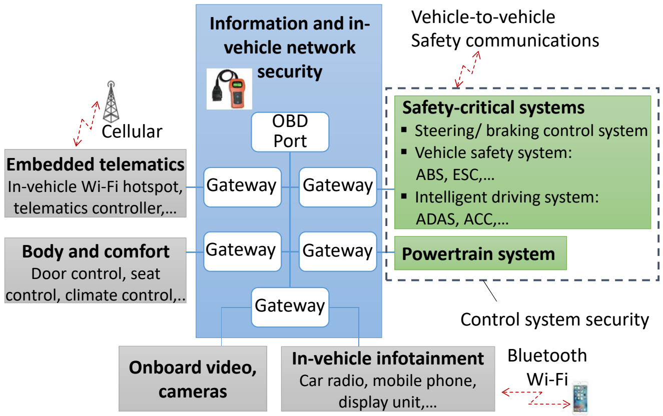

Information and in-vehicle network security
Vehicle-to-vehicle
Safety communications
Cellular
OBD Port
Embedded telematics
In-vehicle Wi-Fi hotspot, telematics controller,...
Gateway
Gateway
Safety-critical systems
Steering/ braking control system
Vehicle safety system: ABS, ESC,...
Intelligent driving system: ADAS, ACC,...
Body and comfort
Door control, seat control, climate control,..
Gateway
Gateway
Powertrain system
Gateway
Control system security
Onboard video, cameras
In-vehicle infotainment
Car radio, mobile phone, display unit,...
Bluetooth
Wi-Fi

Fig. 1: A typical in-vehicle network architecture of modern cars [12], where ABS means antilock brake system; ESC means electronic stability program; ADAS is advanced driver assistance system; ACC is adaptive cruise control.

In recent years, the cyber-physical security of vehicles is gaining interest because the information/network security approach alone cannot guarantee the security of the whole system. The core problem is how to assess, detect, identify, and mitigate such attacks and ensure the safe operation of the vehicles. To address this issue, [21] analyzed the impact of security attack (rear-end collision) on the connected adaptive cruise control (ACC) system. In [22], the stability of the vehicle platoon under jamming attacks was investigated. To defend the vehicles against cyber-attacks, [20] and [23] proposed detection and mitigation strategies to reduce collisions for a vehicle platooning system.

A. Work and Contributions

While the aforementioned studies provide surveys and technical foundations, challenges of cyber-physical security in modern electric vehicles (EVs) remain significant: (1) Most of the existing reviews and studies largely focus on information/network security, and they do not fully address cyber-physical security of vehicle critical control systems. (2) Although several works have been reported concerning automotive control systems (e.g., connected ACC and vehicle platooning), only safety-critical systems are addressed; very few studies focus on cyber-physical security of long-term specifications such as efficiency performance in powertrain systems, which may result in severe degradation of energy efficiency and battery capacity [24], as well as reducing vehicle's monetary value. (3) The existing security studies of internal combustion engine (ICE) vehicles do not specifically address powertrain systems in EVs, namely, energy management system (EMS), battery, and electric drives. With increasing connectivity between EVs, charging stations, and smart grids, EVs are exposed to other serious cyber-threats that do not exist for ICE vehicles. In an ICE vehicle, the control systems, e.g., engine control system, steering system, brake system, transmission system, driver assistance systems like ABS and ESC, are typically distributed. Differently, in an EV, because of the short drive chain and compact drive structure, the control systems in the VCU are more centralized. For example, in four wheel-motor-driven EVs, the torque reference of each motor influence both longitudinal (e.g., regenerative braking system, ABS, and acceleration slip regulation (ASR)) and lateral control performances (e.g., ESC); therefore, controls in an EV are more centralized for coordination between these systems. Then, the more centralized control architecture and higher electrification of EVs will also inevitably expand the attack surfaces and their ultimate impacts, especially on the EMS, battery, and electric drives in powertrain systems.

In this paper, challenges and future visions of the cyber-physical security in powertrain systems are discussed, which to our knowledge, is the first comprehensive study on this area. The main contributions of the paper are as follows:

- For modern EVs, the cyber-physical security of powertrain systems is systematically addressed from aspects of firmware security, vehicle charging safety (vehicle-to-grid (V2G) safety), and powertrain control security.
- The vulnerabilities of EVs are investigated under a variety of cyber-attacks, ranging from energy-efficiency-motivated attacks to safety-motivated attacks. Simulation results, including hardware-in-the-loop (HIL) results, are provided to further analyze the cyber-attack impacts on both converter (device) and vehicle (system) levels.
- An architecture for the next-generation power electronics systems is proposed to address the cyber-physical security challenges of EVs. Potential research opportunities for detection, diagnosis, and mitigation of cyber-attacks are discussed in detail, which will potentially be used in future research on cyber-physical security for modern EVs.

B. Description of the System Architecture

As illustrated in Fig. 2, a modern EV generally includes one or more motors, a battery pack, and other mechanic and electronic components. Unlike a traditional ICE vehicle, the EV is connected to the charging infrastructure that links with the power grid. The powertrain diagram that characterizes longitudinal driving dynamics can be divided into three parts according to their different functions: environmental sensing and perception, upper driver system, and powertrain system. In the environmental sensing and perception part, the vehicle can be available to the extraneous data reflecting the traffic and road conditions by using V2V, V2I, vehicle-to-cloud (V2C), onboard camera, radar, and lidar. Then, the upper driver controller (e.g., auto-driving system or a human driver) provides the torque demand to the powertrain system, which generates the desired

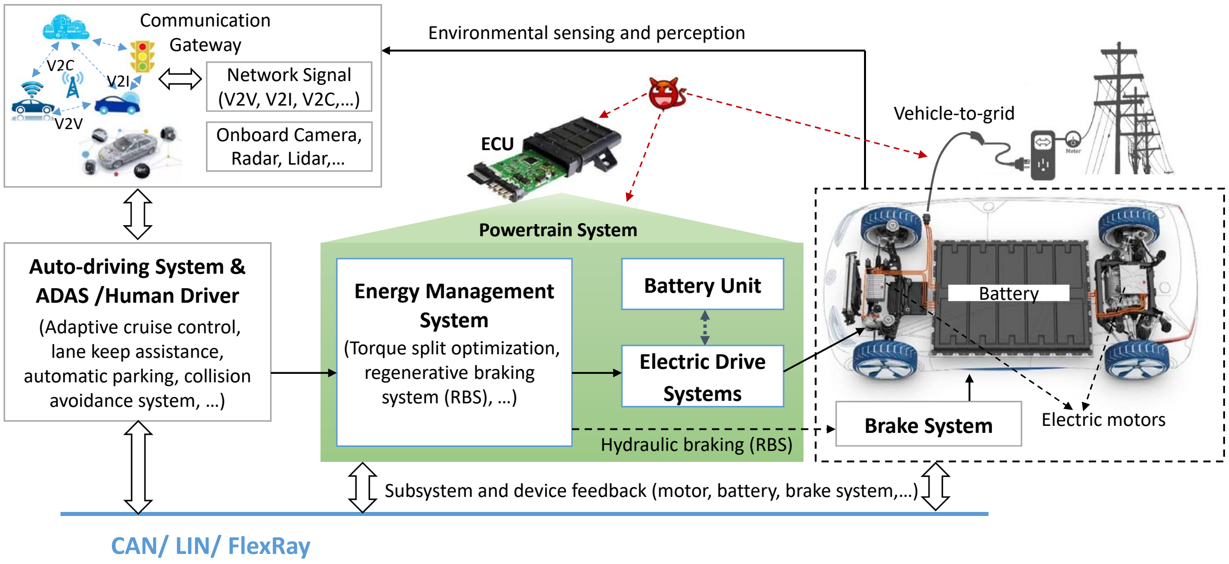

Communication Gateway
V2C
V2I
V2V
Network Signal (V2V, V2I, V2C,...)
Onboard Camera, Radar, Lidar,...
Environmental sensing and perception
ECU
Vehicle-to-grid
Powertrain System
Auto-driving System & ADAS /Human Driver
(Adaptive cruise control, lane keep assistance, automatic parking, collision avoidance system, ...)
Energy Management System
(Torque split optimization, regenerative braking system (RBS), ...)
Battery Unit
Electric Drive Systems
Battery
Brake System
Electric motors
Hydraulic braking (RBS)
Subsystem and device feedback (motor, battery, brake system,...)
CAN/ LIN/ FlexRay

Fig. 2: System diagram of the modern EV.

longitudinal velocity profile under different traffics. All of the signals are transmitted by the high-speed control area network (CAN) buses, local interconnect network (LIN), and FlexRay communication. In the powertrain system, given the total desired torque demand, the EMS focuses on optimizing the torque references (positive or negative values) of each electric drive system (EDS) to maximize the energy efficiency. When considering the brake regenerative control, the brake action is derived by optimizing the electrical and hydraulic braking. When a negative torque is required, the motor works as a generator, and the vehicle's kinetic energy charges the battery during deceleration. In the aspect of hardware, all of the control systems are embedded in the electronic control unit (ECU). For the cyber-physical security study of the EV, it is assumed that the attacker can illegally access the in-vehicle communication buses, arbitrarily modify the sensor measurements, and hijack the powertrain system. In particular, they may also obtain access to the battery through the connection between the battery management system and the charging infrastructure.

As stated above, the vehicle has two lines of defense against invaders. The first one is information security that aims to prevent malicious attacks, e.g., secure hardware, secure communication techniques, firewall, secure software update, etc. Among these security applications, reliable hardware is the most critical. For instance, it can offer secure storage, random number generators, and hardware firewalls. Also, secure micro-controllers and drivers can support real-time control systems and online attack detection, diagnosis, and countermeasures. The second line of defense considers the critical issue: once the car has been attacked, what should we do to assess, detect, and mitigate such attacks and ensure the safe operation of the ECUs? Then, effective detection, diagnosis, and mitigation methodologies should be developed. Therefore, in real-world applications, collaborative efforts should be made from both information and control security perspectives. In the following, we first review the access and taxonomy of cyber-attacks, including cyber-attacks access in terms of firmware security and taxonomy of cyber-attacks in the cyber-physical system. Then, vehicle charging safety in V2G and powertrain control security will be discussed.

II. Preliminary Introduction of Cyber-Attacks

A. Cyber-attack access in terms of firmware security

Perhaps the most well-known vehicle exploit is the 2015 Jeep hack [5]. In this attack, a myriad of common security issues was identified in the in-vehicle infotainment (IVI) system of a Cherokee Jeep. These issues include low-entropy password generation, improper network isolation, lack of access control, and insecure firmware update. This attack is not the first of its kind. Dating back to 2010, researchers have already successfully comprised the GM Onstar Gen8 and the remote telematics system on GM automobiles [25], [26]. They identified a buffer overflow vulnerability, which can be remotely triggered and allows the attackers to penetrate the CAN bus. Nowadays, an average car includes thousands of pieces of hardware on which millions of lines of code run. The greatly enlarged attack surface undoubtedly puts vehicles in danger.

The IVI has been a main target for the attackers. On the one hand, the IVI has direct/indirect access to other ECUs via the CAN bus, which grants the attackers a high return on investment. More specifically, it allows the attackers to directly hijack non-safety and safety-critical functions, including steering or brake systems. On the other hand, the IVI involves multiple components that implement useful features. They inevitably expose more vulnerabilities to cybercriminals. Note that the IVI firmware is usually powered by a full-fledged OS. It is no different from traditional software, which is subject to vulnerabilities, such as buffer overflow, use-after-free, and return-oriented programming attacks. Several attack vectors to the bloated software stack are discussed based on the attacker's required proximity in delivering a malicious input to a particular

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3045667, IEEE Journal of Emerging and Selected Topics in Power Electronics

access vector in the field. To fix a vulnerability, complex in-field update has to be implemented, which itself has become a hot attack target. For clear expression, Table I consolidates the access and taxonomy of cyber-attacks in terms of firmware security. For each attack category, attack prerequisites, the vulnerable interface being targeted, attack approaches, and the consequences will be discussed.

1) Local Attacks: When the attackers have physical access to the car, they could directly or indirectly access the car's internal networks via physical interfaces. For example, there has been work that exploits the firmware of the aftermarket telematics control unit (TCU), which connects to a car via the standard OBD-II port [27]. Since the OBD-II port is connected to the CAN bus directly, insecure firmware of TCUs imposes a disconcerting threat to vehicle security. Researchers from Zingbox used a maliciously crafted USB device to infect the IVI [28]. Once the device is plugged into the car's USB port, the injected malware can then put the IVI system into an unusable state. Using similar methodologies, malformed CD-ROM tracks and multimedia files were used to inject Trojan horses into the car [29].

2) Short-range wireless attacks: Short-range wireless channels include Bluetooth, remote keyless entry, radio frequency identification (RFID), tire pressure monitoring systems (TPMS), WiFi, etc. Crafting a malformed Bluetooth media, the CarsBlues vulnerability allows attackers to steal personally identifiable information (PII) of users who have synced their phones to cars via Bluetooth [30]. By connecting the car to a malicious WiFi hotspot, the attackers could access the CAN bus via the web browser on a Tesla Model S [31]. Since 2008, the U.S. government has mandated that each newly manufactured vehicle needs a TPMS that provides real-time tire pressure diagnosis. However, the wireless communication used by the ECU of the TPMS and other components has been an attack target [25]. The car's remote keyless system has also been compromised. With code grabbers, which is sold at $32 in the dark web, the attackers can intercept the communication between the key and the car.

3) Remote attacks: In the first quarter of 2016, connected cars accounted for a third of all new cellular devices [32]. By 2020, virtually all manufactured vehicles will come with embedded connectivity. The connectivity is enabled by long-range communication channels, including cellular, global positioning system (GPS), satellite radio, digital radio, etc. The ability to use the cellular spectrum as an entry point into the car network provides cybercriminals with unprecedented convenience. Once the attackers have penetrated the internal network via the cellular entry point, more attack sources and surfaces can be reached. This consequence has been clearly demonstrated in the 2015 Jeep hack [5]. In this attack, the attackers first remotely broke into the internal network of the IVI via the 3G cellular access point. Then, as insiders, they reprogrammed the firmware of the V850 chip (gateway ECU to the CAN bus) to get access to the CAN bus eventually. In the 2015 Jeep hack, they could even upload a malicious firmware that directly talks to the CAN bus. At the application level, the insider attackers could exploit a bug in the Just-in-Time engine of the browser render process to cause arbitrary code execution on Tesla Model 3's firmware [33].

B. Cyber-attack modeling in vehicle control systems

Generally speaking, the cyber threats can be categorized into three types based on their different objectives, namely cyber-attacks on confidentiality, integrity, and availability, which are often denoted as CIA triad for carrying out risk assessments on cyber-physical security [34], [35]. In the confidentiality attacks, the malicious attacker attends to obtain the non-disclosure of data, e.g., personal sensitive and private information from unauthorized access. In the second case, the attackers can either physically or remotely gain access to the system or the ECU and generate false signals or modify the system parameters to perform the attack, leading the systems into a dangerous operation region. The cyber-attacks on availability means that timely access to the data or system functionalities is destroyed.

As a cyber-physical control system, the powertrain and power electronic systems in EVs may present similar attack surfaces. Typically, cyber-attacks in a cyber-physical control system can be qualitatively categorized into three types: denial of service (DOS) attacks, replay attacks, and false data injection attacks [51]. Although the three types of cyber-attacks are summarized according to the cybersecurity research in cyber-physical control systems, up to date, they are widely used in vehicle cybersecurity. To clearly express the anomaly of cyber-attacks in vehicle control systems, we summarize the related works in Table II, in which attack setup, attackers' capabilities, and real-world examples are presented. For convenient expression, we consider a general control architecture, which has three components [52]: the plant (physical phenomena of interest including the actuators), sensors to obtain the system outputs y, and control commands u. Let $\widetilde{y}$ and $\widetilde{u}$ represent the compromised sensor measurement and control signal, respectively. The attack duration is denoted as $\mathcal{T}_a = [t_{start}, t_{end}]$, where t_{start} and t_{end} represent the start and end time of attack, respectively. Then, typical mathematical formulas of these three cyber-attacks are described as follows [52], [53].

1) DOS attacks: DOS attack means the attacker sends malicious messages or data with a very high frequency to destroy the traffic condition of the whole communications. The sensor cannot reach the controller in the attack duration, and the control signal does not reach an actuator. Then, a conservative response strategy in real applications is to use the last signal received as the current value, as follows:

$$\widetilde{y}(t) = \begin{cases} y(t), \; t \notin \mathcal{T}_a \\ y(t_{start}), \; t \in \mathcal{T}_a \end{cases} \quad \text{or } \widetilde{u}(t) = \begin{cases} u(t), \; t \notin \mathcal{T}_a \\ u(t_{start}), \; t \in \mathcal{T}_a \end{cases} \tag{1}$$

2) Replay attacks: Replay attack means the attacker records data from original normal conditions during the period of disturbance to fool the operator not to take actions. In equations, a replay attack can be expressed as $\widetilde{y}(t) = \mathbf{Y}$ and $\widetilde{u}(t) = \mathbf{U}$, where $\mathbf{Y}$ and $\mathbf{U}$ represent the recorded set of the past sensor and control signal, respectively.

3) Data injection attacks: Data injection attacks can directly falsify measurements or inject incorrect instructions to the system, which can be expressed in many forms, e.g., scaling and addictive attacks [53], high-frequency harmonics, and periodic

TABLE I: Firmware vulnerability and its impacts.

	Local attacks	Short-range Wireless Attacks	Remote Attacks
Prerequisites	Physical access	Within wireless signal coverage (less than 100m).	
Example interface	OBD-II port, USB port, etc.	Bluetooth, WiFi, RFID, etc.	3G/Long Term Evolution (LTE)/5G, GPS, etc.
Approach	Malicious hardware dongle, malformed media contents, fault injection, etc.	Malformed media contents, signal spoofing, insecure network configuration, etc.	Insecure network configuration, etc.
Consequence	CAN access, firmware reverse engineering, arbitrary code execution, firmware reprogramming, etc.	CAN access, unauthorized car access, PII leak, arbitrary code execution, etc.	CAN access, firmware reprogramming, arbitrary code execution, etc.

TABLE II: Vulnerability and impacts of cyber-attacks on vehicles.

Attack Setup	Targeting System	Attacker Capabilities	Real-word Examples
DOS attack	Cooperative cruise control (CCC) [19], [21], internal vehicle networks [15], [36].	The attacker has no priori knowledge.	Distributed DOS attacks on Amazon web services in 2020, Six Banks in 2012, and GitHub in 2018 [37].
Replay attack	Linear control system [38], CCC [21], [39], operator-vehicle network [40], internal vehicle networks [41].	The attacker has no priori knowledge but has resources to record and manipulate data in the system.	
Data injection attack	Electric drives in EVs [42], energy management system in EVs [43], linear control system [44].	The attacker has limited system knowledge [45], [46] or full system knowledge [34], [47].	Hackers remotely control a Jeep in July 2015 [5]. Cyber-attacks on Tesla [6].
Stealthy attack	EV battery system [48], supervisory control and data acquisition (SCADA) system [49], smart grid [50].	The attacker has full system knowledge and can access to all sensor and actuator channels.	

pulse injection [42]. If the attacker has no prior knowledge of the system, the data injection attacks can be designed by mixing the original value with a malicious factor, as

$$\widetilde{y}(t) = \begin{cases} y(t),\ t \notin \mathcal{T}_a \\ \nu y(t) + \epsilon,\ t \in \mathcal{T}_a \end{cases} \quad \text{or } \widetilde{u}(t) = \begin{cases} u(t),\ t \notin \mathcal{T}_a \\ \nu u(t) + \epsilon,\ t \in \mathcal{T}_a \end{cases} \tag{2}$$

Here, ν and ϵ are unknown signals due to the malicious modification of the signals, for instance, white noise, periodic function, periodic pulse injection, constant value, etc. If an attacker is highly-skilled and has sufficient knowledge of the system, sophisticated and stealthy data injection attacks can be created. These cyber-attacks would constantly affect the system operation while being undetected. For example, in [38], a stealthy cyber-attack was presented, which could remain undetectable to the exploited detector (χ^2-detector based on Kalman filters). In [50], based on the robust extended Kalman filter, a real-time detection for false data injection attacks was proposed. In [54], the authors designed an artificial linear control system, generating a sequence of data injection to sensors that pass the state estimator and statistical fault detector. In general, these kinds of stealthy attacks are based on a linear control model. The difference vectors between normal and compromised systems are functions of the attack sequence of the artificial linear control system. The main objective of the attacker is to maximize the estimation error without triggering the alarm while increasing the system states to infinity [54].

Besides the aforementioned cyber-attack modeling, there are some potential cyber-attacks specific to powertrain and power electronic systems in EVs. These cyber-attacks are generated based on their specific attack targets. For example, the battery-drain attacks are studied in [48], [55], in which the cyber-attacks are conducted to deteriorate the power capability of battery packs. On the one hand, to over-discharge the battery cells, cyber-attacks are designed by using wake-up functions - let the adversary wake up ECUs. On the other hand, a compromised BMS can modify the upper cut-off voltage to realize overcharge - higher charging voltage. Both of the two scenarios would lead to permanent physical damage to the battery packs. For the powertrain system, the authors in [56] demonstrated some potential cyber-attacks aiming at misleading the powertrain control system. For example, an attacker may inform the ECU not to charge the battery when it needs to be charged. Also, through GPS deception, the malicious attack may provide the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3045667, IEEE Journal of Emerging and Selected Topics in Power Electronics

powertrain control system with false information about its location and some other GPS information, which may cause wrong battery consumption prediction and over-discharge of the battery. For the cybersecurity of power electronic systems in EVs, authors in [57] demonstrated the cybersecurity challenges related to power electronic systems. In this study, a spoofing attack aims to modify a signal in the system before quantization and a man-in-the-middle attack can be duplicated by changing the quantized data transmitted by the sensors. In [42], [58], the impact analysis of various data integrity attacks on power electronics and electric drives are analyzed. Overall, up to date, little research work on power electronics security in EVs has been published. For a more detailed discussion on potential cyber-attacks on modern vehicles, please refer to surveys in [13], [34], [59].

III. Vehicle Charging Security

The impacts of large-scale, light-duty EVs charging demand on distribution networks have been well studied. In general, charging demands of light-duty EVs [60] have been considered as active loads through V2G, grid-to-vehicle (G2V), and vehicle-to-building (V2B) modes [61]. It has been well studied and widely acknowledged that charging EVs in an uncontrolled manner could cause reliability issues and negative effects on power grids [62]–[64]. However, the proliferation of electrified, heavy-duty transit buses [65], [66] brings new challenges to power grids as they are operated with high power and high volatility. A major challenge to accurately investigate the impact of cyber-attacks is the lack of real-time, spatial-temporal models to represent the interaction among a large volume of EVs, traffic and driving patterns, and geographically spread charging infrastructures. Furthermore, the size and potential caused by the charging demands of electrified bus fleets are often overlooked. Most major public transportation systems worldwide have announced strategic plans for 100% electric bus fleets in the near future. Moreover, electric buses consume much more power than light-duty EVs due to their size, weight, and loading. For instance, a state-of-the-art Proterra electric bus can be charged at 500 kW. Therefore, the overall charging profile of bus fleets would be high pulsed, and volatile [67]. To summarize, the potential impact of both light-duty EVs and electrified bus fleets with vulnerable powertrain systems on power grids can be summarized as the following two categories.

First, power grids are being operated with inaccurate charging demand models, as almost all state-of-the-art models are based on certain assumptions [68]. For instance, the starting time, initial battery state-of-the-charge, and charging period for EVs in commercial buildings are represented by the normal, log-normal, and truncated normal distributions, respectively [62]. However, it is questionable whether these location-data-driven assumptions can be applied in general to other regions. Therefore, recent efforts have been devoted to identify real-time EV charging profiles [68]–[72]. Furthermore, it is shown that, assuming light-duty EVs are subject to 11-kW charging and tested on Denmark distribution network data, uncontrolled and altering charging demands [73], [74] could cause local voltage unbalances and also trigger grid component overloading [75]. A proof-of-concept demonstration was provided using public sources from New York City has shown that aggregated EVs could be controlled to launch cyber-attacks on the power grid via malicious demand variations [76]. Coordinated attacks on either the cyber or the physical layer could propagate to infect other components and cause cascading effects. The above-discussed literature focuses on coordinated cyber-attacks through altering demand caused by vulnerable charging infrastructures, i.e., V2G and G2V applications. It is worth noting that, if instead powertrain systems are malicious, EVs could also cause similar risks to power grid stability under V2G settings. Furthermore, being operated with much higher wattage levels, heavy-duty electrified transportation fleets could significantly amplify the impact of pulsed charging needs and cause unexpected grid stability issues.

Furthermore, existing EV demand models also do not effectively incorporate traffic models and driver behaviors [75]. If powertrain systems are under cyber-attacks, power grids could encounter greater vulnerabilities due to coupled transportation-power systems. The intrinsic characteristics of transportation systems such as traffic nonlinearities, congestion, instabilities, road capacity, as well as special events like extreme weather or sporting events, could dramatically influence EV travel patterns, and in turn, further impact spatial and temporal distributions of the power grid charging demand profiles. As a demonstration example, if a fleet of combined light-duty EVs and electric buses are under cyber-attacks and break down during peak hours due to powertrain failures, they could induce designed traffic jams and reshape the forecasted load profiles. For instance, a wide area of the residential area could be delayed or cause significant spikes, leading to overloading and voltage stability issues.

A proof-of-concept simulation was conducted by the authors on a 50 km, 4-lane highway with a peak density of 533 vehicles per mile in Orange County, California. With 50% of light-duty EV penetration on the highway (which can be equivalent to fewer EVs with some electric buses), the simulation results showed that several EVs under control could induce a significant traffic jam and cause more EVs to reach their lowest battery state-of-the-charge. In turn, those EVs arrive destination late with an immediate need to recharge. A five-fold increase (4 MW to 20 MW) in total power demand was observed, and a seven-fold increase (0.19 MW/km to 1.4 MW/km) in local peak demand relative to the baseline profile was also a significant threat to power grid stability.

IV. Powertrain Control Security

As shown in Fig. 3, the powertrain control security involves system- and device-level security that directly impacts the functionality and safety of the vehicles. The system-level EMS is usually denoted as the ”Cyber” part, which focuses on the overall performance of the EV, for instance, energy efficiency and battery management. In the device-level EDS, the motor controller and the actuator (plant) are considered as the ”Cyber” and ”Physical” part, respectively. In general, the control period of the system level is 10-20 milliseconds, and the control period of the device-level EDS is usually 0.1 milliseconds or less.

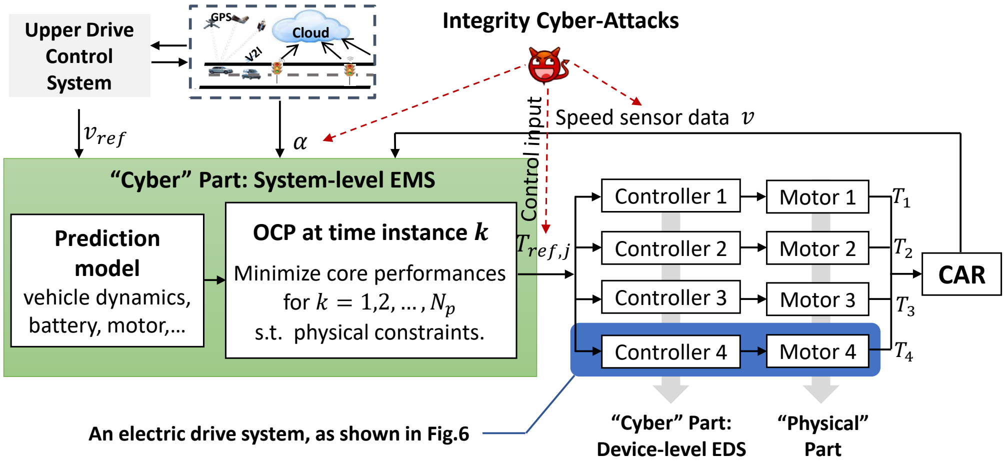


Fig. 3: Diagram of the powertrain control system.

A. *System-level Cybersecurity of EMS*

1) System description: As shown in Fig. 3, the EMS is developed by optimizing the brake, torque, and battery power to maximize energy efficiency while satisfying the desired dynamic performance, e.g., velocity reference, total wheel torque. To observe the impact of the cyber-attacks on EMS, a predictive EMS under the framework of the model predictive control (MPC) is developed. A detailed description of the controller is given in the Appendix.

2) Attack modeling and definition: Different from the safety-critical systems, cyber-attacks on EMS usually impact energy consumption only. Thus, the driver can hardly notice the attack. In this subsection, for a better understanding of cyber-physical security, some preliminary results of cyber-attacks on the EMS are presented. Based on the MPC-based EMS, Fig. 3 shows the potential cyber-attack locations and signals. The cyber-attacks may occur in different locations, including sensor measurements (vehicle speed v and road slope α) and control inputs (torque reference of the jth motor, marked as $T_{ref,j}$). As a case study, we firstly consider the continuous data injection attacks on $T_{ref,j}$. The compromised torque reference that will be used by the motor drive is expressed as

$$T^{atk}_{ref,j} = \nu T_{ref,j} + \epsilon, \tag{3}$$

where ϵ and ν are unknown signals due to the malicious modification; $T_{ref,j}$ denotes the actual signal. Without loss of generality, we set $j = 2$, which means that the second motor is compromised. Four attack scenarios (marked as Cases 1-4) are defined as $\nu = \{-0.5, 0.5, 1.5, 2\}$ ($\epsilon = 0$), respectively; the other four cases (marked as Cases 5-8) are defined as $\epsilon \in \{\pm 0.2T_{\max}, \pm 0.4T_{\max}\}$ ($\nu = 1$), respectively. Here $T_{\max}$ is set to 400Nm.

In addition to the effect on energy efficiency, cyber-attacks on the powertrain system may also degrade the dynamic performance. Based on the developed EMS in the above, four data injection attacks targeting v (marked as Cases v-1 and v-2) are designed, expressed as $v^{atk} = \nu_v v$, where v^{atk} denotes the compromised speed, and $\nu_v \in \{0.8, 1.2\}$.

3) Simulation setup: The simulation is conducted under two typical long-term driving cycles - New European Driving Cycle (NEDC) and Urban Dynamometer Driving Schedule (UDDS), which are widely used in literature [77]–[81]. In [78], under different driving cycles, trajectories, and optimization algorithms of EMSs in electric vehicles (including hybrid electric vehicles and battery electric vehicles) were summarized. Although the real driving scenarios are often more complex, these standardized driving cycles can serve as examples for practical driving tests, as discussed in [79].

4) Results and impact analysis: The results of system performance are presented in Fig. 4, including velocity tracking and energy consumption, which illustrate that despite the compromised torque reference of jth motor, the system presents a similar dynamic performance in terms of speed tracking. This implies that those efficient-goal-oriented attacks (e.g., cyber-attacks in $T_{ref,j}$) can cause significant efficiency degradation while not affecting driving tasks. Based on the comparison between the energy consumption profiles, the cyber-attacks exhibit different effects on energy efficiency. When a reverse command ($\nu < 0$) is input to the objecting motor, e.g., attack case 1, the energy efficiency would be reduced over 20%. This significant reduction of energy efficiency is likely to occur in practical applications. For example, when the initial command of the targeted motor is to drive the car by providing positive torque, and a compromised torque reference makes it constantly work as a generator, then the other motors need to output more power to fulfill the required wheel torque. In such a case, compared to the normal conditions, the extra power will be wasted. Although the negative power from the jth motor can recharge the battery, the energy loss due to the internal resistance and other losses in the motor cannot be ignored. Besides the negative-ν-attack, other false data injection attacks with various definitions of ϵ and positive ν may also lead to higher energy consumption (up to 10%), causing a considerable energy loss in the long term. Therefore, unlike the cyber-attacks on life-critical systems, such as driver assistance systems (e.g., ESC), cyber-attacks that deteriorate system efficiency also require attention and further investigation. From the results in

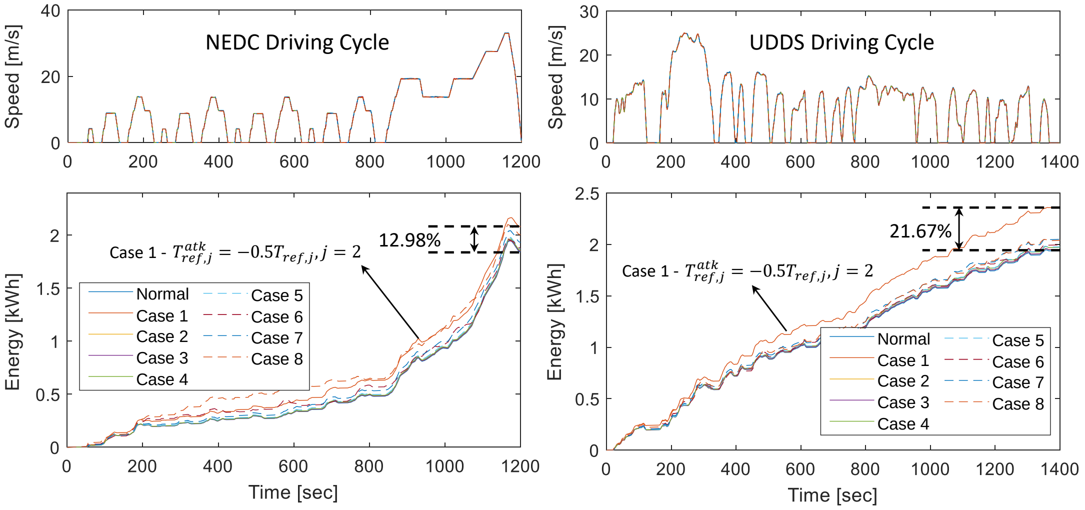


Fig. 4: Impact of cyber-attacks on $T_{ref,j}$ under NEDC and UDDS driving cycles.

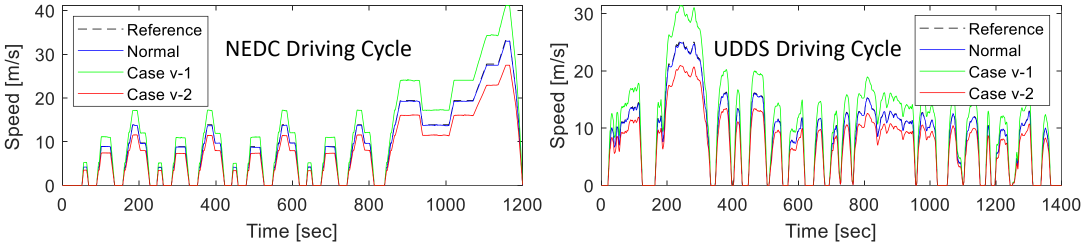


Fig. 5: Impact of cyber-attacks on v under NEDC and UDDS driving cycles.

Fig. 5, it can be seen that cyber-attacks on v may significantly affect the tracking accuracy. In real-world applications, the larger tracking error will lead to poor dynamic performance.

B. Device-level Cybersecurity of EDSs

1) System description: As mentioned earlier, at the device level, the function of an EDS is to track the torque commands given by the system-level controller. Fig. 6 shows the cyber-physical diagram of a typical EDS, wherein the physical systems (DC supply, power converter, electric machine) are denoted in blue, and the cyber systems are denoted in red. According to the feedback signals gathered from sensors and torque command from the system-level controller, the local controller calculates the duty cycles needed for pulse width modulation signals (PWM), which then drive the power converter through a gate driver.

2) Attack modeling and definition: In the traditional EDS, the communication to the external systems is limited; thus, the traditional EDS is hardly targeted by the cyber-attacks, and the physical faults are the primary concerns. For example, as shown in Fig. 6, three types of common physical faults are denoted in yellow: mechanical faults (fault A), open-circuit faults in power electronics (fault B), and machine winding inter-turn short circuit faults (fault C). In the past decades, the physical faults of the EDS and related components and devices are widely studied. In [82], [83], some of the research outcomes and progress of EDS condition monitoring and fault diagnosis were reviewed, such as inter-turn short circuit fault detection in the electric machines and open circuit fault diagnosis in power electronics modules.

However, with the increasing computational capability of the digital signal processors (DSP) and micro control units (MCU), and the development of the communication network techniques, local controllers can achieve advanced functionalities, such as online optimization, fault diagnosis, and multi-mode operations. Such functions require the modern EDS to communicate more frequently with the onboard networks than ever, making the EDS much more vulnerable to malicious attacks from the cyber systems. In Fig. 6, some common attacks are denoted by red attack vectors. Attack A represents the sensor attacks, in which the attacker could fabricate false sensor signals or block the communication between sensors and estimators. Attack B represents the estimator attacks or observer attacks, in which the attacker could use false signals or parameters to modify the estimator. Attack C denotes the local controller attacks, in which the attacker could manipulate the controller parameters or directly modify the control commands to the gate drivers. Besides, data injection attacks targeting the EDS controller parameters could also lead to system instability. Meanwhile, a series of false current reference injected to the current controller could make the EDS operate at deteriorated efficiency without being detected, which will largely reduce the vehicle cruising capability. Also, introducing random delay to the feedback signals could cause a large ripple in the output torque and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3045667, IEEE Journal of Emerging and Selected Topics in Power Electronics

current, which eventually could shorten the battery and machine life.

As a case study, several replay and false data injection attacks on i_a (see Attack A in Fig. 6) in an interior permanent magnet synchronous machine (IPMSM) are conducted. The false data injection attacks are expressed as $i_a^{atk} = \nu_i i_a$, where $\nu \in \{1.2, -0.75\}$. Then, three replay attacks are defined with different attack start timings, denoted as $t^{atk} \in \{72, 103, 181\}$s, wherein the recording time horizon is set to five seconds.

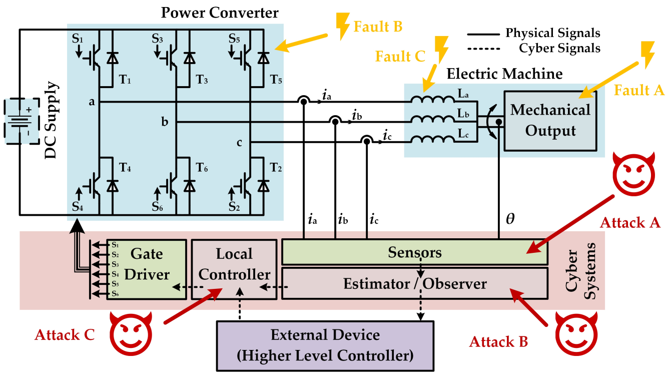


Fig. 6: Diagram of a general electric drive system.

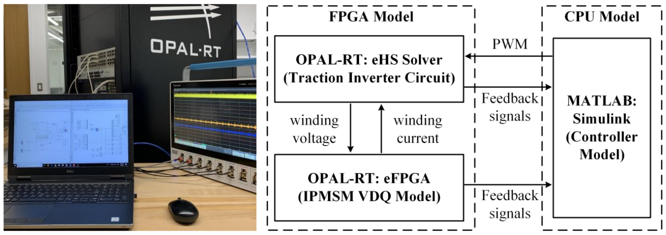

OPAL-RT
FPGA Model
CPU Model
OPAL-RT: eHS Solver (Traction Inverter Circuit)
PWM
Feedback signals
MATLAB: Simulink (Controller Model)
winding voltage
winding current
OPAL-RT: eFPGA (IPMSM VDQ Model)
Feedback signals

Fig. 7: OPAL-RT hardware-in-the-loop (HIL) real-time simulation testbed.

3) Simulation setup: The simulation is conducted under a high-fidelity EV powertrain model in a real-time hardware-in-the-loop (HIL) testbed (OPAL-RT OP5700), as shown in Fig. 7. In this testbed, a detailed model of the motor (IPMSM) and vehicle dynamics are included. The sampling time is set to 25μs.

4) Results and impact analysis: The results in Fig. 8 demonstrate that the compromised i_a may cause a larger tracking error of the motor. Notably, in replay attack scenarios, the torque increases dramatically once the cyber-attacks are activated. From the perspective of the longitudinal performance in powertrain, despite the short attack period, this transient degradation in performance of torque tracking may further cause unexpected jerk of the vehicle body, significantly reducing the driving comfortability. From the lateral performance aspect, if the attack occurs on a curve road segment, the higher tracking error may also lead to lateral instability.

From the attacker's perspective, once the EDS is compromised, the attacker's benefits could be summarized in three categories: safety, economy, and information.

- **Safety:** a malicious attacker could simply aim at causing some damages to the systems. For example, it could increase the current reference in the current control loop or modify the duty cycle from the controller output so that the power converter will be overcharged and eventually damaged.
- **Economic:** a profit-driven attacker could anticipate gaining economic benefits from the attacks. For example, a charging station operator could intrude into the electric drive systems through the charging station and inject some false data into the sensors or estimators. This kind of cyber-attacks will cause higher current harmonics and eventually lead to higher energy loss in the traction inverters. In such a case, the vehicle's cruise range will be reduced, and the customers will have to recharge their vehicles more frequently. Then the operator will gain more money.
- **Information:** some attackers also intend to steal the system information so that they could either intercept the technological property or invade customers' privacy. For example, the attack could be deployed to the estimators, where system operation data will be calculated and sent to external devices.

5) Preliminary discussion on distinguishing between malicious cyber-attacks and physical faults: When it comes to cybersecurity, a broad concern is how to distinguish between malicious cyber-attacks and physical faults. One of the possible fault situations in the powertrain system is motor failures, leading to misbehavior during driving. To observe the difference between malicious cyber-attacks and physical faults, several fault scenarios are presented in Fig. 9. Results of a cyber-attack are also given for comparison. In this figure, physical faults 1 to 3 represent winding grounded short circuit fault on phase A, phase A & B, and phase A & B & C, respectively. Physical fault 4 represents an open circuit fault in upper switch of phase A. Overall speaking, the D-axis current profiles have severe distortion and oscillation for both cyber-attacks and physical faults, but the frequency of the oscillation is different. While the oscillation and distortion patterns due to cyber-attacks are considerably random, the ones due to physical faults show specific regular variation because faults often have a fixed physical model, such as short circuit faults. In particular, we can see that despite the physical faults, the i_d still presents a fixed frequency characteristic. For one type of physical faults, the amplitude is related to the physical parameters of that fault. This feature may provide a guideline to distinguish the cyber-attacks and physical faults. Moreover, for those physical faults causing gradual performance degradation, such as increasing internal resistance, specific physic characteristics should be utilized to address the long-term abnormal behavior. This kind of persistent rule of performance degradation may also be used to distinguish faults from cyber-attacks.

V. Detection and Mitigation Opportunities and Future Visions

To design secure power electronics systems and overcome the issues related to cyber-physical security, this section presents a cyber-secure architecture of next-generation power electronics systems for EVs, considering both hardware and software aspects. The proposed architecture, as shown in Fig. 10, will

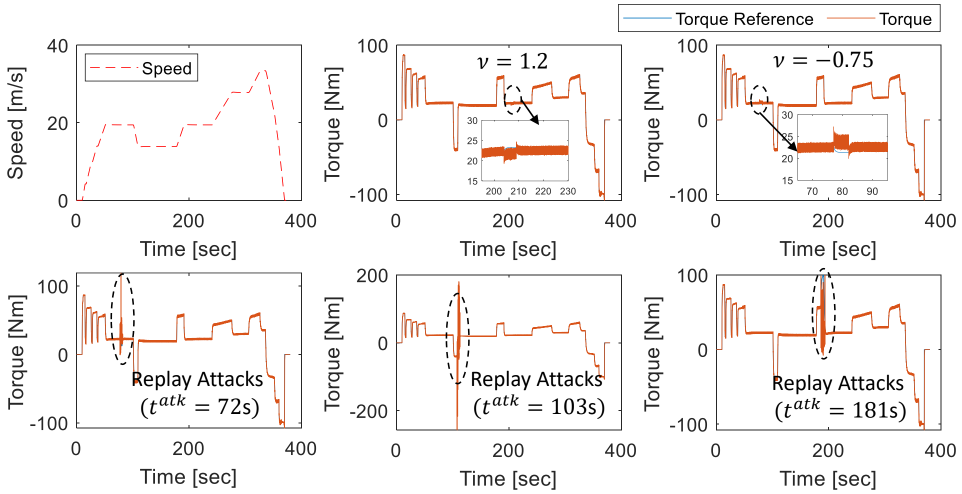


Fig. 8: Impact of cyber-attacks on i_a in an IPMSM under the OPAL-RT HIL testbed.

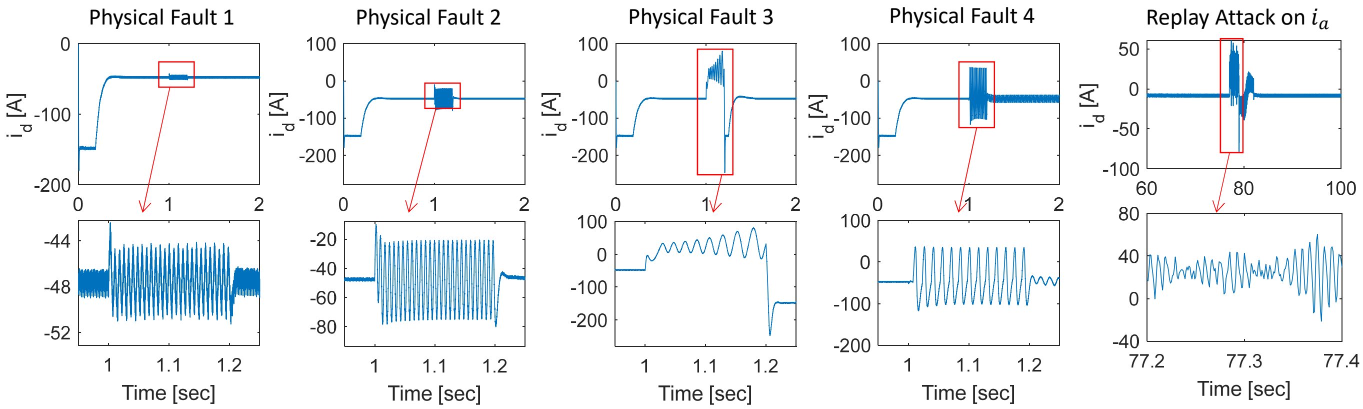


Fig. 9: Comparison between malicious cyber-attacks and physical faults.

provide a cyber-secure solution to the next generation of power electronics systems at the design and operation stage. More importantly, this architecture will focus on both device and system levels, aiming to monitor the vehicle system real-time. Corresponding detection, diagnosis, and mitigation algorithms will be designed and then discussed in subsections V.B and V.C in order to improve the security and resilience of connected electric vehicles.

At both the device and system levels, each controller module includes a primary microcontroller (MC) and a secondary MC. In the recent paper [84], the authors presented a comprehensive review of the state-of-the-art traction inverter designs from several leading automotive manufacturers. In most autonomous applications, only one microcontroller, such as DSP, is included on a dedicated control board within the inverter [85], for instance, traction inverters in Audi MY2016 A3 e-Tron [86] and Nissan MY2012 LEAF [87]. Although in certain vehicles, such as BMW MY2016 i3 [84], two DSPs are used in the control board within the traction inverter, the secondary DSP is not used for security purpose. Unlike the current design methodologies, the proposed cyber-secure architecture introduces and encrypts a secondary MC through a firmware security module to provide extra security. In normal cases, the converter is controlled by the primary controller, while the monitoring systems, including cyber-attack detection and diagnosis algorithms, are integrated into the secondary microcontroller. Once a cyber-attack is identified and the compromised signal is diagnosed, a resilient control algorithm in the secondary microcontroller would be used to replace the primary microcontroller and recover the system from cyber-attacks at the early stage.

At the device level, both primary and secondary microcontrollers can receive sensor feedback signals from the converters, such as phase current and position/speed of the electric machines, and provide a control command to the converter when necessary. At the system level, besides the critical signals in the powertrain system, the secondary microcontroller also collects the sensor measurements and monitoring states of each device (denoted as MC #1, MC #2, ..., MC #N) to identify the presence of the cyber-attacks. It should be noted that Fig. 10 only shows the diagram of the cyber-secure architecture. In real-time applications, this cyber-secure architecture is more complicated. Besides the two microcontrollers, some other devices need to be used. For a detailed discussion on the validation of this dual-microcontroller design methodology, please refer to the literature [88], which provided a cyber-secure power router prototype and results of switching between the

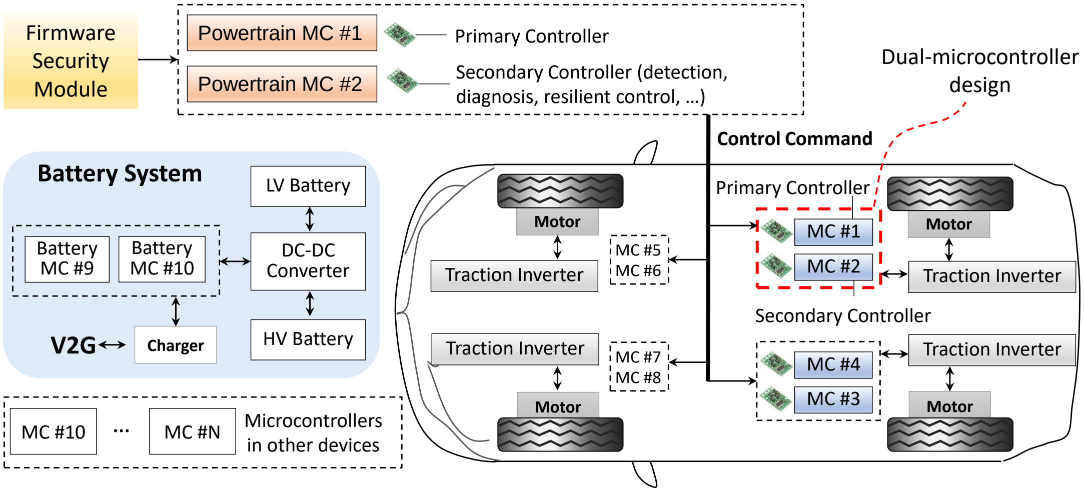


Fig. 10: Diagram of the cyber-secure architecture of next generation power electronics systems for EVs.

primary and secondary microcontrollers.

Cyber-attack detection methods, including data- and physics-based that will be discussed in subsection V.B and V.C, can be used to detect and diagnose cyber-attacks in connected electric vehicles. Through dual microcontroller systems, mitigation algorithms can be applied to improve the resilience and recovery of the powertrain system in an EV once the cyber-attack occurs.

A. Detection and Mitigation for Firmware Security

The software bug is a major source of vehicle hacking. As more vehicles are connected to the Internet, we should expect to see more software attacks. To prevent, detect, and mitigate attacks targeting connected vehicles, multi-layered, autonomous defense systems should be designed.

First, in-house software testing should be extensively applied to mission-critical firmware. Combined with memory checker [89], taint analysis [90] and symbolic execution [91], [92], traditional software bugs such as buffer overflow, use-after-free, double-free, integer error, etc. could be eliminated in the first place.

Second, the state-of-the-art advances in a programming language should be incorporated in software development. In the short term, using more secure programming languages such as RUST [93] is a tangible way of improving code quality. In the long term, OEMs should employ formal verification to prove the security of the released firmware [94] theoretically.

Third, after the firmware has been deployed, mitigation techniques could serve as another line of defense. Currently, code diversity techniques (e.g., address space layout randomization, stack protections (e.g., stack canaries [95]), control-flow integrity [96], data execution prevention (DEP) have been the standard security features on PCs. But how to apply them to vehicle firmware, especially those written for less powerful ECUs, remains an open problem. As an illustrative example, DEP, the fundamental technique to defeat code injection, is achieved on PCs using the *memory management unit*, which is unfortunately not present on most ECUs. Although there has been a significant effort on system-level mitigation techniques for microcontroller systems, existing work either requires radical hardware retrofit [97]–[99] or relies on heavy instrumentation to the binaries [100], [101], which imposes considerable runtime overhead and thus compromises the real-time constraint of many ECU tasks. Towards this direction, we should creatively utilize existing hardware features available on MCUs, such as performance monitoring unit or TrustZone, to minimize the runtime overhead. A clean-slate hardware-software co-design is also a direction that pursues to meet both the security and performance requirements.

Fourth, when the system is suspicious of attacks, logging provides analysts from OEMs with valuable data for quick causality analysis. As such, trusted logging should be implemented to collect and store security-related events from each module. Note that the logging subsystem should be properly isolated from others since a sophisticated attacker could overwrite the logging data once the ECU firmware is compromised.

With hardware support, trusted computing is the ultimate goal. In trusted computing, a dedicated chip is integrated into the system to provide fundamental security features such as memory isolation, platform integrity, and remote attestation. In embedded systems, SMART [102] has been a highly-influential proposal that follows the sprite of trusted computing. It can establish a dynamic root of trust for microcontroller devices. SMART requires no additional hardware – only a few small changes to the microcontrollers. The follow-up work, called TrustLite [103] augments SMART with support for running arbitrary code (trustlets), isolated from the rest of the system. An execution-aware memory protection unit (EA-MPU) ensures that the data of a trustlet can be accessed only by the code of the trustlet itself. These proposals form the fundamental hardware environment for mission-critical firmware to run in. OEMs should closely collaborate with academia to quickly apply these results to the most critical ECU modules.

Apart from software bugs, we should also pay attention to 'logic bugs' that are directly associated with the design logic of the vehicles. For example, limit what kinds of communications a particular device can engage in (e.g., disabling ODB-II dongles from sending CAN message via CAN firewalls). It is necessary to enforce isolation so that compromised IVI could not easily communicate with other critical ECUs. When the firmware is found vulnerable, software patches should be prepared, and OTA updates should kick in immediately [104]. However, the OTA updates should be immune from the attack itself. Otherwise, the attacker could misuse this mechanism to flash malicious firmware. To safeguard OTA updates, end-to-end security should be guaranteed between the update server and the vehicle. This implies that static keys should never be used, and strong encryption should be employed.

B. Model-based Cyber-Attack Detection and Mitigation

As the final protection line, cyber-physical security detection and identification are gaining increasing attention, which is broadly divided into two groups: model-based and data-driven methods. To clearly express the cyber-attacks, vulnerabilities, and potential mitigation techniques, Table III summarizes the related works on cybersecurity of cyber-physical systems, including both model-based and data-driven approaches. Due to the little literature on cyber-attack detection and mitigation for EVs, most of the reviewed methodologies are from cyber-physical control systems. Although they are not developed aiming at cybersecurity of EVs and power electronic systems, they can provide a reference for further research in vehicle cyber-physical security. Meanwhile, considering the different features of vehicle powertrain and power electronic systems, unique cyber-physical security challenges of powertrain systems are discussed later.

Model-based methods show promise in cyber-threat detection and diagnosis based on the known physical models, while data-driven approaches work more effectively in the applications that do not have explicit physical models. The key idea of model-based detection is to compare the predicted measurements based on previous signals and models with real sensor measurements [52]. The prediction model that gives the relationship between the sensor measurements, control commands, and the predicted measurement can be developed from physical equations such as Newton's laws, fluid dynamics, electromagnetic laws, auto-regressive model, and a technique called system identification. For example, in [38], [44], [109], [111], in response to the sensor attacks in the presence of noise, the detection methods were designed based on a linear dynamic system (LDS) with sensor and perturbation noise. In [110], an auto-regressive model-based approach was developed to detect cyber-attacks on process control, wherein the auto-regressive model was used to capture the behavior of the system. Overall speaking, almost all the existing works are based on LDS, static linear state space (SLS), or simply near-linear control systems such that well-known prediction or estimation approaches can be used, e.g., Kalman filter, state observers, parameter estimation techniques, and weighted least-square observers. Typically, research works on the trigger condition of anomaly detection focus on scoring the anomaly and the conditions for raising an alert. In most publications, the residual at the kth time instance is defined as $r(k) = |y(k) - \hat{y}(k)| \geq \tau$, where τ is a threshold, y and $\hat{y}$ represent the measured output the system and its estimated value, respectively. Then, this residual is considered as a proxy for the presence of attacks, such as as [54], [133]. Apart from the deterministic objective, some statistical [120], [134], payload-based [135], and classification-based [136] algorithms are often used for designing an anomaly detector. One of the representative residual-based detection strategies is χ^2-detector based on Kalman filters, which has the capability against both bad data and false data [112].

To protect the system against stealthy cyber-attacks, some studies inserted an additional signal (also named watermark) to the system inputs for cyber-attack detection. In [38], the authors added an authentication signal (Gaussian distribution with zero means) to the control input, with which the stealthy replay attacks were detected. However, the introduced watermark may cause degradation of the system performance in normal conditions. To address this issue, within the context of replay attacks, several publications aimed to design watermarks with consideration of trade-offs between security and control performance [124]–[127]. For example, in [137], based on the game-theoretic paradigm, a suboptimal switching control policy that balances control performance with the intrusion detection rate, was proposed. Specifically, considering the problem of tracking a constant reference at the output, the authors in [124] presented a deterministic watermark based on model inversion, which to a certain extent, allows a defender to achieve control performance during normal operation and detect malicious behavior while under replay attack. Alternatively, some other active defense techniques, e.g., authentication changes to the parameters, sensing, and communication, can also help detect these stealthy attacks [138]. Extensions of watermarking-based methods can be found in [139], [140]. Besides the watermarking-based methods, some other approaches have also been proposed in recent years [54], [129], [130]. In [129], [130], a moving target defense approach was used for identifying sensor attacks in control systems, wherein deterministic and stochastic scenarios were discussed.

Besides cyber-attack detection, attack-resilient controls are applied to guarantee the ability of recovery from cyber-physical attacks [141], and up to date, two representative resilient control strategies have been proposed in the published literature. One is to develop a state estimation algorithm that is resilient to various attacks and modeling errors, provided that the controller can obtain reasonable estimate of states and actuator commands [141]–[143]. On the basis of state estimation, an appropriate controller can be designed by using a switching strategy, for instance, observer-based resilient control [144], [145]. Besides the accurate state estimation, the second attack-resilient control strategy designs a high-assurance control system to mitigate the threat from cyber-physical attacks via various control theories [112], which can be further categorized into two schemes. The first scheme designs a resilient controller that focuses on a certain type of attack such as denial-of-service, various deception attacks (false data injection attacks, zero-dynamic attacks, etc.), and replay attacks. The second scheme uses adaptive control to assure the security and reliability of closed-loop-systems, considering the presence of unknown attacks. For example, in [146]–[148], adaptive resilient control strategies against unknown sensor and actuator attacks are presented, which guarantee the closed-loop stability for linear

TABLE III: Cyber-attack detection and mitigation for cyber-physical system.

Attack Setup	Model-based (attack location; prediction model; detection method)	Data-driven (application; model)
DOS attack	Sensors; LDS [19]; observer-based [19], [105].	Smart grids, industrial control systems, electric vehicles; dynamic state estimation [106], support vector machine (SVM) [107], multi-layer machine learning models [108], etc.
Replay attack	Sensors and actuators; LDS [38], [44], [109], auto-regressive model [110]; state estimation in the presence of sensor noise [111], χ^2-detector based on Kalman filters [112], etc.	Power systems, wide-area measurement systems; self-correlation coefficient [113], singular value decomposition [114], stochastic coding [115], frequency-based signature [116], etc.
Data injection attack	Sensors and controllers; LDS [117], [118], SLS [119]; state estimation [117], MPC [118], statistical anomaly detection technique [120], etc.	Smart grids, CAN bus; support vector machine (SVM) [121], Gaussian mixture model (GMM) [122], neural networks [123], etc.
Stealthy attack	Sensors and controllers; LDS [124]–[127]; water marking method [124]–[127], robust extended Kalman filter [128], moving target defense approach [129], [130], etc.	Networked control systems, smart grid, automatic voltage controls (AVCs); closed-loop recursive identification [69], low-rank and sparse matrix approximation [131], reinforcement learning [132], etc.

dynamic systems. It should be noted that the first scheme assumes that the attack type or schedule are open to the resilient controllers. For instance, in [149], the authors assumed that the replay attacks can always be detected, and on this basis, the attack-resilient receding horizon control law is developed. But for real applications, accurate detection is hard to achieve. In the second scheme, although no prior knowledge of attacks is utilized, the attack values in the dynamic system are often supposed to be state-dependent and bounded, hence in most cases, to guarantee robustness and stability, the designed resilient controllers expose some considerable conservatism.

For cybersecurity of powertrain and power electronic systems in EVs, the above model-based literature provides fundamental methodologies, for instance, observer-based cyber-attack detection during charging for battery packs [150], in which a linear battery dynamics model is used. To improve the cyber-physical security of EVs with four motor drives, [151] proposed a coordinated detection methodology that combines state observer and performance-based evaluation metrics. Currently, the research of cybersecurity of EVs is still at an early stage, and most of the literature focus on driving-level control systems, such as detection and recovery mechanism design for vehicle platooning [19], [20]. Cyber-physical security issues of vehicle powertrain and power electronic systems are not well addressed in both academia and the industries, and few studies have been devoted to this area. In the previous work [42], [58], vulnerabilities of EDSs due to sensor false data injection attacks were analyzed, wherein some innovative metrics were developed. These performance-based metrics can help identify the cyber-attacks.

C. Data-driven Cyber-Attack Detection and Mitigation

Unlike model-based solutions, data-driven based algorithms are model-free; thus, neither system parameters nor models are needed in the attack detection and diagnosis. Data-driven methods have diverse branches, such as statistical models, machine learning (ML) techniques, data-mining techniques, etc. As data-driven methods do not require explicit physical models, they can cope with complex, complicated, and heterogeneous phenomena. There are many data-driven methods for the security issues, such as the geometrically designed residual filter [46], signal analytics based [152], generalized likelihood ratio [153], the cumulative sum (CUSUM) [154], leverage score [155], influential point selection [156], support vector machine (SVM) [121], Gaussian mixture model (GMM) [122], neural networks [123], machine learning [121], deep learning [157], and so on.

More specifically, targeting the three possible attack types in the powertrain systems in modern EVs: DOS, replay attack, and false data injection attacks, the related data-driven solutions will be introduced. In general, data-driven methods can be viewed as using trained models to detect abnormal system behavior based on the observation data collected from the system, which are usually based on the idea that under normal conditions, the observation data would be constant with minor variations due to measurement inaccuracies and system noises. The main motivation is that the normal data and the tampered data tend to be separated in a certain feature space [121], [158] or using given quantitative metrics [107], [159]. Commonly, labeling information is needed for supervised learning, and one can train a classifier to identify attacks according to the class labels. While, if labels are not given, unsupervised learning-based methods cluster unlabeled data into classes according to the hidden features.

In terms of theoretical methods, the linear regression (LR) detects the cyber-attack if the measured data does not fit the linear model fitted from the training data set. Signal temporal logic proposed in [160] compared the DC voltages and currents with the predefined upper and lower boundaries. SVM is another linear discriminative classifier formally defined by a separating hyperplane, which has been widely used to detect attacks [161]. The artificial neural networks (ANN) model is a computational model based on the structure and functions of networked neurons, used for classification and regression. Depending on activation functions and neurons, ANN can model complicated relationships between inputs and outputs [123]. Recurrent neural networks (RNN) is a type of deep neural network (DNN). With the internal memory unit, RNN can better capture the signal dynamics, which is important for the time-series data analytics [162]–[164]. Convolutional neural network (CNN) is another type of DNN which is widely used for image processing. CNN utilizes the convolutional kernels to extract texture features of the measurement matrices [165]. Need to mention, DNNs with a higher number of hidden layers are expected to yield more precise detection results. However, the computation cost will be higher.

For the cybersecurity of vehicles, although there have been a series of research works on data-driven cyber-attack detection for vehicles, most of them are developed for in-vehicle-network security and less for powertrain control systems. For example, authors in [166] proposed a deep learning-based approach for cyber-attack detection in vehicles. In this work, a generative adversarial network classification is used to assess the message frames transferring between the ECU and other hardware in the vehicle. In [167], for cybersecurity of in-vehicle network communication, a cloud-based intrusion detection approach is presented. By using deep learning, distributed DOS, command injection, and network malware can be identified.

D. Challenge and Future Versions

Although these detection and mitigation approaches provide technical foundations against malicious attacks, several challenges remain to be solved for cybersecurity of powertrain and power electronic systems in EVs.

- Notice that in real-world applications, the powertrain system in an EV is nonlinear and complicated, and most of the controllers in ECUs include a large number of engineering-experience-based rules and look-up tables. Under these circumstances, the traditional theory-based methods would be ineffective to analyze the stability, security, robustness, and resilience of the system because most of them are based on a linear dynamic system modeling. One of the potential solutions is to develop index-based attack impact analysis, detection, and diagnosis to fully utilize the physical features and performance of the powertrain system, such as the discussions in the previous work [42], [43], [58], [151].
- Although data-driven methods for cyber-physical control systems provide an alternative way to cyber-attack detection and mitigation, there are still limitations and challenges, especially for EV cybersecurity. On the one hand, unlike the cybersecurity in power grids and other cyber-physical systems with fixed normal conditions, real-time driving cycles of vehicles demonstrate high uncertainty and a broader range of variation (even in normal scenarios). Therefore, it is difficult to distinguish abnormal conditions and varying driving conditions, such as frequent start-stop driving in urban traffic. On the other hand, data scarcity is generally the most critical issue that needs to be solved. However, real EV data can be hard to obtain and are often confidential by the carmakers. Besides, the training data may not be available for every attack scenario in a particular EV. Therefore, more novel solutions to reduce data dependency, improve computation efficiency, and increase the model fidelity need to be explored.
- Most of the current research in cyber-physical control systems does not consider computational requirements. However, power electronic systems, e.g., electric drive systems, are operating faster than other processing control systems. A fast detection methodology needs to be developed such that the cyber-attack could be detected at the early stage. Therefore, besides the detection accuracy, the sampling rate, computational burden, and time to detection need to be considered. From this perspective, model-based approaches that do not require online optimization, such as an observer-based cyber-attack detector with fixed observer gain [19], [105], are available for power electronic systems. Additionally, computational-efficient data-driven methods can be used. It is worth noting that, compared to root-cause diagnosis, the purpose of cyber-attack detection is to distinguish between normal and cyber-attack scenarios, thus requiring less computational time in real applications. Once a potential cyber-attack or a physical fault is detected during driving, the human driver can stop the car and request car maintenance for further cyber-attack diagnosis.
- Besides, advanced root diagnosis methods must be developed to distinguish cyber-attacks and physical failures, as the existing literature is mostly focused on either on physical fault detection or cyber-attack detection. For power electronic systems in the EV, this paper has presented a preliminary discussion on this topic (see Section IV-B). However, it is difficult to distinguish physical faults from various cyber-attacks, especially considering the time-varying and uncertain driving conditions of the powertrain system. Therefore, a comprehensive study on this topic is still an emerging topic in the future.

VI. Conclusions

This paper has presented a comprehensive study of cyber-physical security of modern EVs, with a particular focus on three representative components relevant to the powertrain system: 1) firmware of ECUs; 2) vehicle-to-grid in-vehicle charging system; 3) powertrain control system that includes system-level energy management systems and device-level electric drive systems. For practical guidance, some preliminary results of security assessment on the powertrain control system are also presented, which are further divided into two major parts: the powertrain control system and the electric drive system. Finally, the state-of-the-artwork firmware, model-based and data-driven detection, diagnosis, and mitigation opportunities are discussed comprehensively. Unique cyber-physical security challenges of powertrain systems and future versions are also discussed.

Appendix

Suppose the prediction horizon is discretized into N_p steps on Δt-axis. Then, the EMS is designed by solving an optimization that find the optimal $u = [T_{ref,i}(1), T_{ref,i}(2), ..., T_{ref,i}(N_p - 1)] (i = 1, 2, 3, 4)$, such that

$$\min_{u \in \mathcal{U}} \mathcal{J} = \sum_{k=1}^{N_p} [(v(k) - v_{ref}(k))^2 + \kappa V_{oc}(k) I_{bat}(k)], \quad (4)$$

where $T_{ref,i}$ represents the torque reference of the ith motor; v is the vehicle speed; v_{ref} is the desired vehicle speed of the upper drive controller; κ is the weighting factor; V_{oc} is the battery open-circuit voltage; I_{bat} is the battery current; $\mathcal{U}$ is the closed set of admissible controls. In the above cost function, the first term illustrates the dynamic performance of the vehicle, which reflects the capability to track the velocity profile of the upper drive controller. The second cost denotes the power consumption of the battery. The nonlinear and time-varying system dynamics are summarized in [168]–[170], as follows:

$$v(k+1) = v(k) + [\sum_{i=1}^{4} T_{ref,i}(k)/r_w - \mathcal{G}(k)]\Delta t/M, \quad (5a)$$

$$I_{bat}(k) = [V_{oc}(k) - \sqrt{V_{oc}^2(k) - 4P_{bat}(k)R_b}]/2R_b. \quad (5b)$$

Here r_w is the tire radius; M is the total mass of the vehicle; $\mathcal{G}$ represents the total resistance during driving, including the rolling resistance, air resistance, and gravity resistance caused by road slope; P_{bat} is the power consumption of the battery; R_b is the battery internal resistance. Finally, the first control command is applied to the lower system, and at the next time instance $k + 1$, a receding horizon control is realized.

References

[1] R. Hou, L. Zhai, T. Sun, Y. Hou, and G. Hu, "Steering stability control of a four in-wheel motor drive electric vehicle on a road with varying adhesion coefficient," *IEEE Access*, vol. 7, pp. 32 617–32 627, 2019.

[2] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, vol. 2014, pp. 1–94, 2014.

[3] D. Wise, "Vehicle cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack," US Government Accountability Office [Online]. Available: https://www.gao.gov/products/GAO-16-350, Tech. Rep., Mar. 2016.

[4] L. Guo, J. Ye, and L. Du, "Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks," *IEEE Transactions on Transportation Electrification*, 2020.

[5] A. Greenburg, "Hackers remotely kill a Jeep on the highway - with me in it," [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, Tech. Rep., Jul. 2015.

[6] "Cyber attacks in connected cars: what Tesla did differently to win," [Online]. Available: https://www.appknox.com/blog/cyber-attacks-in-connected-cars, Tech. Rep., Sep. 2017.

[7] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[8] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," in *International Conference on Computer Safety, Reliability, and Security*. Springer, Cham, 2016, pp. 130–141.

[9] A. Chattopadhyay and K. Y. Lam, "Security of autonomous vehicle as a cyber-physical system," in *7th International Symposium on Embedded Computing and System Design*. IEEE, 2017, pp. 1–6.

[10] C. Schmittner and G. Macher, "Automotive cybersecurity standards-relation and overview," in *International Conference on Computer Safety, Reliability, and Security*. Springer, Cham, 2019, pp. 153–165.

[11] E. Yeh, J. Choi, N. G. Prelcic, C. R. Bhat, and R. W. Heath, "Cybersecurity challenges and pathways in the context of connected vehicle systems," University of Texas at Austin., Tech. Rep., Feb., 2018.

[12] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 10–21, 2014.

[13] C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," National Renewable Energy Lab (NREL), Golden, CO (United States), Tech. Rep., 2019.

[14] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

[15] K. Han, A. Weimerskirch, and K. G. Shin, "Automotive cybersecurity for in-vehicle communication," in *IQT Quarterly*, vol. 6, no. 1, 2014, pp. 22–25.

[16] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS One*, vol. 11, no. 6, pp. 1–17, 2016.

[17] M. Levi, Y. Allouche, and A. Kontorovich, "Advanced analytics for connected car cybersecurity," in *87th IEEE Vehicular Technology Conference*. IEEE, 2018, pp. 1–7.

[18] P. Guo, H. Kim, L. Guan, M. Zhu, and P. Liu, "VCIDS: Collaborative intrusion detection of sensor and actuator attacks on connected vehicles," in *International Conference on Security and Privacy in Communication Systems*. Springer, Cham, 2017, pp. 377–396.

[19] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[20] E. Mousavinejad, F. Yang, Q. L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 9, pp. 3821–3834, 2020.

[21] M. Amoozadeh, A. Raghuramu, C. N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[22] A. Alipour-Fanid, M. Dabaghchian, H. Zhang, and K. Zeng, "String stability analysis of cooperative adaptive cruise control under jamming attacks," in *18th IEEE International Symposium on High Assurance Systems Engineering*. IEEE, 2017, pp. 157–162.

[23] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *ACM Cyber-Physical Systems Security and/or Privacy*, 2015, pp. 43–53.

[24] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: an efficiency-motivated attack against autonomous vehicular transportation," in *ACM Computer Security Applications Conference*, 2013, pp. 99–108.

[25] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security Symposium*, vol. 4, 2011, pp. 447–462.

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

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

[28] D. Regalado, "Zingbox identifies new cybersecurity threat for cars and drivers at DefCon 26," [Online]. Available: https://www.businesswire.com/news/home/20180809005216/en/Zingbox-Identifies-New-Cybersecurity-Threat-Cars-Drivers, Tech. Rep., Aug. 2018.

[29] R. McMillan, "With hacking, music can take control of your car," [Online]. Available: https://www.pcworld.com/article/221873/With_Hacking_Music_Can_Take_Control_of_Your_Car.html, Tech. Rep., Mar. 2011.

[30] Privacy4Cars, "CarsBlues vehicle flaw found affecting millions of vehicles worldwide," [Online]. Available: https://cyware.com/news/carsblues-vehicle-flaw-found-affecting-millions-of-vehicles-worldwide-ed357394/, Tech. Rep., Nov. 2018.

[31] M. Griffin, "Exploit allowed hackers to take remote control of a Tesla Model S," [Online]. Available: https://www.fanaticalfuturist.com/2016/09/exploit-allows-hackers-to-remotely-take-control-of-a-tesla-model-s/, Tech. Rep., Sep. 2016.

[32] Kresten Hall Geisler, "More cars than phones were connected to cell service in Q1," [Online]. Available: https://techcrunch.com/2016/06/

20/more-cars-than-phones-were-connected-to-cell-service-in-q1/, Tech. Rep., Jun. 2016.

[33] C. Cimpanu, "Tesla car hacked at Pwn2Own contest," [Online]. Available: https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/, Tech. Rep., Mar. 2019.

[34] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[35] M. Aminzade, "Confidentiality, integrity and availability–finding a balanced it framework," *Network Security*, vol. 2018, no. 5, pp. 9–11, 2018.

[36] E. Yağdereli, C. Gemci, and A. Z. Aktaş, "A study on cyber-security of autonomous and unmanned vehicles," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 369–381, 2015.

[37] P. Nicholson, "Five most famous DDoS attacks and then some," [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/, Tech. Rep., July. 2020.

[38] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing*, 2009, pp. 911–918.

[39] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *2018 Annual American Control Conference*. IEEE, 2018, pp. 5582–5587.

[40] M. Zhu and S. Martínez, "On resilient consensus against replay attacks in operator-vehicle networks," in *2012 American Control Conference*. IEEE, 2012, pp. 3553–3558.

[41] D. Stabili, M. Marchetti, and M. Colajanni, "Detecting attacks to internal vehicle networks through hamming distance," in *2017 AEIT International Annual Conference*. IEEE, 2017, pp. 1–6.

[42] 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.

[43] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W.-Z. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[44] Y. Mo and B. Sinopoli, "Distributed fault detection for interconnected second-order systems," in *1st Workshop on Secure Control Systems*, 2010, pp. 1–6.

[45] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 11 271–11 277, 2011.

[46] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 2195–2201.

[47] Y. Mao, H. Jafarnejadsani, P. Zhao, E. Akyol, and N. Hovakimyan, "Detectability of intermittent zero-dynamics attack in networked control systems," in *58th IEEE Conference on Decision and Control*. IEEE, 2019, pp. 5605–5610.

[48] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," *arXiv preprint arXiv:1711.04822*, 2017.

[49] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Stealthy deception attacks on water scada systems," in *13th ACM international conference on Hybrid systems: computation and control*, 2010, pp. 161–170.

[50] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, 2018.

[51] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.

[52] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, N. O. T. J. Ruths, H. S. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys*, vol. 51, no. 4, p. 76, 2018.

[53] Y. L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[54] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding sensor outputs for injection attacks detection," in *53rd IEEE Conference on Decision and Control, IEEE*, December 2014, pp. 5776–5781.

[55] K.-T. Cho, Y. Kim, and K. G. Shin, "Who killed my parked car?" *arXiv preprint arXiv:1801.07741*, 2018.

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

[57] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, Dec 2017.

[58] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *2019 IEEE Transportation Electrification Conference and Expo*, June 2019, pp. 1–6.

[59] A. Chattopadhyay, K. Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[60] S. Wang, D. Sun, L. Du, and J. Ye, "Noncooperative distributed social welfare optimization with EV charging response," in *44th IECON Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2018, pp. 2097–2102.

[61] O. Teichert, F. Chang, A. Ongel, and M. Lienkamp, "Joint optimization of vehicle battery pack capacity and charging infrastructure for electrified public bus systems," *IEEE Transactions on Transportation Electrification*, vol. 5, no. 3, pp. 672–682, Sep. 2019.

[62] K. Qian, C. Zhou, M. Allan, and Y. Yuan, "Modeling of load demand due to ev battery charging in distribution systems," *IEEE Transactions on Power Systems*, vol. 26, no. 2, pp. 802–810, May 2011.

[63] L. P. Fernandez, T. G. San Román, R. Cossent, C. M. Domingo, and P. Frias, "Assessment of the impact of plug-in electric vehicles on distribution networks," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 206–213, 2010.

[64] E. Veldman and R. A. Verzijlbergh, "Distribution grid impacts of smart electric vehicle charging from different perspectives," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 333–342, 2014.

[65] K. Sitch, D. Sun, and L. Du, "Integration of pulsed electric bus fleet charging profiles through coordinated control of hybrid microgrids," in *2019 IEEE Transportation Electrification Conference and Expo*. IEEE, 2019, pp. 1–6.

[66] K. Sitch, D. Sun, L. Du, and H. Yang, "Pulsed electric bus charging management considering charge redistribution effect," in *2020 IEEE Transportation Electrification Conference and Expo*. IEEE, 2020, pp. 1–6.

[67] D. Zhang, J. Jiang, L. Y. Wang, and W. Zhang, "Robust and scalable management of power networks in dual-source trolleybus systems: A consensus control framework," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1029–1038, 2015.

[68] S. Wang, L. Du, J. Ye, and D. Zhao, "A deep generative model for non-intrusive identification of ev charging profiles," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[69] J. S. Wang and G. H. Yang, "Data-driven methods for stealthy attacks on tcp/ip-based networked control systems equipped with attack detectors," *IEEE Transactions on Cybernetics*, vol. 49, no. 8, pp. 3020–3031, 2018.

[70] H. Zhao, X. Yan, and L. Ma, "Training-free non-intrusive load extracting of residential electric vehicle charging loads," *IEEE Access*, vol. 7, pp. 117 044–117 053, 2019.

[71] A. A. Munshi and Y. A. I. Mohamed, "Unsupervised nonintrusive extraction of electrical vehicle charging load patterns," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 266–279, 2019.

[72] A. F. M. Jaramillo, D. M. Laverty, J. M. del Rincón, J. Hastings, and D. J. Morrow, "Supervised non-intrusive load monitoring algorithm for electric vehicle identification," in *2020 IEEE International Instrumentation and Measurement Technology Conference*. IEEE, 2020, pp. 1–6.

[73] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

[74] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *33rd Annual Computer Security Applications Conference*, 2017, pp. 303–314.

[75] L. Calearo, A. Thingvad, K. Suzuki, and M. Marinelli, "Grid loading due to ev charging profiles based on pseudo-real driving pattern and user behavior," *IEEE Transactions on Transportation Electrification*, vol. 5, no. 3, pp. 683–694, 2019.

[76] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[77] Z. Song, H. Hofmann, J. Li, J. Hou, X. Han, and M. Ouyang, "Energy management strategies comparison for electric vehicles with hybrid energy storage system," *Applied Energy*, vol. 134, pp. 321–331, 2014.

[78] N. Sulaiman, M. Hannan, A. Mohamed, P. J. Ker, E. Majlan, and W. W. Daud, "Optimization of energy management system for fuel-cell hybrid electric vehicles: Issues and recommendations," *Applied energy*, vol. 228, pp. 2061–2079, 2018.

[79] S. F. Tie and C. W. Tan, "A review of energy sources and energy management system in electric vehicles," *Renewable and Sustainable Energy Reviews*, vol. 20, pp. 82–102, 2013.

[80] C. Sun, X. Hu, S. J. Moura, and F. Sun, "Velocity predictors for predictive energy management in hybrid electric vehicles," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 3, pp. 1197–1204, 2014.

[81] H. Hemi, J. Ghouili, and A. Cheriti, "Combination of markov chain and optimal control solved by pontryagin's minimum principle for a fuel cell/supercapacitor vehicle," *Energy Conversion and Management*, vol. 91, pp. 387–393, 2015.

[82] Y. Avenas, L. Dupont, N. Baker, H. Zara, and F. Barruel, "Condition monitoring: A decade of proposed techniques," *IEEE Industrial Electronics Magazine*, vol. 9, no. 4, pp. 22–36, Dec 2015.

[83] M. Riera-Guasp, J. A. Antonino-Daviu, and G. Capolino, "Advances in electrical machine, power electronic, and drive condition monitoring and fault detection: State of the art," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 3, pp. 1746–1759, March 2015.

[84] J. Reimers, L. Dorn-Gomba, C. Mak, and A. Emadi, "Automotive traction inverters: Current status and future trends," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3337–3350, 2019.

[85] M. Anwar, M. Hayes, A. Tata, M. Teimorzadeh, and T. Achatz, "Power dense and robust traction power inverter for the second-generation chevrolet volt extended-range ev," *SAE International Journal of Alternative Powertrains*, vol. 4, no. 1, 2015.

[86] A. Steier and A. Munday, "Advanced strong hybrid and plug-in hybrid engineering evaluation and cost analysis," *Munro and Associates Inc., Ricardo Strategic Consulting, and ZM Associates Environmental Corp, Sacramento, CA, USA, Tech. Rep. 15CAR018*, 2017.

[87] T. Burress, "Benchmarking state-of-the-art technologies," in *presentation at the 2013 US Department of Energy Hydrogen and Fuel Cells Program and Vehicle Technologies Program Annual Merit Review and Peer Evaluation Meeting*, 2013.

[88] S. Moquin, S. Kim, N. Blair, C. Farnell, J. Di, and H. A. Mantooth, "Enhanced uptime and firmware cybersecurity for grid-connected power electronics," in *2019 IEEE CyberPELS*. IEEE, 2019, pp. 1–6.

[89] K. Serebryany, D. Bruening, A. Potapenko, and D. Vyukov, "AddressSanitizer: A fast address sanity checker," in *2012 USENIX Conference on Annual Technical Conference*, 2012.

[90] J. Newsome and D. Song, "Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software," in *12th Annual Network and Distributed System Security Symposium*, 2005.

[91] I. Yun, S. Lee, M. Xu, Y. Jang, and T. Kim, "QSYM: A practical concolic execution engine tailored for hybrid fuzzing," in *27th USENIX Security Symposium*, 2018, pp. 745–761.

[92] N. Stephens, J. Grosen, C. Salls, A. Dutcher, R. Wang, J. Corbetta, Y. Shoshitaishvili, C. Kruegel, and G. Vigna, "Driller: Augmenting fuzzing through selective symbolic execution." in *NDSS*, vol. 16, no. 2016, 2016, pp. 1–16.

[93] N. D. Matsakis and F. S. Klock II, "The rust language," in *ACM SIGAda Ada Letters*, vol. 34, no. 3. ACM, 2014, pp. 103–104.

[94] R. Gu, Z. Shao, H. Chen, X. N. Wu, J. Kim, V. Sjöberg, and D. Costanzo, "Certikos: An extensible architecture for building certified concurrent os kernels," in *12th USENIX Symposium on Operating Systems Design and Implementation*, 2016, pp. 653–669.

[95] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton, "Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks." in *USENIX security symposium*, vol. 98. San Antonio, TX, 1998, pp. 63–78.

[96] A. Martn, "Control-flow integrity," in *12th ACM conference on Computer and communications security*, 2005.

[97] A. Francillon, D. Perito, and C. Castelluccia, "Defending embedded systems against control flow attacks," in *1st ACM workshop on Secure execution of untrusted code*, 2009, pp. 19–26.

[98] L. Davi, M. Hanreich, D. Paul, A.-R. Sadeghi, P. Koeberl, D. Sullivan, O. Arias, and Y. Jin, "Hafix: hardware-assisted flow integrity extension," in *52nd ACM/EDAC/IEEE Design Automation Conference*. IEEE, 2015, pp. 1–6.

[99] Y. Lee, J. Lee, I. Heo, D. Hwang, and Y. Paek, "Integration of ROP/JOP monitoring IPs in an ARM-based SoC," in *2016 Design, Automation and Test in Europe Conference and Exhibition*. IEEE, 2016, pp. 331–336.

[100] A. A. Clements, N. S. Almakhdhub, K. S. Saab, P. Srivastava, J. Koo, S. Bagchi, and M. Payer, "Protecting bare-metal embedded systems with privilege overlays," in *2017 IEEE Symposium on Security and Privacy*, May 2017, pp. 289–303.

[101] D. Kwon, J. Shin, G. Kim, B. Lee, Y. Cho, and Y. Paek, "uXOM: Efficient eXecute-only memory on ARM cortex-m," in *28th USENIX Security Symposium*, 2019, pp. 231–247.

[102] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito, "Smart: secure and minimal architecture for (establishing dynamic) root of trust." in *NDSS*, vol. 12, 2012, pp. 1–15.

[103] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan, "Trustlite: A security architecture for tiny embedded devices," in *9th European Conference on Computer Systems*, 2014, pp. 1–14.

[104] S. Halder, A. Ghosal, and M. Conti, "Secure ota software updates in connected vehicles: A survey," *arXiv preprint arXiv:1904.00685*, 2019.

[105] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.

[106] M. A. Hasnat and M. Rahnamay-Naeini, "A data-driven dynamic state estimation for smart grids under dos attack using state correlations," in *2019 North American Power Symposium*. IEEE, 2019, pp. 1–6.

[107] M. Al-Saud, A. M. Eltamaly, M. A. Mohamed, and A. Kavousi-Fard, "An intelligent data-driven model to secure intravehicle communications based on machine learning," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 6, pp. 5112–5119, 2019.

[108] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4362–4369, 2019.

[109] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011.

[110] D. Hadziosmanovic, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC: semantic security monitoring for industrial processes," in *30th Computer Security Applications Conference*, 2014, pp. 126–135.

[111] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2017.

[112] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[113] M. Ma, P. Zhou, D. Du, C. Peng, M. Fei, and H. M. AlBuflasa, "Detecting replay attacks in power systems: A data-driven approach," in *Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration*. Springer, Singapore, 2017, pp. 450–457.

[114] K. Chatterjee and S. Khaparde, "Data-driven online detection of replay attacks on wide-area measurement systems," in *20th National Power Systems Conference*. IEEE, 2018, pp. 1–6.

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

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

[117] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2015.

[118] A. Rosich, H. Voos, Y. Li, and M. Darouach, "A model predictive approach for cyber-attack detection and mitigation in control systems," in *52nd IEEE Conference on Decision and Control*. IEEE, 2013, pp. 6621–6626.

[119] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *3rd IEEE International Conference on Smart Grid Communications*. IEEE, 2012, pp. 342–347.

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

[121] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[122] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 2017.

[123] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, "Real-time cyber-physical false data attack detection in smart grids using neural networks," in *2017 International Conference on Computational Science and Computational Intelligence*. IEEE, 2017, pp. 1–6.

[124] R. Romagnoli, S. Weerakkody, and B. Sinopoli, "A model inversion based watermark for replay attack detection with output tracking," in *2019 American Control Conference*. IEEE, 2019, pp. 384–390.

[125] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2013.

[126] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.

[127] A. Khazraei, H. Kebriaei, and F. R. Salmasi, "A new watermarking approach for replay attack detection in lqg systems," in *56th IEEE Conference on Decision and Control*. IEEE, 2017, pp. 5143–5148.

[128] M. Necip Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *arXiv*, pp. arXiv–1803, 2018.

[129] S. Weerakkody and B. Sinopoli, "A moving target approach for identifying malicious sensors in control systems," in *54th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2016, pp. 1149–1156.

[130] P. Griffioen, S. Weerakkody, and B. Sinopoli, "An optimal design of a moving target defense for attack detection in control systems," in *2019 American Control Conference*. IEEE, 2019, pp. 4527–4534.

[131] A. Anwar, A. N. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Pacific-Asia Workshop on Intelligence and Security Informatics*. Springer, Cham, 2016, pp. 180–192.

[132] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2018.

[133] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[134] M. J. Desforges, P. J. Jacob, and J. E. Cooper, "Applications of probability density estimation to the detection of abnormal conditions in engineering," in *Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, vol. 212, no. 8, 1998, pp. 687–703.

[135] P. Dussel, C. Gehl, P. Laskov, J. U. Bußer, C. Stormann, and J. Kastner, "Cyber-critical infrastructure protection using real-time payload-based anomaly detection," in *International Workshop on Critical Information Infrastructures Security*, 2009, pp. 85–97.

[136] M. P. Coutinho, G. Lambert-Torres, L. B. da Silva, H. G. Martins, H. Lazarek, and J. C. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," in *3rd IEEE International Conference on Digital Ecosystems and Technologies*, 2009, pp. 733–738.

[137] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *52nd IEEE conference on decision and control*. IEEE, 2013, pp. 1854–1859.

[138] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *50th Allerton Conference on Communication, Control, and Computing*. IEEE, 2012, pp. 1806–1813.

[139] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219–240, 2016.

[140] S. Weerakkody, O. Ozel, and B. Sinopoli, "A bernoulli-gaussian physical watermark for detecting integrity attacks in control systems," in *55th Allerton Conference on Communication, Control, and Computing*. IEEE, 2017, pp. 966–973.

[141] F. Pasqualetti, F. Dorfler, and Bullo, "Attack detection and identification in cyber–physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[142] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas, "Robustness of attack-resilient state estimators," in *5th ACM/IEEE International Conference on Cyber-Physical Systems*. IEEE Computer Society, 2014, pp. 163–174.

[143] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Systems Magazine*, vol. 37, no. 2, pp. 66–81, 2017.

[144] C. Xie and G. H. Yang, "Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 15, pp. 4382–4403, 2018.

[145] H. Fawzi, P., Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[146] T. Yucelen, W. M. Haddad, and E. Feron, "Adaptive control architectures for mitigating sensor attacks in cyber-physical systems," *Cyber-Physical Systems*, vol. 2, no. 1-4, pp. 24–52, 2016.

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

[148] L. An and G. H. Yang, "Improved adaptive resilient control against sensor and actuator attacks," *Information Sciences*, vol. 423, pp. 145–156, 2018.

[149] M. H. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

[150] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyber attack detection during charging," *IEEE Transactions on Industrial Electronics*, 2020.

[151] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives," *IEEE Transactions on Power electronics*, 2020.

[152] B. Yang, F. Li, J. Ye, and W. Song, "Condition monitoring and fault diagnosis of generators in power networks," in *2019 IEEE Power & Energy Society General Meeting*. IEEE, 2019, pp. 1–5.

[153] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[154] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, 2016.

[155] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–10, 2019.

[156] F. Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Z. Song, "Online distributed IoT security monitoring with multidimensional streaming big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2020.

[157] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Z. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, pp. 5224–5231, 2019.

[158] K. Mahapatra, N. R. Chaudhuri, R. G. Kavasseri, and S. M. Brahma, "Online analytical characterization of outliers in synchrophasor measurements: A singular value perturbation viewpoint," *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 3863–3874, 2017.

[159] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys*, vol. 41, no. 3, p. 15, 2009.

[160] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, July 2019.

[161] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *2016 International Joint Conference on Neural Networks*. IEEE, 2016, pp. 1395–1402.

[162] G. Fenza, M. Gallo, and V. Loia, "Drift-aware methodology for anomaly detection in smart grid," *IEEE Access*, vol. 7, pp. 9645–9657, 2019.

[163] L. Guo, Y. Jin, and Y. Bowen, "Cyber-attack detection for electric vehicles using physics-guided machine learning," *IEEE Transactions on Transportation Electrification*, 2020.

[164] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W.-Z. Song, "System statistics learning-based iot security: Feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019.

[165] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *Journal of Information Security and Applications*, vol. 46, pp. 42–52, 2019.

[166] A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin, W. Su, and M. Roustaei, "An evolutionary deep learning-based anomaly detection model for securing vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[167] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017.

[168] H. Chen, L. Guo, H. Ding, Y. Li, and B. Gao, "Real-time predictive cruise control for eco-driving taking into account traffic constraints," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 8, pp. 2858–2868, 2018.

[169] L. Tang, G. Rizzoni, and S. Onori, "Energy management strategy for HEVs including battery life optimization," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 3, pp. 211–222, 2015.

[170] L. Guo, B. Gao, Q. Liu, J. Tang, and H. Chen, "On-line optimal control of the gearshift command for multispeed electric vehicles," *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 4, pp. 1519–1530, 2017.

Jin Ye (S'13-M'14-SM'16) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from McMaster University, Hamilton, ON, Canada, in 2014.

She is currently an Assistant Professor of electrical engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, smart grids, electrified transportation, and cyber-physical systems.

Dr. Jin Ye is the General Chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC), and the Publication Chair and Women in Engineering Chair of 2019 IEEE Energy Conversion Congress and Expo (ECCE). She is an Associate Editor for IEEE TRANSACTIONS ON POWER ELECTRONICS, IEEE OPEN JOURNAL OF POWER ELECTRONICS, IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Lulu Guo received the B.S. degree in vehicle engineering and the Ph.D. degree in control engineering from Jilin University, Changchun, China, in 2014 and 2019, respectively.

He is currently a Postdoctoral Research Associate with the University of Georgia, Athens, GA, USA. His current research interests include advanced vehicle control, energy management, and vehicle cybersecurity.

Bowen Yang received the B.S. degree in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in 2018. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the University of Georgia, Athens, GA, USA.

He is also a Research Assistant with the University of Georgia, USA. His current research interests include advanced control for power electronics and electric machines, energy management system, and cyber-physical security for intelligent electric drives.

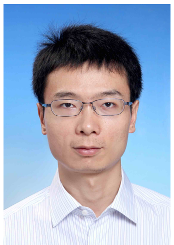
Fangyu Li received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2009, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2013, and the Ph.D. degree in geophysics from The University of Oklahoma, Norman, OK, USA, in 2017.

Between 2017 and 2020, he did the Postdoctoral Fellowship with the College of Engineering, University of Georgia, Athens, GA, USA. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering at the Kennesaw State University, Marietta, GA, USA. His research interests include signal processing, machine learning, deep learning, distributed computing, Internet of things (IoT), and cyber-physical systems (CPS).

Liang Du (S'09–M'13–SM'18) received the Ph.D. degree in electrical engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2013.

He was a Research Intern at Eaton Corp. Innovation Center (Milwaukee, WI), Mitsubishi Electric Research Labs (Cambridge, MA, USA), and Philips Research N.A. (Briarcliff Manor, NY) in 2011, 2012, and 2013, respectively. He was also an Electrical Engineer with Schlumberger, Sugar Land, TX, USA, from 2013 to 2017. He is currently an Assistant Professor with Temple University, Philadelphia, USA.

Dr. Du received the Ralph E. Powe Junior Faculty Enhancement Award from ORAU in 2018 and is currently an Associate Editor for IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS and IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION.



Le Guan received the B.S. degree in information security from the University of Science and Technology of China, Hefei, China, in 2009, and the Ph.D. degree in information security from the Institute of Information Engineering, Chinese Academy of Science, Beijing, China, in 2015.

He is currently an Assistant Professor with the Department of Computer Science, University of Georgia (UGA), USA. Before joining UGA, he was a Postdoctoral Researcher with the Pennsylvania State University. His current research interests include many topics in cybersecurity, including operating system security and mobile security.

Wenzhan Song received B.S. and M.S. degrees from Nanjing University of Science and Technology, Nanjing, China, in 1997 and 1999, respectively, and the Ph.D. degree in Computer Science from Illinois Institute of Technology, Chicago, IL, USA, in 2005.

He is currently the Chair Professor of electrical and computer engineering with University of Georgia, Athens, GA, USA. His current research interests include cyber-physical systems and their applications in energy, environment, food and health sectors.

Dr. Song was the recipient of the NSF CAREER award in 2010.