# Cyber-Physical Security of Electric Vehicles With Four Motor Drives

Lulu Guo and Jin Ye, *Senior Member, IEEE*

***Abstract*—In recent years, the cyber-physical security of power electronics systems has become increasingly prominent. In this article, we present a vulnerability assessment and a coordinated detection method to improve the cyber-physical security of electric vehicles with four motor drives, which is one of the emerging power electronics applications. As the lateral stability control system (LSCS) is designed through the yaw moment generated by the torque deviation between distributed motors, cyber-threats to motor drives will cause vehicle instability and hence life-threatening consequences. In response to this issue, we propose a set of innovative index-based metrics to evaluate the performance degradation due to cyber-physical attacks on the LSCS and motor drives. Evaluation results, including both transient and statistic results, are provided for a variety of threat scenarios. To further improve the cyber-physical security of the electric vehicle, we propose a coordinated detection methodology that combines the state observer and the proposed evaluation metrics. The simulation results have validated the effectiveness of the proposed detection method.**

***Index Terms*—Cyber-physical security, electric vehicles (EVs), lateral stability control system (LSCS), motor drives, power electronics systems.**

## I. Introduction

With the growing penetration in Internet-of-Things-enabled applications, e.g., electric vehicles (EVs), power electronics systems are becoming more vulnerable to cyber-physical. Meanwhile, due to the lack of cyber awareness in the power electronics community [1], [2], 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 in the early stage, they can lead to a catastrophic failure and substantial economic loss. In response to this emerging need, a cyber-physical-security initiative has been recently launched by the IEEE Power Electronics Society (PELS) and the first IEEE Power Electronics Security Workshop (Cyber PELS) was held in April 2019.

As one of the distributed-driven power electronics systems, a novel powertrain topology in an EV that comprises four motor drives has been actively studied over the past few years [3]. Because of the quick and accurate response to the traction or braking force in the wheel, this distributed-driven powertrain platform provides great potential and opportunities to enhance the dynamic performances of both longitudinal and lateral systems. Among the works relevant to the vehicle's steering system, the lateral stability control system (LSCS) has aroused extensive attention in recent years because of the significant enhancement of the vehicle's yaw stability via various approaches. For example, in [3], a hierarchical electronic steering control strategy was presented to improve the steering stability of a four-in-wheel-motor-independent-drive EV. An appropriate yaw moment can be obtained by adaptively changing the torque allocation between the four motor drives. In [4], a vehicle stability controller was designed by using a fuzzy logic control technique considering the dynamic analysis of vehicle instability. In [5], an LSCS was proposed based on a sliding-mode control algorithm, which can adaptively adjust the yaw moment directly. Besides, some optimization-based methods are also published in recent years, for instance, [6], [7]. It should be noted that, in the published literature relevant to LSCSs, the terminology for referring such a control system includes vehicle stability control [4], [8], electronic stability control (ESC) [9], [10], yaw stability control [11]–[13], LSCS [14]–[16], etc. Still, in general, they represent the same concept.

However, once the vehicle's network, sensors, and control units are infected by malicious cyber-physical attacks, the LSCS may instead cause severe consequences, for instance, taking over steering [17]–[21] and real incidents such as cyber-attacks targeting Cherokee Jeep [22] and Tesla [23]. In a traditional vehicle, the LSCS (usually named ESC) is typically developed by using brake-based technologies, in which a reasonable brake force distribution at each wheel is derived to improve yaw stability. In these systems, the human driver can still dominantly control the steering system because of the mechanical construction and the limit of brake force distribution, whereas, for an EV with four motor drives, due to the higher level control freedom, tremendous intensity, and networked electric drive systems (EDSs), the attack surfaces and their ultimate impacts are heavily expanded. For example, an attacker can orchestrate a cyber-threat to one of the motor drives to cause instability. This concern requires more attention in modern EVs that communicate with the cloud, surrounding vehicles, and infrastructure because the number and complexity of embedded electronic control units are increasing rapidly [24], [25]. This connectivity allows remote access to the attacker. In [21] and [26]–[30], researchers have demonstrated ways to take control of vehicle functionality through both

Manuscript received March 15, 2020; revised June 22, 2020 and August 13, 2020; accepted September 17, 2020. Date of publication September 21, 2020; date of current version November 20, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1946057. Recommended for publication by Associate Editor D. G. Xu. *(Corresponding author: Jin Ye.)*

The authors are with the Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602 USA (e-mail: lulu.guo@uga.edu; jin.ye@uga.edu).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPEL.2020.3025718

physical and remote access. Once a car is affected by cyber-attacks, it may lead to severe consequences, especially for the steering control system. Aware of the cybersecurity problem, the automotive industry has taken high efforts in designing and producing security standards for modern vehicles, for instance, Society of Automotive Engineers (SAE) J3061 [31], International Organization for Standardization (ISO) 26262 [32], committee draft of the "ISO-SAE Road Vehicles—Cybersecurity Engineering" standard [33], etc. However, up to date, few studies have been devoted to the cyber-physical security of motor drive systems in an EV. In the previous work [25], [34], we presented the potential cyber-threats on the motor drive at the device level, including sensor data integrity attacks, wherein the deteriorated tracking performance is observed. While this work provides very first fundamental knowledge about the cyber-physical security of motor drives, it mainly focuses on the device level, and interaction between the motor drive and the vehicle (system-level) has not yet been well studied.

It should be noted that, although there are many research works focusing on the safety problem of modern cars, especially for autonomous (or unmanned) vehicles, the research domain of the so-called vehicle "safety" and "cyber-physical security" is quite different. In general, the driving safety mainly addresses the functional safety of driving software systems because an autonomous vehicle eliminates human involvement from driving, which may threaten safety, as mentioned in many publications [35]–[40]. Then, the aim of research works on driving safety is to make the designed unmanned driving systems to be safe, trustworthy, and reliable, and the main research works are developing better environmental perception, decision making, and planning of autonomous vehicles. Differently, cyber-physical security (or cybersecurity) deals with the issue of cyber-attacks elaborated by malicious attackers. The aims of those cyber-attacks may include causing a severe traffic accident, large economic loss, etc. In such cases, despite the reliable unmanned driving systems, the vehicle would be dangerous due to the compromised signals, such as information from the vehicle-borne radar and camera.

In general, the efforts to defend vehicles against cyber-physical attacks can be categorized into two schemes, from the perspective of vehicle cybersecurity. The first scheme focuses on information and in-vehicle network safety by improving the ability to prevent malicious threats, e.g., secure hardware, secure software update, secure controller area network [41], and other technologies reviewed in [42]–[45]. The second scheme, however, focuses on a more reliable and resilient control system that can mitigate the impact of cyber-attacks during driving, which will at least ensure life safety. Once the anomaly is detected, the system will be switched to a resilient controller and alert the driver to enter a safety zone. Therefore, the cyber-physical security and resilience of vehicular control systems are significant challenges that must be addressed by carmakers and researchers.

The critical step toward secure and resilient vehicle control systems is vulnerability assessment and malicious attack detection, which, to our knowledge, has not been attempted before, especially for those safety-critical control systems. In this article,

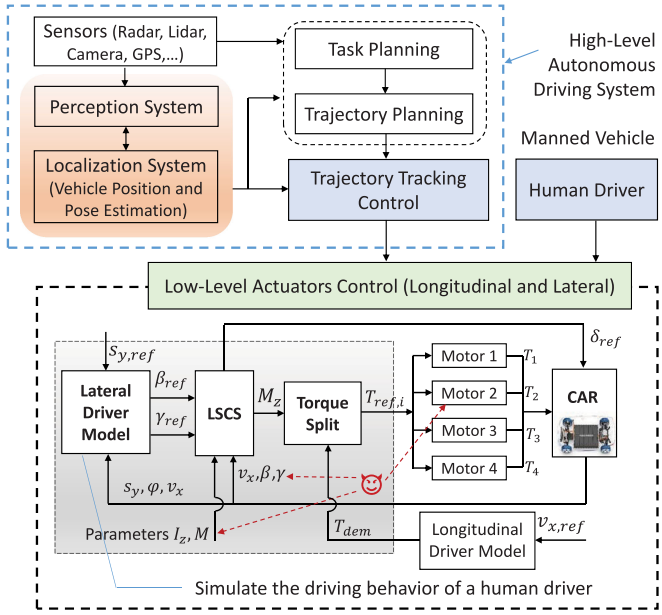


Fig. 1. Diagram of the control system and signals (or devices) potentially affected by a malicious attacker in the investigated EV. Detailed attack anomaly is described in Section III-A.

for an EV with four motor drives, we present a systematic vulnerability assessment of the LSCS and then propose a new coordinated detection method. The main contributions of this article are listed as follows.

1) We design a driver-in-the-loop steering system, based on which the vulnerability is analyzed. Compared to the current literature, we develop a model-predictive control (MPC)-based driver model to reflect the increasing difficulty of completing the steering action.
2) Besides the sensor and system parameter attacks on the LSCS, the cyber-physical attacks/faults on the motor drives are analyzed, which aims to deteriorate the tracking performance of motor drives. Then, the impact of the performance degradation of the motor drives on the vehicle's safety is analyzed.
3) We develop innovative index-based evaluation metrics in terms of system performance, with which the transient and statistic results are analyzed for a variety of threat scenarios.
4) We propose and validate a coordinated detection methodology to detect threats and improve the cyber-physical security of EVs with four motor drives.

The rest of this article is organized as follows. In Section II, the vehicle steering system is described. Section III provides attack modeling and innovative evaluation metrics. Section IV presents the simulation results and vulnerability assessment. In Section V, the coordinated attack detection method is proposed and validated. Finally, Section VI concludes this article.

## II. Vehicle Modeling and System Description

Fig. 1 presents an overview of the software system architecture for the EVs under investigation, which demonstrates

that the research on the LSCS system in the article is also compatible with autonomous driving systems (or unmanned operating systems) [46]. In general, an autonomous driving system is comprised of a variety of modules, e.g., sensors, perception systems, localization systems, task planning, trajectory planning, and trajectory tracking control. The autonomous driving system's primary function is to replace a human driver to control the car; hence, it is often marked as the high-level controller, parallel with the human driver. Then, after obtaining the trajectory command from the high-level control, such as desired speed, traveling distance, heading angle, etc., controllers in low-level actuators part are designed to fulfill the references of variables. In this article, we focus on the cyber-physical security of the power electronics systems in low-level actuator control, which is essential for both autonomous driving vehicles and manned vehicles. Specifically, the lateral and longitudinal control systems in an EV with four motor drives are considered, in which the lateral control system includes an MPC-based driver model to fulfill multiple driving maneuvers and an LSCS to track the desired references: sideslip angle $\beta_{\text{ref}}$ and yaw rate $\gamma_{\text{ref}}$ of the vehicle body. Through the torque distribution in each in-wheel motor, the yaw stability can be improved. The longitudinal driver model is developed by using a proportional–integral–derivative controller to track the given speed profile. Then, the original total torque demand $T_{\text{dem}}$ is derived from the longitudinal vehicle dynamics

$$\frac{T_{\text{dem}}}{r_w} = Ma_r + \frac{1}{2}\rho_a A_f C_d v_x^2 + Mg[\sin(\theta) + f\cos(\theta)] \quad (1)$$

where $r_w$ is the dynamic tire radius, $M$ represents the vehicle mass, $a_r$ is the desired acceleration of the longitudinal driver model, $\rho_a$ is the air density, $A_f$ is the vehicle face area, $C_d$ is the air resistance coefficient, $v_x$ represents the vehicle speed, $g$ is the gravitational constant, $\theta$ is the road slope, and $f$ is the rolling resistance coefficient. A typical two-degree-of-freedom yaw plane vehicle model is used in this article, wherein only the vehicle's lateral and yaw motion are considered for simplification. Detailed description can be found in [47].

### A. Outer Loop: Lateral MPC-Based Driver Model

In real-time applications, the desired $\gamma$ and $\beta$ are determined by the lateral driving behavior of the human driver (or an autonomous driving system, as shown in Fig. 1), e.g., steering wheel angle. For simulation, we develop a lateral driver model to simulate a human driver in the outer loop, by tracking the lateral traveling distance $s_{y,\text{ref}}$. Then, the references of $\gamma$ and $\beta$ obtained are provided to the inner loop controller—LSCS. Suppose that the longitudinal speed is constant, as $v_x = v_{x0}$; then, the dynamics for the driver modeling can be summarized as

$$\frac{d}{dt}s_y(t) = v_x\sin(\varphi(t)) + v_y(t)\cos(\varphi(t)) \quad (2a)$$

$$\frac{d}{dt}\varphi(t) = \gamma(t) \quad (2b)$$

where $s_y$ is the lateral traveling distance, $\varphi$ represents the heading angle in the global coordinate system, $\gamma$ is the yaw rate of the vehicle body, and $v_y$ is the lateral velocity, which is determined by $v_x$ and $\beta$, expressed as $v_y(t) = \tan(\beta(t))v_x$. In general, given the desired trajectory of the vehicle, a human driver uses a dynamic model (based on the driving experience) to predict the future dynamic response of the vehicle and then generates a steering maneuver by tracking the desired path. This demonstrates an inherent similarity between the MPC and the driver's driving behavior [48]. Therefore, in this article, we use an MPC-based controller to model the driver's behavior by solving an optimal control problem (OCP), as

$$\min \int_t^{t+T} [(s_y(t) - s_{y,\text{ref}}(t))^2 + p_1\gamma^2(t) + p_2\beta^2(t)]dt \quad (3)$$

where $p_1$ and $p_2$ are weighting factors. The control input to be solved is $u = [\gamma, \beta]^T$, and the system state is $x = [s_y, \varphi]$. As described in [6] and [47], the maximum yaw rate that the tires can provide to the vehicle body is $|\gamma_{\max}| = \mu g/v_x$, where $\mu$ represents the road friction coefficient. Once the real yaw rate is larger than this limit, the vehicle would be out of control. Besides, the sideslip angle must be bounded by a function of the tire–road friction coefficient, as mentioned in [47] and [49]. The widely used formula is expressed as $|\beta_{\max}| = \arctan(0.02\mu g)$, which roughly corresponds to the desirable limits on different roads. Particularly, on a packed snow road ($\mu \approx 0.3 - 0.35$), the upper bound of the sideslip angle is set to $|\beta_{\max}| \approx 0.06$. Then, the above OCP is subject to the physical constraints $|\gamma_{\max}|$ and $|\beta_{\max}|$.

### B. Inner Loop: LSCS and Motor Drives

*1) LSCS:* In the inner loop, the controller is designed to track the required sideslip angle $\beta_{\text{ref}} = \beta^\circ$ and yaw rate $\gamma_{\text{ref}} = \gamma^\circ$ generated by the driver model. The simplified vehicle dynamics can be described as follows:

$$\frac{d}{dt}\beta(t) = \frac{F_{yf}(t) + F_{yr}(t)}{v_x M} - \gamma(t) \quad (4a)$$

$$\frac{d}{dt}\gamma(t) = \frac{L_f F_{yf}(t) - L_r F_{yr}(t) + M_z(t)}{I_z} \quad (4b)$$

where $F_{yf}$ and $F_{yr}$ represent the resultant lateral forces of the front and rear tires, respectively; $L_f$ and $L_r$ are the distances from the center of mass to the front and rear axles, respectively; $M_z$ is the additional yaw moment from the difference between longitudinal tire forces; and $I_z$ is the moment of inertia of each wheel. In the above equation, $F_{yf}$ and $F_{yr}$ are determined by the tire characteristics, road conditions, tire sideslip angle, front-wheel steering angle, etc. Due to the high complexity of tires, the tire model to establish the lateral forces is typically simplified to an empirical formula through a large amount of experimental data. As one of these empirical expressions, the single friction coefficient Fiala tire model is widely used in yaw stability control [50]. Suppose that the front-wheel steering angle $\alpha$ is small and $\tan(\alpha) \approx \alpha$. Then, there is

$$F_y(t) = -2C_y\alpha(t) + \frac{C_y^2}{3\mu F_z}|\alpha(t)|\alpha(t) - \frac{C_y^3}{3\mu^2 F_z^2}\alpha^3(t) \quad (5)$$

for $\alpha \leq \arctan(3\mu F_z/C_y)$, and otherwise, $F_y = -\mu F_z \text{sgn}(\alpha)$. Here, $C_y$ represents the cornering stiffness of the corresponding tire, and $C_{y,f}$ and $C_{y,r}$ are the cornering stiffness of the front and the rear tires, respectively; and $F_z$ is the nominal load at the tire. During a steering process, the sideslip angle of the front and rear tires is expressed as

$$\alpha_f(t) = \beta(t) + \frac{L_f}{v_x}\gamma(t) - \delta(t),\ \alpha_r(t) = \beta(t) - \frac{L_r}{v_x}\gamma(t) \quad (6)$$

where $\delta$ denotes the steering angle of the front wheel. Then, the lateral forces can be derived by $F_{y,f}(t) = F_y(C_{y,f}, \alpha_f, F_{z,f})$ and $F_{y,r}(t) = F_y(C_{y,r}, \alpha_r, F_{z,r})$, respectively.

For the design of LSCS, we use a simplified linear tire model by simplifying the resultant lateral force as $F_y(t) \approx -2C_y\alpha(t)$. Then, based on the system dynamics from (4) to (6), a linear state-space equation is formulated as follows:

$$\frac{d}{dt}X(t) = AX(t) + BU(t). \quad (7)$$

The state of the system is defined as $X = [\beta, \gamma]^T$; the control input is $U = [\delta, M_z]^T$. Then, a linear–quadratic regulator controller can be designed to track $X_{\text{ref}} = [\beta_{\text{ref}}, \gamma_{\text{ref}}]^T$ with $U^\circ = -KX + U_r$, where $U_r$ brings the outputs to the desired point, and $K$ is the feedback gain matrix to minimize the cost

$$J = \int_t^\infty [(X - X_{\text{ref}})^T Q(X - X_{\text{ref}}) + U^T RU]dt. \quad (8)$$

Here, $Q$ and $R$ are the positive weighting matrices.

*2) Torque Split and Motor Drives:* The function of a motor drive system is to track the torque commands to fulfill the yaw moment given by the LSCS. Suppose motors 1–4 represent the motor drives in the front left, front right, rear left, and rear right, respectively. Then, the torque reference of each motor can be calculated with $T_{\text{dem}}$ and the yaw moment $M_z$. The torques of the two left wheels are given by

$$\widetilde{T}_{\text{ref},1} = \frac{1}{4}T_{\text{dem}} - \Delta T_{\text{ref},1},\ \widetilde{T}_{\text{ref},3} = \frac{1}{4}T_{\text{dem}} - \Delta T_{\text{ref},3} \quad (9)$$

where $\Delta T_{\text{ref},1}$ and $\Delta T_{\text{ref},3}$ represent the extra torques to fulfill the yaw moment $M_z$, expressed as

$$\Delta T_{\text{ref},1} = \frac{L_f r_w}{(L_f + L_r)L_d}M_z \quad (10a)$$

$$\Delta T_{\text{ref},1} = \frac{L_r r_w}{(L_f + L_r)L_d}M_z \quad (10b)$$

where $L_d$ represents the distance from the front axle to the rear axle. Considering the physical limit, there is

$$T_{\text{ref},j} = \begin{cases} \widetilde{T}_{\text{ref},j}, & \text{if } \widetilde{T}_{\text{ref},j} \in [T_{mj,\min}, T_{mj,\max}] \\ T_{mj,\min}, & \text{if } \widetilde{T}_{\text{ref},j} < T_{mj,\min} \\ T_{mj,\max}, & \text{else} \end{cases} \quad (11)$$

where $T_{mj,\min}$ and $T_{mj,\max}$ are the minimum and maximum torques of the $j$th motor ($j = 1, 3$), respectively. Then, the torques of the two right wheels are determined by

$$\widetilde{T}_{\text{ref},2} = \frac{1}{4}T_{\text{dem}} + \frac{L_f r_w}{(L_f + L_r)L_d}M_z + \Delta T_{\text{ref},1} \quad (12a)$$

$$\widetilde{T}_{\text{ref},4} = \frac{1}{4}T_{\text{dem}} + \frac{L_r r_w}{(L_f + L_r)L_d}M_z + \Delta T_{\text{ref},3} \quad (12b)$$

and subject to the limits $[T_{mj,\min}, T_{mj,\max}]$, $j = 2, 4$.

Due to the high power density and smooth torque production, the interior permanent magnet synchronous machine (IPMSM) has been widely used as the traction motor of EVs. Fig. 2 shows the configuration of the IPMSM-based EDS, which includes both cyber and physical parts. Based on the torque command received from the vehicle control unit (VCU) and the feedback signals gathered from sensors, a flux controller is adopted alongside the maximum torque per ampere (MTPA) algorithm to generate the pulsewidth modulation (PWM) signals, which is then used to drive the IPMSM. The interaction between the cyber and physical systems is conducted through the sensors and the PWM drivers. The sensors collect the physical information, and the PWM drivers receive the cyber commands and feed physical signals into the power switches. In the cyber part, the reference flux vector $[\Phi_d, \Phi_q]^T$ is selected to track the torque command. To generate the maximum energy efficiency under the same torque requirement, various methods have been proposed in the literature, such as [51]–[54]. Because the main work of this article is to address the cyber-physical security of EVs, and the focus of the motor is dynamic performance, e.g., the capability of tracking the torque reference, we use MTPA to optimize the flux reference vector, which is a widely implemented algorithm in real applications. The diagram of the optimization is shown in Fig. 2. In addition, two proportional–integral controllers are used in the EDS to regulate the tracking error of the output torque and $d$-axis and $q$-axis current. Detailed procedures of the algorithm are described as in [25] and [34].

## III. Attack Taxonomy and Evaluation Metrics

### A. Modeling of Attack Taxonomy

To model the attack taxonomy, we assume that the attacker can illegally get access to in-vehicle communication buses while having no prior knowledge of the system. As shown in Fig. 1, we consider two categories of cyber-attacks: 1) sensor and parameter attacks; and 2) motor drive attacks, which may cause a degradation of tracking performance, reducing the dynamic performance of the actuator.

*1) Sensor and Parameter Attacks:* In the case of sensor and parameter attacks, a malicious attacker can either physically or remotely gain access to the powertrain sensors and generate false signals to perform the attack. According to the LSCS described above, the most dominating signals that might be attacked include the vehicle speed $v_x$, $\beta$, and $\gamma$. The parameters that may be modified are the moment of inertia $I_z$ and vehicle mass $M$ because both of them are hard to measure accurately. For example, in most situations, the moment of inertia is estimated, and the value applied to the control system is a nominal term. Once it is maliciously modified while within the boundary $I_z^{\text{atk}} \in [I_{z,\min}, I_{z,\max}]$, it is difficult to identify it. Similarly, the vehicle's mass is given by an estimator, which may vary with the number of passengers, road slope, and driving conditions. In this article, aiming at the five signals and parameters, we define

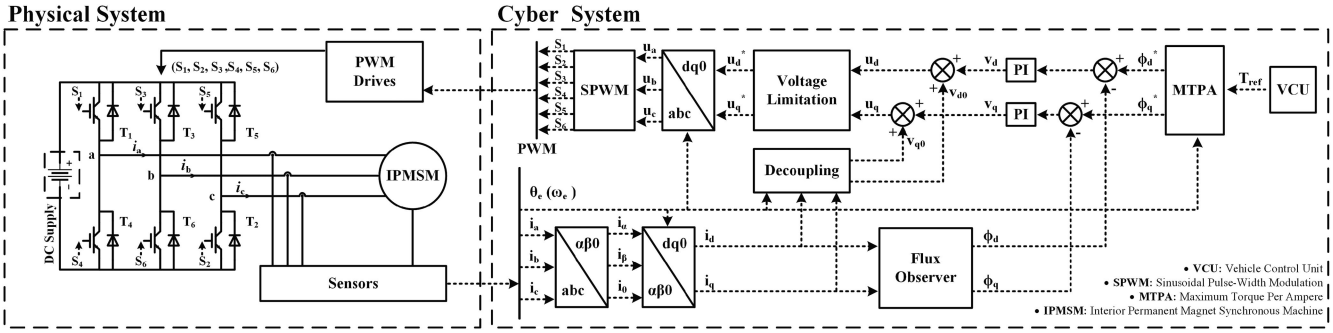


Fig. 2. Schematic diagram of the IPMSM drive.

TABLE I
DEFINITIONS OF ATTACKS ON SENSOR MEASUREMENTS AND PARAMETERS

| Attack Type | $\gamma$ [rad/s] | $\beta$ [rad] | $v_x$ [m/s] | $I_z$ [kg/m$^2$] | $M$ [kg] |
|---|---|---|---|---|---|
| Integrity Attack-1 | $\gamma_{\max} = 0.26$ | $\beta_{\max} = 0.06$ | $v_{x,\max} = 40$ | $I_{z,\max} = 5000$ | $M_{\max} = 2000$ |
| | $\gamma_{\min} = -0.26$ | $\beta_{\min} = -0.06$ | $v_{x,\min} = 5$ | $I_{z,\min} = 1000$ | $M_{\min} = 1000$ |
| | Cases 1-5 | Cases 6-10 | Cases 11-15 | Cases 16-20 | Cases 21-25 |
| Integrity Attack-2 | Cases 26-32 | Cases 33-39 | Cases 40-46 | Cases 47-53 | Cases 54-60 |

several types of cyber-attacks, including data integrity, replay, and denial of service (DOS) attacks. In each case, we denote the signal being attacked as $\bar{y}^{\text{atk}}$ ($\bar{y} \in \{\gamma, \beta, v_x, I_z, M\}$), which satisfies $\bar{y} \in [\bar{y}_{\min}, \bar{y}_{\max}]$.

The data integrity attacks are formulated as $\bar{y}^{\text{atk}} = \nu\bar{y} + \epsilon$, where $\epsilon$ and $\nu$ are unknown signals due to the malicious modification. Then, for each signal, we set five attack cases (denoted as integrity attack-1) as $\nu = 0$ and $\epsilon \equiv \bar{y}_{\min} + n(\bar{y}_{\max} - \bar{y}_{\min})/4$, $n = 0, 1, 2, 3, 4$, respectively. Then, the following seven cases (denoted as integrity attack-2) are designed by $\nu \in \{0.5, 1.5\}$ ($\epsilon = 0$) and $\epsilon \in \{\pm 0.1|\bar{y}|_{\max}, \pm 0.2|\bar{y}|_{\max}, white\,noise\}$ ($\nu = 1$), respectively. Here, $\epsilon$ satisfies $\epsilon \leq 0.2|\bar{y}|_{\max}$ to ensure fair comparison. The settings of case number are summarized in Table I.

In replay attacks, the measurements are repeated as $\bar{y}^{\text{atk}} \in \mathbf{y}$, where $\mathbf{y}$ is the set of past information. Three levels of attack intensity are used, as $t_{\text{replay}} \in \{0.01, 0.02, 0.04\}$ for $\gamma$ (Cases 61–63) and $t_{\text{replay}} \in \{0.05, 0.1, 0.2\}$ for $\beta$ (Cases 64–66), where $t_{\text{replay}}$ represents the replay time horizon. Due to the assumption that the attackers have no prior knowledge of the control system, the attacker cannot elaborate a stealthy replay attack to the control system, as discussed in [55]. In the DOS attacks, a sensor signal cannot reach the controller, and then, the missing sensor measurement is considered as the same as the value it last received. Suppose that the attacks start at $t^{\text{atk}}$ and end at the final time of a steering process; then, in the DOS attacks, $\bar{y}^{\text{atk}} \equiv y(t^{\text{atk}})$. For each of the system state ($\gamma$ and $\beta$), we set four DOS attack cases by using different attack start times, as $t^{\text{atk}} = 13$ s, $t^{\text{atk}} = 14$ s, $t^{\text{atk}} = 15$ s, and $t^{\text{atk}} = 16$ s, respectively. Accordingly, these attacks are denoted as Cases 67–70 for $\gamma$ and Cases 71–74 for $\beta$. For others cases, we set $t^{\text{atk}} = 12$ s, and in all of the cases, $t^{\text{final}} = 22$ s.

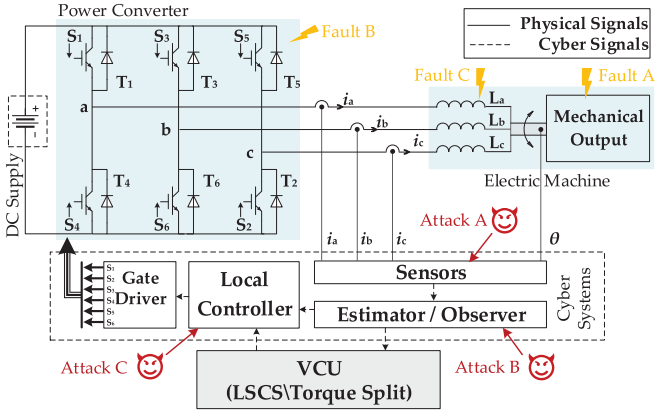


Fig. 3. Potential cyber-physical threats in the EDS.

*2) Anomaly in a Motor Drive:* Due to the communication between the local devices to the higher controller—LSCS—and torque split in the VCU, the local EDS is vulnerable to cyber-threats. Hence, besides the sensor measurements and parameters, the device-level motor drive might also show misbehavior in tracking the torque requirement caused by certain cyber or physical threats. In traditional EDSs, the communication to the external systems is limited. Thus, the local EDS is hardly targeted by the cyber-attacks, and then, the physical failures are the primary concerns. For example, as shown in Fig. 3, 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 interturn short-circuit faults (Fault C).

In the past few decades, the physical failures of the EDS and related components and devices are widely studied. In [56]

and [57], some of the research outcomes and progress of EDS condition monitoring and fault diagnosis were reviewed, such as interturn short-circuit fault detection in the electric machines and open-circuit fault diagnosis in power electronics modules. With the increasing computational capability of the digital signal processors and microcontrol units, and the development of the communication network techniques, the local controllers can achieve advanced functionalities, such as online optimization, fault diagnosis, and multimode operations. Such functions require the modern motor drive system to communicate more frequently with the onboard networks than ever, which makes the EDS much more vulnerable not only to the faults from the physical domains but also the malicious attacks from the cyber networks.

In Fig. 3, some common attacks are denoted. Attack A represents the sensor attacks, in which the attacker could fabricate false sensor signals or block the communication between sensors and estimators so that the control systems may crash because of the false feedback signals. Attack B represents the estimator attacks or observer attacks, in which the attacker could use false signals or parameters to deactivate the estimator so that the estimated system states could be the ones in favor of the attacker. 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 so that the physical systems may be misguided to an unsafe operation region. Note that both of the malicious attacks and physical faults may lead to failure to track its torque reference. To observe the impact of the attacks/faults in the motor drive on the steering system, from the aspect of the tracking capability of the motor, first, we consider several attack strategies to make the actual output torque a constant value $T_2^{\text{atk}} \equiv \mathcal{C}$. Accordingly, we define Cases 75–77 as $\mathcal{C} \in \{T_{m2,\min}, 0, T_{m2,\max}\}$, respectively. More generally, the actual output torque of the damaged motor is set to $T_2^{\text{atk}} = T_{2,\text{ref}} + w$, where $w$ represents the tracking error, which is limited by a boundary $[w_{\min}, w_{\max}]$. We set Cases 78–80 as $w = w_{\min} = -200$ N·m, $w = w_{\max} = 200$ N·m, and $w = white\ noise$, respectively.

*Remark 1:* In fact, if the attackers have more knowledge of the system, they can perform much more subtle and powerful attacks [58]. However, to identify the underlying model of the system is usually a hard problem, and only highly skilled attackers have the ability to do so. Therefore, in this article, we will focus on simple attack strategies that are easy to implement. Because $v_x$, $I_z$, and $M$ are constant, we will not perform replay and DOS attacks on them.

### B. Evaluation Metrics for Vulnerability Assessment

As stated above, the cyber-attacks are orchestrated to cause more significant tracking errors and instability. Although, in some cases, the LSCS cannot track the references well, the vehicle may also complete the steering task because of the robustness of the outer loop control system (driver model), especially for those skilled drivers. To emphasize the damage caused by the malicious behaviors in terms of system performance, we set the time horizon of observation as $[t_{\text{obv}}, t_{\text{obv}} + T_{\text{obv}}]$. In the LSCS, we define the overall tracking error as

$$\boldsymbol{I}_{\text{error}} = \frac{1}{\|X_{\text{ref}}\|_{\max} T^{\text{obv}}} \int_{t^{\text{obv}}}^{t^{\text{obv}}+T^{\text{obv}}} \|X - X_{\text{ref}}\|_{Q_m} dt \quad (13)$$

where $\|X_{\text{ref}}\|_{\max}$ represents the maximum norm of $X_{\text{ref}}$, $\|X - X_{\text{ref}}\|_{Q_m}$ represents $(X - X_{\text{ref}})^T Q_m (X - X_{\text{ref}})$, and $Q_m$ is the weighting factor. In the outer loop system, the metric reflecting the difference between the desired and actual trajectories can be derived by

$$\boldsymbol{I}_{\text{driver}} = \frac{1}{|s_{y,\text{ref}}|_{\max} T^{\text{obv}}} \int_{t^{\text{obv}}}^{t^{\text{obv}}+T^{\text{obv}}} |s_y - s_{y,\text{ref}}| dt. \quad (14)$$

To reflect the difficulty of completing the steering action, we define another two evaluation metrics, as follows:

$$\boldsymbol{I}_u = \frac{1}{T^{\text{obv}}} \int_{t^{\text{obv}}}^{t^{\text{obv}}+T^{\text{obv}}} U^T R_m U \, dt \quad (15)$$

and $\boldsymbol{I}_\delta = |\delta|_{\max}$, where $R_m$ is the weighting factor. The larger $\boldsymbol{I}_\delta$ and $\boldsymbol{I}_u$, the harder the driver can control the vehicle. In this article, we set $t^{\text{obv}} = 10$ s and $T^{\text{obv}} = t^{\text{final}} - t^{\text{obv}}$.

## IV. Simulation Results and Impact Analysis

In this section, we present the evaluation results of the specified attack cases under a double-lane-change maneuver, in which the sampling time is set to 1 ms. In the following, based on the different effects of the defined attacks, we analyze the cyber-physical security of the LSCS, which can serve as guidelines for attack detection and countermeasures.

### A. Observation of Specific Attack Cases

For a detailed analysis of the cyber-physical attacks, we show the results of Cases 1, 26, 61, and 67 for $\gamma$ to observe the impact of different cyber-attacks. Trajectories of the system states and control inputs are shown in Fig. 4, which indicates that cyber-threats can heavily damage the system. From the results of Cases 1 and 26, we can observe that data integrity attacks can lead to a significant tracking error of $\gamma$ and $\beta$, but has little influence on the outer loop system (the MPC-based driver model). Thus, although the LSCS is affected by cyber-attacks, if the attacker cannot continuously hijack the control system and cause its divergence, to some extent, the driver can still complete the steering operation.

In Case 61, the replay attack has a significant influence on system stability. During the attack, the inner loop system rapidly moves beyond their bounds. More specifically, when the system states and their references are constant values or vary slowly, the impact of replay attacks is relatively smaller (e.g., the results during [12,13.72] s despite the start time $t^{\text{atk}} = 12$ s). It implies that in a real driving scenario, the replay attacks have little influence when the driving conditions are straight travel or lane-keeping maneuver in a road with a large radius of curvature. However, once the reference starts to change massively within a steering process, this impact will be more considerable, even cause divergence. In such a case (Case 61), although the resulting $s_y$ seems to work regularly, only showing a larger ripple in tracking its reference, the system has been unstable because of

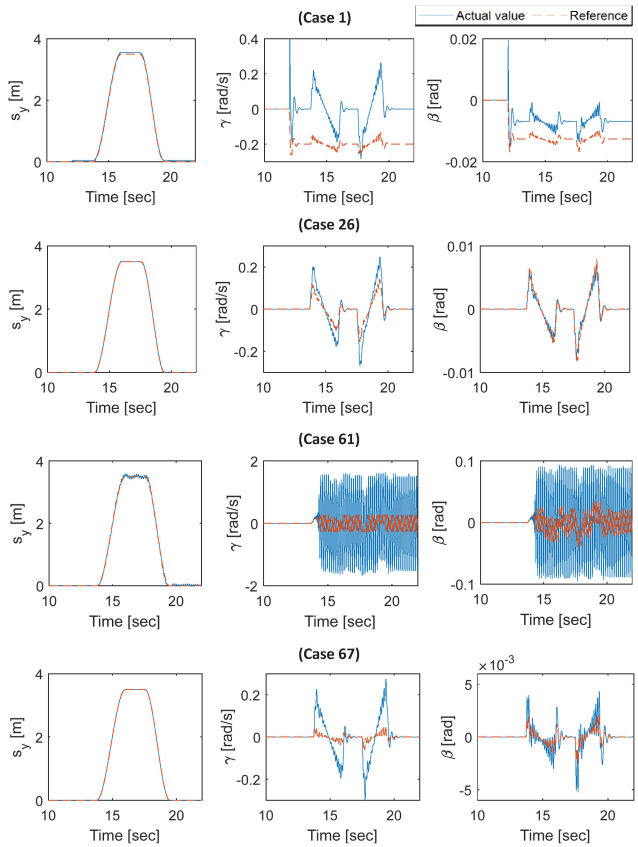


Fig. 4. Results of different attack cases and types.

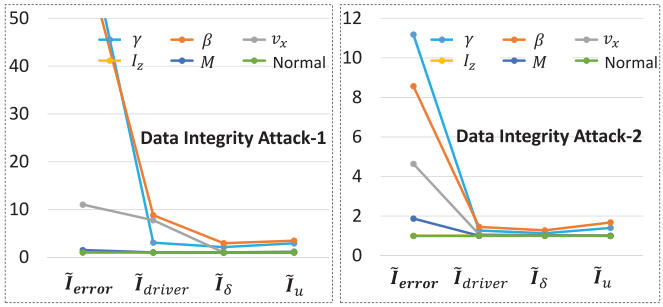


Fig. 5. Results of data integrity attacks, where $\widetilde{\boldsymbol{I}}_{\text{error}}$ of $\gamma$ and $\beta$ in the left graph are 72.97 and 65.91, respectively.

TABLE II
AVERAGE EVALUATION METRICS IN DIFFERENT ATTACKS

| Attack & Target | $\widetilde{\boldsymbol{I}}_{error}$ | $\widetilde{\boldsymbol{I}}_{driver}$ | $\widetilde{\boldsymbol{I}}_{\delta}$ | $\widetilde{\boldsymbol{I}}_{u}$ |
|---|---|---|---|---|
| Replay attacks on $\gamma$ | – | – | – | – |
| Replay attacks on $\beta$ | 1.887 | 2.552 | 0.681 | 4.967 |
| DOS attacks on $\gamma$ | 48.01 | 3.588 | 0.610 | 7.910 |
| DOS attacks on $\beta$ | 10.21 | 2.471 | 0.662 | 7.794 |
| Attacks on $T_{m,2}$ | 3.464 | 2.629 | 0.634 | 5.869 |

the limitation of tire force. The results also show that the DOS attack is similar to the data integrity attack-1 because both of them generate a constant value to the controller and cause more substantial tracking errors.

### B. Statistical Results and Impact Analysis

For a comprehensive analysis of these impacts with different attack types and targets, we conduct the simulation with various cyber-threats. Because of the space limitation, we present the results by the statistical form. Based on the massive results, the evaluation metrics are reformulated by $\widetilde{\boldsymbol{I}}_{\kappa} = \Sigma_{k=N_c}^{N_c+m-1} \boldsymbol{I}_{\kappa,k}/\boldsymbol{I}_{\kappa,\text{nom}}/m$ for each attack target with a certain attack type, where $\kappa = \{error, driver, \delta, u\}$ denote the corresponding metrics, $\boldsymbol{I}_{\kappa,\text{nom}}$ represents the corresponding value in normal situations, $N_c$ represents the start case number of an attack target, and $m$ represents the number of attack cases. For example, for integrity attack-1 on $v_x$, $N_c = 11$ and $m = 5$, and for integrity attack-2, $N_c = 40$ and $m = 7$. Then, the statistical graphs of data integrity attacks are given in Fig. 5, and other results are given in Table II, wherein the term "–" indicates the situation of unstable situations.

From the results in the tables and graphs, we can conclude that replay attacks can severely damage the steering system and may cause instability in the system. By comparing the results of replay and DOS attacks targeting $\gamma$ and $\beta$, we note that the system state $\gamma$ is much more sensitive to the cyber-attacks, which indicates that in real-life applications, the accuracy and communication delay of $\gamma$ is a worthy focus of concern. By comparing the different attack types, the replay, DOS, and data integrity attack-1 have more influence on the system than other types. The metrics of different attack targets show that the impacts of cyber-threats on sensor measurements are larger than parameters. It is worth noting that in addition to the replay attack, the data integrity attack-1 may also cause instability in the system. To clarify this, we present one of the unstable results, as shown in Fig. 6, wherein $\bar{v}_x^{\text{atk}} = v_{x,\max}$. The trajectory of $s_y$ shows the dangerous situation once the system is affected.

Compared to data integrity attack-1, integrity attack-2 that only changes the signal's amplitude and average value has less impact on system performance. Although the references of $\gamma$ and $\beta$ are not tracked well, the MPC-based driver can adjust its behavior to complete the steering action, which benefits from the robustness of MPC. For further analysis, we present the trajectories of Case 26, as shown in Fig. 7. We can observe that although the actual value is $\gamma \approx 2\gamma_{\text{ref}}$ due to the modified sensor measurement $\bar{\gamma}^{\text{atk}} = 0.5\gamma$, the final trajectory of $\gamma$ is similar to the normal conditions. It is because the MPC-based driver controller can adjust the uncertainty of control inputs, as $u_{\text{actual}} \neq u_{\text{command}}$, so that the generated reference is lower than the normal values as well. Therefore, in real-life applications, when the LSCS is affected within a certain boundary, a skilled driver can still stabilize the system. Note that in real-life applications, for most unskilled human drivers, they cannot correctly complete the steering action with the abnormal steering system.

Moreover, the attacks on $I_z$ and $M$ are generally utilized by the attacker to cause performance degradation. While they may not immediately cause physical damages and out of control, it

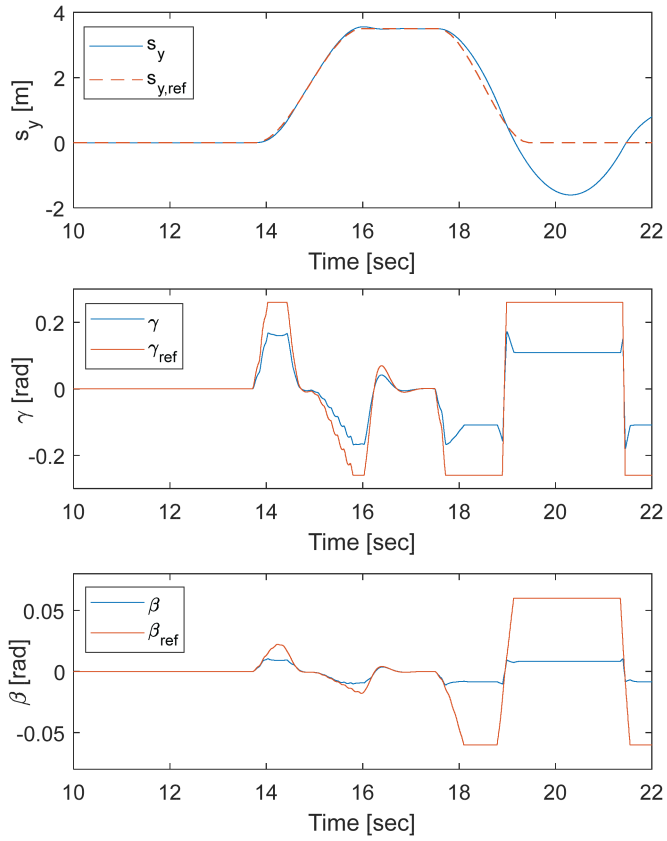


Fig. 6. Example of system instability (Case 15).

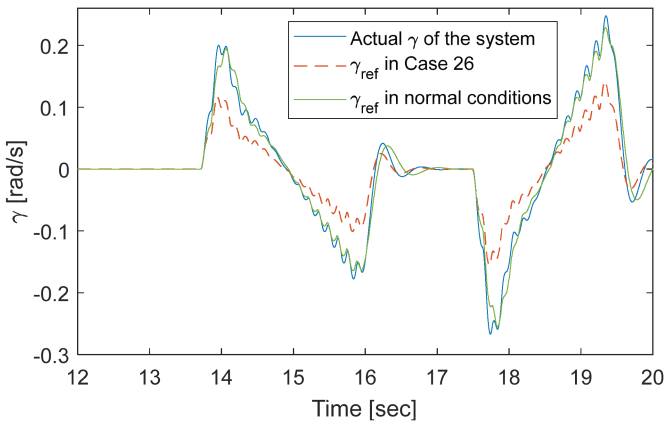


Fig. 7. Data integrity attacks on $\gamma$ (Case 26).

will potentially result in a long-term deterioration in the steering system, leading to poor driving experience and reduction of vehicle's monetary value. Furthermore, because of the limitation of the influence of the additional yaw moment $M_z$, the cyber-physical attacks on the motor drive system (e.g., $T^{\text{atk}}_{m,2}$) only have little influence on the system stability, but can also cause the degradation of the lateral driving performance. Concerning the evaluation metrics, the statistical graphs demonstrate that $\boldsymbol{I}_{\text{error}}$ and $\boldsymbol{I}_u$ can better reflect the negative consequences caused by cyber-physical attacks. In most cases, the steering angle of the front wheel shows a noticeable increase, which indicates more challenging to complete the steering process.

In summary, we have shown that all of the evaluation metrics can reflect the impact of various cyber-attacks, especially the tracking error $\boldsymbol{I}_{\text{error}}$. Then, by using these metrics, one can develop data-based or model-based detection and diagnosis approaches in practical applications. However, when using these evaluation metrics to develop an attack detector, the critical problem is how to obtain the actual signal value while being attacked. One of the simple solutions is to use a separate sensor in the detection system, which is assumed and cannot be affected. Nevertheless, this strategy will increase the manufacturing cost. Therefore, in the following section, we present a model-based observer to calculate the evaluation metrics to improve the cyber-physical security of EVs.

## V. Detection Methodology

### A. Coordinated Detection Methodology

Followed by the system dynamics in (7), we design a state observer to estimate the system states, as follows:

$$\frac{d}{dt}\hat{X} = A\hat{X} + BU + L(\widetilde{X} - \hat{X}) \tag{16}$$

where $\hat{X}$ and $\widetilde{X}$ represent the estimated and feedback states, respectively; and $L$ is the observer gain that ensures observer stability. In general, the index to detect the attacks is the output estimation error at time instant $k$, which is expressed as $r_k = \mathcal{G}(\widetilde{X}_i, \hat{X}_i), i = k-l+1, ..., k$ ($l = 10$ represents the window size of detection). Then, $r_k$ can be applied into the cyber-physical attack detection by using the threshold $\tau > 0$. Based on the sequences $\hat{X}_i$ and $X_i$ ($i = k-l+1, ..., k$) over the window size of detection, the residual signal at time instant $k$ can be defined as

$$r_k = \sum_{i=k-l+1}^{k} (X_i - \hat{X}_i)^T Q_m (X_i - \hat{X}_i)/l. \tag{17}$$

Typically, the residual $r_k > \tau$ is considered as a proxy for the presence of attacks. However, when considering the system uncertainty (e.g., the nonlinear lateral dynamics) and the stochastic attack scenarios, the residual alone cannot guarantee the accuracy of detection. Then, based on the impact analysis, we propose a coordinated detector by using both the residual $r_k$ and the introduced evaluation metric $\boldsymbol{I}_{\text{error}}$. Suppose the current time instance is $k$; then, within the same window size of detection, the estimated index of $\hat{\boldsymbol{I}}_{\text{error},k}$ is calculated by

$$\hat{\boldsymbol{I}}_{\text{error},k} = \sum_{i=k-l+1}^{k} (\hat{X}_i - X_{ref})^T Q_m (\hat{X}_i - X_{\text{ref}})/l. \tag{18}$$

The detector will also trigger an alarm if $\hat{\boldsymbol{I}}_{\text{error},k} > |\boldsymbol{I}_{\text{error,nom}}|_{\max}$, where $|\boldsymbol{I}_{\text{error,nom}}|_{\max}$ represents the maximum of $\boldsymbol{I}_{\text{error,nom}}$ under the normal driving condition. Note that in real-world applications, the two thresholds should be statistical values extracted from a large number of simulations and experiments. As a case study, we set thresholds as the maximum values in the same driving conditions with no cyber-physical

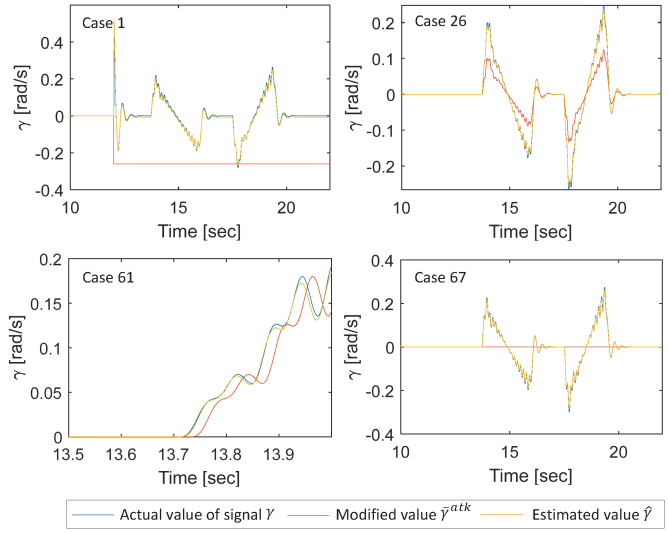


Fig. 8. Sensor measurements of $\gamma$ in different attack cases.

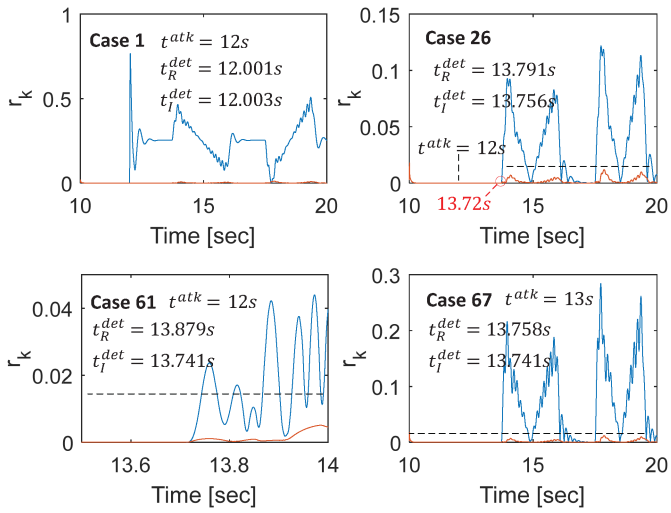


Fig. 9. Residual $r_k$ and the detection results $t_R^{\text{det}}$ and $t_I^{\text{det}}$ in different attack cases, where "13.72 s" in the second graph is the start time of the steering process.

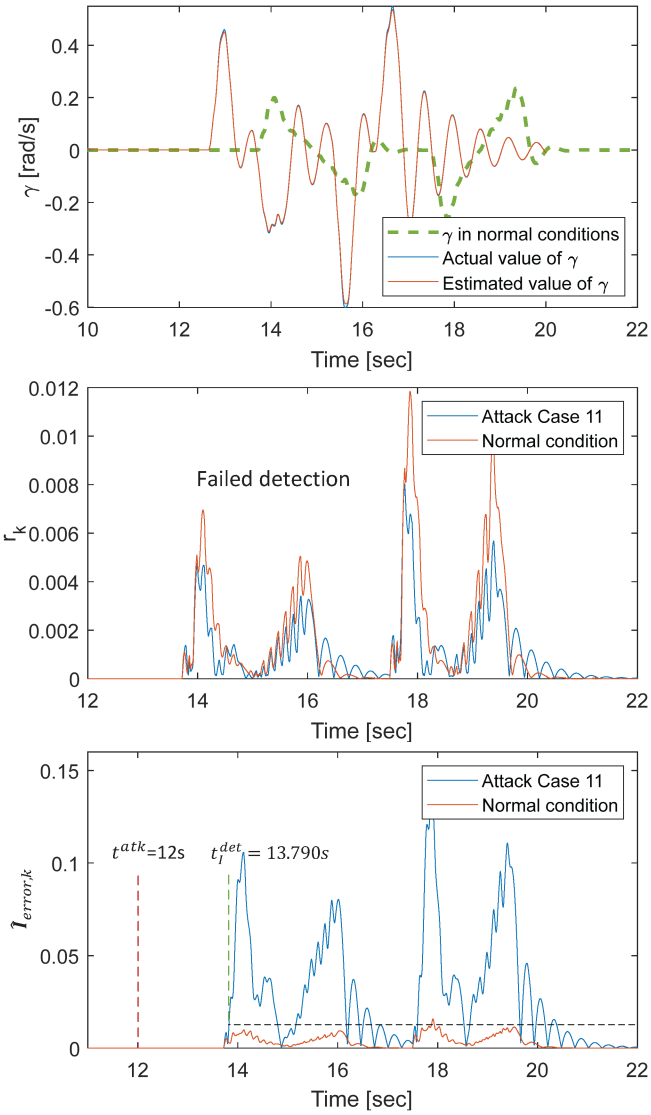


Fig. 10. Results of attack Case 11, where failed detection means unable to detect the cyber-attacks.

attacks. Then, according to the simulation results, $\tau = 0.0119$ and $|\boldsymbol{I}_{\text{error,nom}}|_{\max} = 0.0159$. Moreover, we denote $t^{\text{det}}$ as the time when the threats are detected.

The results of Cases 1, 26, 61, and 67 are shown in Figs. 8 and 9, from which we can see that the designed observer can estimate the system states well, even though the attacker maliciously modifies the sensor measurements. Based on the residual $r_k$ in (17), the cyber-threats can be quickly identified. It should be noted that in those data integrity attacks expressed as $\hat{y}^{\text{atk}} = \nu\hat{y}$ and replay attacks, e.g., Cases 26 and 61, if the system states are approximately zero (straight-line driving condition), the impact of these cyber-attacks is little. Accordingly, the $r_k$ remains within reasonable limits. Once the steering action is given by the driver, the residual will significantly increase. Besides, consider the detection time $t^{\text{det}}$ by using $\boldsymbol{I}_{\text{error},k}$; we can see that the index $r_k$ shows better capability. In fact, for the scenario that the system states are affected, the residue can directly reflect the negative consequence of the cyber-attacks, but $\boldsymbol{I}_{\text{error},k}$ is an indirect response. However, when the parameters or other parts of the control system are affected rather than the states, the situation will be different. For example, for Case 11 (the vehicle speed $v_x$ is affected) in Fig. 10, $\boldsymbol{I}_{\text{error},k}$ still performs a drastic change compared to the normal conditions, while the residual $r_k$ fails to identify the attack despite the accurate estimation of the system states. In should be noted that in the second graph of Fig. 10, we can see that the resulting residual is rather small and even lower than the normal values. It is because the estimation accuracy would be influenced by the working conditions, for instance, the difference between the trajectories of $\gamma$ in Case 11 and normal conditions.

Based on the above analysis, we propose a coordinated detection method by using both of the residual $r_k$ and $\boldsymbol{I}_{\text{error},k}$.

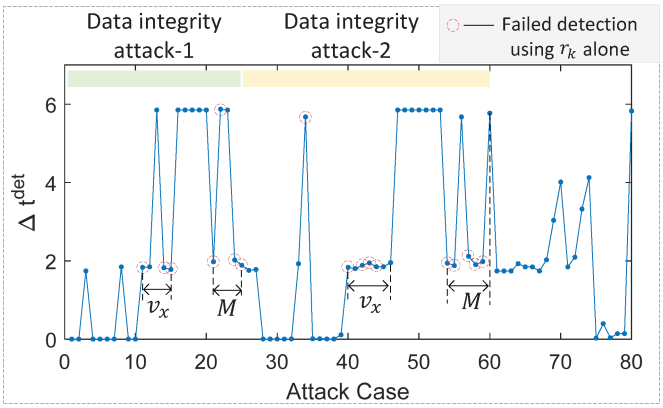


Fig. 11. Detection time of the proposed state-observer- and evaluation-metric-based detection method (blue line).

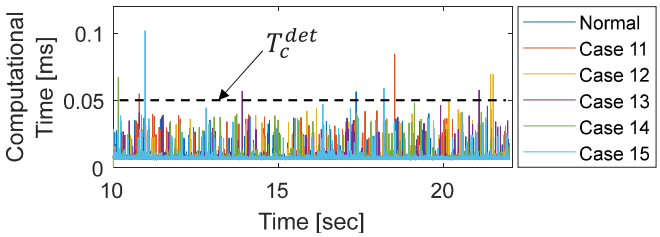


Fig. 12. Extra computational time required for the detection.

The final detection time $t^{\text{det}}$ is calculated by $t^{\text{det}} = \min\{t_R^{\text{det}}, t_I^{\text{det}}\}$, where $t_R^{\text{det}}$ and $t_I^{\text{det}}$ represent the detection times of $r_k$ and $\boldsymbol{I}_{\text{error},k}$, respectively. The results of all of the defined attack cases are shown in Fig. 11, wherein $\Delta t^{\text{det}} = t^{\text{det}} - t^{\text{atk}}$ and is used to reflect the timeliness of detection. By using the residual-based detection method alone, the detection rate is $63/80 \approx 79\%$, and most of the failure detection is in the data-integrity attacks on $v_x$ and $M$. With the proposed coordinated detection method, the overall detection rate is improved to 100%, which demonstrates better effectiveness.

*Remark 2:* In this article, for a case study, we only use one of the proposed evaluation metrics $\boldsymbol{I}_{\text{error},k}$ to design the anomaly detector. In real engineering applications, one can also choose the other one or more metrics as the detection indexes according to the characteristics of a specific system.

### B. Extra Computational Burden Required for the Detector

To observe the extra computational burden required for this method when applied in a real-time situation, we record the computational time of the developed detector. The simulation is run on an Intel(R) Core (TM) i7-9750 CPU (2.60 GHz), and the computational time is obtained by using the CPU command in MATLAB. Fig. 12 presents the results of normal and attack scenarios over the whole driving cycle, from which we can see that the average extra computational burden caused by the developed detector is less than $T_c^{\text{det}} = 0.05$ ms. Typically, the control period of an LSCS (for a car in production) is 20 ms (denoted as $\Delta T_c$), and the CPU computation capability in a computer is about 30–50 times (denoted as $\xi$) more than the controller chip in the VCU (in a production car). Then, the equivalent burden in online computation of the introduced detector can be as $\xi T_c^{\text{det}}/\Delta T_c \times 100\% \approx 7.5\% - 12.5\%$, which demonstrate that the extra computational burden is acceptable. The reason for the little computational burden is the fact that the observer gain in (16) is derived offline, and in a real-time situation, the proposed detection method only calculates the algebraic equations (16)–(18).

### C. Influence of the Delay in the Driver Model

Note that the MPC-based driver model in this article does not consider the delay because the main focus is to analyze the impact of cyber-physical attacks on LSCS. The MPC-based driver model reflects the ideal driver's ability to deal with emergency events during driving. If the car under investigation is driven by an autonomous driving system, the delay is negligible for system designs. However, if a human driver drives the vehicle, the delay problem due to the driver's reaction time needs to be addressed, which may influence the impact of cyber-attacks on the LSCS. To observe the system performance under both normal and abnormal situations with consideration of delay, we introduce a delay block in the control command of the lateral driver model, $\beta_{\text{ref}}$ and $\gamma_{\text{ref}}$ (without changing the MPC-based driver mode). According to the literature relevant on understanding and modeling the lateral human driver's behavior [59]–[61], the ability of humans to look ahead and preview information helps to reduce the time delay. One of the widely used delay models is Padé delay formula, expressed as

$$e^{-\tau_p s} = \frac{1 - 0.5\tau_p s}{1 + 0.5\tau_p s} \tag{19}$$

which approximates the human processing time delay, where $\tau_p$ is the delay time and is typically set to 0.04 s.

For the sake of detailed analysis, we present the results of Cases 1, 6, 26, and normal situations under different $\tau_p$, as shown in Fig. 13. From the results, we can see that, in normal situations, the delay time has little influence on the system performance. However, in attack cases, the increasing delay time would significantly influence the system stability, especially for integrity attack-1 on $\gamma$. The results indicate that the delay problem should be one of the major considerations when addressing the impact analysis of attacks on the LSCS, especially for vehicles driven by a human driver. In that case, a more accurate driver model needs to be established to reflect the driving characteristics better. Besides, in real-time applications, more factors need to be considered, such as the reaction and delay time, driving skill, driving habitus, etc. In fact, establishing an accurate description of the driver's characteristics is still a challenge due to the stochastic feature of driving behavior. Alternatively, one can improve the MPC-based driver model used in the article, by reoptimizing the driver's action considering the delay in the system dynamics, as $\dot{x}(t) = f(x(t), u(t - \tau_p), p)$ [61], where $f(\cdot)$ denotes lateral dynamics equations in (2), and $p$ represents the vector of parameters in the vehicle. Due to the space limit, in this article, we will not present the corresponding results.

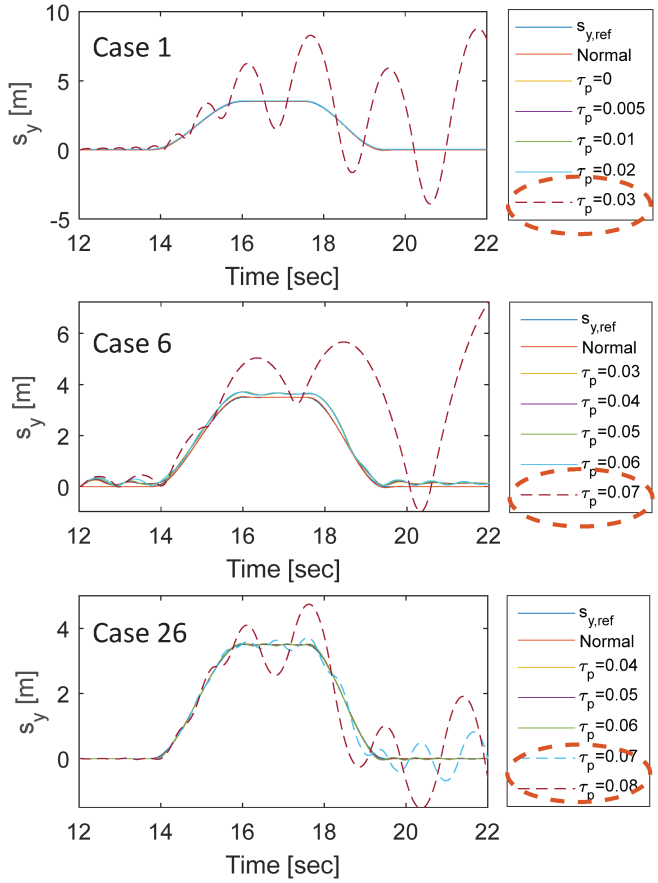


Fig. 13. Results of Cases 1, 6, 26, and normal situations under different $\tau_p$, wherein the delay time that may cause system instability is marked by a dashed box.

### D. 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 in tracking the torque reference. In the above, we have analyzed the impact of abnormal conditions in a motor drive on the vehicle's performance. In this subsection, we focus on distinguishing between malicious cyber-attacks and physical faults in a motor drive. Based on Fig. 3 and the corresponding description in Section III-A, several cyber-attack on sensors (see Attack A in Fig. 3) and an open-circuit fault (see Fault B in Fig. 3) are designed. The fault event is emulated by setting the switching signal for one of the insulated-gate bipolar transistors in the IPMSM traction inverter to zero. The target of replay and false data injection attacks is set to $i_a$. Specific definitions of these cyber-attacks are summarized in Table III, where $t^{\text{atk}}$ represents the start time of attacks and $t_{\text{replay}}$ represents the replay time horizon.

Then, we establish a high-fidelity EV powertrain model in a real-time hardware-in-the-loop (HIL) testbed (OPAL-RT OP5700), as shown in Fig. 14. In this testbed, we included a detailed model of both the motor (IPMSM) and the vehicle.

TABLE III
DEFINITIONS OF CYBER-ATTACKS ON $i_a$

| No. | Target | Description |
|---|---|---|
| A-1 | $i_a$ | $i_a^{atk} = 1.2i_a,\ t^{atk} = 152$s |
| A-2 | $i_a$ | $i_a^{atk} = -0.75i_a,\ t^{atk} = 77$s |
| A-3 | $i_a$ | $i_a^{atk} = -0.75i_a,\ t^{atk} = 360$s |
| A-4 | $i_a$ | $t_{replay} = 5$s, $t^{atk} = 72$s |
| A-5 | $i_a$ | $t_{replay} = 5$s, $t^{atk} = 103$s |

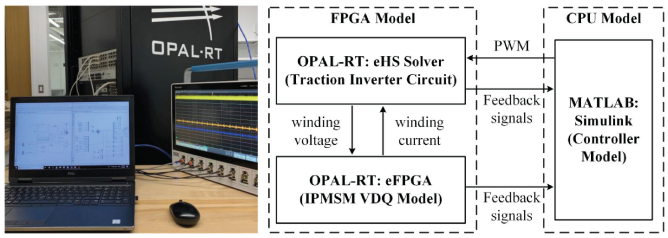


Fig. 14. OPAL-RT HIL real-time simulation testbed. The IPMSM here is modeled by the D–Q model (VDQ) from eFPGA library.

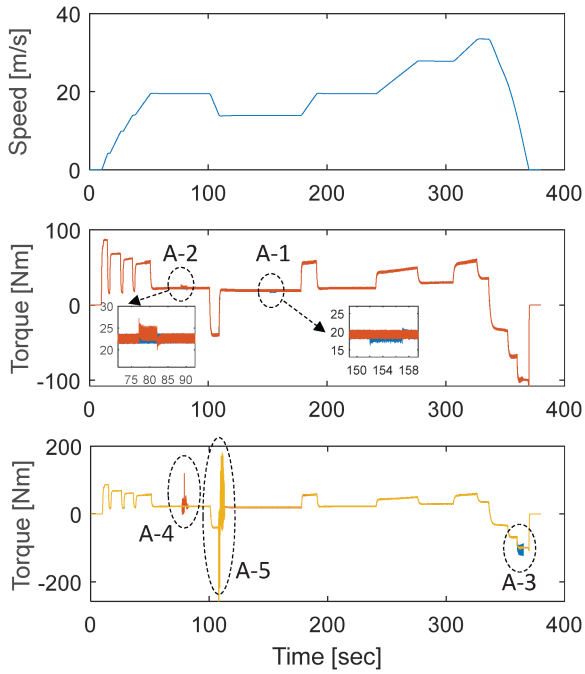


Fig. 15. Cyber-attacks on $i_a$ in real-time OPAL-RT testbed.

The sampling time is set to 25 $\mu$s. The driving cycle is chosen as a part of the New European Driving Cycle. Results of the cyber-attacks and faults on the motor drive are presented in Figs. 15 and 16. Overall speaking, we can observe that the torque increases dramatically once the fault is activated, while in most cyber-attacks, the impact is relatively smaller, such as cyber-attacks from A-1 to A-4 in Table III. Besides, by comparing the torques under the fault and the cyber-attack A-5, especially the local enlarged curves in Fig. 16(b), we can observe that

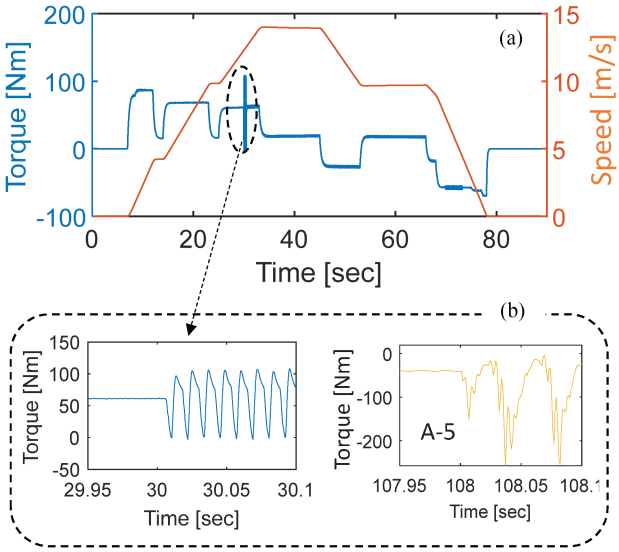


Fig. 16. (a) and (b) Open-circuit fault (Fault B in Fig. 3) in real-time OPAL-RT testbed, where the figure marked A-5 in (b) is a local enlarged results of A-5 in Fig. 15.

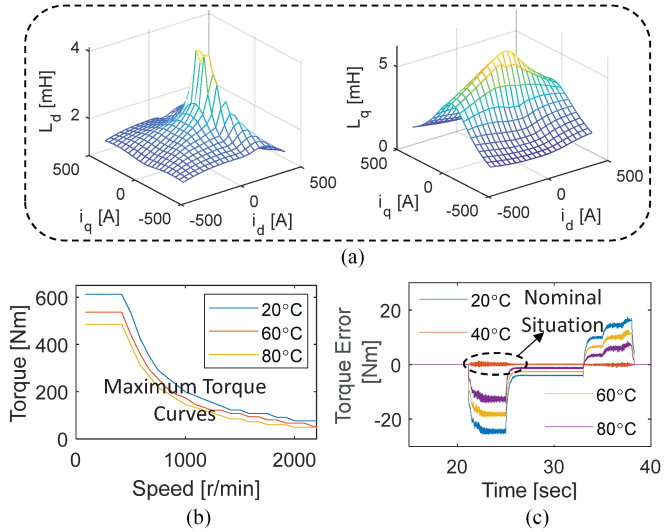


Fig. 17. Influence of the nonlinear characteristics of motor drives. (a) Saturation effects. (b) and (c) Maximum torque curves and toque tracking error, respectively. The nominal temperature of the MTPA is 40 °C.

there is an obvious distinction between their torque waveforms. Particularly, in a cyber-attack, the torque in a short period after the attack event presents an irregular torque ripple, while in the fault, the result shows a higher frequent periodic variation. This distinction may be caused by the different nature of cyber-attacks and faults. Essentially, from the perspective of control, the ways of cyber-attacks affecting the system are indirect—by causing an incorrect control input to the physical part. Therefore, the consequence depends on the controller, and the consequence is often irregular. Conversely, the results of a fixed type of fault may present a similar waveform pattern. This difference may help distinguish physical faults and cyber-attacks further.

### *E. Influence of the Nonlinear Characteristics of Motor Drives*

In real-time applications, the nonlinear characteristics that are not modeled in the control system, e.g., the saturation and heating effect, may also cause a higher tracking error of torque. According to the previous literature [62], [63], temperature variation (especially for long-term driving situations) will impact the physical model such as flux, ohmic resistance, efficiency, and the performance of the MTPA, for instance, saturation effects in the motor drive, as shown in Fig. 17(a), where $i_d$ is the $d$-axis current, $i_q$ is the $q$-axis current, and $L_d$ and $L_q$ are the inductances of $d$-and $q$-axis, respectively. In addition, we included temperature variation in the model, such as the maximum torque curves due to saturation and different temperatures in Fig. 17(b) and (c). We can observe that, even in normal conditions, there is a tracking error after taking to account model uncertainty due to temperature variation and saturation. Therefore, while analyzing the impact of cyber-attacks or faults on EVs, the varying performance due to model uncertainty and nonlinear characteristics has been thoroughly considered, which will serve as the guideline for selection of residual $\tau_k$. It should be noted that a higher level of residual may reduce detection accuracy. For example, cyber-attacks on the motor drive that cause limited torque ripple, tracking error, etc., will be mistaken for a normal variation of the system performance. Hence, designing an adaptive residual considering driving conditions, mode uncertainty, and varying nonlinear characteristics of motor drives is necessary.

### *F. Experiments Demo for Observation of the Impact of Cyber-Attacks on Motor Drives*

Note that the main focus of this article is cyber-physical security in EVs. Therefore, we consider the sensor and system parameter attacks on the vehicle level that will be impossible to validate by experiment. This is because for experimental validation of the proposed cyber-attack detection methodology, a human-in-loop vehicle testbed is needed to include both longitudinal (drive motors, battery, etc.) and lateral (driver simulator to generate the desired references of sideslip angle and yaw rate) components. Then, we present an experimental demo in this subsection to evaluate the impact of sensor attacks on the device-level motor drive prototype. While this lower power prototype is not the same as the motor drive we simulate for EVs, it serves as an example to illustrate the impacts of cyber-attacks on motor drives. Fig. 18 shows the testbed and results of preliminary experiments. In this demo test, we consider data integrity attacks, replay attacks, and DOS attacks targeting one of the current in the motor, $i_a$. Specifically, we observe the effect on the capability of tracking the torque reference. From the results, we can see that cyber-attacks may have a significant influence on the output torque of a motor drive, which would further affect the steering performance of the LSCS. After suffering from malicious attacks, the motor drive presents a larger tracking error for a period of time. This persistent effect needs to be considered in real-time attack detection.

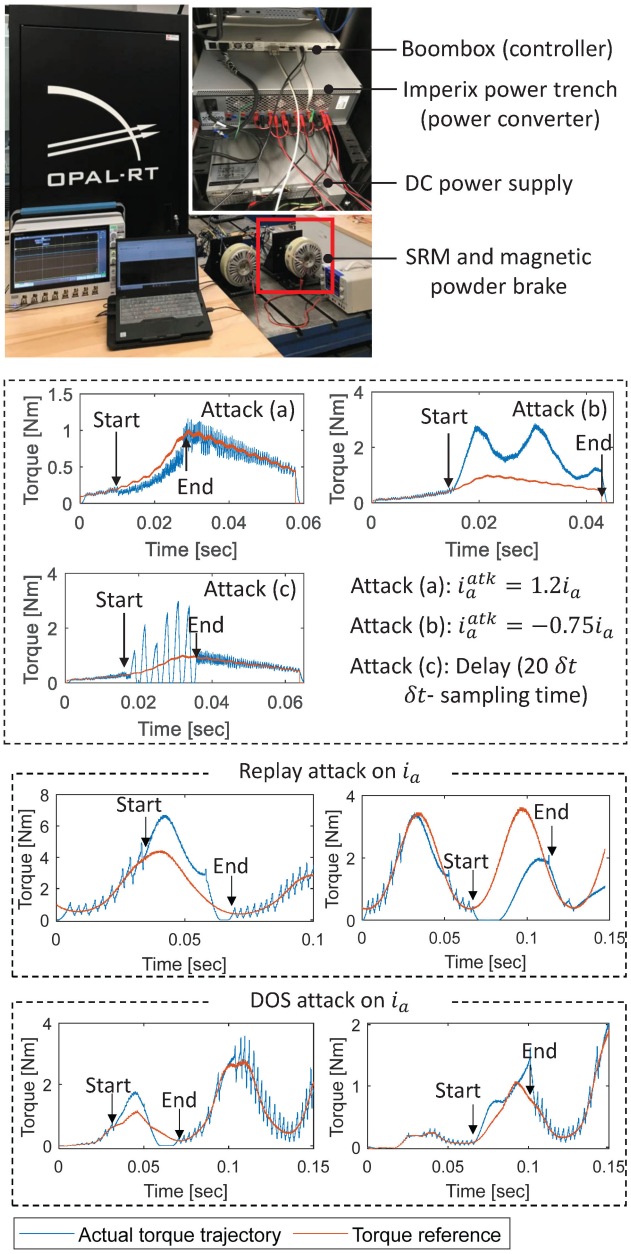


Fig. 18. Experimental demo results under a motor testbed. SRM represents switched reluctance motor.

## VI. Conclusion

In response to the cyber-physical-security initiative launched by the IEEE PELS, this article presents a systematic assessment of the cyber-physical security in EVs with four motor drives. Besides the sensor and system parameter attacks on the LSCS, we also consider the cyber-physical attacks/faults on the motor drive, which may deteriorate the tracking performance. The impact of performance degradation of the motor drive on the vehicle's safety is evaluated. Based on the driver-in-the-loop steering system, innovative index-based evaluation metrics in terms of system performance are developed, with which the transient and statistic results of cyber-physical attacks are analyzed. The simulation results indicate that replay, DOS, and data integrity attacks targeting the system parameters, sensors, and motor drive systems can significantly influence the system stability and its critical performance. To address this issue, we propose a coordinated residual and evaluation-metric-based detection method. The simulation results have shown a significant improvement in the detection accuracy. In real-time applications, the designed detector collects the sensor measurements and identifies the presence of a cyber-attack.

It should be noted that although the proposed cyber-detection method is simple, it shows satisfactory performance to detect a variety of cyber-attacks ranging from replay and DOS attacks to and data integrity attacks that may cause severe damage to the vehicle. Note that those cyber-attacks are the most common and devastating based on both academic literature and industrial studies [64]. The proposed detection method also provides a preliminary concept of performance-oriented cyber-attack detection methodology, which can be further studied in future. For example, use more types of performance indexes to reflect the system characteristics comprehensively. Besides, methodologies that can address the identified cyber-threat should be further developed, for instance, cyber-threat diagnosis, location, and antiattack (or attack-resilient) control. In general, an antiattack system is designed to improve the ability to mitigate the effect of cyber-attacks and recover the system after suffering from malicious attacks. For example, in [65], by introducing a two-step backstepping approach, an adaptive resilient control against sensor and actuator attacks was proposed, which can improve the transient performance when the attacks occur. Therefore, future investigation relevant to the issue of cybersecurity in EVs should include the design of antiattack systems.

## References

[1] 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 Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017.

[2] F. Li *et al.*, "Detection and identification of cyber and physical attacks on distribution power grids with PVS: An online high-dimensional data-driven approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, to be published.

[3] 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. 32617–32627, 2019.

[4] F. Li, J. Wang, and Z. Liu, "Motor torque based vehicle stability control for four-wheel-drive electric vehicle," in *Proc. IEEE Veh. Power Propulsion Conf.*, 2009, pp. 1596–1601.

[5] X. Wang, Y. Zhao, Y. Lian, and Y. Tian, "Lateral stability control algorithm of intelligent electric vehicle based on dynamic sliding mode control," SAE Tech. Paper 2016-01-1902, 2016.

[6] B. Ren, H. Chen, H. Zhao, and L. Yuan, "MPC-based yaw stability control in in-wheel-motored EV via active front steering and motor torque distribution," *Mechatronics*, vol. 38, pp. 103–114, 2016.

[7] B. Huang, S. Wu, S. Huang, and X. Fu, "Lateral stability control of four-wheel independent drive electric vehicles based on model predictive control," *Math. Probl. Eng.*, vol. 2018, 2018, Art. no. 6080763.

[8] X. Xin, X. Lu, H. Yuye, T. Guowen, and Y. Zhuoping, "Vehicle stability control based on driver's emergency alignment intention recognition," *Int. J. Automot. Technol.*, vol. 18, no. 6, pp. 993–1006, 2017.

[9] J. Sharifi and A. Amirjamshidi, "Fuzzy electronic stability control system for electric vehicle with four motor in wheel," *J. Control*, vol. 9, no. 4, pp. 41–53, 2016.

[10] Y. Zhao and C. Zhang, "Electronic stability control for improving stability for an eight in-wheel motor-independent drive electric vehicle," *Shock Vibr.*, vol. 2019, 2019, Art. no. 8585670.

[11] J.-S. Hu, Y. Wang, H. Fujimoto, and Y. Hori, "Robust yaw stability control for in-wheel motor electric vehicles," *IEEE/ASME Trans. Mechatronics*, vol. 22, no. 3, pp. 1360–1370, Jun. 2017.

[12] W. Zhao, X. Qin, and C. Wang, "Yaw and lateral stability control for four-wheel steer-by-wire system," *IEEE/ASME Trans. Mechatronics*, vol. 23, no. 6, pp. 2628–2637, Dec. 2018.

[13] F. Jia, Z. Liu, H. Zhou, and T. Teng, "A robust control invariant set approach to yaw stability of four-wheel drive electric vehicle," *IFAC-PapersOnLine*, vol. 51, no. 31, pp. 325–330, 2018.

[14] K. Nam, H. Fujimoto, and Y. Hori, "Lateral stability control of in-wheel-motor-driven electric vehicles based on sideslip angle estimation using lateral tire force sensors," *IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 1972–1985, Jun. 2012.

[15] M. Emırler *et al.*, "Lateral stability control of fully electric vehicles," *Int. J. Automot. Technol.*, vol. 16, no. 2, pp. 317–328, 2015.

[16] X. Jin, G. Yin, C. Bian, and P. Li, "Robust guaranteed cost state-delayed vehicle lateral stability control with applications to in-wheel-motor-driven electric vehicles," in *Proc. Amer. Control Conf.*, 2015, pp. 5408–5413.

[17] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, 2010, pp. 447–462.

[18] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, 2011, pp. 1–16. [Online]. Available: https://www.usenix.org/legacy/event/sec11/tech/full_papers/Checkoway.pdf

[19] B. Yang, L. Guo, and J. Ye, "Real-time simulation of electric vehicle powertrain: Hardware-in-the-loop (HIL) testbed for cyber-physical security," in *Proc. IEEE Transp. Electrific. Conf. Expo*, 2020, pp. 63–68.

[20] L. Guo *et al.*, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Trans. Ind. Inform.*, to be published.

[21] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Trans. Ind. Inform.*, vol. 16, no. 2, pp. 1417–1426, Feb. 2020.

[22] A. Greenberg, "Hackers remotely kill a jeep on the highway—With me in it," 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[23] P. Panda, "Cyber attacks in connected cars: What tesla did differently to win," 2017. [Online]. Available: https://www.appknox.com/blog/cyber-attacks-in-connected-cars

[24] L. Guo, J. Ye, and L. Du, "Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks," *IEEE Trans. Transp. Electrific.*, to be published.

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

[26] C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," Nat. Renew. Energy Lab., Golden, CO, USA, Tech. Rep. NREL/TP-5400-74247, 2019.

[27] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *Proc. IEEE Intell. Veh. Symp.*, 2018, pp. 421–426.

[28] M. Levi, Y. Allouche, and A. Kontorovich, "Advanced analytics for connected car cybersecurity," in *Proc. IEEE 87th Veh. Technol. Conf.*, 2018, pp. 1–7.

[29] X. Shao, C. Dong, and L. Dong, "Research on detection and evaluation technology of cybersecurity in intelligent and connected vehicle," in *Proc. Int. Conf. Artif. Intell. Adv. Manuf.*, 2019, pp. 413–416.

[30] C. Watney and C. Draffin, "Addressing new challenges in automotive cybersecurity," R Street Inst., Washington, DC, USA, R Street Policy Study no. 118, 2017.

[31] *Vehicle Electrical System Security Committee: SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems*, Society of Automotive Engineers, Warrendale, PA, USA, 2016. [Online]. Available: https://saemobilus.sae.org/content/j3061_201601

[32] *International Organization for Standardization: ISO 26262 Road Vehicles Functional Safety*, 2018. [Online]. Available: https://www.iso.org/standard/68383.html

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

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

[35] K. Chitnis *et al.*, "Enabling functional safety ASIL compliance for autonomous driving software systems," *Electron. Imag.*, vol. 2017, no. 19, pp. 35–40, 2017.

[36] D. Rao, P. Pathrose, F. Huening, and J. Sid, "An approach for validating safety of perception software in autonomous driving systems," in *Proc. Int. Symp. Model-Based Saf. Assessment*, 2019, pp. 303–316.

[37] C.-H. Cheng, C.-H. Huang, and G. Nührenberg, "nn-dependability-kit: Engineering neural networks for safety-critical autonomous driving systems," 2018, *arXiv:1811.06746*.

[38] J.-G. Lee, K. J. Kim, S. Lee, and D.-H. Shin, "Can autonomous vehicles be safe and trustworthy? Effects of appearance and autonomy of unmanned driving systems," *Int. J. Human-Comput. Interact.*, vol. 31, no. 10, pp. 682–691, 2015.

[39] G. BagschiNak, T. Stoltea, and M. Maurera, "Safety analysis based on systems theory applied to an unmanned protective vehicle," *Procedia Eng.*, vol. 179, pp. 61–71, 2017.

[40] A. Collin, A. Siddiqi, Y. Imanishi, E. Rebentisch, T. Tanimichi, and O. L. de Weck, "Autonomous driving systems hardware and software architecture exploration: Optimizing latency and cost under safety constraints," *Syst. Eng.*, vol. 23, no. 3, pp. 327–337, 2020.

[41] A. Weimerskirch and R. Gaynier, "An overview of automotive cybersecurity: Challenges and solution approaches," University of Michigan Transportation Research Institute, 2015. [Online]. Available: https://pdfs.semanticscholar.org/0dad/59a91ff57532011d188f3e53bd4387d7dbbf.pdf

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

[43] 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, 2016. [Online]. Available: https://www.gao.gov/assets/680/676064.pdf

[44] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017.

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

[46] X. Li, Z. Sun, D. Cao, Z. He, and Q. Zhu, "Real-time trajectory planning for autonomous urban driving: Framework, algorithms, and verifications," *IEEE/ASME Trans. Mechatronics*, vol. 21, no. 2, pp. 740–753, Apr. 2016.

[47] R. Rajamani, *Vehicle Dynamics and Control* New York, NY, USA: Springer, 2011.

[48] H. Chen, L. Guo, T. Qu, B. Gao, and F. Wang, "Optimal control methods in intelligent vehicles," *J. Control Decis.*, vol. 4, no. 1, pp. 32–56, 2017.

[49] J. Wu, S. Cheng, B. Liu, and C. Liu, "A human-machine-cooperative-driving controller based on AFS and DYC for vehicle dynamic stability," *Energies*, vol. 10, no. 11, 2017, Art. no. 1737.

[50] H. Pacejka, *Tire and Vehicle Dynamics*. New York, NY, USA: Elsevier, 2005.

[51] C. B. Butt, M. A. Hoque, and M. A. Rahman, "Simplified fuzzy-logic-based MTPA speed control of IPMSM drive," *IEEE Trans. Ind. Appl.*, vol. 40, no. 6, pp. 1529–1535, Nov./Dec. 2004.

[52] Y. A.-R. I. Mohamed and T. K. Lee, "Adaptive self-tuning MTPA vector controller for IPMSM drive system," *IEEE Trans. Energy Convers.*, vol. 21, no. 3, pp. 636–644, Sep. 2006.

[53] A. Dianov, Y.-K. Kim, S.-J. Lee, and S.-T. Lee, "Robust self-tuning MTPA algorithm for IPMSM drives," in *Proc. 34th Annu. Conf. IEEE Ind. Electron. Soc.*, 2008, pp. 1355–1360.

[54] G. Wang, Z. Li, G. Zhang, Y. Yu, and D. Xu, "Quadrature PLL-based high-order sliding-mode observer for IPMSM sensorless control with online MTPA control strategy," *IEEE Trans. Energy Convers.*, vol. 28, no. 1, pp. 214–224, Mar. 2013.

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

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

[57] 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 Trans. Ind. Electron.*, vol. 62, no. 3, pp. 1746–1759, Mar. 2015.

[58] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput.*, 2009, pp. 911–918.
[59] C. C. Macadam, "Understanding and modeling the human driver," *Veh. Syst. Dyn.*, vol. 40, nos. 1–3, pp. 101–134, 2003.
[60] B. Mashadi, M. Mahmoudi-Kaleybar, P. Ahmadizadeh, and A. Oveisi, "A path-following driver/vehicle model with optimized lateral dynamic controller," *Latin Amer. J. Solids Struct.*, vol. 11, no. 4, pp. 613–630, 2014.
[61] L. Saleh, P. Chevrel, F. Mars, J.-F. Lafay, and F. Claveau, "Human-like cybernetic driver model for lane keeping," *IFAC Proc. Vol.*, vol. 44, no. 1, pp. 4368–4373, 2011.
[62] J. Ye, K. Yang, H. Ye, and A. Emadi, "A fast electro-thermal model of traction inverters for electrified vehicles," *IEEE Trans. Power Electron.*, vol. 32, no. 5, pp. 3920–3934, May 2017.
[63] H. Ge, J. Jiang, J. Ye, and A. Emadi, "Behavior study of permanent magnet synchronous machines based on a new normalized model," *IEEE Trans. Ind. Electron.*, vol. 66, no. 10, pp. 7539–7550, Oct. 2019.
[64] 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.
[65] L. An and G. H. Yang, "Improved adaptive resilient control against sensor and actuator attacks," *Inf. Sci.*, vol. 423, pp. 145–156, 2018.

**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.

**Jin Ye** (Senior Member, IEEE) received the B.S. and M.S. degrees from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree from McMaster University, Hamilton, ON, Canada, in 2014, all in electrical engineering.

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