Fast Detection for Cyber Threats in Electric Vehicle Traction Motor Drives

Bowen Yang, *Graduate Student Member, IEEE*, Jin Ye, *Senior Member, IEEE*, and Lulu Guo, *Member, IEEE*

***Abstract*— While cyber-physical security of electric vehicles (EVs) is gaining increased concerns due to the fast development of vehicle onboard communication networks, the existing literature focuses on the vehicle level and it does not explicitly address cyber-threat detection for the EV powertrain traction motor drives. Therefore, in this article, we propose a fast, model-free approach to detect cyber threats in EV traction motor drives with only four easy-to-get, trustworthy sensor signals. First, the trustworthy motor current signals are selected to undermine the impacts of the vehicle's random driving cycles. Then, a set of innovative time-domain current features that are the most sensitive to a wide range of anomalies are selected to reduce the number of observations needed, thus vastly reducing the computational burden and the time-to-detect. Next, four binary classifiers are developed to detect cyber threats, while a majority vote mechanism is adopted to reduce the false alarm rate. Finally, the proposed method is validated by the real-time hardware-in-the-loop simulations. Validation results show that the proposed detection method achieves much faster detection compared with traditional current signature analysis (CSA). Furthermore, the proposed detection methods achieve an accuracy higher than 98% with the false alarm rate less than 0.01%.**

***Index Terms*— Pattern classification, road vehicle reliability, traction motor drives.**

I. Introduction

In RECENT years, researchers have witnessed the drastic development of electric vehicles (EVs). Meanwhile, due to the benefits of the modern electric platforms, the vehicle onboard communication networks and vehicle-to-X (V2X) techniques are also developed to adapt to the market requirement of advanced vehicle functionalities and performances. Therefore, large amounts of electronic units are deployed to the vehicle networks to realize modern vehicle technologies, such as online powertrain optimizations and advanced driver assistance systems (ADASs). According to [1], even for a premium-class automobile in 2009, the vehicle contains approximately 100 million lines of codes executed on 70–100 electronic control units (ECUs). While this progress has driven significant advancements in efficiency, functionality, and safety, it has also brought cyber threats, including electronic device failures and malicious cyberattacks. These threats could cause severe consequences to the drivers, passengers, and surrounding traffic systems. In 2010, Koscher *et al.* [2] experimentally evaluated the cyber-physical security issues on a modern automobile and demonstrated the fragility of the underlying system structure. They demonstrated that an attacker who can infiltrate virtually any ECUs could completely circumvent a broad array of safety-critical systems. Over a range of experiments, both in the lab and in the road test, they demonstrated the ability to control a wide range of automotive functions adversarially while ignoring the driver's requirements, for instance, disabling the brakes, power interruption, and other safety-critical functions. Recently, the IEEE Power Electronics Society (PELS) launched a cyber-physical-security initiative to address cyber networks' reliability and security issues in power electronics systems. Furthermore, according to Forbes, more than 150 cybersecurity incidents were reported in 2019 targeting the automotive industry. It states that the first vehicle-targeted hack happened in 2002, in which the hackers reprogram powertrain calibrations of Audi, Porsche, and Ford for more aggressive performance. Meanwhile, one of the most recent incidents happened in 2020. The hackers exposed security flaws of Ford and Volkswagen range from remotely exposing private customer information to disabling the traction control system [3].

Many communities have studied cyber-physical security issues in the past decades. For example, Han *et al.* [4] classified the intrusion detection techniques for the cyber-physical system from two different aspects based on the proposed four-layer structure of cyber-physical systems. Vuković and Dán [5] addressed the detection and localization of false data injection attacks against state estimation in distribution power systems (PSs) based on the evolution of the exchanged data and the convergence properties of the distributed algorithms. Meanwhile, Cui *et al.* [6] devoted their efforts to enriching the detection solutions from the following perspectives: 1) attacker versus defender dynamics and 2) distributed attack detection and state recovery. Kwon *et al.* [7] researched the intelligent cyberattacks that can avoid being detected by the current monitoring system, and Dan and Sandberg [8] studied the stealthy false-data attacks against state estimators in PSs. Besides the above work, other techniques and methodologies have

Manuscript received June 15, 2021; accepted July 22, 2021. Date of publication August 3, 2021; date of current version March 22, 2022. This work was supported by the U.S. National Science Foundation under Grant ECCS-1946057 and Grant ECCS-EPCN-2102032. *(Corresponding author: Jin Ye.)*

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

Lulu Guo is with the Department of Control Science and Engineering and Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai 201804, China (e-mail: guoll1510@163.com).

Digital Object Identifier 10.1109/TTE.2021.3102452

proven effective for attack detection, such as the onboard self-detection method in [9], the collaborative detection strategies in [10]–[13], and the remote offloaded detection techniques in [14].

In addition, there is related research in the aircraft community as well. Baskaya *et al.* [15] reviewed current fault detection and diagnosis methods using machine learning techniques. Chen *et al.* [16] proposed an improved version of fault diagnosis method via convolutional neural networks. Imai *et al.* [17] developed a self-healing avionics mechanism using a dynamic data-driven approach. Also, Wu *et al.* [18] analyzed the cascading failure based on operational process states.

Nevertheless, most studies from the above communities cannot be directly applied to the EV traction systems for the following reasons.

1) Considering the fact that vehicles are operating in relatively random scenarios while current research targets such as PSs and common process control systems (PCS) have relatively more stationary operation cycles, current approaches developed for PS and PCS may not be feasible. Loukas *et al.* [19] pointed out that most of existing techniques may not be feasible for modern vehicles due to the dynamic and unique operation characteristics.
2) Due to the limitations of vehicle onboard space and computational resources, a simple and fast detection method is required before triggering advanced root cause diagnosis based on resource-consuming diagnosis process, such as current signature analysis (CSA) [20]–[22] and redundant control [23].
3) As cyber threats include malicious cyberattacks from public networks, the trusted information is also limited. Most of the current detection methods use signals from networked ECUs, which could already be modified by those attacks. For example, in [23], they use the control sequence u_k to calculate the residual-based metrics, but actually, u_k itself is not trustworthy due to potential cyber threats. In this case, if the attacker sends a "healthy" u_k to the monitor but sends a modified $\hat{u}_k$ to the actuator, the attacks could bypass the existing monitoring systems. Therefore, a cyberattack detector using only trustworthy physical signals is preferred to avoid such issues.

Although the cyber-physical security of EVs has received increasing attention, most of the research still focuses on the vehicle level rather than traction motor drives. For example, in [24]–[26], the cyber-physical security of the energy management system and steering system for EVs is studied, in which the issues of cybersecurity and system stability are addressed. However, as the focus is on the vehicle system level, a linear vehicle model is used for the analysis. Thus, it does not work effectively for device-level analysis such as for powertrain traction motor drives, as these systems suffer from severe nonlinearity and uncertainty.

In this article, we propose a binary-classifier-based fast detection method for cyber-physical security of traction motor drives using four easy-to-get sensor signals. The general diagram of the proposed method is shown in Fig. 1.

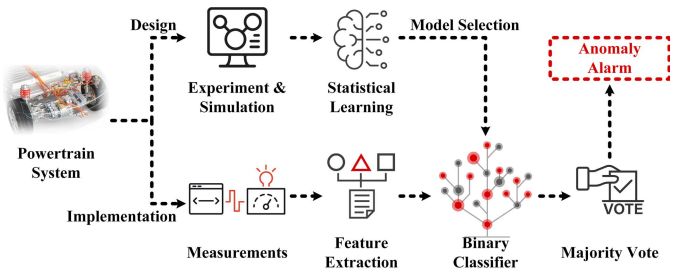


Fig. 1. General diagram for the proposed detection method.

The proposed method includes two stages: the design stage and the implementation stage. Training datasets are collected from the experiments and simulations in the design stage and then fed to a preselected statistical learning model to generate the binary-classifier-based detector. Then, in the implementation stage, the monitors acquire real-time measurements, calculate the instantaneous features, and feed the well-trained binary classifier. During the implementation stage, a majority vote mechanism is also included for better detection performance. The novelty and contributions for the proposed method are summarized as follows.

1) The proposed detection method selects motor current and position signals that are easier to obtain and secure compared with cyber signals, such as control signals, so these signals and proposed algorithms are considered trustworthy against cyberattacks.
2) The proposed detection method uses the motor current signals in the dq0 reference frame to undermine the impacts of the vehicle random driving cycles. The reason is that the operational patterns for motor currents are limited by the motor control algorithms regardless of the vehicle driving cycles. For example, if the traction drives are well controlled by maximum torque per ampere (MTPA) and proportional–integral (PI) controllers, the normal current features under the dq0 reference frame should be restricted to certain boundary established by the control algorithms. This will be further demonstrated in Section III and Figs. 8 and 9.
3) The proposed detection method achieves much faster detection compared to traditional CSA through selecting a set of innovative time-domain current features. These time-domain features are selected to be the most vulnerable to a wide range of anomalies, so a shorter time period of observations is needed, largely reducing the computational burden and the time-to-detect.
4) The proposed detection method does not rely on the physical model of motor drive systems compared to traditional residual-based methods that estimate or predict information from the linear model. Thus, strong nonlinearity and uncertainty of motor drive systems can be better addressed to improve detection accuracy and robustness.

The rest of the article is organized as follows. Section II clarifies the model assumptions and the trusted signals. Section III elaborates the details of the proposed approach. Section IV demonstrates the proposed method by real-time simulation results. Section V addresses the conclusions.

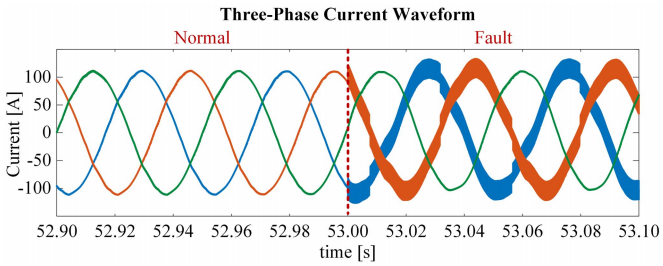


Fig. 2. Three-phase current waveform of IPM motor drive in a machine short-circuit fault case study.

II. Model Assumptions and Trusted Signals

The general idea of the proposed method is to establish a boundary between all the extracted physical features using binary classifiers, which could distinguish whether or not the system is operating under healthy conditions. In order to better illustrate the proposed approach and to maintain the focus of cyber threats, some assumptions are elaborated in this section. In addition, the trusted signals assumptions will also be elaborated in this section.

A. Physical Faults and Failures

Generally, the anomalies of a traction motor drive include both physical faults and cyber threats. However, in this article, we only focus on the cyber threats and assume that there are no physical faults or failures in the target systems. The reasons for this assumption could be explained as follows. First, the physical faults could be classified into two categories: one is short-term faults and the other one is long-term faults. The former ones have short transient periods between the fault occurrence and the system failure, such as power switch open-circuit faults and electric machine short-circuit faults. For such faults, the system operation point will suddenly deviate from the normal trajectory; and such faults could also be detected by the proposed method due to its similar characteristics on the proposed features. For example, Fig. 2 shows the three-phase current waveform of the interior permanent magnet (IPM) motor drive from a machine short-circuit fault case study. In this case, a dual-phase partially short-circuit fault is simulated after time 53 s. We then extract 50 samples of the fault current waveform and test them using our proposed method. The results show that all 50 samples are correctly detected. The other type of faults has a relatively longer transient period between the fault occurrence and the system failure, such as inter-turn short-circuit faults of electric machines. These kinds of faults tend to evolve slowly after their appearances and will only cause severe damages after a certain amount of time, so such faults actually provide much larger time windows for the fault detectors than other faults. In addition, it usually requires a long period of observations to extract the evolving trends of such faults, so these kinds of faults are not the main focus of the proposed fast detection method. Therefore, to maintain the focus of cyber threats, we will assume that there is no physical fault in the target systems in the rest of this article.

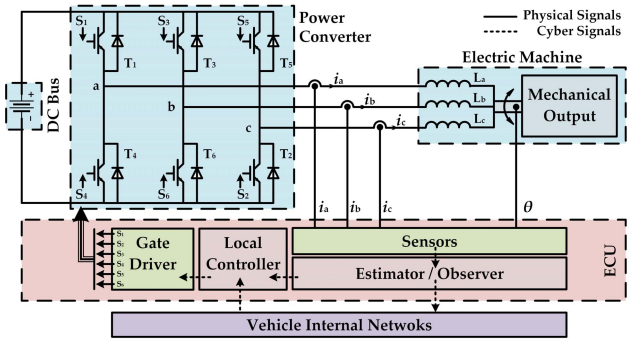


Fig. 3. General control framework of the traction motor drives.

B. General Control Framework of Traction Motor Drives

In this article, we assume that the traction motor drives have a general control framework shown in Fig. 3, which includes a networked motor controller (or ECU), traction inverter, electric machine, current sensors, and rotor position encoder. More specifically, we will use an IPM synchronous machine drive for demonstration, whose detailed control diagram is shown in Fig. 4. Meanwhile, we also assume that winding current can be directly or indirectly controlled.

C. System-Level Cyber Threats

As shown in Fig. 3, the motor controller also communicates with the vehicle onboard networks and exchanges information such as reference signals and system operation conditions. In this article, we define threats occurring on this communication channel as system-level cyber threats and define threats within the motor controller as device-level threats. Then, the proposed method only focuses on detecting device-level threats. The reason is that, first, as shown in Fig. 5 [26], [27], in order to detect the system-level threats, the detector will need information from other subsystems connected to the vehicle networks, and this target could be achieved by the system-level detector. Second, as long as the reference signals shown in Figs. 3 and 5 do not exceed the safety margins of the traction motor drives, such threats will not cause direct damages to the motor drive systems. Therefore, the proposed method will only focus on the device-level attacks, which could cause direct impacts on the motor drive systems.

D. Trusted Signals

Whenever dealing with the problems of cyberattacks, the assumption of trusted signals is always one of the most important questions. As shown in Figs. 3 and 5, the motor controller is directly connected to the vehicle onboard networks. This indicates that the motor controller is directly exposed to all the cyber threats in the networks. Therefore, all the information and signals in the motor controller are not trustworthy as any one of them may be modified. Fig. 6 shows three common cyberattacks targeting on motor drives, which are shown as follows.

1) Attacks on the feedback signals, where $y_k \neq \hat{y}_k$.
2) Attacks on the control sequences, where $u_k \neq \hat{u}_k$.
3) Attacks on the control parameters.

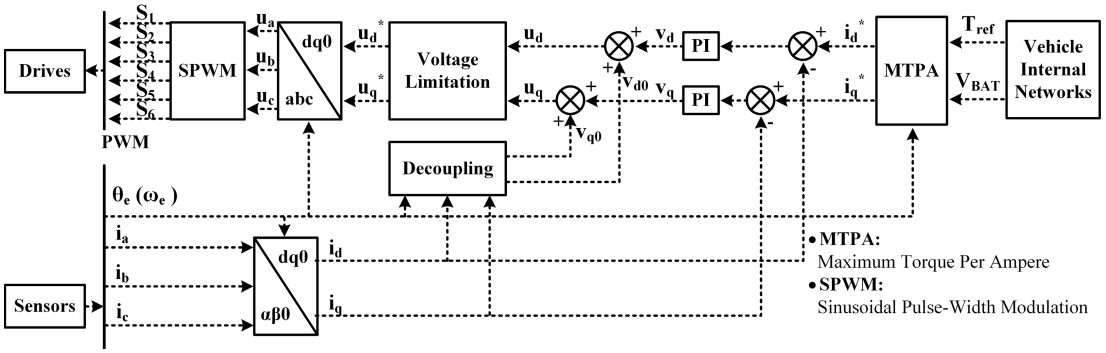


Fig. 4. Detail control diagram of IPM drive.

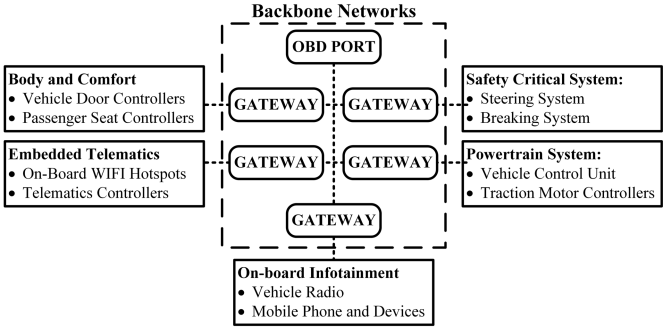


Fig. 5. General configuration of the EV onboard networks.

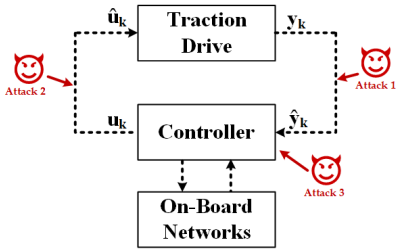


Fig. 6. Some common attacks targeting on the motor controllers.

In this article, we assume four sensor signals are trustworthy, which are three-phase current sensor signals i_a, i_b, and i_c and the rotor position encoder signal θ_r. The reasons could be summarized as follows.

1) Motor drive sensors are physical components, which are not connected to the vehicle networks.
2) Extra sensors from a third party, which are completely isolated, could also be easily installed to the system.

For the reasons above, the proposed approach will be based on these four trustworthy signals.

III. Cyber Attack Detection Method Using Binary Classifiers

As shown in Fig. 1, the proposed approach is to establish a boundary among all the target system physical features so that the anomalies of the traction motor drive could be detected within a very short time period. The proposed approach could be separated into two stages: the detector design stage and the detector implementation stage.

For the design stage, the general process is described by Algorithm 1, and the major target for this stage is to generate an optimal fast detector for the target system. Details of each step will be elaborated later in this section.

The second stage is the implementation of the optimal fast detector acquired in the first stage. Fig. 7 shows a general diagram of this stage. The general algorithm is shown in Algorithm 2 and each step will be discussed in detail in the following contents.

Algorithm 1 Design Algorithm for Model-Free Fast Detector Using Binary Classifiers

1: **Input**: Four sensor data (i_a, i_b, i_c, θ_r) and related condition label.
2: **Output**: Optimal binary classifier based fast detector model.
3: Input data re-sampling using sliding window with length of m and sampling time of t_s;
4: Time-domain feature extraction from the re-sampled observations;
5: Model fitting based on the extracted time-domain features with different binary classifiers;
6: Optimal Model selection by comparing the k-fold cross validation results of different fit models;

A. Time-Domain Feature Extraction

As shown in Algorithms 1 and 2, time-domain feature extraction plays an important role in both stages, as those features are used as predictors in the binary classifier models. The reason why choosing time-domain features is that compared with frequency- and time-frequency domain, time-domain features could reflect the system instant characteristics with much smaller window size as they do not need to consider the tradeoff between the frequency resolution and the window size. This point is crucial for the fast detector as large window size will consume a lot of online memory and computational resources. More specifically, the proposed method chooses 16 features from the two traction drives' current signals in the dq0 reference frame, i_d and i_q. Such signals are transferred from the original real measurements i_a, i_b, i_c, and θ_r using the

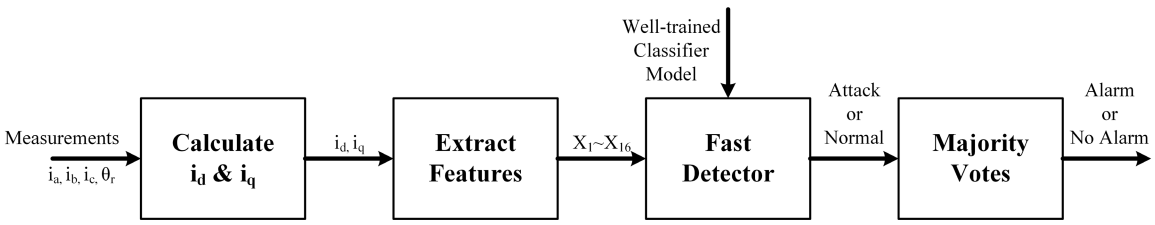


Fig. 7. General diagram of the implementation stage (Algorithm 2).

Algorithm 2 Implementation Algorithm for the Optimal Fast Detector Acquired in the First Stage

Input: Well trained fast detector model and real time measurements of i_a, i_b, i_c, θ_r.
Output: Abnormal detection results.
Generating a sliding window with the same length m and sampling time t_s as in stage 1;
for $k = 0$ **to** $m - 1$ **do**
  read and save i_a, i_b, i_c, θ_r at $t = k * t_s$ to form the initial monitoring window $\mathcal{W}_0$, $t = 0$ is the initial point;
end for
setting the number of voting decision $v = 0$ and total voting capacity as v_{max};
for $k = m, m+1, m+2, m+3, \ldots$ **do**
  time domain feature extraction from monitoring window $\mathcal{W}_{k-m}$;
  classifying the feature of $\mathcal{W}_{k-m}$ using the input binary classifier model and generate the decision D_{k-m};
  if $v \leq v_{max}$ **then**
    save the decision D_{k-m} as voting candidate V_{k-m};
    $v++$;
  else
    conducting a majority vote among the voting candidates $V_{k-m-v_{max}}$ to V_{k-m-1};
    if more votes for "threats" **then**
      output "cyber threat alert";
    else
      output "healthy condition";
    end if
    save the decision D_{k-m} as voting candidate V_{k-m};
    delete voting candidate $V_{k-m-v_{max}}$;
  end if
end for

Park transformation. The expression for the transformation is shown as follows:

$$\begin{bmatrix} i_d \\ i_q \end{bmatrix} = \frac{2}{3} \cdot \mathbf{P} \cdot \begin{bmatrix} i_a \\ i_b \\ i_c \end{bmatrix} \tag{1}$$

$$\mathbf{P} = \begin{bmatrix} \cos(\theta_e) & \cos\left(\theta_e - \frac{2\pi}{3}\right) & \cos\left(\theta_e + \frac{2\pi}{3}\right) \\ -\sin(\theta_e) & -\sin\left(\theta_e - \frac{2\pi}{3}\right) & -\sin\left(\theta_e + \frac{2\pi}{3}\right) \end{bmatrix} \tag{2}$$

where $\theta_e = \theta_r * \text{polepairs}$. In addition, the 16 features extracted from i_d and i_q are developed from the four sample moments (mean, variance, skewness, and kurtosis) of the data within the sliding window, which depict the data distribution characteristics. The detailed expression of the four sample moments is shown as follows:

$$\text{Mean} = \mu = \frac{1}{m}\sum_{i=1}^{m}(X_i) \tag{3}$$

$$\text{Variance} = \sigma^2 = \frac{1}{m}\sum_{i=1}^{m}(X_i - \mu)^2 \tag{4}$$

$$\text{Skewness} = \mu_3 = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{X_i - \mu}{\sigma}\right)^3 \tag{5}$$

$$\text{Kurtosis} = \mu_4 = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{X_i - \mu}{\sigma}\right)^4 \tag{6}$$

where X represents i_d and i_q.

Generally speaking, these 16 features describe the data distribution of the d- and q-axis currents. The reasons for choosing such features could be summarized by two aspects: simplicity and interpretability. First, as shown in (3)–(6), the four sample moments are extremely easy to calculate, especially for sliding window, as only two data points will be changed in single step, the first data points in the previous window and the new observation. This largely reduces the online computation requirement and is crucial for the fast detector as discussed in Section I. Meanwhile, these 16 features could accurately reflect the system operation characteristics from multiple angles. The mean value depicts the instant current level, which should alongside the trajectory of the optimized current reference if the system operates in a healthy condition, as the motor drive either directly or indirectly controls the winding currents. For example, in our demonstration, we use an IPM drive with MTPA optimization method; therefore, the mean values of d- and q-axis currents should be alongside the MTPA current profiles when the IPM drive is operating in a healthy condition. In addition, the variance could reveal the current ripple level, skewness could imply the asymmetry of the current profiles, and the kurtosis could examine the extreme values in the sliding window like sudden changes in the system. For example, Fig. 8 shows a sample of current mean-value features in the dq0 frame. It could be seen that each one of the features alone cannot fully distinguish the normal and abnormal conditions due to variation of feature sensitivity in different case scenarios. Therefore, the proposed approach needs to use all 16 features in the binary classifier models. Meanwhile, as discussed in Section II, the short-term physical faults will have similar characteristics, such as the mean value deviating from the optimized current trajectory, large current ripple reflected by the variance, and sudden

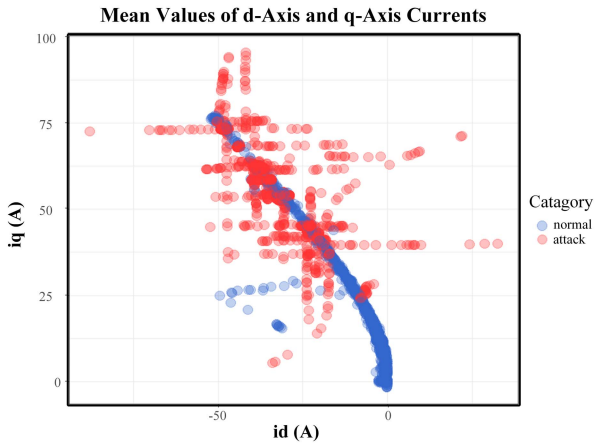


Fig. 8. Sample of time-domain features in the dq0 reference frame: mean values of d- and q-axis currents from the front wheel drive.

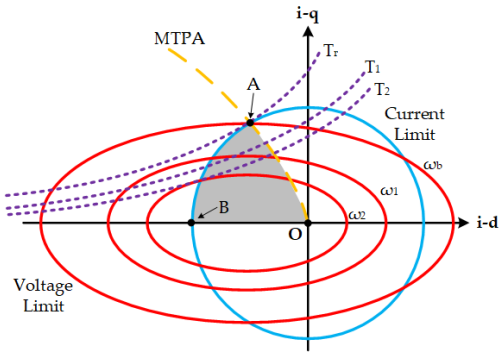


Fig. 9. Current profiles for IPM drive with MTPA (yellow line).

change of system states implied by skewness and kurtosis. These similarities imply that the proposed fast detector could also detect the short-term physical faults as stated in Section II.

B. Binary Classifier

In this article, we select four binary classifier candidates, which are the random forest (RF)-based classifier, the k-nearest-neighbor (KNN)-based classifier, the support vector machine (SVM)-based classifier, and the adaptive boosting (AdaBoost) classification tree-based classifier. The reason for adopting binary classifier-based detector is their simplicity and interpretability, which are both important in the context of cyber-threats detection. Among these four classifier candidates, each of them has its own characteristics and has different levels of sensitivity to different cyber threats and different systems.

1) Random Forest Classifier: RF classifier is a modified decision tree-based classifier, which operates by constructing a multitude of decision trees at training and outputting the dominant class among all the classes generated from each individual decision tree. RF output model contains the node information and its splitting criteria of all the decision trees in the forest; thus, the model computational size depends on the number of nodes and trees in the forest. Therefore, in order to further reduce the consumption of computational resources, it is necessary to simplify the final model by adjusting the predictors with respect to the mean decrease Gini index of each predictor.

2) K-Nearest-Neighbor Classifier: KNN classifier is a nonparametric method, which classifies the new observation by a plurality vote of its neighbors in the feature space and assigns the new observation to the most common class among its KNNs. KNN is a common classifier with good prediction accuracy; however, due to its nonparametric nature, the KNN classifier tends to occupy a lot more online computational resources, especially when the training data size is large. The reason why KNN classifier is still chosen as the candidate classifier is that for some contexts when the boundary for healthy operation conditions is clear, such as drives with limited operation trajectories, adopting KNN could largely reduce the simulation and experiment cases.

3) Support Vector Machine Classifier: SVM model is a representation of the training dataset as support vectors (or points) in the feature space, which maps the training dataset to the separate classes dividing by a clear gap, and new observations are then mapped into the same space and predicted to belong to the class based on the side of the gap on which they fall. SVM is a robust classifier with benefits of low consumption of online computational resources as it only needs to store the support vectors that map the gap between the two classes.

4) AdaBoost Classification Trees: AdaBoost is a boosting algorithm in machine learning. Improving week learners and creating an aggregated model to improve model accuracy is a key concept of boosting algorithms. A weak learner is defined as the one with poor performance or slightly better than a random guess classifier. AdaBoost classification trees improve those classifiers by increasing their weights and get their votes to create the final combined model.

Generally speaking, these four classifier candidates represent the typical characteristic of the commonly used binary classifiers: RF and AdaBoost methods represent the rule-based classification tree algorithms, KNN represents the nonparametric classifier, and SVM represents the support vector-based classifier. The reason for choosing multiple classifier candidates is that the detection results depend on the time-domain feature characteristics, such as the optimized current trajectory. Therefore, in order to overcome such variations among different traction drive systems, it is necessary to choose multiple classifier candidates and select the model with optimal performance for stage 2 implementation. For the proposed approach, we adopt k-fold cross validation to estimate the detector performance.

C. Majority Vote Mechanism

As shown in Algorithm 2, a majority vote mechanism is adopted before the final decision. This is because there are many uncertainties in real-world traction motor drives, such as road conditions and temperature variations. Such external uncertain factors may cause a lot of false alerts, and therefore, the majority vote mechanism could effectively reduce the number of false alerts. In addition, the number of voters $\upsilon_{\max}$ is chosen with respect to the tradeoff between the time to detect

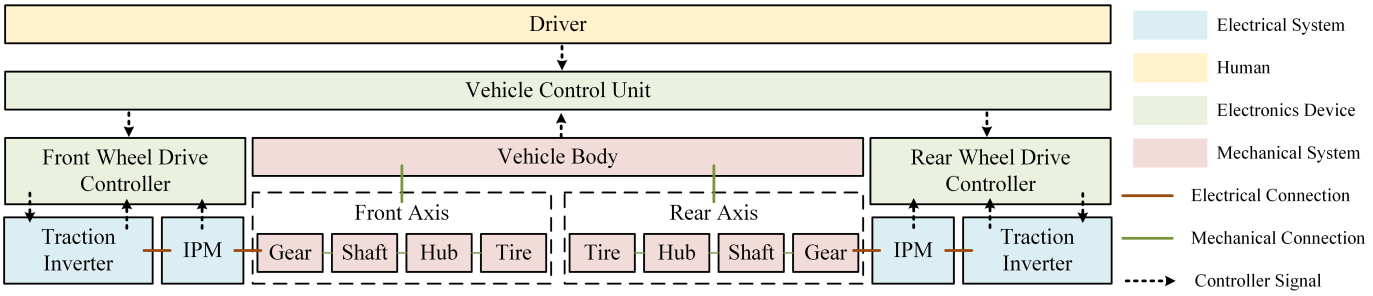


Fig. 10. General diagram of the powertrain model used in the HIL real-time simulation.

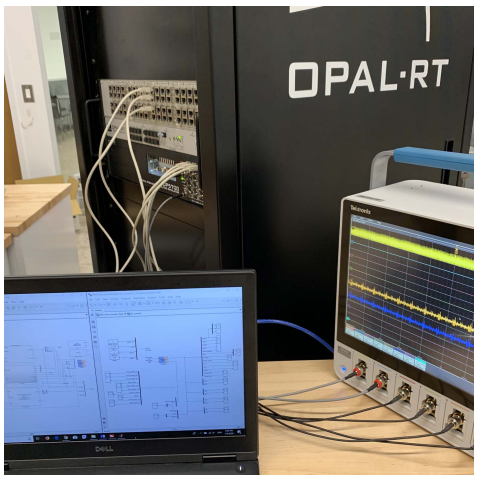


Fig. 11. Hardware-in-the-loop real-time simulation platform.

and the number of false alarms. When $v_{\max}$ is large, the time for detection will increase as it requires a certain amount of votes to determine the system has cyber threats, but there will be more redundancy for the external uncertain factors. In this article, $v_{\max}$ is set to six.

IV. Method Demonstration With Real-Time Simulation

Considering the potential risk of conducting cyber-threat experiments on real-world EV powertrain testbed, we use the OPAL-RT real-time simulation instead to demonstrate and validate the proposed detection method. Fig. 11 shows a picture of the simulator platform and Fig. 12 shows four samples of the motor three-phase current waveform during the attacks in our case studies. In order to fully emulate the real-world EV powertrain operation conditions, a detailed real-time EV powertrain model is adopted. Fig. 10 shows the powertrain structure used in the hardware-in-the-loop (HIL) real-time simulation. The model includes two IPM traction motor drives at the front axis and the rear axis, respectively. In addition, vehicle mechanical systems, including reduction gear box, shaft stiffness, and tire-road interactions, and vehicle dynamics, including road conditions and aerodynamics, are also considered in the real-time simulation models. The detail descriptions of this testbed are elaborated in [28]. Meanwhile, the vehicle model is tested in the New European Driving Cycle (NEDC) driving cycles shown in Fig. 13 and 40 cyber-threat cases described in Table I. The case studies focus on the d- and q-axis current references of the two traction motors (totally four target signals). In order to emulate the behavior of a typical false data injection attack, we adopt a random walk time series model, which is shown in (7), where the true data and false data are denoted as y and $\hat{y}$, respectively, and the attack period is $\mathbf{T_{ATK}} = [t_0, t_0 + T_a]$. R is a normal distribution random variable with zero mean and 0.5 variance. $[R \sim \mathcal{N}(0, 0.5)]$

$$\hat{y_k} = \begin{cases} y_k, & (t \notin \mathbf{T_{ATK}}) \\ y_{k-1} + R, & (t \in \mathbf{T_{ATK}}). \end{cases} \tag{7}$$

From the real-time simulation of the 82 case studies among three standard vehicle testing driving cycles, NEDC, urban dynamometer driving schedule (UDDS), and Highway Fuel Economy Test Cycle (HWFET). We then generate 200 windows of abnormal observations from each case, thus totally 16 400 observations, labeled as "attack." Among the 16 400 abnormal observations, we randomly choose 13 120 (80%) of them to participate in the training process so that, during the testing, there will be 3280 new observations, which does not participate in the training. Then, we also randomly select 13 120 observations from the normal conditions to participate in the training process. In order to demonstrate the performance of the classifier candidates, we conduct extra testing with all the 82 attack cases to calculate their corresponding time to detect. In addition, we also use the 3208 normal observations from the testing datasets to test the model false alarm rates.

In the following sections, the proposed method is demonstrated and validated from three aspects: performance of the proposed method in vehicle driving cycles, evaluation of online memory savings with window size comparison, and time-to-detect of different binary classifiers.

A. Performance of the Proposed Method Based on Testing Datasets

For demonstration purpose, we choose four binary classifiers, as described in Section III. In Table II, the accuracy, the κ statistics, and the 95% confident interval of four binary classifier candidates based on the testing data are listed, the confusion matrices are shown in Fig. 14, and the histogram of these results is shown in Fig. 15 for a clear comparison. According to these results, the classification accuracy of all four classifiers is above 95%, which suggests that

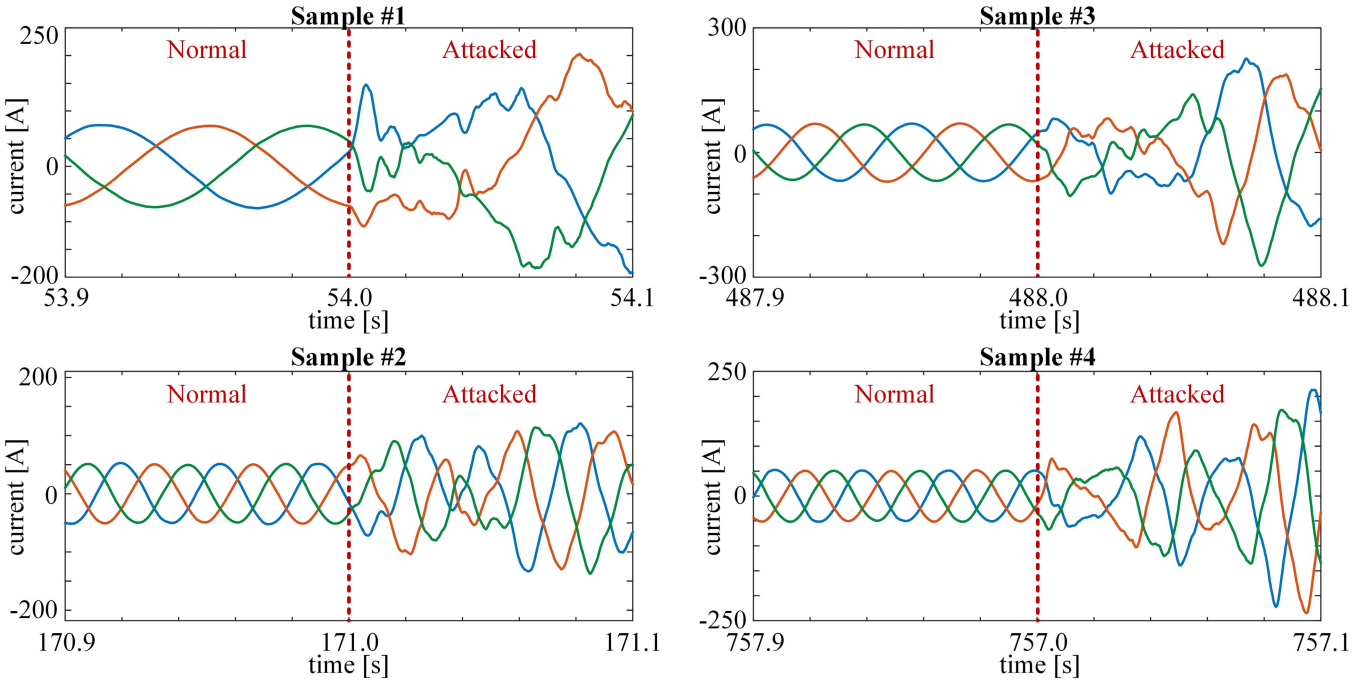


Fig. 12. Samples of the motor three-phase current waveform from the case studies.

the time-domain features extracted from the d- and q-axis currents are able to distinguish most of the attack conditions from the normal conditions. Furthermore, RFs and AdaBoost classification tree classifiers achieve an accuracy above 99%, which suggests that these two classifiers are highly sensitive to the anomalies reflected by the extracted features and could detect almost all the abnormal observations.

Meanwhile, Table III shows the results of the false alarm rates among the 3280 normal observations that do not participate in the training process. From Table III, the RF classifier and the AdaBoost classifier could achieve a false alarm rate less than 0.5%, while the other two can achieve a false alarm rate less than 4%. However, these results only show the performance of the classifiers, if including the assistance of the majority vote mechanism, the false alarm of all four binary classifiers will be completely eliminated. However, the majority vote mechanism will increase the time to detect the anomalies and the computational resources as well. In our simulations, we adopt a voting mechanism with vote capacity of six.

In addition, impacts of the distorted position signals are discussed as follows. First of all, as discussed in Section II, the reason we assume that d- and q-axis current signals are secure is that these two signals could be calculated from the three-phase measurements and the rotor position directly. More specifically, the three-phase measurements could be acquired from the original sensors or extra third-party sensors. Both ways could easily guarantee the security of the current signals. On the other hand, the rotor position could be acquired from the original rotor encoders or estimated from the three-phase currents. Therefore, if we could guarantee the security of three-phase current signals, we could assume that the position is secure.

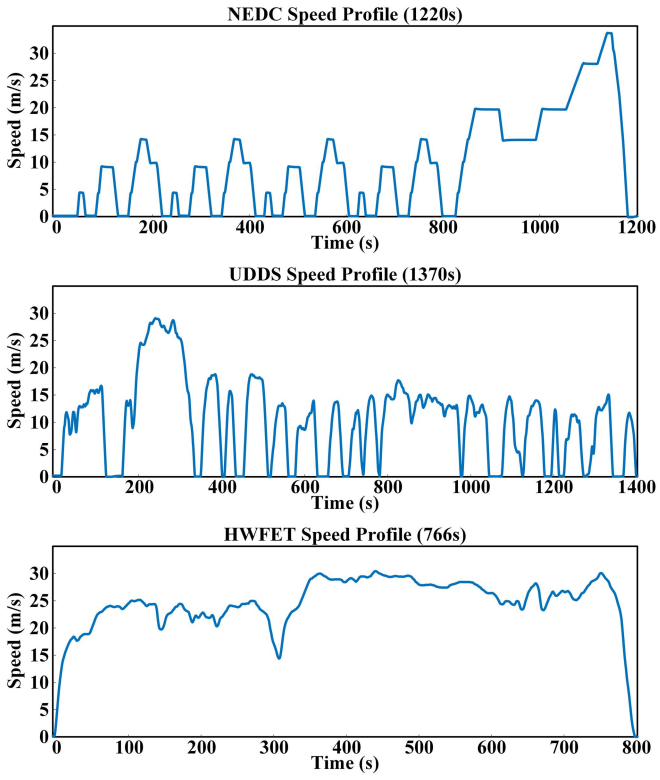


Fig. 13. Plots of the driving cycles.

Second, if the position signal gets distorted, the motor drive controller will receive incorrect d- and q-axis current feedback. Then, the actual currents fed to the detector will be deviated from the normal region and the proposed detector will be able to detect these kinds of anomalies.

TABLE I
LISTS OF CASE STUDIES

Case No.	Driving Cycle	Attack Time (s) (attacks last 0.5 seconds)
1-40	NEDC	[54 98 171 250 289 366 488 573 758 873]
41-80	UDDS	[23 168 357 458 523 572 647 777 1058 1169]
81-82	HWFET	[320]

TABLE II
PERFORMANCE STATISTICS OF THE BINARY CLASSIFIER

	RF	SVM	KNN	AdaBoost
Accuracy	0.9979	0.9809	0.9562	0.9994
κ	0.9957	0.9619	0.9125	0.9988
95% Confident Interval (lower)	0.9964	0.9773	0.9510	0.9984
95% Confident Interval (upper)	0.9988	0.9841	0.9611	0.9998

TABLE III
FALSE ALARM TEST RESULTS AMONG 3280 NORMAL OBSERVATIONS

Detect Results	RF	SVM	KNN	AdaBoost
Normal	3266	3163	3163	3278
Attack	14	117	117	2
False Alarm Rate (%)	0.43	3.57	3.57	0.06
Normal (with Majority Votes)	3280	3280	3280	3280
Attack (with Majority Votes)	0	0	0	0

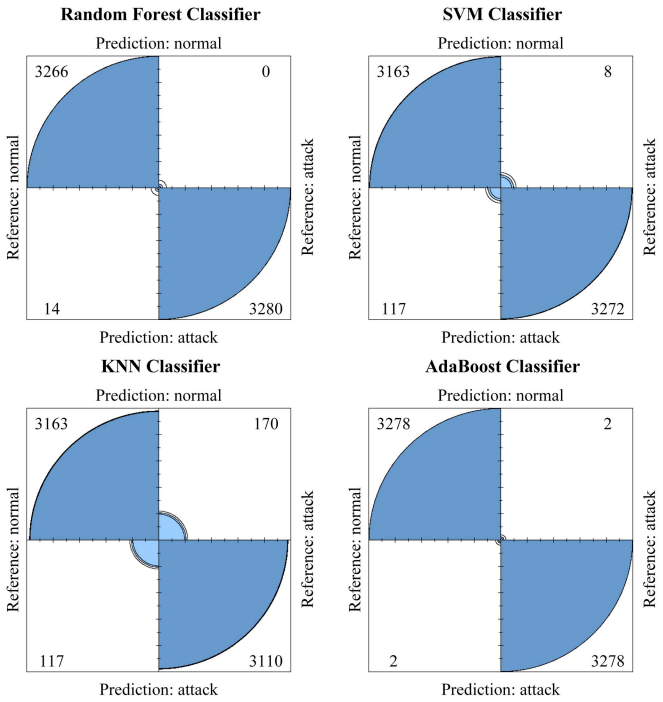


Fig. 14. Confusion matrix of testing results of the four binary classifiers.

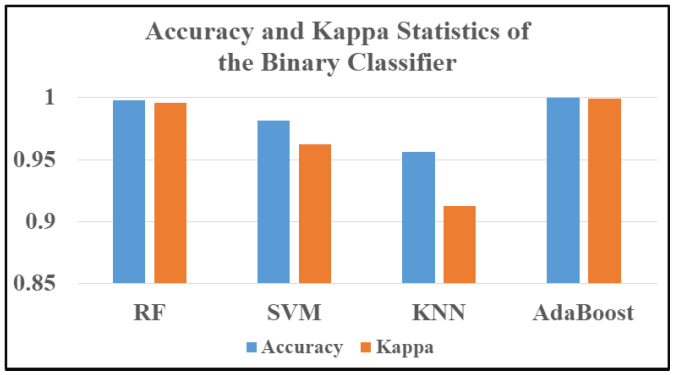


Fig. 15. Accuracy and κ statistics of the binary classifiers.

Therefore, the proposed detection method will still work even if the position signal gets distorted.

B. Evaluation of Computational Resource Savings With Window Size Comparison

In order to evaluate the computational resource savings, we compare the proposed methods with traditional spectrum-based methods from two aspects: online memory savings and computational complexity. First, to compare the online memory savings, we use the monitoring window size as the evaluation criteria, because saving observations occupies most of the online memory and the larger window size required by the algorithms, the more online memory is required. As stated in [21], using CSA requires a high-resolution frequency spectrum. Commonly, the frequency resolution for CSA is less than 10 Hz, and therefore, Table IV lists the window size requirement for the proposed method and the CSA with different frequency resolutions. The results are based on a sampling time of 0.2 ms (5-kHz sampling frequency). As the results suggest, even the frequency resolution is 10 Hz, and the window size requirement is still twice the one for the proposed method. Therefore, the proposed method will save huge amount of online memory. In addition, from the aspect of computational complexity, the proposed method

TABLE IV
WINDOW SIZE REQUIREMENT FOR THE PROPOSED ALGORITHM AND THE CSA WITH DIFFERENT FREQUENCY RESOLUTIONS

	Proposed Method	Traditional CSA		
Resolution	NA	2Hz	5Hz	10Hz
Size (points)	500	5000	2000	1000
Size (s)	0.1	1.00	0.40	0.20

requires linear computational time, $O(n)$, because it is based on the calculation of mean, variance, skewness, and kurtosis. Meanwhile, the spectrum-based method requires quadratic computational time, $O(n^2)$. Apparently, the proposed method requires less online computational resources than the traditional spectrum-based methods.

C. Time-to-Detect of Different Binary Classifiers

As the time-to-detect of anomalies depends on many external factors, such as hardware computational performance and sensor sampling frequency, we compare the time-to-detect of the proposed method with traditional spectrum-based methods by comparing the number of sliding windows required to generate an anomaly alarm. For the proposed methods, the detection accuracy of RF classifiers and AdaBoost classifier could achieve as high as 99.9%. This means that a detector based on these two classifiers could immediately generate an anomaly alarm, even without majority vote mechanisms. Therefore, for these detectors, the number of sliding windows required is 1. The other candidate binary classifiers have lower accuracy; therefore, they need the assists of majority vote mechanisms. Among them, the KNN-classifier-based detector has the worst performance, and it requires a vote capacity of six to achieve 100% accuracy. This means that the proposed method at most requires six sliding windows to generate an accurate anomaly alarm. On the other hand, considering the high sampling rates of the traditional spectrum-based methods, they require much longer observations to reflect the attack impact on the spectrum. Therefore, in our case studies, the spectrum-based methods require at least 20 sliding windows to generate an accurate anomaly alarm. These results support that the proposed method could detect those anomalies in a lot shorter time.

V. CONCLUSION

In this article, we proposed fast anomaly detection approaches for the EV traction motor drives due to cyber threats. The proposed approach uses only four easy-to-get sensor signals and highly compact binary classifier models so that the proposed detector could detect the cyber threats at the early stage and does not require many online computational resources. With the validations conducted by real-time simulation, the proposed method has been proven to be effective and efficient on detecting different cyber threats in a very short time period.

REFERENCES

[1] R. Charette, "This car runs on code," *IEEE Spectr.*, vol. 46, no. 3, p. 3, Feb. 2009.

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

[3] S. Tengler, "Top 25 auto cybersecurity hacks: Too many glass houses to be throwing stones," Forbes Bus., Tech. Rep., 2020. [Online]. Available: https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=349969b67f65

[4] S. Han, M. Xie, H. H. Chen, and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Syst. J.*, vol. 8, no. 4, pp. 1052–1062, Dec. 2014.

[5] O. Vuković and G. Dán, "Detection and localization of targeted attacks on fully distributed power system state estimation," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2013, pp. 390–395.

[6] S. Cui, Z. Han, S. Kar, T. T. Kim, H. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[7] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. Amer. Control Conf.*, Jun. 2013, pp. 3344–3349.

[8] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 214–219.

[9] A. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, "Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian networks," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jun. 2017, pp. 98–103.

[10] A. Broggi, P. Cerri, M. Felisa, M. C. Laghi, L. Mazzei, and P. P. Porta, "The VisLab intercontinental autonomous challenge: An extensive test for a platoon of intelligent vehicles," *Int. J. Vehicle Auton. Syst.*, vol. 10, no. 3, pp. 147–164, 2012.

[11] D. Wu *et al.*, "ADDSEN: Adaptive data processing and dissemination for drone swarms in urban sensing," *IEEE Trans. Comput.*, vol. 66, no. 2, pp. 183–198, Feb. 2017.

[12] S. Martini *et al.*, "Distributed motion misbehavior detection in teams of heterogeneous aerial robots," *Robot. Auton. Syst.*, vol. 74, pp. 30–39, Dec. 2015.

[13] R. Mitchell and I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 5, pp. 593–604, May 2014.

[14] G. Loukas, Y. Yoon, G. Sakellari, T. Vuong, and R. Heartfield, "Computation offloading of a vehicle's continuous intrusion detection workload for energy efficiency and performance," *Simul. Model. Pract. Theory*, vol. 73, pp. 83–94, Apr. 2017.

[15] E. Baskaya, M. Bronz, and D. Delahaye, "Fault detection & diagnosis for small UAVs via machine learning," in *Proc. IEEE/AIAA 36th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2017, pp. 1–6.

[16] S. Chen, H. Ge, J. Li, and M. Pecht, "Progressive improved convolutional neural network for avionics fault diagnosis," *IEEE Access*, vol. 7, pp. 177362–177375, 2019.

[17] S. Imai, S. Chen, W. Zhu, and C. A. Varela, "Dynamic data-driven learning for self-healing avionics," *Cluster Comput.*, vol. 22, no. S1, pp. 2187–2210, Jan. 2019.

[18] Y. Wu, G. Xiao, and M. Wang, "Cascading failure analysis method of avionics based on operational process state," *IEEE Access*, vol. 8, pp. 148425–148444, 2020.

[19] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, Mar. 2019.

[20] S. Choi, M. S. Haque, A. Arafat, and H. A. Toliyat, "Detection and estimation of extremely small fault signature by utilizing multiple current sensor signals in electric machines," *IEEE Trans. Ind. Appl.*, vol. 53, no. 3, pp. 2805–2816, May/Jun. 2017.

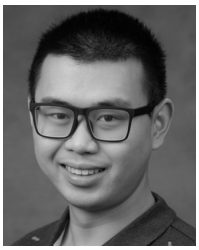
[21] W. T. Thomson and M. Fenger, "Current signature analysis to detect induction motor faults," *IEEE Ind. Appl. Mag.*, vol. 7, no. 4, pp. 26–34, Jul. 2001.

[22] I. Culbert and W. Rhodes, "Using current signature analysis technology to reliably detect cage winding defects in squirrel cage induction motors," in *Proc. Rec. Ind. Appl. Soc. 52nd Annu. Petroleum Chem. Ind. Conf.*, 2005, pp. 95–101.

[23] J. Giraldo *et al.*, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, 2018.

[24] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives," *IEEE Trans. Power Electron.*, vol. 36, no. 4, pp. 4463–4477, Apr. 2021.

[25] L. Guo, B. Yang, and J. Ye, "Enhanced cyber-physical security of steering stability control system for four-wheel independent drive electric vehicles," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2020, pp. 1240–1245.
[26] L. Guo *et al.*, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3335–3347, May 2021.
[27] 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.
[28] 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 (ITEC)*, Jun. 2020, pp. 63–68.



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

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

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

Lulu Guo (Member, IEEE) 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 was a Post-Doctoral Research Associate with the University of Georgia, Athens, GA, USA. He is currently a Research Professor with the Department of Control Science and Engineering and Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai, China. His current research interests include advanced vehicle control, energy management, and vehicle cybersecurity.