2022 IEEE/AIAA Transportation Electrification Conference and Electric Aircraft Technologies Symposium (ITEC+EATS) | 978-1-6654-0560-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITEC53557.2022.9814017

Data-Driven Detection of Physical Faults and Cyber Attacks in Dual-Motor EV Powertrains

Bowen Yang
School of Electrical and Computer Engineering
University of Georgia
Athens, Georgia 30602
Email: bowen.yang@uga.edu

Jin Ye
School of Electrical and Computer Engineering
University of Georgia
Athens, Georgia 30602
Email: jin.ye@uga.edu

Abstract—In the last decades, with the pervasive utilization of digital control units and communication networks in modern electric vehicle powertrains, such safety-critical systems have become highly vulnerable to potential cyber threats. Current research primarily focuses on aggressive attacks, which usually cause drastic changes and disturbances to the systems. However, little research has addressed how to detect more stealthy attacks targeting electric vehicle powertrains and distinguish between such attacks and common physical faults. This paper bridges this gap by proposing a data-driven approach to detecting and diagnosing hidden attacks and common physical faults in the dual-motor electric vehicle powertrain. The proposed method achieves promising performance in detecting and diagnosing cyber-attacks and physical faults. It reaches an accuracy of nearly 100% on detecting anomalies and above 90% on distinguishing stealthy attacks from common physical faults.

I. Introduction

With the pervasive utilization of digital control units and communication networks in the modern electric vehicle powertrains, such safety-critical systems become highly vulnerable to potential cyber threats. In 2010, Koscher et al. experimentally evaluated the cyber-physical security issues on a modern automobile and demonstrated the fragility of the underlying system structure [1].

As the traction motor drive is one of the most critical components in an EV powertrain, its safety and reliability are always priorities during design, implementation, and maintenance. So far, there has been much literature on the safety and security of motor drive systems. Among this literature, the proposed anomaly detection and root-cause diagnostic methods lie in model-based and data-driven methods. Most model-based methods use time-domain or frequency-domain signals. For example, fast Fourier Transform (FFT) is used in monitoring steady-state conditions in the frequency domain, while short-time Fourier Transform (STFT) is used in fluctuating load and speed conditions. Other examples are spectrograms and time-frequency analysis using wavelets and Wigner-Ville transforms. Usually, the system current, flux, mechanical vibration, torque, and speed signals are analyzed. One of the most widely used frequency-domain methods is motor current signature analysis (MCSA), based on the FFT of system line currents. Such methods usually pre-locate characteristic frequencies for specific fault scenarios and then use these frequency components' magnitudes and phase angles for detection and diagnosis. [2]–[4] Meanwhile, time-domain methods usually rely on pre-defined residuals. These methods compare the system outputs and the sets of reference values. The reference values could be acquired from two primary approaches. One comes from the signal itself, such as the average or limit values. The other one often relies on pre-defined system models from prior system knowledge. These models calculate the reference values by predicting the system outputs based on the given inputs at each instant. Then, the differences between actual outputs and reference values are defined as residuals. Alarms will be generated when such residuals exceed some pre-defined thresholds. [5]–[7] On the other hand, most data-driven approaches follow a similar framework, which includes three primary tasks: (1) a preprocessing task where input data from sensors and logs is normalized and organized for further analysis, (2) a pre-defined anomaly detector that analyzes the system status, (3) a pre-trained classifier that, based on the current system status and monitoring signals, provides a diagnosis for the system. [8] By following this framework, [9] utilized a statistical learning approach to differentiate the physical faults from cyber-attacks based on data generated by the IEEE 30 bus benchmark test system; Furthermore, [10] proposed an intelligent anomaly identification (IAI) technique for inverter-based systems by utilizing data-driven artificial intelligence tools that employ multi-class support vector machines (MSVM) for anomaly classification and localization. Meanwhile, Ye et al. researched the threat detection and attack resilient control from both global vehicle control level and local motor drive control level in [11]–[18].

Nevertheless, most current literature only addresses cyber-security or physical safety individually instead of simultaneously. [19] In addition, most studies have focused on really aggressive attacks. Such attacks usually will cause drastic changes and disturbances to the systems, which makes these attacks easier to detect. Meanwhile, little of the current research has addressed the importance of distinguishing between

This research was partially supported by U. S. National Science Foundation NSF-ECCS-1946057 and ECCS-EPCN #2102032.

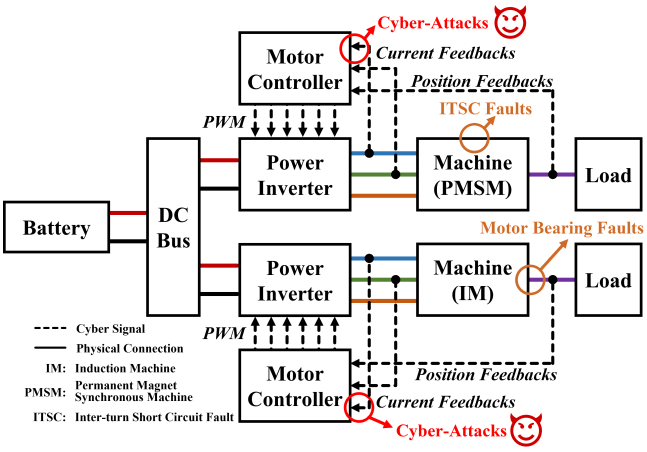

Fig. 1. Diagram of the dual-motor electric vehicle powertrain.

cyberattacks and physical faults.

This paper proposed a data-driven approach to detect and diagnose cyberattacks and physical faults in the dual-motor electric vehicle powertrain. The proposed method uses the motor line current spectra and four widely used data-driven classification methods to detect anomalies and distinguish the stealthy cyber-attacks from common physical faults. In addition, we used motor-bearing faults, inter-turn short circuit faults, and false data injection attacks as case studies to verify the performance of the proposed method.

The rest of the paper first describes the bearing fault and false data injection attack models in section II. Then, it will discuss the proposed method and the validation results in section III and section IV, respectively. Finally, section V addresses the conclusions.

II. Models for Physical Faults and Cyberattacks

To validate the proposed approach, we first formed a comprehensive case study in a dual-motor powertrain system including one permanent magnet synchronous machine (PMSM) and one induction machine (IM). Fig. 1 shows a general diagram of the system. The case study includes motor-bearing faults in IM, inter-turn shorts faults in PMSM, and false data injection attacks on controllers of both machine drives. In this section, the dynamic models of these faults and attacks are discussed in detail.

A. Physical Faults: Bearing Faults in IM

Bearing faults are one of the most common physical failures in electric machines. According to [20], bearing faults account for more than 40% of all the electric motor failures. Therefore, it is one of the best candidates to study the differences between physical faults and cyberattacks. When a bearing fault appears in the machine, some periodic vibration pulses will be generated due to the impact among the rolling elements, the bearing raceways, and the cage. The periodic pulses have different characteristic frequencies depending on the fault types. As demonstrated in [21], there are primarily five types of common bearing faults, and these different bearing faults will generate some periodic vibration pulses due to the impact among the rolling elements. The types and characteristic frequencies of these bearing faults are shown below, where the number of balls is denoted as N_b, the ball diameter is d, and the pitch or cage diameter is D. The point of contact between the ball and the raceway is characterized by the contact angle θ, and f_r is the mechanical frequency of the rotor. The geometry parameters of the bearing are shown in Fig. 2.

1) Cage defect hits the outer raceway:
$f_{co} = \frac{f_r}{2}(1 - \frac{d}{D}\cos\theta)$;
2) Cage defect hits the inner raceway:
$f_{ci} = \frac{f_r}{2}(1 + \frac{d}{D}\cos\theta)$;
3) Outer raceway defect hits balls:
$f_o = N_b\frac{f_r}{2}(1 - \frac{d}{D}\cos\theta)$;
4) Inner raceway defect hits balls:
$f_i = N_b\frac{f_r}{2}(1 + \frac{d}{D}\cos\theta)$;
5) Ball defect hits both raceways:
$f_b = \frac{D}{d}f_r(1 - \frac{d^2}{D^2}\cos^2\theta)$.

The periodic pulses caused by vibration will then introduce geometry asymmetry to the machine. Such asymmetry will then change the inductance of the machine. Ideally, the inductance variation should be composed of an infinite number of characteristic frequency harmonics. To simplify the model, we only choose the fundamental frequency component to represent the inductance variation. Then, we introduce a fault inductance to the induction machine state-space model in Eq. (1) and Eq. (2), where u is the stator input voltage, R and L are the motor resistance and inductance, ω_r is the electrical rotor speed, λ is the flux linkage, subscripts s, r, and m denote the stator, rotor, and their mutual electromagnetic parameters. Eq. (3) shows the new inductance after the bearing fault appears, where L_m^{fault} denotes the fault inductance, ω_c is

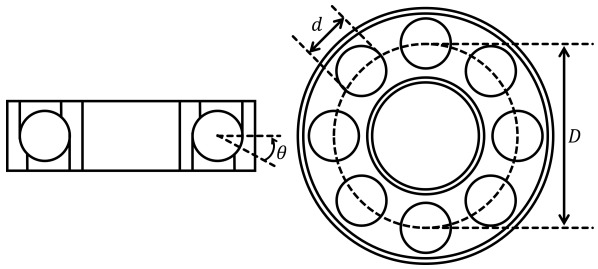

Fig. 2. Geometry parameters of the bearing.

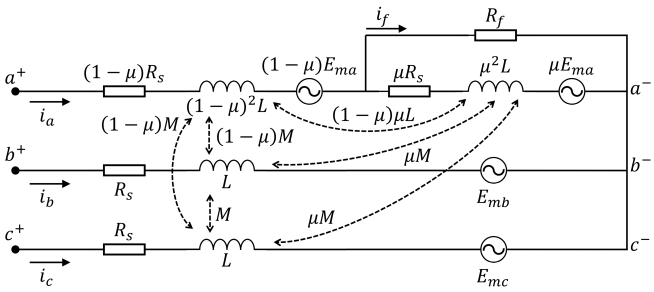

Fig. 3. The equivalent circuit of the ITSC fault.

the characteristic frequency described above, and ΔL_m is the inductance variation magnitude describing the fault severity.

$$\begin{cases} u_{ds} = R_s i_{ds} + \frac{d}{dt}\lambda_{ds} - \omega_s \lambda_{qr} \\ u_{qs} = R_s i_{qs} + \frac{d}{dt}\lambda_{qs} + \omega_s \lambda_{dr} \\ 0 = R_r i_{dr} + \frac{d}{dt}\lambda_{dr} - (\omega_s - \omega_r)\lambda_{qr} \\ 0 = R_r i_{qr} + \frac{d}{dt}\lambda_{qr} + (\omega_s - \omega_r)\lambda_{dr} \end{cases} \quad (1)$$

$$\begin{cases} \lambda_{ds} = L_s i_{ds} + L_m i_{dr} \\ \lambda_{qs} = L_s i_{qs} + L_m i_{qr} \\ \lambda_{dr} = L_m i_{ds} + L_r i_{dr} \\ \lambda_{qr} = L_m i_{qs} + L_r i_{qr} \end{cases} \quad (2)$$

$$L_m^{fault} = L_m + \Delta L_m \cos\omega_c t \quad (3)$$

B. Physical Faults: Inter-Turn Short Circuit Faults in PMSM

The inter-turn short circuit (ITSC) fault is caused by partially short circuit faults in some turns of stator windings due to isolation aging or failures. Such aging and failures are usually caused by line current harmonics and chemical corrosion. When the ITSC faults appear, a local loop will be generated in the fault location. This loop will induce a high-amplitude short circuit fault current and cause local overheat. Then, further damage to the machine windings. In this paper, the ITSC fault is modeled in the context of permanent magnet synchronous machines. The equivalent circuit of such ITSC fault is shown in Fig. 3. (Suppose the fault appears in phase A.) In Fig. 3, there are n turns out of N-turn-winding shorted. The fault turn ratio μ is then defined as $\mu = \frac{n}{N}$. In addition, the short circuit contact resistance is defined as R_f, and i_f is the circulating current caused by the short circuit fault.

According to the equivalent circuit in Fig. 3, the system equations under ITSC fault could be written as followings:

$$v_{a,f} = R_s \cdot i_{a,f} - \mu R_s \cdot i_f + \frac{d}{dt}\lambda_{a,f} \quad (4)$$

$$v_{b,f} = R_s \cdot i_{b,f} + \frac{d}{dt}\lambda_{a,f} \quad (5)$$

$$v_{c,f} = R_s \cdot i_{b,f} + \frac{d}{dt}\lambda_{a,f} \quad (6)$$

$$\lambda_{a,f} = L_{aa} \cdot i_{a,f} + M_{ab} \cdot i_{b,f} + M_{ac} \cdot i_{c,f} - \mu L_{aa} \cdot i_f + \lambda_{PM} \cdot \cos(\theta) \quad (7)$$

$$\lambda_{b,f} = M_{ba} \cdot i_{a,f} + L_{bb} \cdot i_{b,f} + M_{bc} \cdot i_{c,f} - \mu M_{ba} \cdot i_f + \lambda_{PM} \cdot \cos(\theta - \frac{2\pi}{3}) \quad (8)$$

$$\lambda_{c,f} = M_{ca} \cdot i_{a,f} + M_{cb} \cdot i_{b,f} + L_{cc} \cdot i_{c,f} - \mu M_{ca} \cdot i_f + \lambda_{PM} \cdot \cos(\theta + \frac{2\pi}{3}) \quad (9)$$

$$v_f = 0 = -(R_f + \mu R_s) \cdot i_f + \mu R_s \cdot i_{a,f} + \frac{d}{dt}\lambda_f \quad (10)$$

$$\lambda_f = \mu L_{aa} \cdot i_{a,f} + \mu M_{ab} \cdot i_{b,f} + \mu M_{ac} \cdot i_{c,f} - \mu^2 L_{aa} \cdot i_f + \mu \lambda_{PM} \cdot \cos(\theta) \quad (11)$$

C. Cyberattacks: False Data Injection Attacks

The cyberattack in this case study is also one of the most common attacks, the false data injection (FDI) attack. It means the attacker maliciously injects false data sequences into the digital control units after compromising, such as wrong parameters, abnormal register status, Etc. In this paper, the case study of FDI attacks includes two types of false data injections: 1) bias injections to the motor line current feedback signals; 2) malicious control sequences injected into the motor voltage commands. These attacks are designed to mimic the behaviors of ITSC and bearing faults discussed in previous sections. The goal of such attacks is to confuse the original fault detectors and cause unnecessary downtime and maintenance costs. The attack model is shown in Eq. (12) and Eq. (13), where $\hat{s_k}$ is the attacked signal, s_k is the original signal, K_{atk} is the bias coefficient, $M \cdot \sin\omega_{atk}t$ is the malicious control sequences, and ω_{atk} is selected according to the characteristic frequencies of bearing faults. The attack period is denoted as T_{ATK}.

$$\text{Type I: } \hat{s_k} = \begin{cases} s_k & (t \notin T_{ATK}) \\ s_k \cdot K_{atk} & (t \in T_{ATK}) \end{cases} \quad (12)$$

$$\text{Type II: } \hat{s_k} = \begin{cases} s_k & (t \notin T_{ATK}) \\ s_k + M \cdot \sin\omega_{atk}t & (t \in T_{ATK}) \end{cases} \quad (13)$$

III. Data-Driven Approach for Detecting and Diagnosing Physical Faults and Cyberattacks

The proposed approach is to search for features and patterns in the motor line current spectra, which could distinguish the system status among the healthy, fault, and attack conditions. As shown in Fig. 4 - Fig. 6, the line current waveforms of these three statuses are highly similar and are not distinguishable via human eyes. Therefore, the traditional rule-based methods through establishing some pre-defined thresholds are not feasible in these situations. The proposed approach adopts and compares four data-driven classification methods, namely random forests (RF), logistic regression (LR), support vector machines (SVM), and k-nearest-neighbor (KNN). These four classification methods represent four of the most widely used approaches for classification:

1) Random Forests (RF) 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 decision tree.
2) K-Nearest-Neighbor (KNN) 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 k nearest neighbors.
3) Support Vector Machines (SVM) is a representation of the training data set as support vectors (or points) in the feature space, which map the training data set to the separate classes divided 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.
4) Logistic Regression (LR) models the probability function of a certain class based on the predictors. For example, $l = \log_b \frac{p}{1-p} = \beta_0 + \sum_{i=1}^{q} \beta_i x_i$

The proposed method will monitor the motor line current

signals using sliding windows. The window size will be determined by the signal sampling frequency and required spectrum frequency resolution. The proposed method will first extract the signal spectra using fast Fourier transformation at every instant. Then, it will feed the frequency features to the pre-trained classification models. According to the current and previous classification results, a majority vote mechanism will be applied to determine the final detection outcomes. The detection results will then determine whether or not to generate an alarm. The detailed algorithm is shown in Algorithm 1.

Algorithm 1 Anomaly Detection Algorithm for Distinguishing Stealthy Cyber-Attacks from Common Physical Faults

Input: Real time line current measurements of both motor drives.
Output: Detection and diagnostic alarms.
Setting total voting capacity as v_{max};
for $i = 0, 1, 2, 3, 4, \ldots$ do
  for $k = 0, 1, 2, 3, \ldots, v_{max}$ do
    Recording and storing real-time measurements in a sliding window with size m and sampling time t_s;
    Extracting frequency features using FFT;
    Calculating the classification results by feeding the frequency features into pre-trained data-drive classification model;
    Saving the classification result D_k;
  end for
  Selecting the dominant classification result in D as A_i;
  Ouptut detection and diagnostic alarms A_i.
  Clearing the voting array D;
end for

IV. Case Study and Simulation Results

In this paper, the case study adopted a dual-motor electric vehicle powertrain to simulate the fault and attack scenarios to validate the performance of the proposed method. The general diagram of the powertrain is shown in Fig. 1. The powertrain consists of two motor drives: the front-wheel-drive is a permanent magnet synchronous machine (PMSM), and the rear-wheel-drive is an induction machine (IM). Both machines are controlled by Filed-Oriented-Control (FOC) with proportional-integral (PI) regulators. The detector extracts the motor line winding current signals from both front and rear drives. The sampling rate is 20 kHz, and a sliding window of size 400 is adopted. Then, the detector calculates the spectra from both current signals and extracts the magnitudes for frequencies ranging from 0 Hz to 1000Hz. The case study includes 128 scenarios covering different bearing faults, ITSC faults, FDI attacks, and operating conditions. The details of these scenarios are described in TABLE I - TABLE IV, and some samples of line current waveforms in the case study are shown in Fig. 4 - Fig. 6. According to the waveforms in Fig. 4 - Fig. 6, the cyber-attacks and physical faults are hard to distinguish using traditional residual-based methods.

TABLE I
List of Steady-State Operating Conditions

No.	Machine Speed (rpm)	Load Torque (Nm)
1	1000	200
2	1500	150
3	1000	50
4	1500	50

TABLE II
List of ITSC Fault Scenarios

No.	Short-Turn Ratio μ	Short Resistance R_f
1	0.10	1
2	0.15	1
3	0.20	1
4	0.25	1
5	0.10	5
6	0.15	5
7	0.20	5
8	0.25	5

TABLE III
List of Bearing Fault Scenarios
(Characteristic frequency is calculated according to the model in section II-A.)

No.	Characteristic Frequency	$\Delta L_m / L_m$
1	f_{co}	0.4
2	f_{ci}	0.4
3	f_o	0.4
4	f_i	0.4
5	f_{co}	0.6
6	f_{ci}	0.6
7	f_o	0.6
8	f_i	0.6

TABLE IV
List of FDI Attack Scenarios

No.	Bias Injection K_{atk}	Malicious Control
1	+0.1	NA
2	-0.1	NA
3	+0.2	NA
4	-0.2	NA
5	NA	$M = 8, f_{atk} = f_{co}$
6	NA	$M = 8, f_{atk} = f_{ci}$
7	NA	$M = 8, f_{atk} = f_o$
8	NA	$M = 8, f_{atk} = f_i$

With the 128 scenarios in the case study, we generated 12800 samples of the line current frequency features. Among these samples, 80% are randomly selected as the training data sets, and the rest 20% are the testing sets.

The testing results and detection accuracy of the four classification methods are shown in TABLE V - TABLE IX. In addition, normalized confusion matrices of each method are shown in Fig. 7 as well.

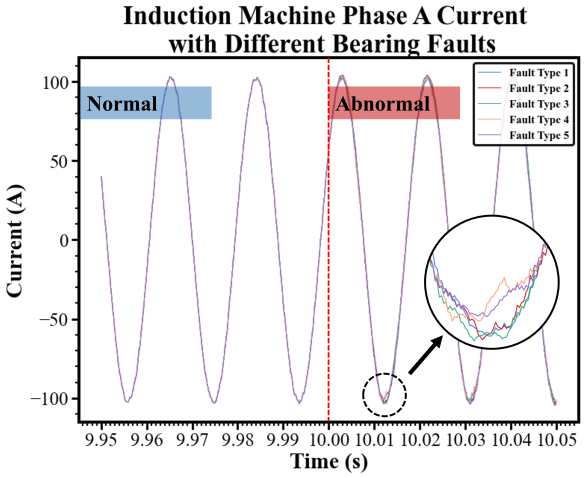

Fig. 4. Samples of the line current waveforms with different bearing faults in the induction machine.

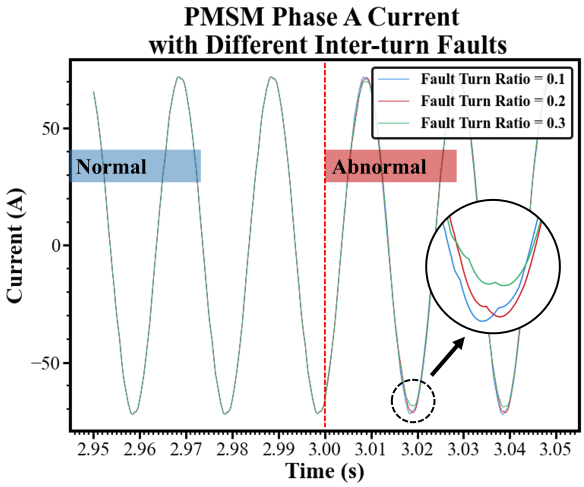

Fig. 5. Samples of the line current waveforms with different ITSC faults in the PMSM.

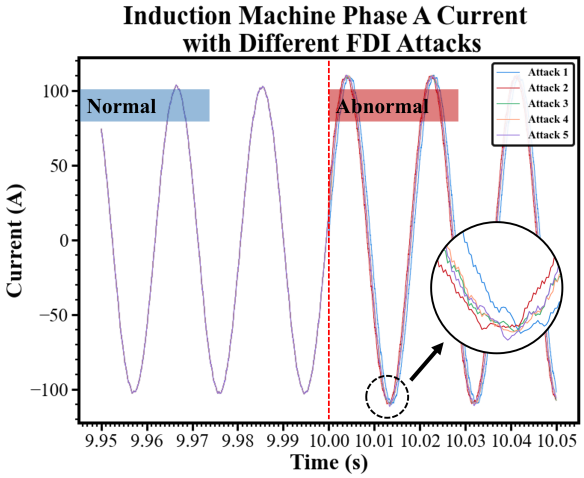

Fig. 6. Samples of the line current waveforms with different FDI attacks in the induction machine.

Among these results, all the classification methods could achieve an accuracy above 80% apart from the Logistic Regression, and Random Forests could reach an accuracy higher than 90%. Meanwhile, according to the confusion matrices and detection outcomes, distinguishing such cyber-attacks from common physical faults is much more challenging than distinguishing abnormal conditions from normal conditions. For all four methods, the accuracy of detecting anomalies is almost 100%.

TABLE V
ACCURACY OF DATA-DRIVEN CLASSIFIERS

Random Forests	90%
K-Nearest-Neighbor	84%
Support Vector Machine	82%
Logistic Regression	63%

TABLE VI
CONFUSION MATRIX OF TESTING REUSLTS: KNN

		Prediction		
		Attack	Normal	Fault
Reference	Attack	345	37	273
	Normal	0	1264	0
	Fault	64	42	535

TABLE VII
CONFUSION MATRIX OF TESTING REUSLTS: LR

		Prediction		
		Attack	Normal	Fault
Reference	Attack	211	404	40
	Normal	7	1257	0
	Fault	51	451	139

TABLE VIII
CONFUSION MATRIX OF TESTING REUSLTS: RF

		Prediction		
		Attack	Normal	Fault
Reference	Attack	494	0	161
	Normal	0	1264	0
	Fault	69	4	568

TABLE IX
CONFUSION MATRIX OF TESTING REUSLTS: SVM

		Prediction		
		Attack	Normal	Fault
Reference	Attack	374	150	131
	Normal	0	1264	0
	Fault	79	112	450

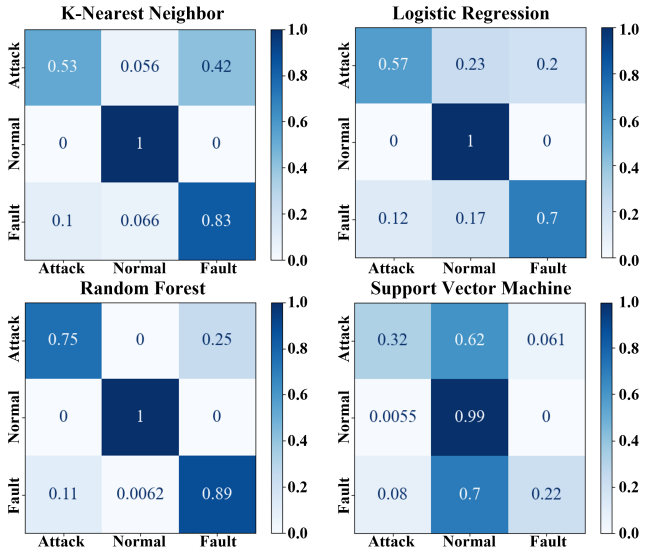

Fig. 7. Confusion matrices of 4 data-driven classifiers.

V. Conclusion

This paper proposed a data-driven approach to detect and diagnose stealthy cyberattacks and common physical faults. The proposed method is tested and validated from a case study with a simulated dual-motor electric vehicle powertrain. A case study includes 128 scenarios covering ITSC faults, bearing faults, and FDI attacks. The detection and diagnostic results of the case study prove this method's high accuracy and performance. Meanwhile, it also demonstrated that distinguishing stealthy attacks from common physical faults is much more challenging than detecting anomalies from normal conditions.

References

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

[2] G. Kliman and J. Stein, "Methods of motor current signature analysis," Electric Machines and power systems, vol. 20, no. 5, pp. 463–474, 1992.

[3] C. Kar and A. Mohanty, "Monitoring gear vibrations through motor current signature analysis and wavelet transform," Mechanical systems and signal processing, vol. 20, no. 1, pp. 158–187, 2006.

[4] W. T. Thomson and M. Fenger, "Current signature analysis to detect induction motor faults," IEEE Industry Applications Magazine, vol. 7, no. 4, pp. 26–34, 2001.

[5] K. Kim and A. G. Parlos, "Induction motor fault diagnosis based on neuropredictors and wavelet signal processing," IEEE/ASME Transactions on mechatronics, vol. 7, no. 2, pp. 201–219, 2002.

[6] N. Eldin et al., "Explicit modelling of the stator winding bar water cooling for model-based fault diagnosis of turbogenerators with experimental verification," in 1994 Proceedings of IEEE International Conference on Control and Applications. IEEE, 1994, pp. 1403–1408.

[7] A. Dexter, "Fuzzy model based fault diagnosis," IEE Proceedings-Control Theory and Applications, vol. 142, no. 6, pp. 545–550, 1995.

[8] P. Bo, A. Granato, M. E. Mancuso, C. Ciccotelli, and L. Querzoni, "Fada-cps—faults and attacks discrimination in cyber physical systems," in Policy-Based Autonomic Data Governance. Springer, 2019, pp. 91–112.

[9] A. Anwar, A. N. Mahmood, and Z. Shah, "A data-driven approach to distinguish cyber-attacks from physical faults in a smart grid," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management, 2015, pp. 1811–1814.

[10] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," Electric Power Systems Research, vol. 193, p. 107024, 2021.

[11] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3301–3310, 2020.

[12] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," IEEE Transactions on Transportation Electrification, vol. 7, no. 3, pp. 2010–2022, 2021.

[13] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639–4657, 2021.

[14] B. Yang, L. Guo, and J. Ye, "Physics-based attack detection for traction motor drives in electric vehicles using random forest," in 2021 IEEE Applied Power Electronics Conference and Exposition (APEC), 2021, pp. 849–854.

[15] L. Guo, B. Yang, and J. Ye, "Detection and diagnosis of long-term cyber-attacks for predictive energy management system in hevs," in 2021 IEEE Applied Power Electronics Conference and Exposition (APEC), 2021, pp. 842–848.

[16] L. Guo, B. Yang, J. Ye, and J. M. Velni, "Attack-resilient lateral stability control for autonomous in-wheel-motor-driven electric vehicles," in 2021 IEEE Transportation Electrification Conference Expo (ITEC), 2021, pp. 200–205.

[17] L. Guo, B. Yang, J. Ye, J. M. Velni, and W. Song, "Attack-resilient lateral stability control for four-wheel-driven evs considering changed driver behavior under cyber threats," IEEE Transactions on Transportation Electrification, pp. 1–1, 2021.

[18] B. Yang, J. Ye, and L. Guo, "Fast detection for cyber threats in electric vehicle traction motor drives," IEEE Transactions on Transportation Electrification, pp. 1–1, 2021.

[19] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 2, pp. 319–333, 2021.

[20] H. A. Toliyat, S. Nandi, S. Choi, and H. Meshgin-Kelk, Electric machines: modeling, condition monitoring, and fault diagnosis. CRC press, 2012.

[21] S. Zhang, B. Wang, M. Kanemaru, C. Lin, D. Liu, M. Miyoshi, K. H. Teo, and T. G. Habetler, "Model-based analysis and quantification of bearing faults in induction machines," IEEE Transactions on Industry Applications, vol. 56, no. 3, pp. 2158–2170, 2020.