Data-Driven Approach for Detection of Physical Faults and Cyber Attacks in Manufacturing Motor Drives

Bowen Yang
College of Engineering
University of Georgia
Athens, GA, U.S.A.
bowen.yang@uga.edu

Jin Ye
College of Engineering
University of Georgia
Athens, GA, U.S.A.
jin.ye@uga.edu

Stephen Coshatt
Center for Cyber-physical Systems
University of Georgia
Athens, GA, U.S.A.
stephen.coshatt@gmail.com

Wenzhan Song
Center for Cyber-physical Systems
University of Georgia
Athens, GA, U.S.A.
wsong@uga.edu

Feraidoon Zahiri
402 CMXG/MXDEO
Robins Air Force Base
Warner Robins, GA, U.S.A.
feraidoon.zahiri@us.af.mil

2022 IEEE Energy Conversion Congress and Exposition (ECCE) | 978-1-7281-9387-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ECCE50734.2022.9948143

Abstract—In recent decades,the utilization of digital control units and communication networks in modern manufacturing systems has increased significantly. These valuable and safety-critical systems are facing new threats from physical and cyber domains. There is still a gap between studies of physical faults and cyber-attacks on motor drives. it is critical for future motor drives in manufacturing systems to develop attack and fault detection and diagnostic solutions to guarantee system safety and security. To narrow this gap, this paper proposes a data-driven method for detecting and distinguishing cyber-attacks and some common physical faults for manufacturing motor drives. The proposed method integrates the PCC line current spectra and four widely used data-driven classifiers to detect and distinguish cyber-attacks and physical faults. We form a comprehensive case study to validate the proposed methods, including sophisticated false data injection attacks and the two most common physical faults, inter-turn short circuit faults and bearing faults. The final testing results suggest that the proposed method could achieve 95% or higher detection accuracy.

Index Terms—motor drives, manufacturing, security, anomaly detection, diagnostics

I. Introduction

Valuable and safety-critical systems are facing new threats from physical and cyber domains due to the pervasive utilization of digital control units and communication networks in modern manufacturing systems. There is an urgent need for future manufacturing systems to have an advanced monitoring solution targeting physical faults and cyber-attacks, especially for high-power motor drives. Gap still exists between stud-ies of physical faults and cyber-attacks on motor drives. Such a gap could be summarized in three aspects. First, cyber-attacks and physical faults have different dynamics and mechanisms. Physical faults will essentially change part of the fundamental physics of the systems. For example, inter-turn short circuit faults will create a local short circuit loop within the fault winding. Moreover, bearing faults will cause machine shaft vibrations, leading to periodic changes in the machine winding inductances. However, cyber-attacks will not necessarily change the system's fundamental physics. Instead, they will directly or indirectly change the digital controller behaviors to achieve some objectives established by attackers. The second gap is that cyber-attacks and physical faults have different countermeasures. For physical faults, the most common protocol is to shut down and isolate the fault system and conduct thorough maintenance to eliminate the faults. On the other hand, when the system detects cyber-attacks, some standard approaches include rebooting the system or conducting a hot patch. Finally, in most recent literature, cyber-attacks and physical faults are still two different topics in different communities. Therefore, most research focuses on physical faults or cyber-attacks individually instead of simultaneously. [1] For motor drives, studies of physical faults are more mature than cyber-attacks. In the last decades, there have been many literatures addressing physical faults from different directions, such as motor current signature analysis [2]–[4], time-domain analysis [5]–[7], data-driven methods [8]–[10], etc. Nevertheless, studies addressing cyber-attacks on motor drives did not arise until recent years. For example, [11] studied the vulnerabilities of motor drives due to sensor attacks, and [12], [13] proposed a fast attack detection method based on motor time-domain and frequency-domain features, respectively. Meanwhile, most studies addressing cyber-attacks focused on general cyber-physical systems instead of motor drives. For example, [14]–[16] propoosed some detection solu-

This research was partially supported by US Air Force, U. S. National Science Foundation NSF-ECCS–1946057 and ECCS-EPCN-2102032.

978-1-7281-9387-8/22/$31.00 ©2022 IEEE

tions using the attacker versus defender dynamics, distributed attack detection, and state recovery.

To guarantee system safety and security of thr future motor drives in manufacturing systems, it is critical to developing fast detection and accurate diagnostic solutions targeting cyber-attacks and physical faults. To narrow this gap, this paper proposed a data-driven method for detecting and distinguishing cyber-attacks and common physical faults for manufacturing motor drives.

The rest of the paper first describes fault and 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. Modeling

In most motor drive literature, physical faults and cyber-attacks are still two different topics in different communities. Therefore, they addressed physical faults and cyber-attacks individually instead of simultaneously. For future motor drives in manufacturing systems, it is necessary to develop solutions targetting faults and attacks at the same time. This paper forms a comprehensive case study to achieve such goals, including common physical faults and cyber-attacks in a dual-motor network. Such a network consists of a permanent magnet synchronous machine (PMSM) and an induction machine (IM), and fig. 1 shows its system diagram. This section will discuss the mathematical models adopted for these fault and attack scenarios.

A. Physical Fault Modeling

This paper adopts two of the most common physical faults in motor drives: the inter-turn short circuit faults (ITSCs) and the bearing faults. As shown in fig. 1, the ITSCs are considered in the PMSM, and the bearing faults are in the IM.

1) Inter-Turn Short Circuit Faults in PMSM: The Inter-turn short circuit (ITSC) fault is caused by partially short circuited faults in some turns of stator windings due to isolation aging or failures. Such aging and failures are usually caused by mechanical frictions and chemical corrosion. The equivalent

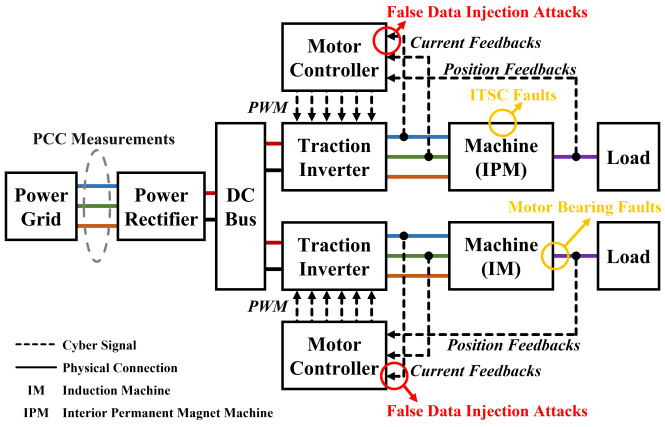

Fig. 1. System diagram of the dual-motor network.

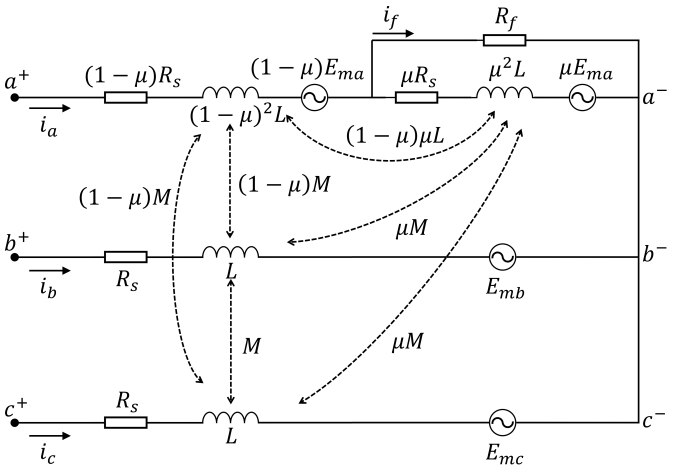

Fig. 2. The equivalent circuit of the ITSC fault.

circuit of the such ITSC is shown in Fig. 2. (Suppose the fault appears in phase A.) As shown in Fig. 2, the ITSC fault will change the winding structures and lead to winding parameter changes, such as inductance, resistance, and back-EMF. In Fig. 2, there are n turns out of N-turn-winding shorted. The fault turn ratio μ is then defined as $\mu = \frac{n}{N}$. The short circuit contact resistance is defined as R_f, and i_f is the circulating current caused by the short circuit fault.

2) Bearing Faults in IM: Bearing faults are one of the primary fault conditions in the induction machine. Such faults account for more than 50% of the total failure cases in real-world applications. [17] Bearing faults are usually caused by mechanical frictions and chemical corrosion. When a bearing fault appears, it will cause the eccentricity to the rotor shaft and break the symmetry among all the phase windings. Such eccentricity will lead to periodic changes in the machine winding inductance. The periodic changes have different characteristic frequencies depending on the fault types. Below are five typical bearing faults and the related characteristic frequencies.

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

where N_b is the number of balls, f_r is the mechanic rotating frequency of the rotor, and the geometry parameters of the bearing is shown in Fig. 3.

B. Cyber-Attack Modeling

The primary attack surface in manufacturing motor drive networks is the communication network. [18] Attackers could

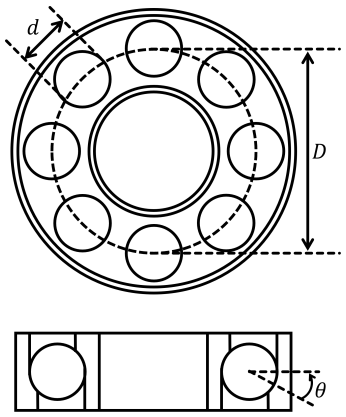

Fig. 3. Geometry parameters of the bearing.

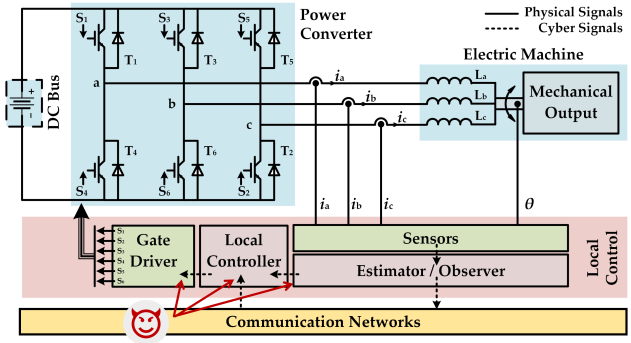

Fig. 4. Diagram of attack targets on manufacturing motor drive controllers.

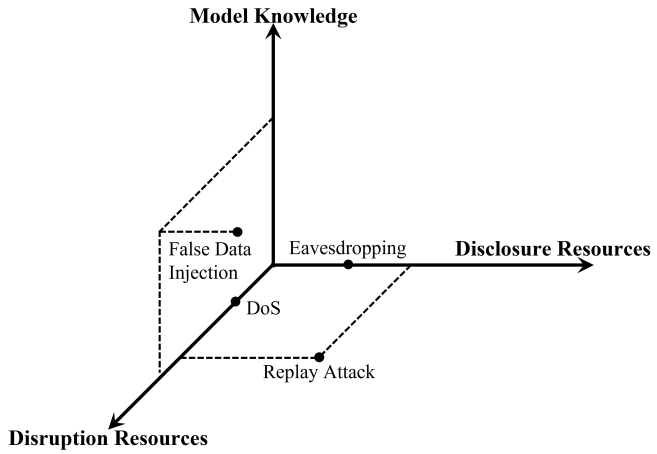

Fig. 5. Diagram of the attack space.

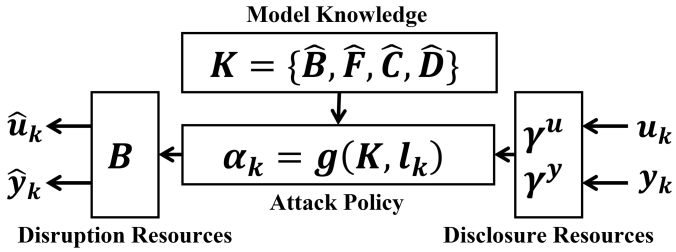

Fig. 6. Diagram of the adversary model.

compromise different digital controllers by exploring the vulnerabilities of various communication protocols and controller firmware. For example, communication buses like Modbus and CAN are widely used in manufacturing systems, but these communication protocols are commonly designed without sufficient encryptions and authentications. Therefore, there have been many reports on the vulnerabilities of these protocols. Then, after compromising the networks or the digital controllers, the attacker could seek various objectives, such as damaging the devices and causing unexpected financial loss.

We summarize primary targets for the motor drive controllers into three categories: controller feedback signals, controller reference settings, and critical register data. Fig. 4 depicts a diagram of these attack targets on manufacturing motor drive controllers. The attackers could easily manipulate the motor drive behaviors by maliciously modifying these data, usually referred as false data injection attacks. For example, the attacker could deliberately increase or decrease the motor speed and change control parameters to lower the system performance.

To formally quantify these cyber attacks in motor drive networks, we adopted the threat models in this paper. This model uses the available adversary's resources to map different attacks into a three-dimension attack space. Fig. 5 shows a conceptual diagram to visualize the attack space.

The adversary's resources include the a priori system model knowledge, disclosure resources, and disruption resources. The a priori model knowledge can be used by the adversary to construct more complex attacks, possibly harder to detect, and with more severe consequences. The disclosure resources enable the adversary to obtain sensitive information about the system during the attack by violating data confidentiality. Note that disclosure of resources alone cannot disrupt the system operation. On the other hand, the disruption resources can be used to affect the system operation. For instance, when data integrity or availability properties are violated.

Based on the above attack space, every cyber attack could be developed through the adversary model shown in Fig. 6. In this model, the attack is composed of an attack policy and the adversary's resources.

III. Methodology

The detection method proposed in this paper is based on four different types of data-driven classifiers and uses only the line current signals from the Point of Common Coupling (PCC).

Fig. 7 shows a flowchart of the proposed method. The detection algorithm first acquires independent measurements from the isolated current sensors at the PCC. Then, the line current data is transformed to the frequency domain with Fast-Fourier-Transformation (FFT). After extracting and normalizing the spectrum features, the algorithm will then

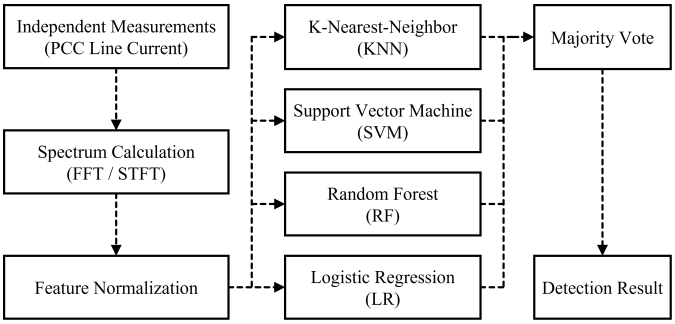

Fig. 7. Flowchart of the proposed detection procedure.

feed these features to four individual classifiers, namely k-nearest-neighbor (KNN), support vector machine (SVM), random forests (RF), and logistic regression (LR). These four classifiers will calculate the detection results independently. Finally, the algorithm will conduct a majority vote among the results generated from the classifiers, and generate an alarm when three or more classifiers detect a fault or an attack.

The rest of this section will discuss each step in more detail.

A. Independent Measurements at PCC and Feature Extraction

The proposed method uses only the line current signals at the PCC for the following reasons:

1) It will be much easier to guarantee the safety and security of the monitoring system since it only requires one set of sensors at the PCC;
2) It will be possible to isolate the entire monitoring system from the original system and those vulnerable communication networks.
3) The monitoring system will be easy to install or upgrade due to its simplicity.
4) The overall cost of the monitoring system will be much lower than other solutions requiring extra information from individual machines.

In addition, it should be pointed out that the sampling frequency of these measurements should be no less than 2kHz because the maximum spectrum frequency required by the algorithm is at least 1kHz.

After acquiring the measured line current signals, the algorithm uses a sliding window to segregate the measurement data into batches. Within each sliding window, FFT is adopted to extract the current spectrum.

B. Data-Driven Classificatiers

Because the cyber-attacks targetting motor drive controllers could be highly sophisticated and it is challenging to distinguish such attacks from physical faults, using a single classifier will result in low detection accuracy. Therefore, this paper adopted four different types of data-driven classifiers to improve detection accuracy. Each classifier processes the same features independently, and then a majority vote procedure will determine the final results based on the outcomes of each individual classifier. Such an approach will largely reduce the false detection results. The four classifiers represent four typical classification methods with different characteristics:

- RF represents classification tree based methods;
- KNN represents non-parametric classifiers;
- SVM represents support vector based classifiers;
- LR represents regression based algorithms.

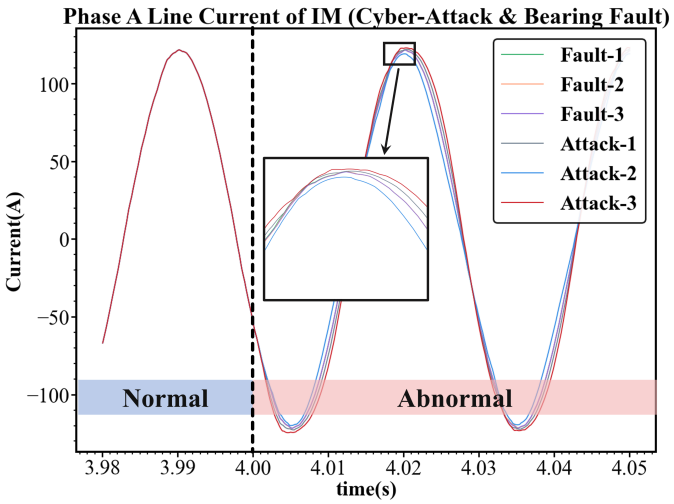

Fig. 8. IM line current waveforms in different bearing faults and FDI attacks scenarios.

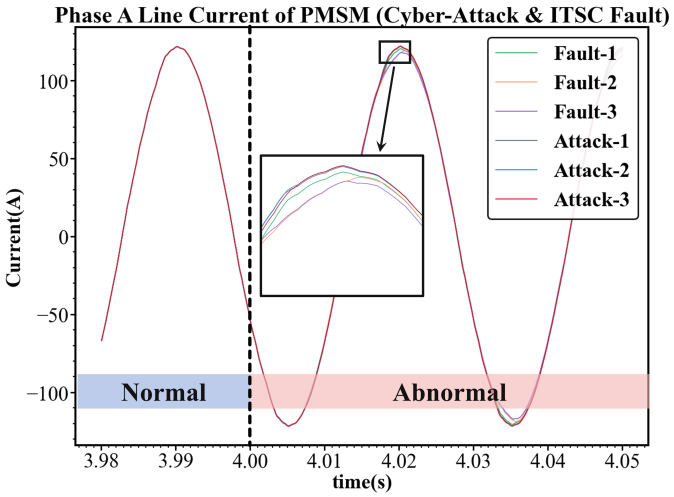

Fig. 9. PMSM line current waveforms in different ITSC faults and FDI attacks scenarios.

IV. Simulation

As stated in Section II, this paper formed a comprehensive case study including physical faults and cyber-attacks in a dual-motor manufacturing motor drive network. Fig. 1 shows the system diagram of the simulation model for this dual-motor network. The system consists of two motor drives: a permanent magnet synchronous machine (PMSM) and an induction machine (IM). Both machines are controlled by Filed-Oriented-Control (FOC) with proportional-integral (PI)

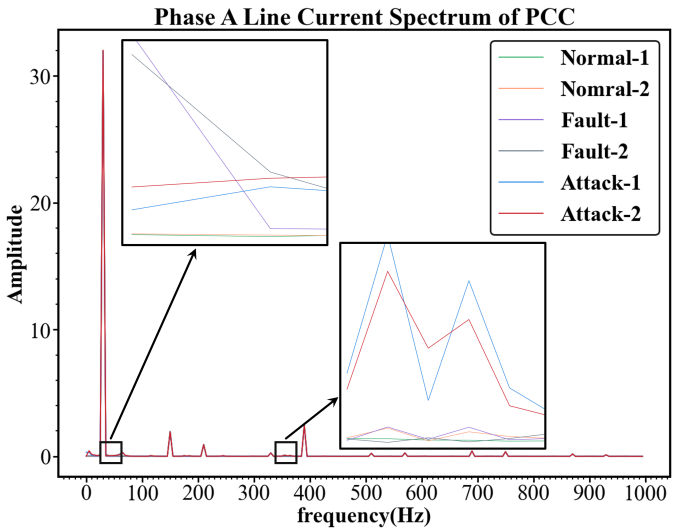

Fig. 10. Spectrum of PCC line currents in different fault and attack scenarios.

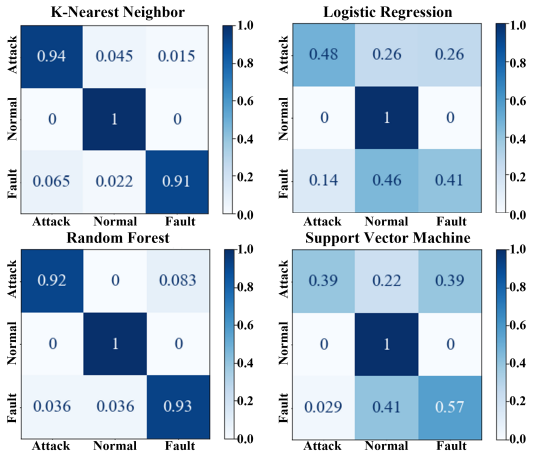

Fig. 11. Confusion matrices of the detection accuracy from individual classification methods (Normalized).

TABLE I
CONFUSION MATRIX OF TESTING REUSLTS (NORMALIZED)
(OVERALL DETECTION ACCURACY: 95.5%)

		Prediction		
		Attack	Normal	Fault
Reference	Attack	0.96	0.01	0.03
	Normal	0	1	0
	Fault	0.04	0.01	0.95

regulators on motor speed and current. The detector locates at the PCC, denoted as a grey dashed circle in fig. 1 and extracts the PCC line current signals.

In this case study, the fault scenarios include the inter-turn short circuit faults in PMSM stator windings and bearing faults in the induction machine. Different fault scenarios are designed by setting different fault parameters in the fault models described in section II. Meanwhile, the cyber-attack scenarios are also designed using the adversary models described in section II. According to the adversary model, the attacks are dependent on the available resources to the attackers. Usually, the more resources they have, the more sophisticated the attack will be. On the other hand, naive attacks with limited adversary resources are more likely to cause drastic impacts on the systems. Such naive attacks are comparably easier to detect because the attack impacts are more significant and noticeable to the detectors. However, the impacts will be more subtle and much more challenging to detect for more sophisticated attacks. For these more sophisticated attacks, traditional detectors will not be sufficient. Therefore, the attack scenarios considered in this paper are specifically designed to achieve the objectives established by the attackers. More specifically, these attacks will try to emulate some of the fault responses and trigger the false alarms to the original system monitors. Recently, as many applications have adopted physical fault detectors based on current signature analysis, the detection results heavily depend on specific frequency components. Therefore, these attacks could confuse the original fault detectors and trigger false alarms, leading to unnecessary shutdown and maintenance. For example, fig. 8 and fig. 9 show some waveforms of IM and PMSM in different fault and such types of attack scenarios. In these scenarios, the attackers use FDI attacks on the motor drive controller current feedbacks and voltage command outputs to mimic the bearing and ITSC faults in IM and PMSM, respectively. As suggested by these waveforms, the faults and attacks are highly similar. However, these attacks are not identical and leave traces in the PCC line currents. Fig. 10 shows some PCC line current spectra from the above scenarios. According to the spectra, there are still some distinguishable signatures, but it will be challenging for traditional current signature analysis because the signatures are too subtle. Therefore, it is beneficial to adopt the proposed data-driven detection method in these situations.

In summary, the case study in this paper includes 128 scenarios covering different bearing faults, ITSC faults, FDI attacks, and operating conditions, and, with these scenarios, we generated 12800 samples of the PCC line current measurements. Among these samples, 80% are randomly selected as the training data sets, and the rest 20% are the testing sets.

Table I shows the overall testing results, and fig. 11 shows the detection results of individual classification methods. According to the results, the individual classifiers tend to have poor performances as predicted, and the majority vote procedure is proved promising.

V. CONCLUSION

This paper first studied the impacts of different cyber-attacks and physical faults on manufacturing motor drives in different scenarios and then proposed a data-driven approach to detect and distinguish sophisticated cyber-attacks and common physical faults. The proposed method is tested and validated from a comprehensive case study with a simulated dual-motor-drive network in manufacturing systems. The final testing results suggest that the proposed method could achieve 95% or higher detection accuracy.

REFERENCES

[1] 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.

[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 cool-ing 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] 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.

[13] 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.

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

[15] O. Vukovic´ and G. Dań, "Detection and localization of targeted attacks on fully distributed power system state estimation," in 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2013, pp. 390–395.

[16] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in 2013 American control conference. IEEE, 2013, pp. 3344–3349.

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

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