Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 70 (2023) 44–51

Transportation Research Procedia

www.elsevier.com/locate/procedia

8th International Electric Vehicle Conference (EVC 2023)

Cyber Attack Detection and Classification for Integrated On-board Electric Vehicle Chargers subject to Stochastic Charging Coordination

Ali Arsalan[a,*], Laxman Timilsina[b], Behnaz Papari[c], Grace Muriithi[d], Gokhan Ozkan[e], Phani Kumar[f], and Christopher S. Edrington[g]

[a,c,d] *Department of Automotive Engineering, Clemson University, Greenville 29607, U.S.*
[b,e,f,g] *The Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson 29631, U.S*
Distribution A. Approved for public release; distribution unlimited. (OPSEC 7474)

Abstract

Cyber-physical system (CPS) of EV on-board chargers is connected to an IOT-based communication network for coordinated control, which is highly vulnerable to cyber-attacks. This charging coordination control incorporating hundreds of EVs and associated charging sessions, feed in a stochastic reference input to energy management system (EMS) of on-board EV chargers. Hence, under these varying operating conditions, a pure data-driven-based detection model can experience a disturbance detection failure. Therefore, a model predictive control (MPC) based machine learning (ML) network, integrated with a residual based training data pre-processing is proposed in this paper. This MPC based ML approach can effectively detect a tempered response while addressing the aleatory behaviour of cooperative control with enhanced disturbance detection accuracy. The proposed model utilizing various system level signals can also efficiently classify a normal condition, cyber-attack, and a physical fault. The superior performance of the proposed approach is validated by using different case study scenarios of training datasets.

Keywords: Integrated on-board chargers (IOBCs); cyber-attack; MOSFET fault, neural networks; model predictive control; direct power control

1. Introduction

EV supply equipment (EVSE) technologies will have a great impact on the expansion of EV market at both commercial and domestic level. These EVSEs can be generally categorized into an on-board and off-board architecture

* Corresponding author. Tel.: +1-864-765-4881
E-mail address: aarsala@clemson.edu

10.1016/j.trpro.2023.10.007

with unidirectional/bidirectional power flow characteristics (Jalakas et al., 2012; Timilsina et al., 2023). In on-board configurations, integrated on-board chargers exploit the existing EV propulsion system components including motor winding and bidirectional AC/DC traction converter for battery energy storage (Shi et al., 2017). This bidirectional power converter of traction drive can operate in charging/discharging mode while providing grid to vehicle (G2V), vehicle to grid (V2G), and vehicle to vehicle (V2V) energy transactions. These energy transactions utilize the cooperative capacity sharing schemes (Hoang et al., 2022; Hoang et al., 2023; Arsalan et al., 2020) for energy management that controls the power electronics systems (PESs). So, we can say that the electronic control unit (ECU) operates the power converters to control the overall operation of EVs from on-board charging/discharging to distributed-driven e-powertrain. These power converters further implement the coordinated control via inter or intra-connectivity to a vast control network through ECUs. This connectivity makes the EV cyber-physical systems more vulnerable to cyber-attacks with a broader attack surface (Hodge at al., 2019). A compromised power converter can cause the performance degradation by overcharging or depleting the EV battery while destabilizing the normal operation of the energy management system (EMS) and electric drive system. In (Gumrukcu et al., 2022), a single point failure case is studied for a charging coordination approach managing charging sessions for hundreds of EVs under cyber-attack. According to a report, hackers disabled the traction control system and exposed the private information of a consumer by exploiting the security flaws of Volkswagen range and Ford (Tengler et al., 2020). In addition, around 150 cyber-attacks were recorded in 2019, targeting the automobile sector (Tengler et al., 2020). Therefore, the need of an efficient, and smart detection strategy is inevitable to maintain a stable and continuous operation of EV integrated PESs. In this regard, a fast detection scheme for PESs is proposed based on binary classifiers with a majority vote mechanism to improve the model accuracy (Yang at al., 2022). A coordinated detection approach by considering the state observer and system performance evaluation metrics is presented to detect the cyber-attacks in EVs (Guo et al., 2021). The impact of cyber-attacks on power converters is assessed in (Dayanikli et al., 2020) and (Yang et al., 2019), along with the effects of intentional electromagnetic interference on the operation of voltage, current and gate drive outputs (Dayanikli et al., 2020). A random forest-based classifier is presented in (Yang et al., 2021), to distinguish between a normal and abnormal operation of EV motor drive by using phase current. In (Kwon et al., 2013) and (Dán et al., 2010), intelligent and stealthy deception cyber-attacks are researched which can avoid detection by detection control layer.

In general, cyber-attack detection can be categorized as model based and data-driven based approach. The main idea of model-based approach is to obtain a residual signal between a predicted and actual values in order to check the proximity of a cyber-attack (Giraldo et al., 2018; Mo et al., 2013). However, PESs with a complex cyber physical layer due to multiple nonlinear constraints involved makes it inapplicable to use a simple linear model for intrusion detection. Therefore, data driven approach is preferred in most of the recent studies, which is a machine learning (ML) based model free method, where system parameters are used to train a ML model. The abnormal conditions are detected by using different classifier such as K-nearest neighbor, logistic regression, random forest, and support vector machine (Yang et al., 2022). However, the stochastic behaviour of EVSE charging coordination, EMS nonlinearities, and varying operating conditions leads to training failure in pure data-driven approaches. In addition, the above discussed studies are mainly focused on distinguishing between a normal and abnormal operation. However, it is also important to distinguish whether the disturbance is due to a physical fault or a cyber-attack.

Therefore, in this proposed research a model predictive based ML model is presented where the model based, and data driven based solutions are used together to improve the accuracy of the classifier as compared to pure data driven approach under the stochastic behaviour of EVSE. In addition, the control parameters having strong correlation with cyber-attack and physical faults are used in the training process, to effectively distinguish between cyber-attacks and physical faults. In this paper, section-2 explains the architecture of device-under-test along with impact of cyber-attacks and physical faults. Section-3 is comprised with the proposed machine learning model for detection and classification. Section-4 presents the simulation results to validate the proposed concept.

2. Integrated On-board EV Model Control Layer Description

Various topologies of Integrated on-board chargers (IOBCs) based on utilizing the EV propulsion system with both charging mode and traction mode operation are presented in (Metwly et al., 2020; Hoang et al., 2022). The cyber-physical system of 3-phase two level traction motor drive used as an IOBC in the proposed study is shown in Figure

1. The control layer for power converter is based on direct power control (DPC) integrated with model predictive control (MPC) via duty cycle optimization. As compared to conventional MPC with only one active vector, duty cycle optimization considers an active and zero vector to obtain better steady-state performance (Zhang et al., 2016). The power error minimization based objective function with duty cycle optimization is shown below,

$$objective(min.) = |(P_{k+1}^{ref} - P_{k+1})|^2 + |(Q_{k+1}^{ref} - Q_{k+1})|^2 \quad (1)$$
$$s.t: \quad P_{k+1} = P_k + t_s(\eta_{pn}D + \eta_{p0}(1-D))$$
$$Q_{k+1} = Q_k + t_s(\eta_{qn}D + \eta_{q0}(1-D))$$
$$0 \le D \le 1$$

where $P_{k+1}^{ref}, Q_{k+1}^{ref}, P_{k+1}$ and Q_{k+1} are reference and estimated values for real and reactive power, where Q_{k+1}^{ref} will always be zero. In additions, $\eta_{pn}, \eta_{qn}, \eta_{p0}$ and η_{q0} are the slopes of active and zero voltage vectors for active and reactive power, D is the duty cycle, and t_s is the sampling time (Zhang et al., 2016).

$$\eta_{pn} = \frac{3}{2L}[|e|^2 - Re(v^*.e)] - \frac{R}{L}P - \omega Q^{ext} \quad (2)$$
$$\eta_{qn} = \frac{3}{2L}Re[(e^* - v^*).e'] - \frac{R}{L}Q^{ext} - \omega P \quad (3)$$

The constrained optimization problem in equation (1) provides the MPC based predicted values of real and reactive power with optimized duty cycle for active and zero vector. In addition, active vector is selected based on the difference between predicted and reference values in each sector by using a conventional switching table (Zhang et al., 2016). Equation (2) and (3) provides the slopes of real and reactive power for each voltage vector. The current sensor is used to feedback the three phase line currents, which are converted in d-q frame of reference in control layer for easy computation. Furthermore, EMS is interlinked with a charging coordination algorithm to provide a reference value of active power. This P_{ref} does not remain constant during each charging session due to nonlinearities involved in the charging coordination based cooperative control. In addition, a ML multi-class classifier for disturbance detection is continuously monitoring the system state at each sampling period to detect the anomalies with a trigger circuit to turn off the power converter. Further, it is assumed that an attacker can hijack the in-vehicle communication network to modify the device level signals.

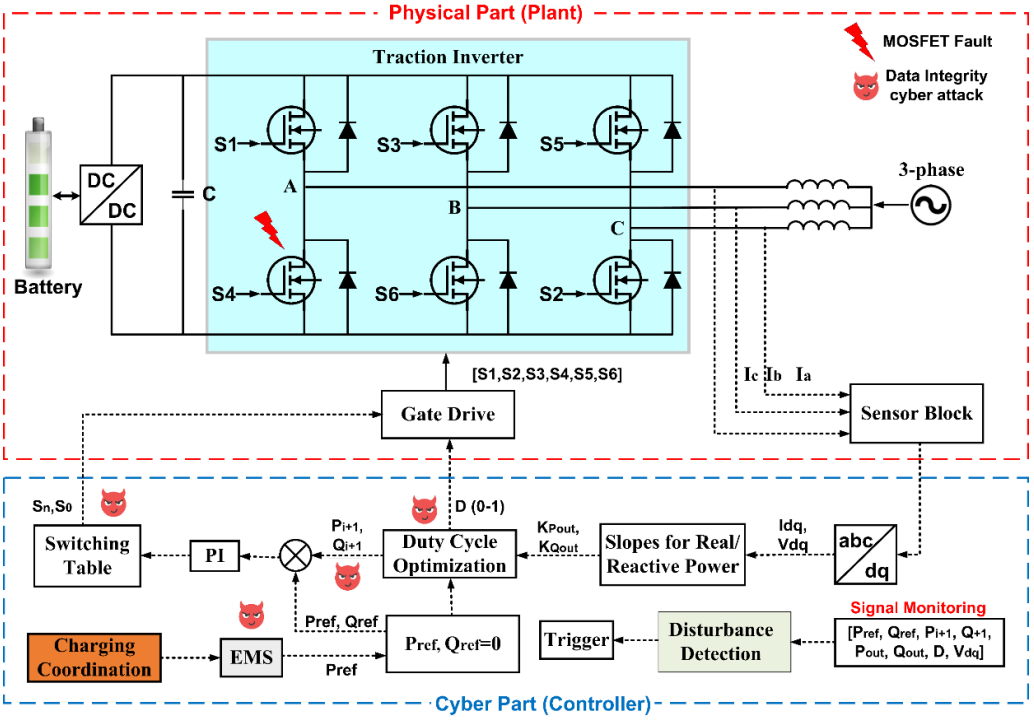


Fig. 1. Cyber-physical system of 3-phase two level motor drive as IOBC

2.1. Cyber and Physical Disturbance Modelling

To model a detection approach for cyber-attacks and physical disturbances, first it is important to understand the assumption of trusted signals.

2.1.1. Data Integrity Cyber Attacks

As shown in Figure 1, there are two types of incoming signals in the control layer: 1) sensor feedback; and 2) charging coordination reference signal. It is assumed that the in-vehicle input signals that are more exposed to the external communication network are more vulnerable towards cyber threats. Therefore, the control parameters feed-in by charging coordination and then EMS are assumed to be under cyber-attacks as shown in Figure 1. On the other hand, the sensor block has a standalone operation without any external interference, therefore the three phase current signalsI_a, I_b and, I_c are considered as trusted signals. In this proposed research, data integrity attacks are considered where the original data is tempered with falsify data or incorrect measurements. It is assumed that the attacker does not have any previous knowledge about the system, then the data integrity attacks can be modelled in terms of scaling as shown in equation (4).

$$\overline{Y} = \begin{cases} \delta.y(t), & if\ t \in [t_a,\ t_a + \tau] \\ y(t), & else \end{cases} \tag{4}$$

where, $\overline{Y}$ represent the modified signal after data integrity attack with t_a, and τ as attack start time, and attack duration, δ is the weighting factor to control the intensity of attack and $y(t)$ is the actual data. As shown in Figure 2, multiple data integrity based cyber-attacks are introduced in IOBC model presented in Figure 1. Due to false data injection for one variable of the system, the impact propagates to other control blocks as well. The weighting factor is assumed both positive and negative, which abruptly increase or decrease the value of real power but to decrease real power a large value of negative weighting factor was required. The propagated impact of positive weighting factor-based data integrity attacks compared negative weighting factor. So, MPC based DPC control approach is more resilient towards negative weighting factor-based data integrity attacks compare to positive ones.

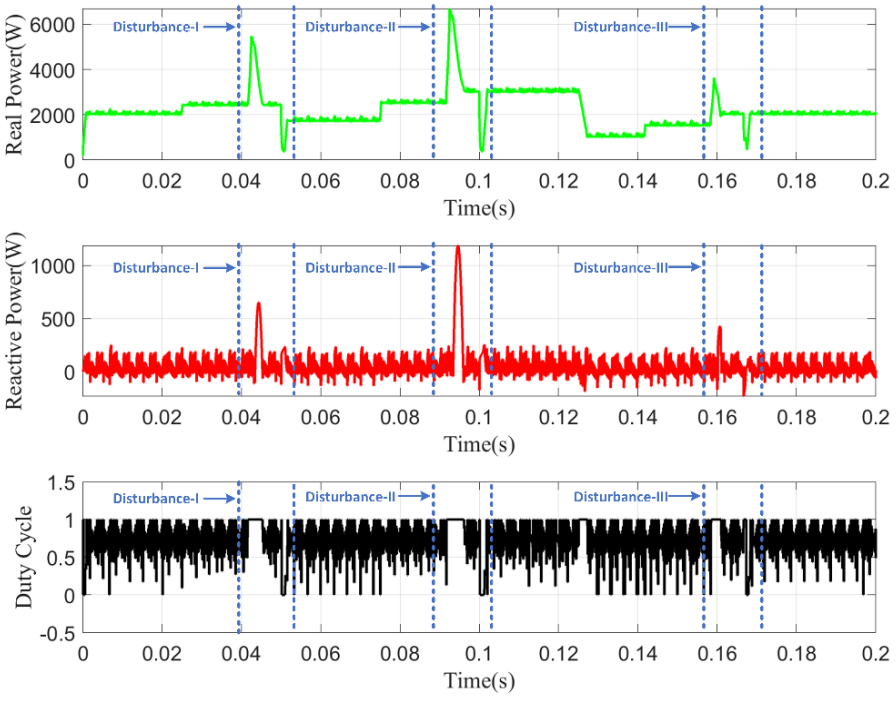
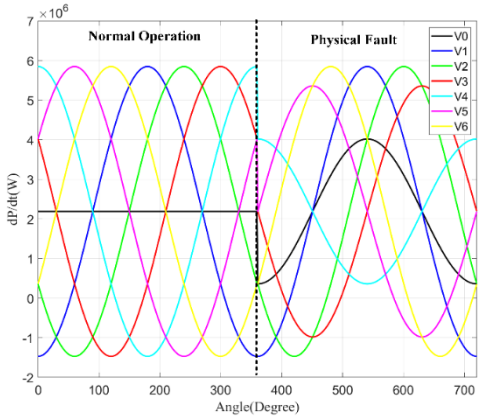


Fig. 2. Data integrity cyber-attacks impact on Real Power, Reactive Power, and Duty cycle

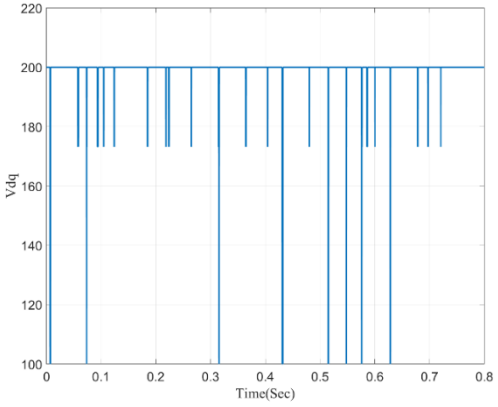
2.1.2. Physical Fault

Power transistors are the most vulnerable device in power electronics converters with physical faults such as short circuit fault and open circuit fault. During short circuit fault the switches are operated in saturation region with maximum drain to source current due to positive temperature coefficient and drain to source voltage equal to DC bus voltage. This leads to device failure and result in an open circuit fault. An FPGA based short circuit protection circuit is presented in (Ji et al., 2018), which can detect a short circuit fault in 1.5us. In this proposed work, only open circuit fault is considered as a physical fault for detection model. In this regard, an open circuit fault (OCF) is simulated for only one power switch of power converter. Figure 3 shows the impact OCF on the slopes of real power for six active voltage vectors and one null vector, by using equation (2) and equation (3). So, open circuit fault effects both the magnitude and phase of voltage vectors with highest impact on V4 and V0. In addition, random OCFs with a duration of ten sampling periods are simulated in IOBC during its normal operation. The OCFs effect on the output voltage of power converter in dq frame of reference can be seen in Figure 4. These results are used to extract the associated features of each type disturbances, which are further used to train the ML based disturbance detection model.



(a)

Fig. 3. Slopes of Real Power for various voltage vectors under normal operation and physical fault



(b)

Fig. 4. Absolute value of output phase voltage of power converter with random OCFs

3. MPC Based ML Model for Disturbance Detection

In this section, a ML based classifier is presented which utilizes the data of IOBC control layer for disturbance (cyber-attack; physical fault) detection, as shown in Figure 1. Due to the stochastic working conditions and nonlinearities involved in system dynamics, alone machine learning networks relying only on the raw data does not perform well in classification problems. Therefore, the proposed method involves the physics-based prepossessing of the raw data to enhance the correlation between features and target variable, hence improving the classifier accuracy. The device level signals used for the training of MPC based ML model is given below,

$$Input\ Features = [P_{ref}, Q_{ref}, P_{i+1}, Q_{i+1}, P_{out}, Q_{out}, V_{dq}, D] \tag{5}$$

where P_{ref}, P_{i+1}, P_{out} and Q_{ref}, Q_{i+1}, $Q_{out}$are the reference values, estimated values, and output values of real and reactive power; D is the duty cycle and V_{dq} is the power converter output phase voltage in dq frame of reference. Pearson correlation coefficient is used to determine the correlation between input and output variables. The input data features given in equation (5) are not directly fed to ML model because of low correlation with targeted labels. Instead, a residual parameter ($\widetilde{X_r}$) is calculated between the sensor measured values (X_{sensor}) and reference values (X_{ref}), which has a strong correlation with targeted labels. The residual can be calculated as given below,

$$\widetilde{X_r}(i) = \left|X_{sensor(i)} - X_{ref(i)}\right| \tag{6}$$

$$X_{sensor(i)} = [P_{out}, Q_{out}, P_{i+1}, Q_{i+1}] \tag{7}$$

$$X_{ref(i)} = [P_{ref}, Q_{ref}] \tag{8}$$

The values of input features are obtained by using power error minimization-based optimization problem given in equation (1). The predicted values of P, Q, and D obtained using basic assumptions can reflect the critical features of the system. In addition, the residuals remain within a specific limit during the normal operation of the system despite the varying values of P_{ref}, unless there is some abnormality. Note that the residual itself is not used to detect anomalies instead it is being used as an input to neural network. The refined data is applied to the long short-term memory (LSTM) based neural network shown in Figure 5. LSTM is an extended version of recurrent neural networks, which can effectively capture long term temporal patterns and dynamic features of the system as compared to conventional ML models. Based on the relationship established by LSTM between time series data sets, normal and abnormal operation can be distinguished. LSTM cells are further connected to a fully connected layer, a softmax layer to obtain a normalized probability distribution, and a classification layer with cross entropy error as a cost function for ground truth and predicted output.

$$C_{cross\ entropy} = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C_T} y_j^i . log\ (\hat{y}_j^i) \tag{9}$$

Where, N is the total number of training examples, C_T is the number of target classes, y_j is the ground truth, and $\hat{y}_j$ is the predicted output. The out labels used to detect normal operation, data-integrity attacks, physical faults are 0, 1, and 2. For the assumed LSTM model TensorFlow is used, and the hyper parameters are as follows, learning rate=0.001, batch size= 150, optimizer= Adam.

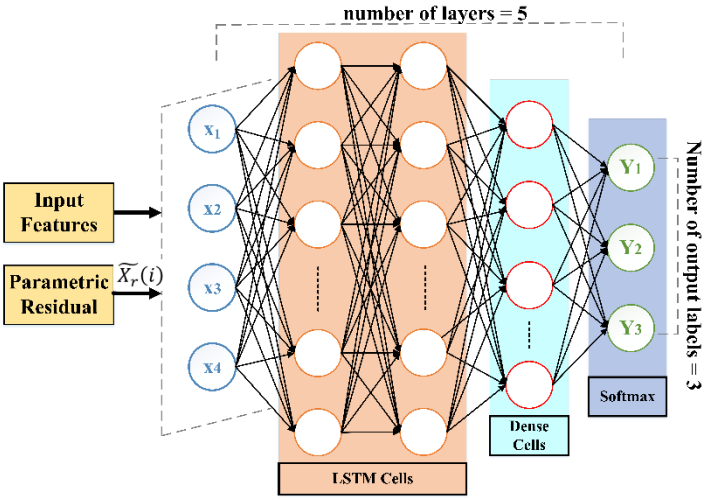


Fig. 5. MPC based ML model based on LSTM cells and fully connected layers.

4. Simulation Results and Performance Evaluation

In this section, the proposed MPC based ML model is integrated with the control layer power converter for disturbance detection, as shown in Figure 1. The optimization problem given in equation (1) is implemented by using Mosek ApS toolbox in MATLAB. The IOBC controller and power converter is simulated with a sampling rate of 83µs and 0.5µs respectively. The input features dataset in split into 80% training dataset and 20% testing dataset. To validate the effectiveness of the proposed classification approach, accuracy is calculated as given below,

$$Accuracy = \frac{T_{normal} + T_{attack} + T_{fault}}{T_{normal} + T_{attack} + T_{fault} + F_{normal} + F_{attack} + F_{fault}} \tag{10}$$

where, T_{normal}, T_{attack}, and T_{fault} represent the number of times when the normal condition, data-integrity attack and physical fault are identified correctly, respectively. Whereas F_{normal}, F_{attack}, and F_{fault} represent the number of times when the normal condition, data-integrity attack and physical fault are identified wrongly, respectively. To evaluate the performance of the proposed approach, both data-integrity attacks and physical faults are introduced randomly for a specific amount of time during normal operation. The cyber-attacks that reflect a pulsating effect are

considered for performance evaluation. In addition, OCF is only considered for low side MOSFET of phase-A in this case study. The OCF is simulated by assuming zero gate signal for all the time during this fault. By devising these disturbances randomly during simulation, the accuracy of the proposed classifier is validated for two different training datasets, such as $\widetilde{D}_1$ and, $\widetilde{D}_2$ as shown from Figure 6 to Figure 9. These datasets are obtained by randomly instigating the cyber-attacks and OCF in IOBC, as shown in Figure 2 and 4. In addition, after the disturbance is withdrawn, the system begins its normal operation due to the robustness and stability of feedback controller. In Figure 6 and Figure 8, rate of change of accuracy w.r.t epochs is shown, the proposed classifier has a better training accuracy compared to pure data-driven approach. In addition, the superior performance of the presented work is also validated via confusion matrix as well in Figure 7 and Figure 9 for both datasets. By training the LSTM model using a residual based dataset along with other input feature, the effect of fluctuations in P_{i+1}, Q_{i+1} and P_{out}, Q_{out} due to varying values of P_{ref} and Q_{ref}, reduced significantly by using residual values from MPC rather than measured values.

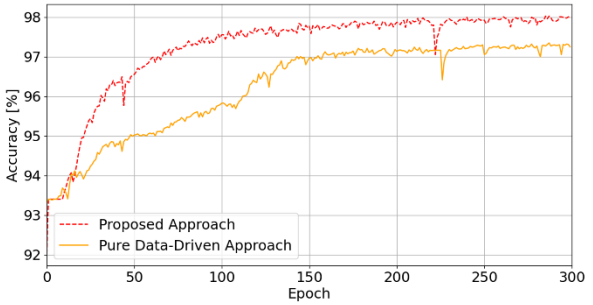


Fig. 6. Accuracy comparison plot for dataset $\widetilde{D}_1$

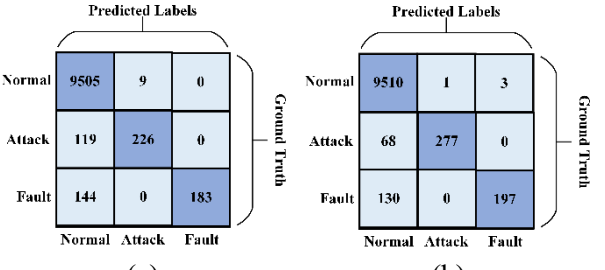


Fig. 7. Confusion Matrix for Figure 6. (a) Pure data-driven (b) Proposed approach.

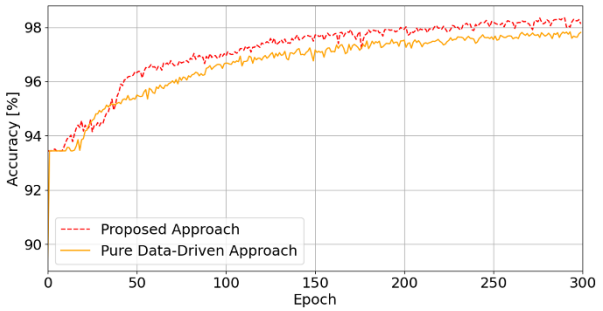


Fig. 8. Accuracy comparison plot for dataset $\widetilde{D}_2$

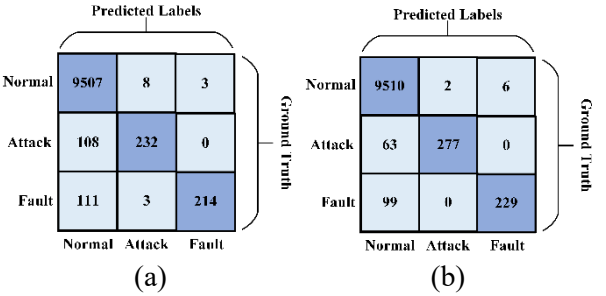


Fig. 9. Confusion Matrix for Figure 8. (a) Pure data-driven (b) Proposed approach.

5. Conclusion

In this article, an MPC-based ML approach is presented for disturbance detection in IOBCs under highly varying operating conditions due to charging coordination mechanism. The proposed work presents an LSTM based classifier with a training data pre-processing approach to enhance the detection accuracy. This proves that by improving the quality of trained data and its correlation with predicted class labels, same neural network-based classifier can perform better. As, these physics-based data features better reflect the system dynamics in response to cyber-attacks and OCF, therefore it results in improves accuracy of the classifier, which to the best of our knowledge has not been attempted before for IOBC applications. Hence, by adding more in-depth features of the physical system to train the ML based models, we can further enhance the capability of this proposed approach.

Acknowledgments

This work was supported by the Simulation Based Reliability and Safety Program for modeling and simulation of military ground vehicle systems, under the technical services contract No. W56HZV-17-C-0095 with the U.S. Army

DEVCOM Ground Vehicle Systems Center (GVSC). Distribution A. Approved for public release; distribution unlimited. (OPSEC 7474).

References

T. Jalakas, I. Roasto and D. Vinnikov, "Analysis of battery charger topologies for an electric vehicle," in *2012 13th Biennial Baltic Electronics Conference*, 2012.

L. Timilsina, P. R. Badr, P. H. Hoang, G. Ozkan, B. Papari and C. S. Edrington, "Battery Degradation in Electric and Hybrid Electric Vehicles: A Survey Study," in IEEE Access, vol. 11, pp. 42431-42462, 2023, doi: 10.1109/ACCESS.2023.3271287.

C. Shi, Y. Tang and A. Khaligh, "A single-phase integrated onboard battery charger using propulsion system for plug-in electric vehicles," IEEE Transactions on Vehicular Technology, vol. 66, p. 10899–10910, 2017.

P. H. Hoang, G. Ozkan, P. R. Badr, B. Papari, C. S. Edrington, M. A. Zehir, B. Hayes, L. Mehigan, D. A. Kez and A. M. Foley, "A Dual Distributed Optimal Energy Management Method for Distribution Grids With Electric Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 23, pp. 13666-13677, 2022.

Hoang, P. H., Ozkan, G., Badr, P. R., Timilsina, L., Papari, B., & Edrington, C. S. (2023). Integrating degradation forecasting into distribution grids' advanced distribution management systems. International Journal of Electrical Power & Energy Systems, 150, 109071.

A. Arsalan, J. Ahmad, M. Tahir and S. K. Mazumder, "Distributed Control and Power Management of Islanded DC Nanogrids with Applications to Rural Electrification," in 2020 IEEE Energy Conversion Congress and Exposition (ECCE), 2020.

C. Hodge, K. Hauck, S. Gupta and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," 2019.

E. Gumrukcu, A. Arsalan, G. Muriithi, C. Joglekar, A. Aboulebdeh, M. A. Zehir, B. Papari and A. Monti, "Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure," in 2022 4th Global Power, Energy and Communication Conference (GPECOM), 2022.

S. Tengler, "Top 25 auto cybersecurity hacks: Too many glass houses to be throwing stones," Forbes Business, 2020.

B. Yang, J. Ye and L. Guo, "Fast Detection for Cyber Threats in Electric Vehicle Traction Motor Drives," IEEE Transactions on Transportation Electrification, vol. 8, pp. 767-777, 2022.

L. Guo and J. Ye, "Cyber-Physical Security of Electric Vehicles With Four Motor Drives," IEEE Transactions on Power Electronics, vol. 36, pp. 4463-4477, 2021.

G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in 2020 IEEE Security and Privacy Workshops (SPW), 2020.

B. Yang, L. Guo, F. Li, J. Ye and W. Song, "Impact Analysis of Data Integrity Attacks on Power Electronics and Electric Drives," in 2019 IEEE Transportation Electrification Conference and Expo (ITEC), 2019.

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.

C. Kwon, W. Liu and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in 2013 American control conference, 2013.

G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in 2010 first IEEE international conference on smart grid communications, 2010.

J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," ACM Computing Surveys (CSUR), vol. 51, p. 1–36, 2018.

Y. Mo, R. Chabukswar and B. Sinopoli, "Detecting integrity attacks on SCADA systems," IEEE Transactions on Control Systems Technology, vol. 22, p. 1396–1407, 2013.

B. Yang and J. Ye, "Data-Driven Detection of Physical Faults and Cyber Attacks in Dual-Motor EV Powertrains," in 2022 IEEE Transportation Electrification Conference & Expo (ITEC), 2022.

M. Y. Metwly, M. S. Abdel-Majeed, A. S. Abdel-Khalik, R. A. Hamdy, M. S. Hamad and S. Ahmed, "A review of integrated on-board EV battery chargers: Advanced topologies, recent developments and optimal selection of FSCW slot/pole combination," Ieee Access, vol. 8, p. 85216–85242, 2020.

Hoang, P., Ozkan, G., Badr, P., Timilsina, L. et al., "A Prognostic Based Control Framework for Hybrid Electric Vehicles," SAE Technical Paper 2022-01-0352, 2022, https://doi.org/10.4271/2022-01-0352.

Y. Zhang, C. Qu and J. Gao, "Performance improvement of direct power control of PWM rectifier under unbalanced network," IEEE Transactions on Power Electronics, vol. 32, p. 2319–2328, 2016.

S. Ji, M. Laitinen, X. Huang, J. Sun, W. Giewont, F. Wang and L. M. Tolbert, "Short-circuit characterization and protection of 10-kV SiC MOSFET," IEEE Transactions on Power Electronics, vol. 34, p. 1755–1764, 2018.