Cyber-Physical GNN-Based Intrusion Detection in Smart Power Grids

Jacob Sweeten[§], Abdulrahman Takiddin[†], Muhammad Ismail[§], Shady S. Refaat[‡], and Rachad Atat[*]
[§]Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA
[†]Department of Electrical and Computer Engineering, Florida State University, Tallahassee, FL, USA
[‡]Department of Engineering and Technology, University of Hertfordshire, Hertfordshire, UK
[*]Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha, Qatar
Emails: jmsweeten42@tntech.edu, a.takiddin@fsu.edu, mismail@tntech.edu,
s.khalil3@herts.ac.uk, rachad.atat@qatar.tamu.edu

***Abstract*—The smart power grid is a critical infrastructure that has been targeted recently by several cyber-attacks. Hence, it is important that advancements are made in intrusion detection systems (IDSs). Recently, promising results have been reported using deep machine learning techniques to develop effective IDSs. However, the existing studies suffer from the following limitations: (a) The adoption of either only physical features (power system measurements) or only cyber features (network logs) in the development of IDSs; (b) The adoption of deep learning techniques that operate on 2D data, while power system measurements are graph-structure data. In this paper, we address these limitations and propose an effective IDS against false data injection and ransomware attacks. Our proposed IDS improves the attack detection performance by (a) fusing cyber-physical features collected from a practical testbed and (b) adopting a topology-aware model based on a graph neural network (GNN) to exploit the spatial and temporal correlation within the data. Our experimental results demonstrate the superior performance of our IDS compared with benchmarks that are based on topology-unaware models and use solely cyber or physical data.**

***Index Terms*—Intrusion detection systems, false data injection attacks, ransomware attacks, and graph neural networks.**

I. Introduction

The power grid is a critical infrastructure that provides energy to almost all vital systems including water and gas distribution systems, medical facilities, industry, defense facilities, etc. A failure in the power grid, even partially, may result in loss of life due to a lack of heat, loss of medical equipment functionality, loss of emergency response communication, etc. Therefore, it is crucial to defend the power grid from adversaries for the safety and security of our communities. As the power grid advances, more sensors and actuators are integrated, thus, making it a smart power grid. This advancement enhances the observability and controllability of the power grid. Hence, the modern power grid represents a cyber-physical system where the physical layer consists of the power grid generators, breakers, transmission lines, loads, etc., and the cyber layer consists of the Supervisory Control and Data Acquisition (SCADA) equipment, switches, routers, cables, etc. The cyber layer is usually indirectly connected to the Internet via firewalls and layered networks, thus, making it possible for an adversary from across the world to launch attacks on the smart power grid. Hence, this cyber-physical setup exposes the power grid to all of the vulnerabilities associated with being connected to a network.

Recently, several attacks have been reported on cyber-physical power systems. For example, in 2015, the Ukrainian power grid was attacked, which disabled power to more than $225,000$ customers [1] for up to 6 hours [2]. Other attacks were attempted against Ukraine in 2022, this time more aggressively utilizing wiper malware [3]. This serves as a real-world demonstration of how highly targeted the power grid is. Thus, it is necessary to advance intrusion detection systems (IDSs) in smart power grids to detect and recover from attacks.

A. Related Works

Several efforts have been made to develop IDSs in power systems. However, the existing works mostly consider features collected from one of the two layers of the cyber-physical system (either the cyber or the physical layer). Yet, some attacks are better captured through physical measurements (e.g., false data injection (FDI)), while other attacks are better captured through cyber features (e.g., ransomware). Hence, the existing detectors do not portray a complete picture of the cyber-physical system, and thus, offer a limited detection performance. Closely related works are discussed next.

1) Cyber-Only Detectors: Some of the existing IDSs in smart grids are trained only on cyber features collected from the network logs. For instance, Babu in [4] uses a Snort-based IDS with specific rules for DNP3-based attacks. Ustun et. al. in [5] adopt machine learning models to detect attacks that target the IEC 61850 GOOSE messages. Kwon et. al. in [6] propose an IDS for IEEE 1815.1-based power systems.

2) Physical-Only Detectors: The dominant majority of the existing research considers only features from the physical layer for intrusion detection. For instance, Upadhyay et. al. in [7] examine the effectiveness of using a majority vote ensemble algorithm on physical measurements using a dataset from Oak Ridge National Laboratory. Baul et. al. in [8] attempt to detect FDI attacks on the IEEE 14-bus test system using measurements from each bus with a long-short-term-memory (LSTM) recurrent neural network (RNN). Saber et. al. in [9] propose an IDS using an anomaly-based scheme (ABS) on physical measurements to detect false fault trips in circuit breakers. Mukherjee et. al. in [10] propose using a non-

This work was supported by NSF Award #2043324.

linear LSTM structure to detect FDI attacks on the IEEE 14-bus test system. Roy et. al. in [11] employ several machine learning models in a decentralized IDS to detect attacks on automatic generation control (AGC). Molzahn et. al. in [12] examine FDI attacks on the control station of a power grid. Efstathopoulos et. al. in [13] use physical data to perform intrusion detection on a single power plant. Prasad et. al. in [14] analyze power-line communication tapping attacks using physical measurement data from the power lines.

3) Other Notable Detectors: Siniosoglou et. al. in [15] developed an IDS and used it on either physical or cyber data. Hence, the detector is only used on one or the other, not both. Also, the data is only collected from one substation, similar to [16], rather than a power system with a number of substations. Ganesan et. al in [17] use physical data from a simulation of a small power system along with the KDD99 dataset. While this attempt uses both cyber and physical data, the physical dataset is not correlated with the attacks and the KDD99 dataset is not applicable to power systems.

B. Limitations and Challenges

The aforementioned works are limited in that almost all of them consider features from the cyber or the physical layer. This ignores the fact that the smart power grid is a cyber-physical system and inhibits the IDS's ability. Additionally, some papers only consider a small system such as one substation, but a utility company may have several power plants or substations under its control, and having more data on many of these nodes may also help detect attacks. Lastly, existing IDSs that adopt a data-driven approach rely on deep learning models that are best suited for 2D data. However, the power system is best described as a graph, and thus, the relevant cyber-physical dataset is best represented as graph-structured data. Adopting 2D topology-unaware models on graph-structured data limits the IDS's ability to exploit the spatial and temporal correlation within the data to improve detection performance.

To improve the detection performance, we aim to develop an IDS that fuses features from the cyber and physical layers and exploits spatio-temporal correlation within the data. However, this is challenged by the fact that there is currently no smart power grid dataset readily available that: (a) includes cyber and physical features reflecting the state of the power system under normal operation and attack conditions and (b) reflects both spatial and temporal aspects of the power system. Instead, there are generic industrial control system (ICS) datasets, generic network attack datasets, and simple datasets of FDI attacks on a single power substation (not a complete power system). In order to create a dataset with the aforementioned characteristics, a cyber-physical testbed mimicking the power system is required. This testbed is necessary to collect benign data, launch cyber-attacks and collect malicious data, and then use the benign and malicious dataset to train and test the desirable multi-modal cyber-physical IDS.

C. Contributions

To address the aforementioned challenges and develop effective IDS, the following contributions have been made:

- We developed a cyber-physical power system testbed where OPAL-RT and RT-Lab were used to emulate the physical layer of the power grid and the cyber range was used to emulate the cyber layer of the power grid based on the Modbus/TCP protocol and a set of routers and firewalls. The developed cyber-physical testbed is based on the IEEE 14-bus test system.
- We created a comprehensive multi-modal dataset that covers the normal operation of the power grid and the operation of the power grid under cyber-attacks that include FDI and state-of-the-art ransomware attacks.
- We developed a topology-aware graph neural network (GNN)-based multi-modal IDS that fuses cyber-physical features. The proposed IDS is compared with a set of benchmarks that include deep 2D machine learning models, namely, feedforward neural network (FNN), RNN, and auto-encoder with attention (AEA).

Our experimental results show the superior performance of the GNN-based IDS compared with the benchmarks ($5-13\%$ improvement in detection rate (DR) and $6-13\%$ reduction in false alarms (FA)). Also, our results demonstrate that multi-modal cyber-physical fusion can improve detection performance (5% improvement in DR and 5% reduction in FA).

The remainder of this paper is as follows: The testbed used for data collection along with the benign and attack data collection process are described in Section II. The proposed multi-modal GNN-based IDS is discussed in Section III. Experimental results are presented in Section IV. Finally, conclusions are given in Section V.

II. Cyber-Physical Power System Testbed

The testbed consists of two layers, physical and cyber layers. The physical layer is based on real-time simulation on OPAL-RT [18]. The cyber layer consists of several Docker containers that host the software for the SCADA system (programmable logic controllers (PLCs) and human-machine interfaces (HMIs)), routers, firewalls, etc. The two layers are interfaced together via a transmission control protocol (TCP) connection and an interface network to which all PLCs are connected. An overview of the data flow in the testbed is shown in Fig. 1. The human operator sends control signals to the PLCs through the HMIs. The PLCs communicate with the cyber interface which sends signals to the physical interface, and this will have some effect on the simulation of the physical layer. Physical data is sent from the simulation environment to the cyber interface which is sent back to the PLCs. A relay is responsible for querying the PLC via Modbus/TCP and reporting the measurements to ElasticSearch.

A. Physical Layer

The physical layer of the testbed is based on the IEEE 14-bus test system modeled in MATLAB Simulink. The Simulink model is created according to the OPAL-RT specifications defined in [19] and compiled using the RT-Lab software which then sends the compiled simulation executable to the OPAL-RT. After compiling the model and loading it onto the OPAL-RT, RT-Lab is used for starting, stopping, and monitoring the

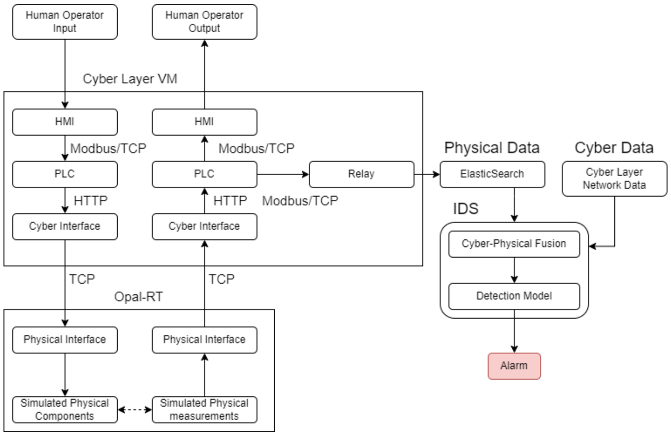

Fig. 1: Illustration of the data flow in the testbed.

simulation. A 6-month load profile is applied to the IEEE 14-bus test system to mimic practical consumption patterns throughout days and seasons. The load profile is created as per the following MATLAB function

$$L_{\text{bus}}(t) = L_{\text{base}} \times \mathcal{N}(1 + K[t] \times 0.07, 0.01), \qquad (1)$$

where $L_{\text{bus}}(t)$ denote the load value at a given bus (i.e., the value of active P and reactive Q power values) and timestamp t, L_{base} is the base load values (P and Q) according to the IEEE data [20], and $\mathcal{N}$ represents a normal random variable with a mean of $L_{\text{base}} \times \mathcal{N}(1 + K[t] \times 0.07)$ and a standard deviation of 0.01, and K is an array containing the 6-month load profile values. The load profile is scaled to 15 minutes. Lastly, a physical interface is built into the model to create a TCP server for exchanging data with the cyber layer.

B. Cyber Layer

The cyber layer is composed of Docker containers connected by Docker networks. First, we discuss setting up the Docker network. Most real-world communication networks are observed to exhibit a scale-free property [21], where only a few nodes (routers) have a degree and a betweenness score much larger than the rest of the nodes [22]. Hence, we generated a synthetic scale-free communication network with the average degree following the power-law distribution [23]: $\tilde{\kappa} \sim k^{-\delta}, (2 \leq \delta \leq 2.6)$, where k is the node degree and δ is an exponent. The MATLAB code provided by [24] is used to generate a random scale-free network with an average degree $\tilde{\kappa} = 7$ and an exponent $\delta_{\text{exp}} = 2.2$. The routers are connected via links, and each router is connected to the local network of a given substation (bus/node in the physical layer). The routers establish their routes using the OSPF protocol, and there is a central node from which the HMIs are accessed and an external Internet connection is provided. In order to select a control center from the nodes in the cyber layer, we adopt the highest degree node approach [22]. It should be noted that other methods of selecting control centers exist in literature such as selecting the node with the highest betweenness centrality [25] and the geometric median of all nodes [26]. However, since the communication network has scale-free characteristics, we assume, similar to [22], that the control center is the node with the highest degree.

The substation local network is composed of a few containers. One container is the HMI which is port-forwarded to by the router using IP tables. For each bus that the cyber node controls, there is one PLC and one relay. The HMI and the relays both collect measurements from the PLCs. The HMI can send circuit breaker control signals to the PLC as well. The relay polls the PLC and sends the data through the central cyber node (control center) to an ElasticSearch database.

C. Cyber-Physical Coupling

Each power node (bus) is coupled with a communication node (router). Hence, the number of routers in the synthetic communication network is made equal to the number of buses in the IEEE test system. To couple the cyber and physical nodes, we use the Random Positive Degree Correlation Coupling (RPDCC) scheme presented in [27], which is shown to mimic the coupling of real-world interdependent systems [28]. In RPDCC, power nodes of high degrees tend to couple with communication nodes of high degrees, and so do nodes with low degrees. For each of the power and communication graphs (i.e., physical and cyber layers), we obtain a weighted random permutation set of the vertices (using the MATLAB function provided by [29]), where the weights are the corresponding degrees. Then, the two weighted sets are coupled together.

A single interface Docker container is attached to both the host bridge network (for accessing the OPAL-RT) and a Docker network called INTERFACE. The interface software acts as both a client to the OPAL-RT's TCP server and a server to the PLCs. The PLCs send an HTTP request to the interface container and it replies with the data from the real-time simulation that applies to that PLC. When the PLCs receive a control signal, they send it to the interface container which creates a packet and sends the command to the OPAL-RT's TCP server. An illustration of the cyber and physical interfaces is shown in Fig. 2.

D. Benign Data Collection and Imputation

The physical data were collected through ElasticSearch and the cyber data was collected from the Docker host with tcpdump. For both, data was collected every 15 minute. First, the cyber data that was collected was encoded in PCAP files, which are raw network traffic dumps. Then, the program TShark, included with the WireShark installation, was used to export the PCAP files to CSV files. This generated one CSV file for each cyber node in the system. The physical data collected from ElasticSearch was exported as one CSV file. As the rates of cyber and physical data are not the same within each data collection period, a data imputation step is carried out where the measurements were duplicated between timestamps such that for every row in the cyber data, there is a physical row to match. A similar approach was used in [16] where null packets were inserted into the cyber dataset in order to match the number of rows in the physical data.

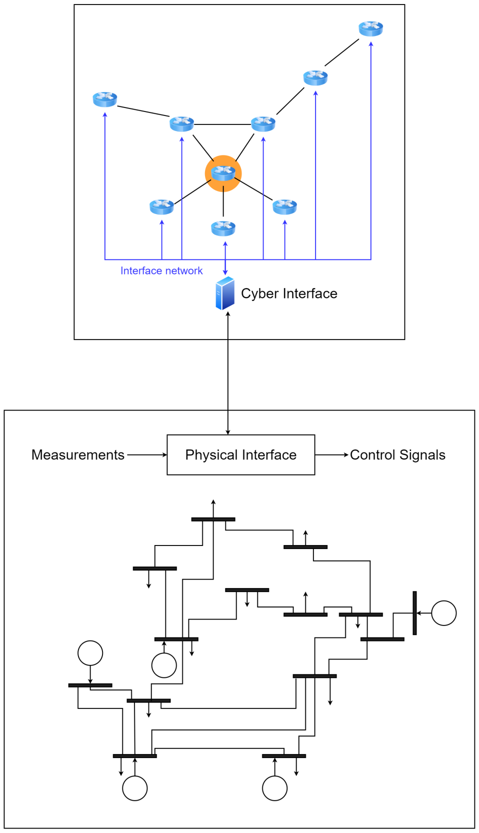

Fig. 2: Illustration of IEEE 14-bus Cyber (top) and Physical (bottom) Layers Connected.

TABLE I: Multi-modal features collected from both cyber and physical layers.

Cyber	Physical
Source MAC Address	Phase 1 RMS Voltage (V)
Destination MAC Address	Phase 2 RMS Voltage (V)
Source IP Address	Phase 3 RMS Voltage (V)
Destination IP Address	Phase 1 RMS Current (A)
Packet Size (Bytes)	Phase 2 RMS Current (A)
Packet Protocol	Phase 3 RMS Current (A)
Source TCP Port	Frequency (Hz)
Destination TCP Port	Phase Angle (Degrees)
Source UDP Port	Active Power (W)
Destination UDP Port	Reactive Power (VAR)

Table I summarizes the multi-modal features collected from the cyber and physical layers.

E. Attack Data

The attacks assume a compromised control center desktop from which attacks are launched. Two attacks were performed on the testbed to collect the malicious dataset:

- False Data Injection (FDI): The attack was launched by performing an ARP spoof such that all the Modbus/TCP traffic is redirected to a dummy PLC that holds the last valid data from the real PLC. A signal is then sent to the real PLC to turn off the circuit breaker. The dummy PLC reports the last valid measurements via Modbus/TCP as if it were the real PLC. This attack was considered as it is a common attack on SCADA systems, and it mostly manifests on the physical layer. This attack utilizes IP spoofing as a means of impersonating the real PLC.
- Ransomware (RW): ICS ransomware is on the rise [30], and so this attack cannot be ignored. In this attack, a user logged into the PLC retrieved a file from the Internet that contained the ransomware to simulate a malicious download. The ransomware was then run. It conducted an ICMP scan of the local network, sent some data to the command and control server, and disabled Modbus/TCP communications in order to simulate a lockdown. There was no change to the breaker state, so this attack is better manifested on the cyber layer. In a real ransomware attack, the ransomware would have some impact on the physical layer after some amount of time if the operators failed to pay the ransom [31].

III. Cyber-Physical GNN-based IDS

Cyber-physical power systems can be modeled as connected, undirected, weighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{W})$ where $\mathcal{V}$ denotes the set of heterogeneous physical (power substations) and cyber (router) nodes, $\mathcal{E}$ represents set of intra-edges within each layer and inter-edges connecting the two-layers, and $\mathbf{W}$ is the weighted adjacency matrix. The intra-edges represent the transmission lines connecting the power substation nodes in the physical layer. In the cyber layer, these represent the communication links connecting the routers. Finally, the inter-edges are based on the coupling between the physical and cyber nodes. For the inter-edges in the physical layer, the corresponding weight values $\mathbf{W}_\mathrm{p}$ are based on the line admittance value for the connected nodes. If they are not connected, then, the corresponding weight value equals zero. For the inter-edges in the cyber layer and the intra-edges, the corresponding weight values $\mathbf{W}_\mathrm{c}$ and $\mathbf{W}_\mathrm{cp}$, respectively, are binary values based on the adjacency matrix.

To develop the IDS, we adopt the graph convolutional neural network (GCNN) model. This represents a supervised model that is trained and tested on benign and malicious data. The input features are based on the collected multi-modal cyber-physical features shown in Table I and the labels are binary values indicating whether or not this sample represents the system operation under normal or attack conditions. All input features are fed to the model as raw numerical inputs except for the cyber feature representing the protocol type where we first apply one hot encoding before passing it to the model.

The adopted GCNN model, shown in Fig. 3, exhibits a deep structure that uses multiple stacked Chebyshev graph convolution layers that capture the graphs' spatial features through the graph convolution operation [32]. The Chebyshev graph convolution layers are followed by a dense layer to estimate the attack probability of a given sample. The decision is then provided to the output layer, accordingly. Hyper-parameter optimization is carried out to specify the number of graph convolution layers, the number of units/layer, the

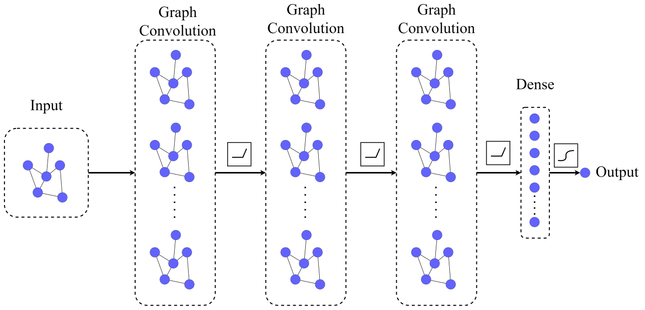

Fig. 3: Illustration of the layers used in a GCNN. Several GNN layers are applied to the input graph before a dense layer is finally applied. A final activation function with an output between 1 and 0 is used to set the output.

dropout rate, the order of neighborhood, the optimizer, and the activation function.

IV. Experimental Results

A. Benchmark IDS Models

We compare the GNN-based IDS with deep supervised and unsupervised benchmark models. Deep models are based on neural networks and involve multiple stacked hidden layers. The considered supervised models are FNN and RNN, while the considered unsupervised model is AEA. Unlike supervised models, the unsupervised model does not use labeled data for training. Instead, it attempts to find patterns in the data and make predictions based on those patterns. Then, the IDS finds deviations from the predicted pattern which indicates an attack.

B. Hyper-parameter Optimization Results

For all the listed hyper-parameters, we adopted a sequential grid search method to find their optimal values [33]. Table II details the optimal hyper-parameters for each detection model.

C. Performance Metrics

Two metrics have been considered, namely detection rate (DR) and false alarm (FA). The detection rate (DR = TP/(TP + FN)) specifies the portion of correctly detected malicious samples. False alarm rate (FA=FP/(FP + TN)) determines the portion of benign samples incorrectly marked as malicious. TP (true positive) denotes the correctly identified malicious samples and TN (true negative) represents the correctly identified benign samples. Also, FP (false positive) are the incorrectly identified benign samples and FN (false negative) are the incorrectly identified malicious samples.

D. Performance Results

We trained and tested three types of models, namely, cyber-only (C), physical-only (P), and cyber-physical (CP). The cyber-only models are trained and tested using features collected only from the cyber layer. The physical-only models are trained and tested using features collected only from the physical measurements. The cyber-physical models are trained and tested using features collected from the cyber and physical layers. This is carried out to quantify the improvement in detection when cyber-physical fusion is adopted.

The following observations can be made based on the summarized results in Table III:

- GNN-based IDSs offer the best detection performance in terms of DR and FA. This is because the power system data is best represented as graph-structured data and GNN models capture the spatial relationships among the features, and hence, yield the best detection results. As shown in Table III, the GNN-based IDS offers consistent performance improvements in DR and FA compared to all benchmark models.
- The ransomware attack is best detected based on the cyber features compared with the physical features. On the other hand, an FDI attack is best detected using physical features compared with cyber features. Overall, cyber-physical fusion yields consistent improvement in DR and FA for both attacks.

TABLE II: Optimal hyper-parameters for each model.

Model	Hyper-parameter	Optimal Value
FNN	Number of Layers	5
	Number of Neurons	32
	Dropout Rate	0.2
	Optimizer	Adam
	Activation Function	ReLU
RNN	Number of Layers	3
	Number of Units	32
	Dropout Rate	0
	Optimizer	SGD
	Activation Function	ReLU
AEA	Number of Layers	6
	Number of Units	32
	Dropout Rate	0.2
	Optimizer	SGD
	Activation Function	Sigmoid
GNN	Number of Layers	5
	Number of Units	16
	Neighborhood Order	4
	Optimizer	RMSProp
	Activation Function	ReLU

TABLE III: Performance of each detection model.

Attack	Model	Metric	P	C	CP
RW	FNN	DR	75.8	78.1	80.3
		FA	25.2	22.1	21.0
	RNN	DR	79.2	81.6	83.9
		FA	19.7	17.5	15.1
	AEA	DR	85.3	86.4	88.3
		FA	16.5	15.8	13.5
	GNN	DR	88.7	90.4	92.1
		FA	10.3	8.3	7.5
FDI	FF	DR	86.2	81.3	88.3
		FA	15.2	17.5	13.5
	RNN	DR	89.8	85.7	92.3
		FA	14.6	15.3	12.4
	AEA	DR	90.7	87.2	94.9
		FA	12.3	13.1	11.9
	GNN	DR	93.4	90.1	97.8
		FA	7.2	8.2	6.1

V. Conclusions

In this paper, a cyber-physical IEEE 14-bus power system testbed was developed on which attacks were launched and multi-modal data was collected. The collected multi-modal cyber-physical features consist of benign data and cyber-attack data that includes FDI and ransomware. A cyber-physical GNN-based IDS was developed and compared with a set of deep learning-based benchmark detectors. Our experimental results show the superior performance of the GNN-based IDS compared with the benchmarks. Specifically, our results demonstrated a $5-13\%$ improvement in DR and $6-13\%$ reduction in FA. Also, our results demonstrated that multi-modal cyber-physical fusion can improve detection performance with up to 5% increase in DR and 5% reduction in FA. The results presented herein pave the way toward developing effective IDS in cyber-physical power systems.

References

[1] (2021) Cyber-attack against Ukrainian critical infrastructure. Online; Retrieved 20-March-2023. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[2] (2015) Compromise of a power grid in eastern Ukraine. Online; Retrieved 20-March-2023. [Online]. Available: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

[3] J. Pearson. (2022) Ukraine says it thwarted Russian cyberattack on electricity grid. Online; Retrieved 20-March-2023. [Online]. Available: https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/

[4] J. R. Babu, "Design, implementation, and field-testing of distributed intrusion detection system for smart grid SCADA network." M.S. thesis, Iowa State University, 2021. [Online]. Available: https://doi.org/10.31274/etd-20210609-154

[5] T. S. Ustun, S. M. S. Hussain, A. Ulutas, A. Onen, M. M. Roomi, and D. Mashima, "Machine learning-based intrusion detection for achieving cybersecurity in smart grids using iec 61850 goose messages," *Symmetry*, vol. 13, no. 5, 2021. [Online]. Available: https://www.mdpi.com/2073-8994/13/5/826

[6] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," *IEEE Access*, vol. 8, pp. 77 572–77 586, 2020.

[7] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Intrusion detection in SCADA based power grids: Recursive feature elimination model with majority vote ensemble algorithm," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2559–2574, 2021.

[8] A. Baul, G. C. Sarker, P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "XTM: A novel transformer and LSTM-based model for detection and localization of formally verified fdi attack in smart grid," *Electronics*, vol. 12, no. 4, p. 797, 2023. [Online]. Available: https://www.proquest.com/scholarly-journals/xtm-novel-transformer-lstm-based-model-detection/docview/2779476556/se-2

[9] M. A. H. Sadi, D. Zhao, T. Hong, and M. H. Ali, "Time sequence machine learning-based data intrusion detection for smart voltage source converter-enabled power grid," *IEEE Systems Journal*, pp. 1–12, 2022.

[10] D. Mukherjee, S. Chakraborty, A. Y. Abdelaziz, and A. El-Shahat, "Deep learning-based identification of false data injection attacks on modern smart grids," *Energy Reports*, vol. 8, pp. 919–930, 2022, 2022 The 5th International Conference on Renewable Energy and Environment Engineering. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484722022065

[11] S. D. Roy, S. Debbarma, and A. Iqbal, "A decentralized intrusion detection system for security of generation control," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18 924–18 933, 2022.

[12] D. K. Molzahn and J. Wang, "Detection and characterization of intrusions to network parameter data in electric power systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3919–3928, 2019.

[13] G. Efstathopoulos, P. R. Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. K. Angelopoulos, and S. K. Athanasopoulos, "Operational data based intrusion detection system for smart grid," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[14] G. Prasad, Y. Huo, L. Lampe, and V. C. M. Leung, "Machine learning based physical-layer intrusion detection and location for the smart grid," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–6.

[15] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137–1151, 2021.

[16] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119 118–119 138, 2021.

[17] S. A. E. X. P. Ganesan, "An intelligent intrusion detection system in smart grid using PRNN classifier," *Intelligent Automation & Soft Computing*, vol. 35, no. 3, pp. 2979–2996, 2023. [Online]. Available: http://www.techscience.com/iasc/v35n3/49378

[18] Opal-rt. Online. Retreived 20-March-2023. [Online]. Available: https://www.opal-rt.com/

[19] Building models. Online. Retrieved 20-March-2023. [Online]. Available: https://opal-rt.atlassian.net/wiki/spaces/PRD/pages/144148947/Building+Models

[20] R. Christie. Power systems test case archive. Online; Retrieved 20-March-2023. [Online]. Available: http://labs.ece.uw.edu/pstca/

[21] S. Bornholdt and H. G. Schuster, *Handbook of Graphs and Networks: From the Genome to the Internet*. USA: John Wiley & Sons, Inc., 2003.

[22] Y. Cai *et al.*, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, 1 2016.

[23] M. Xiang and Q. Qu, "A congestion control strategy for power scale-free communication network," *Applied Sci.*, vol. 7, no. 10, p. 1054, 2017.

[24] D. Fasino, A. Tonetto, and F. Tudisco, "Generating large scale-free networks with the chung–lu random graph model," *Networks*, 12 2020.

[25] M. Korkali, J. G. Veneman, B. F. Tivnan, J. P. Bagrow, and P. D. H. Hines, "Reducing cascading failure risk by increasing infrastructure network interdependence," *Scientific Reports*, vol. 7, 3 2017.

[26] Y. K. Tamandani, M. U. Bokhari, and M. Z. Kord, "Computing geometric median to locate the sink node with the aim of extending the lifetime of wireless sensor networks," *Egyptian Inform. J.*, vol. 18, no. 1, pp. 21 – 27, 2017.

[27] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

[28] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, "Inter-similarity between coupled networks," *EPL (Europhysics Letters)*, vol. 92, p. 68002, 01 2011.

[29] A. Gripton. (2012, 3) Random weighted selection. [Online; Retrieved 11-Jul-2021]. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/35790-random-weighted-selection

[30] A. Culafi. (2023) Dragos: ICS/OT ransomware attacks up 87%. Online; Retrieved 20-March-2023. [Online]. Available: https://www.techtarget.com/searchsecurity/news/365531080/Dragos-ICS-OT-ransomware-attacks-up-87

[31] (2017) New proof-of-concept ransomware can target plcs at industrial sites. Online; Retrieved 20-March-2023. [Online]. Available: https://www.tripwire.com/state-of-security/new-proof-concept-ransomware-can-target-plcs-industrial-sites

[32] J. Zhou *et al.*, "Sparsity-induced graph convolutional network for semisupervised learning," *IEEE Trans. on Artificial Intelligence*, vol. 2, no. 6, pp. 549–563, 12 2021.

[33] A. Takiddin, M. Ismail, M. Nabil, M. M. E. A. Mahmoud, and E. Serpedin, "Detecting electricity theft cyber-attacks in ami networks using deep vector embeddings," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4189–4198, 2021.