Multi-Task Graph-Based Attack Detection and Localization in Cyber-Physical Power Systems

Hayden Keller*, Salma Aboelmagd†, Shady S. Refaat‡, Abdulrahman Takiddin†, Muhammad Ismail*, and Erchin Serpedin§

*Department of Computer Science, Tennessee Tech University, Cookeville, TN, USA
†Department of Electrical and Computer Engineering, Florida State University, Tallahassee, FL, USA
‡Department of Engineering and Technology, University of Hertfordshire, Hertford, UK
§Electrical & Computer Engineering Department, Texas A&M University, College Station, TX, USA

***Abstract*—Securing critical infrastructure, such as power grids, against cyber threats is essential for national security. As power grids become increasingly interconnected and reliant on advanced technologies, the risk of cyber incidents rises significantly. While existing research offers advanced cyber threat detection methods, precise attack detection and localization remain crucial. Recent developments in graph convolutional neural networks (GCNNs) show promise for detecting and localizing attacks. Existing approaches typically rely solely on either physical data (e.g., power measurements) or cyber data (e.g., network traffic) and detect only a single attack type, failing to capture diverse real-world scenarios. In this work, we generate a comprehensive dataset containing both benign and malicious data—from single-node attacks to complex simultaneous multi-node attacks—using a cyber-physical testbed. We propose a multi-task GCNN model that integrates cyber-physical features for attack detection and localization. We test the model against various attack types, including simultaneous ransomware and false data injection attacks at different locations. Our experimental results demonstrate that leveraging the fusion of cyber and physical features using our multi-task GCNN model yields detection rate enhancements of $15-18\%$ and $10-14\%$ for attack detection and localization, respectively, compared to benchmark models, highlighting the robustness of our approach.**

***Index Terms*—Cyber-physical fusion, false data injection, graph neural network, multi-task learning, and ransomware.**

I. Introduction

The power grid serves as a cornerstone of global infrastructure, underpinning critical services [1]. Recently, deliberate cyber attacks targeting critical infrastructure, particularly power grids, have increased in the United States [2], becoming more sophisticated, pervasive, and costly, and underlining the need for robust cyber defense strategies to protect public welfare. In Ukraine, cyber attacks on the power grid occurred in both 2015 and 2022. In 2015, the Ukrainian grid suffered blackouts affecting more than 225,000 people as a result of a Russian cyber campaign [3]. In 2022, another Russian attack targeted Ukraine's power grid, causing localized outages [3]. Similar incidents have been reported in Texas, Hawaii, and India [4], [5], where power utilities were victims of malicious actors. Through these recent events, it has been made apparent that the need exists for improvement in the realm of cyber defense, intrusion detection, and localization for critical infrastructure.

This work was supported by the NSF CyberCorps SFS grant #2043324.

A. Related Works

Existing research on intrusion detection systems (IDSs) for power systems focuses on either cyber or physical data, overlooking the benefits of integrating both layers. Attack detection or localization techniques were proposed using only cyber or only physical features, as reviewed next.

A snort-based IDS against smart grid communications protocol attacks was proposed [6], but such a system relies solely on cyber data and does not employ machine learning techniques. A co-simulated model using synthetic cyber data was introduced in [7], but it excludes physical measurements, limiting its effectiveness in detecting cyber-physical interactions. A multi-task approach for detection and localization was proposed [8], but focuses only on physical measurements and false data injection (FDI) attacks. Similarly, a joint detection and localization model was presented [9], but it is based exclusively on physical data and does not adopt a multi-task architecture. A model trained on physical features was proposed [10], but it lacks real-time testing capabilities. A recurrent long short-term memory-based (LSTM) model for detection and localization was introduced [11], but it does not address diverse attack types. Another detection model, using an expectation maximization algorithm, for FDI attacks was proposed [12], but it only generates physical data in MATLAB rather than real-time testbeds. A semi-supervised approach for detecting FDI attacks was presented [13], but it relies on algorithmically generated physical measurements. Time synchronization attacks were investigated [14], but the study focuses exclusively on physical data. A graph-based detection and localization framework for FDI attacks was proposed [15], but the physical data was derived from power flow calculations, which simulate steady states rather than dynamically generating data through a real-time testbed.

The aforementioned works are limited by their reliance on simulations, single-node attacks, and the absence of cyber-physical fused data, failing to reflect real-world attack scenarios, including simultaneous multi-node attacks, which introduces the need for a more robust multi-task IDS that considers the cyber-physical nature of power grids.

B. Contributions

To address the limitations of existing IDSs, we carry out the following contributions:

- We generate a comprehensive dataset with benign and malicious samples, with attacks on single-node, complex multi-node, and multi-attack cases. The data generation is based on a real-time cyber-physical testbed. The physical layer is simulated using Opal-RT based on the IEEE 14-bus system with a load profile to simulate realistic power fluctuation over time. The cyber layer presents Docker containers acting as relays and routers.
- We develop a multi-task graph convolutional neural network (GCNN) for simultaneous detection and localization of attacks by leveraging fused cyber-physical features to capture spatial and temporal relationships in the power system, boosting the detection performance compared to models relying on only temporal or spatial features.
- We evaluate our multi-task GCNN on fused cyber-physical data against simultaneous FDI and ransomware attacks, achieving detection rate (DR) enhancements of $15-18\%$ and $10-14\%$ for attack detection and localization, respectively, compared to benchmarks.

This paper is outlined as follows. Section II describes the cyber-physical testbed, attack scenarios, and data collection. Section III presents the proposed multi-task GCNN model architecture. Section IV presents the experimental results. Section V concludes the paper.

II. Cyber-Physical Testbed Development

Our testbed comprises a physical layer and a cyber layer. The physical layer—simulated on an Opal-RT using RT-Lab—includes generators, loads, and programmable logic controllers (PLCs), while the cyber layer consists of Docker containers acting as relays, routers, and interfaces between the PLCs and the network. Power measurements collected via Modbus Transmission Control Protocol (TCP) are sent to ElasticSearch [16]. The testbed data flow is shown in Fig. 1.

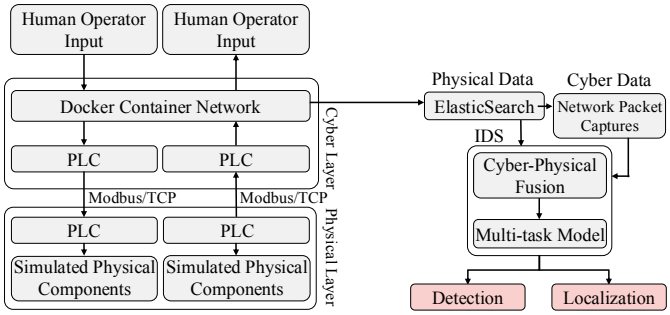

Fig. 1. Data flow through the testbed.

A. Physical Layer

Based on the IEEE 14-bus test system, the physical layer is implemented via a MATLAB Simulink model running on an Opal-RT 4610XG hardware accelerator. RT-Lab compiles and deploys the simulation, which uses a 20-minute load profile to simulate realistic power fluctuations. The load profile adjusts default power values by a factor, resulting in deviations of 1–2 MW per timestep. Our Opal-RT supports Modbus TCP, allowing relays to query bus measurements every 5 seconds.

B. Cyber Layer

The cyber layer comprises 10 cyber nodes managing 14 PLC containers, each with a unique IP address. These containers simulate devices, such as PLCs, relays, and routers, within substations, ensuring that traffic appears to originate from individual PLCs rather than the Opal-RT.

C. Cyber-Physical Interface

Building on our previous design [17], the upgraded interface enables relays to connect directly to PLCs on the Opal-RT. Instead of establishing a new connection for each query, each relay maintains a single persistent Modbus TCP connection to its assigned PLC, reducing load and preventing system crashes. Fig. 2 illustrates the revised cyber-physical interface.

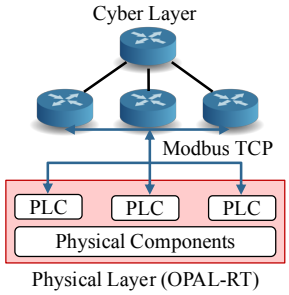

Fig. 2. Abstraction of cyber-physical interface.

D. Cyber Attack Types

We perform three attack types: FDI and ransomware, as well as a simultaneous combination of FDI and ransomware. An attacker container is added to the target substation's local network to enable the IP spoofing needed for FDI, while the ransomware attack assumes that the malicious file is already present on the target device. We launch the three attack types described next using two cases, against a single node and multiple nodes at the same time.

- FDI: This multi-stage attack uses address resolution protocol spoofing to reroute traffic from a target PLC to a "dummy" PLC, which mimics valid data. A command injection then disables the circuit breaker, disrupting power. Exploiting Modbus TCP's weakness, this attack deceives the control systems while causing physical disruptions.
- Ransomware: This attack starts when an operator runs a malicious file that connects to a command center, scans the local network, sends results back, and blocks Modbus TCP traffic to simulate a lockout. It affects the cyber layer without altering the breaker state until a full lockdown.
- Simultaneous FDI and ransomware: This attack launches a combination of FDI and ransomware samples at once.

E. Data Collection and Preparation

We collect physical measurements using ElasticSearch as a data lake, with relays sampling every five seconds and forwarding the data, while cyber data is continuously gathered via tcpdump on all cyber nodes and later converted from

packet capture (PCAP) to comma-separated value (CSV) files. For each scenario, including a 15-minute benign baseline and various attack cases, a complete dataset is compiled. The cyber-physical features collected are detailed in Table I.

TABLE I
COLLECTED CYBER AND PHYSICAL FEATURES

Cyber Features	Physical Features
Source MAC Address	PLC ID
Destination MAC Address	Voltage
Source IP Address	Current
Destination IP Address	Phase Angle
Protocol	Active Power
Packet Length	Reactive Power
Source TCP Port	Generator Breaker Status
Destination TCP Port	Load Breaker Status
Source UDP Port	Shared Edge Active Power
Destination UDP Port	Shared Edge Reactive Power

To prepare the data for the multi-task GCNN, the cyber data and physical data are processed into CSV files. PCAP files are converted using tshark and mergecap, then concatenated and sorted chronologically, while the physical data is directly exported from ElasticSearch. Finally, a PLC-to-IP address mapping function aligns physical measurements with corresponding cyber traffic.

III. PROPOSED MULTI-TASK GCNN MODEL

We model our system as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, A)$, where vertices $\mathcal{V}$ represent physical buses and associated cyber components, edges $\mathcal{E}$ denotes the connections between them, and A is the unweighted adjacency matrix describing the relationships between the nodes. Our multi-task GCNN model captures the grid's inherent spatial and temporal dynamics, which our testbed replicates. Our model leverages the cyber-physical structure for simultaneous detection and localization through supervised training on benign and malicious datasets. The labeling scheme of the data is denoted by $\mathcal{Y}$ and $\mathcal{Z}$, where $\mathcal{Y}$ is the binary detection label, and $\mathcal{Z}$ are the localization labels. $\mathcal{Y}$ is 0 or 1 for normal and malicious states, respectively. $\mathcal{Z}$ represents a vector of size equal to the number of PLCs, or nodes, where a 1 is in the position of the affected node, or 0 otherwise. Input features are fed into the model in a scaled numerical format. As illustrated in Fig. 3, the multi-task GCNN presents a deep architecture with multiple layers operating on a single graph. The GCNN structure described next enables the model to learn representations for both graph-wide detection and node-level localization simultaneously.

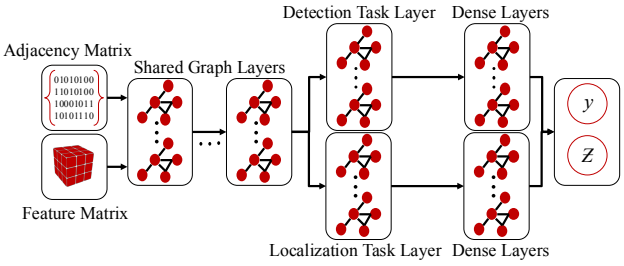

Fig. 3. Illustration of the proposed multi-task GCNN.

A. Model Input

The inputs to the shared graph layers are the adjacency matrix and three-dimensional feature matrix $\mathcal{M}$, i.e.,

$$\mathcal{M} \in \mathbb{R}^{T \times N \times F}, \tag{1}$$

where T is the number of timestamps, N is the number of nodes, and F represents the number of features for a given node at a given timestamp.

B. Shared Graph Layers

The shared graph layers L process node-level features and extract node-level embeddings. Each graph convolutional layer l applies a Chebyshev polynomial filter:

$$X^l = \text{ReLU}(\mu^l *_{\mathcal{G}} X^{l-1} + b^l), \tag{2}$$

where $\mu^l \in \mathbb{R}^{K \times c_{l-1} \times c_l}$ are the Chebyshev coefficients, c denotes the features, $*_{\mathcal{G}}$ represents the graph convolution operator, and $b^l \in \mathbb{R}^{c_l}$ is the bias. Beyond the shared layers are two task-specific paths: detection and localization.

C. Detection and Localization Layers

Following the shared graph layers L are the task specific Chebyshev layers $L_{T\{1,2\}}$ where $\{1, 2\}$ are the detection and localization tasks, respectively. The task-specific layers extract the features most relevant to their assigned task. The first layer l_T in each task receives output from $X_l \in \mathbb{R}^{n \times c_l}$ of the last shared layer then generate the output $X_{l_T} \in \mathbb{R}^{n \times c_{L_T}}$. Then the rest of the task specific layers take $X_{l_{T-1}} \in \mathbb{R}^{n \times c_{L_{T-1}}}$ as their inputs. The task specific layers then output $X_{L_{T\{1,2\}}} \in \mathbb{R}^{n \times c_{L_{T\{1,2\}}}}$.

D. Model Output

After passing through the shared L and task-specific $L_{T\{1,2\}}$ layers, a dense layer determines the probability of an attack and generates outputs using the sigmoid activation function

$$\text{sigmoid}(W_{L_T} X_{L_T} + b_{L_T}) \tag{3}$$

where $W_{L_T} \in \mathbb{R}^{n \times c_{L_T}}$ represents the feature weights for each task, and $b_{L_T} \in \mathbb{R}$ is the corresponding bias. Incorporating bias terms alongside activation functions such as sigmoid improves the ability of the model to capture complex patterns by increasing non-linearity [18]. The task-specific output layer then generates a prediction for each task, classifying the entire graph for the first task (detection) and pinpointing the affected node for the second task (localization). The final layer serves as an aggregation module, refining the final decision by leveraging information extracted in earlier stages.

E. Model Training

The multi-task GCNN objective function is described as:

$$C(p, \theta) = -\frac{1}{S} \sum_{\mathbf{X}_{\text{TR}}} \{a \log(p) + (1 - a) \log(1 - p)\}, \tag{4}$$

where θ represents the trainable parameters (μ^l, b^l, W^L, b^L) for all layers $l(\cdot)$. S is the number of training samples X_{TR}. p and a are the final predicted and actual labels, respectively.

TABLE II
DETECTION RESULTS OF ATTACKS ON A SINGLE NODE (%)

Scenario	Data	Model											
		FNN			LSTM			CNN			GCNN		
		DR	FAR	F1	DR	FAR	F1	DR	FAR	F1	DR	FAR	F1
Single-node Ransomware	**C**	77.8	25.3	75.5	81.7	19.9	80.2	83.8	14.2	85.4	95.5	2.1	92.1
	P	76.0	29.0	73.4	79.3	23.4	78.0	83.2	18.8	84.3	94.0	2.9	90.8
	CP	81.2	22.5	79.4	84.9	15.6	83.6	86.1	11.4	87.6	97.4	0.03	94.1
Single-node FDI	**C**	74.9	28.4	74.3	78.3	20.2	77.0	79.3	15.6	81.4	93.9	2.8	95.0
	P	73.1	31.8	72.0	75.9	23.7	74.4	77.9	20.4	80.0	92.4	3.3	94.1
	CP	79.3	24.6	77.2	81.1	17.1	80.0	82.4	13.0	84.1	96.4	0.04	97.3
Single-node FDI & Ransomware	**C**	73.6	28.8	71.6	75.9	22.0	75.6	77.6	16.2	80.7	92.9	3.6	93.6
	P	71.1	32.3	69.0	73.3	25.6	73.2	76.4	21.0	79.8	91.6	4.1	92.5
	CP	77.9	26.0	75.7	79.9	18.7	78.6	80.9	14.3	82.9	95.3	0.1	96.4

TABLE III
LOCALIZATION RESULTS OF ATTACKS A SINGLE-NODE (%)

Scenario	Data	Model											
		FNN			LSTM			CNN			GCNN		
		DR	FAR	F1	DR	FAR	F1	DR	FAR	F1	DR	FAR	F1
Single-node Ransomware	**C**	83.2	21.0	82.5	85.3	14.8	84.4	90.1	11.6	90.9	96.9	2.8	97.0
	P	81.2	25.0	80.4	83.2	18.8	82.2	89.1	15.8	89.5	96.1	3.3	95.9
	CP	86.3	17.3	86.1	88.5	12.1	88.4	92.0	8.2	92.8	98.0	0.01	99.0
Single-node FDI	**C**	80.0	23.3	81.1	81.1	17.5	81.3	86.2	11.8	85.9	96.1	2.0	95.9
	P	77.6	27.1	78.6	79.3	21.4	78.8	85.3	15.9	84.7	94.8	2.6	94.5
	CP	84.1	19.2	84.4	84.9	13.7	84.7	88.3	9.7	88.9	97.7	0.02	98.7
Single-node FDI & Ransomware	**C**	78.0	24.6	78.8	79.9	19.2	79.8	83.7	14.4	84.6	95.4	1.3	96.4
	P	75.6	27.9	77.0	77.9	23.2	77.6	82.3	18.6	83.6	94.4	2.2	95.5
	CP	82.5	20.7	83.1	83.4	15.3	83.1	86.9	11.3	87.6	97.0	0.08	98.2

TABLE IV
DETECTION RESULTS OF ATTACKS ON MULTI-NODES (%)

Scenario	Data	Model											
		FNN			LSTM			CNN			GCNN		
		DR	FAR	F1	DR	FAR	F1	DR	FAR	F1	DR	FAR	F1
Multi-node Ransomware	**C**	74.3	29.0	73.1	75.6	22.7	76.1	78.9	17.6	79.6	95.2	2.3	95.1
	P	71.7	32.7	70.9	73.6	26.0	74.2	78.1	21.9	78.8	93.7	2.9	93.5
	CP	78.1	25.9	76.2	79.8	18.5	78.9	81.1	14.2	82.9	96.4	0.04	97.3
Multi-node FDI	**C**	73.1	30.9	71.0	75.3	23.1	73.7	77.9	18.4	78.4	93.9	3.1	95.3
	P	70.7	34.2	68.8	73.3	26.3	71.3	76.9	22.9	77.2	92.3	3.9	94.3
	CP	77.3	26.5	75.4	79.3	19.2	78.0	80.6	15.0	81.9	96.1	0.06	97.2
Multi-node FDI & Ransomware	**C**	73.0	25.5	70.6	75.2	18.2	74.4	77.1	12.9	79.1	93.2	2.2	93.9
	P	71.1	29.1	68.2	72.6	22.2	72.2	76.5	17.5	78.2	92.1	3.2	93.0
	CP	77.1	22.2	74.9	78.8	14.8	77.6	80.2	10.6	81.8	94.9	0.3	95.8

TABLE V
LOCALIZATION RESULTS OF ATTACKS ON MULTI-NODES (%)

Scenario	Data	Model											
		FNN			LSTM			CNN			GCNN		
		DR	FAR	F1	DR	FAR	F1	DR	FAR	F1	DR	FAR	F1
Multi-node Ransomware	**C**	79.4	24.5	80.6	80.2	17.8	80.6	85.0	13.8	85.2	95.8	2.7	97.4
	P	76.8	27.8	78.3	78.0	21.3	78.4	84.2	17.8	84.1	95.0	3.6	96.1
	CP	82.9	20.5	83.4	83.6	14.8	83.3	87.3	10.7	87.5	97.3	0.03	98.7
Multi-node FDI	**C**	78.4	25.7	77.8	79.6	19.2	79.6	83.1	14.9	85.1	95.2	2.7	97.1
	P	76.0	29.2	75.6	77.7	22.7	77.8	82.3	19.7	84.5	94.4	3.5	96.3
	CP	82.3	21.3	82.1	82.9	15.5	82.6	86.5	11.5	87.1	97.4	0.05	98.6
Multi-node FDI & Ransomware	**C**	78.8	20.1	78.2	78.1	14.9	78.6	82.5	10.9	83.2	93.7	1.5	96.0
	P	76.9	23.6	75.9	75.9	18.5	76.5	81.7	15.3	82.1	92.1	1.9	95.0
	CP	81.7	16.7	82.1	82.5	11.2	82.3	86.0	7.6	86.7	95.9	0.1	97.4

IV. EXPERIMENTAL RESULTS

For a comprehensive evaluation of detection and localization, we use DR $= \frac{\text{TP}}{\text{TP+FN}}$, F1-score $= \frac{2\cdot\text{TP}}{2\cdot\text{TP+FP+FN}}$, and FAR $= \frac{\text{FP}}{\text{FP+TN}}$, where TP, FN, FP, TN denote true positives, false negatives, false positives, and true negatives, respectively.

A. Model Setup

We evaluate the spatio-temporal-aware multi-task GCNN trained on cyber-physical fused data against benchmark deep models. All models are trained on identical setups, datasets, attack scenarios, and sequential hyperparameter tuning methods [19]. FNN utilizes 3 layers, 32 units, no dropout, and Adam optimizer. LSTM utilizes 2 layers, 64 units, 0.2 dropout rate, and Sigmoid optimizer. CNN employs 3 layers, 32 units, 0.2 dropout rate, and Sigmoid optimizer. The proposed GCNN comprises 3 layers, 64 units, 0.4 dropout rate, the Adam optimizer, and ReLu activation function.

B. Detection and Localization Performance Results

Our experimental results (as per Tables II - V) reveal that leveraging the fused cyber-physical dataset consistently outperforms models trained solely on cyber or physical data

across all tasks and scenarios. Specifically, using the fused dataset, all investigated models (for detection and localization tasks) offer improved DR by 10.5% and 9.8% compared to using cyber-only and physical-only datasets, respectively, as the fused dataset utilizes the strengths of each data type to offer a more holistic system representation. Moreover, using the fused dataset, our multi-task GCNN model yields, on average, DR improvements of $14.6-17.6\%$ and $10.0-14.4\%$ in the detection and localization tasks, respectively, and FAR enhancements of 12.3–23.9% and 9.4–18.6% for the detection and localization tasks, respectively, compared to benchmarks, when evaluated against simultaneous FDI and ransomware attacks. Analyses of each attack case are provided next.

1) Single-Node Attacks: Tables II and III detail the performance of the investigated models against ransomware and FDI, as well as a combination of ransomware and FDI simultaneously launched on a randomly selected node as follows.

a) Detection Task: The proposed GCNN model outperforms benchmarks by $15.3-19.3\%$, $15.2-20.5\%$, and $14.4-17.4\%$ in DR using the cyber (C), physical (P), and fused (CP) datasets, respectively. The GCNN model also outperforms benchmarks by $12.6-25.2\%$, $16.9-28.2\%$, and $14.2-25.9\%$ in FAR for the C, P, and CP datasets, respectively.

b) Localization Task: The proposed GCNN model outperforms benchmarks by $18.3-22.4\%$, $12.1-18.8\%$, and $10.1-14.5\%$ in DR using the C, P, and CP datasets, respectively. The GCNN model also outperforms benchmarks by $13.1-23.3\%$, $16.4-25.7\%$, and $11.2-20.6\%$ in FAR for the C, P, and CP datasets, respectively.

2) Multi-Node Analysis: Tables IV and V detail the performance of the investigated models against ransomware and FDI, as well as a combination of ransomware and FDI simultaneously launched on a randomly selected set of nodes as follows.

a) Detection Task: The proposed GCNN model outperforms benchmarks by $16.1-20.0\%$, $15.6-21.0\%$, and $14.7-17.8\%$ in DR using the C, P, and CP datasets, respectively. The GCNN model also outperforms benchmarks by $10.7-23.3\%$, $14.3-25.9\%$, and $10.3-21.9\%$ in FAR for the C, P, and CP datasets, respectively.

b) Localization Task: The proposed GCNN model outperforms benchmarks by $11.2-14.9\%$, $10.4-15.2\%$, and $9.9-14.2\%$ in DR using the C, P, and CP datasets, respectively. The GCNN model also outperforms benchmarks by $9.4-18.6\%$, $13.4-21.7\%$, and $7.5-16.6\%$ in FAR for the C, P, and CP datasets, respectively.

V. Conclusion

This paper investigated the performance of our spatio-temporal-aware multi-task GCNN for detecting and localizing cyber attacks, including single-node and multi-node FDI, ransomware, and simultaneous attack scenarios. Our experimental results demonstrated that leveraging the fusion of cyber and physical features using our multi-task GCNN model offered detection rate enhancements of $15-18\%$ and $10-14\%$ for attack detection and localization, respectively. The ability of the multi-task GCNN model in capturing spatio-temporal dependencies through graph structures and leveraging multi-task learning contributed to its robustness, showcasing its effectiveness in addressing complex, multi-modal attack scenarios. Future works include performing feature selection for more efficient training.

References

[1] A. Takiddin *et al.*, "Resilience of data-driven cyberattack detection systems in smart power grids," in *2024 32nd European Signal Processing Conference (EUSIPCO)*, Lyon, France, 2024, pp. 1992–1996.

[2] L. Kearney, "Us electric grid growing more vulnerable to cyberattacks, regulator says," [Online: accessed Feb. 2025]. [Online]. Available: https://tinyurl.com/2fwtuhcm

[3] J. Pearson, "Russian spies behind cyber attack on ukraine power grid in 2022 - researchers," [Online: accessed: Feb. 2025]. [Online]. Available: https://tinyurl.com/mrya55ab

[4] C. Huber, "Chinese hackers targeted texas power grid, hawaii water utility, other critical infrastructure," [Online: accessed: Feb. 2025]. [Online]. Available: https://tinyurl.com/neywnbzt

[5] A. Greenberg, "China-linked hackers breached a power grid–again," [Online: accessed: Feb. 2025]. [Online]. Available: https://tinyurl.com/fjhsn9nc

[6] J. R. Babu, "Design, implementation, and field-testing of distributed intrusion detection system for smart grid scada network," Master's thesis, Iowa State University, 2021, online. [Online]. Available: https://dr.lib.iastate.edu/server/api/core/bitstreams/5ddbc254-e1da-4925-bd64-05e011292315/content

[7] A. Presekal *et al.*, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. on Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sept. 2023.

[8] A. Takiddin *et al.*, "A graph neural network multi-task learning-based approach for detection and localization of cyberattacks in smart grids," in *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Rhodes Island, Greece, 2023, pp. 1–5.

[9] O. Boyaci *et al.*, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Trans. on Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.

[10] X. Su *et al.*, "Damgat-based interpretable detection of false data injection attacks in smart grids," *IEEE Trans. on Smart Grid*, vol. 15, no. 4, pp. 4182–4195, Jul. 2024.

[11] A. Baul *et al.*, "Xtm: A novel transformer and lstm-based model for detection and localization of formally verified fdi attack in smart grid," *Electronics*, vol. 12, no. 797, 2023.

[12] P. Hu *et al.*, "Detection of false data injection attacks in smart grids based on expectation maximization," *Sensors*, vol. 23, no. 1683, 2023.

[13] Y. Zhang *et al.*, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. on Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[14] E. Shereen *et al.*, "Detection and localization of pmu time synchronization attacks via graph signal processing," *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 3241–3254, Jul. 2022.

[15] S. H. Haghshenas *et al.*, "A temporal graph neural network for cyber attack detection and localization in smart grids," in *2023 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2023, pp. 1–5.

[16] "What is elasticsearch?" [Online: accessed Feb. 2025]. [Online]. Available: https://tinyurl.com/5n8systy

[17] J. Sweeten *et al.*, "Cyber-physical gnn-based intrusion detection in smart power grids," in *2023 IEEE Int. Conf. on Comm., Cont., and Comp. Tech. for SG (SmartGridComm)*, Glasgow, United Kingdom, 2023, pp. 1–6.

[18] A. Takiddin *et al.*, "Generalized graph neural network-based detection of false data injection attacks in smart grids," *IEEE Trans. on Emerging Topics in Computational Intelligence*, vol. 7, no. 3, pp. 618–630, June 2023.

[19] A. Takiddin *et al.*, "Spatio-temporal graph-based generation and detection of adversarial false data injection evasion attacks in smart grids," *IEEE Trans. on AI*, vol. 5, no. 12, pp. 6601–6616, 2024.