IEEE Open Access Journal of
Power and Energy

Received 12 March 2025; revised 29 June 2025; accepted 26 July 2025.
Date of publication 31 July 2025; date of current version 7 August 2025.

Digital Object Identifier 10.1109/OAJPE.2025.3594625

Cyber-Physical Fusion for GNN-Based Attack Detection in Smart Power Grids

JACOB SWEETEN[1,2], AMR ELSHAZLY[1,2], ABDULRAHMAN TAKIDDIN[3] (Member, IEEE), MUHAMMAD ISMAIL[1,2] (Senior Member, IEEE), SHADY S. REFAAT[4] (Senior Member, IEEE), AND RACHAD ATAT[5] (Senior Member, IEEE)

[1]Cybersecurity Education, Research, and Outreach Center (CEROC), Tennessee Technological University, Cookeville, TN 38505 USA
[2]Department of Computer Science, Tennessee Technological University, Cookeville, TN 38505 USA
[3]Department of Electrical and Computer Engineering, FAMU-FSU College of Engineering, Florida State University, Tallahassee, FL 32310 USA
[4]School of Physics, Engineering, and Computer Science, University of Hertfordshire, AL10 9EU Hatfield, U.K.
[5]Department of Computer Science and Mathematics, Lebanese American University, Beirut 1102-2801, Lebanon
CORRESPONDING AUTHOR: A. ELSHAZLY (aaelshazly42@tntech.edu)

This work was supported by NSF Energy-Power-Control-Networks (EPCN) Award under Grant 2220346.

ABSTRACT Recent research has shown promise in using machine learning for cyberattack detection in power systems. However, current studies face limitations: a) dependence on either physical or cyber features, overlooking multi-modal cyber-physical (CP) correlations; b) unrealistic full observability assumptions; c) focus on detecting basic attacks instead of advanced threats such as ransomware (RW); and d) use of deep learning (DL) models built for 2D data, despite the graph-structured nature of power systems. To address these gaps, we develop a CP testbed using OPAL-RT and a cyber range to simulate both physical and cyber layers under full and partial observability. The testbed produces a realistic multi-modal dataset covering normal operations and various cyberattacks, including RW, brute force, false data injection, reverse shell, and backdoor. Using this dataset, we design graph neural network (GNN)-based multi-modal intrusion detection systems (IDSs) that fuse CP features and capture spatio-temporal dependencies. Results show that CP fusion improves detection rates (DRs) by up to 16% compared to single-modal inputs. The proposed GNN-based IDSs outperform benchmarks by up to 26% in DR, remain effective under partial observability, and demonstrate up to 6% improvement in scalability when applied to larger system topologies.

INDEX TERMS Cyber-physical, cyberattack detection, power systems, graph neural networks, machine learning, smart grids.

NOMENCLATURE

ACRONYMS

BD	Backdoor.
BF	Brute Force.
CP	Cyber-Physical.
DR	Detection Rate.
FA	False Alarm Rate.
FDI	False Data Injection.
GNN	Graph Neural Network.
HMI	Human-Machine Interface.
IDS	Intrusion Detection System.
PLC	Programmable Logic Controller.
RS	Reverse Shell.
RW	Ransomware.
SCADA	Supervisory Control and Data Acquisition.

INDICES AND SUBSCRIPTS

i, j	Node indices in the graph.
l	Layer index in the GNN.
t	Time index.

PARAMETERS AND VARIABLES

b_l	Bias term for layer l.
$C(\tilde{y}, \Theta)$	Cross-entropy loss function.
E	Set of edges (intra- and inter-layer).
$G = (V, E, W)$	Graph representing the CP power system.
$K[t]$	Load profile scaling factor at time t.
L_{base}	Base load value.
$L_{\text{bus}}(t)$	Load at a bus at time t.
$N(\cdot)$	Normal distribution function.

V	Set of nodes (cyber and physical).
W	Weighted adjacency matrix.
W_L	Weights of the final dense layer.
X^l	Output of the l-th GNN layer.
X_{TR}	Training dataset.
$y, \tilde{y}$	True and predicted labels.
μ_l	Chebyshev coefficients for layer l.

I. INTRODUCTION

SMART power grids (SGs) play a crucial role in modern infrastructure, supplying energy to essential services such as hospitals, defense systems, and emergency response facilities [3], [4]. By integrating computation, communication, and control, these cyber-physical systems (CPSs) enhance operational efficiency and grid resilience [5]. However, as the grid becomes more interconnected, it also becomes more vulnerable to cyber threats that can disrupt operations, compromise stability, and lead to widespread outages [6]. A single attack can have cascading effects, impacting not only power distribution but also public safety and economic stability. Given these risks, developing robust intrusion detection mechanisms is essential to safeguarding SG security and ensuring continuous and reliable power delivery [7].

SGs integrate tightly coupled cyber and physical layers. The physical layer includes generators, circuit breakers, transmission lines, and loads, while the cyber layer comprises Supervisory Control and Data Acquisition (SCADA) systems, routers, switches, and networked communication devices. This integration enhances system observability and control but introduces vulnerabilities inherent in interconnected systems [8]. Attackers exploit these weaknesses, using cyber-layer entry points to disrupt physical operations. The 2015 Ukraine power grid attack, which caused a six-hour outage, and subsequent incidents involving advanced threats such as wiper malware, highlight the growing sophistication of cyberattacks on critical infrastructure [9], [10]. These events underscore the need for robust intrusion detection systems (IDSs) tailored to SG security.

A. RELATED WORKS

Existing detectors consider features gathered from only one of the two CPS layers. For example, physical measurements are more effective when detecting False Data Injection (FDI), whereas cyber features are more effective for ransomware (RW) detection. Thus, existing detectors are only provided with an incomplete view of the power system, resulting in hindered detection performance. Related works are discussed next.

1) CYBER-ONLY DETECTORS

The following IDSs rely only on cyber features gathered from network logs for training. A Snort-based IDS with specific rules for a distributed network protocol (DNP3)-based attacks is proposed [11]. Other IDSs are employed to detect attacks targeting IEC 61850 GOOSE signals [12]. Another IDS is proposed for IEEE 1815.1-based power systems [13].

2) PHYSICAL-ONLY DETECTORS

Attack detection in the prevailing body of research primarily focuses on physical-layer features for attack detection. A majority vote ensemble technique on physical measurements is examined using data from Oak Ridge National Laboratory [14]. Two long-short-term memory (LSTM) recurrent neural network (RNN)-based detectors are employed to detect FDI attacks on the IEEE 14-bus test system using measurements from each bus [15]. A cluster-driven ensemble learning machine learning detectors are employed in a decentralized IDS to detect attacks on automatic generation control (AGC) [16]. An autoencoder (AE)-based model employing physical data is proposed to detect attacks on a single power station [17]. Support vector machine (SVM) and boosting machine learning algorithms using physical measurement data collected from the power lines are adopted to investigate power-line communication tapping attacks [18].

3) OTHER NOTABLE DETECTORS

An IDS that is either trained on physical or cyber data is proposed [19]. A similar approach gathers data from one substation rather than multiple substations [20]. Another study uses a combination of the KDD99 dataset and simulated physical data of a small power system [21]. Despite adopting physical and cyber data, datasets are not coupled realistically, and the KDD99 data is irrelevant to power systems. The related works are summarized in Table 1.

B. LIMITATIONS AND CHALLENGES

Existing studies exhibit the following limitations:

- Most of the proposed IDSs adopt either physical features (i.e., power system measurements such as active and reactive power, voltage, and/or current measurements) [14], [15], [16], [17], [18], [22], [23], [24], [25], [27], [29] or cyber features (i.e., network log information such as IP addresses and port numbers) [11], [12], [13] while building IDSs. While a few detectors, e.g., [19], [20], and [21], explore cyber and physical features, they are either not fused [19], limited to a single substation [20], or rely on cyber data irrelevant to power systems [21]. As CPSs, power systems present multi-modal features covering both the cyber and physical domains. Building IDSs that fuse features from both domains and from multiple substations is expected to improve detection performance.
- Existing IDSs that consider a power system with multiple substations, e.g., [23], [24], and [25], assume full system observability, which means that measurements from all the power nodes (substations) are assumed to be available at the IDS. In practice, power systems do not have full observability, making IDS performance with partial observability unexplored.

TABLE 1. Summary of related works.

Reference	Cyber	Physical	Attacks
[11]	✓		DNP3-specific
[12]	✓		IEC 61850 GOOSE-specific
[13]	✓		IEEE 1815.1-specific Attacks
[22]		✓	FDI Attacks
[23]		✓	FDI Attacks
[24]		✓	FDI Attacks
[25]		✓	FDI Attacks
[26]		✓	FDI Attacks
[27]		✓	FDI Attacks
[28]		✓	FDI Attacks
[29]		✓	FDI Attacks
[14]		✓	Generic SCADA Attacks
[15]		✓	FDI Attacks
[16]		✓	AGC Attacks
[30]		✓	FDI Attacks
[17]		✓	Anomalies at Power Plant
[18]		✓	Communication Tapping
[19]	✓	✓	Generic SCADA Attacks
[20]	✓	✓	FDI Single Power Substation
[21]	∼	✓	Not Described

- In the literature, examined attacks primarily focus on basic SCADA attacks such as FDI and DoS [14], [15], [16], [19], [20], [22], [24], [25], [26], [27], [28], [29], [30] or protocol-specific attacks [11], [12], [13], while the performance of IDSs against state-of-the-art attacks like RW, reverse shell (RS), and backdoor (BD) is not examined.
- Most existing IDSs are based on deep learning (DL) techniques (e.g., feedforward neural networks (FNNs), RNNs, and AEs that operate on 2D data [27], [28], [29]. Thus, they do not capture the spatial correlations within measurements from nodes (substations and routers). The power system may be represented as a graph with nodes (i.e., power substations) and edges (i.e., transmission lines). Thus, the power system involves graph-structured data. Hence, we anticipate that adopting topologically-aware DL models (e.g., graph neural networks (GNNs)) improves the detection performance as they better capture the spatio-temporal interactions among the features compared to other 2D DL models.

Existing IDS approaches face several key limitations:

- Data Reliance: They often depend solely on either cyber or physical data, lacking an integrated CP perspective.
- Dataset Limitations: There's a scarcity of real-world datasets that incorporate CP fusion, hindering comprehensive evaluation. Due to security policies and confidentiality requirements imposed by utilities and governments, real-world datasets from operational power systems are rarely available for research purposes, and researchers commonly rely on IEEE standard test systems to overcome this limitation [25].
- Observability Constraints: Many are not evaluated under partial observability conditions, limiting their applicability in real-world scenarios.

Addressing these gaps necessitates a system that:

- Integrates both cyber and physical features to reflect the system's state under varying observability conditions.
- Captures spatial and temporal aspects of power system behavior.
- Covers a wide range of attack scenarios beyond traditional SCADA-based threats.

Existing datasets are limited to generic industrial control system (ICS) datasets, isolated network attack logs, or FDI attack datasets on individual substations—none providing a holistic CP view of power grids. To address this, we have developed a CP testbed capable of collecting benign and attack data across multiple system layers.

C. CONTRIBUTIONS

In this paper, we present GNN-based multi-modal IDSs that fuse CP features to capture spatial dependencies and enhance attack detection in power systems. The key contributions of this work include:

- **Development of a comprehensive CP testbed:** We constructed a testbed simulating IEEE 14-bus and 30-bus power systems, integrating real-time simulation tools (OPAL-RT and RT-Lab) and a cyber range for network emulation, enabling comprehensive multi-modal data collection.
- **Introduction of a GNN-based IDS:** Our proposed IDS fuses cyber and physical features to model spatial dependencies within graph-structured data, effectively capturing the interactions between the two layers.
- **Comprehensive attack coverage:** We include advanced threats such as RW, brute force (BF), RS, and BD attacks.
- **Scalability and robust detection performance:** The GNN-based IDS demonstrates enhanced detection rates (DRs) (up to 26% improvement) compared to benchmarks and remains effective under partial observability with minimal degradation (1)–2%) when compared to full observability.
- **Comparison with benchmarks:** Extensive evaluations against shallow and DL-based IDSs highlight the advantages of CP fusion and GNNs in delivering consistent and superior detection performance.

The remainder of the paper is organized as follows. Section II describes the development of the CP testbed and dataset generation. Section III introduces the GNN-based IDS and benchmarks. Section IV presents experimental results and discussion. Finally, conclusions and future work are drawn in Section V.

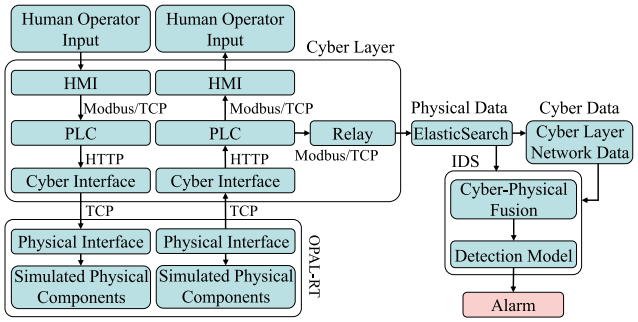


FIGURE 1. Illustration of the data flow in the testbed.

II. CYBER-PHYSICAL POWER SYSTEM TESTBED

The power system testbed comprises into two layers; physical and cyber. Real-time simulation on an OPAL-RT device is the basis of the physical layer. The software for programmable logic controllers (PLCs), human-machine interfaces (HMIs), routers, firewalls, and servers is housed in a number of Docker containers that make up the cyber layer. The aforementioned layers are coupled together via a TCP connection and an interfacing network which all PLCs are members of. Fig. 1 shows the flow of collected data in the testbed. Through the HMIs, the human operators transmit control commands to the PLCs. This will affect the physical layer as the PLCs communicate with the cyber interface, and forward the received signals to the physical interface. Physical data is sent from the simulation to the cyber interface which is sent back to the PLCs and HMIs. Using Modbus/TCP, a relay queries the PLC and reports the collected data to ElasticSearch. The details of the physical and cyber layers along with their coupling are discussed next.

A. PHYSICAL LAYER

Two physical layers are considered in the testbed based on the IEEE 14-bus and the IEEE 30-bus test systems modeled in MATLAB Simulink. The Simulink model is developed in accordance with the OPAL-RT, Then it is compiled using the RT-Lab software, which transmits the resulting simulation executable to the OPAL-RT. RT-Lab is used to start, halt, and monitor the simulation after the model is compiled and loaded onto the OPAL-RT. A six-month load profile is applied to both IEEE test systems to mimic practical consumption patterns throughout various days and seasons. The following load profile is generated using a MATLAB function, a widely used tool for numerical computation and simulation in power system analysis

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

where $L_{\text{bus}}(t)$ denotes the active and reactive power values of a load at a given bus and timestamp t, L_{base} depicts the load value (P and Q) according to the IEEE data [31], 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. K is an array of the six-month load profile values. The load profile is down-scaled to 15 minutes. To construct a TCP server for data exchange with the cyber layer, a physical interface is included.

B. CYBER LAYER

The cyber layer is implemented using Docker, a lightweight containerization platform that enables efficient deployment and management of isolated virtualized environments. Docker provides an efficient way to encapsulate software components, ensuring reproducibility, security, and scalability in complex CPSs. In our framework, multiple Docker containers are interconnected via Docker networks to simulate various cyber-layer entities such as PLCs, HMIs, routers, firewalls, and servers. This architecture allows for flexible and modular system configuration, mimicking real-world ICS. The majority of real-world communication networks are found to exhibit the scale-free property [32], where only a small number of nodes (routers) have a degree and betweenness scores higher than the rest of nodes [33]. We create a scale-free communication network whose average degree follows the power-law distribution: $\tilde{\kappa} \sim \kappa^{-\delta}$, $(2 \leq \delta \leq 2.6)$ [34], where κ is the node degree and δ is an exponent. Specifically, a random scale-free network with an average degree of $\tilde{\kappa} = 7$ and an exponent $\delta_{\text{exp}} = 2.2$ is created using MATLAB [35]. Each router is connected to the local network of a specific substation (bus/node at the physical layer), and the routers are connected together via links. The routers establish their routes using the Open Shortest Path First protocol, and there is a central node from which the HMIs are accessed as well as an external Internet connection is provided. We use the highest degree node strategy [33] to choose a control center from among the nodes in the cyber layer. The literature describes various strategies for choosing control centers, including selecting the node with the highest betweenness centrality [36] and the geometric median of all nodes [37]. Since the communication network is scale-free, we make the same assumption as [33] that the control center is the node with the highest degree.

The local substation network is made up of several containers. The HMI is one container that the router uses IP tables to port forward to. Other containers are for PLC and relay for each bus that the cyber node supervises. Both the HMI and the relays gather data from the PLCs. The PLC can also receive circuit breaker control signals from the HMI. The relay queries the PLC and transmits the collected data through the central cyber node (control center) to an ElasticSearch database, which serves as a centralized historian for logging and analyzing CPS data. ElasticSearch is a distributed search and analytics engine designed for real-time indexing, retrieval, and visualization of structured and unstructured data. It enables efficient querying of historical system states, making it an essential component for monitoring and detecting anomalies in CP infrastructures. Firewall rules are set to default deny for inbound packets with regards to its local

substation network with the exception of the port forwards required for accessing the HMI within the network.

C. CYBER-PHYSICAL COUPLING

To establish connections between the cyber and physical layers, two cyber topologies are created for each IEEE test system, one with full observability of all physical nodes and another with partial observability. This setup enables evaluating IDS performance under both observability conditions.

1) CYBER TOPOLOGY FOR FULL OBSERVABILITY

Each power node (bus) in this architecture is connected to a communication node (router). Thus, the quantity of routers in the simulated communication network equals the number of buses given in the IEEE test system. We adopt the random positive degree correlation coupling (RPDCC) methodology [38] to connect the cyber and physical nodes. This method is shown to closely resemble the coupling of real-world interconnected systems [39]. In RPDCC, power nodes with high degrees tend to couple with communication nodes with high degrees, and the same trend occurs in nodes of low degrees. We obtain a weighted random permutation set of the vertices for each power and communication graph (physical and cyber layers) using the MATLAB tool, where weights are the corresponding degrees. The two weighted sets are then connected to couple the physical and cyber layers.

2) CYBER TOPOLOGY FOR PARTIAL OBSERVABILITY

In this topology, the number of routers in the synthetic communication network equals the number of generators and the most critical loads. To determine the most critical loads, the approach described in [40] is adopted. In this case, each node is given a score based on some electrical metrics (effective graph resistance [41], load shedding [42], and percentage of drop in net-ability [43]) and topological metrics (connectivity impact [42], connectivity level [44], geodesic vulnerability [42], efficiency [45], and topological damage [44]). Then, the analytical hierarchical process (AHP) determines the corresponding weight of each metric based on how much it contributes to the overall system vulnerability. After obtaining the weights for each of the topological and electrical metrics, we have the topological and electrical vulnerability scores for each node. Then, we use AHP to obtain the weights of the corresponding overall weighted topological and the overall weighted electrical scores. Finally, we sort the power nodes based on their overall vulnerability scores where we select the top $V\%$ (35% herein) of the most critical physical nodes and generators that are then to the routers so that critical nodes in the system can always be monitored and controlled by the operator through the SCADA system. We select 35% of power nodes as critical based on prior studies in power grid resilience, which often identify 30-40% of substations as critical due to their impact on system stability and cascading failures [44].

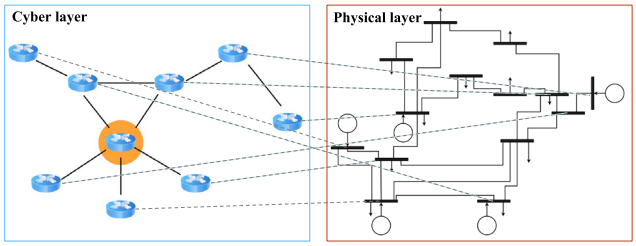


FIGURE 2. Partial-observable IEEE 14-bus system with cyber and physical layers connected. Only critical loads and generators are connected to the cyber layer. The orange node represents the control center. Each router is connected to the local network of a substation, which includes a PLC, relay, and HMI. This setup reflects a realistic SCADA configuration under partial observability, where only a subset of substations is monitored based on vulnerability scoring.

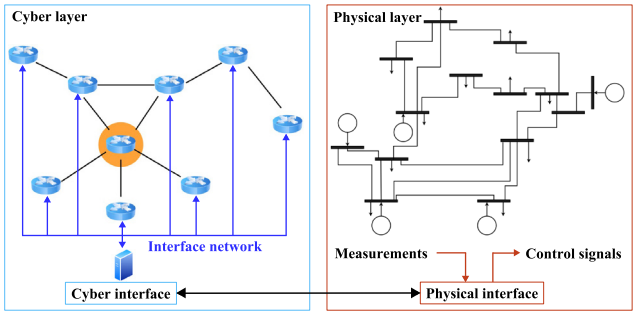


FIGURE 3. Illustration of the partial-observable IEEE 14-bus system with cyber and physical interfaces.

The host bridge network (through which OPAL-RT is accessed) and the Docker networks are both connected by an interface Docker container. The interface serves as both a client to the OPAL-RT's TCP server and a server to the PLCs. The interface container receives an HTTP request from the PLCs and responds with data from the relevant real-time simulation. When a control signal is sent to the PLCs, it is forwarded to the interface container which forwards the command to the OPAL-RT's TCP server. The interconnection between cyber and physical nodes on the IEEE 14-bus with partial observability is shown in Fig. 2 where Fig. 3 shows the interfaces for the cyber and physical layers. Fig. 2 visually illustrates this partial observability configuration, the orange node represents the control center, which is selected based on the highest degree in the scale-free communication network. Each router connects to a local substation network that includes a PLC, HMI, and relay, all virtualized using Docker containers. Only the most critical substations identified through vulnerability scoring [40] are connected to the cyber layer, reflecting a realistic SCADA deployment where full observability is not feasible. Fig. 2 highlights the selective monitoring strategy and the layered architecture of the cyber-physical testbed.

D. BENIGN DATA COLLECTION AND IMPUTATION

ElasticSearch is used to collect the physical data, and tcpdump is used to capture the cyber data from the Docker host.

TABLE 2. Collected multi-modal features.

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)

For a comprehensive CP-IDS, data is collected from both the cyber and physical layers every 15 minutes. The data collection process is described next.

- Cyber Layer Data Collection: Network traffic is captured in Packet Capture (PCAP) format, which stores raw packet-level data. This format preserves the complete network communication flow, enabling in-depth forensic analysis of cyber threats such as brute-force attacks, RW, and BD intrusions. Since PCAP files store raw binary data, they are converted into a structured format using TShark (a command-line utility of WireShark). The conversion process extracts relevant network features and stores them in Comma-Separated Values (CSV) format, facilitating efficient processing and analysis for intrusion detection models.
- Physical Layer Data Collection: Real-time physical measurements (e.g., voltage, frequency, and power flows) are continuously logged in ElasticSearch. A structured CSV file is generated from ElasticSearch, ensuring seamless integration with cyber-layer data for multi-modal machine learning models.

A data imputation step [20] is used to match every row in the cyber data with a corresponding row in the physical data since the rates of cyber and physical data are not equal during each data collecting period. To match every row in the cyber data with a corresponding row in the physical data because the rates of cyber and physical data are not equal during each data collecting period, a data imputation step is used. A similar method is applied in [20] where null packets are added to the cyber dataset to match the number of rows in the underlying physical data. Table 2 summarizes the multi-modal features collected from the cyber and physical layers of the testbed.

E. ATTACK DATA

The attacks assume a compromised control center desktop (e.g., via social engineering) as the launch point. Vulnerabilities are introduced in PLCs (e.g., BD users, vulnerable services), with some attacks using router port forwarding to establish attack channels. The FDI attack differs by introducing a malicious device into the substation network for IP spoofing. The following real-time attacks are conducted on the testbed to generate the under-attack dataset:

- FDI: Uses Address Resolution Protocol (ARP) spoofing to redirect Modbus/TCP traffic to a fake PLC, which transmits falsified measurements while sending commands to disable the circuit breaker. This attack primarily affects the physical layer and is the only one employing IP spoofing. Fig. 4 shows an illustration of the FDI attack flowchart.
- Backdoor: A hidden user account and Secure Shell (SSH) server are set up on the PLC, exploiting potential manufacturer-installed BDs. Once accessed, the attacker disables the PLC and turns off the breaker, impacting both cyber and physical layers.
- Reverse Shell: An unnecessary HTTP web server on the PLC is exploited via a POST request, granting shell access through Netcat. The attacker then disables the PLC and breaker, affecting both layers.
- Brute Force: The Hydra tool cracks HMI passwords, granting unauthorized access to disable breakers across multiple HMIs. This attack impacts both layers.
- Ransomware: A malicious file is downloaded and executed on the PLC, scanning the network, relaying data to a command server, and blocking Modbus/TCP connections. While no immediate breaker state change occurs, prolonged infection could disrupt physical operations. This attack manifests on the cyber layer.

The aforementioned attack types have been observed in major cyber incidents affecting critical infrastructure. The 2017 Ukraine RW attack disrupted institutions, including Chernobyl's radiation monitoring system [9]. BF attacks threaten IoT-based energy systems by exploiting weak authentication. The 2015 Ukraine power grid hack [10] exemplifies an FDI attack used to manipulate control systems, leading to power outages. These incidents underscore the real-world relevance of our selected attack scenarios.

F. DATASET STATISTICS AND CLASS BALANCE

To ensure balanced evaluation, the dataset is carefully constructed with an equal number of benign and malicious samples for both attack-specific and generalized models. For the attack-specific models, the number of benign and malicious samples is always equal for each attack type. Specifically, for the IEEE 14-bus system: under partial observability, there are approximately 400,000 benign samples and 400,000 malicious samples per attack type; under full observability, approximately 600,000 benign and 600,000 malicious samples per attack type. For the IEEE 30-bus system: under partial observability, around 700,000 benign and 700,000 malicious samples per attack type; under full observability, approximately 1,100,000 benign and 1,100,000 malicious samples per attack type. For the generalized models, the number of benign samples is equal to the total number of malicious samples combined across all attacks. For example, if 400,000 benign samples are used, the malicious samples

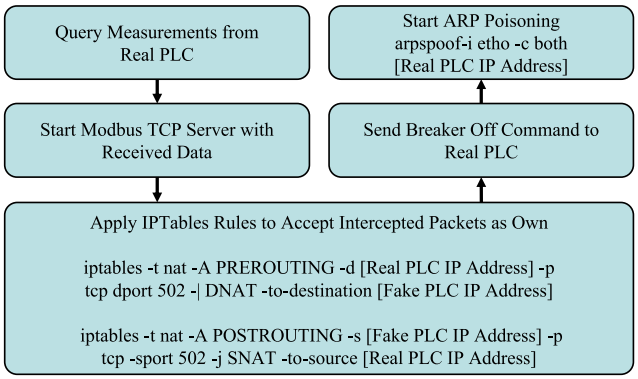


FIGURE 4. Flowchart of the FDI attack.

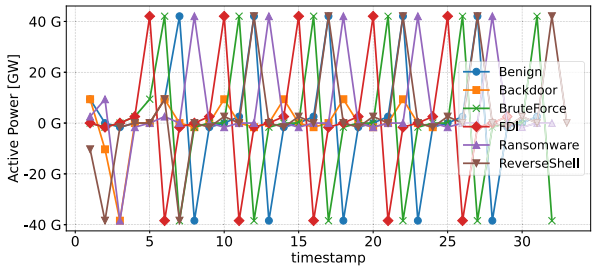


FIGURE 5. Illustration of active power (*P*) samples under benign and cyberattack scenarios.

consist of 80,000 samples from each of the five attack types, totaling 400,000 malicious samples. This balanced construction avoids class imbalance issues and ensures that metrics such as DR, False Alarm Rate (FA), and F1-score remain reliable and comparable across models and scenarios. To further illustrate the difference between benign and malicious behaviors in the physical layer, Fig. 5 plots representative Active Power (P) samples under benign and various cyber-attack scenarios. As shown in Fig. 5, the attacks induce noticeable deviations from normal operation, which supports the learning of effective IDS models.

G. COMPARISON WITH PRIOR DATASETS

To highlight the novelty of our dataset, we compare it against several benchmark datasets that have been widely used in the literatures [46] and [47].

1) SWaT DATASET

The Secure Water Treatment (SWaT) dataset was collected from a scaled-down water treatment plant with 51 sensors and actuators. It recorded normal and attack scenarios over 11 days. While it offered realistic process behavior, it targeted ICS in water infrastructure, not electric grids, and lacked cyber-level interaction data.

2) WADI DATASET

The Water Distribution (WADI) dataset captured physical-layer sensor data over 16 days in a water distribution testbed. It included attacks on control logic and actuators but was similarly domain-specific and lacked cyber communication traces.

3) MARS SCIENCE LABORATORY (MSL) DATASET

The MSL dataset contained spacecraft telemetry for anomaly detection using LSTM models. Although it was time-series based, the domain, data characteristics, and anomaly types differed significantly from smart grid operations.

4) PSA DATASET

The Power System Attack (PSA) dataset consisted of time-synchronized PMU (phasor measurement unit) data under normal and cyber-attack conditions. While relevant to power systems, the data was tabular and did not include cyber-layer behavior or dynamic agent interactions.

5) GAS PIPELINE DATASET

This dataset contained process control data and labels collected from gas pipeline simulations. It included basic features like pressure, flow rate, and valve status but lacked complex cyber-physical feedback or adaptive adversarial modeling.

6) BoT-IoT DATASET

The BoT-IoT dataset included a wide range of network attacks on IoT traffic. While useful for network intrusion detection, it was not specific to industrial control or power system environments, and it lacked physical sensor context.

7) OUR DATASET

In contrast to the above, our dataset [48] is generated from a real-time cyber-physical power system testbed based on the IEEE 14-bus model. The physical layer is simulated via OPAL-RT, while the cyber layer is containerized using Docker to emulate realistic components like PLCs, HMIs, relays, and firewalls. Communication occurs over Modbus/TCP and is logged at the packet level. We simulate a variety of realistic cyberattacks, including FDI, RS access, and RW. This tight cyber-physical coupling enables us to support real-time intrusion detection capabilities not available in prior datasets.

III. CYBER-PHYSICAL GNN-BASED IDS

A connected, undirected, weighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{W})$ can be used to model CP power systems. $\mathcal{V}$ is the set of heterogeneous physical (power substation) nodes and cyber (router) nodes. $\mathcal{E}$ is the set of edges including the edges within each layer and the edges that connect the two layers. $\mathbf{W}$ is the weighted adjacency matrix of the graphs. In the physical layer, the transmission lines are represented by the intra-edges (edges within one layer of the coupled graph). In the cyber layer, intra-edges are used to represent the network links connecting the routers. Finally, the inter-edges represent the coupling between the physical and cyber layers. In the physical layer, the weight values for the intra-edges

W_p are based on the line admittance values for the connected substations. If there is no connection, the weight value for that edge equals zero. For the inter-edges in the cyber layer and the intra-edges, the corresponding weight values W_c and W_{cp}, respectively, are binary values extracted from the adjacency matrix.

A. THE GNN MODEL

To implement the IDS, we utilize the GNN model, which is a supervised model that uses benign and malicious datasets for training and testing. The features of the model are the multi-modal CP features shown in Table 2 and the labels used for training are binary values indicating whether or not a given sample represents the system operating during normal or attack conditions. It should be highlighted that when the system is fully observable, all physical and cyber data are available for the GNN model training. In contrast, when the system is partially observable, only a subset of the cyber and physical data are given to the GNN model, which corresponds to the features collected from the packets and measurements provided by the critical loads and generators. All features are given to the model as unaltered numerical data except for the cyber feature indicating the packet protocol where one hot encoding is applied.

The choice of the GNN model is motivated by its effectiveness in capturing the spatial dependencies within the graph-structured data of the power system. The Chebyshev approximation used in our GNN implementation enables computational efficiency while retaining the ability to model topological relationships. This is particularly important for large-scale power systems, where the graph structure reflects interactions between buses, generators, and loads. Furthermore, GNNs provide a good balance between simplicity and performance, making them well-suited for the real-time detection of CP attacks. Fig. 6 illustrates the workflow of the GNN-based IDS. The system preprocesses input data (cyber features X_c, physical features X_p, and adjacency matrix W), constructs a graph, and applies GNN layers to extract spatial and topological features, producing a binary classification as benign or malicious.

The GNN model employs a multi-layer architecture that utilizes many stacked Chebyshev graph convolution layers that capture the graphs' spatial features through the graph convolution operation. The Chebyshev graph convolution layers are succeeded by a dense layer to predict probability that an attack has occurred for a given input. The prediction is then passed to the final output layer. The following details the operations carried out through the GNN model. The input layer receives the power system graph $\mathcal{G}$ with the node features listed in Table 2 that could belong to either benign samples, $\boldsymbol{X}_b$, or malicious samples, $\boldsymbol{X}_m$. L hidden Chebyshev graph convolution layers follow the input layer. Each hidden layer l has as input X^{l-1} and output of X^l. Each layer l captures the spatial features within the graph by performing the graph convolution operation, adding bias, and applying a ReLU function. The ReLU function produces the output

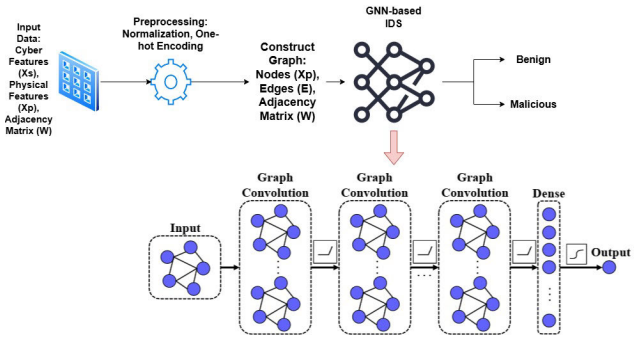


FIGURE 6. **Illustration GNN model architecture.**

tensor X^l of l such that

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

where $\boldsymbol{\mu}^l$ and $\boldsymbol{b}^l$ denote the Chebyshev coefficients and bias of l, respectively, and $*_G$ denotes the graph convolution operation. The graph convolution layers are followed by a dense layer that determines the probability of having an attacked sample where the decision is presented in the output layer. The dense layer takes the output X^L of the last hidden layer and results in the output of the following sigmoid function

$$\text{sigmoid}(W^L X^L + \boldsymbol{b}^L), \tag{3}$$

where W^L and $\boldsymbol{b}^L$ denote the feature weights and bias, respectively. The bias and activation functions enhance the detector's nonlinear capability. A final activation function with an output between 1 and 0 is used to set the output. To train the GNN detector and determine the model's parameters, a cross-entropy loss function is used, i.e.,

$$C(\tilde{y}, \Theta) = \frac{-1}{|\boldsymbol{X}_{\text{tr}}|} \sum_{\boldsymbol{X}_{\text{tr}}} \{y \log(\tilde{y}) + (1-y)\log(1-\tilde{y})\}, \tag{4}$$

where $|\boldsymbol{X}_{\text{tr}}|$ denotes the number of training samples. Θ depicts the trainable parameters. y and $\tilde{y}$ are the true and predicted labels of a given sample, respectively. An iterative gradient descent-based optimization algorithm is used to train the model, where training samples $\boldsymbol{X}_{\text{tr}}$ are split into equally-sized mini-batches and fed into the model over 128 epochs. To further clarify the CP fusion process within our GNN-based IDS, we provide pseudocode as shown in Algorithm 1 illustrating the data preprocessing, feature extraction, and model training steps.

B. BENCHMARK DETECTORS

The GNN-based IDS is evaluated against shallow, deep, supervised, and unsupervised benchmarks following the same feature representation and observability conditions. Supervised models are trained and tested on labeled benign and malicious data, while unsupervised models are trained on benign data and tested on both benign and malicious samples. The benchmarks include:

- SVM (Supervised): Separates data into classes using a hyperplane [49].

Algorithm 1 Cyber-Physical Data Fusion and GNN Training

Input: Cyber data $\mathcal{D}_c$, Physical data $\mathcal{D}_p$, Adjacency matrix $\mathbf{W}$, Labels $\mathbf{Y}$

Output: Trained GNN model for intrusion detection

procedure TrainGNN($\mathcal{D}_c$, $\mathcal{D}_p$, $\mathbf{W}$, $\mathbf{Y}$)

Step 1: Data Preprocessing

Extract cyber features $\mathbf{X}_c$ from $\mathcal{D}_c$

Extract physical features $\mathbf{X}_p$ from $\mathcal{D}_p$

Perform feature normalization on $\mathbf{X}_c$ and $\mathbf{X}_p$

Apply one-hot encoding for categorical cyber features

Step 2: Cyber-Physical Data Fusion

Define power system graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{W})$

Assign node attributes: $\mathbf{X} = [\mathbf{X}_c, \mathbf{X}_p]$ ▷ Fused features

Construct adjacency matrix $\mathbf{W}$ capturing intra- and inter-layer edges

Step 3: GNN Model Training

for $t = 1$ to T **do** ▷ Iterate over epochs

Compute graph convolution:

$$\mathbf{X}' = \text{ReLU}(\boldsymbol{\mu}^l *_{\mathcal{G}} \mathbf{X}^{l-1} + \mathbf{b}^l)$$

Update node representations using Chebyshev polynomials

Apply dropout regularization

end for

Compute final classification output using sigmoid:

$$\hat{\mathbf{Y}} = \text{sigmoid}(\mathbf{W}^L \mathbf{X}^L + \mathbf{b}^L)$$

Compute cross-entropy loss $C(\hat{\mathbf{Y}}, \mathbf{Y})$

Update parameters via gradient descent

return Trained GNN model

end procedure

- AutoRegressive Integrated Moving Average (ARIMA) (Unsupervised): Predicts normal operation patterns, detecting anomalies when the mean square error exceeds a threshold [50].
- FNN (Supervised): Learns patterns through stacked feedforward layers [51].
- LSTM-RNN (Supervised): Utilizes recurrent connections to retain past information [28].
- AutoEncoder with Attention (AEA) (Unsupervised): Reconstructs normal operation data via an attentive recurrent mechanism [28].

IV. EXPERIMENTAL RESULTS

For each power system (IEEE 14-bus and 30-bus systems), three detection models are built: cyber-only (C), physical-only (P), and CP, where CP fusion integrates both feature sets for improved detection. Both attack-specific and general models are developed to compare detection performance across multiple threats. The analysis evaluates whether certain attacks are better detected using cyber or physical features and examines the impact of full vs. partial observability. To determine the optimal hyper-parameters for the GNN-based IDS and benchmark models, we adopt a sequential grid search strategy [29]. Given the high dimensionality of the hyper-parameter space, an exhaustive grid search is computationally expensive. Instead, we optimize each hyper-parameter in a staged manner. In each stage, one hyper-parameter (e.g., number of GNN layers, hidden units, learning rate, batch size, activation function) is varied while keeping the others fixed at their current best values. The best-performing value is selected based on cross-validation performance, and this value is then fixed for subsequent stages. This process is repeated iteratively until all hyper-parameters are tuned. While this approach may not guarantee a globally optimal configuration, it significantly reduces computational complexity and has been shown to yield strong empirical performance [28]. The final selected hyper-parameters are summarized in Table 3.

TABLE 3. Optimal hyper-parameters for each model.

Model	Hyper-parameter	Optimal Value
ARIMA	Moving Average	0
	Diff Degree	1
SVM	Kernel	Sigmoid
	Gamma	Scale
	Regularization	1
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

A. PERFORMANCE METRICS

Detection performance is assessed using DR, FA, and F1-Score. The mathematical definitions of these metrics are provided in Table 4. DR measures the percentage of correctly identified malicious samples, FA quantifies the percentage

TABLE 4. Adopted metrics for IDS evaluation.

Metric	Formula
Detection Rate (DR)	$\mathrm{DR}(\%) = \frac{\mathrm{TP}}{\mathrm{TP+FN}} \times 100$
Precision (PR)	$PR(\%) = \frac{TP}{TP+FP} \times 100$
F1 Score ($F1$)	$F1(\%) = \frac{2\times PR\times DR}{PR+DR} \times 100$
False Alarm Rate (FA)	$\mathrm{FA}(\%) = \frac{\mathrm{FP}}{\mathrm{FP+TN}} \times 100$

of benign samples misclassified as malicious, precision measures the proportion of correctly identified attacks among all samples flagged as attacks, providing insight into the false alarm rate, and the F1-Score provides a balanced evaluation by combining precision and recall into a single metric, offering a concise measure of the trade-off between correctly identifying attacks which are the true positives and avoiding missed detections defined as false positives.

B. PERFORMANCE ANALYSIS AND BENCHMARK COMPARISON

Tables 5 and 6 summarize the performance of the attack-specific detectors, while Table 7 presents the performance of generalized detectors on the IEEE 14 and 30-bus CP power systems. The following key observations and comparisons are made:

- **GNN-Based IDS Superiority in DR, FA, and F1-Scores:** GNN-based IDSs consistently outperform benchmark models in all key metrics (DR, FA, and F1-Score) across both attack-specific and generalized detectors. As shown in Tables 5, 6, and 7, the GNN effectively models graph-structured data and captures spatial dependencies between cyber and physical layers, achieving up to 26% higher DR compared to traditional baselines. For example, in RW detection on the IEEE 30-bus system, the GNN-based IDS achieves the highest DR of 97.8% under full observability with CP fusion, compared to ARIMA (80.6%) and SVM (85.3%). In addition, GNN-based IDSs consistently achieve the highest F1-Scores across all attack types on both the 14-bus and 30-bus systems, as shown in Tables 5 and 6. For the 30-bus system, the GNN-IDS attains F1-Scores exceeding 96% under CP fusion, demonstrating excellent balance between detection rate and false alarm rate compared to traditional models whose F1-Scores often remain below 85%. Furthermore, the GNN-based IDS maintains competitive FA rates as low as 6.4% for generalized models on the 30-bus system under CP fusion, while ARIMA and SVM often exhibit higher FA rates exceeding 10%, potentially resulting in more false positives.
- Generalized Detector Performance: As summarized in Table 7, generalized IDSs trained on multi-attack CP

TABLE 5. Attack-specific detectors performance on 14-Bus system (%).

Attack	Model	Metric	Partial Observability			Full Observability		
			P	C	CP	P	C	CP
RW	ARIMA	DR	64.3	66.3	69.2	68.9	71.4	73.8
		F1	63.2	65.1	68.9	69.5	71.2	72.9
		FA	33.1	30.6	27.7	28.4	26.5	25.1
	SVM	DR	65.3	71.3	73.0	70.4	73.6	76.2
		F1	65.2	71.0	72.9	70.4	73.5	76.1
		FA	32.9	28.5	25.8	25.2	73.6	21.0
	FNN	DR	71.2	74.1	76.6	75.8	78.1	80.3
		F1	70.7	73.8	76.6	75.7	77.9	79.9
		FA	28.4	25.9	22.1	25.2	22.1	21.0
	RNN	DR	77.6	80.1	82.4	79.2	81.6	83.9
		F1	77.6	79.8	82.4	79.1	81.2	83.7
		FA	25.6	19.2	18.2	19.7	17.5	15.1
	AEA	DR	82.4	84.4	85.3	85.3	86.4	88.3
		F1	81.9	84.4	85.0	85.2	86.1	88.2
		FA	17.3	13.6	12.5	16.5	15.8	13.5
	GNN	DR	89.2	89.7	91.3	88.7	90.4	92.1
		F1	89.1	89.7	91.2	88.7	90.3	92.1
		FA	9.0	10.4	8.3	10.3	8.3	7.5
BF	ARIMA	DR	68.1	71.4	73.2	72.3	73.8	75.9
		F1	67.7	71.3	73.1	72.3	73.7	75.4
		FA	29.5	27.1	24.3	23.1	22.2	20.4
	SVM	DR	71.2	74.4	75.0	75.2	77.4	80.2
		F1	70.8	74.2	75.0	74.9	77.3	80.2
		FA	25.2	23.5	22.1	21.4	20.0	18.3
	FNN	DR	75.4	77.4	81.5	78.0	81.7	84.5
		F1	75.0	77.3	81.3	78.0	81.6	84.2
		FA	20.8	19.1	18.7	18.2	17.5	15.7
	RNN	DR	84.2	83.3	86.5	85.4	85.7	87.2
		F1	83.9	83.1	86.0	85.4	85.5	86.7
		FA	13.6	15.2	17.4	15.3	13.1	11.2
	AEA	DR	87.2	90.4	91.4	89.5	91.3	92.0
		F1	86.8	90.2	91.2	89.2	91.2	91.8
		FA	12.3	10.0	10.4	13.1	11.1	9.5
	GNN	DR	91.3	91.7	92.0	93.2	93.8	94.1
		F1	91.2	91.5	92.0	93.1	93.6	94.0
		FA	9.1	8.3	7.3	11.0	8.2	6.4
FDI	ARIMA	DR	79.3	72.2	80.4	81.3	75.2	83.9
		F1	78.8	72.1	80.0	80.8	75.2	83.5
		FA	22.4	26.8	20.1	20.9	24.3	18.4
	SVM	DR	81.2	77.3	83.1	83.8	78.1	85.7
		F1	80.7	76.8	83.0	83.8	77.8	85.2
		FA	19.5	23.9	17.2	18.3	22.3	15.1
	FNN	DR	83.8	80.1	86.1	86.2	81.3	88.3
		F1	83.7	79.6	86.0	85.8	81.3	88.2
		FA	17.6	19.5	15.1	15.2	17.5	13.5
	RNN	DR	85.0	82.7	88.3	89.8	85.7	92.3
		F1	84.9	82.3	87.9	89.6	85.7	92.1
		FA	14.2	16.7	12.5	14.6	15.3	12.4
	AEA	DR	88.7	85.3	89.7	90.7	87.2	94.9
		F1	88.2	85.1	89.3	90.2	87.2	94.5
		FA	11.8	13.1	10.0	12.3	13.1	11.9
	GNN	DR	91.3	89.7	92.4	93.4	90.1	97.8
		F1	91.2	89.6	92.3	93.3	90.0	97.7
		FA	8.3	10.5	8.8	7.2	8.2	6.1
RS	ARIMA	DR	68.8	72.4	74.3	71.8	75.9	87.4
		F1	68.4	72.3	74.3	71.4	75.5	87.1
		FA	34.8	29.2	24.6	28.5	30.1	26.4
	SVM	DR	70.2	73.4	78.0	73.5	79.7	88.8
		F1	70.1	73.0	77.8	73.1	79.7	88.6
		FA	32.7	29.6	27.9	26.2	22.3	20.1
	FNN	DR	71.5	77.0	79.7	75.9	83.3	92.1
		F1	71.2	77.0	79.4	75.6	82.9	91.9
		FA	28.4	23.4	21.6	24.8	18.4	16.5
	RNN	DR	84.1	82.1	86.8	85.3	89.4	93.8
		F1	83.8	82.1	86.8	85.1	89.3	93.6
		FA	15.1	18.3	14.4	18.1	16.8	14.9
	AEA	DR	86.5	88.1	90.3	90.6	92.8	94.7
		F1	86.2	87.7	89.9	90.4	92.5	94.4
		FA	13.5	10.1	9.4	13.7	11.4	10.5
	GNN	DR	89.3	90.1	92.7	91.8	94.1	96.8
		F1	89.2	90.1	92.5	91.7	94.0	96.6
		FA	10.4	8.4	5.2	9.5	8.1	7.4
BD	ARIMA	DR	75.3	81.1	85.3	78.2	83.1	91.1
		F1	75.0	81.0	85.0	77.7	82.6	90.7
		FA	25.4	21.2	13.1	23.4	11.4	14.8
	SVM	DR	76.6	77.3	87.2	80.7	78.9	93.5
		F1	76.4	76.9	86.8	80.3	78.4	93.4
		FA	24.1	21.2	11.4	21.7	21.3	12.0
	FNN	DR	80.1	81.5	88.8	83.1	84.6	94.2
		F1	79.6	81.2	88.4	83.0	84.4	93.8
		FA	19.0	18.6	9.5	16.8	17.4	10.2
	RNN	DR	83.2	84.5	90.3	86.2	88.3	97.2
		F1	83.0	84.1	90.1	86.0	88.0	97.0
		FA	14.5	12.5	8.1	13.8	12.8	8.9
	AEA	DR	84.2	86.0	92.1	86.8	89.7	97.6
		F1	83.9	85.6	91.8	86.8	89.4	97.6
		FA	11.7	9.2	6.8	11.5	10.5	9.3
	GNN	DR	88.2	90.2	93.7	91.4	93.7	98.2
		F1	88.1	90.2	93.5	91.2	93.4	98.1
		FA	10.2	6.0	4.9	8.6	9.1	5.4

TABLE 6. Attack-specific detectors performance on 30-Bus system (%).

Attack	Model	Metric	Partial Observability			Full Observability		
			P	C	CP	P	C	CP
RW	ARIMA	DR	68.2	71.5	74.8	73.1	78.4	80.6
		F1	68.1	71.0	74.7	72.8	78.1	80.5
		FA	29.8	27.8	24.9	25.8	21.1	18.0
	SVM	DR	69.3	74.0	79.0	75.5	80.2	83.7
		F1	69.2	73.9	78.6	75.3	79.8	83.7
		FA	29.1	24.7	21.2	22.1	17.2	15.5
	FNN	DR	76.0	78.6	82.4	78.4	83.9	87.1
		F1	75.6	78.2	82.0	78.2	83.8	86.6
		FA	25.4	20.0	17.1	18.6	15.7	13.8
	RNN	DR	82.2	84.5	87.3	84.5	88.8	91.2
		F1	81.8	84.3	86.9	84.4	88.7	90.7
		FA	21.5	17.2	14.2	15.6	13.2	10.7
	AEA	DR	85.1	87.5	89.9	87.1	90.6	93.7
		F1	85.0	87.4	89.6	87.0	90.1	93.5
		FA	15.7	11.3	9.0	13.2	10.5	8.5
	GNN	DR	93.2	94.1	96.0	91.2	94.1	97.8
		F1	93.1	94.1	95.8	91.1	94.0	97.7
		FA	7.8	5.4	3.9	6.2	4.1	2.1
BF	ARIMA	DR	72.1	74.2	79.1	74.6	78.6	81.2
		F1	72.0	74.2	79.0	74.5	78.1	81.1
		FA	26.2	22.1	19.2	19.4	17.1	14.9
	SVM	DR	75.5	79.6	84.5	78.2	72.1	84.0
		F1	75.2	79.2	84.5	77.7	72.0	83.9
		FA	24.4	21.2	17.3	17.6	15.8	14.1
	FNN	DR	81.8	84.3	85.1	81.4	87.2	89.5
		F1	81.5	84.0	85.0	81.1	87.0	89.3
		FA	18.9	15.6	14.0	15.5	12.9	10.4
	RNN	DR	86.7	89.7	89.8	89.5	92.6	93.5
		F1	86.3	89.3	89.7	89.3	92.1	93.4
		FA	11.8	10.8	10.1	12.8	10.9	8.5
	AEA	DR	88.2	91.8	93.9	92.0	94.4	95.1
		F1	88.1	91.4	93.9	91.9	94.3	94.7
		FA	9.1	8.4	9.5	10.7	9.8	7.8
	GNN	DR	93.1	94.1	95.6	96.1	98.1	99.4
		F1	93.0	94.1	95.4	96.0	98.1	99.2
		FA	7.8	5.4	4.1	5.2	3.3	2.4
FDI	ARIMA	DR	81.2	78.4	82.1	84.1	81.7	85.3
		F1	81.2	78.0	81.6	84.1	81.4	84.8
		FA	20.0	23.3	18.7	17.2	18.4	15.3
	SVM	DR	83.2	79.5	85.2	85.8	82.4	86.1
		F1	82.8	79.1	85.1	85.5	82.3	85.9
		FA	17.3	19.5	16.5	15.8	17.5	13.0
	FNN	DR	86.6	83.5	88.3	89.8	85.6	90.4
		F1	86.4	83.2	88.0	89.5	85.1	90.0
		FA	14.4	16.4	11.4	13.1	14.1	11.1
	RNN	DR	88.7	85.6	90.1	91.2	89.1	93.8
		F1	88.5	85.4	90.0	91.1	88.8	93.7
		FA	13.2	14.5	10.3	12.8	13.2	10.8
	AEA	DR	91.8	88.7	91.4	93.1	88.8	94.6
		F1	91.5	88.3	91.3	93.0	88.5	94.4
		FA	10.7	11.9	9.1	10.4	11.4	8.9
	GNN	DR	91.8	88.7	91.4	97.3	95.6	98.4
		F1	91.6	88.5	91.2	97.1	95.2	98.2
		FA	7.1	8.2	6.9	6.6	7.5	4.3
RS	ARIMA	DR	71.8	74.2	77.1	73.0	77.9	81.4
		F1	71.4	73.9	76.9	72.7	77.5	81.3
		FA	31.3	26.1	23.0	25.6	24.6	22.0
	SVM	DR	72.7	76.3	80.2	75.8	81.8	83.3
		F1	72.4	76.0	80.1	75.6	81.7	82.8
		FA	29.6	25.6	21.1	22.1	20.1	18.1
	FNN	DR	74.6	79.4	83.6	78.5	85.5	97.8
		F1	74.1	78.9	83.1	78.3	85.1	97.4
		FA	25.7	18.9	17.3	21.5	18.5	17.8
	RNN	DR	86.5	88.2	89.3	88.4	91.2	92.4
		F1	86.4	88.0	89.3	88.4	91.2	92.2
		FA	14.4	11.5	13.5	15.4	14.6	13.9
	AEA	DR	88.4	91.1	92.4	93.6	94.1	95.8
		F1	88.1	90.7	92.3	93.1	93.8	95.6
		FA	12.3	11.2	8.2	10.1	8.8	7.8
	GNN	DR	91.2	92.9	94.2	93.6	94.1	95.8
		F1	91.0	92.6	94.1	93.2	94.1	95.7
		FA	8.1	6.2	4.5	5.6	3.1	2.8
BD	ARIMA	DR	79.5	80.4	87.1	80.5	83.7	92.8
		F1	79.0	80.3	86.7	80.1	83.6	92.3
		FA	23.1	19.7	17.8	19.3	17.3	13.5
	SVM	DR	79.6	82.2	88.3	82.9	85.8	94.9
		F1	79.2	82.0	88.3	82.5	85.7	94.6
		FA	22.2	19.1	16.9	18.8	15.6	10.2
	FNN	DR	81.7	83.0	90.1	84.5	87.4	95.6
		F1	81.5	82.7	89.8	84.2	86.9	95.3
		FA	17.3	16.1	14.5	15.8	13.0	9.8
	RNN	DR	84.4	86.7	92.8	89.4	90.7	98.3
		F1	84.2	86.4	92.5	88.9	90.5	97.9
		FA	13.5	11.5	12.1	12.7	10.3	7.9
	AEA	DR	83.1	88.1	92.5	91.1	92.3	98.2
		F1	82.9	87.9	92.3	91.1	91.9	98.0
		FA	10.1	8.5	7.9	9.8	8.5	7.1
	GNN	DR	90.2	92.2	93.9	97.5	99.1	99.2
		F1	90.0	92.2	93.5	97.2	99.0	99.1
		FA	8.9	5.3	3.9	4.1	3.7	1.9

data demonstrate competitive performance compared to attack-specific models, reducing the need for retraining when new attack types emerge. Notably, the GNN-based IDS achieves superior F1-Scores exceeding 98% and maintains low FA rates (as low as 3.2%) on the 30-bus system under CP fusion. This highlights its strong generalization capability across diverse attacks, unlike traditional models such as ARIMA and SVM, which exhibit lower F1-Scores and higher FA rates.

- Feature Contributions and CP Fusion: Cyber features (e.g., network logs) are particularly effective in detecting RW, BF, RS, and BD attacks, while physical features (e.g., voltage and current anomalies) are more effective for FDI attacks. For instance, in the IEEE 14-bus system, FDI attack detection using only physical features achieves a DR of 86.5% with RNN, compared to 83.0% with cyber features alone. Overall, CP fusion improves detection performance by up to 16% compared to models using a single feature set.
- Impact of Partial Observability: Partial system observability results in only a 1-2% reduction in DR compared to full observability, demonstrating the robustness of the proposed IDSs. For instance, in the IEEE 14-bus system, the DR for RW detection using GNN decreases slightly from 92.1% (full observability) to 91.3% (partial observability).
- Architectural Scalability Across Different Networks: The proposed GNN-based IDS achieves improved detection performance on the larger IEEE 30-bus system compared to the IEEE 14-bus system. This improvement is not due to a change in features, both systems use the same set of cyber-physical features, but rather due to the increased number of nodes in the IEEE 30-bus system, which generates a richer dataset with more training samples. This richer dataset enables the model to capture more complex patterns and correlations.
- Robustness Across Network Sizes: Despite differences in network size and observability level, the model maintains consistent performance. Specifically, the fully observable IEEE 14-bus system (14 nodes) and the partially observable IEEE 30-bus system (11 observed nodes, representing 35% observability) yield detection results within a 1—4% margin. This close performance reflects the generalization capability and robustness of the proposed IDS across systems of different scales and visibility conditions.
- Empirical Performance with Larger Grids: GNN-based IDSs scale well with grid size, achieving higher DRs (up to 6% improvement) in the IEEE 30-bus system compared to the IEEE 14-bus system. For example, for BD attack detection, the GNN DR increases from 93.7% (IEEE 14-bus) to 98.2% (IEEE 30-bus) under full observability with CP fusion. While this study focuses on the IEEE 14-bus and 30-bus systems, our results demonstrate that the proposed GNN-based IDS is

TABLE 7. General detectors performance on 14 and 30-Bus systems (%).

Model	Metric	IEEE 14-Bus System						IEEE 30-Bus System					
		Partial Observability			Full Observability			Partial Observability			Full Observability		
		P	C	CP	P	C	CP	P	C	CP	P	C	CP
ARIMA	DR	76.2	72.1	78.5	80.3	78.3	82.6	80.6	75.8	83.5	83.5	82.1	85.7
	F1	76.0	71.8	78.2	80.1	77.9	82.1	80.4	75.7	83.3	83.3	81.8	85.6
	FA	23.5	30.4	20.3	18.1	20.0	16.4	20.8	12.7	18.4	15.7	17.3	14.2
SVM	DR	78.5	79.4	80.4	82.1	81.4	84.2	82.4	81.5	83.6	85.8	83.2	87.6
	F1	78.2	79.2	79.9	81.7	81.0	84.1	82.0	81.1	83.4	85.8	83.0	87.3
	FA	21.6	20.5	18.4	16.2	19.5	14.1	18.4	20.6	15.3	13.8	15.8	12.3
FNN	DR	81.3	80.3	84.1	84.8	83.0	87.9	84.1	83.4	87.6	87.7	86.8	89.8
	F1	81.0	79.8	83.8	84.8	82.8	87.5	84.0	83.2	87.4	87.7	86.5	89.8
	FA	18.7	17.3	12.5	15.9	17.3	13.2	15.5	17.0	10.7	12.9	14.0	10.6
RNN	DR	83.5	81.1	87.5	87.5	85.8	89.1	87.1	85.0	89.2	90.8	89.7	91.4
	F1	83.4	80.9	87.1	87.3	85.5	88.9	86.8	84.7	89.2	90.7	89.5	91.1
	FA	15.8	16.8	11.1	14.8	15.4	11.1	13.9	15.3	9.1	10.2	11.8	9.5
AEA	DR	86.3	85.2	89.1	90.2	88.2	91.5	90.2	88.4	91.2	92.2	90.8	93.3
	F1	86.2	85.1	88.7	89.7	87.7	91.0	90.1	88.2	91.0	92.0	90.6	92.9
	FA	13.2	12.9	9.7	11.6	12.7	10.0	11.1	14.2	8.4	8.1	10.8	7.8
GNN	DR	91.3	90.2	92.3	93.2	91.1	94.4	93.8	92.6	94.1	97.8	96.8	98.2
	F1	91.2	90.1	92.1	93.1	91.0	94.2	93.6	92.5	94.0	97.6	96.9	98.1
	FA	8.1	6.9	5.8	7.1	9.2	6.4	6.5	4.1	3.5	4.2	5.0	3.2

inherently scalable due to its graph-based architecture. The model can be extended to more complex systems, such as the IEEE 118-bus or real-world utility networks, by leveraging distributed GNN frameworks and hierarchical graph partitioning.

- Real-World Applicability: The proposed IDS is designed to reflect real SCADA environments through a cyber-physical testbed using OPAL-RT and Docker-based cyber emulation. While validated on IEEE test systems, its modular, graph-based architecture suggests adaptability to real utility networks. Practical deployment may require integration with SCADA protocols, model tuning on operational data, and consideration of real-time constraints.

V. CONCLUSION AND FUTURE WORKS

In this paper, we developed a CP power system testbeds based on IEEE 14-bus and 30-bus systems. We launched a set of attacks on these testbeds, including RW, BF, FDI, RS, and BD attacks. Benign and malicious data were collected under both full and partial observability conditions. A CP GNN-based IDS was implemented and evaluated against a comprehensive set of shallow and DL-based benchmark detectors. Our experiments demonstrated that adopting the GNN model improved the DR by up to 26% compared to benchmarks. Moreover, performing multi-modal CP data fusion for attack detection led to an improvement of up to 16% compared to using solely cyber or physical features. Additionally, the models achieved up to a 10% higher DR in the larger IEEE 30-bus test system compared to the smaller IEEE 14-bus system, attributed to capturing more spatial features. Partial observability resulted in a DR reduction of only 1–2% when compared to full observability. Our findings facilitate the further development of effective IDSs in CP power systems. Future works include extending the framework to large-scale power systems with distributed computation for efficient processing, integrating adaptive learning mechanisms to detect emerging attack patterns. An important direction for future work is to evaluate the system's performance against slow injection attacks, which are increasingly used in power systems to evade detection. These attacks will be simulated in the testbed by gradually altering measurements over time to mimic stealthy behavior. Also, future research could explore improvements such as online learning to adapt to evolving threats, generalization to unseen attack types without retraining, and optimization for real-time deployment in large-scale power systems using distributed GNN architectures and hardware acceleration.

ACKNOWLEDGMENT

An earlier version of this paper was presented in part at the 2023 IEEE SmartGridComm [1]. Part of this work was submitted as the M.S. thesis [2].

REFERENCES

[1] J. Sweeten, A. Takiddin, M. Ismail, S. S. Refaat, and R. Atat, "Cyber-physical GNN-based intrusion detection in smart power grids," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Glasgow, U.K., Oct. 2023, pp. 1–6.

[2] J. Sweeten, "Multi-model intrusion detection in cyber-physical power systems," M.S. thesis, Dept. Comput. Sci., Tennessee Tech Univ., Cookeville, TN, USA, 2023.

[3] B. G. de Soto, A. Georgescu, B. Mantha, Ž. Turk, A. Maciel, and M. S. Sonkor, "Construction cybersecurity and critical infrastructure protection: New horizons for construction 4.0," *J. Inf. Technol. Construction*, vol. 27, pp. 571–594, Jun. 2022.

[4] A. A. Elshazly, M. M. Badr, M. Mahmoud, W. Eberle, M. Alsabaan, and M. I. Ibrahem, "Reinforcement learning for fair and efficient charging coordination for smart grid," *Energies*, vol. 17, no. 18, p. 4557, Sep. 2024.

[5] A. Albaseer, N. Abdi, M. Abdallah, M. Qaraqe, and S. Al-Kuwari, "FedPot: A quality-aware collaborative and incentivized honeypot-based detector for smart grid networks," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 4, pp. 4844–4860, Aug. 2024.

[6] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/18/6225

[7] K. Prateek, M. Das, S. Surve, S. Maity, and R. Amin, "Q-secure-P^2-SMA: Quantum-secure privacy-preserving smart meter authentication for unbreakable security in smart grid," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 5, pp. 5149–5163, Oct. 2024.

[8] S. Aggarwal and G. Kaddoum, "Authentication of smart grid by integrating QKD and blockchain in SCADA systems," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 5, pp. 5768–5780, Oct. 2024.

[9] N. Perlroth, M. Scott, and S. Frenkel, "A cyberattack hits Ukraine, then spreads," New York Times, New York, NY, USA, Tech. Rep., 2017.

[10] ICSCER Team. (2016). *Cyber-Attack Against Ukrainian Critical Infrastructure*. ICS Alert (IR-ALERT-H-16-056-01). [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[11] J. R. Babu, "Design, implementation, and field-testing of distributed intrusion detection system for smart grid SCADA network," M.S. thesis, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, Iowa, Jan. 2021.

[12] 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, p. 826, May 2021.

[13] 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. 77572–77586, 2020.

[14] 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 Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2559–2574, Jul. 2021.

[15] 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, Feb. 2023.

[16] S. D. Roy, S. Debbarma, and A. Iqbal, "A decentralized intrusion detection system for security of generation control," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18924–18933, Oct. 2022.

[17] G. Efstathopoulos et al., "Operational data based intrusion detection system for smart grid," in *Proc. IEEE 24th Int. Workshop Comput.-Aided Model. Design Commun. Links Netw. (CAMAD)*, Limassol, Cyprus, Sep. 2019, pp. 1–6.

[18] 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 *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, Beijing, China, Oct. 2019, pp. 1–6.

[19] 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 Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021.

[20] A. Sahu et al., "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119118–119138, 2021.

[21] P. Ganesan and S. A. E. Xavier, "An intelligent intrusion detection system in smart grid using PRNN classifier," *Intell. Autom. Soft Comput.*, vol. 35, no. 3, pp. 2979–2996, 2023.

[22] W. Liao, A. Takiddin, M. Tariq, S. Chen, L. Ge, and Z. Yang, "Sample adaptive transfer for electricity theft detection with distribution shifts," *IEEE Trans. Power Syst.*, vol. 39, no. 6, pp. 7012–7024, Nov. 2024.

[23] A. Takiddin, M. Ismail, R. Atat, K. R. Davis, and E. Serpedin, "Robust graph autoencoder-based detection of false data injection attacks against data poisoning in smart grids," *IEEE Trans. Artif. Intell.*, vol. 5, no. 3, pp. 1287–1301, Mar. 2023.

[24] A. Takiddin, R. Atat, M. Ismail, K. Davis, and E. Serpedin, "A graph neural network multi-task learning-based approach for detection and localization of cyberattacks in smart grids," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Rhodes Island, Greece, Jul. 2023, pp. 1–5.

[25] A. Takiddin, R. Atat, M. Ismail, O. Boyaci, K. R. Davis, and E. Serpedin, "Generalized graph neural network-based detection of false data injection attacks in smart grids," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 7, no. 3, pp. 618–630, Jun. 2023.

[26] A. A. Elshazly, I. Elgarhy, M. Mahmoud, M. I. Ibrahem, and M. Alsabaan, "A privacy-preserving RL-based secure charging coordinator using efficient FL for smart grid home batteries," *Energies*, vol. 18, no. 4, p. 961, Feb. 2025.

[27] A. Takiddin, M. Ismail, and E. Serpedin, "Robust data-driven detection of electricity theft adversarial evasion attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 663–676, Jan. 2023.

[28] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4106–4117, Sep. 2022.

[29] 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 Syst. J.*, vol. 15, no. 3, pp. 4189–4198, Sep. 2021.

[30] A. A. Elshazly et al., "False data injection attacks on reinforcement learning-based charging coordination in smart grids and a countermeasure," *Appl. Sci.*, vol. 14, no. 23, p. 10874, Nov. 2024.

[31] *Power Systems Test Case Archive*. Accessed: Mar. 2025. [Online]. Available: http://labs.ece.uw.edu/pstca/

[32] S. Bornholdt and H. G. Schuster, *Handbook of Graphs and Networks: From the Genome to the Internet*. Hoboken, NJ, USA: Wiley, 2003.

[33] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

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

[35] D. Fasino et al., "Generating large scale-free networks with the Chung–Lu random graph model," *Networks*, vol. 78, no. 2, pp. 174–187, Dec. 2020.

[36] 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," *Sci. Rep.*, vol. 7, no. 1, p. 44499, Mar. 2017.

[37] 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 Informat. J.*, vol. 18, no. 1, pp. 21–27, Mar. 2017.

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

[39] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, "Inter-similarity between coupled networks," *Europhysics Lett.*, vol. 92, no. 6, p. 68002, Jan. 2011.

[40] R. Atat, M. Ismail, and E. Serpedin, "Limiting the failure impact of interdependent power-communication networks via optimal partitioning," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 732–745, Jan. 2023.

[41] X. Wang, Y. Koç, R. E. Kooij, and P. Van Mieghem, "A network approach for power grid robustness against cascading failures," in *Proc. 7th Int. Workshop Reliable Netw. Design Model. (RNDM)*, Munich, Germany, Oct. 2015, pp. 208–214.

[42] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electric Power Syst. Res.*, vol. 101, pp. 71–79, Aug. 2013.

[43] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Joint substation-transmission line vulnerability assessment against the smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 1010–1024, May 2015.

[44] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *Eur. Phys. J. B*, vol. 46, no. 1, pp. 101–107, Aug. 2005.

[45] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.*, vol. 87, no. 19, Oct. 2001, Art. no. 198701.

[46] K.-D. Lu, J.-C. Huang, G.-Q. Zeng, M.-R. Chen, G.-G. Geng, and J. Weng, "Multi-objective discrete extremal optimization of variable-length blocks-based CNN by joint NAS and HPO for intrusion detection in IIoT," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 4, pp. 4266–4283, Jul. 2025.

[47] G.-Q. Zeng, Y.-W. Yang, K.-D. Lu, G.-G. Geng, and J. Weng, "Evolutionary adversarial autoencoder for unsupervised anomaly detection of industrial Internet of Things," *IEEE Trans. Rel.*, pp. 1–15, Jan. 2025.

[48] J. Sweeten, A. Elshazly, A. Takiddin, M. Ismail, S. Refaat, and R. Atat. (2025). *Smartgrid-Cyberphysical-Attack-Dataset*. [Online]. Available: https://dx.doi.org/10.21227/symr-bz19

[49] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in *Proc. 5th Annu. Workshop Comput. Learn. Theory*, Pittsburgh, PA, USA, 1992, pp. 144–152.

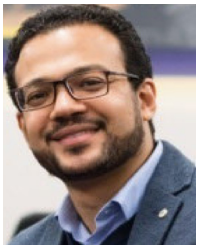
[50] V. Krishna et al., "ARIMA-based modeling and validation of consumption readings in power grids," in *Critical Information Infrastructures Security*. Cham, Switzerland: Springer, May 2016, pp. 199–210.

[51] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019.

JACOB SWEETEN received the M.S. degree in computer science from Tennessee Technological University in 2024. As part of the Cybersecurity Education, Research and Outreach Center (CEROC), Tennessee Technological University, he contributed to top-ranked Collegiate Penetration Testing Teams and helped create a cyber-physical grid testbed for intrusion detection research. His research interests include cyber-physical systems security, hardware-in-the-loop testbed development, machine learning for intrusion detection, and adversarial threats in power system environments.

AMR ELSHAZLY received the B.Sc. degree in mechanical engineering, the P.G.Dip. degree in computer science, and the M.Sc. degree in computer science from Tennessee Technological University, USA, in 2025, where he is currently pursuing the Ph.D. degree with the Department of Computer Science. He is a Graduate Research Assistant with the Department of Computer Science, Tennessee Technological University. He has published multiple peer-reviewed articles on secure energy management and federated learning for privacy preservation. His research interests include reinforcement learning, cybersecurity for cyber-physical systems, and AI-driven anomaly detection in smart grids and UAV systems.

ABDULRAHMAN TAKIDDIN (Member, IEEE) received the B.Sc. degree (Hons.) in information systems from Carnegie Mellon University, Pittsburgh, PA, USA, in 2014, the M.Sc. degree in data analytics from Hamad Bin Khalifa University, Doha, Qatar, in 2020, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2023. He is currently an Assistant Professor of electrical and computer engineering with the FAMU-FSU College of Engineering, Florida State University, Tallahassee, FL, USA. His research interests include machine learning, cyber-physical systems, smart grid, smart transportation, and security.



MUHAMMAD ISMAIL (Senior Member, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees in electrical engineering (electronics and communications) from Ain Shams University, Cairo, Egypt, in 2007 and 2009, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2013. He is currently the Director of the Cybersecurity Education, Research, and Outreach Center (CEROC) and an Associate Professor with the Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA. He was a co-recipient of the Best Paper Awards in the 2014 IEEE ICC, the 2014 IEEE GLOBECOM, the 2015 and 2024 SGRE, the 2016 Green, and the 2020 IEEE IS; and the Best Conference Paper Award from the IEEE Communications Society Technical Committee on Green Communications and Networking for his publication in the 2019 IEEE ICC. He was the Track Chair of the 2024 IEEE Globecom, the Track Co-Chair of the 2023 IEEE SmartGridComm and the 2017 and 2016 IEEE VTC, the Workshop Co-Chair of the 2018 IEEE Greencom, the Publicity and Publication Co-Chair of the 2015 CROWNCOM, and the Web-Chair of the 2014 IEEE INFOCOM. He was an Associate Editor of *IET Communications*, PHYCOM, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE INTERNET OF THINGS JOURNAL, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was an Editorial Assistant of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2011 to 2013. He has been a technical reviewer of several IEEE conferences and journals.

SHADY S. REFAAT (Senior Member, IEEE) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical engineering from Cairo University, Giza, Egypt, in 2002, 2007, and 2013, respectively. He has over 12 years of industrial experience, having served as an Engineering Team Leader, a Senior Electrical Engineer, and an Electrical Design Engineer across a range of electrical engineering projects. For more than 11 years, he was an Associate Research Scientist at the Department of Electrical and Computer Engineering, Texas A&M University at Qatar. He is currently a Reader of electrical power engineering with the University of Hertfordshire and an Adjunct Associate Professor with Texas A&M University. He has authored over 220 journals and conference publications, one patent, and one book. His research interests include electrical machines, power systems, smart grids, big data analytics, energy management systems, power grid reliability, electric machinery, fault detection, condition monitoring, and the development of fault-tolerant systems. Over the past decade, he has led and contributed to numerous scientific research projects, successfully translating research into practical solutions. He is a member of the Institution of Engineering and Technology (IET) and the Smart Grid Center-Extension in Qatar (SGC-Q).

RACHAD ATAT (Senior Member, IEEE) received the Bachelor of Engineering degree in computer engineering from Lebanese American University (LAU) in 2010, the master's degree in electrical engineering from the King Abdullah University of Science and Technology in 2012, and the Ph.D. degree (Hons.) in electrical engineering from the University of Kansas, KS, USA, in 2017. He was a Post-Doctoral Research Associate and an Assistant Research Scientist at Texas A&M University at Qatar in 2018 and 2022. He is currently an Assistant Professor with the Computer Science Department, LAU. He has authored numerous peer-reviewed journal articles and conference papers in the top venues. He is an investigator in grants on applications of AI in cybersecurity and networking, and leads a research team of undergraduate and graduate students with national and international collaborations.