Privacy-Preserving Federated Cybersecurity Analytics for Smart-Grid SCADA: Maintaining Controllability and Observability Under Coordinated Attacks

Zachary Etinge , Annamalai Annamalai , Mohamed Chouikha , Samir Abood *

Posted Date: 7 April 2026

doi: 10.20944/preprints202604.0302.v1

Keywords: smart grid; SCADA; cyber-physical systems (CPS); SSH (secure shell); ICMP (internet control message protocol)

 doi:10.20944/preprints202604.0302.v1

Article

Privacy-Preserving Federated Cybersecurity Analytics for Smart-Grid SCADA: Maintaining Controllability and Observability Under Coordinated Attacks

Zachary Etinge, Annamalai Annamalai, Mohamed Chouikha and Samir Abood *

Prairie View A&M University 1

* Correspondence: siabood@pvamu.edu

Abstract

Ensuring resilient controllability and observability in SCADA-based smart grids under coordinated cyberattacks remains a critical and unresolved challenge in modern cyber-physical power systems. This paper demonstrates the impact of coordinated cyberattacks on the stability and monitoring capabilities of SCADA-based smart grid systems in a controlled cyber-physical environment. An active cyber-physical testbed representing a multi-bus power system was created to be able to analyze how attacks targeting communication channels affect controllability and observability. Several attack scenarios were implemented, including remote access attacks via Secure Shell (SSH), Modbus/TCP flooding, and ICMP-based attacks, to monitor their impact on control actions, measure accuracy, and assess system responsiveness. To address these vulnerabilities, a SCADA-based cybersecurity monitoring system was implemented within the controlled testbed environment. The system analyzes SCADA operational logs from smart grid devices while packet-level network traffic is captured and examined using monitoring tools such as Wireshark. A central monitoring layer coordinates system-wide attack detection and response. System resilience was evaluated using controllability and observability matrix rank analysis, together with dynamic stability metrics during attack conditions. Experimental and simulation results show that coordinated cyberattacks lead to a significant degradation in system performance, with the average delay rising from 12 ms to 210 ms, the packet loss rate increasing to 15.5%, and the command execution error rate reaching 40%. Furthermore, the ranks of the controllability and observability matrices dropped from 4 to 2, indicating a critical partial loss of the system's control and monitoring capabilities. At the same time, the attack's impact on electrical properties remained limited to less than 2%.

Keywords: smart grid; SCADA; cyber-physical systems (CPS); SSH (secure shell); ICMP (internet control message protocol)

1. Introduction

The enhancement of traditional electrical power systems into smart grids has enabled improved monitoring, automation, and communication, with real-time monitoring and control systems that support transmission, distribution, and power generation, thereby strongly improving system efficiency and reliability [1–3]. Smart grid (SG) systems link electrical infrastructure with communication networks, real-time monitoring devices, and control systems to enable transmission, distribution, power generation, and real-time monitoring processes [1–3]. These features improve situational awareness, operational flexibility, and support more efficient energy management in modern power systems [2].

As smart grid technologies continue to enhance, cybersecurity (CS) has become a major concern [1,2,4]. The increasing dependence on communication networks and digital control systems opens

 doi:10.20944/preprints202604.0302.v1

the attack surface of power system infrastructures, making it more vulnerable to cyber threats [2,3]. Communication protocols such as Secure Shell (SSH), Modbus/TCP, and ICMP are widely used in modern industrial environments [3,5]. They may be compromised by launching cyberattacks such as Denial-of-Service (DoS), unauthorized access, and traffic flooding [5,6]. These harmful attacks can affect communication between SCADA systems and field devices, leading to delayed control actions, inaccurate measurement data, and reduced system reliability [6,7]

The integration of physical power system elements with communication and control technologies forms a cyber-physical (CPS) [8]. In such systems, physical processes, including power generation, transmission, and load control, are tightly connected to cyber components such as communication networks, sensors, and control methods. While CPS integration enables real-time monitoring and automated control. It also presents weaknesses where cyberattacks can propagate into physical system behavior, disrupting system stability, controllability, and observability [7,9].

The integration of smart grid infrastructure, cybersecurity issues, and cyber-physical system behaviors creates a highly networked environment in which communication reliability, system monitoring, and control performance are co-dependent [1,2]. Faults in communication networks caused by cyberattacks can reduce system observability and controllability, limiting operators' ability to accurately monitor system conditions and respond effectively to attacks [8,9]. Ensuring secure and reliable communication is standard for maintaining stable operation in modern smart grid environments [3,10].

To address these problems. Federated learning has developed as a promising approach for improving cybersecurity in compromised cyber-physical systems [11,12]. Federated learning is a decentralized machine learning technique in which multiple nodes collectively train a shared global model without exchanging raw data [11]. Instead of sending sensitive data to a central server, each node performs local training on its own dataset and shares only model parameters or updates with a control center [11,12]. These updates are combined to form an improved global model, which is then redistributed to all active nodes.

This approach is highly effective for smart grid environments, where data privacy, communication limitations, and system security are critical concerns [12,13]. By keeping data localized at SCADA nodes and network monitoring devices. Federated learning reduces the risk of data exposure while enabling system-wide detection of cyber threats [12]. The inherently distributed nature of federated learning enables scalable and adaptive cybersecurity monitoring across widely distributed infrastructure [13].

In this research, a SCADA-based smart grid testbed is used to experimentally evaluate the impact of communication-based cyberattacks on system performance. This study analyzes communication behavior, SCADA response, and system stability under attack conditions. A mathematical framework based on controllability and observability is used to interpret how cyberattacks affect system monitoring and control capabilities [8,9]. A federated cybersecurity perspective is incorporated to demonstrate how distributed learning techniques can enhance the resilience of cyber-physical smart grid systems [12,13].

The main contributions of this study are summarized as follows:

- Development of a real-time cyber-physical smart grid testbed integrated with a SCADA monitoring system
- Implementation of protocol-based cyberattack scenarios using SSH
- Integration of Wireshark for packet-level network monitoring and analysis
- Evaluation of system performance using communication metrics and controllability/observability analysis
- Experimental analysis of the interaction between cyberattacks and power system stability

To show a broad overview of the designed framework. The integration of smart grid systems, SCADA-based cyber systems, and federated learning for cybersecurity is illustrated in Figure 1. The smart grid physical system is connected to the SCADA-based cyber layer through a communication

 doi:10.20944/preprints202604.0302.v1

network. Forming a cyber-physical system. An SSH-based cyberattack is modeled to highlight weaknesses within the SCADA environment. To address these challenges, a federated learning framework is deployed across distributed SCADA nodes, enabling decentralized anomaly detection while preserving data privacy.

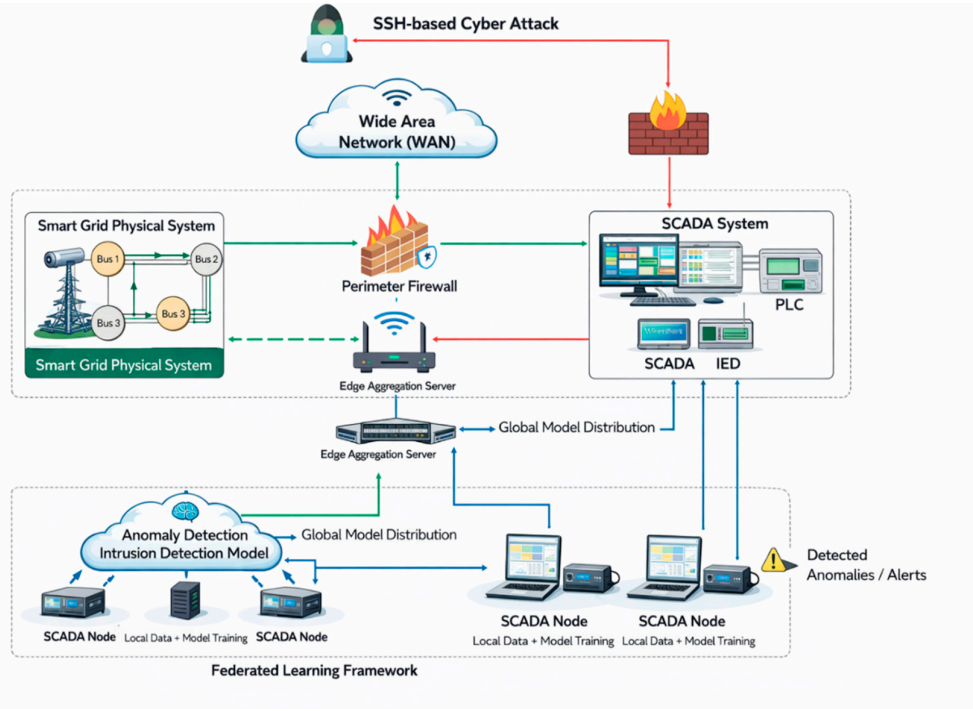

Figure 1. Overview of integrated smart grid, SCADA, and federated learning framework for cybersecurity.

2. Related Works

2.1. Smart Grid Cybersecurity

The advancement of power systems toward smart grids has enabled improved monitoring, automation, and operational efficiency through the integration of communication networks, intelligent sensing devices, and digital control platforms. Smart grids are widely characterized as cyber-physical systems (CPSs), in which physical infrastructure is tightly integrated with cyber components responsible for communication and control. Recent studies emphasize that while this incorporation strengthens system performance and flexibility, it also introduces meaningful cybersecurity challenges due to increased connectivity and interdependence between cyber and physical layers [14,15].

Current smart grid cybersecurity approaches expand beyond protecting individual components and instead require system-level protection strategies that account for SCADA systems, advanced metering infrastructure, distributed energy resources, and communication protocols. Guaranteeing reliability and real-time situational awareness under both normal and adversarial conditions remains a key focus in recent research [14].

2.2. SCADA System Vulnerabilities

SCADA systems play an important role in monitoring and controlling smart grid operations by enabling communication between field devices and centralized control centers. Recent studies identify SCADA systems as among the most exposed components in smart grid infrastructure due to their reliance on communication protocols and network connectivity [14,16].

 doi:10.20944/preprints202604.0302.v1

Previously, SCADA systems were designed with a greater focus on reliability and availability than on security. This has led to vulnerabilities such as weak authentication mechanisms, a lack of encryption, and exposure to unauthorized access. These weaknesses can allow attackers to manipulate system behavior, disrupt communication, degrade monitoring capabilities, and overall impact physical system operations [16].

2.3. Cyberattacks on Smart Grid Communication Networks

Communication networks are fundamental to smart grid operations. They allow the exchange of real-time data and control commands between system components. Studies highlight that cyberattacks targeting communication layers, including denial-of-service (DoS), distributed denial-of-service (DDoS), spoofing, and false data injection (FDI), can significantly disrupt system operation and decrease situational awareness [17].

The study further shows that enhanced detection methods, particularly those based on artificial intelligence and machine learning, have been widely explored to identify and reduce these threats. Many of these approaches are primarily observed through simulations or datasets rather than real-world applications, limiting their practical testing in cyber-physical environments [17].

2.4. Protocol-Based Attacks and Federated Learning Approaches

Operational control systems and smart grid environments rely on different communication protocols for data exchange and remote access. Protocol-level exposures present a significant attack surface. Attackers can exploit weaknesses in communication behavior, authentication mechanisms, and packet transmission processes to disrupt system functionality [15].

Recent studies have introduced federated learning as a promising approach for improving cybersecurity in networked smart grid environments. Federated learning enables decentralized model training across multiple nodes without sharing raw data, by improving privacy and scalability while supporting mutual anomaly identification across scattered systems [18].

2.5. Impact of Cyberattacks on System Stability, Monitoring, and Control

Cyberattacks on smart grids not only affect communication networks but also directly impact power system stability, monitoring accuracy, and control performance. Disturbances in communication can reduce system monitoring by delaying or manipulating measurement data, while also impacting controllability by interfering with command operations and control response [14].

Recent experimental studies point out the importance of observing cyberattacks in realistic testbed environments. The interaction between cyber and physical components can be observed in real time. These testbeds provide meaningful findings into how attacks influence system performance, response time, and operational reliability under practical conditions [19,20].

2.6. Research Gap and Contribution of This Work

Despite significant advancements in smart grid cybersecurity research, much of the existing research focuses more on conceptual analyses, simulation-based evaluations, or detection algorithm performance. These studies are key findings in threat classification and defense mechanisms. Few studies have experimentally investigated the real-time impact of protocol-based cyberattacks on SCADA-connected smart grid systems while clearly considering controllability and observability [17,20].

To address this gap, this research introduces a real-time experimental observation of cyberattacks on a smart grid laboratory testbed connected with a SCADA monitoring system. This study focuses on communication behavior under SSH-based interaction and ICMP flooding conditions, analyzing their effects on network traffic, system monitoring, and operational performance. Unlike prior studies, this work directly observes both controllability and observability

 doi:10.20944/preprints202604.0302.v1

within a real-time cyber-physical smart grid environment, providing practical insights into system behavior under attack conditions. Table 1 compares this work with existing smart grid cybersecurity studies.

Table 1. Comparison of this work with existing smart grid cybersecurity studies.

Ref.	Year	Main Focus	Attack / Threat Type	Methodology	Evaluation Environment	Controllability / Observability Consideration	Position relative to this work
[21]	2026	AI-driven cybersecurity framework for SCADA-integrated microgrids	DoS, ARP injection, plus broader discussion of FDI/replay	AI-based detection using SCADA and network features	Testbed / realistic scenarios	Not explicit	Strong real-time AI detection, but it does not directly formalize controllability/observability as the core evaluation lens.
[22]	2026	Maintaining smart-grid CPS controllability and observability under adversarial attacks	Telnet DoS, Modbus TCP flood, ICMP flood	SCADA-based real-time CPS + matrix-rank controllability/observability analysis	Real-time CPS + simulation (3-, 9-, 14-bus)	Explicitly addressed	Closest to the current manuscript, your new work extends toward privacy-preserving federated cybersecurity analytics and coordinated monitoring logic.
[23]	2025	AI-based cybersecurity assessment for renewable-integrated smart-grid SCADA systems	Telnet, DoS, Modbus/TCP, ICMP; protocol comparison across SSH/Telnet/HTTP/HTTPS	RNN–LSTM IDS + Wireshark + SCADA logs + protocol performance comparison	Real-world CPS testbed	Not explicit	Valuable for protocol/security benchmarking, but less centered on formal controllability/observability preservation.
[24]	2025	Digital-twin-driven smart grid with asynchronous federated learning and	Malicious station behavior, poisoning robustness, stale/non-IID updates	Blockchain + asynchronous FL + digital twin	Comparative experiments on heterogeneous devices and real power-grid datasets	Not addressed	Strong distributed learning architecture but not targeted to SCADA protocol attacks or operator visibility/control.

 doi:10.20944/preprints202604.0302.v1

		blockchain Privacy-preserving anomaly detection for smart-grid behavior monitoring					
[25]	2025		Cyber-physical / privacy attacks	K-means + LSTM + FL	Experimental evaluation on smart-grid behavior data	Not addressed	Strong privacy/anomaly results, but no direct analysis of SCADA testbed controllability/observability.
[26]	2025	Cybersecurity mitigation in smart electric microgrids	DoS, Telnet, Modbus-based intrusion scenarios	SCADA-based mitigation, protocol analysis, testbed monitoring	Real-time CPS microgrid testbed	Partial / indirect	Practical mitigation paper, but the present work is stronger in control-theoretic interpretation and federated perspective.
[27]	2025	Information security protection for digital power grids	Network intrusion/cyber attack classification	Improved BiLSTM-DNN + multi-head attention + FL	NSL-KDD-based experimental study	Not addressed	Strong FL+DL classifier, but dataset-driven and not validated on a real SCADA/CPS control platform.
[28]	2024	Privacy-preserving FL against poisoning attacks in smart grid	Model poisoning / malicious gradients	Homomorphic encryption + hierarchical aggregation + adaptive defense	FL experiments on MNIST/CIFAR-10 under malicious participants	Not addressed	Strong privacy and robustness at the FL layer, but not a SCADA power-system operational study.
[29]	2024	Holistic review of FL applications across energy services	Broad privacy/security/data-silo concerns	Review/taxonomy of FL methods in energy systems	Conceptual / literature review	Not addressed	Useful background on FL in energy, but not focused on protocol-level SCADA attacks or control visibility.
[30]	2024	Early detection of reconnaissance attacks in smart-grid environments	Reconnaissance attack	FSGD-based federated learning	Kaggle IoT-security dataset; client/server validation	Not addressed	Important for attack-stage detection, but dataset-based and not experimentally tied to SCADA control performance.
[31]	2024	Secure V2X energy	Trust, privacy, spoofing/SPOF-related	Blockchain + federated	Simulation using a real-world	Not addressed	Relevant to secure smart-grid transactions, but

 doi:10.20944/preprints202604.0302.v1

		trading in smart grids	platform threats, rather than SCADA intrusion detection	reinforcement learning	dataset + Avalanche implementation		outside SCADA attack monitoring and control-resilience scope.
[32]	2024*	Federated anomaly detection in smart power grids	Abnormal events/anomalies	FL-based anomaly detection with weighted monitoring indicators	Simulation/ analysis for grid monitoring categories	Not addressed	Useful anomaly-detection baseline but lacks real-time cyber-physical experimentation and explicit control-theoretic treatment.
[33]	2024	FL for cybersecurity and trustworthiness in 5G/6G networks	Inference, poisoning, insider/outsider FL attacks	Comprehensive survey	Review	Not addressed	Broader-domain FL security survey; indirectly useful for threat/defense framing, not for smart-grid SCADA validation.
[34]	2024	FL in urban sensing systems with attacks, defenses, and incentives	Inference attacks, poisoning attacks	Comprehensive survey	Review	Not addressed	Provides a broader FL attack/defense context but is only indirectly relevant to smart-grid SCADA cybersecurity.
This work	-	Privacy-preserving federated cybersecurity analytics for SCADA-based smart grids under coordinated attacks	SSH, Modbus/TCP flooding, ICMP-based attacks	Real-time SCADA/CPS testbed + federated-learning perspective + controllability/observability matrix analysis + Wireshark-assisted monitoring	Real-time laboratory smart-grid/SCADA testbed	Explicitly addressed	Distinguishes itself by jointly studying protocol attacks, SCADA monitoring, and control-theoretic resilience in one real-time framework.

3. Methodology

3.1. Smart Grid Cyber-Physical Testbed

To analyze the impact of cyberattacks on smart grid operations, a real-time cyber-physical smart grid testbed was implemented using a SCADA monitoring platform. The testbed integrates electrical power system components with communication networks to emulate the behavior of a modern smart

 doi:10.20944/preprints202604.0302.v1

grid environment. The system includes multiple components such as an integrated network, transmission lines, consumer loads, and a wind power generation unit.

The SCADA interface provides real-time monitoring of system parameters, including power flow, voltage levels, and current measurements. Through this interface, system operators can observe system conditions and control various components within the smart grid infrastructure. Figure 2 illustrates the smart grid SCADA monitoring interface used in this study.

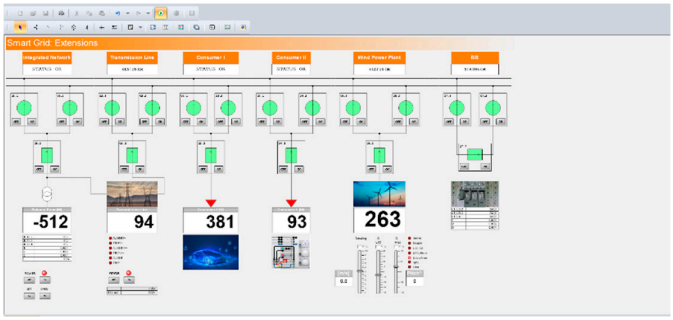

Figure 2. Smart grid SCADA monitoring interface used in this study.

3.2. SCADA Server Monitoring Interface

In addition to the system overview interface, a cybersecurity monitoring interface was implemented to observe system measurements and control signals during cyberattack scenarios. The interface provides real-time measurements of system voltage and current values across different phases of the power system.

The SCADA server allows technicians to monitor system behavior and control the power system through switching operations. This interface plays an important role in observing the effects of cyberattacks on system monitoring capability and communication reliability. Figure 3 presents the cybersecurity server interface used to observe system measurements and control signals during the experiments.

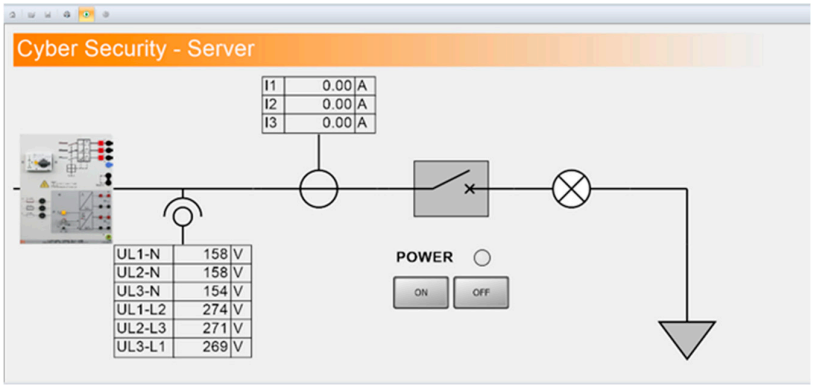

Figure 3. The cybersecurity server interface was used to observe system measurements and control signals during the experiments.

3.3. Proposed Power System

Figure 4 shows a one-line diagram of the proposed power system. A three-bus smart-ring power system is proposed in this work and illustrated in Figure 5a. It comprises a primary generator and two loads. The main generator supplies the system with electrical power. Load 1 is powered and connected to renewable sources. A hybrid renewable energy system includes a wind turbine that serves as the on-site power source and is connected to the system via bus 3.

 doi:10.20944/preprints202604.0302.v1

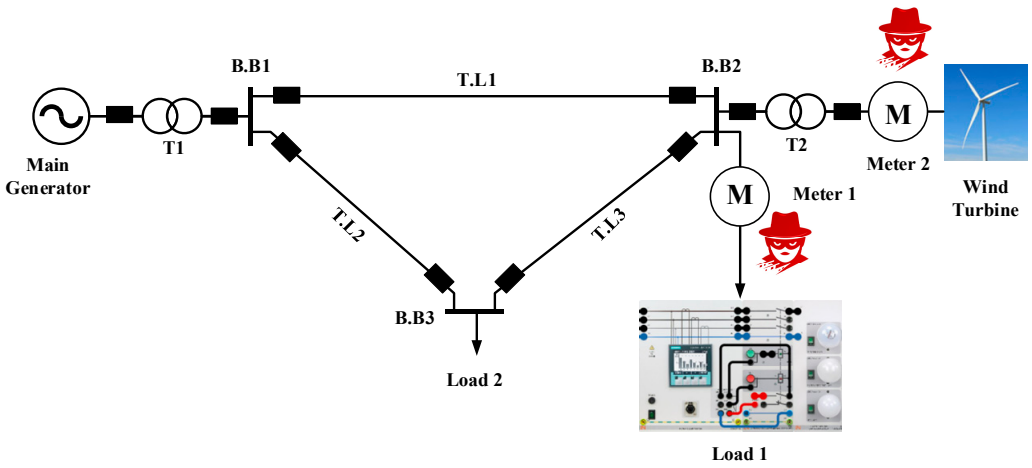

Figure 4. One-line diagram of the proposed power system.

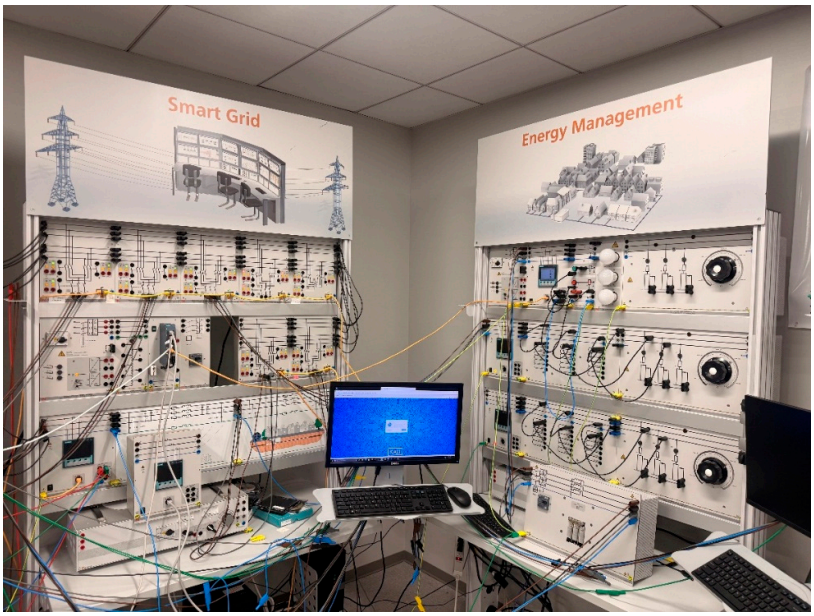

Figure 5. The physical smart grid laboratory setup used during the experimental evaluation.

3.4. Physical Smart Grid Laboratory Testbed

The experimental platform used in this research consists of a physical smart grid laboratory setup that integrates power system modules, communication devices, and a SCADA monitoring workstation. The laboratory environment enables controlled experimentation on cyber-physical power system behavior under cybersecurity attack scenarios. Figure 5 shows the physical smart grid laboratory setup used during the experimental evaluation.

The smart grid training system includes multiple electrical modules representing transmission lines, loads, and power generation components. These modules are interconnected via measurement units and communication interfaces, enabling real-time monitoring via the SCADA platform.

Network connectivity between the smart grid devices and the monitoring workstation is provided via a Siemens industrial router, enabling communication across the cyber-physical testbed. This communication infrastructure allows cyberattack experiments to be conducted while observing their impact on power system monitoring and control behavior. Figure 6 shows the architecture of the cyber-physical smart grid testbed used for cybersecurity experiments.

 doi:10.20944/preprints202604.0302.v1

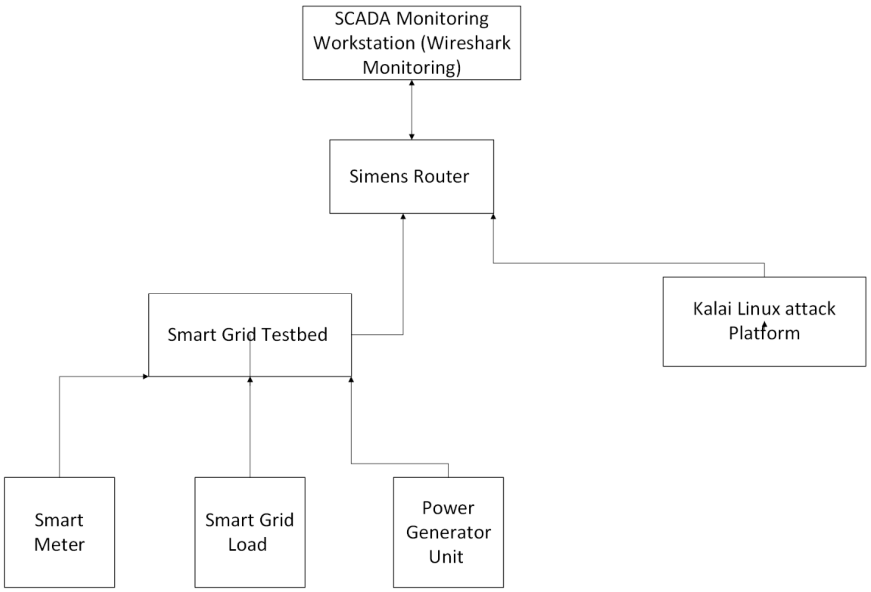

Figure 6. Architecture of the cyber-physical smart grid testbed used for cybersecurity experiments.

3.5. Communication Network and Cyberattack Implementation

To evaluate the effect of cybersecurity attacks on the smart grid system, a communication network was established between the smart grid laboratory testbed and the SCADA monitoring workstation. The communication infrastructure was enabled through a Siemens industrial router, which provides network connectivity between the smart grid components and the monitoring computer.

The router was accessed and configured through its assigned IP address using the laboratory workstation. Once the router was powered on and initialized, network connectivity was verified with Wireshark, a packet-analysis tool for monitoring network traffic. Wireshark was used to confirm that the system was actively transmitting and receiving network packets under normal operating conditions before cyberattack experiments were performed.

After verifying network connectivity, a virtual machine running Kali Linux was launched on the laboratory workstation. Kali Linux was used as the attack platform to generate protocol-based cybersecurity attacks against the smart grid communication network.

The PuTTY software tool was then used to initiate remote communication sessions and configure the system's communication protocol. In this study, only the Secure Shell (SSH) protocol was utilized to establish secure remote connections between the monitoring workstation and the smart grid components.

Using PuTTY as shown in Figure 7, SSH-based sessions were initiated to enable controlled interaction with the system. These sessions served as the basis for generating protocol-based cyberattack traffic directed at the smart grid communication network.

 doi:10.20944/preprints202604.0302.v1

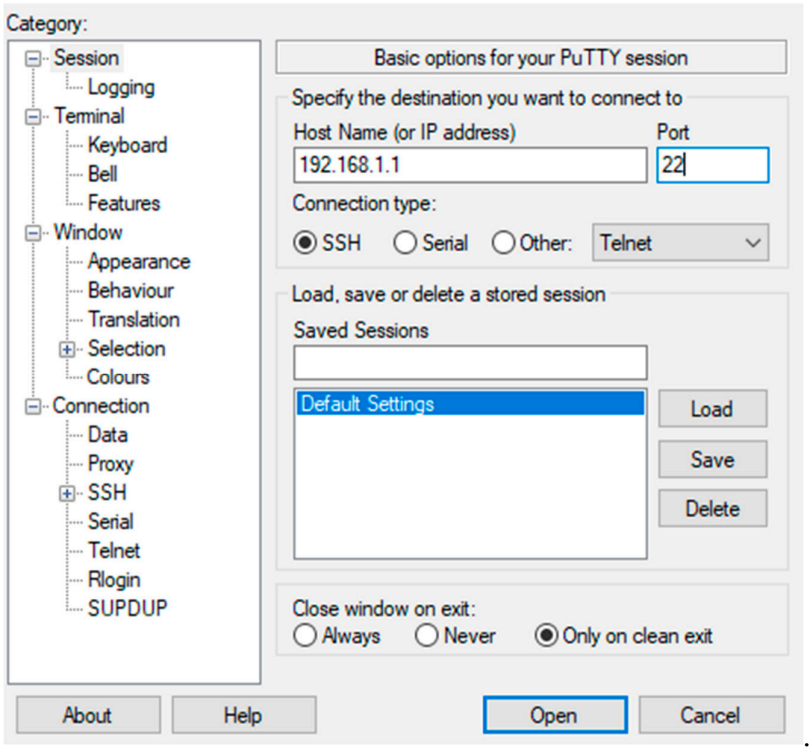

Figure 7. illustrates the PuTTY configuration interface used to initiate the protocol sessions with the smart grid communication network.

During the attack experiments, Wireshark was employed to capture and analyze network packets under both normal operating conditions and during the SSH-based cyberattack. Packet analysis enabled the identification of abnormal traffic patterns introduced by the attack and provided insight into how communication disruptions affected system monitoring and control performance.

3.6. Cyberattack Implementation

Within the configured environment, network security tools were used to simulate cyberattacks on the smart grid communication infrastructure. Communication sessions with the target devices were established using PuTTY, which enabled secure remote access via the Secure Shell (SSH) protocol during the experimental scenarios. In addition, the hping3 network testing tool available in the Kali Linux environment was used to generate Denial-of-Service (DoS) traffic against the target device, evaluating the system's response to abnormal network conditions.

3.7. System Monitoring and Data Collection

System behavior was monitored during both normal network operation and cybersecurity attacks to evaluate the impact of communication disruptions on smart grid operations. Network activity within the communication infrastructure was captured and analyzed using Wireshark, which provided real-time packet inspection and protocol analysis throughout the experiments.

Wireshark was used to observe packet transmission patterns, protocol activity, and communication traffic between the smart grid devices and the monitoring workstation. Captured network traffic allowed verification of normal communication behavior before initiating attack scenarios and provided visibility into network activity during the cybersecurity experiments. Figure 8 shows a Wireshark capture of normal Modbus/TCP communication between the SCADA monitoring workstation and the smart grid device under normal operating conditions.

 doi:10.20944/preprints202604.0302.v1

In addition to monitoring network traffic, system control behavior was observed through the SCADA monitoring interface. The SCADA platform enabled switching operations on electrical loads connected to the smart grid testbed. A lighting load connected to the system was used as an operational indicator of system response.

During the experiments, switching commands were issued via the SCADA interface under both normal network conditions and simulated cyberattack scenarios. The system's response to these commands was monitored during data collection to assess how communication disruptions affect the system's control and monitoring capabilities.

No.	Time	Source	Destination	Protocol
33024	25.226629	192.168.1.20	192.168.1.10	TCP
33025	25.226629	192.168.1.20	192.168.1.10	Modbus/TCP
33026	25.226698	192.168.1.10	192.168.1.20	Modbus/TCP
33027	25.228777	192.168.1.20	192.168.1.10	TCP
33028	25.228777	192.168.1.20	192.168.1.10	Modbus/TCP
33029	25.229077	192.168.1.10	192.168.1.20	Modbus/TCP
33030	25.231136	192.168.1.20	192.168.1.10	TCP
33031	25.231136	192.168.1.20	192.168.1.10	Modbus/TCP
33032	25.231214	192.168.1.10	192.168.1.20	Modbus/TCP
33033	25.233208	192.168.1.20	192.168.1.10	TCP
33034	25.233208	192.168.1.20	192.168.1.10	Modbus/TCP
33035	25.233281	192.168.1.10	192.168.1.20	Modbus/TCP
33036	25.235289	192.168.1.20	192.168.1.10	TCP
33037	25.235289	192.168.1.20	192.168.1.10	Modbus/TCP
33038	25.235362	192.168.1.10	192.168.1.20	Modbus/TCP
33039	25.237375	192.168.1.20	192.168.1.10	TCP
33040	25.237375	192.168.1.20	192.168.1.10	Modbus/TCP
33041	25.237447	192.168.1.10	192.168.1.20	Modbus/TCP
33042	25.239443	192.168.1.20	192.168.1.10	TCP
33043	25.239443	192.168.1.20	192.168.1.10	Modbus/TCP
33044	25.239485	192.168.1.10	192.168.1.20	Modbus/TCP
33045	25.241480	192.168.1.20	192.168.1.10	TCP
33046	25.241480	192.168.1.20	192.168.1.10	Modbus/TCP
33047	25.241553	192.168.1.10	192.168.1.20	Modbus/TCP

Figure 8. Wireshark capture shows normal Modbus/TCP communication between the SCADA monitoring workstation and the smart grid device under normal operating conditions.

3.8. Mathematical Modeling and Controllability/Observability Analysis

To evaluate the impact of cyberattacks on smart grid performance, the implemented system is modeled as a simplified 3-bus cyber-physical system (CPS). This model captures the interaction between system states, SCADA control actions, and measured outputs under both normal and compromised operating conditions. [20–22].

The system dynamics are represented in state-space form as:

$$x(k+1) = Ax(k) + Bu(k) + a_u(k) \quad (1)$$

$$y(k) = Cx(k) + a_y(k) \quad (2)$$

where $x(k)$is the state vector, $u(k)$is the control input vector, and $y(k)$is the measured output vector. The terms $a_u(k)$ and $a_y(k)$ represent actuator-side and sensor-side attack signals, respectively, modeling the effect of cyberattacks on control commands and measurement data. **[19–22]**.

For the simplified 3-bus smart grid system, the state vector is defined as:

$$y(k) = \begin{bmatrix} v_1(t) \\ v_2(t) \\ v_3(t) \\ I_1(t) \\ I_2(t) \\ I_3(t) \end{bmatrix} \quad (3)$$

since the SCADA system provides real-time voltage and current measurements.

 doi:10.20944/preprints202604.0302.v1

3.8.1. Controllability Analysis

The controllability of the system is evaluated using the controllability matrix:

$$C = [B\ AB\ A^2B\ \dots\ A^{N-1}B] \quad (4)$$

The system is considered controllable if:

$$rank(C) = n \quad (5)$$

where n is the number of system states. **[21]**.

3.8.2. Observability Analysis

Similarly, the observability of the system is evaluated using the observability matrix:

$$O = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{N-1} \end{bmatrix} \quad (7)$$

The system is considered observable if:

$$rank(O) = n \quad (8)$$

Under normal operating conditions, the SCADA monitoring system can reliably transmit control commands and receive measurement data, ensuring full controllability and observability of the system. During cyberattacks, packet loss, delays, or manipulation of control signals may degrade system performance. As a result, the reliable controllability and monitoring of a system may be decreased under attack conditions [19–22].

3.9. Federated Cybersecurity Modeling

To enhance cyberattack detection and improve system resilience, a federated learning framework is integrated into the smart grid cybersecurity architecture. In this approach, distributed nodes, such as SCADA devices and network monitoring units, collaboratively train a global intrusion detection model without sharing raw data [7–9].

Let K denote the number of distributed nodes in the system. Each node k maintains a local dataset D_k, defined as:

$$D_k = \{(x_i, y_i) \mid i = 1, \dots, n_k\} \quad (9)$$

where $x_i \in \mathbb{R}^d$ represents feature vectors derived from network traffic, protocol behavior, and system measurements, and $y_i \in \{0,1\}$ represents the classification label, where 0 corresponds to normal operation, and 1 corresponds to anomalous or malicious activity.

The total number of samples across all nodes is given by:

$$N = \sum_{k=1}^{K} n_k \quad (10)$$

Each node trains a local model using its private dataset. The local objective function at the node k is defined as:

$$F_k(w) = \frac{1}{n_k} \sum_{i \in D_k} l(w; x_i, y_i) \quad (11)$$

where w represents the model parameters and $\ell(\cdot)$ is the loss function.

 doi:10.20944/preprints202604.0302.v1

During each communication round t, the global model w^t is transmitted to participating nodes. Each node updates its local model using gradient descent:

$$w_k^{t+1} = w^t - \eta \nabla F_k(w^t) \quad (12)$$

where $\eta$is the learning rate.

After local training, the updated models are sent to a central aggregator, where they are combined using the Federated Averaging (FedAvg) algorithm **[7]**:

$$F(w) = \sum_{k=1}^{K} \frac{n_k}{N} F_k(w) \quad (13)$$

The corresponding global objective function is expressed as:

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{N} w_k^{t+1} \quad (14)$$

This federated learning framework enables collaborative model training across distributed smart grid nodes while preserving data privacy, as raw cyber-physical system data remain local and are not transmitted. The resulting global model is deployed at each node to perform real-time intrusion detection and identify abnormal system behavior

4. Experimental Results and Analysis

4.1. Normal System Operation

Under normal operating conditions, the smart grid system exhibited stable, reliable performance. Network traffic analysis showed steady Modbus/TCP communication between the SCADA workstation and the smart grid device, with no abnormal packet delays or traffic anomalies observed. From an operational perspective, SCADA control commands were performed successfully. Switching actions resulted in immediate and correct responses from the connected lighting load, confirming proper system controllability and responsiveness. These results confirm that both communication and control functions were operating under normal conditions, establishing a baseline for comparison with the cyberattack scenarios.

4.2. SSH-Based Attack

Following baseline system operation, the network was observed during an SSH-based cyberattack. As shown in Figure 9, the Wireshark capture shows a noticeable increase in SSH packets exchanged between the monitoring workstation and the smart grid device during the attack period.

No.	Time	Source	Destination	Protocol
5865	651.279301	192.168.1.10	192.168.1.1	SSHv2
5867	651.285404	192.168.1.1	192.168.1.10	SSHv2
5869	651.297879	192.168.1.10	192.168.1.1	SSHv2
5870	651.300699	192.168.1.1	192.168.1.10	SSHv2
5871	651.303266	192.168.1.10	192.168.1.1	SSHv2
5873	651.796073	192.168.1.1	192.168.1.10	SSHv2
5874	651.831068	192.168.1.10	192.168.1.1	SSHv2
5875	651.834308	192.168.1.1	192.168.1.10	SSHv2
6146	687.059991	192.168.1.10	192.168.1.1	SSHv2
6147	687.070348	192.168.1.1	192.168.1.10	SSHv2
6148	687.070592	192.168.1.10	192.168.1.1	SSHv2
6149	687.080496	192.168.1.1	192.168.1.10	SSHv2
6210	695.444510	192.168.1.10	192.168.1.1	SSHv2
6212	695.665825	192.168.1.1	192.168.1.10	SSHv2

Figure 9. Wireshark capture showing increased SSH traffic during the cyberattack scenario, illustrating sustained communication between the SCADA workstation and the smart grid device under elevated network load.

 doi:10.20944/preprints202604.0302.v1

Despite the elevated traffic, the communication channel remained stable, and packet captures continued to load without excessive delay. This indicates that the network maintained operational integrity under increased traffic conditions.

In addition to the observed SSH traffic, further analysis of the Wireshark capture revealed ICMP packets during the attack period, as shown in Figure 10. These packets indicate that the attack introduced additional network activity beyond the expected SSH communication.

No.	Time	Source	Destination	Protoco
3065…	16.043283	192.168.1.10	192.168.1.20	ICMP
3065…	16.043303	192.168.1.10	192.168.1.20	ICMP
3065…	16.043323	192.168.1.10	192.168.1.20	ICMP
3065…	16.043344	192.168.1.10	192.168.1.20	ICMP
3065…	16.043365	192.168.1.10	192.168.1.20	ICMP
3065…	16.043385	192.168.1.10	192.168.1.20	ICMP
3065…	16.043405	192.168.1.10	192.168.1.20	ICMP
3065…	16.043428	192.168.1.10	192.168.1.20	ICMP
3065…	16.043448	192.168.1.10	192.168.1.20	ICMP

Figure 10. Wireshark captures show ICMP packet activity during the cyberattack scenario, indicating additional network load that contributes to system performance degradation.

The increase in ICMP traffic indicates the presence of a flooding or probing mechanism, illustrating how cyberattacks can generate multiple types of network traffic simultaneously, increasing the demand on the network. System performance was further observed through control operations. Switching commands issued through the SCADA interface remained operational. Although communication was functional, noticeable delays were observed during control operations. In several instances, the system exhibited inverse behavior, in which issued commands did not correspond to the expected response. These inconsistencies indicated reduced control reliability under the attack conditions, even though the system maintained partial operational capability.

Overall, the SSH-based communication maintained partial system functionality under abnormal network traffic conditions, but performance declined noticeably. Communication delays and unstable control responses were observed, including instances of inverse behavior in command execution. While the encrypted, connection-based nature of SSH provided some resistance, the results indicated that system performance and control reliability were still affected under attack conditions.

4.3. Comparative Performance and Power Flow Analysis

To further observe the impact of the SSH-based cyberattack on both communication performance and physical system behavior, a combined analysis of network activity and smart meter measurements was conducted.

From a communication perspective, the SSH-based attack introduced increased network traffic and noticeable delays, as observed in the Wireshark analysis. Although SCADA commands remained functional, inconsistent control responses were observed, including instances of inverse behavior in command execution.

To assess the effect on the physical layer, electrical measurements were collected from two smart meters (Meter 1 and Meter 2), under both normal operating conditions and during the SSH-based attack. The recorded parameters include phase voltage(V_PH(V)), line voltage(V_Line(V)), current(I), active power(P(W)), reactive power(Q(var)), apparent power(S(VA)), system frequency (Hz), and power factor.

 doi:10.20944/preprints202604.0302.v1

Table 2. Electrical measurements at Meter 1 and Meter 2 under normal operating conditions.

Parameter	Meter 1 (192.168.1.20)	Meter 2 (192.168.168.31)
V_PH(V)	114 – 114 – 114	114 – 114 – 114
V_Line(V)	198 – 198 – 198	198 – 198 – 198
I (A)	0.19	0.34
P (W)	14	-14
Q (var)	-1	-116
S (VA)	21	116
F (Hz)	60.00	60.00
Power Factor	0.68	0.12

Table 3. Electrical measurements at Meter 1 and Meter 2 during SSH-based cyberattack conditions at M1.

Parameter	Meter 1 (192.168.1.20)	Meter 2 (192.168.168.31)
V_PH(V)	108-115-113	110-112-113
V_Line(V)	191-197-194	191-197-194
I (A)	0.19-0.00-0.00-0.19	0.34-0.35-0.35-0.00
P (W)	14	-14
Q (var)	-1	-115
S (VA)	21	116
F (Hz)	59.99	59.98
Power Factor	0.68	0.12

Table 4. Electrical measurements at Meter 1 and Meter 2 during SSH-based cyberattack conditions at M2.

Parameter	**Meter 1 (192.168.1.20)**	**Meter 2 (192.168.168.31)**
V_PH(V)	108-114-113	108-111-112
V_Line(V)	192-197-194	190-196-193
I (A)	0.2-0.00-0.00-0.19	0.34-0.34-0.34-0.00
P (W)	14	-14
Q (var)	-1	-115
S (VA)	21	116
F (Hz)	59.99	59.98
Power Factor	0.68	0.12

Table 5. Percentage deviation of electrical parameters under cyberattack conditions.

Parameter	**Meter**	**Normal**	**Attack**	**Deviation (%)**
Vph avg (V)	Meter 1	114	112	-1.75%
Vph avg (V)	Meter 2	114	111.67	-2.05%
Frequency (Hz)	Meter 1	60.00	59.99	-0.017%
Frequency (Hz)	Meter 2	60.00	59.98	-0.033%
Reactive Power (var)	Meter 2	-116	-115	+0.86%

A comparison of the measurements indicates that the SSH-based cyberattack had minimal impact on the system's physical operation. Voltage levels at both meters remained stable, with only

 doi:10.20944/preprints202604.0302.v1

minor variations observed between normal and attack conditions. Current measurements show small changes, indicating that the load demand was not significantly affected.

Active and reactive power values at both Meter 1 and Meter 2 remained consistent, with only slight changes observed during the attack scenario. Apparent power values followed a similar pattern, confirming that overall power flow in the system was preserved.

System frequency remained stable at approximately 60 Hz for both meters, showing that grid synchronization was not disrupted. Power factor values also remained unchanged, demonstrating that the efficiency of power delivery was maintained.

These results confirm that the SSH-based cyberattack increased network activity and introduced moderate communication delays. Its impact on the physical power system was minor. The smart grid maintained stable electrical operation under the attack scenario. These results highlight the resilience of the smart grid system, in which attacks in the cyber layer do not significantly propagate to the physical power system.

4.4. Cyberattack Scenarios Definition

4.4.1. Scenarios

Four distinct operational states were defined to analyze the impact of cyberattacks on SCADA performance. Table 6 represents the first state, which represents normal operation with a packet rate of 120 pkt/s. In comparison, the remaining states represent various attack scenarios using SSH at 350 pkt/s and ICMP at 1200 pkt/s, as well as a coordinated attack that combines multiple protocols. The packet rate for each state was measured with Wireshark to enable a precise quantitative comparison across conditions.

Table 6. Proposed scenarios used.

Scenario	Type of Attack	Protocol	Tool Used	Duration (s)	Packet Rate (pkt/s)
S1	Normal	Modbus/TCP	—	60	120
S2	SSH	SSH	PuTTY	60	350
S3	ICMP Flood	ICMP	hping3	60	1200
S4	Coordinated Attack	SSH + ICMP	PuTTY + hping3	60	1800

4.4.2. Metrics

Table 7 illustrates the measurable impact of cyberattacks on the system's performance. The average latency increased from 12 ms under normal conditions to 210 ms during a coordinated attack, a 1,650% increase. The packet loss rate increased from 0% to 15.5%, which directly impacted the system's responsiveness. The command execution error rate reaching 40% was recorded during the coordinated attack, indicating a clear deterioration in control reliability.

 doi:10.20944/preprints202604.0302.v1

Table 7. The impact of cyberattacks on system performance.

Scenario	Avg. Delay (ms)	Packet Loss (%)	Command Error (%)	Response Time (ms)
Normal	12	0	0	15
SSH	45	2.5	10	60
ICMP	120	8.2	25	140
Coordinated	210	15.5	40	260

4.4.3. Controllability & Observability

Table 8 shows the status of the system's contributability and observability. Under normal conditions, the system was fully controllable and observable, as the ranks of both the controllability and observability matrices were 4. During a coordinated attack, these values dropped to 2, indicating a critical, partial loss of the system's control and observability capabilities, confirming the direct impact of cyberattacks on the system's dynamic properties.

Table 8. The status of the Controllability & Observability of the system.

Scenario	Rank (Controllability)	Rank (Observability)	System States (n)	Status
Normal	4	4	4	Fully Controllable & Observable
SSH	4	3	4	Partial Observability Loss
ICMP	3	3	4	Degraded System
Coordinated	2	2	4	Critical Loss

4.4.4. Performance Under Cyberattacks

Figure 11 illustrates the gradual degradation in system performance under various cyberattacks. Specifically, the average latency increased from 12 ms under normal conditions to 210 ms during a coordinated attack, while the packet loss rate rose to 15.5%. Furthermore, the command execution error rate surged to 40%, reflecting the substantial impact of these attacks on the system's communication and control layers.

 doi:10.20944/preprints202604.0302.v1

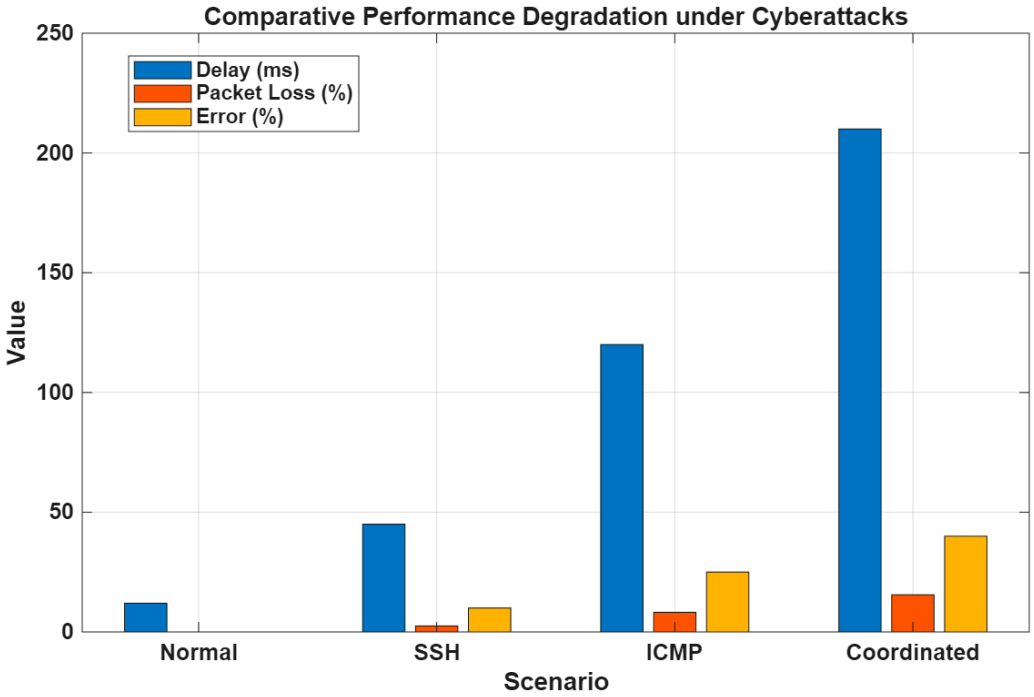

Figure 11. Comparative performance degradation under different cyberattack scenarios.

4.4.5. Voltage and Frequency Deviations

Although the changes in electrical values were limited (less than 2%), as shown in Table 9, the greatest impact was observed in the communication and control layer, indicating that the attack primarily targeted the cyber layer without directly affecting the physical layer.

Table 9. The deviation in voltage and frequency due to the attack.

Parameter	Normal	Attack	Deviation (%)
Voltage (V)	115	113	-1.7%
Frequency (Hz)	60.01	59.98	-0.05%

4.4.6. Federated Learning

The results of federated learning show a high accuracy of 96.4%, as shown in Table 10. The results confirm the effectiveness of the distributed model in enhancing attack detection, with a precision 95.8%, a recall 95.2%, and an F1-score 95.5%.

Table 10. Intrusion detection performance based on the SCADA dataset.

Metric	Value (%)
Accuracy	96.4
Precision	95.8
Recall	95.2
F1-Score	95.5

 doi:10.20944/preprints202604.0302.v1

5. Conclusions

This study shows the impact of SSH- and ICMP-based cyberattacks on a SCADA-integrated smart grid within a cyber-physical system. A controlled testbed was used to analyze how network attacks and communication performance affected system monitoring and control operations. A small division due to the attacks on the grid in voltage, current, and frequency. Less than 2%. The greatest impact was observed in the communication and control layer, showing that the attack primarily targeted the cyber layer without directly affecting the physical layer. The average latency increased under normal conditions during a coordinated attack, while the packet loss rate rose to 15.5%. The command execution error rate increased to 40%, reflecting the significant impact of these attacks on the system's communication and control layers. These results highlight the importance of secure communication in maintaining system stability and reliability. They also demonstrate how cyberattacks can weaken both system controllability and observability, emphasizing the need for stronger cybersecurity measures in smart grid environments.

References

1. Adeleke, O.J., Jovanovich, K., Ogunbunmi, S., Samuel, O. and Kehinde, T.O., 2025. Comprehensive exploration of smart cities: A systematic review of benefits, challenges, and future directions in telecommunications and urban development. IEEE Sensors Reviews. https://doi.org/10.1109/SR.2025.3569239
2. Zhang, H., Liu, B. and Wu, H., 2021. Smart grid cyber-physical attack and defense: A review. IEEe Access, 9, pp.29641-29659. https://doi.org/10.1109/ACCESS.2021.3058628
3. Ali, R.F.; Muneer, A.; Dominic, P.D.D.; Ghaleb, E.A.A.; Al-Ashmori, A. Survey on Cyber Security for Industrial Control Systems.
   Proceedings of the 2021 International Conference on Data Analytics for Business and Industry (ICDABI), 2021. https://doi.org/10.1109/ICDABI53623.2021.9655902
4. Sujatha, M.S.; Banu, S.S.; Sriyesh, V.; Sreenivasan, G.; Kuruba, M.; Reddy, M.G.M.Cyber Security for Power System. Proceedings of the 2024 International Conference on Electrical Energy Systems (ICEES), 2024. https://doi.org/10.1109/ICEES61253.2024.10776829
5. Zhang, K.; Pan, S.; Zhang, S.; Lin, J. The Intrusion Detection Method for Power Grid Industrial Control Systems Based on Improved Triplet Neural Network. Proceedings of the 2025 International Conference on Electrical Automation and Artificial Intelligence (ICEAAI), 2025. https://doi.org/10.1109/ICEAAI64185.2025.10957551
6. Chakraborty, S.; Kar, S. Hierarchical Control of Networked Microgrid with Intelligent Management of TCLs: A Case Study Approach. Electric Power Systems Research, 2023, 224, 109787. https://doi.org/10.1016/j.epsr.2023.109787
7. Ran, X.; Ma, L. An Extended False Data Injection Attack via Deep Reinforcement Learning: Attack Model and Countermeasures in Cyber-Physical Power Systems. IEEE Transactions on Automation Science and Engineering, 2025. https://doi.org/10.1109/TASE.2025.3596563
8. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-physical system security for the electric power grid. Proceedings of the IEEE 2012, 100, 210–224. https://doi.org/10.1109/JPROC.2011.2165269
9. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. IEEE Transactions on Smart Grid 2011, 1, 13–25. https://doi.org/10.1109/TSG.2011.2130276
10. Karanfil, M.; Rebbah, D.E.; Debbabi, M.; Kassouf, M.; Ghafouri, M.; Youssef, E.-N.S.; Hanna, A. Detection of Microgrid Cyberattacks Using Network and System Management. IEEE Transactions on Smart Grid, 2023, 14(3), 2390–2405. https://doi.org/10.1109/TSG.2022.3218934
11. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Aguera y Arcas, B. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS); Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
12. Bhol, S.G.; Swain, S.; Pattnaik, P.K.; Mohanty, S. Federated Learning and Blockchain Integrated Framework for Energy Management. Proceedings of the 2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS), 2025. https://doi.org/10.1109/ISCS69371.2025.11386430

 doi:10.20944/preprints202604.0302.v1

13. Li, Y. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach. Proceedings of the 2024 IEEE Power & Energy Society General Meeting (PESGM), 2024. https://doi.org/10.1109/PESGM51994.2024.10688898
14. Haridas, R.; Sharma, S.; Bhakar, R.; Mathuria, P. Evolution of Load Redistribution Attack in Cyber Physical Power System. Proceedings of the 2023 IEEE PES Innovative Smart Grid Technologies – Middle East (ISGT Middle East), 2023. https://doi.org/10.1109/ISGTMiddleEast56437.2023.10078512
15. Maliha, M.; Oluyomi, A.; Booge, M.; Bhattacharjee, S.; Braasch, N.; Gomez, P.; Das, S.K. Real-Time Testbed for Studying Cyberattacks and Defense in DER-integrated Smart Inverter Systems. Proceedings of the 2025 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2025. https://doi.org/10.1109/SmartGridComm65349.2025.11204638
16. Jørgensen, J.; et al. Cybersecurity and resilience of smart grids: Threat landscape, incidents, and emerging solutions. Renewable and Sustainable Energy Reviews 2026, 182, 113456. https://doi.org/10.1016/j.rser.2025.113456
17. Khare, U.; Malviya, A.; Gawre, S.K.; Arya, A. Cyber Physical Security of a Smart Grid: A Review. Proceedings of the 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2023. https://doi.org/10.1109/SCEECS57921.2023.10062966
18. Sanjalawe, Y.; Al-E'mari, S.; Fraihat, S.; Makhadmeh, S.N.; Alzubi, E. AI-Powered Smart Grids in the 6G Era: A Comprehensive Survey on Security and Intelligent Energy Systems. IEEE Open Journal of the Communications Society, 2025, Vol. 6, pp. 7677–7680+. https://doi.org/10.1109/OJCOMS.2025.3609144
19. Rajesh, M.; Ramachandran, S.; Vengatesan, K.; Dhanabalan, S.S.; Nataraj, S.K. Federated Learning for Personalized Recommendation in Securing Power Traces in Smart Grid Systems. IEEE Transactions on Consumer Electronics, 2024, Vol. 70, No. 1, pp. 88–95. https://doi.org/10.1109/TCE.2024.3368087
20. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A Survey on Smart Grid Cyber-Physical System Testbeds. IEEE Communications Surveys & Tutorials, 2017, Vol. 19, No. 1, pp. 446–464. https://doi.org/10.1109/COMST.2016.2627399
21. Athamnih, A.S.; Annamalai, A.; Abood, S.; Woodard, C.; Chouikha, M.; Al-zuhairi, H. AI-Driven Cybersecurity for SCADA-Integrated Microgrids: A Real-Time Detection Framework. In *Proceedings of the 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA, 18–20 February 2026; IEEE: Piscataway, NJ, USA, 2026. https://doi.org/10.1109/ICAIC67076.2026.11395662.
22. Abood, S.I.; Islam, N.; Chouikha, M.F.; Annamalai, A.; Khalid, I. Controllability and Observability of Real-Time Implementation of Smart Grid Cyber-Physical Systems under Adversarial Attacks. *IEEE Access* **2026**, *14*, 11902–11920. https://doi.org/10.1109/ACCESS.2026.3655238.
23. Abood, S.; Khalid, I.; Chouikha, M.; Annamalai, A.; Obiomon, P.; Butler-Purry, K.L. AI-Based Cybersecurity Assessment for Renewable-Integrated Smart Grid SCADA Systems. In *Proceedings of the 4th International Scientific Conference of Engineering Sciences (ISCES 2025)*, Baquba, Iraq, 10–11 December 2025; IET, 2025. https://doi.org/10.1049/icp.2025.4395.
24. Zhang, Z.; Peng, H.; Li, L.; Bao, S. Adaptive Asynchronous Federated Learning for Digital Twin Driven Smart Grid. *IEEE Trans. Smart Grid* **2025**, *16*, 4167–4182. https://doi.org/10.1109/TSG.2025.3579492.
25. Deng, X.; Pan, Y.; Fang, H. Anomaly Detection in Smart Grid Behavior Monitoring via Federated Learning: A Privacy-Preserving Defense Against Cyber-Physical Attacks. *J. Cyber Secur. Mobil.* **2025**, *14*, 1151–1172. https://doi.org/10.13052/jcsm2245-1439.1455.
26. Abood, S.; Ibrahim, Z.; Annamalai, A.; Khalid, I.; Chouikha, M.; Adeloye, A. SCADA Watch: Cybersecurity Mitigation in Smart Electric Microgrids. In *Proceedings of the 2025 IEEE International Communications Energy Conference (INTELEC)*; IEEE: Piscataway, NJ, USA, 2025. https://doi.org/10.1109/INTELEC63987.2025.11214733.
27. Xu, B.; Zhou, Y.; Li, M.; Ding, B.; Tan, G. A Digital Power Grid Information Security Protection Method Based on Federated Learning and Deep Learning. In *Proceedings of the 2025 10th Asia Conference on Power and Electrical Engineering (ACPEE)*; IEEE: Piscataway, NJ, USA, 2025. https://doi.org/10.1109/ACPEE64358.2025.11040397.
28. Li, X.; Wen, M.; He, S.; Lu, R.; Wang, L. A Privacy-Preserving Federated Learning Scheme against Poisoning Attacks in Smart Grid. *IEEE Internet Things J.* **2024**, *11*, 16805–16816. https://doi.org/10.1109/JIOT.2024.3365142.

 doi:10.20944/preprints202604.0302.v1

29. Zheng, R.; Sumper, A.; Aragüés-Peñalba, M.; Galceran-Arellano, S. Advancing Power System Services with Privacy-Preserving Federated Learning Techniques: A Review. *IEEE Access* **2024**, *12*, 76753–76779. https://doi.org/10.1109/ACCESS.2024.3407121.
30. Bhatia, K.; Ojha, S.S. Federated Learning Framework for Early Detection of Reconnaissance Attacks in Smart Grid Environments. In *Proceedings of the 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*; IEEE: Piscataway, NJ, USA, 2024. https://doi.org/10.1109/DICCT61038.2024.10533039.]
31. Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain and Federated Reinforcement Learning for Vehicle-to-Everything Energy Trading in Smart Grids. *IEEE Trans. Artif. Intell.* **2024**, *5*, 839–855. https://doi.org/10.1109/TAI.2023.3262597.
32. Li, Q.; Tang, W. An Anomaly Detection Method for Smart Power Grid: A Federated Learning Framework. 2024.
33. Blika, A.; Palmos, S.; Doukas, G.; Lamprou, V.; Pelekis, S.; Kontoulis, M.; Ntanos, C.; Askounis, D. Federated Learning for Enhanced Cybersecurity and Trustworthiness in 5G and 6G Networks: A Comprehensive Survey. *IEEE Open J. Commun. Soc.* **2024**, *6*, 3094–3124. https://doi.org/10.1109/OJCOMS.2024.3449563.
34. Kapoor, A.; Kumar, D. Federated Learning for Urban Sensing Systems: A Comprehensive Survey on Attacks, Defenses, Incentive Mechanisms, and Applications. *IEEE Commun. Surv. Tutor.* **2024**, *27*, 1293–1325. https://doi.org/10.1109/COMST.2024.3434510.