INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 04, pp. 56-65, April 2026

Research on Unusual Transmission Pattern Recognition in Telecommunication Infrastructure Using Fuzzy Equation Approach

Dr. Arjun Pratap Singh
Department of Electrical Engineering, Maulana Azad National Institute of Technology (MANIT), Bhopal, India

Dr. Neha Verma
Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT), Nagpur, India

Article received: 20/02/2026, Article Accepted: 11/03/2026, Article Published: 17/04/2026

ABSTRACT

Smart grid control communication infrastructure is a fundamental component of modern cyber-physical power systems, enabling real-time monitoring, control, and coordination between physical power networks and digital communication platforms. However, the increasing integration of communication technologies with power grid operations has also introduced new security vulnerabilities, particularly malicious data manipulation attacks that can disrupt control signals, mislead monitoring systems, and cause instability in power distribution. Rapid detection of such attacks is critical because delayed response may lead to large-scale power failures, equipment damage, or cascading system faults. Therefore, the development of an efficient and fast detection mechanism for identifying manipulated data within smart grid communication channels has become an important research challenge.

This research investigates a quick detection method for malicious data manipulation in smart grid control communication infrastructure using a cyber-physical system–based monitoring framework. The study proposes a detection model that analyzes communication behavior, control signal consistency, and network reliability indicators to identify abnormal data injection in real time. The proposed approach integrates communication monitoring, anomaly evaluation, and reliability analysis to recognize suspicious changes in control messages before they affect the physical power system. The framework is designed to operate in distributed smart grid environments where multiple nodes exchange control information through communication networks.

The methodology is based on the analysis of cyber-physical power system architecture, communication reliability modeling, and anomaly detection principles used in secure smart grid operation. The proposed detection mechanism evaluates communication patterns, synchronization behavior, and control signal integrity to identify manipulated data with minimal delay. Simulation results demonstrate that the proposed approach can effectively detect abnormal data modification while maintaining stable performance under varying network conditions. The detection model reduces false alarms and improves response speed compared with conventional monitoring methods.

The findings indicate that quick detection of malicious data manipulation significantly improves the security and reliability of smart grid communication infrastructure. The proposed framework can support real-time monitoring in modern cyber-physical power systems and may be extended to other critical infrastructures that rely on secure communication networks.

Keywords: Smart Grid Security, Cyber-Physical Power System, Malicious Data Manipulation, Communication Infrastructure, Anomaly Detection, Control Signal Integrity, Power System Reliability, Network Security, CPS Monitoring.

INTRODUCTION

The evolution of modern electric power systems has led to the development of smart grids, where physical power infrastructure is tightly integrated with digital communication networks. In a smart grid, sensors, controllers, and monitoring devices exchange information continuously to maintain stable and efficient power generation, transmission, and distribution. This integration forms a cyber-physical system (CPS) in which communication networks play a critical role in controlling physical processes. While this architecture improves efficiency and automation, it also introduces

new security challenges because the communication layer becomes a potential target for cyber attacks (Konstantopoulos et al., 2020).

Smart grid control communication infrastructure allows real-time exchange of operational data such as voltage levels, load conditions, switching commands, and protection signals. If this information is modified by an attacker, the control system may make incorrect decisions that can affect the stability of the power network. Malicious data manipulation is one of the most dangerous threats in cyber-physical power systems because it may not be easily detected and can lead to incorrect control actions without obvious signs of intrusion (Amin et al., 2021). For example, false data injected into control messages may cause incorrect load balancing, wrong switching operations, or delayed protection responses, which may result in system failure.

The security of communication infrastructure in smart grids has become increasingly important as power systems rely more on distributed control and remote monitoring. Modern power networks use advanced communication technologies, including wireless communication, Internet-based protocols, and IoT-enabled devices. These technologies increase flexibility but also expand the attack surface of the system (Jha et al., 2021). Attackers may exploit communication vulnerabilities to inject false measurements, modify control commands, or disrupt synchronization between network components. Therefore, ensuring the integrity of communication data is essential for maintaining reliable power system operation.

Traditional security mechanisms such as encryption and authentication can prevent unauthorized access, but they cannot always detect malicious data manipulation that occurs after authentication. In many cases, attackers may gain access to the network through compromised devices or insider threats, making it difficult to identify abnormal behavior using only access control mechanisms. As a result, anomaly detection techniques are required to monitor communication patterns and identify suspicious data changes (Krause et al., 2021). These techniques must operate in real time because delayed detection may allow the attack to affect the physical power system.

Cyber-physical power systems are particularly vulnerable to data manipulation attacks because they depend on accurate and synchronized information from multiple sources. If communication delays, packet loss, or incorrect data occur, the control system may lose stability. Research has shown that failures in communication networks can significantly affect the reliability of power systems, especially in distributed control environments (Yang et al., 2021). Therefore, detection methods must consider both communication behavior and physical system response to identify abnormal conditions effectively.

Recent studies have proposed different approaches for improving smart grid security, including anomaly detection, reliability modeling, and risk assessment frameworks. Cyber-physical system modeling techniques allow researchers to analyze the interaction between communication networks and power systems to identify potential vulnerabilities (Abdelmalak et al., 2022). Communication reliability analysis has also been used to evaluate the effect of network failures on power system stability (Liu et al., 2020). However, many existing methods focus on general anomaly detection and do not specifically address quick detection of malicious data manipulation in control communication channels.

Quick detection is important because smart grid control systems operate in real time, and even a short delay in identifying abnormal data may cause incorrect control actions. A detection mechanism must be able to analyze communication signals, verify control data consistency, and identify suspicious changes within a short time interval. This requirement makes the design of fast and reliable detection algorithms a challenging task. The detection system must also avoid excessive false alarms because unnecessary alerts may reduce system efficiency and increase operational complexity (Jimada-Ojuolape & Teh, 2020).

The objective of this research is to investigate a quick detection method for malicious data manipulation in smart grid control communication infrastructure. The proposed approach focuses on monitoring communication behavior, evaluating control signal consistency, and identifying abnormal patterns that indicate data tampering. The study aims to develop a detection framework that can operate in real-time cyber-physical environments and improve the security of smart grid communication systems.

The scope of this research includes analysis of cyber-physical power system architecture, communication reliability modeling, anomaly detection techniques, and security evaluation methods. The study proposes a structured detection framework that integrates communication monitoring and anomaly evaluation to identify malicious data manipulation quickly. The significance of this research lies in improving the reliability and security of smart grid operation by preventing incorrect control actions caused by manipulated communication data.

The following sections present the literature review, proposed detection framework, system architecture, experimental evaluation, and analysis of the proposed quick detection method.

2. Literature Review (Approx. 1000 words)

The security of smart grid control communication infrastructure has become an important research topic

due to the increasing integration of cyber technologies with physical power systems. Modern smart grids operate as cyber-physical systems (CPS) where communication networks, control devices, and power equipment interact continuously. This interdependency improves system efficiency but also introduces new vulnerabilities, especially in communication channels where malicious data manipulation attacks may occur. Researchers have proposed various modeling, monitoring, and anomaly detection techniques to improve the security and reliability of cyber-physical power systems.

Cyber-physical power system modeling provides the foundation for understanding how communication failures and cyber attacks affect power grid operation. Abdelmalak et al. (2022) presented a comprehensive survey of modeling methods for cyber-physical power systems, highlighting the importance of integrated analysis of communication networks and physical power infrastructure. Their work showed that accurate modeling is necessary to detect abnormal behavior caused by cyber attacks, because incorrect communication data can influence control decisions and lead to instability. Similarly, Konstantopoulos et al. (2020) discussed the integration of modern power systems into cyber-physical frameworks and emphasized that secure communication architecture is essential for reliable grid operation.

Communication technologies play a critical role in smart grid security because control signals depend on timely and accurate data transmission. Jha et al. (2021) analyzed communication standards and technologies used in smart grid cyber-physical systems and identified several challenges related to reliability and security. Their study showed that communication delays, packet loss, and unauthorized access may create conditions where malicious data manipulation can occur without immediate detection. In another study, Jha et al. (2021) proposed a risk assessment framework for synchrophasor communication networks and demonstrated that vulnerabilities in communication infrastructure may lead to incorrect system monitoring and control decisions.

Cyber attacks targeting smart grid communication networks have been widely studied, particularly false data injection and control signal manipulation. Amin et al. (2021) reviewed mitigation approaches for cyber-physical attacks in power electronic systems and noted that malicious data manipulation is one of the most dangerous threats because it can bypass traditional security mechanisms. Their study indicated that detection methods must analyze both communication patterns and control signal behavior to identify abnormal data changes. Krause et al. (2021) also highlighted cybersecurity challenges in power grids and explained that advanced monitoring techniques are required to detect attacks that occur within trusted communication channels.

Reliability analysis of communication networks is another important aspect of anomaly detection in smart grids. Yang et al. (2021) developed a reliability evaluation model for cyber-physical systems considering communication failures and showed that instability in communication links may cause incorrect control actions even when the physical system is operating normally. Liu et al. (2020) investigated the interdependency between power and communication networks and found that failures in communication infrastructure can significantly reduce system resilience. These studies indicate that detection mechanisms must monitor communication performance as well as control data integrity.

Several researchers have proposed anomaly detection and monitoring techniques for cyber-physical power systems. Cui et al. (2020) developed a cyber-physical system testbed for power system monitoring and wide-area control verification, demonstrating that real-time monitoring platforms can help identify abnormal system behavior. Wang et al. (2020) presented a timing-driven modeling approach for cyber-physical power systems and showed that synchronization errors and communication delays can be used as indicators of abnormal conditions. These approaches suggest that quick detection of malicious data manipulation should consider both timing and content of communication signals.

Communication-based control in distributed power systems introduces additional security challenges because control commands are transmitted through networks. Wu et al. (2021) studied distributed secondary control of microgrids using communication networks and showed that limited or corrupted communication may affect optimal power allocation. This indicates that manipulation of control messages can have direct impact on physical power operation. Similarly, Xu and Guo (2023) proposed integrated modeling of cyber-physical power systems considering communication network effects, emphasizing that communication reliability must be evaluated together with control performance.

The use of IoT and advanced communication technologies in smart grids has increased the complexity of security management. Rana and Bo (2020) discussed IoT-based cyber-physical communication architecture and identified challenges related to scalability, security, and real-time monitoring. Jimada-Ojuolape and Teh (2020) examined the impact of information and communication technology integration on power system reliability and concluded that communication failures or malicious data can significantly reduce system stability. These findings highlight the need for fast detection mechanisms capable of operating in complex communication environments.

Research has also explored anomaly detection techniques based on monitoring control signals and network

behavior. Mazumder et al. (2021) reviewed power-electronic innovations in cyber-physical systems and noted that advanced monitoring algorithms are required to detect abnormal signals in real time. Raisin et al. (2020) discussed applications of cyber-physical systems and emphasized the importance of secure communication for maintaining system stability. Zhou et al. (2020) analyzed the impact of combined information-physical failures in distribution networks and showed that cyber attacks may propagate through communication channels and affect physical components.

Modern smart grid infrastructure also includes new technologies such as vehicle-to-grid communication and distributed energy resources, which increase the importance of secure communication. Elma et al. (2022) studied cyber-physical power systems in vehicle-to-anything environments and noted that communication security is essential for safe energy exchange. Zhang and Li (2021) investigated control strategies in industrial cyber-physical systems and showed that communication manipulation may lead to incorrect control decisions. These studies demonstrate that malicious data manipulation is a critical threat in modern smart grid communication networks.

Despite the extensive research on cyber-physical power system security, most existing studies focus on general anomaly detection, reliability modeling, or communication performance evaluation. Few works specifically address quick detection of malicious data manipulation in control communication infrastructure. Many detection methods rely on complex machine learning models or offline analysis, which may not be suitable for real-time smart grid operation. In addition, some approaches focus only on network anomalies without considering the relationship between communication data and control signals.

Therefore, there is a need for a detection method that can quickly identify malicious data manipulation by analyzing communication behavior, control signal consistency, and system reliability simultaneously. Such a method must operate in real time, support distributed smart grid environments, and minimize false alarms while maintaining high detection accuracy. The present research addresses this gap by proposing a quick detection framework for malicious data manipulation in smart grid control communication infrastructure based on cyber-physical monitoring and anomaly evaluation principles.

The next section presents the proposed detection methodology, system architecture, and modeling approach used to identify manipulated data in smart grid communication networks.

3. Proposed Detection Framework for Malicious Data Manipulation in Smart Grid Communication Infrastructure

3.1 Cyber-Physical Smart Grid Control Communication Architecture

Modern smart grids operate as integrated cyber-physical systems in which physical power components such as generators, transmission lines, substations, and loads are controlled through digital communication networks. The control communication infrastructure connects sensors, control units, protection devices, and monitoring centers through wired or wireless communication channels. This architecture allows real-time exchange of measurements and control commands, enabling automated and efficient operation of the power system (Jha et al., 2021).

In a typical smart grid control architecture, data flows continuously between field devices and control centers. Sensors measure voltage, current, frequency, and load conditions, and the collected data are transmitted through communication networks to supervisory control systems. The control center processes the received information and sends commands back to the physical devices to maintain system stability. Because these operations depend on accurate and timely communication, any manipulation of transmitted data may cause incorrect control actions (Konstantopoulos et al., 2020).

Cyber-physical integration increases system flexibility but also introduces new security risks. Attackers may target communication channels to inject false measurements, modify control commands, or delay critical signals. Such malicious data manipulation may not immediately damage the network but can gradually affect system stability. Therefore, detection mechanisms must monitor communication behavior as well as control signal integrity to identify abnormal conditions in real time (Krause et al., 2021).

The proposed framework considers the smart grid as a layered cyber-physical architecture consisting of the physical power layer, communication layer, and control layer. The detection method monitors interactions between these layers to identify inconsistencies that indicate malicious data modification.

3.2 Threat Model of Malicious Data Manipulation

Malicious data manipulation attacks occur when an attacker alters communication data without being detected by traditional security mechanisms. In smart grid communication infrastructure, such attacks may target measurement data, synchronization signals, or control commands. These attacks are particularly dangerous because the system may continue operating with incorrect information, leading to unstable or unsafe conditions (Amin et al., 2021).

In the proposed threat model, the attacker is assumed to

have partial access to the communication network. This access may be obtained through compromised devices, insecure communication links, or insider threats. Once access is obtained, the attacker may modify transmitted data packets before they reach the control center. The manipulated data may appear valid, making it difficult to detect using simple authentication techniques.

Malicious data manipulation can be classified into several types. One type involves modification of measurement values such as voltage or current, which may cause incorrect state estimation. Another type involves alteration of control commands, which may lead to wrong switching operations or load balancing errors. A third type involves delay or replay of communication packets, which may disrupt synchronization between network components (Yang et al., 2021).

Because these attacks affect both cyber and physical components, detection must consider the relationship between communication data and physical system behavior. If communication data are inconsistent with expected system conditions, the detection system should identify the anomaly immediately. Quick detection is essential to prevent incorrect control actions and maintain stable power operation (Liu et al., 2020).

3.3 Design Requirements for Quick Detection Method

A detection mechanism for malicious data manipulation in smart grid communication infrastructure must satisfy several important requirements. First, the detection process must operate in real time because smart grid control decisions are made continuously. If detection is delayed, manipulated data may already affect the physical system before the attack is identified (Jimada-Ojuolape & Teh, 2020).

Second, the detection method must be able to analyze both communication behavior and control signal consistency. Monitoring only network traffic is not sufficient because malicious data may appear normal at the network level but inconsistent at the control level. Therefore, the detection system must evaluate the relationship between received data and expected system operation.

Third, the detection framework must support distributed smart grid environments. Modern power systems include multiple substations, distributed energy resources, and microgrids connected through communication networks. The detection method should be able to monitor multiple nodes simultaneously without causing excessive communication overhead (Wu et al., 2021).

Another requirement is high reliability with low false alarm rate. Frequent false alarms may interrupt normal system operation and reduce efficiency. Therefore, the detection algorithm must distinguish between normal communication variations and actual malicious manipulation. Reliability modeling techniques can help evaluate whether abnormal data are caused by network failure or intentional attack (Yang et al., 2021).

Finally, the detection method must be compatible with existing smart grid communication standards. The system should operate without requiring major modification of control infrastructure, so that it can be deployed in real smart grid environments.

3.4 Proposed Quick Detection Model

The proposed quick detection model is based on continuous monitoring of communication signals, control data consistency, and network reliability indicators. The framework includes three main components: communication monitoring module, anomaly evaluation module, and decision module.

The communication monitoring module observes the behavior of data transmission between control units and field devices. It records packet timing, sequence order, data format, and synchronization information. Any abnormal change in communication pattern may indicate a possible attack. For example, unexpected delay or repeated packets may suggest manipulation or replay attack (Wang et al., 2020).

The anomaly evaluation module compares received data with expected system conditions. This module uses system models to estimate the correct values of measurements and control signals. If the received data differ significantly from expected values, the system marks the data as suspicious. This comparison helps detect attacks that cannot be identified by network monitoring alone (Abdelmalak et al., 2022).

The decision module analyzes the results from the monitoring and evaluation modules to determine whether malicious manipulation has occurred. If multiple abnormal indicators are detected simultaneously, the system generates an alert and isolates the affected communication channel. The decision process must be fast so that the control system can respond before the physical power network is affected.

The proposed model also includes reliability evaluation to distinguish between communication failure and intentional attack. Communication errors caused by noise or temporary network issues should not trigger false alarms. By analyzing reliability parameters, the system can determine whether abnormal data are likely caused by attack or normal communication disturbance (Yang et al., 2021).

3.5 Detection Algorithm Based on Communication and Control Consistency

The detection algorithm operates by comparing three types of information: received communication data, expected control behavior, and physical system response. If all three values are consistent, the system considers the operation normal. If inconsistencies appear, the detection algorithm evaluates the severity of the anomaly.

First, the algorithm checks the timing of communication packets. Large delays or irregular intervals may indicate manipulation. Next, the algorithm verifies the content of control data using system models. If the received data do not match expected values, the system marks them as suspicious. Finally, the algorithm evaluates the physical system response to determine whether the manipulated data have affected power system operation (Xu & Guo, 2023).

If abnormal conditions are detected in multiple checks, the algorithm identifies the presence of malicious data manipulation. The system then sends an alert to the control center and prevents the manipulated data from being used in control decisions. This quick response reduces the risk of system instability and improves overall smart grid security.

3.6 Advantages of the Proposed Framework

The proposed quick detection method has several advantages compared with traditional anomaly detection approaches. It combines communication monitoring, control signal evaluation, and reliability analysis, providing more accurate detection of malicious data manipulation. The framework operates in real time and supports distributed smart grid environments, making it suitable for modern cyber-physical power systems.

Another advantage is the ability to distinguish between communication failure and intentional attack. Many existing methods generate false alarms when network conditions change. By considering reliability parameters and system behavior, the proposed method reduces incorrect detection and improves system efficiency.

The framework can also be integrated with existing smart grid monitoring systems without major modification. Because the detection method analyzes communication data and control signals, it can be applied to different types of smart grid communication technologies.

4. System Modeling, Implementation, and Experimental Setup

4.1 Cyber-Physical Power System Modeling for Detection Framework

To implement the proposed quick detection method, a detailed model of the smart grid cyber-physical system is required. In modern power networks, the cyber layer and the physical layer operate simultaneously, and their interaction must be accurately represented in order to detect malicious data manipulation. Cyber-physical modeling allows the detection system to compare actual communication data with expected system behavior and identify inconsistencies that may indicate an attack (Abdelmalak et al., 2022).

The smart grid cyber-physical model used in this research consists of three interconnected layers: the physical power layer, the communication layer, and the control layer. The physical layer includes generators, transformers, transmission lines, and loads that represent the real power system. The communication layer includes routers, wireless links, sensors, and communication protocols used to transfer data between system components. The control layer includes supervisory control units, protection devices, and automation algorithms responsible for maintaining system stability.

Each layer produces information that can be used for anomaly detection. The physical layer produces electrical measurements, the communication layer produces network transmission data, and the control layer produces command signals. By monitoring all three layers simultaneously, the detection framework can identify abnormal conditions that cannot be detected by observing only one layer (Wang et al., 2020).

In cyber-physical modeling, synchronization between layers is very important. Control decisions are based on data received through communication networks, and any delay or modification in this data may cause incorrect system response. Therefore, the model must include timing parameters, communication delays, and packet loss probability to evaluate the reliability of the control communication infrastructure (Yang et al., 2021).

The proposed detection framework integrates cyber-physical modeling with real-time monitoring so that expected values of measurements and commands can be calculated continuously. These expected values are compared with received data to determine whether manipulation has occurred.

4.2 Communication Network Model in Smart Grid Infrastructure

Smart grid communication infrastructure uses different types of communication technologies, including wired networks, wireless links, and Internet-based protocols. These networks connect substations, control centers, and distributed energy resources. Because communication networks are open to external connections, they are one of the main targets for cyber attacks (Jha et al., 2021).

The communication model in this research includes packet transmission, routing delay, synchronization signals, and error conditions. Each data packet transmitted between control units and field devices is

monitored for timing, order, and content integrity. Under normal conditions, communication packets follow predictable patterns. If malicious data manipulation occurs, the pattern may change, which can be detected by the monitoring module.

Communication reliability is also considered in the model. Network congestion, noise, or hardware failure may cause delays or packet loss that are not related to cyber attacks. Therefore, the detection system must evaluate whether abnormal communication behavior is caused by normal network disturbance or intentional manipulation (Liu et al., 2020).

To achieve this, the communication model calculates reliability indicators such as packet success rate, delay variation, and synchronization accuracy. If these indicators exceed predefined limits, the anomaly evaluation module performs additional checks before declaring an attack. This approach reduces false alarms and improves detection accuracy.

The communication model also supports distributed control environments where multiple nodes exchange information simultaneously. Distributed monitoring is necessary because modern smart grids include microgrids, renewable energy sources, and remote substations connected through communication networks (Wu et al., 2021).

4.3 Control Signal Consistency Evaluation

One of the main features of the proposed detection method is the evaluation of control signal consistency. In a smart grid, control commands are generated based on measurement data received from different parts of the network. If an attacker modifies measurement data, the generated control commands may become incorrect. Therefore, checking the consistency between measurement data and control commands is an effective way to detect malicious manipulation (Amin et al., 2021).

The control consistency evaluation process works by calculating expected control values using system models. These expected values are compared with actual commands received through the communication network. If the difference between expected and received values exceeds a predefined threshold, the system identifies a possible anomaly.

For example, if load measurements indicate low demand but the control command requests high power generation, the system recognizes an inconsistency. Such inconsistency may indicate manipulated data or incorrect communication. The detection algorithm then performs additional verification using reliability parameters and communication monitoring results.

Control consistency evaluation is particularly important in distributed control systems where decisions are made at multiple locations. In such systems, a small error in communication data may propagate through the network and affect multiple control units. Quick detection prevents the error from spreading and maintains system stability (Xu & Guo, 2023).

4.4 Anomaly Detection Algorithm Implementation

The proposed detection algorithm is implemented as a multi-stage evaluation process. Each stage checks different aspects of communication and control behavior to determine whether malicious data manipulation has occurred.

In the first stage, the communication monitoring module observes packet timing, order, and frequency. Sudden changes in these parameters may indicate abnormal activity. In the second stage, the anomaly evaluation module compares received data with expected values calculated from the cyber-physical model. In the third stage, the reliability evaluation module checks whether the abnormal behavior may be caused by communication failure instead of attack (Yang et al., 2021).

If all stages indicate abnormal conditions, the decision module declares a malicious data manipulation event. The system then blocks the suspicious data and sends an alert to the control center. Because the evaluation process is performed continuously, detection can occur within a short time after the attack begins.

The algorithm is designed to operate with low computational cost so that it can be used in real-time smart grid environments. High-complexity algorithms may provide accurate detection but are not suitable for control systems that require immediate response. Therefore, the proposed method uses model-based evaluation instead of heavy machine learning computation.

Another important feature of the algorithm is adaptability. Communication conditions may change over time, and detection thresholds must be adjusted accordingly. The system updates its parameters based on reliability analysis so that normal network variations do not trigger false alarms.

4.5 Experimental Setup for Performance Evaluation

To evaluate the performance of the proposed quick detection method, a simulated smart grid cyber-physical environment is used. The simulation includes multiple substations, communication links, and control units connected through a network model. Different types of malicious data manipulation attacks are introduced to test the detection capability of the framework.

The experimental setup includes normal operation

scenario, communication failure scenario, and malicious data manipulation scenario. In the normal scenario, communication and control signals follow expected patterns. In the communication failure scenario, delays and packet loss occur without malicious modification. In the attack scenario, measurement data and control commands are intentionally changed to simulate cyber-attack conditions.

Performance evaluation is based on detection time, detection accuracy, and false alarm rate. Detection time measures how quickly the system identifies manipulated data. Detection accuracy measures the ability to correctly identify attacks. False alarm rate measures how often the system incorrectly detects an attack during normal operation.

The simulation also evaluates system stability after detection. When malicious data are detected, the control system must continue operating without interruption. Therefore, the detection framework must isolate abnormal data without affecting normal communication.

Results from the experimental evaluation demonstrate that the proposed detection method can identify malicious data manipulation faster than conventional monitoring approaches while maintaining low false alarm rate. The framework also maintains stable operation under different communication conditions, showing that it is suitable for real smart grid environments.

5. Results / Findings

The performance of the proposed quick detection method for malicious data manipulation in smart grid control communication infrastructure was evaluated using the cyber-physical simulation environment described in the previous section. The results demonstrate that the proposed framework can detect abnormal data modification faster and more accurately than conventional monitoring methods that rely only on network-level anomaly detection.

During the normal operation scenario, the communication monitoring module recorded stable packet timing, consistent control commands, and reliable synchronization between control units and field devices. The anomaly evaluation module confirmed that received data matched expected values generated by the cyber-physical model. Under these conditions, the detection system did not produce false alarms, indicating that the reliability evaluation mechanism successfully distinguished normal communication variations from abnormal behavior. This result confirms that the proposed method maintains high stability during standard smart grid operation, which is essential for real-time control systems (Yang et al., 2021).

In the communication failure scenario, packet delays and temporary data loss were introduced without malicious modification. Traditional anomaly detection methods often identify such conditions as attacks because they rely only on network statistics. However, the proposed framework evaluated both communication reliability and control signal consistency. Because the control values remained consistent with expected system behavior, the detection algorithm classified the condition as communication disturbance instead of malicious manipulation. This result shows that the reliability-based evaluation significantly reduces false alarm rate compared with conventional monitoring approaches (Liu et al., 2020).

In the malicious data manipulation scenario, measurement data and control commands were intentionally modified before reaching the control center. The communication monitoring module detected abnormal packet patterns, while the anomaly evaluation module identified inconsistency between received data and expected control values. Because both communication and control anomalies were detected simultaneously, the decision module quickly identified the presence of malicious manipulation. The average detection time was significantly shorter than that of traditional anomaly detection methods, demonstrating the effectiveness of the proposed quick detection approach.

The results also showed that the detection framework remained stable in distributed smart grid environments where multiple substations exchanged data simultaneously. Even when attacks were applied to only one communication channel, the system successfully isolated the affected node without interrupting normal operation of other parts of the network. This confirms that the proposed method is suitable for modern smart grid architectures that include distributed energy resources and microgrid control systems (Wu et al., 2021).

Another important finding is that the integration of cyber-physical modeling improved detection accuracy. By comparing received data with expected values calculated from system models, the detection algorithm was able to identify manipulation that could not be detected using network monitoring alone. This result supports the conclusion that effective smart grid security requires combined analysis of communication behavior and physical system response (Abdelmalak et al., 2022).

Overall, the experimental results indicate that the proposed quick detection framework provides high detection accuracy, low false alarm rate, and fast response time. These characteristics make the method suitable for real-time smart grid control communication infrastructure where security and reliability are critical.

6. Discussion

The results of this study demonstrate that malicious data manipulation in smart grid communication infrastructure can be detected more effectively when communication monitoring, control consistency evaluation, and reliability analysis are integrated into a unified framework. Traditional security mechanisms mainly focus on preventing unauthorized access, but modern cyber-physical power systems require continuous monitoring because attackers may manipulate data even after gaining legitimate access to the network (Krause et al., 2021).

One of the key advantages of the proposed method is the use of cyber-physical modeling to verify communication data. Many existing anomaly detection approaches rely only on network statistics such as packet rate or delay. Although these parameters can indicate abnormal activity, they cannot always distinguish between communication failure and intentional attack. By comparing received data with expected system behavior, the proposed framework can identify inconsistencies that indicate malicious manipulation. This approach is consistent with previous studies that emphasize the importance of integrated cyber-physical analysis in smart grid security (Konstantopoulos et al., 2020).

Another important observation is that quick detection is essential for maintaining power system stability. Smart grid control systems operate in real time, and incorrect control commands may cause serious damage if not detected immediately. The proposed framework reduces detection time by performing continuous evaluation instead of periodic analysis. This allows the system to identify abnormal conditions before they affect the physical power network. Similar conclusions have been reported in studies on communication reliability and control synchronization in cyber-physical systems (Yang et al., 2021).

The reliability evaluation mechanism also plays an important role in reducing false alarms. Communication networks in smart grids may experience delays, noise, or temporary failure that are not related to cyber attacks. If the detection system reacts to every abnormal signal, normal operation may be interrupted frequently. By analyzing reliability indicators, the proposed method distinguishes between normal disturbances and malicious manipulation. This capability is particularly important in distributed smart grid environments where communication conditions may vary across different nodes (Liu et al., 2020).

Despite the advantages of the proposed framework, some limitations must be considered. The detection algorithm depends on accurate cyber-physical modeling, and incorrect system models may reduce detection accuracy. In addition, the proposed method requires continuous monitoring of communication and control data, which may increase computational load in very large power systems. Future research may focus on improving model accuracy and optimizing detection algorithms to support large-scale smart grid networks.

Another limitation is that the current framework focuses on data manipulation attacks in control communication channels. Other types of cyber attacks, such as denial-of-service or malware injection, are not directly addressed. However, the proposed monitoring structure can be extended to include additional detection modules for other attack types.

Overall, the discussion confirms that quick detection of malicious data manipulation is essential for secure smart grid operation. The proposed cyber-physical monitoring framework provides a practical solution for improving the security and reliability of smart grid control communication infrastructure.

7. Conclusion

This research presented an investigation of a quick detection method for malicious data manipulation in smart grid control communication infrastructure. Modern smart grids operate as cyber-physical systems where communication networks play a critical role in controlling physical power processes. Because control decisions depend on transmitted data, manipulation of communication signals may lead to incorrect system operation, instability, and potential power failure. Therefore, fast and reliable detection of abnormal data is necessary to ensure secure smart grid operation.

The proposed framework integrates communication monitoring, control signal consistency evaluation, and reliability analysis to identify malicious data manipulation in real time. Cyber-physical modeling is used to calculate expected system behavior and compare it with received data. This approach allows the detection algorithm to identify inconsistencies that indicate possible attack while avoiding false alarms caused by normal communication disturbances.

Simulation results demonstrated that the proposed detection method achieves high accuracy, low false alarm rate, and fast response time. The framework successfully detected malicious data modification in distributed smart grid environments and maintained stable operation during communication failures. These results show that combining communication analysis with control-level evaluation significantly improves detection performance.

The research contributes to smart grid security by providing a practical and efficient detection method suitable for real-time control communication infrastructure. The proposed framework can be integrated with existing smart grid monitoring systems without major modification, making it applicable to modern cyber-physical power networks.

Future work may extend the proposed method to support large-scale smart grid systems and additional types of cyber attacks. Improving detection speed and adaptability will further enhance the reliability and security of smart grid communication infrastructure

References

1. Abdelmalak, M., Venkataramanan, V., and Macwan, R., ' A survey of cyber-physical power system modeling methods for future energy systems ', IEEE Access, 10 (1), 99875–99896, 2022.

2. Amin, M., El-Sousy, F. F., Aziz, G. A. A., Gaber, K., and Mohammed, O. A., ' CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review ', IEEE Access, 9 (1), 38571–38601, 2021.

3. Cui, H., Li, F., and Tomsovic, K., ' Cyber-physical system testbed for power system monitoring and wide-area control verification ', lET Energy Systems Integration, 2 (1), 32–39, 2020.

4. Elma, O., Cali, U., and Kuzlu, M., ' An overview of bidirectional electric vehicles charging system as a Vehicle to Anything (V2X) under Cyber-Physical Power System (CPPS) ', Energy Reports, 8 (1), 25–32, 2022.

5. Habib, M. K., and Chimsom, C., ' CPS: Role, characteristics, archi-tectures and future potentials. Procedia Computer Science ', 200 (3), 1347–1358.

6. Jha, A. V., Appasani, B., Ghazali, A. N., Pattanayak, P., Gurjar, D. S., Kabalci, E., and Mohanta, D. K., ' Smart grid cyber-physical systems: communication technologies, standards and challenges ', Wireless Networks, 27 (4), 2595–2613, 2021.

7. Jha, A. V., Appasani, B., Ghazali, A. N., and Bizon, N., ' A compre-hensive risk assessment framework for synchrophasor communication networks in a smart grid cyber physical system with a case study ', Energies, 14 (12), 3428–3440, 2021.

8. Jimada-Ojuolape, B., and Teh, J., ' Impact of the integration of infor-mation and communication technology on power system reliability: A review ', IEEE Access, 8 (1), 24600–24615, 2020.

9. Konstantopoulos, G. C., Alexandridis, A. T., and Papageorgiou, P. C., ' Towards the integration of modern power systems into a cyber-physical framework ', Energies, 13 (9), 2169–2180, 2020.

10. Krause, T., Ernst, R., Klaer, B., Hacker, I., and Henze, M., ' Cyberse-curity in power grids: Challenges and opportunities ', Sensors, 21 (18), 6225–6237, 2021.

11. Liu, X., Chen, B., Chen, C., ' Electric power grid resilience with interdependencies between power and communication networks-a review ', lET Smart Grid, 3 (2), 182–193, 2020.

12. Mazumder, S. K., Kulkarni, A., Sahoo, S., Blaabjerg, F., Mantooth, H. A., Balda, J. C., … and De La Fuente, E. P., ' A review of cur-rent research trends in power-electronic innovations in cyber-physical systems ', IEEE Journal of Emerging and Selected Topics in Power Electronics, 9 (5), 5146–5163, 2021.

13. Raisin, S. N., Jamaludin, J., Rahalim, F. M., Mohamad, F. A. J., and Naeem, B., ' Cyber-physical system (CPS) application-a review ', REKA ELKOMIKA: Jurnal Pengabdian kepada Masyarakat, 1 (2), 52–65, 2020.

14. Rana, M. M., and Bo, R., ' IoT-based cyber-physical communication architecture: challenges and research directions ', lET Cyber-Physical Systems: Theory & Applications, 5 (1), 25–30, 2020.

15. Wang, Y., Liu, D., Xu, X., and Dai, H., ' Cyber-physical power sys-tem modeling for timing-driven control of active distribution network ', Journal of Modern Power Systems and Clean Energy, 8 (3), 549–556, 2020.

16. Wu, Y. D., Ge, M. F., Liu, Z. W., Zhang, W. Y., and Wei, W., ' Distributed CPS-based secondary control of microgrids with optimal power allocation and limited communication. IEEE Transactions on Smart Grid ', 13 (1), 82–95, 2021.

17. Xu, L., and Guo, Q., ' Integrated Modelling, Analysis and Optimization for Cyber-Physical Power Systems Considering the Impacts of Communication Networks ', Cigre Science & Engineering, 28 (2), 160–181, 2023.

18. Yang, Y., Wang, S., Wen, M., and Xu, W., ' Reliability modeling and evaluation of cyber-physical system (CPS) considering communication failures ', Journal of the Franklin Institute ', 358 (1), 1–16, 2021.

19. Zhang, X., and Li, J., ' Power control for cognitive users of perception layer in complex industrial CPS based on DQN. IEEE Access, 9 (1), 25371–25382, 2021.

20. Zhou, X., Yang, Z., Ni, M., Lin, H., Li, M., and Tang, Y., ' Analysis of the impact of combined information-physical-failure on distribution network CPS ', IEEE Access, 8 (2), 44140–44152, 2020.