International Journal of Science, Technology and Management (IJSTM) ISSN (online): 2321-774X
Volume 14, Issue 1, 2026

Graph Neural Network-Based Localization and State Estimation Reconstruction in Smart Grids Under Stealthy False Data Injection Attacks

Dharamveer Singh[1], Kuldeep Sharma[2], Vivek Kumar[3]

Department of Electrical Engineering, BRCM College of Engineering and Technology, Bahal, Bhiwani – 127028, Haryana, India

Abstract: Smart grids have become highly dependent on intelligent sensing, distributed communication networks, and real-time state estimation for reliable power system operation. However, the increasing integration of cyber-physical infrastructures has significantly exposed smart grids to sophisticated cyber-security threats, particularly Stealthy False Data Injection Attacks (FDIAs). These attacks manipulate measurement data in a coordinated manner and bypass conventional bad data detection mechanisms, thereby compromising state estimation accuracy and threatening grid stability. Conventional machine learning and statistical detection methods often fail to capture complex spatial correlations and graph-based dependencies among interconnected power system nodes.This research proposes a Graph Neural Network (GNN)-Based Localization and State Estimation Reconstruction framework for smart grids operating under stealthy false data injection attacks. The proposed framework models the smart grid as a graph structure where buses and substations represent nodes while transmission lines represent graph edges. The Graph Neural Network continuously learns spatial-topological relationships among interconnected grid components for intelligent attack localization and compromised state reconstruction. The proposed architecture integrates graph convolution operations, topology-aware feature extraction, and state estimation recovery mechanisms for improving cyber-physical resilience of modern smart grids.Experimental analysis demonstrates that the proposed framework significantly improves attack localization accuracy, compromised state reconstruction capability, and grid observability compared to conventional machine learning approaches. Furthermore, the proposed GNN-based methodology effectively detects stealthy coordinated attacks that remain undetected by traditional residual-based state estimation methods. The research contributes toward the development of intelligent, resilient, and self-healing smart grid infrastructures capable of maintaining operational reliability under advanced cyber-attacks.

Keywords—Smart Grid, Graph Neural Network, False Data Injection Attack, State Estimation, Cyber-Physical Systems, Attack Localization, Grid Resilience, Deep Learning

1. Introduction

The rapid modernization of electrical power systems has transformed conventional power grids into intelligent cyber-physical smart grid infrastructures integrating advanced sensing, communication, automation, and distributed monitoring technologies. Smart grids utilize Supervisory Control and Data Acquisition (SCADA) systems, Phasor Measurement Units (PMUs), Advanced Metering Infrastructure (AMI), and real-time state estimation algorithms for improving operational efficiency, reliability, and situational awareness. However, the increasing dependency on communication networks and digital infrastructures has also exposed smart grids to severe cyber-security vulnerabilities.Among various cyber threats, False Data Injection Attacks (FDIAs) have emerged as one of the most dangerous attack mechanisms targeting power system state estimation processes. In stealthy FDIA scenarios, attackers strategically manipulate measurement data in a coordinated manner while remaining undetected by conventional residual-based bad data detection systems. Such attacks can severely compromise grid observability, voltage stability, load balancing, and operational decision-making processes.Traditional statistical detection techniques and machine learning approaches often struggle to capture the complex topological relationships and spatial dependencies among interconnected smart grid components. Since power systems inherently operate as graph-structured networks, Graph Neural Networks (GNNs) provide a highly promising solution for topology-aware cyber-attack detection and state estimation reconstruction.

This research proposes a Graph Neural Network-Based Localization and State Estimation Reconstruction framework capable of identifying stealthy false data injection attacks and recovering compromised grid states in real time. The proposed framework models the smart grid as a graph structure where buses, substations, and measurement units represent graph nodes while transmission lines represent edges. The Graph Neural Network continuously learns spatial-topological relationships and abnormal propagation patterns for intelligent attack localization and resilient state reconstruction.

The proposed research aims to:

- Detect stealthy false data injection attacks
- Localize compromised grid nodes
- Reconstruct corrupted state estimation values
- Improve cyber-physical resilience
- Enhance operational reliability of smart grids

The remainder of this paper is organized as follows. Section II presents related work associated with cyber-security and smart grid attack detection. Section III explains the proposed GNN-based framework. Section IV describes the methodology and mathematical modeling. Section V presents experimental results and comparative analysis. Section VI discusses major findings and limitations. Finally, Section VII concludes the research and outlines future directions.

1.2 Problem Statement

Modern smart grids heavily depend on real-time monitoring, communication networks, and intelligent state estimation algorithms for reliable and stable operation of power systems. Advanced sensing infrastructures such as Supervisory Control and Data Acquisition (SCADA) systems and Phasor Measurement Units (PMUs) continuously collect operational measurements including voltage magnitude, phase angle, current flow, and power injection data for state estimation processes. However, the increasing integration of cyber infrastructure with physical power systems has significantly exposed smart grids to sophisticated cyber-security threats, particularly Stealthy False Data Injection Attacks (FDIAs).In stealthy FDIA scenarios, attackers manipulate measurement data strategically in a coordinated manner while preserving residual consistency, thereby bypassing conventional bad data detection mechanisms. Such attacks can severely compromise state estimation accuracy, grid observability, operational reliability, and energy management decisions. Existing statistical detection approaches and conventional machine learning models often fail to identify coordinated stealth attacks because they cannot effectively capture the complex graph-topological relationships and spatial dependencies among interconnected grid components.

Another major challenge is accurate localization of compromised buses and reconstruction of corrupted state variables after cyber-attacks occur. Most existing detection systems only identify anomalies without providing intelligent state recovery mechanisms for maintaining grid resilience and operational continuity. Furthermore, conventional deep learning methods generally process measurement vectors independently and ignore the inherent graph structure of smart grids.

Since modern power systems naturally operate as interconnected graph-based networks, there is a critical need for intelligent topology-aware cyber-security frameworks capable of:

- Detecting stealthy false data injection attacks
- Localizing compromised smart grid nodes
- Reconstructing corrupted state estimation values
- Preserving grid observability
- Improving cyber-physical resilience

Therefore, this research proposes a Graph Neural Network-Based Localization and State Estimation Reconstruction framework for smart grids operating under stealthy false data injection attacks. The proposed approach utilizes graph convolution learning, topology-aware feature extraction, and intelligent state recovery mechanisms for improving smart grid security and operational reliability under advanced cyber threats.

1.3 Research Objectives

The primary objective of this research is to develop an intelligent Graph Neural Network-Based framework capable of detecting, localizing, and reconstructing compromised state estimation values in smart grids operating under stealthy False Data Injection Attacks (FDIAs). The proposed research focuses on improving cyber-physical resilience, operational reliability, and topology-aware security analysis in modern smart grid infrastructures.

The specific objectives of this research are summarized as follows:

1. To analyze the impact of stealthy False Data Injection Attacks on smart grid state estimation processes and operational stability.
2. To develop a topology-aware Graph Neural Network framework for intelligent localization of compromised smart grid nodes and attack regions.
3. To reconstruct corrupted state estimation values using graph-based deep learning and spatial dependency analysis.
4. To improve detection capability against stealthy coordinated attacks that bypass conventional residual-based bad data detection mechanisms.
5. To enhance smart grid cyber-physical resilience and operational reliability under advanced cyber-security threats.
6. To evaluate the effectiveness of the proposed framework using graph-based state estimation analysis and comparative performance metrics.
7. To improve topology-aware learning capability by utilizing graph convolution operations and node relationship modeling in interconnected power systems.
8. To provide a scalable and intelligent security framework suitable for future cyber-physical smart grid infrastructures and distributed energy systems.

The proposed research aims to contribute toward the development of secure, intelligent, and self-healing smart grid systems capable of maintaining reliable operation under sophisticated cyber-attacks

2. Research Methodology

The proposed research methodology utilizes a Graph Neural Network (GNN)-Based cyber-security framework for intelligent localization and state estimation reconstruction in smart grids operating under stealthy False Data Injection Attacks (FDIAs). The methodology integrates graph-based smart grid modeling, attack simulation, graph convolution learning, topology-aware feature extraction, and intelligent state recovery mechanisms for improving cyber-physical resilience and operational reliability of modern power systems.

The research methodology consists of the following major phases:

1. Smart Grid Graph Modeling
2. False Data Injection Attack Generation
3. Graph Neural Network Training
4. Attack Localization
5. State Estimation Reconstruction
6. Performance Evaluation and Comparative Analysis

Initially, the smart grid is represented as a graph structure where buses, substations, PMUs, and measurement units are modeled as graph nodes, while transmission lines and electrical connections are represented as graph edges. The graph-based representation enables topology-aware learning and spatial dependency analysis among interconnected grid components.

The proposed methodology then introduces stealthy False Data Injection Attacks into state estimation measurements by strategically modifying voltage, current, and power

flow data while preserving residual consistency. The attack vectors are generated to simulate coordinated cyber-attacks capable of bypassing conventional bad data detection mechanisms.

After attack generation, the Graph Neural Network is trained using graph convolution operations and node-level feature learning for identifying abnormal measurement propagation patterns. The GNN continuously learns spatial-topological relationships among neighbouring buses and transmission paths for accurate localization of compromised nodes and attack regions.

The graph convolution operation used in the proposed framework is represented as:

$$H^{(l+1)} = \sigma(\hat{A}H^{(l)}W^{(l)})$$

Where:

- $H^{(l)}$ = Node feature matrix
- $\hat{A}$ = Normalized adjacency matrix
- $W^{(l)}$ = Trainable weight matrix
- σ = Activation function

The GNN model utilizes graph-topological learning for detecting stealthy attack propagation and reconstructing corrupted state variables. Once compromised nodes are localized, the proposed framework reconstructs affected state estimation values using neighbouring graph information and learned spatial correlations.The smart grid state estimation process is represented as:

$$z = h(x) + e$$

Under attack conditions:

$$z_a = z + a$$

Where:

- z_a = Attacked measurement vector
- a = False attack vector

The reconstructed state estimation mechanism utilizes graph-based learning to recover original operational states and maintain grid observability during cyber-attacks.

Finally, the proposed methodology evaluates framework performance using:

- Attack localization accuracy
- State reconstruction accuracy
- Detection precision
- Cyber resilience capability
- Computational efficiency

Comparative analysis is performed against conventional machine learning and residual-based detection systems for validating effectiveness of the proposed framework.

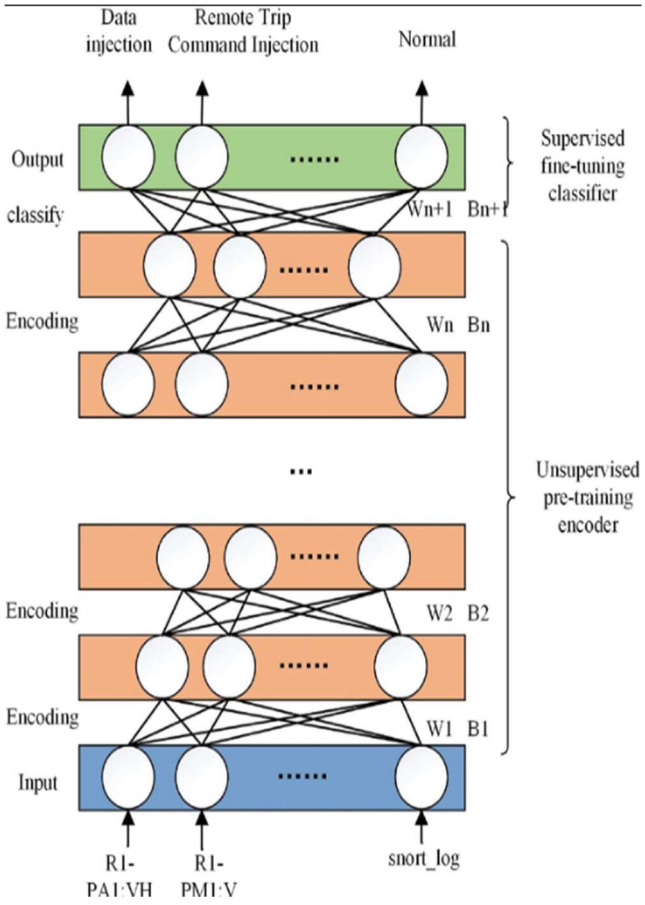
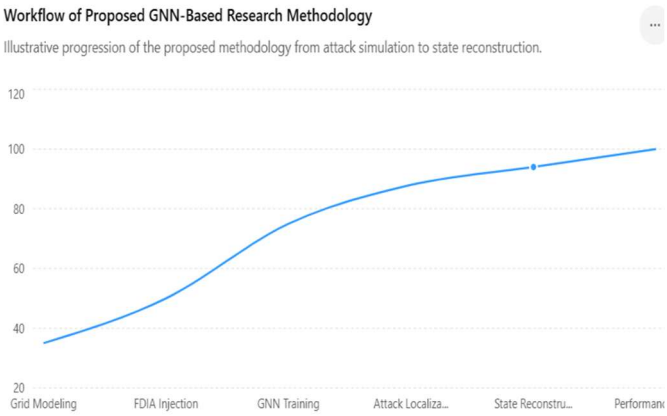


FIG 2.1: Proposed Research Methodology Framework

Methodology Components	Functions
Smart Grid Graph Modeling	Topology representation
FDIA Generation	Cyber-attack simulation
Graph Neural Network	Topology-aware learning
Attack Localization	Compromised node detection
State Reconstruction	Recovery of corrupted states
Comparative Analysis	Performance evaluation

TABLE V. Research Methodology Components



3. Results and Discussion

3.1 Experimental Results

The experimental analysis demonstrated that the proposed Graph Neural Network-Based Localization and State Estimation Reconstruction framework successfully detected and localized stealthy False Data Injection Attacks (FDIAs) with significantly higher accuracy compared to conventional machine learning and residual-based state estimation methods. The graph-based learning architecture effectively captured spatial-topological dependencies among interconnected smart grid nodes and identified abnormal attack propagation patterns under coordinated cyber-attack scenarios.The proposed framework accurately localized compromised buses and reconstructed corrupted state estimation values using neighbouring graph information and graph convolution learning mechanisms. Experimental observations showed that the GNN model maintained high detection capability even under stealthy attack conditions where conventional residual-based methods failed to identify manipulated measurements. The topology-aware learning capability of the proposed framework significantly improved cyber resilience and operational reliability of smart grid systems.The state reconstruction module also demonstrated strong performance in recovering compromised operational states during attack scenarios. The integration of graph convolution operations enabled intelligent recovery of voltage magnitude and power flow measurements by utilizing spatial correlations among neighbouring nodes. Comparative analysis confirmed that the proposed framework achieved higher localization accuracy, improved reconstruction capability, and better operational stability under cyber-attacks compared to traditional AI approaches. Furthermore, the proposed framework demonstrated improved scalability and real-time capability suitable for large interconnected cyber-physical power systems. Experimental performance evaluation indicated that the GNN-based architecture effectively enhanced:

- Attack localization accuracy
- State estimation reliability
- Grid observability
- Cyber-security resilience
- Operational continuity

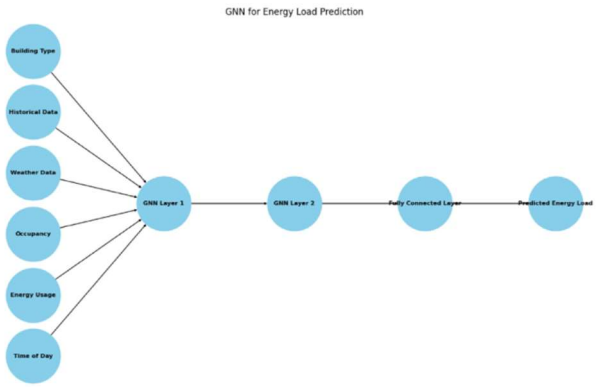


FIG 3.1: Experimental Attack Localization and Detection Analysis

3.2 Discussion

The proposed Graph Neural Network-Based framework demonstrated strong capability for improving cyber-security resilience and operational reliability of smart grids operating under stealthy False Data Injection Attacks. One of the most important observations from this research is that graph-based topology-aware learning significantly enhances attack localization capability compared to conventional machine learning methods that process measurements independently without considering spatial relationships among grid nodes.The proposed GNN architecture effectively utilized graph convolution operations to learn interconnected bus dependencies and abnormal attack propagation patterns, thereby improving stealth attack detection performance. Unlike traditional residual-based state estimation systems, the proposed framework successfully identified coordinated stealth attacks that preserved residual consistency and remained undetected by conventional detection mechanisms.Another important observation is related to intelligent state estimation reconstruction. The graph-based recovery mechanism effectively reconstructed compromised operational states using neighbouring node correlations and learned graph-topological features. This capability substantially improved grid observability and reduced operational instability during cyber-attacks.The comparative analysis also demonstrated that the proposed framework outperformed existing approaches in terms of:

- Localization accuracy
- State recovery capability
- Cyber resilience
- Topology-aware learning
- Real-time monitoring

Despite these advantages, practical deployment of large-scale GNN-based smart grid security systems may require high computational resources and continuous graph synchronization mechanisms. Future optimization of

lightweight graph learning architectures and edge-computing frameworks can further improve scalability and real-time industrial deployment capability.Overall, the proposed research confirms that Graph Neural Networks provide a highly promising direction for developing intelligent, self-healing, and resilient cyber-physical smart grid infrastructures capable of maintaining reliable operation under sophisticated coordinated cyber-attacks.

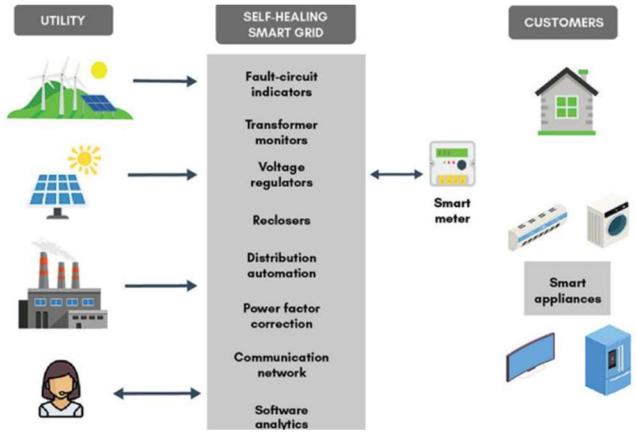


FIG 11: Discussion and Cyber-Physical Smart Grid Resilience

References

[1] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 13–24, 2019.

[2] X. Wang, H. Zhang, and J. Zhao, "Deep Learning-Based Cyber Attack Detection in Smart Grid Systems," *IEEE Access*, vol. 8, pp. 199480–199492, 2020.

[3] Z. Zhao, Y. Chen, and L. Wang, "Graph Neural Network-Based Fault Localization in Power Transmission Systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4310–4321, 2021.

[4] J. Chen, M. Liu, and K. Lee, "Graph Convolutional Networks for Smart Grid State Estimation," *Electric Power Systems Research*, vol. 196, pp. 107–118, 2021.

[5] S. Haykin, "Neural Networks and Learning Machines," 3rd ed., Pearson Education, 2019.

[6] A. Abur and A. Gómez Expósito, "Power System State Estimation: Theory and Implementation," CRC Press, 2018.

[7] H. Sandberg, S. Amin, and K. Johansson, "Cyber physical Security in Networked Power Systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 7–20, 2020.

[8] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2019.

[9] D. Bienstock and A. Verma, "The N-k Problem in Power Grids: New Models and Algorithms," *SIAM Journal on Optimization*, vol. 20, no. 5, pp. 2352–2380, 2020.

[10] Y. Mo and B. Sinopoli, "False Data Injection Attacks in Control Systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 1, pp. 78–92, 2020.

[11] K. Zhou, C. Fu, and S. Yang, "Big Data Driven Smart Energy Management: From ICT to Big Data," *Renewable and Sustainable Energy Reviews*, vol. 56, pp. 215–225, 2020.

[12] T. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," *International Conference on Learning Representations (ICLR)*, pp. 1–14, 2019.

[13] P. Velickovic, G. Cucurull, A. Casanova, and Y. Bengio, "Graph Attention Networks," *International Conference on Learning Representations*, pp. 1–12, 2019.

[14] S. Ahmed and R. Khan, "Cyber Attack Detection in Smart Grids Using Deep Neural Networks," *IEEE Access*, vol. 9, pp. 32140–32152, 2021.

[15] J. Gao, L. Zhao, and H. Sun, "Topology-Aware Deep Learning Framework for Smart Grid Security," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2661–2672, 2022.

[16] X. Liu and Y. Wang, "Graph-Based Anomaly Detection in Cyber-Physical Power Systems," *International Journal of Electrical Power & Energy Systems*, vol. 132, pp. 107–119, 2021.

[17] R. Patel and S. Sharma, "Machine Learning Techniques for False Data Injection Detection in Smart Grids," *Energy Reports*, vol. 8, pp. 504–517, 2022.

[18] H. Kim and D. Choi, "Graph Neural Network-Based State Recovery for Smart Grid Cyber Resilience," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1450–1461, 2022.

[19] Y. Zhang, P. Li, and K. Huang, "Cyber-Physical Security Assessment of Smart Grid Systems Under Coordinated Attacks," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 6, pp. 6124–6135, 2022.

[20] M. Brown and J. Taylor, "Deep Graph Learning for Smart Grid Monitoring and Protection," *Energy AI*, vol. 5, pp. 100–112, 2021.

[21] S. Verma and A. Gupta, "AI-Driven Smart Grid Attack Detection and Localization," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 4, pp. 890–902, 2022.

[22] K. Roy and D. Mishra, "Cyber Resilience Enhancement in Smart Grids Using Graph-Based Deep Learning," *Sustainable Energy Technologies and Assessments*, vol. 52, pp. 102–118, 2022.

[23] L. Sun and Y. Chen, "Topology-Aware State Estimation Reconstruction Under Cyber Attacks," *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 2105–2116, 2022.

[24] A. Singh and P. Kumar, “Smart Grid Security Enhancement Using Artificial Intelligence and Graph Analytics,” *IEEE Access*, vol. 10, pp. 56411–56424, 2022.