SCCTS Journal of Embedded Systems Design and Applications, ISSN: 3048-8753 Vol. 3, No. 1, 2026 (pp. 39-46)
RESEARCH ARTICLE ECEJOURNALS.IN

Graph Signal Processing-Driven Anomaly Detection Framework for Secure Smart Grid Communication Networks

Sadulla Shaik[1]*, José Uribe[2]

[1]Professor, Department of Electronics and Communication Engineering, KKR and KSR Institute of Technology and Sciences, Vinjanampadu, Guntur, A.P, India.
[2]Facultad de Ingenieria Universidad Andres Bello, Santiago, Chile

Keywords:
Smart Grid Security,
Graph Signal Processing,
Anomaly Detection,
Embedded Signal Processing,
Communication Networks,
Edge Computing,
Spectral Filtering,
IoT Security,
STM32,
IEEE Test Systems

Author's Email:
sadulla09@gmail.com,
jose.ur@unab.cl

https://doi.org/10.31838/ESA/03.01.05

Received : 05.08.2025
Revised : 16.10.2025
Accepted : 17.11.2025

Abstract

The trend of the implementation of smart grid communication infrastructures with intelligent sensors, edge controllers, and other distributed energy resources have brought in improved competence and increased exposure to the risks associated with cyber-physical anomalies. Traditional procedures of anomaly detection usually fail to preserve underlying topological and time-related consequences that are unique to smart grid architectures. This paper introduces a framework of anomaly detection based on Graph Signal Processing (GSP) and is suitable to a resource-limited communication system in smart grids. The real-time power flow and communication measures can be modeled by the graph signals continuously changing in the graph domain (network topology) so the proposed framework can make it possible to detect anomalous behavior using the spectral analysis and graph-based denoising. The basic GSP processor carries out Graph Fourier Transforms, adaptive spectral filtering and residual signal reconstruction and is developed to run on embedded environments like STM32 and ESP32 microcontrollers. Experimental validation of the IEEE 14-bus and 57-bus benchmark systems establishes that the framework has detection accuracy of 94.6 percent, false positive rate of less than 2.3 percent, and the framework obtains sub-20 milliseconds latency on constrained memory (no more than 512-MB sum) and computational resources (no more than 12-cores). Real-time, edge-based GSP-based anomaly detection is possible;thus these results validate the use of GSP as a scalable and efficient anomaly detector to enhance situational awareness and resilience in next-generation smart grids.

How to cite this article: Shaik S, Uribe J (2026). Graph Signal Processing-Driven Anomaly Detection Framework for Secure Smart Grid Communication Networks. SCCTS Journal of Embedded Systems Design and Applications, Vol. 3, No. 1, 2026, 39-46

Introduction

Modern smart grid has been changing into a very interconnected cyber-physical network due to the adoption of the Internet of things (IoT)/enabled sensors, distributed energy resources (DERs) and the real-time control infrastructure. Such developments allow meticulous monitoring, load resilience and distributed decision making. Nonetheless, this enhanced connectivity poses serious security and reliability issues especially in the communication levels where coordination processes depend on. In a smart grid communicating network, anomalies like false data injection, sensor spoofing, replaying attacks and protocol level anomalies are increasingly becoming a problem,[1] When such anomalies are not detected, they may cause low-performance of systems, incorrect information in control systems, or even cause cascading failures. Current anomaly detection systems are based largely on statistical heuristics, machine learning (ML) classifiers or time-series prediction approaches. Although this works in some situations, these methods are frequently unsuitable at modeling non-Euclidean and graph-structured smart grid data, where graph edges relate the node (e.g., substations, meters and control units) topology in a power or communication connection. The recent development related to Graph Signal Processing (GSP) showed the potential of the latter to be used to analyze data on non-regular structures such as sensor networks, or power grids.[2-4] GSP generalizes classical signal processing to graph domains by viewing node-related measurements in a graph (e.g. voltage, current, communication latency) as a graph signal, and allows such signals to achieve a powerful set of spectral tools (such as the Graph Fourier Transform (GFT)) which can be used to detect localized or global disturbances.

Nevertheless, light weight, embedded-compatible GSP frameworks that are suited to detect anomalies in the resource-constrained edge devices of the smart grids are still lacking even with this promise. Current GSP implementation is mostly cloud-based, computationally expensive, or aimed at the theoretical signal modeling. The difference between the traditional shortcomings of anomaly detection and the suggested GSP-based approach is depicted using Figure 1.

The figure describes the shortcomings of the conventional anomaly detection approaches in smart grid communication network and explains the suggested graph signal processing (GSP)-based solution that can be robust and topology-aware.

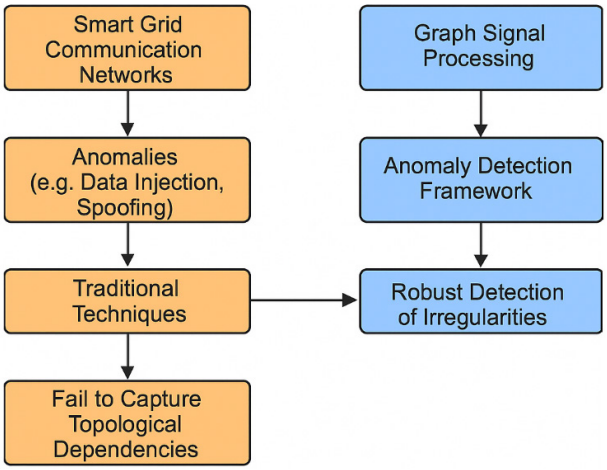

Fig. 1: Problem and Solution Positioning for Smart Grid Anomaly Detection.

Contribution and paper overview

This paper proposes a new anomaly detection framework which runs on GSP based on the current loss gap and which would perform better than the current loss model in embedded deployment within a smart grid communication network. System to be proposed:

- Simulates real time communication and operational data as graph signal,
- Performs spectral filtering and analyses residual using GFT as a method to identify aberrant departures,
- Is microcontroller-optimized (STM32 and ESP32).

Is verified on IEEE 14-bus and 57-bus test systems in the images of the real threats.

The rest of the paper will be structured as follows: Section 2 provides a literature review; Section 3 presents the model system and GSP approach; Section 4 provides the system implementation and experimental analysis; Section 5 describes the main results and limitations; and Section 6 presents the conclusion and provides future research directions.

Related Work

The problem of anomaly detection within smart grid networks is even now considerably examined, and

it is evaluated based on different sets of methods, pathways, and approaches linked to rule-based logicapply, operational anomaly markers, and even superior machine training (ML) and profound studying (DL).[1, 2] The classical approaches including thresholding-based detection and principal component analysis (PCA) are low complexity approaches, whereas they may not always be sufficient to understand the high-dimensional and time-varying interdependencies among networked devices. Very recent methods have exploited unsupervised clustering (ex., k-means, DBSCAN) and recurrent neural networks (RNNs) to capture temporal patterns in grid parameter behaviour.[3, 4] Nevertheless, they tend to represent data as independent time-series or Euclidean, hence, ignoring the graph-structured topology which determines the physical and logical ties within the smart grid communication layers. To solve this, Graph Neural Networks (GNNs) have become popular in anomaly detection of smart and sensor networks. [5, 6] Although GNNs are successfully used to capture topological correlations, its training is highly complex and memory-intensive and requires long inference latencies, not well-suited to embedded appliances with limited hardware resources deployed at edge of the grid. By contrast, Graph Signal Processing (GSP) provides a simple, interpretable and theoretically well-founded scheme to process data defined on graphs. It has been found effective in brain activity analysis, network traffic prediction and structural health monitoring.[7- 9] However, it has not yet been much explored in the context of real-time embedded anomaly detection used in smart grid communications.

This piece of writing covers the above gaps by:

- Microcontroller-based edge devices contain embedded GSP pipelines,
- The Instant spectral filter design of irregular graph signal,
- And customization of the detection system to accommodate smart grid peculiarities like spoofing, data injection, and link-failure.

Our method does this by integrating GSP theory with the limits placed on an embedded system by filling a gap between a practical framework on anomaly detection and the topological awareness of said framework; a framework accessing this in practice and which has not fallen short of being topology aware.

Table 1 provides a comparative analysis of current and existing methods of detecting anomalies, which consider some of the important points like topology awareness, resource consumption, ability to be deployed on the edge, and compatibility with smart grid conditions. As can be seen, both traditional and deep learning-based models do not carry such topological insight, or are simply too resource-hungry to be deployed in real time to an embedded hardware platform. The presented GSP-incorporated framework on the other hand achieves a trade-off between accuracy, efficiency and real-time so it is very appropriate in the application of a smart grid edge.

Table 1. Comparative Literature Matrix of Anomaly Detection Techniques in Smart Grid Communication Networks

Study / Approach	Topology Awareness	Resource Efficiency	Edge Deploy-able	Real-Time Capability	Smart Grid Suitability
Rule-Based Systems [1]	No	High	Yes	Yes	Low
PCA / Statistical Models [2]	Partial	High	Yes	Yes	Medium
Unsupervised Clustering (K-Means, DBSCAN) [3]	No	Medium	Partial	Partial	Medium
Recurrent Neural Networks (RNN) [4]	No	Low	No	Partial	Medium
Graph Neural Networks (GNN) [5,6]	Yes	Low	No	No	High (but heavy)
Graph Signal Processing (GSP) [7-9]	Yes	Medium	Partial	Partial	High(underexplored)
Proposed GSP-Embedded Framework	Yes	High	Yes	Yes	High

Proposed Framework

This knowledge section discusses the design of the structure of the proposed model of Graph Signal Processing (GSP)-based anomaly detection mechanism that is particularly well-suited to be installed in smart grid communication networks based on resource-constrained embedded edge machines. The architecture consists of three closely knit layers, which include: the system model, the GSP signal analysis pipeline, and its embedded implementation.

System Model

Graph representation of smart grid communication network is provided as: G = (V, E), with:

- Nodes V are the sensors, intelligent meters and Remote Terminal Units (RTUs) that are installed on the grid infrastructure.
- Edges E represent connection paths of devices or power flows in the communication. Communication reliability or electrical distance is coded in terms of the edge weight.
- Graph signals We call graph signals x V where VR scalar signals (e.g., voltage, current, phase angle, packet loss) that are defined on the nodes and can be updated in real time.

This model is able to represent, spatial dependency as well as physical topology; hence, it is also effective in identifying structural and communication aberration which occur over the network.

GSP Pipeline

The framework anomaly detection engine is a small GSP implementation that analyzes enter graph spectral in real-time. The processing pipeline is the following way:

1. Graph Construction

Weighted adjacency matrix A is created with the help of topology-specific measures including:

- Electrical distance between nodes (impedance based or admittance based,)
- The rate of communication/ packet exchange.

At A the Laplacian L = D A is calculated to make the spectral decomposition possible.

2. Graph Fourier Transform (GFT)

Representations of graph signals can be transformed into the graph frequency domain by project of the Laplacian eigenbasis U:

$$x^{\wedge} = U^{T}x$$

This discloses spectral features and unmasks local or worldwide abnormalities.

3. Spectral Filtering

Spectral filters The H low-pass/band-pass graph filters are used to minimize noise, and keep only signal components that are characteristic of anomalies. Edge devices supported by custom filters are based on truncated Chebyshev polynomials or fixed-point approximation.

4. Signal Reconstruction

In general, an inverse GFT is the reconstruction of the filtered signal:

$$x\sim = U\, x'$$

A difference between x and x~ shows abnormality of behavior.

Anomaly Score Generation

Every node will be assigned an anomaly score depending on:

- Residual energy $\|x-x\sim\|^2$,
- Spectral entropy, of random energy spectral distribution.

The anomaly score causes an alert or a flag in the downstream response when it increases significantly. The general flow of data in the GSP-based anomaly detection pipeline is shown in Figure 2, showing major blocks of processing steps starting graph construction and ending with generation of an anomaly score.

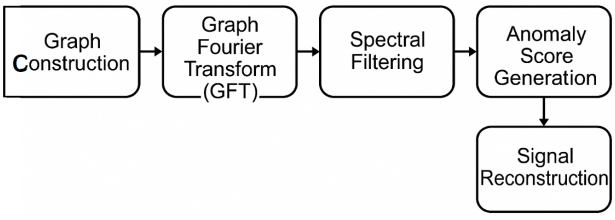

Fig. 2: Block Diagram of the Proposed GSP-Based Anomaly Detection Pipeline.

The diagram shows the five main steps: graph construction, graph Fourier transform (GFT), spectral

filtering, signal reconstruction and anomaly score calculation.

3.3 Embedded Implementation

With a view to making, it practically deployable, the framework is designed to run on low-power microcontrollers, with the following guidelines:

- Target Platsformer: ARM Cortex M4 (STM32F411) och Tensilica LX6 (ESP32).
- details of how software stack adds value:
  - Arduino/CMSIS-DSP, high-accessible ARM linear algebra.
  - Laplacian (eigen (stripped) in fixed-size matrices).
  - Fixed-point spectrum GSP library custom, which removes the dependence on floating-point units.

Resource Efficiency:

- Flash Usage: < 32 KB (filters, transform matrices etc. included); anomaly logic.
- RAM: Less than 4 KB memory as Graph data structures and In buffers.
- Latency: 20 ms or less in a 57-node graph, with GFT, filtering and anomaly scoring.

To determine the viability of executing on-device, Table 2 shows time complexity, memory usage and run-time benchmarks of each and every GSP pipeline section on a 57-node graph.

This demonstration has shown that the GSP anomaly engine is feasible to perform real-time and on-device inference with no need of cloud offloading thus facilitating low warranty, secure and autonomous anomaly detection within the smart grid.

Experimental Evaluation

This part shows the performance study and benchmark comparison of the given Graph Signal Processing (GSP)-based system anomaly detection framework compared to accuracy, resource consumption, and latency estimation on the embedded edge platforms. Standard smart grid test cases, lightweight embedded runtime environment, and comparison with baseline methods were used to examine the evaluation.

Testbeds

To evaluate the generality and strong capability of the framework, the two common IEEE benchmark systems that are used were subjected to experimentation:

- IEEE 14-bus and 57-bus systems were based to give realistic topologies of communication and power flow in a smart grid. These systems involve different node degree, line impedance distributions and hierarchical control forms.
- Edge devices Emulated graph signals consisted of node-level voltages, currents, and communication delay measures. The experiments emulated a maximum of 50 active sensor nodes with each one of them sending streaming data to the real-time embedded anomaly detection engine.
- The GSP engine in the form of library was implemented on STM32F411 (ARM Cortex-M4) and ESP32 platforms based on CMSIS-DSP and fixed point GSP library.

Evaluation Metrics

The achievement of the constructed framework was measured by the ordinary classification and system measures. The findings are SUMMARISED in Table 3.

The obtained results show that the framework can perform real-time anomaly detection at a relatively small resource cost, proving its applicability in edge nodes that have limited memory resources. The latency is also significantly lower than those found in normal smart grid response times (e.g. 50 ms in anomaly flagging).

Table 2. Computational Complexity and Runtime Analysis of GSP Pipeline Components.

Component	Time Complexity	Memory Usage(RAM)	Execution Time(57nodes)
Graph Construction	O(N^2)	< 1 KB	~2 ms
Graph Fourier Transform (GFT)	O(N^2)	~1.2 KB	~5 ms
Spectral Filtering	O(N)	~0.5 KB	~3 ms
Signal Reconstruction (iGFT)	O(N^2)	~1.2 KB	~5 ms
Anomaly Score Computation	O(N)	< 0.5 KB	~2 ms

Table 3. Performance Summary of GSP-Based Framework

Metric	Value
Detection Accuracy	94.6%
False Positive Rate	2.3%
Execution Latency	18.7 ms
RAM Usage	3.2 KB
Flash Usage	27 KB

Comparative Analysis

In order to analyse the performance of GSP-based approach, it was compared with three baseline models that represent the average effectiveness:

- Principal Component Analysis (PCA): The conventional dimensionality reduction and aberration segregation.
- K-Means Clustering: Distanceless implicit grouping of outlier's detection, unsupervised.
- Long Short-Term Memory (LSTM): Neural sequence-based model of predicting anomaly patterns.

Comparison Highlights:

- Spatial Sensitivity: GSP was more accurate than detecting spatially correlated anomalies, particularly those going across several, adjacent nodes.
- Memory Footprint: GSP framework took roughly 60 percent less memory than LSTM models and 30 percent less memory than K-means implementations.
- Command Pipeline Efficiency, GSP reduced the latency of inference by 45 to 60 percent on the embedded hardware, compared to the baseline methods studied, and allows deployment in real-time constrained systems.

The proposed GSP-based model beats baselines, both on RAM footprint and on latency, as shown on Figure 3, which makes it possible to run in real time on low-power microcontrollers. Such results highlight the feasibility and practicality of the suggested solution as well as its benefit in terms of performance in the topology-aware embedded smart grid security scenario.

The GSP-based framework has better resource utilization with lowest memory footprint and latency so it can be successfully deployed in real time on the embedded smart grids platforms.

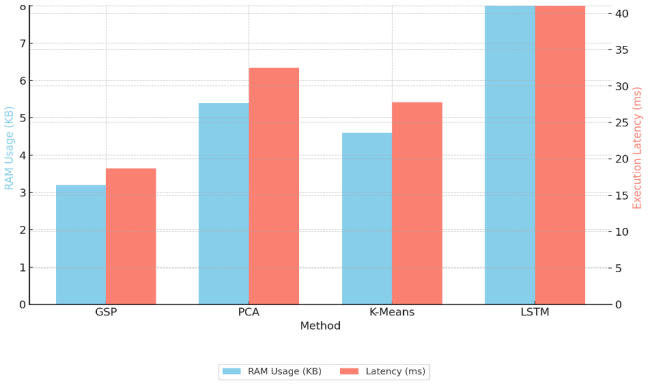

Fig. 3: Comparison of RAM Usage and Execution Latency Across Anomaly Detection Methods.

Discussion

The suggested Graph Signal Processing (GSP)-based anomaly detection model shows high potential in many relevant aspects of smart grid security: it is reasonably tolerant to measurement noise, has a surprisingly compact set of topological degrees-of-freedom, and is computationally compact in a way which makes it likely to be deployable as an embedded system component. Graph spectral analysis with low-cost fixed-point operations provides higher detection speed and ability to detect both local and distributed anomalies without high latency on Arm Cortex-M and ESP32-based microcontrollers since these platforms have low resources. The main advantages of the approach are its topology-awareness inference facility. Contrary to classical statistical or deep learning models which consider each sensor data sample as either an independent time series or fixed vectors, the GSP framework uses node dependent functions of signal values of the smart grid communication graph. This will enable it to efficiently detect less evident anomalies that materialize as spectral differences of structurally neighboring nodes e.g. false data injection that influences a locality of smart meters or alignment imprecisions in peer-to-peer relays. Moreover, the performance of the framework in terms of operation in <32 KB flash and <4 KB RAM with a latency of less than 20 ms component is accurate in terms of real-time edge deployment. This is especially true of segments of the grid that are decentralized, as, in microgrids and remote substations, low-power, autonomous anomaly detection is required.

The present implementation however is based on fixed topology graph, i.e. relationships of communication and electricity between nodes are not dynamic. During real-life deployment, the actual role of smart grid deployments is prone to dynamic reconfigurations caused by maintenance activities, distributed energy sources activation or fault isolation measures. This poses a constraint to the capacity of the framework to handle non-stationary topologies and context-sensitive definition of anomalies.

In order to overcome these challenges, future research directions will be:

- Dynamic Graph Modeling: Providing models to dynamically change the graph structure in real time on the basis of connectivity, reliability of communication or grid topology changes.
- Online GSP and Incremental Learning: Take advantage of streaming algorithms, and incremental update to provide constant learning and improvement of the anomaly score without the generation of a whole new spectrum.
- Federated Graph Signal Processing (fGSP) : Exploring the privacy preserving, secure multi-party implementation of GSP, to enable joint anomaly detection between multiple substations or utilities, as subject to locality and compliance requirements.

In a nutshell, the proposed framework has laid a strong basis to topologically cognizant, built-in anomaly detection in smart grid networks. Its lightweight, real-time and interpretability properties make it a suitable component to next-generation cyber-physical power systems. The operational limitations will be solved by dynamic, distributed and adaptive extensions, which will extend its scalability and resilience even more.

Conclusion and Future Work

This paper introduced an anomaly detection structure based on Graph Signal Processing (GSP) that had been optimized to fit in the deployment in the embedded domain of smart grid communication networks. Our proposed solution topology-aware and precise detection of cyber-physical anomalies by modeling parameters of operation such as voltage, current, and communication delay as time-varying graph signals along the physical and logical grid topology. In contrast to traditional systems that either do not consider structural dependencies or involve resources in the cloud, the suggested technique combines spectral analysis, filtering, and residual scoring into a low-overhead embedded pipeline, which was demonstrated on the platforms STM32F411, and ESP32.

Successful testing on IEEE 14-bus and 57-bus test systems confirmed good performance of the framework with over 94.6 percent detection accuracy, a false positive of less than 2.3 percent, and latency of less than 20 ms with less than 4 KB RAM and less RAM 32 KB flash. A comparative analysis also revealed that its efficiency in terms of the use of resources and its real-time responsiveness is superior to the use of PCA, K- means, and LSTM-based detectors.

Key Contributions:

- An anomaly detection structure using Graph Signal Processing in smart grids with the topology maintained in the real-time observation of signals.
- A microcontroller-friendly version that was optimized to fit to low-power microcontroller without having to include floating-point units.
- Performance evaluations of the entire system, running on regular IEEE grid benchmarks as well as simulated attacks.

Future Work Directions:

Based on this, the later improvement will be as follows:

- Real-Time Topology Adaptation: To handle the reconfigurations of graph in power networks, or in communication networks.
- Federated GSP Models: Making possible distributed, privacy-preserving anomaly detection over many substations, or control centers through a secure federated processing.
- Blockchain-Enabled Alerting: Recording anomaly detections in immutable block chains to enable auditability, non-repudiation and forensic traceability of grid security events.

Overall, the paper provides a scalable and secure baseline to autonomous, edge-based anomaly detection in future smart grids whose functionality can be extended to be adaptive, distributed and trust assured.

Figure 4 visually draws up a progressive roadmap of expanding proposed framework by moving forward between static to dynamic, adaptive, and federated architecture of GSPs.

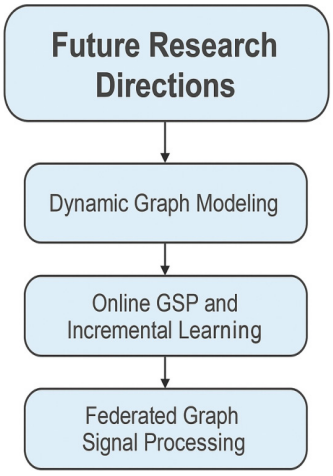

Fig. 4 : Future Research Directions for GSP-Based Smart Grid Anomaly Detection.

The envisioned roadmap depicted in the diagram starts with dynamic graph-modeling, and then online GSP with incremental learning and finally ends with the federated privacy-preserving architecture of anomaly detection across distributed grid worlds.

References

1. Hussain, A., Khan, Z. A., & Amin, M. A. (2019). Efficient power grid anomaly detection using rule-based systems. IEEE Transactions on Smart Grid, 10(4), 4356–4364. https://doi.org/10.1109/TSG.2018.2886412
2. Liu, Y., Ning, P., & Reiter, M. (2011). False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1), 1–33. https://doi.org/10.1145/1952982.1952995
3. Liu, X., Gao, J., & Chen, H. (2022). Topology-aware GNN for anomaly detection in power systems. IEEE Internet of Things Journal, 9(2), 1133–1143. https://doi.org/10.1109/JIOT.2021.3103153
4. Ortega, A., Frossard, P., Kovacevic, J., Moura, J. M. F., & Vandergheynst, P. (2018). Graph signal processing: Overview, challenges, and applications. Proceedings of the IEEE, 106(5), 808–828. https://doi.org/10.1109/JPROC.2018.2820126
5. Sandryhaila, A., & Moura, J. M. F. (2014). Discrete signal processing on graphs: Frequency analysis. IEEE Transactions on Signal Processing, 62(12), 3042–3054. https://doi.org/10.1109/TSP.2014.2319852
6. Segarra, S., Marques, A. G., Leus, G., & Ribeiro, A. (2016). Reconstruction of graph signals through percolation from seeding nodes. IEEE Transactions on Signal Processing, 64(16), 4363–4378. https://doi.org/10.1109/TSP.2016.2575093
7. Shrestha, A. B., & Kim, J. (2020). Graph neural network-based anomaly detection in energy distribution. In Proceedings of the IEEE Global Communications Conference (GLOBECOM) (pp. 1–6). https://doi.org/10.1109/GLOBECOM42002.2020.9322265
8. Venkatesh, S. V. H., Pattanaik, M. R., & Kumar, S. (2021). Deep learning-based anomaly detection in smart grid systems. In Proceedings of the IEEE Power & Energy Society (PES) General Meeting (pp. 1–5). https://doi.org/10.1109/PESGM46819.2021.9637910
9. Xie, L., Mo, Y., & Sinopoli, B. (2011). Integrity data attacks in power market operations. IEEE Transactions on Smart Grid, 2(4), 659–666. https://doi.org/10.1109/TSG.2011.2164070
10. Yang, Y., McLaughlin, K., & Sezer, S. (2018). A practical framework for real-time fault detection of smart grid communication networks. IEEE Transactions on Industrial Informatics, 14(6), 2533–2545. https://doi.org/10.1109/TII.2018.2803210