AI-driven Anomaly Detection with ICS Protocols in Smart Grids

Mamdouh Muhammad, Kanwardeep Singh, Reinhard German
Computer Networks and Communication Systems
Friedrich-Alexander-Universität Erlangen-Nürnberg
Erlangen, Germany
{mamdouh.muhammad, kanwardeep.singh, reinhard.german}@fau.de

***Abstract*—Smart grids are a modern approach to implementing and managing power grids, requiring the integration of Information Technology (IT) and Operational Technology (OT). This integration involves the use of Industrial Control System (ICS) protocols not only within air-gapped networks but also in networks connected to the internet. However, this advancement introduces cybersecurity vulnerabilities, making anomaly detection crucial for protecting grid infrastructure. Traditional detection methods, which rely on predefined signatures and static thresholds, struggle to counter evolving cyber threats. This paper proposes an AI-based anomaly detection framework tailored for ICS protocols in Smart Grids, with a specific focus on the Manufacturing Message Specification (MMS) protocol (IEC 61850). The system employs a Machine Learning (ML) model trained on simulated Smart Grid networks to identify deviations from normal patterns and detect cyber attacks in the form of Denial of Service (DoS) attacks. The experimental results demonstrate that the proposed approach improves anomaly detection evaluation metrics compared to statistical and other ML methods. This research contributes to Smart Grid security by leveraging AI techniques to detect subtle patterns of anomalies and offers a scalable, adaptive, and AI-driven solution for identifying cyber threats.**

***Index Terms*—Smart Grids, ICS, MMS Protocol, AI-driven, Cybersecurity, Anomaly Detection.**

I. Introduction

The digital transformation of power systems has led to the evolution of Smart Grids, which leverage advanced communication networks, automation, and real-time monitoring to enhance energy efficiency and reliability [1]. Unlike traditional power grids, Smart Grids integrate ICS protocols within IT networks, enabling intelligent decision-making, optimizing energy distribution, and improving resilience against faults [2]. However, this increased connectivity also introduces cybersecurity challenges, making Smart Grids more susceptible to cyber threats, system intrusions, and operational anomalies [4].

One of the key components in Smart Grid communication is the use of ICS protocols, such as IEC 61850 Manufacturing Message Specification (MMS), which facilitate real-time data exchange between critical infrastructural components [5]. While MMS enhances automation and interoperability, it also presents new security vulnerabilities. Traditional anomaly detection methods in ICS rely on rule-based or signature-based techniques, which are often ineffective against evolving and zero-day cyber threats [6]. These limitations necessitate the development of intelligent and adaptive real-time security solutions capable of detecting more sophisticated threats.

Recent advancements in Artificial Intelligence (AI) and Machine Learning (ML) models have shown great potential in cybersecurity applications, particularly in anomaly detection. By leveraging AI-driven techniques, it is possible to identify suspicious patterns and deviations from normal network behavior, allowing for early threat detection and mitigation [7]. However, integrating AI-based security measures with ICS protocols in real-time Smart Grid environments remains a challenge due to factors such as high data complexity, false alarm rates, and computational constraints.

This paper contributes:

1) An AI-based anomaly detection framework tailored for Smart Grids using the MMS protocol (IEC 61850) [3].
2) The experiment targets DoS attacks, which form over 41.1% of ICS threats [18], enabling precise detection and SHAP-based explainability.
3) The system boosts detection accuracy, lowers false positives, and strengthens MMS-based grid resilience.

The remainder of this paper is structured as follows: Section II outlines the related work in this field along with State-of-the-Art. Section III defines the system architecture and provides a threat model for the system. Section IV details the methodology, including data pre-processing, extraction, and ML models. Section V discusses experimental setup and performance evaluation. Finally, Sections VI, VII, and VIII conclude the paper with the results, the Discussion and the limitations of the model, the conclusion and future research directions.

II. Related Work

Several studies have explored leveraging anomaly detection techniques in Smart Grid security, merging ML and AI to improve threat detection and cybersecurity.

Regev et al. [9] presented a hybrid model utilizing AI, which integrates Long Short-Term Memory (LSTM) networks with Convolutional Neural Networks (CNNs) to detect anomalies in phasor measurement unit data. This

ISBN 978-3-903176-72-0 © 2025 IFIP

method successfully recognized anomalies in grid data, thereby improving the Smart Grid's resilience to cyber threats.

Sharma et al. [11] introduced a hybrid anomaly detection model combining Random Forests and Autoencoders to detect FDI and DoS attacks in ICS networks. Their study demonstrated improved accuracy and lower false positives compared to single-model approaches, though their dataset did not include real-time MMS communication logs, limiting its applicability to Smart Grid operations.

In their paper, Li et al. [19] proposed an unsupervised multivariate anomaly detection method based on Generative Adversarial Network (GAN)s and Long-Short Term-Memory Recurrent Neural Network (LSTM-RNN)s as the base model in GAN framework to capture the temporal correlation of time series distributions in CPSs. The experimental results proposed in this paper are effective in reporting anomalies caused by various cyber-intrusions compared in these complex real-world systems.

III. System Overview and Threat Model

A. System Architecture

The system architecture of the proposed Smart Grid model is structured into three layers, each playing a critical role in power distribution, communication, and monitoring. The architecture ensures efficient energy management and secure data exchange between power grid, control systems, and end-user devices. Fig. 1 illustrates this layered structure, where the power grid layer supplies electricity, the Neighborhood Area Network (NAN) Layer facilitates communication and control, and the Home Area Network (HAN) Layer manages energy consumption and smart devices at the user end.

- NAN Layer: This layer includes Utility Server, NAN Gateway, and MMS Protocol Communication. It manages energy distribution and communication between HANs and the central control system. It also integrates MMS Client for data requests from HANs and MMS Server for data response processing.
- HAN Layer: It contains AMI, Smart Meter, Hub, Smart Devices, Solar Panel, and Display Meter. Each HAN is responsible for monitoring energy consumption, solar output, and device control. The AMI module collects data from smart meters and interacts with the MMS Server.

B. Attack Scenarios and Threat Model

The Smart Grid integrates ICS protocols into traditional power grid to manage generation, distribution and open communication between key components such as AMI, Smart Meters, Utility Server, and Smart Devices. Despite its many advantages, these protocols are vulnerable to various cyber threats due to the open communication networks.
The attack scenarios in this paper focus on the NAN gateway, a critical communication node responsible for bi-directional communication between Utility Server and the two HANs.

TABLE I
Impact of DoS Attack at Each Layer of the Smart Grid

Component	Effect of DoS Attack	Detection Signature
HAN (Local)	Delayed/dropped outbound MMS reports from Smart Meters to Servers	Reduced response activity; irregular `Time`
MMS Server (HAN)	Backlog of unacknowledged messages; session timeouts	Delay in `MMS_Response` values
NAN Gateway	Flooded with fake MMS requests; communication bottleneck	Spike in traffic rate; unusual `MMS_Request_Type`
Utility Center	Misses real-time grid updates; late or false decisions	Stale/missing `Control_Signal` logs
AMI & Smart Devices	Delayed or no commands; instability in demand-response loops	`Device_Status` anomalies; wrong logs
Scope Blocks	Delays in timestamps; surge in request/response imbalance	Timing spikes; missing signals in CSV logs

DoS attack: This attack floods the NAN Gateway with excessive traffic, blocking legitimate MMS messages. Continuous connection requests overwhelm the network, disrupting communication between AMI and the Utility Server. This impairs real-time demand response and monitoring due to the gateway's limited resources, exposing a critical Smart Grid vulnerability and emphasizing the need for a robust detection framework.

These scenarios highlight key weaknesses in Smart Grid ICS communication, particularly at the NAN Gateway—crucial for AMI data flow. Without effective anomaly detection, such threats can cause service outages, financial loss, and grid instability. The proposed AI-driven system detects anomalies in MMS and IEC 61850 traffic, flags abnormal message behavior, and enables real-time cyber threat alerts. Table I outlines the DoS impact across Smart Grid layers.

IV. Methodology

This section presents the proposed approach, workflow and methodology by defining the scope, workflow approach, attack scenarios, validation and evaluation matrices. The developed method is designed to detect anomalies in the Smart Grids and minimize false positives to enhance the system security.

A. Workflow Approach

The methodology begins by defining the scope of the proposed solution in which the critical protocols are analyzed and the MMS protocol (IEC 61850) is selected to identify potential vulnerabilities and anomaly detection requirements.
This is followed by a system modeling phase, where a Smart Grid environment is simulated with the help of MATLAB Simulink to replicate real-world traffic and to communicate between different Smart Grid components such as HAN,

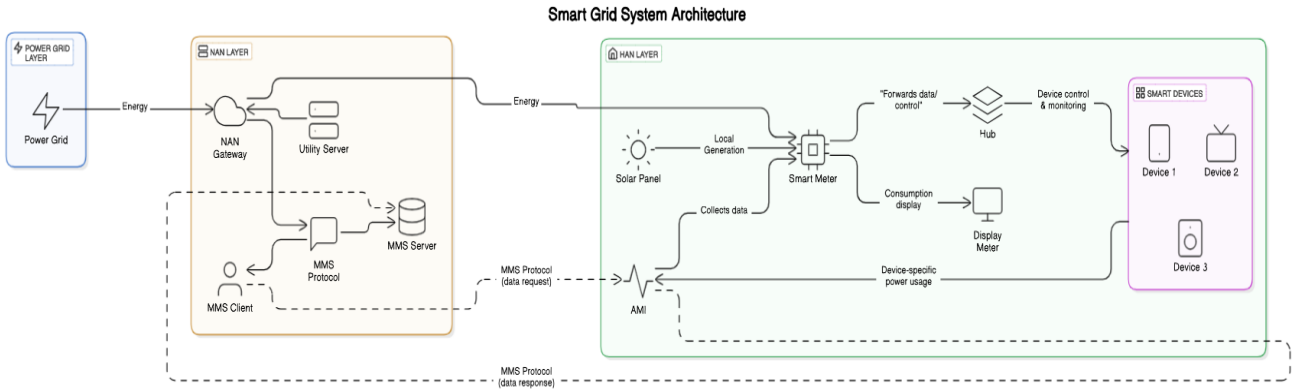

Fig. 1. System Architecture.

NAN, Utility Server, SCADA system and smart meter.
Once the modeling is complete, the feature extraction process is carried out to capture essential characteristics of the simulated network. These characteristics include timestamp, power and voltage outputs, device status, MMS request type, MMS response code, MMS command code and attack flag. In the ML model training phase, various AI models are applied to classify the data as normal or anomalous. In this paper, Isolation Forest (IF) and Local Outlier Factors (LOF) models are trained on simulated attack scenarios to improve the evaluation metrics of the anomaly detection.
DoS attack is introduced to ensure the robustness of the framework, targeting the MMS protocol communication within the Smart Grid model. The attack is systematically introduced to assess the effectiveness of the anomaly detection models in case of adversarial conditions.

The AI-based anomaly detection system is then integrated into the MATLAB Simulink environment, where real-time classification of anomalies is performed based on extracted features. The trained models are deployed in a MATLAB Function block, allowing the detection mechanism to operate dynamically on live Smart Grid data.

Subsequently, in the evaluation phase, accuracy, precision, recall, and F1-score of the ML models are assessed. The detection results are then compared against baseline statistical methods to demonstrate the effectiveness of AI-driven anomaly detection in reducing false positives and improving threat identification.
Finally, the results are visualized through dashboards and graphical plots, allowing system operators to monitor grid health and respond to anomalies in real-time.

B. MMS Protocol Integration

To enable secure and standardized communication, MMS protocol is integrated via various components.

The MMS Client in the Utility Server sends data requests (e.g., GetDataValues, Read, Write) to the *MMS Server* in the HAN, which processes these requests and returns data like PowerConsumption or SolarOutput. Communication between client and server is handled via *TCP/IP blocks*, simulating real-world Smart Grid operations. *MATLAB functions* generate the necessary MMS transaction codes, including RequestCode, ResponseCode, and CommandCode.

C. Data Collection and Analysis

This section elaborates on how the data is acquired, organized, and utilized for model evaluation While data pre-processing, feature selection, and normalization will be addressed in the Experiment Setup.

1) Data Acquisition: The dataset used for this research is generated through MATLAB Simulink-based simulations, replicating real-world Smart Grid communications. Multiple *To Workspace* blocks are strategically placed across critical components such as HAN, NAN, Smart Meter, AMI, and Utility Server to collect diverse operational and communication parameters. The recorded parameters include:

- Smart Grid Metrics: Voltage, frequency, power consumption, and solar output.
- MMS Protocol Transactions: RequestType, ResponseCode, CommandType, and TransmissionDelay.
- Attack Indicators: System anomalies caused by the DoS attacks.

2) Data Organization and Storage: The collected data is systematically structured in CSV format, ensuring compatibility with ML models for anomaly detection. Two distinct datasets are created:

- Normal Dataset: Captures standard grid operations under normal conditions.
- Attack Dataset: Includes malicious MMS transactions and their corresponding impact on grid stability.

Each dataset entry is timestamped, allowing for time-series analysis of anomalies and potential correlations between attack occurrences and grid performance fluctuations.

3) Exploratory Data Analysis (EDA) and Visualization: Before AI model training, EDA techniques are applied to uncover patterns in normal vs. attack traffic.

D. AI-Based Anomaly Detection

To identify cyber threats, IF and LOF are employed. These ML techniques analyze traffic patterns at the NAN

gateway, detecting anomalies that indicate potential security breaches. By leveraging a combination of unsupervised learning and deep learning approaches, the aim is to enhance detection metrics, adaptability to new attack patterns, and real-time threat identification.

- Isolation Forest: In a data-driven random tree, data instances are recursively partitioned until isolated. This random partitioning leads to noticeably shorter paths for anomalies due to the limited number of anomalous instances resulting in fewer partitions, which create shorter paths in the tree structure. Also, instances with clearly distinguishable attribute values are more likely to be separated during the early stages of partitioning [13]. Therefore, when a collection of random trees generates shorter path lengths for certain points, those points are likely to be anomalies.
- Local Outlier Factors: The LOF algorithm is defined in [14] by using density-based methods. For each data point, the process of finding the LOF includes calculating the degree of outlyingness. LOF is defined as the distance between the two data points p and o, which can be calculated by using a Euclidean n-dimensional space [15].

E. Comparison with related methodologies

Several studies in section II have proposed AI-based anomaly detection methods in Smart Grid environments. Regev et al. [9] utilized a hybrid deep learning model combining LSTM and CNN to detect general anomalies in real phasor measurement unit (PMU) data. Huang et al. [10] focused on MMS-based Advanced Metering Infrastructure (AMI) under False Data Injection (FDI) attacks, using statistical and threshold-based methods in a simulated AMI environment. Sharma et al. [11] proposed a hybrid model based on Random Forest and Autoencoders for detecting FDI and DoS attacks in generic ICS datasets. In contrast, this work specifically targets Denial-of-Service (DoS) attacks in MMS (IEC 61850) protocol-based Smart Grids using a real-time Simulink environment. It leverages unsupervised learning models—IF and LOF to detect anomalies effectively.

V. Experiment Setup

The experimental configuration aims to assess how well the AI-driven anomaly detection framework can identify cyber threats in MMS-based Smart Grid communications. The experiment is divided into three main phases: generating data, implementing the anomaly detection model, and evaluating the performance. The Smart Grid model, based on MATLAB Simulink, serves as the testing platform, simulating typical grid operation alongside traffic generated by cyber-attacks at the NAN Gateway.

A. Smart Grid Simulation Environment

This paper aims to replicate a realistic Smart Grid architecture via MATLAB Simulink environment as depicted in Fig. 2. This figure consists of the following:

- An NAN connected to the Utility Server via the NAN Gateway .
- Two HANs connected to NAN and contain AMI, Smart Meters, Display Meters and Smart Devices.
- MMS Client and Server to facilitate data exchange between grid components
- A power grid connected to the entire system to generate power supply.

B. Attack Traffic Generation

In order to evaluate the resilience of the anomaly detection framework, this experiment incorporates DoS attack at the NAN Gateway:

The experiment begins with a uniform sample generator at the NAN gateway, which receives over 5,000 MMS message requests within seconds, depleting its computational and bandwidth resources. The sampling frequency of the generator is subsequently randomized to ensure a realistic replication of the attack scenario. Overloading the NAN gateway with irrelevant MMS messages leads to communication delays and packet loss.

C. Data Preparation & Pre-processing

During runtime, the *To Workspace* blocks in the environment collect simulation data from various points in the model. This data is then processed and structured using MATLAB scripts, which generate a comprehensive CSV file for analysis and validation.

1) Data Preparation and Collection: The dataset is collected directly from the MATLAB Simulink Smart Grid simulation model during runtime. *To Workspace* blocks are strategically placed at key locations in the system, including:

- Smart Meters and AMI to capture Power Consumption, Voltage, and Frequency.
- NAN Gateway to extract MMS RequestTypes, ResponseCode, and Control Signals.
- Utility Server and HANs to monitor Outage Alerts, Device Status, and Solar Output.

Once the simulation completes execution, the recorded data is automatically stored in the MATLAB workspace as structured variables. A MATLAB script is used to extract logged variables from the workspace, ensuring that each row represents a unique timestamped event. The script performs automatic synchronization of variables, aligning them based on their respective timestamps.

2) Dataset Features: Ten key features were generated from the simulation and are divided into three primary categories based on the nature of the features:

- Grid Operational Parameters: Power_Consumption, Voltage, Frequency, Solar Output, and Device Status.
- MMS Communication Logs: MMS RequestType, and ResponseCode.
- Anomaly Indicators: Outage alerts, Control_Signals, and an attack flag indicating cyber threats.

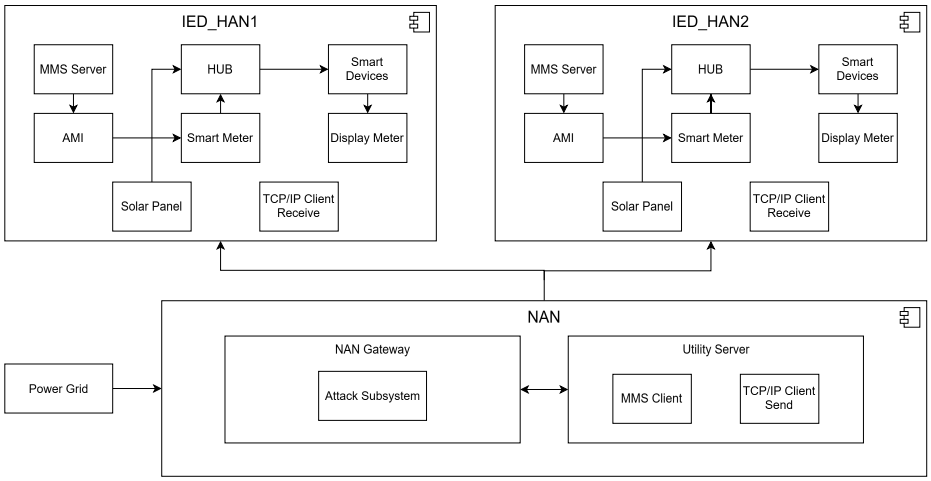

Fig. 2. The Smart Grid Setup (1 NAN and 2 HANs).

3) Data Pre-processing: Prior to training the anomaly detection models, the dataset is subjected to numerous pre-processing steps to guarantee data consistency and to enhance model effectiveness.

- Timestamp synchronization: Every logged event is synchronized in time to ensure a consistent sequence in the flow of messages. Any absent timestamps are interpolated linearly to bridge gaps without introducing any bias.
- Feature encoding: Categorical variables like MMS_Request_Type, MMS_Response, and MMS_Command are transformed into numerical representations through one-hot encoding. Categorical features such as Control_Signal and Device_Status are encoded numerically to enhance processing efficiency.
- Feature normalization: To ensure uniform scaling, numerical features like Power_Consumption, Voltage, Frequency and Solar_Output are normalized between 0 and 1 using Min-Max Scaling:

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

This prevents models from biasing towards high-magnitude features, improving learning stability [17].

D. AI-Based Anomaly Detection Implementation

The framework for detecting anomalies driven by AI is designed to identify cyber threats within MMS-based Smart Grid communications at the NAN Gateway. The detection mechanism utilizes two unsupervised ML methods, IF and LOF. These models analyze real-time MMS request-response traffic, control signals, power measurements, and voltage variations to differentiate between normal grid operations and anomalies caused by attacks.

1) Model selection justification: Two AI techniques for detecting anomalies are employed to examine the behavior of network traffic in the Smart Grid simulation:

- IF: This ensemble technique that relies on trees identifies anomalies by segmenting the feature space. It is effective for detecting DoS attacks, where unusual patterns in traffic volume are observed.
- LOF: This is a density-based approach that detects outliers by assessing local variations in relation to neighbors. It is also effective at identifying DoS attacks, where minor delays to messages take place.

2) Feature Selection for Anomaly Detection: Fig. 3 refers to the features that contribute to identifying abnormalities in ICS protocol behavior using SHAP (SHapley Additive exPlanations). To provide model interpretability and to better understand how individual features influence anomaly predictions, SHAP analysis was conducted on the IF model. The resulting summary plot revealed that features such as Power_Consumption, Voltage, and MMS_Request_Type were the most influential in determining anomalies. Notably, extreme values in power usage and voltage, either too high or too low, were consistently associated with elevated anomaly scores, indicating their critical role in identifying disruptions during DoS attack conditions. Furthermore, a high frequency of atypical MMS requests, particularly command-oriented operations, were strongly tied to anomalous behavior, reinforcing the protocol-level sensitivity of the detection framework.

E. Performance Validation & Evaluation

This section presents an in-depth assessment of the system's behavior under various attack scenarios, its practical deployment capabilities, and comparative performance analysis.

1) Validation Approach: To validate the reliability and efficiency of the system, multiple real-world-inspired attack scenarios were executed within the MATLAB Simulink simulation. The validation process includes:

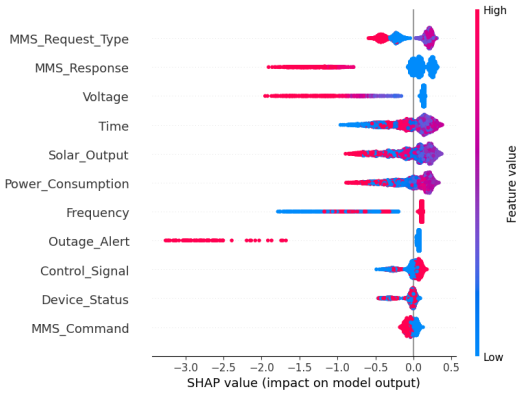

Fig. 3. Feature selection for ML model training.

- Scenario-based testing: The system is evaluated under different conditions, including normal grid operations, cyber-attacks, and post-attack recovery phases.
- Anomaly injection and model performance Evaluation: The effectiveness of anomaly detection is examined through logs, alerts, and system responses.

2) Effectiveness of Attack Detection: The AI-based detection system is evaluated by examining how well it identifies and differentiates normal vs. malicious MMS transactions. The following are considered:

- Attack impact on Smart Grid operations: The power flow disruptions, voltage fluctuations, and energy consumption anomalies caused by cyber-attacks are examined.
- Detection speed and false alarm rate: The rate of detection of false alarms vs. actual attack is examined to ensure high detection accuracy while minimizing unnecessary alerts.

3) Visualization and Operational Deployment: To enhance usability for Smart Grid operators, a real-time visualization dashboard is integrated into the system. This includes:

- Time-Series graphs: Tracking MMS protocol behavior under attack conditions.
- Alert system integration: Automating notifications for security teams.

VI. Results

This section showcases the experimental findings of the suggested AI-driven anomaly detection system within an MMS-integrated Smart Grid. The framework's effectiveness is evaluated through its classification performance.

A. AI Model Performance Analysis

1) Confusion Matrices: Fig. 4 shows the confusion matrix for the LOF and IF ML models trained on normal and attack traffic. These models, in general, demonstrate high accuracy in identifying cyber threats, with minimal false positives and false negatives.

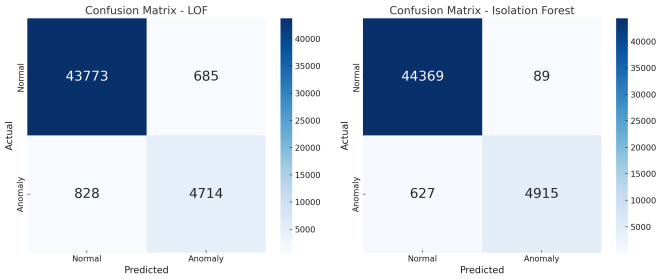

Fig. 4. Confusion Matrix for Local Outlier Factor & Isolation Forest.

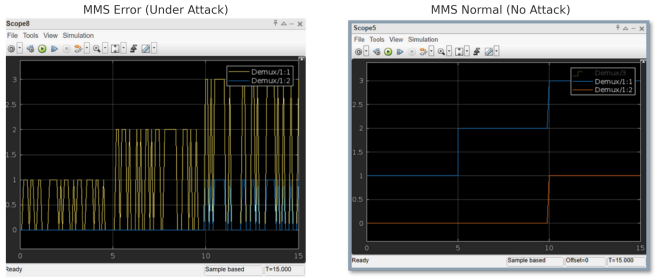

Fig. 5. MMS Request Code in Smart Grid Under Attack vs No Attack.

2) Classification Performance Metrics: Based on the comparison in Table II, the IF model outperforms LOF across all key performance metrics. IF achieves the highest accuracy (98.71%), ensuring reliable anomaly detection with minimal misclassification. Additionally, it records the best precision (99.11%), implying its low FPR, which is crucial for minimizing unnecessary alerts in a real-time Smart Grid environment. However, despite its high precision, its recall (89.2%) indicates that some attack instances remain undetected.

On the other hand, LOF demonstrates competitive accuracy, with 96.3%. However, the precision and recall values of LOF are significantly lower, suggesting a trade-off between false positives and false negatives.

The F1-score, which balances precision and recall, further highlights IF as the more effective model (93.89%) compared to LOF (86.9%). The comparison with the State-of-the-Art model in [19] is discussed in section VII.

TABLE II
Evaluation Metrics Comparison of DoS Detection Models

Metric	Isolation Forest	LOFs	LSTM [9]	MADGAN [19]
Accuracy (%)	96.71	94.3	90.38	–
Precision (%)	98.21	87.3	94.0	94.0
Recall (%)	88.7	85.07	91.23	88.0
F1-Score (%)	92.78	85.8	92.16	91.0

B. Impact of DoS Attacks on Smart Grid

Fig. 5 shows how a DoS attack disrupts MMS transactions, causing power communication delays and inaccurate Smart Meter readings. Below are the key areas affected:

1) Impact on MMS Protocol and Communication: DoS attacks increase latency in MMS exchanges between AMI and the Utility Server, often leading to errors or timeouts in TCP/IP communication.

2) Impact on Power Grid and Energy Flow: Communication delays prevent AMI and Smart Meters from updating power data, resulting in voltage fluctuations visible during attacks.

3) Effect on Attack Detection and Anomaly Flags: As shown in Fig. 5, Scope visualizations reveal network request spikes. The anomaly detection system triggers alerts (e.g., indicator lights), while Display Meters show incorrect consumption values.

VII. Discussion & Limitations

A. Discussion

1) Suitability of Unsupervised Models: Unsupervised models like IF and LOF are well-suited for real-time Smart Grid applications, particularly when labeled data is limited. Unlike deep learning methods such as LSTMs, CNN-AEs, and GANs, which demand substantial data and computational resources, IF and LOF are lightweight and efficient. IF is especially appropriate for memory-constrained nodes like HAN and NAN gateways due to its simplicity and low overhead, making it a practical choice for resource-limited environments.

2) Comparison with DL Models: Compared to models like MAD-GAN, IF delivers comparable or better performance with significantly less complexity. Its minimal resource requirements and independence from labeled data make it more suitable for real-time deployment in Smart Grids.

B. Limitations

Integrating ML-based anomaly detection into Smart Grid systems provides advantages but also introduces challenges in simulation and deployment.

Data Availability and Quality: Real Smart Grid data is difficult to access due to privacy concerns. As a result, synthetic data must be used, but accurately mimicking real-world variability remains a challenge.

Protocol Integration and Configuration: Integrating protocols into simulations can lead to version conflicts and timing mismatches. Synchronizing simulation clocks with server responses was necessary to avoid false positives and maintain model accuracy.

VIII. Conclusion

Based on the experiments conducted in this study, IF emerges as the more robust anomaly detection model compared to LOF due to its superior accuracy, precision, and balanced recall. Given these findings, IF is the preferred choice for real-time anomaly detection in MMS-based Smart Grid systems. Future work will focus on the generation of comprehensive datasets—if not publicly available—covering other widely used Industrial Control System (ICS) protocols, such as Modbus/TCP and DNP3, to ensure broader applicability and robustness across diverse Smart Grid environments. Additionally, we plan to explore the integration of advanced AI techniques, such as Large Language Models (LLMs), for contextual threat analysis.

References

[1] IEA (2025): Smart grids - IEA. Available online at https://www.iea.org/energy-system/electricity/smart-grids, updated on 3/2/2025, checked on 3/2/2025.

[2] V. C. Gungor et al., "Smart Grid Technologies: Communication Technologies and Standards," in *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, Nov. 2011, doi: 10.1109/TII.2011.2166794 .

[3] International Electrotechnical Commission, "IEC 61850 Standard for Communication Networks and Systems in Substations," [Online]. Available: https://iec61850.dvl.iec.ch/

[4] Mamdouh Muhammad, Abdullah S. Alshra'a, and Reinhard German. *Survey of Cybersecurity in Smart Grids Protocols and Datasets*. Procedia Computer Science, Volume 241, Pages 365–372, 2024. ISSN 1877-0509. https://doi.org/10.1016/j.procs.2024.08.049.

[5] T. S. Ustun and S. M. S. Hussain, "IEC 62351-4 Security Implementations for IEC 61850 MMS Messages," in *IEEE Access*, vol. 8, pp. 123979–123985, 2020, doi: 10.1109/ACCESS.2020.3001926 .

[6] Rules-based vs. anomaly detection (2025). Available online at https://www.ataccama.com/blog/anomaly-detection-rules-based/, updated on 3/2/2025, checked on 3/2/2025.

[7] Alsirhani, A., Tariq, N., Humayun, M. et al. Intrusion detection in Smart Grids using AI-based ensemble modelling. *Cluster Comput* 28, 238 (2025). https://doi.org/10.1007/s10586-024-04964-9.

[8] Bank, Dor, Koenigstein, Noam, and Giryes, Raja. (2020). Autoencoders. *arXiv preprint arXiv:2003.05991* . https://doi.org/10.48550/arXiv.2003.05991.

[9] A. Regev, H. Vassdal, U. Halden, F. O. Catak, and U. Cali, "Hybrid AI-based anomaly detection model using phasor measurement unit data," *preprint arXiv:2209.12665* , 2022.

[10] X. Huang, D. Zhao, and B. Wang, "False data injection attacks on MMS-based AMI: Detection and prevention," *IEEE Access*, vol. 9, pp. 75236–75245, 2021.

[11] A. Sharma, V. Gupta, and P. Ranjan, "A hybrid AI framework for anomaly detection in industrial control networks," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 16721–16730, 2022.

[12] Naidu, G., Zuva, T., Sibanda, E.M. (2023). A Review of Evaluation Metrics in Machine Learning Algorithms. In: Silhavy, R., Silhavy, P. (eds) *AI Application in Networks and Systems*. CSOC 2023. Lecture Notes in Networks and Systems, vol 724. Springer, Cham.

[13] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in *2008 Eighth IEEE International Conference on Data Mining*, Pisa, Italy, 2008, pp. 413–422, doi: 10.1109/ICDM.2008.17 .

[14] Breunig, M.M., Kriegel, H.-P., Ng, R.T., and Sander, J. LOF: Identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (SIGMOD '00)*, Dallas, TX, USA, 16–18 May 2000.

[15] Alghushairy, O., Alsini, R., Soule, T., and Ma, X. A Review of Local Outlier Factor Algorithms for Outlier Detection in Big Data Streams. *Big Data Cogn. Comput.* 2021, 5, 1.

[16] Rumelhart, D.E., Hinton, G.E., and Williams, R.J. Parallel distributed processing: Explorations in the microstructure of cognition, vol. 1. chap. Learning Internal Representations by Error Propagation, pp. 318–362. MIT Press, Cambridge, MA, USA (1986).

[17] Selim Aksoy and Robert M. Haralick, Feature normalization and likelihood-based similarity measures for image retrieval, *Pattern Recognition Letters*, Volume 22, Issue 5, 2001.

[18] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2024 – July 2023 to June 2024," European Union Agency for Cybersecurity, 2024, doi: 10.2824/0710888 .

[19] D. Li, D. Chen, L. Shi, B. Jin, J. Goh, and S.-K. Ng, MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks. [Online]. Available: http://arxiv.org/pdf/1901.04997.