Detecting Denial of Service Attacks in Smart Grids Using Machine Learning: A Study of IEC 61850 Protocols

Antonin Delhomme
National Graduate School of Engineering of Caen (ENSICaen)
Caen, France
e-mail: antonin.delhomme@ecole.ensicaen.fr

Livinus Obiora Nweke
Noroff University College
4612 Kristiansand S, Norway
e-mail: livinus.nweke@noroff.no

Sule Yildirim Yayilgan
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway
e-mail: sule.yildirim@ntnu.no

***Abstract*—The increasing digitalization of power grids, often referred to as smart grids, has revolutionized the efficiency and functionality of electrical infrastructure. Smart grids integrate advanced communication technologies and digital controls to optimize the generation, distribution, and consumption of electricity. However, this digital transformation has also introduced significant cybersecurity challenges. As these grids are critical national infrastructures, ensuring their protection against cyber threats is essential. This study investigates the application of various machine learning algorithms to detect Denial of Service (DoS) attacks within the International Electrotechnical Commission (IEC) 61850 communication protocols, specifically Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV). We employed a simulated substation communication environment to generate normal and attack scenarios, utilizing both GOOSE and SV messages. The machine learning models used in our experiment include a Random Forest Classifier, Decision Tree, Support Vector Machine (SVM), Neural Networks, K-Nearest Neighbors (KNN), Logistic Regression, Gradient Boosting, and a Voting Classifier. The results demonstrated that the Random Forest Classifier and Decision Tree models consistently achieved high accuracy and F1 scores, making them effective for DoS detection in IEC 61850 protocols. The Voting Classifier also showed strong performance, leveraging the strengths of multiple models. Despite the generally good performance of these models, the SVM and Voting Classifier provided the best results in a specific instance with reduced data volume. Training time was also considered, highlighting Decision Tree and Logistic Regression as the most efficient models for quick deployment. This study underscores the potential of machine learning-based approaches for enhancing the security of substation communication systems, providing valuable insights for future research and practical applications in the field of smart grid cybersecurity.**

Keywords-Smart Grids; Digital Substation; Machine Learning; Deep Learning; DoS Attacks; Cyber-Attack Detection.

I. INTRODUCTION

The modernization of electrical power systems has led to the integration of advanced communication technologies to enhance the efficiency and reliability of power delivery. Among these technologies, the IEC 61850 standard [1] has emerged as the foundation for substation automation, enabling real-time data exchange and event-triggered messaging through protocols, such as Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV). These protocols facilitate crucial functions like protection, control, and monitoring of substations, which are the basis of smart grid communications [1]. However, the increasing reliance on digital communications within substations has also exposed these systems to a range of cyber threats. One of the most significant and pervasive threats is the Denial of Service (DoS) attacks, which aim to overwhelm the communication network with a flood of malicious traffic, thereby disrupting normal operations and potentially leading to catastrophic failures in power delivery [2]. The critical nature of these systems necessitates robust and reliable methods for detecting and mitigating such attacks to ensure the security and stability of the power grid.

Despite advancements in substation automation and security measures, detecting DoS attacks within the IEC 61850 protocols remains a difficult task. Tradition Intrusion Detection Systems (IDS) typically rely on predefined thresholds and signatures to identify malicious activity [3]. However, these methods struggle to keep up with sophisticated and evolving attack patterns. Consequently, there is an urgent need for innovative approaches that can dynamically learn and adapt to new threats. To address this need, this study investigates the efficacy of various machine learning algorithms in detecting DoS attacks within the IEC 61850 communication protocols, with a primary focus on the GOOSE and SV protocols.

The main contributions of this paper are as follows:

1) We develop a testbed using the IEC 61850 protocols (GOOSE and SV) to simulate both normal and DoS attack scenarios in a substation environment.
2) We employ a variety of machine learning models, including Random Forest, Decision Tree, SVM, Neural Networks, KNN, and a Voting Classifier, to detect DoS attacks in these protocols.
3) We provide a comprehensive evaluation of these models based on performance metrics like accuracy, F1-score, training time, and computational efficiency, identifying Random Forest and Decision Tree as the best-performing models.
4) We introduce a new feature, “Timediff", which improves the ability of models to distinguish between normal and

attack traffic, further enhancing the detection of anomalies in GOOSE and SV messages.

This study holds significant importance for several reasons. Firstly, it addresses a critical gap in the cybersecurity of smart grids by focusing on the detection of DoS attacks within the IEC 61850 communication protocols. As the adoption of smart grid technologies continues to grow, ensuring the security of these systems becomes paramount to maintaining reliable power delivery and preventing potential blackouts. Secondly, by exploring the application of machine learning algorithms for intrusion detection, this research contributes to the broader field of cybersecurity by demonstrating the potential of advanced analytical techniques in identifying and mitigating cyber threats. Moreover, the insights gained from this research can guide future studies and practical implementations, providing a foundation for ongoing efforts to enhance the resilience of smart grid communications against cyber attacks.

The rest of the paper is structured as follows. Section 2 delves deeper into this topic. Section 3 describes our data collection process. Section 4 outlines the subsequent steps, such as training models and converting data for these models. Section 5 presents our findings and conclusions. Finally, Section 6 provides a concise summary of the results, discusses their implications, and suggests potential areas for future research and improvements in this field.

II. Related Work

The field of cybersecurity, particularly in the context of digital substations and the detection and mitigation of DoS attacks, has garnered significant attention in recent years. Numerous studies have advanced our understanding of the unique challenges and effective solutions for protecting these crucial infrastructures. Our research extends the work in [4], which emphasizes the necessity of realistic simulation environments to test and improve detection mechanisms. The study highlights the critical role of advanced simulators that replicate various attack scenarios, thus enhancing our ability to respond to cyber threats without jeopardizing real power grids. The authors in [5] explore the vulnerabilities inherent in power system automation and protection schemes, providing a detailed analysis of the impacts of cyber-attacks on power system stability and reliability. This work aids in developing robust protection mechanisms against threats like DoS attacks.

The paper in [6] addresses core cybersecurity issues in digital substations, identifying challenges associated with the integration of digital technologies and underscoring the need for specialized cybersecurity measures. Complementary to this, the work in [7] proposes a method for identifying network anomalies using the IEC 61850 standard, which enhances real-time monitoring and detection capabilities. The authors in [8], provide a comprehensive survey of cybersecurity challenges within the smart grid, including digital substations. They outline major threats and evaluate current cybersecurity measures, providing insights into future research directions. Similarly, the authors in [9] review existing Intrusion Detection and Prevention systems (IDPS) for digital substations, assessing their effectiveness against specific threats in these environments. Also, the paper in [10] evaluates security threats to smart grid communication networks, covering a range of potential attacks, including DoS, and assessing their impact on grid operations.

The work in [11] highlights the threat posed by DoS attacks on IEC 61850-based substation automation systems, emphasizing their vulnerabilities and the need for robust detection and mitigation strategies. Likewise, the authors in [12] focus on developing a lightweight and effective Network Intrusion Detection System (NIDS) that balances detection effectiveness with resource efficiency. In the realm of intrusion detection, the paper by [13] introduces a system designed for IEC 61850 automated substations that enhances detection accuracy and response times. This is further supported by work in [2], which presents a novel method for detecting DoS attacks using Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) modeling of GOOSE communication.

Furthermore, the study in [14] addresses the simulation modeling and analysis of DoS attacks, with a particular focus on the SYN-Flood attack method, providing practical insights into various mitigation strategies. In the same way, the authors in [15] investigate how DoS attacks can compromise protection schemes and propose methods to enhance their resilience.

While significant progress has been made in applying machine learning to detect cyber threats in power systems, there remains a need for comprehensive studies that evaluate multiple machine learning models under realistic substation communication scenarios. Most existing research either focuses on a limited set of algorithms or lacks detailed analysis of the performance metrics across different traffic conditions.

This study aims to fill this gap by providing a thorough evaluation of various machine learning algorithms for detecting DoS attacks within IEC 61850 GOOSE and SV protocols. To achieve this, we simulate DoS attacks in a controlled digital substation environment using the emulator described in [16]. We then apply various machine learning methods to detect these attacks. We also compare these multiple machine learning algorithms, offering a comprehensive evaluation of their strengths and weaknesses to identify the most effective approach. This research provides valuable insights into the effectiveness of these models in real-world substation environments.

III. Methodology

This section details the experimental setup, data collection, preprocessing, feature engineering, and the machine learning models used to detect DoS attacks in IEC 61850 protocols (GOOSE and SV messages).

A. Experimental setup

For the simulation environment, we used the SGSim emulator [16] to simulate the substation communication, including devices such as Intelligent Electronic Devices (IEDs), Digital Primary Substations (DPS), and Digital Secondary Substations (DSS), as illustrated in Figure 1. The testbed ran on a system with the following hardware and software specifications:

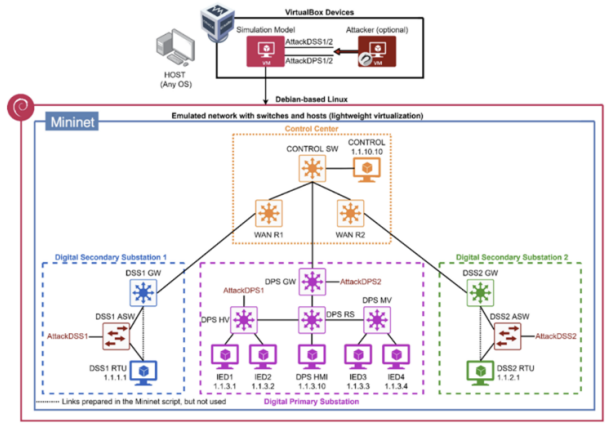

Figure 1. Complete Topology of the Simulator SGSim [16].

- Hardware: Intel Core i7-9700K processor, 16 GB RAM, NVIDIA GTX 1080 GPU.
- Software: The emulator ran on Ubuntu 20.04, and the machine learning algorithms were implemented using Python 3.8 with Scikit-learn 0.24.2 for the model training and evaluation. Wireshark (v3.4.5) and Tshark were used for data capture and conversion to CSV format.

These specifications ensure the results are reproducible in similar environments, and provide a foundation for researchers looking to replicate or extend this work.

B. Data Collection

The dataset used for this experiment was generated based on the topology as shown in Figure 1. It consisted of the components listed in the previous section where the IED communicate with each other using the GOOSE and/or SV protocol defined in the IEC 61850 standard. GOOSE and/or SV network packets were generated to represent normal and attack scenarios. A comprehensive approach was taken to identify and mitigate DoS attacks through machine learning models, setting the stage for experimental findings. By leveraging the unique features of GOOSE and SV messages, it becomes possible to detect anomalies and protect digital substations more effectively.

Table I shows the basic features of a GOOSE message [17]. These features are extracted from network packet headers and can be observed in captured messages, for example, using the Wireshark tool [18]. The first two columns show the feature name and its description, while the last column refers to the protocol analyzer name ‘tshark’ [19], which reads previously captured network files and decodes those packets to the standard output (Comma-Separated Value (CSV) files). These CSV files are then used in machine learning algorithms, as described in further sections.

Similarly, Table II presents the basic features of an SV message [20]. These features are also extracted from network packet headers and can be observed in captured messages using Wireshark [18]. These features laid the groundwork for analyzing GOOSE and SV messages to identify anomalies

TABLE I
BASIC FEATURES OF GOOSE MESSAGES.

Feature Name	Description	tshark Name
GOOSE APPID	Application Identification	goose.appid
GOOSE Length	GOOSE message length	goose.length
GOOSE gocbRef	GOOSE control block reference	goose.gocbRef
GOOSE TTL	Maximum wait time for message	goose.timeAllowedtoLive
GOOSE dataset	Object reference of control block	goose.datSet
GOOSE goID	GOOSE message identification	goose.goID
GOOSE time	Time to stNum increase	goose.t
GOOSE stNum	Status number	goose.stNum
GOOSE sqNum	Sequence number	goose.sqNum
GOOSE confRev	Configuration revision	goose.confRev
GOOSE numDataSetEntries	Number of dataset entries	goose.numDatSetEntries
GOOSE data	Variable sensor data	goose.data
Time of packet	Time of packet recording	frame.time
Time interval	Time interval from the previous packet	frame.time_delta
Interval_between_devices	Time interval between use of field devices	NA
Interval_between_state_info	Time interval between control command or state information retrieval	NA

TABLE II
BASIC FEATURES OF SV MESSAGES.

Feature Name	Description	tshark Name
SV APPID	Application Identification	sv.appid
SV Length	SV message length	sv.length
SV svID	SV message identifier	sv.svID
SV smpCnt	Sample count	sv.smpCnt
SV confRev	Configuration revision	sv.confRev
SV smpSynch	Sample synchronization	sv.smpSynch
SV datSet	Data set reference	sv.datSet
SV smpRate	Sample rate	sv.smpRate
SV time	Time of sample	sv.time
SV data	Sampled data values	sv.data
Time of packet	Time of packet recording	frame.time
Time interval	Time interval from the previous packet	frame.time_delta
Interval_between_devices	Time interval between use of field devices	NA
Interval_between_state_info	Time interval between control command or state information retrieval	NA

and potential DoS attacks. By converting these features into CSV files using ‘shark’ [19], machine learning algorithms can process them to train and assess models, thus establishing a solid framework for securing IEC 61850-based digital substations. With data collection complete, our next step was to define the scenarios and how to process the data.

C. Scenarios and Data Preprocessing

The GOOSE and SV protocols, part of the IEC 61850 standards, are critical for real-time data exchange and event-triggered messaging, essential for substation automation and control. In this setup, both protocols were utilized to simulate a realistic substation communication environment, with specific scenarios designed to evaluate normal operations and potential attack conditions. These scenarios allowed us to create a comprehensive dataset that includes both normal and attack conditions, ensuring our models could learn and generalize well. The data preprocessing steps were crucial in transforming raw data into a structured format suitable for machine learning.

1) Normal and Attack Scenarios: The following scenarios were developed to assess the performance of machine learning algorithms in identifying DoS attacks within IEC 61850 protocols (GOOSE and SV messages).

a) Normal Scenario: Two types of normal traffic scenarios were utilized to establish baseline data for the models:

- Normal Traffic: This scenario portrays the typical communication load within a substation, including the regular exchange of GOOSE and SV messages between Intelligent Electronic Devices (IEDs), substations, and the control center.
- Increased Traffic (2 times): This scenario simulates a higher load of normal traffic, doubling the amount of regular communication. It tests the performance of the models under heavier but legitimate communication loads. Both traffic scenarios were evaluated by considering three types of messages:
- GOOSE-only: Messages exclusively using the GOOSE protocol, typically employed for event-driven communication like protection relay signaling.
- SV-only: Messages exclusively using the SV protocol, often used for transmitting sampled measurement values from the primary equipment.
- GOOSE + SV: Combined traffic of both GOOSE and SV messages, representing a comprehensive communication environment within a substation.

b) Attack Scenario: Three types of attack scenarios were designed, each characterized by an increasing amount of malicious traffic, to assess the models' ability to detect threats under different levels of stress. These scenarios were:

- 4 times the amount of normal traffic: This scenario represents a moderate DoS attack, with the traffic load quadrupled compared to normal conditions. It tests the models' capability to detect early signs of an attack.
- 5 times the amount of normal traffic: This scenario represents a severe DoS attack, with the traffic load quintupled. It assesses the performance of the models under significant attack conditions.
- 6 times the amount of normal traffic: This scenario represents an extreme DoS attack, with the traffic load increased sixfold. It tests the models' limits in detecting and responding to very high levels of malicious traffic.

Due to simulator constraints, it was nearly impossible to generate combined GOOSE + SV traffic for the 6 times scenario. Each scenario was carefully monitored to ensure the integrity and accuracy of the data collected, providing a robust foundation for the subsequent data preprocessing steps.

2) Data Preprocessing Steps: Once the GOOSE and SV messages features were identified from the literature, the next step in the experiment was to pre-process the data collected using Wireshark [18]. The following are the main steps involved in the experiment for this process:

1) Identify relevant features required for the experiment from GOOSE and SV messages. It was found that in this experiment, only the following features were found relevant: Source, Destination, Timestamp, Length.
2) Use of 'tshark' scripts to convert wireshark files (pcap format) to machine learning readable format (csv).
3) Label data rows (0 for normal and 1 for attack). This labelling is done manually based on the context of the data, if it was during the attack or normal scenario.
4) Use feature engineering. A new feature named Timediff was introduced in the experiment, representing the time difference between two packets from the same protocol. This feature was designed to aid the model in understanding the relationship between these features and the target variable.
5) Scaling the values of each column.
6) Training different algorithms as mentioned in the next section.

These preprocessing steps ensured that the data was in a suitable format for training and evaluating machine learning models. With the data prepared, we then proceeded to the next phase of our experiment: employing machine learning algorithms to detect anomalies.

D. Machine Learning Based Anomaly Detection

Machine learning is a field that focuses on computational algorithms that can learn from their environment by mimicking human intelligence [21]. It can be divided into three modes of operation: Supervised, Unsupervised, and Semi-Supervised. In supervised learning, both the training and test datasets are labeled. The experiment utilized labeled datasets. The primary advantage of using machine learning in this context was that it allows for the detection of attacks without the need for a packet rate threshold. Thus, when raw GOOSE and SV messages were received, the system could extract relevant features and classify them as either an intrusion or normal event based on these trained models.

As mentioned in the previous section, attack-free data was initially generated using the experimental setup. This data was captured using Wireshark, after which the attack data was produced using the same setup. GOOSE and SV messages were extracted from the captured data for training various machine learning algorithms. The effectiveness of the proposed anomaly detection system was evaluated by introducing DoS attacks.

The following machine learning and deep learning models were employed in the experiment:

- Random Forest Classifier (RFC): This is an ensemble learning method for classification, which aggregates the results of multiple decision trees built on different subsamples of the training data.
- Support Vector Machines (SVM): This is a supervised learning algorithm used for classification and regression. It separates data into classes by finding the hyperplane in a high-dimensional space.
- Neural Network: We used the MLPClassifier from scikit-learn, a Neural Network model for Multi-Layer Perceptron (MLP) classification. It has parameters for the number of

hidden layers, activation functions, solver, and regularization, among others.

- K-Nearest Neighbors (KNN): This is a non-parametric, instance-based, supervised learning algorithm that classifies data points based on the majority class of its k-nearest neighbours in the feature space.
- Logistic Regression: This is a statistical method for binary and multi-class classification that models the relationship between the dependent variable and independent variables using a logistic function.
- Gradient Boosting: This is an ensemble machine learning technique that combines the predictions of multiple weak models to make a strong prediction using a gradient descent optimization algorithm.
- Decision Trees (DTs): This is a non-parametric supervised learning method used for classification and regression. It aims to create a model that predicts the value of a target variable by learning simple decision rules inferred from the data features.
- Voting Classifier: This machine learning model trains on a collection of several models and predicts an output (class) based on the class with the highest likelihood of becoming the output. The models used were LogisticRegression, DecisionTreeClassifier, SVC, MLPClassifier, and RandomForestClassifier. These choices will be explained in the results section.

For each machine learning model, we tuned key hyperparameters to optimize performance. For the Random Forest Classifier, we evaluated various values for the number of estimators, ranging from 50 to 200, and found that 100 estimators provided the best balance between accuracy and computational efficiency. Similarly, for Support Vector Machines, we adjusted the kernel function (linear, Radial Basic Function (RBF)), with RBF yielding the best results for our dataset. The hyperparameter tuning process was conducted using a grid search cross-validation, ensuring that each model's configuration was optimized for both accuracy and training time. These choices improved model robustness and reliability in detecting anomalies. Also, the 'train-test-split' function from the 'scikit-learn' library [22] was utilized to test the machine learning algorithms on 20% of the data points, which were randomly selected. The results from testing these algorithms are presented in the following section.

IV. Results

This section presents the outcomes of our experiments, evaluating the performance of various machine learning algorithms in detecting DoS attacks within IEC 61850 protocols. Different datasets were created using a simulated environment that mimics real-world substation conditions, including IEDs, gateways, control centers, and network communication protocols like GOOSE and SV. This setup allows for the introduction and monitoring of cyberattacks, providing a valuable data source for training and testing machine learning models. During the experiment, normal data was classified as 0, while attack data was classified as 1. We compared the best results with other models using various metrics, including training time, precision, recall, F1-Score, and accuracy. These metrics allowed us to evaluate the performance of different machine learning algorithms and identify the most effective approach for detecting DoS attacks in the dataset.

A. Complete dataset

Figure 2 presents the results of the various machine learning and deep learning algorithms described in the previous section, but only for those that produced good results. Some algorithms were biased or unable to draw conclusions. This may be due to the fact that during our experiment, the source and destination IP addresses were the same for each packet, which made class prediction more difficult.

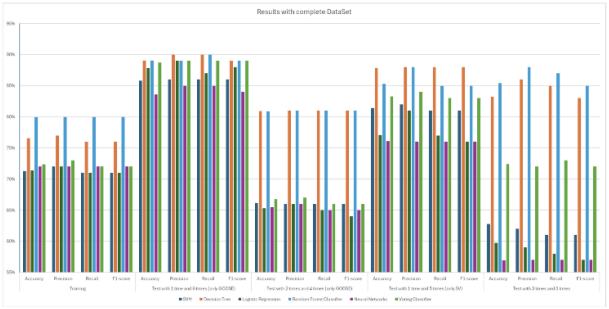

Figure 2. Results of the training and tests for different models.

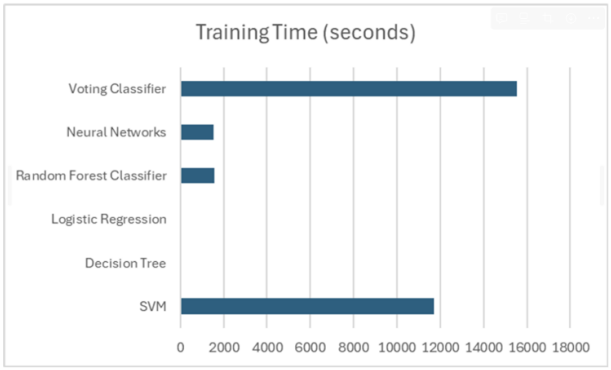

Figure 3. Time needed for different models to train on the dataset.

- Training Performance:
  - Random Forest Classifier: Achieved the highest training accuracy (79.95%) and F1-score (0.80), indicating strong learning capabilities from the training data.
  - Decision Tree: Showed an accuracy of 76.54% and an F1-score of 0.76, performing well but slightly less effective than Random Forest.
  - Voting Classifier: Demonstrated a 72.37% accuracy and a 0.72 F1-score, highlighting the effectiveness of combining multiple models.
  - Neural Networks, SVM, and Logistic Regression: Had similar performances with accuracies around 71-72% and F1-scores of 0.71-0.72.
- Testing Performance:

  - 1 Time and 6 Times GOOSE: Decision Tree and Random Forest led with accuracies of 89.07% and 89.06%, respectively, followed closely by Voting Classifier at 88.73%.
  - 2 Times and 4 Times GOOSE: Decision Tree and Random Forest were again the top performers with accuracies around 80.91%, whereas Voting Classifier dropped to 66.76%. SVM, Neural Networks, and Logistic Regression lagged behind.
  - 1 Time and 5 Times SV: Decision Tree achieved the highest accuracy of 87.86%, with Random Forest closely following at 85.30%. SVM and Neural Networks performed moderately well, while Logistic Regression trailed.
  - 3 Times and 5 Times: Random Forest excelled with 85.40% accuracy, while Decision Tree and Voting Classifier performed moderately.
- Training Time as shown in Figure 3:
  - SVM had the longest training time, making it less practical for quick deployments.
  - Decision Tree and Logistic Regression had the shortest training times, suitable for real-time applications.
  - Random Forest, Neural Networks, and Voting Classifier had moderate training times.

To summarize, Random Forest Classifier and Decision Tree consistently provided the best performance across various test scenarios, making them suitable choices for detecting DoS attacks in IEC 61850 protocols. The Voting Classifier also demonstrated strong performance by combining the strengths of multiple models. Neural Networks performed well in some scenarios but not as consistently as tree-based methods. SVM and Logistic Regression had mixed results and might not be the best choices considering SVM's longer training times and Logistic Regression's lower performance. Training time is a critical factor, with Decision Tree and Logistic Regression offering the quickest training, which can be advantageous for real-time or iterative model updates.

B. Incomplete dataset

For the incomplete dataset scenario, the data was halved to evaluate the models' performance with limited data. This helps assess the robustness of models when less data is available for training and testing. The results are shown in Figure 4. Previous models not represented here are missing because they gave the same results as before.

- Training Performance:
  - Voting Classifier: Achieved higher training accuracy (84.11%) compared to SVM (82.25%), with slightly better precision, recall, and F1-scores.
  - SVM: Although slightly lower in training accuracy, it excelled in testing scenarios.
- Testing Performance:
  - 1 Time and 6 Times GOOSE: SVM showed near-perfect performance with 99.74% accuracy, and perfect precision, recall, and F1-score. Voting Classifier also performed well with 98.18% accuracy.
  - 2 Times and 4 Times GOOSE: SVM outperformed Voting Classifier with 91.51% accuracy, while Voting Classifier struggled significantly in this scenario.
  - 1 Time and 5 Times SV: SVM continued its strong performance with 92.32% accuracy. Voting Classifier was slightly lower but still respectable.
  - 3 Times and 5 Times: SVM maintained good performance with 85.25% accuracy, while Voting Classifier showed a significant drop in performance.
- Training Time as shown in Figure 5:
  - Both models showed efficient training times compared to the complete dataset, with SVM being faster than the Voting Classifier.

SVM is highly recommended for detecting DoS attacks in IEC 61850 protocols due to its consistent high accuracy, precision, recall, and F1-score across various test scenarios. The Voting Classifier also shows potential but may need further tuning to handle specific test scenarios more effectively and reduce the training time. The reduced dataset indicates that SVM can handle limited data availability well, while the Voting Classifier's performance is more variable, potentially overfitting the larger dataset.

The findings from both datasets highlight the importance of

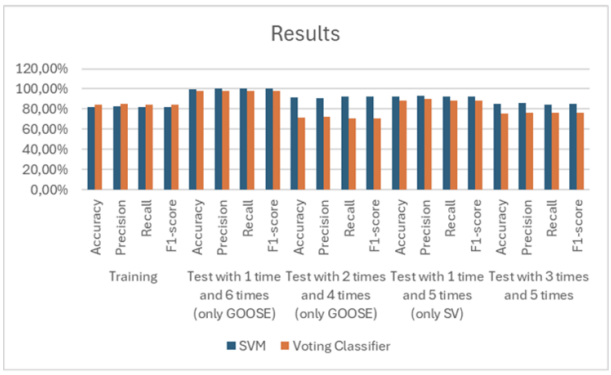

Figure 4. Results of the training and tests for 2 models with incomplete dataset.

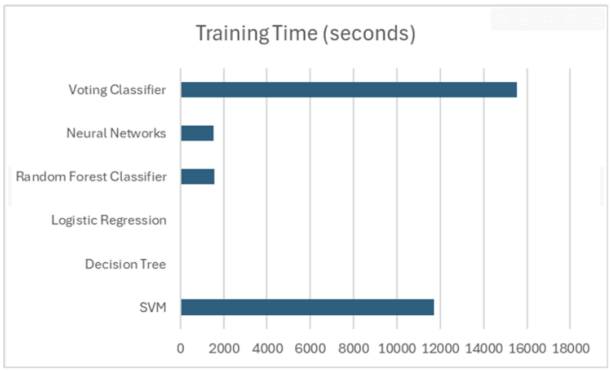

Figure 5. Time needed for models to train on the incomplete dataset.

selecting appropriate machine learning models based on data availability and specific application scenarios. The Random Forest and Decision Tree models perform exceptionally well with a complete dataset, while SVM excels in scenarios with limited data. This suggests that different models may be preferred depending on the operational context and data constraints in digital substations.

V. Discussion

The goal of this study is to evaluate the effectiveness of machine learning models in detecting DoS attacks in digital substations using IEC 61850 protocols. The Random Forest and Decision Tree classifiers showed superior detection capabilities with accuracies of 84.12% and 83.52%, respectively, while SVM excelled with limited data, achieving nearly perfect accuracy in some scenarios. Tree-based models like the Random Forest and Decision Tree are effective in detecting DoS attacks with comprehensive datasets, while SVM shows high accuracy and efficiency with limited data. These findings support the use of tailored intrusion detection systems in digital substations to enhance power grid resilience against cyber threats.

These findings also have several important implications for cybersecurity in smart grid systems. The robust performance of tree-based methods suggests that these should be primary choices for developing intrusion detection systems within smart grid environments. Their ability to perform well consistently across different scenarios also highlights their potential for deployment in diverse operational contexts. The variability observed in ensemble methods like the Voting Classifier points to the potential benefits and challenges of such approaches. While they can offer improved accuracy by combining different models, their effectiveness is highly dependent on the correct alignment and tuning of individual models. Additionally, the significant role of feature engineering, as demonstrated by the inclusion of the TimeDiff feature, cannot be understated. It highlights the need for domain-specific knowledge in enhancing model performance, which is crucial for detecting sophisticated cyber threats.

The computational complexity of the proposed methods was evaluated in terms of both time and space. The Decision Tree and Random Forest models demonstrated relatively efficient training times, with the Decision Tree being the fastest due to its greedy algorithmic approach. Memory consumption, measured during the training phase, showed that ensemble methods like Random Forest and Voting Classifier consumed significantly more memory compared to simpler models like Logistic Regression. However, these methods also provided superior performance in terms of accuracy. The space complexity scales with the depth of trees in tree-based models, where deeper trees require more memory but yield better results. These findings suggest that while the models are computationally more demanding, their enhanced detection capabilities justify the overhead in real-world applications.

Our study's findings align with existing literature that underscores the effectiveness of tree-based methods in network intrusion detection. Studies in [23] and [24] support our observations, noting the superiority of these methods in various cybersecurity applications. However, our research contributes unique insights by focusing specifically on the IEC 61850 protocols and providing a detailed analysis of performance under simulated attack scenarios that mimic real-world conditions. This protocol-specific focus and the comprehensive evaluation of model performance under different traffic conditions offer new contributions to the field of smart grid cybersecurity.

Moreover, our findings align with [5], which analyzed vulnerabilities in power systems. Our study complements the work by providing empirical evidence of the efficacy of machine learning models in mitigating these vulnerabilities, particularly against DoS attacks. Unlike the traditional methods discussed in [6], which focus on cybersecurity challenges at a theoretical level, our approach uses machine learning for practical intrusion detection. This advancement highlights the importance of integrating advanced analytics into cybersecurity frameworks, a theme also echoed by authors in [7], in their exploration of network anomaly detection.

Despite these contributions, our study is not without limitations. The inability to generate combined GOOSE and SV traffic for the most intense attack scenarios due to simulator constraints may have affected the comprehensiveness of our evaluation. Additionally, the potential exists for further enhancing model performance through more extensive feature engineering and the exploration of additional machine learning models, including deep learning architectures which were not included in this study. Lastly, the necessity for real-world validation remains, as our experiments were conducted in a simulated environment, which, while controlled and informative, may not fully capture the complexities of operational smart grid systems.

This study enhances cybersecurity by demonstrating how machine learning models can improve intrusion detection systems in digital substations. It provides a framework for selecting suitable algorithms based on data and context, advancing the understanding of machine learning in cybersecurity and offering practical solutions for protecting critical infrastructure. The demonstrated effectiveness of the Random Forest Classifier and Decision Tree offers a promising avenue for future research and practical implementations aimed at strengthening the cybersecurity postures of smart grid systems.

VI. Conclusion

This study focused on evaluating the performance of various machine learning algorithms in detecting DoS attacks within IEC 61850 protocols, specifically GOOSE and SV messages. The Random Forest Classifier and Decision Tree models were identified as the most effective models due to their high accuracy and reliability in detecting DoS attacks in IEC 61850 protocols, accompanied by reasonable training times. However, the SVM model outperforms others in this comparison due to its robust performance, even when trained with half of the data. The Voting Classifier also holds potential but may require further enhancements to achieve the consistency of the

SVM model. These findings underscore the potential of tree-based methods for real-time anomaly detection in smart grid communications, providing a reliable approach to enhancing cybersecurity measures in substation automation systems.

Future research should focus on overcoming simulator constraints to evaluate models under more extensive attack scenarios, exploring a broader set of machine learning algorithms, and conducting real-world validations. Expanding the feature set and refining model parameters could further enhance detection capabilities. The insights gained from this study offer valuable directions for advancing the security frameworks of smart grid systems, ensuring their resilience against sophisticated cyber threats.

REFERENCES

[1] T. Xu *et al.*, "Analysis on iec 61850 interoperability support", in *2007 IEEE Power Engineering Society General Meeting*, 2007, pp. 1–6. DOI: 10.1109/PES.2007.386057.

[2] G. Elbez, H. Keller, A. Bohara, K. Nahrstedt, and V. Hagenmeyer, "Detection of dos attacks using arfima modeling of goose communication in iec 61850 substations", *Energies*, vol. 13, no. 19, p. 5176, 2020. DOI: 10.3390/en13195176.

[3] L. O. Nweke, "A survey of specification-based intrusion detection techniques for cyber-physical systems", *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, 2021, ISSN: 2158-107X. DOI: 10.14569/ijacsa.2021.0120506.

[4] D. Abraham, S. Y. Yayilgan, F. Holík, S. Acevedo, and A. Gebremedhin, "Cyber attack simulation and detection in digital substation", in *2023 IEEE International Conference on Smart Cities, Cybernetics, and Computational Intelligence (ICSCCC)*, 2023, pp. 762–768. DOI: 10.1109/ICSCCC58608.2023.10176955.

[5] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis", in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 247–254. DOI: 10.1109/ISGT-Europe47291.2020.9248840.

[6] I. Kolosok and E. Korkina, "Problems of cyber security of digital substations", in *Proceedings of the 3rd International Workshop on Computer Intelligence (IWCI-19)*, 2019, pp. 75–78. DOI: 10.2991/iwci-19.2019.13.

[7] H. Yoo and T. Shon, "Novel approach for detecting network anomalies for substation automation based on iec 61850", *Multimedia Tools and Applications*, vol. 74, pp. 303–318, 2014. DOI: 10.1007/s11042-014-1870-0.

[8] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges", *Computer Networks*, vol. 57, pp. 1344–1371, 2013. DOI: 10.1016/j.comnet.2012.12.017.

[9] S. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations", *Computer Networks*, vol. 184, p. 107 679, 2021. DOI: 10.1016/j.comnet.2020.107679.

[10] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid", in *2010 IEEE Military Communications Conference*, 2010, pp. 1830–1835. DOI: 10.1109/MILCOM.2010.5679551.

[11] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. Muyeen, "Denial-of-service attack on iec 61850-based substation automation system: A crucial cyber threat towards smart substation pathways", *Sensors*, vol. 21, no. 19, p. 6415, 2021. DOI: 10.3390/s21196415.

[12] M. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. Michael, "Light-weight and robust network intrusion detection for cyber-attacks in digital substations", in *2021 IEEE Innovative Smart Grid Technologies Asia (ISGT Asia)*, 2022, pp. 1–5. DOI: 10.1109/ISGTAsia49270.2021.9715626.

[13] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for iec 61850 automated substations", *IEEE Transactions on Power Delivery*, vol. 25, pp. 2376–2383, 2010. DOI: 10.1109/TPWRD.2010.2050076.

[14] J. Zhang, Y. Chen, N. Jin, L. Hou, and Q. Zhang, "Opnet based simulation modeling and analysis of dos attack for digital substation", in *2017 IEEE Power & Energy Society General Meeting*, 2017, pp. 1–5. DOI: 10.1109/PESGM.2017.8274254.

[15] I. Kharchouf, M. Abdelrahman, A. Alrashide, and O. Mohammed, "Assessment of protection schemes and their security under denial of service attacks", in *2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, 2022, pp. 1–6. DOI: 10.1109/EEEIC/ICPSEurope54979.2022.9854745.

[16] F. Holík, S. Y. Yayilgan, and G. Olsborg, "Emulation of digital substations communication for cyber security awareness", *Electronics*, vol. 13, no. 12, p. 2318, 2024. DOI: 10.3390/electronics13122318.

[17] O. Hegazi, E. Hammad, A. Farraj, and D. Kundur, "Iec 61850 goose traffic modeling and generation", in *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2017, pp. 1100–1104. DOI: 10.1109/GlobalSIP.2017.8309131.

[18] Wireshark, *About wireshark*, https://www.wireshark.org/, retrived: October, 2024.

[19] Tshark, *Tshark manual page*, https://www.wireshark.org/docs/man-pages/tshark.html, retrived: October, 2024.

[20] Typhoon Hill, *Iec 61850 sampled values protocol*, https://www.typhoon-hil.com, retrived: October, 2024.

[21] I. El Naqa and M. Murphy, "What is machine learning?", in *Machine Learning in Radiation Oncology*, 2015, pp. 3–11. DOI: 10.1007/978-3-319-18305-3_1.

[22] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in python", *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[23] M. A. Bouke, A. Abdullah, S. H. ALshatebi, M. T. Abdullah, and H. E. Atigh, "An intelligent ddos attack detection tree-based model using gini index feature selection method", *Microprocessors and Microsystems*, vol. 98, p. 104 823, Apr. 2023, ISSN: 0141-9331. DOI: 10.1016/j.micpro.2023.104823.

[24] A. Coscia, V. Dentamaro, S. Galantucci, A. Maci, and G. Pirlo, "Automatic decision tree-based nidps ruleset generation for dos/ddos attacks", *Journal of Information Security and Applications*, vol. 82, p. 103 736, May 2024, ISSN: 2214-2126. DOI: 10.1016/j.jisa.2024.103736.

[25] D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, "Cybersecurity in smart grids, challenges and solutions", *AIMS Electronics and Electrical Engineering*, vol. 5, no. 1, pp. 24–37, 2021. DOI: 10.3934/electreng.2021002.

[26] T. A. Youssef, M. El Hariri, N. Bugay, and O. A. Mohammed, "Iec 61850: Technology standards and cyber-threats", in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Florence, Italy, 2016, pp. 1–6.

[27] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid", in *2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015, pp. 1–5.