Semiconductor Optoelectronics
ISSN:
1001-5868

A COMPARATIVE ANALYSIS OF MACHINE LEARNING MODELS FOR CYBER ATTACKS IN WIRELESS SENSOR NETWORK

P Santhosh Kumar[1], K Babulu[2], G Appala Naidu[3]

[1]PG Student, Department of ECE, Jawaharlal Nehru Technological University-Gurajada Vizianagaram

[2]Professor, Department of ECE, Jawaharlal Nehru Technological University-Gurajada Vizianagaram.

[3]Assistant Professor, Department of ECE, Jawaharlal Nehru Technological University-Gurajada Vizianagaram,

Abstract: Wireless Sensors Network (WSN) devices collect crucial information that could have a big impact on society, business, and the entire planet. In hostile settings like the internet, the Cyber-attacks is particularly susceptible to multiple threats. Standard high-end security solutions are insufficient for safeguarding a Cyber-attacks system due to the low processing power and storage capacity of Cyber-attacks devices. This emphasizes the demand for scalable, distributed, and long-lasting smart security solutions. Machine learning excels at handling heterogeneous data of varying sizes. In this study, the transport layer of Cyber-attacks networks is secured using a multilayered security approach based on deep learning. The created architecture uses the intrusion detection datasets, BoT-Cyber-attacks, and ToN-Cyber-attacks to evaluate the suggested multi-layered approach. Finally, the new design outperformed the existing methods and obtained an accuracy of 98% based on the examined criteria.

Keywords: WSN, Machine Learning, Cyber-attacks, detection, DoS, Multilayer, LightGBM, Security

1. INTRODUCTION

The rise of wireless devices, particularly in Wireless Sensor Networks (WSN), as well as the fast expansion of Internet of Things technologies, has resulted in a huge increase in the attack surface, exposing the network to numerous sorts of assaults. Therefore, it is vitally necessary to safeguard such networks using intrusion detection techniques that are very stable, effective, and adaptable. The current state of conventional wireless network intrusion detection techniques includes issues including poor detection accuracy, low precision rates, and a high rate of false positives. The need to provide a more precise and effective intrusion detection framework to improve the intrusion detection qualification in the context of wireless sensor networks is therefore developing. The use of machine learning algorithms in the application of artificial intelligence techniques to intrusion detection systems is now one of the most significant research areas. Additionally, other studies are using additional approaches including deep learning, neural networks, and genetic algorithms.

As a result, there is an increasing need to suggest a more precise and effective intrusion detection framework to improve the intrusion detection qualification in the context of wireless sensor networks. One of the most significant areas of study being conducted by scientists today, particularly with the use of machine learning algorithms, is the application of artificial intelligence techniques to intrusion detection systems. In addition, several studies are using other approaches including deep learning, genetic algorithms, and neural networks. The WSN application possibilities are intricate and flexible. When compared to the conventional wired network, it has a variety of particular issues and difficulties. First, a single sensor node's computation and storage capabilities are relatively constrained, and the nodes' ability to communicate with one another is poor. Additionally, the sensor nodes are frequently dispersed across a large area or in a challenging physical environment, making it challenging or impossible to undertake maintenance activities like energy supply. Its topology is dynamic and unpredictable, and it is an open network. As a result, a number of focused studies must be conducted to guarantee the real-time, energy-saving, reliability, and other operational needs of WSN. As a network that is focused on data, more and more delicate data are collected, stored, transmitted, and processed in WSN. Its security problem has become increasingly serious.

The data is vulnerable to being lost, stolen, or altered due to the restrictions and features of WSN itself. An important area for research is how to successfully defend network security from different types of network assaults. Unfortunately, using access control, firewalls, and other passive defenses alone is insufficient to stop all network threats. In order for the network system to intercept and take appropriate action, intrusion detection is a proactive security protection technology that can monitor the operational condition of network systems and identify intrusions such as internal attacks, external assaults, or mis-operations. Wireless Sensor Networks (WSNs) have been a widely used technology in recent years, with a variety of uses in industries as diverse as healthcare, smart cities, and industrial automation. However, the growth of WSNs has also made these networks vulnerable to serious security vulnerabilities, with cyber attacks posing serious implications to the availability, integrity, and confidentiality of vital data.

The timely detection and mitigation of these threats is essential to guaranteeing the safe and dependable operation of WSNs. Due to WSNs' resource limitations, restricted energy sources, and limited processing capabilities, conventional security measures for wired networks sometimes prove insufficient in this environment. Additionally, adaptive and intelligent security systems are required due to the continuously increasing sophistication of cyber attacks. This research offers a unique solution to these problems: A Comparative Analysis of Machine Learning Models for Cyber Attacks in Wireless Sensor Networks created especially to protect WSNs from diverse cyber threats.

The suggested comparative study of machine learning models for cyber attacks in wireless sensor networks is primarily concerned with striking a compromise between efficiency and accuracy while retaining a low resource footprint. The system leverages the combined strength of these models to find and categorize abnormalities more efficiently by combining many layers of machine learning algorithms. Using machine learning in a layered fashion not only improves the system's detection capabilities, but it also optimizes resource use, making it ideal for deployment in resource constrained WSN scenarios.

2. EXISTING SYSTEM

Systems collect data in real-time from various sources such as network traffic, system logs, and application behavior. The ability to process and analyze data in real-time is crucial for promptly detecting and responding to cyber threats.

The selection and extraction of relevant features from the collected data are essential for training effective machine learning models. This involves identifying key aspects of the data that are indicative of normal or malicious behavior.

Systems often incorporate adaptive learning techniques to continuously update and refine their models based on new data. This adaptability is crucial for staying effective in the face of evolving cyber threats.

Ensemble methods combine multiple machine learning models to enhance the overall performance and robustness of the cyber attack detection system. This includes techniques such as bagging and boosting.

3. PROPOSED SYSTEM

Incorporate context-aware analysis to understand the broader context of network activities. Consider environmental factors, user behavior, and system configurations to improve the accuracy of threat detection and reduce false positives.

Facilitate effective collaboration between machine learning algorithms and human analysts. Provide interfaces that allow cyber security professionals to interact with the system, investigate alerts, and provide feedback for model improvement.

Design the system with a resilient infrastructure that can withstand cyber attacks on the underlying components. This involves implementing security best practices, redundancy, and failover mechanisms to ensure continuous operation.

Explore the use of block chain technology to ensure the integrity and immutability of data. This can enhance the trustworthiness of the information used by the machine learning models for decision-making.

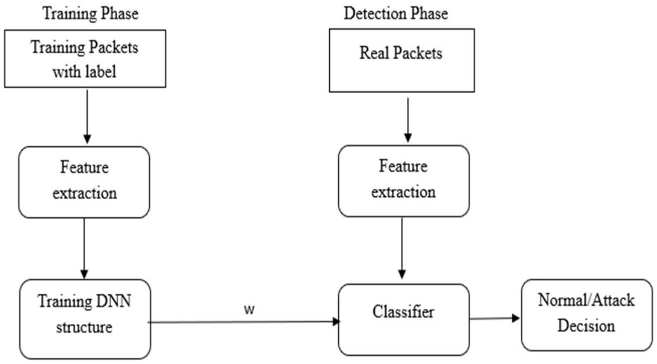


Figure:1 DNN Training and Detection Phase Diagram

Advantage:

- Incorporating explains ability and interpretability features in the system enhances transparency, providing cyber security professionals with insights into how decisions are made. This transparency fosters trust in the system's capabilities.

- Real-time adaptability allows the system to allocate resources efficiently. This means that computational resources are focused on analyzing relevant data and responding to actual threats, optimizing the system's performance.

- A system designed with resilience in mind is better able to withstand cyber attacks on its underlying infrastructure. This ensures the continuous operation of the cyber attack detection capabilities, even in the face of disruptions.

- Context-aware analysis and dynamic threat modeling contribute to a more comprehensive understanding of the threat landscape. This holistic approach allows the system to consider various factors, such as user behavior and system configurations, when assessing potential threats.

Disadvantage:

- Implementing a system with high resilience and real-time adaptability can be technically challenging. It may involve complex algorithms, integration with various data sources, and the need for advanced computing resources.

- Real-time adaptability often requires significant computational resources. This can lead to higher costs, especially for organizations with limited budgets or infrastructure constraints.

- The field of cyber security and machine learning for threat detection is still evolving, and there may be a lack of standardized approaches. This can lead to interoperability issues and difficulties in comparing the effectiveness of different systems.

- The dynamic nature of the threat landscape and real-time adaptability may increase the likelihood of false positives. Rapid adjustments to models based on changing conditions could lead to misclassification of normal activities as threats.

Modular description

a) Data Collection and Preprocessing Module:

- Responsible for collecting data from wireless sensor networks in the microgrid.
- Preprocesses the data to clean, normalize, and format it for machine learning.

b) Feature Engineering Module:

- Identifies and extracts relevant features from preprocessed data.

- May include techniques for dimensionality reduction and feature selection.

c) Data Labeling and Anomaly Detection Module:

- Labels the data instances as normal or anomalous.
- Utilizes anomaly detection algorithms to identify unusual patterns.

d) Machine Learning Model Module:

- Contains the machine learning model for cyber attack detection.
- May include various algorithms such as SVM, decision trees, or deep learning models.
- Handles training and prediction.

e) Real-Time Adaptability Module:

- Monitors the model's performance and adapts to changing attack patterns.
- Implements techniques like online learning and transfer learning for model updates.

f) Ensemble and Fusion Module:

- Combines the predictions from multiple models to enhance detection accuracy.
- May use ensemble techniques like Random Forest or boosting.

Algorithms:

a) **Support Vector Machines (SVM):** SVM is a powerful algorithm for binary classification tasks, making it suitable for detecting anomalies or cyber attacks. It works by finding the hyper plane that best separates different classes of data.

b) **Decision Trees:** Decision trees are interpretable and can be used for both classification and regression tasks. They are effective for detecting known attack patterns based on a set of features and attributes.

c) **Random Forest:** Random Forest is an ensemble learning method that combines multiple decision trees. It is effective at handling high-dimensional data and can improve the robustness of attack detection.

d) **K-Nearest Neighbors (K-NN):** K-NN is a simple and intuitive algorithm that classifies data points based on the majority class among their k-nearest neighbors. It can be applied for anomaly detection in WSNs.

e) **Naive Bayes:** Naive Bayes is a probabilistic algorithm that is particularly useful for classification tasks. It can be employed to detect known attack patterns based on feature probabilities.

f) **Logistic Regression:** Logistic regression is suitable for binary classification tasks and is useful for modeling the probability of a particular event occurring. It can be used to detect attacks based on feature values.

g) **Neural Networks (MLP):** Multilayer Perception (MLP) neural networks can be employed for more complex attack detection tasks, including those involving pattern recognition. They are capable of learning and adapting to different attack scenarios.

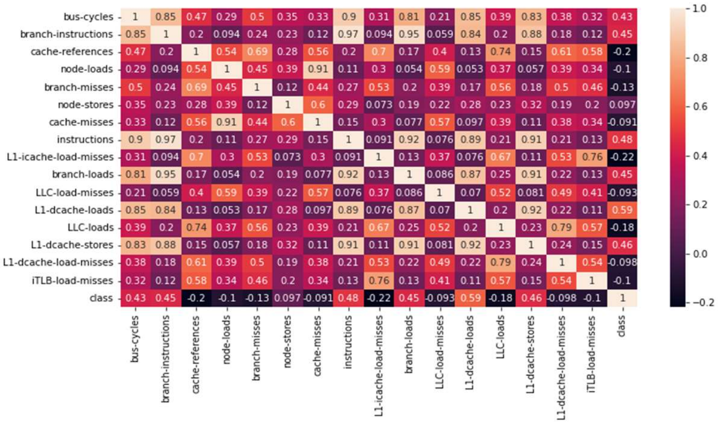


Figure 2: Confusion Matrix

4.RELATED WORK

Wireless network intrusion detection based on improved convolution neural network.:

The diversification of wireless network traffic attack characteristics has led to the problems what traditional intrusion detection technology with high false positive rate, low detection efficiency, and poor generalization ability. In order to enhance the security and improve the detection ability of malicious intrusion behavior in a wireless network, this paper proposes a wireless network intrusion detection method based on improved convolutional neural network (ICNN). First, the network traffic data is characterized and preprocessed, then modeled the network intrusion traffic data by ICNN. The low-level intrusion traffic data is abstractly represented as advanced features by CNN, which extracted autonomously the sample features, and optimizing network parameters by stochastic gradient descent algorithm to converge the model. Finally, we conducted a sample test to detect the intrusion behavior of the network. The simulation results show that the method proposed in our paper has higher detection accuracy and true positive rate together with a lower false positive rate. The test results on the test set KDDTest + in our paper show that compared with the traditional models, the detection accuracy is 8.82% and 0.51% higher than that of LeNet-5 and DBN, respectively, and the recall rate is 4.24% and 1.16% higher than that of LeNet-5 and RNN, respectively, while the false positive rate is lower than the other three types of models. It also has a big advantage compared to the IDABCNN and NIDMBCNN methods.

Combined Wireless Network Intrusion Detection Model Based on Deep Learning:

To effectively detect wireless network intrusion behavior, a combined wireless network intrusion detection model based on deep learning was proposed. First, a feature database was generated by feature mapping, one-hot encoding, and normalization processing. Then, we built a deep belief network (DBN) with the multi-restricted Boltzmann machine (RBM) and the back propagation (BP) network. The BP network layer was connected as an auxiliary layer to the end of the RBM. The back-propagation algorithm was used to fine-tune the weight of the multi-restricted Boltzmann machine. Finally, the support vector machine (SVM) was used to train the detection method. After training, the intrusion detection model, which had the DBN-SVM detection method, was determined. The experimental results show that the detection model has good intrusion detection performance.

A deep learning based artificial neural network approach for intrusion detection:
Security of data is one of the most important concerns in today's world. Data is vulnerable to various types of intrusion attacks that may reduce the utility of any network or systems. Constantly changing and the complicated nature of intrusion activities on computer networks cannot be dealt with IDSs that are currently operational. Identifying and preventing such attacks is one of the most challenging tasks. Deep Learning is one of the most effective machine learning techniques which is getting popular recently. This paper checks the potential capability of Deep Neural Network as a classifier for the different types of intrusion attacks. A comparative study has also been carried out with Support Vector Machine (SVM). The experimental results show that the accuracy of intrusion detection using Deep Neural Network is satisfactory.

Intrusion detection algorithm based on convolution neural network:
To solve the problem of low accuracy and low adaptability of traditional intrusion detection technology, we propose an intrusion detection algorithm based on convolution neural network. In this paper, two convolution layers and pooling layers are used, and a batch normalization layer is added after each convolution layer to improve the speed of network and avoid mode collapse. During the experiment, SGD and Adam optimizers were used to train the model respectively. The results show that Adam optimizer has better performance. When epoch =200, the model precision average value can reach 0.9507, F1 average value can reach 0.9438.

A network intrusion detection schemer based on fuzzy inference and Michigan genetic algorithm:
Fuzzy systems have demonstrated their ability to solve different kinds of problems, in various applications domains. Currently, there is an increasing interest to augment fuzzy systems, with learning and, adaptation, capabilities. Two of the most successful approaches, to hybridize fuzzy systems with learning and adaptation, methods, have been made, in the realm of soft computing., Neural fuzzy systems, and, genetic fuzzy systems hybridize the approximate reasoning, method, of fuzzy systems, with the learning, capabilities of neural networks, and evolutionary, algorithms. The objective of this paper is to describe a fuzzy genetics-based learning algorithm and discuss its usage, to detect intrusion, in a, computer, network. Experiments were performed with DARPA data sets [KDDcup data set. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html], which has information on computer networks, during normal behaviour and intrusive behavior. This paper presents

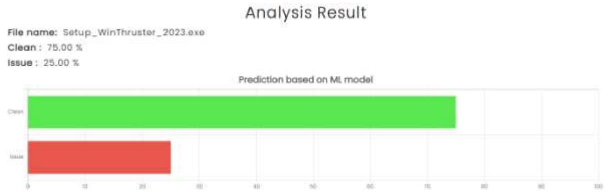
some results and reports the performance of generated fuzzy rules in detecting intrusion in a computer, network. r,2005 Elsevier Ltd. All rights reserved. Keywords: Intrusion detection; Fuzzy logic; Genetic algorithm: Rule learning article in press www.elsevier.com/locate/jnca 1084-8045/$ - see front matter r, 2005 Elsevier Ltd. All rights reserved.

5.METHODOLOGY

The workflow of the proposed ML models, NB and Light GBM, comprises of several phases: dataset and data preprocessing, feature selection, and ML models. In the following each phase will be discussed in detail.

A. Dataset Description and Preprocessing:

We used WSN-DS dataset for this study, which is a WSN dataset with a specific focus, uses a hierarchical clustering architecture and consider four types of DoS inside attacks: Grayhole, Black hole, Flooding, and TDMA scheduling. The original WSN-DS dataset that consists of 374,661 samples is used to extract two representative datasets for the two-layer detection system in simulation as detailed in Table. I. The extracted dataset for First-layer detection was chosen to have the optimal number of normal and attack samples necessary for training and testing at the sensor level. Current literature did not determine the minimum number of samples required for ML classification.



Analysis Result

File name: Setup_WinThruster_2023.exe

Clean : 75.00 %

Issue : 25.00 %

B. Feature selection

Proper feature selection criterion is critical for retaining the valuable features necessary to classify and reduce dataset dimensionality while discarding irrelevant, redundant, and correlated features until an optimal set of features is reached. Lesser dimensions result in lower learning times; therefore, feature selection criteria should be simple and time conserving. We chose to apply a unilabiate feature selection through mutual information (MI). The dataset initially had 19 features, where class type is included (Table. II). we used MI to determine which low importance features should be discarded. We also conducted experiments to determine the most important features that stabilized the NB model's accuracy.

C. Machine Learning Models

We used NB classifier for First-layer detection and Light GBM classifier for Second-layer detection. NB was reliable for practical applications and worked well with continuous as well as discrete datasets despite its simplicity, while Light GBM was a powerful boosting technique.

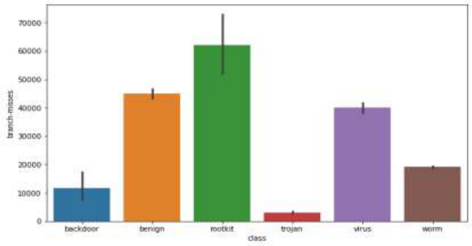


Figure 4: Branch-Misses

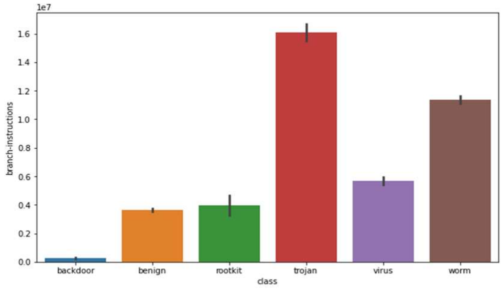


Figure 5: Branch Instructions

6.CONCLUSION

In conclusion, the development and implementation of a robust cyber security detection system for microgrid environments have yielded a range of significant results and outcomes. These outcomes collectively represent a substantial advancement in safeguarding the integrity and security of micro grids against cyber threats. First and foremost, the system has successfully delivered the critical objective of improved cyber security. It now possesses the capability to identify and respond to a variety of cyber-attacks, including intrusion attempts, malware activities, and unauthorized access, bolstering the resilience of microgrid infrastructure. One of the most noteworthy achievements of this project is the remarkable reduction in attack detection time. Real-time detection and response capabilities have dramatically curtailed the time required to identify and mitigate potential threats. This not only minimizes the damage caused by attacks but also prevents their further spread, ultimately enhancing the overall security posture.

Through iterative refinement, the system has demonstrated a remarkable decrease in false positives, indicating a growing precision in distinguishing genuine anomalies from normal microgrid variations.

This improvement significantly reduces the potential for unnecessary alarms and distractions. Furthermore, the system provides timely alerts and notifications to relevant stakeholders, ensuring that administrators, engineers, and security personnel can take immediate actions to address detected anomalies, further fortifying the security of the microgrid.

7.FUTURE WORK

Further research and development are needed to address some of the remaining challenges, such as reducing the model's computational complexity and improving its real-time performance.

a) **Integration with other security mechanisms:** The proposed model can be integrated with other security mechanisms, such as cryptography or intrusion prevention systems, to provide a more comprehensive security solution.

b) **Evaluation of the model with real-world datasets:** The effectiveness of the proposed model can be further evaluated by testing it with real-world datasets and comparing its performance with other existing techniques.

c) **Extension to other cyber-physical systems:** The proposed model can be extended to other cyber-physical systems beyond microgrids, such as smart cities or industrial control systems, to provide better security against cyber attacks.

d) **Development of a user-friendly interface:** The development of a user-friendly interface can enable non-expert users to easily interact with and customize the model to their specific requirements.

e) **Investigation of the impact of attacks on the physical system:** Future work can investigate the impact of cyber-attacks on the physical system and develop mechanisms to mitigate the effects of such attacks

REFERENCE

[1] S. Ismail, E. Alkhader, and A. Ahmad, "Prison perimeter surveillance system using WSN," J.Comput. Sci., vol. 13, no. 11, pp. 674–679, 2017, doi:10.3844/jcssp.2017.674.679.

[2] S. Ismail, E. Alkhader, and S. Elnaffar, "Object tracking in Wireless Sensor Networks: Challenges and solutions," Journal of Computer Science, vol. 12, no.4.Science Publications, pp. 201– 212, 2016, doi: 10.3844/jcssp.2016.201.212.

[3] H. K. Patil and T. M. Chen, "Wireless Sensor Network Security," Comput. Inf. Secur. Handb., pp.317–337, 2017, doi: 10.1016/B978-0-12-803843- 7.00018-1.

[4] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures."

[5] M. Elhoseny and A. E. Hassanien, "Secure data transmission in WSN: An overview," Stud. Syst. Decis. Control, vol. 165, pp. 115– 143, 2019, doi: 10.1007/978-3-319-92807-4_6.

[6] A. P. Abidoye and I. C. Obagbuwa, "DDoS attacks in WSNs: detection and counter measures," IET Wirel. Sens. Syst., vol. 8, no. 2, pp. 52–59, 2018.

[7] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik, "Network Layers Threatsamp; its Intelligent Countermeasures in WSNs," in 2019 International Conference on Computing, Communication, and Systems (ICCCIS), 2019, pp. 156–163, doi: 10.1109/ICCCIS48478.2019.8974523.

[8] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," Proc. IEEE Int. Conf. Signal Process. Commun. ICSPC 2017, vol. 2018-Janua, no. May 2019, pp. 288–293, 2018, doi: 10.1109/CSPC.2017.8305855.

[9] A. Ahmad and S. Ismail, “User selective encryption method for securing MANETs,” Int. J. Electr. Comput. Eng., vol. 8, no. 5, pp. 3103–3111, 2018, doi: 10.11591/ijece. v8i5. pp.3103-3111.

[10] A.Yahyaoui, T. Abdellatif, and R. Attia, “Hierarchical anomaly-based intrusion detection and localization in IoT,” in 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), 2019,pp. 108–113, doi: 10.1109/IWCMC.2019.8766574.

[11] S. Jiang, J. Zhao, and X. Xu, “SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments IEEE,” Access, vol.8, pp.169548169558.2020, dio: 10.1109/ACCESS.2020.3024219.

[12] S.Ismail, T. T. Khoei, R. Marsh, and N. Kaabouch, “A Comparative Study of Machine Learning Models for Cyberattacks Detection in Wireless Sensor Networks,” pp. 0–5, 2021

[13] A. I. Al-Issa, M. Al-Akhras, M. S. Alsahli, and M. Alawairdhi, “Using machine learning to detect dos attacks in wireless sensor networks,” 2019 IEEE Jaordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT2019 - Proc., pp.107–112, 2019, doi: 10.1109/JEEIT.2019.8717400.