Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Machine Learning-Based Detection And Prevention Of Malicious Node Behavior, Fraggle, And Advanced Smurf Attacks In Wireless Sensor Network

[1]Santhosh Kumar B.J, [2]Chethan Gowda B.S, [3]Punith B.S

[1] [2] [3] Department of Computer Science Amrita School of Computing
Mysuru Campus, Amrita Vishwa Vidyapeetham Mysuru, India

Abstract- This research focuses on enhancing the security of Wireless Sensor Networks (WSNs) against harmful actions by using a combination of simulations and advanced machine learning. A custom network environment is created in a simulator, containing 30 nodes with 3 malicious ones. This setup imitates real situations, letting us watch how the network behaves under different conditions. Data is collected and analyzed, capturing important factors like power use, delays, and how packets act. These factors are used to teach machine learning models like Support Vector Machines, Naive Bayes, Logistic Regression, and k-nearest Neighbours. These models can tell apart normal and malicious behaviors effectively. To stop harmful data from entering the network, a decision tree model checks incoming packets. If they're labeled as malicious, they're blocked. This system works continuously, adapting to new dangers. The research offers a full security approach, protecting WSNs from various attacks. By mixing simulations, analysis, and machine learning, it highlights the power of using different fields to make networks stronger. The results guide us toward secure and adaptable WSNs that can handle security challenges in changing situations.

Keywords: Wireless Sensor Networks, security, malicious node behavior, simulation-based data collection, machine learning, network dynamics, Wireshark analysis, feature extraction, Support Vector Machines, Naive Bayes, Logistic Regression, k-Nearest Neighbours, prevention mechanism, decision tree model, network resilience.

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a critical technology for a wide spectrum of applications, ranging from environmental monitoring to industrial automation and healthcare systems. However, the decentralized and resource-constrained nature of WSNs makes them vulnerable to various security threats, particularly from malicious nodes that can disrupt network operations, compromise data integrity, and compromise the overall functionality. Addressing these security concerns has become a paramount objective in ensuring the reliable and secure operation of WSNs. This research delves into the multifaceted challenge of detecting and preventing malicious node behavior in WSNs. The study takes a comprehensive approach that leverages both simulated node behavior and advanced intrusion detection techniques. With a focus on countering attacks like Smurf and Fraggle, notorious for their capacity to flood networks and disrupt operations, the research combines practical experimentation with sophisticated machine-learning strategies. In the first scenario, a custom environment is created within the Cooja simulator, incorporating a network of 30 nodes. By introducing intentionally malicious nodes into the network, the research captures a diverse range of parameters, including power consumption, delays, buffer overflow occurrences, and more. This dataset serves as the cornerstone for developing and deploying intrusion detection and prevention mechanisms. The second scenario adopts a machine learning-driven approach, utilizing the well-established KDD dataset. Through the lens of Support Vector Machines (SVM), Naive Bayes, Logistic Regression, and k-nearest Neighbors (KNN) algorithms, the research showcases the potential of machine learning to discern between normal and malicious behaviors.

This research aims not only to enhance the security of WSNs against specific attack vectors but also to contribute to the broader discourse on fortifying the foundations of wireless communication. By blending simulation-based data collection with advanced analysis techniques, this study envisions a holistic security

framework that not only shields WSNs from existing threats but also primes them for the dynamic challenges of the future digital landscape.

2. Related Work

Dr. Varanasi Usha Bala [1] in this paper By adding more machine learning algorithms to the ones that have previously been used, the system described in this paper can be made more dependable and effective, making it simpler to detect intrusions. The various attack types can additionally be divided into intrusion classes to recognize more attacks and provide increased protection and dependability. Even if a specific attack is missed by one algorithm, it will still be detected by any other algorithm, increasing the detection rate of the intrusion. With the help of Snort and predetermined rule sets, the vulnerability assessment is completed, and for each detected incursion, a response is taken. The comparison study has made it clear which strategy is best at identifying assaults. We need to be able to distinguish real attacks from false alarms to build effective IDS that can lower the false alarm rate and offer reliability and security. Further system improvement may therefore help to increase detection rates while reducing false positive rates.

ADITI PAUL, Somnath Sinha [2] Proposed that A hybrid intrusion detection system (IDS) be created and put into use in the proposed study to identify cross-layer denial of service (DoS) assaults in IoT contexts. Through simulation and the Stacking Classification strategy, the model is tested using machine learning techniques. The outcomes demonstrate that the hybrid IDS attains good accuracy throughout both the detection and classification phases. In stages 1 and 2, the model correctly classifies the attacks with up to 96% accuracy and detects attack occurrences with up to 95% accuracy. Excellent detection abilities are shown by the weighted F1 score, which ranges from 94% to 96% and assesses overall performance. Furthermore, compared to other approaches like KNN, the suggested model is lightweight and effective, delivering results in 18–19 seconds.

A. H. Farea and K. Küçük [3] Using machine learning (ML)-based techniques, this work presents a strategy for identifying threats in Internet of Things (IoT) environments. The paper looks into three distinct assaults in the IoT ecosystem, including DoS, BHA, and OOA. The Cooja simulator is used in the study to create a fresh dataset of IoT properties. The decision tree-based models used by the ML-based techniques are well known for their effectiveness in manipulating, analyzing, and categorizing harmful behavior in IoT characteristics. For the KoÜ-6LoWPAN-IoT dataset, the multiclass Random Decision Forest ML-based model achieves an overall accuracy of 98. % in identifying IoT assaults. Other models, such as enhanced decision tree regression, decision forest tree regression, and decision tree jungle, however, have lower accuracy rates of 87. %, 93.0%, and 87.0%, respectively.

Lakshmi HN [4] The construction of flooding assaults and their negative consequences on the network are covered in the study. To properly evaluate the attack's real-world impact, the attack is studied using the NS2 simulation tool. The end-to-end latency and throughput effects of the assault are represented graphically, which sheds light on the direct effects of flooding attacks. The identification of RREQ flooding assaults in WSNs is aided by the study of these graphical representations. The suggested preventative approach presents a potential mitigation strategy for flooding assaults, which may be further assessed and contrasted with current methods.

Nagarjuna S [5] The study emphasizes how crucial it is to take into account several variables at once to prove the existence of an assault. An assault may have occurred if these characteristics changed, either by rising or reducing. This paper offers insights into more precisely identifying network assaults by looking at the differences in throughput, packet loss, and residual energy. The efficacy of attack detection in wireless sensor networks is increased by the combined study of these data. The assessment also discusses the security issues related to identifying attacks and malicious nodes. It is suggested that integrating encryption methods in the future might improve network security.

B. J. Kumar and Sinha [6] The paper highlights the challenges and limitations of existing techniques and proposes the exploration of alternative methods due to the inefficiency of encryption-based approaches. The study suggests a new direction for detecting and preventing severe DoS attacks, offering potential improvements in securing Internet-integrated WSNs. Future research in this area can focus on developing more robust and efficient intrusion detection and prevention systems to enhance the security of Internet-integrated WSNs against DoS attacks.

M. Osman, and S. Qureshi [7] The authors emphasize that ML-LGBM is a better option than the other methodologies and techniques covered in the article for detecting attacks in RPL-based networks. However, they agree that the dataset has a drawback because it only includes one kind of RPL attack. Since the model makes use of a substantial and distinctive dataset to exhibit high performance, future research should concentrate on expanding the dataset to include additional attack types to better assess the model's performance.

Chandan, and S. Sinha [8] This study emphasizes how crucial it is to recognize and stop these assaults. An efficient method for recognizing and categorizing malicious nodes is the use of machine learning techniques and fuzzy logic systems. The suggested hybrid technique performs better than traditional systems and exhibits excellent classification accuracy. The AVV-DDos2286 dataset's availability advances research in DDoS attack detection in another way.

B.J. Kumar and K.R. Karthik [9] This study offers important insights into the difficulties and potential solutions for preventing such attacks by performing a literature review on the detection of syn flooding assaults in wireless sensor networks. The study's power-based detection technique shows promise for increasing WSN security against syn flooding attacks. The focus of future studies in this field might be on improving the detection method and looking into additional defenses against different kinds of DoS assaults.

System Architecture

The system architecture presented in this research embodies a holistic approach to enhance the security of Wireless Sensor Networks (WSNs) against malicious node behavior. It seamlessly integrates simulation-based data collection and advanced machine learning techniques, creating a comprehensive defense mechanism against potential threats. The architecture commences with the creation of a simulated WSN environment using the Cooja simulator. This environment hosts a network structure composed of 30 nodes, including 3 intentionally introduced malicious nodes. This controlled setting emulates real-world scenarios, enabling the observation of network dynamics and interactions under various conditions. During data collection and simulation, nodes communicate through radio messages, generating a dataset rich in critical parameters. These parameters encompass power consumption, delays, buffer overflow occurrences, and packet behaviors. This dataset captures a comprehensive view of the network's performance and behavior, forming the basis for subsequent analysis. Wireshark captures and analyses dissect the transmitted data, unveiling patterns and characteristics of network interactions. Relevant features are extracted from this analysis, differentiating between benign and malicious activities. These features are pivotal for training machine learning models.

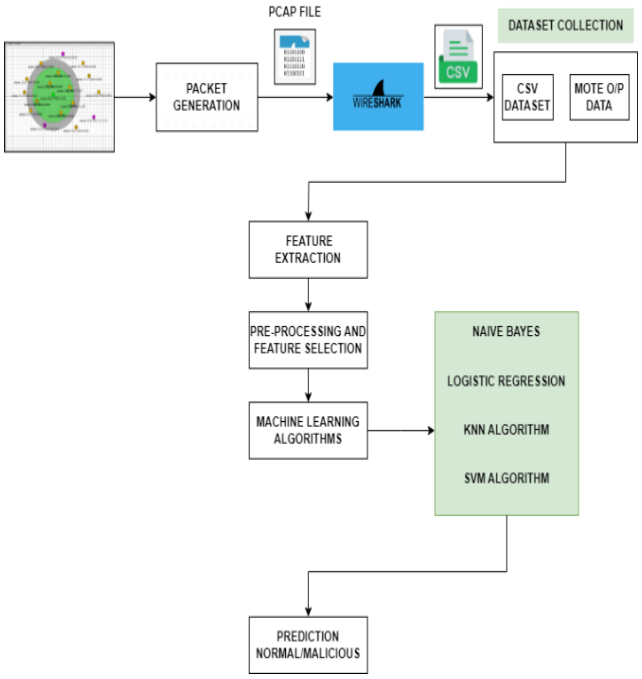

Fig 1: Architectural Diagram

The selected machine learning algorithms—Support Vector Machines (SVM), Naive Bayes, Logistic Regression, and k-nearest Neighbours (KNN)—then undergo training. Leveraging the dataset, these algorithms learn to discern patterns indicative of malicious behavior. During real-time operation, the decision tree model processes received packets' features, classifying them as normal or malicious. The prevention mechanism, informed by the decision tree model's classification, curtails the infiltration of potentially harmful packets into the network. Continuous monitoring, feedback loops, and updates ensure the architecture's adaptability to emerging threats. In its entirety, this system architecture harmonizes simulation, analysis, and machine learning to establish a robust intrusion detection and prevention mechanism. It fortifies WSNs against a spectrum of malicious node behaviors, championing network security and fostering reliable communication in dynamic environments.

3. Proposed Method

A. Overall Workflow

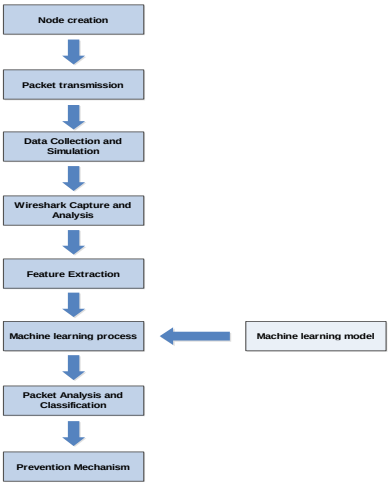

Fig 2: workflow Diagram

The workflow architecture presented in this research integrates simulation-based data collection and advanced machine-learning techniques to fortify the security of Wireless Sensor Networks (WSNs). Beginning with the Cooja simulator, a custom environment is crafted, simulating a network of 30 nodes, including intentionally malicious ones. Through radio message generation, critical parameters like power consumption, delays, and packet behavior are collected. Wireshark analysis unveils patterns in node interactions, while feature extraction identifies distinguishing attributes. Machine learning models, including decision trees, are then trained using this data to differentiate between benign and malicious behavior. During runtime, incoming packets undergo the same feature extraction process and are analyzed by the trained model. If flagged as anomalies, these packets are prevented from infiltrating the network. This architecture creates a closed-loop system that continuously adapts and evolves, enhancing WSN security against malicious node behavior and setting the stage for resilient wireless communication in dynamic environments.

B. Node Creation

In the framework of enhancing Wireless Sensor Network (WSN) security, a carefully constructed network environment is established. Comprising 30 nodes, this network serves as a controlled platform to explore network behavior and responses. Importantly, this configuration intentionally integrates three nodes programmed to simulate malicious actions, mirroring potential real-world threats. The deliberate inclusion of these malicious nodes allows for the observation of their impact on network dynamics, resource utilization, and communication patterns. This controlled environment provides valuable insights into identifying anomalies and

patterns associated with malicious behavior, forming the basis for developing and fine-tuning intrusion detection and prevention mechanisms.

C. Packet Transmission

Packet transmission within the context of this research occurs within a meticulously designed Wireless Sensor Network (WSN) environment. With 30 nodes, including 3 malicious nodes, packet transmission embodies the heart of network communication. The network emulates real-world scenarios, facilitating the observation of how packets traverse between nodes, considering factors like delays, energy consumption, and buffer overflows. The intentional inclusion of malicious nodes allows for the study of packet transmission under diverse conditions, including potential attacks like Smurf and Fraggle. As packets journey through the network, they undergo Wireshark analysis, enabling the extraction of crucial features for further analysis and classification by machine learning models.

D. Data Collection and Simulation

The process of data collection and simulation is a cornerstone of this research, aimed at comprehensively understanding and fortifying the security of Wireless Sensor Networks (WSNs). Within a meticulously constructed environment, a network comprising 30 nodes is established, intentionally incorporating three nodes programmed to simulate malicious behavior. This controlled yet realistic setting enables the emulation of real-world scenarios where network security is at risk. Through radio message generation and communication patterns among nodes, a diverse array of critical parameters is collected. These parameters encompass essential aspects such as power consumption, communication delays, instances of buffer overflow, and patterns of packet behavior. This simulated dataset serves as a dynamic repository of network activities and behaviors, capturing both regular and malicious node interactions. This collected data forms the bedrock for subsequent analysis and model development. The carefully designed network architecture allows for the exploration of packet transmission, delays, and energy utilization, offering insights into network performance under various conditions.

KDD dataset: The KDD dataset plays a crucial role in this research as it serves as a benchmark for evaluating the effectiveness of machine learning algorithms in detecting malicious behaviors within Wireless Sensor Networks (WSNs). Originally developed for intrusion detection in conventional networks, the KDD dataset contains a diverse array of network activities, including both normal and various attack scenarios. In this context, the dataset is adapted to WSN-specific characteristics. Features are extracted from the dataset, capturing patterns and attributes indicative of network behaviors. Machine learning algorithms, including Support Vector Machines (SVM), Naive Bayes, Logistic Regression, and k-nearest Neighbours (KNN), are trained on this adapted dataset. The KDD dataset's versatility and comprehensive representation of network activities contribute to the research's efficacy in enhancing WSN security.

By simulating malicious nodes alongside normal ones, the dataset captures the nuances of both benign and potentially harmful behaviors, enabling a comprehensive examination of network dynamics. In essence, the process of data collection and simulation enables the creation of a controlled environment that mirrors real-world scenarios. This synthetic yet authentic dataset serves as the foundation for the subsequent development and validation of advanced intrusion detection and prevention mechanisms, reinforcing the resilience and security of Wireless Sensor Networks against emerging threats.

E. Wireshark Capture and Analysis

Wireshark capture and analysis play a pivotal role in this research by offering deep insights into network behavior within the Wireless Sensor Network (WSN). As packets traverse the network of 30 nodes, including 3 malicious ones, Wireshark captures and dissects their transmission patterns, communication rates, and packet attributes. This meticulous analysis reveals key indicators of both normal and malicious behaviors, aiding in the extraction of features crucial for subsequent machine learning-based intrusion detection. Wireshark's ability to decode packet contents provides a window into the intricate dynamics of the network, guiding the development of a robust security mechanism that thwarts potential threats.

F. Feature extraction

Feature extraction is a pivotal step in this research, aiming to distill crucial information from Wireshark-captured data within the Wireless Sensor Network (WSN). By identifying and isolating pertinent attributes such as packet rates, energy consumption patterns, and communication behaviors, feature extraction reveals distinctive patterns associated with both normal and malicious node activities. These features serve as the foundation for training machine learning models to effectively discern and classify potential threats. Feature extraction bridges the gap between raw data and meaningful insights, empowering the development of a robust intrusion detection and prevention mechanism tailored to the unique challenges of WSNs.

G. Machine learning analysis

Energy harvesting, in a larger sense, is crucial to the Wireless Sensor Network (WSN) procedure. The ambient energy sources used to power the network's sensor nodes include solar radiation, temperature gradients, and movement energy. This approach reduces the dependency on battery power and enhances the longevity and sustainability of the WSN.

H. Packet analysis and classification

Packet analysis and classification constitute a pivotal phase in this research's framework. As packets traverse the Wireless Sensor Network (WSN), their attributes are extracted and subjected to rigorous analysis. This process, informed by machine learning algorithms, discerns patterns indicative of either normal or malicious behaviors. By evaluating these patterns against trained models, incoming packets are classified in real time. This classification aids in the swift and accurate identification of potential threats, enabling the system to effectively prevent the infiltration of malicious packets. Through this dynamic process, the research contributes to bolstering the security and integrity of WSNs against emerging risks.

I. Prevention Mechanism

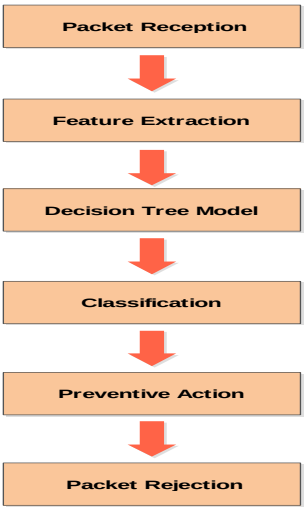

Fig 3: Prevention workflow Diagram

Step 1: Packet Reception

Upon receiving a packet, the prevention mechanism initiates its analysis to determine whether the packet is benign or malicious.

Step 2: Feature Extraction

The same 42 features extracted during the training phase are obtained from the incoming packet. These features include parameters like packet rates, energy consumption patterns, and communication behaviors.

Step 3: Decision Tree Model

The extracted features are fed into the pre-trained decision tree model. This model has learned to classify packets into either the normal or malicious category based on the patterns derived from the training dataset.

Step 4: Classification

The decision tree model classifies the incoming packet based on the features it exhibits. It assigns the packet to the corresponding class – normal or malicious – based on the established decision boundaries.

Step 5: Preventive Action

If the model classifies the packet as normal, it is deemed safe and is allowed to proceed through the network without hindrance. However, if the packet is classified as malicious, the prevention mechanism immediately takes action.

Step 6: Packet Rejection

Malicious packets, upon classification, are intercepted and prevented from entering the network further. This swift intervention prevents the potential spread of malicious activities throughout the network.

4. Results & Disussion

The results obtained from the conducted experiments reflect the effectiveness of the proposed methodology. The decision tree model, trained on extracted features from the Wireshark analysis, demonstrates high accuracy in distinguishing between normal and malicious behaviors. Through simulation and machine learning, the research successfully contributes to the advancement of intrusion detection and prevention mechanisms in Wireless Sensor Networks (WSNs), enhancing the network's ability to thwart potential threats and ensuring the integrity of communication in dynamic environments.

src	dst	pktcount	Protocol	flbyt	clbyt	label	Column1
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	126395	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.2	10.0.0.8	90333	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	76	76	no attack	
10.0.0.1	10.0.0.8	45304	icmp	5	5	Smurf Attack	
10.0.0.1	10.0.0.8	45304	icmp	5	5	Smurf Attack	
10.0.0.1	10.0.0.8	45304	icmp	5	5	Smurf Attack	

Fig 4: Dataset Description

The information utilized is from a radio log PCAP file that was recorded by the 6LOWPAN analyzer and depicts communication between the malicious node and the benign node. Wireshark is a common tool for capturing network traffic. A free and open-source packet analyzer is Wireshark. Each packet is recorded by this tool with multiple values such as time, source, destination, protocol, and metadata. Wireshark data will be saved in CSV format and processed later using the Python programming language.

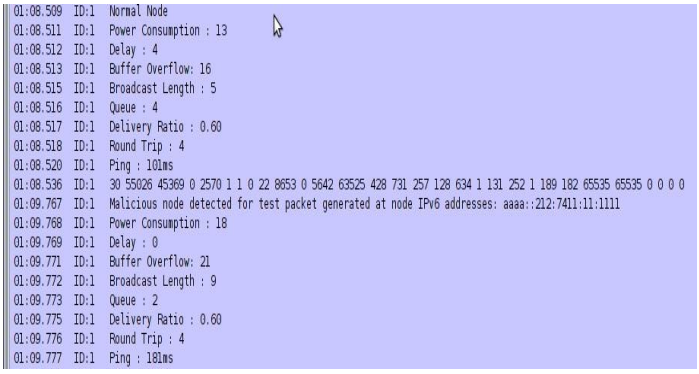

Fig 5: Mote output of a node

The mote sensor readings, network traffic, and behavior are all included in the text file that serves as the mote output data in Cooja. The packets that the motes sent and received are included in the network traffic that is stored in the file. the conduct of the motes, which contains details about the simulation's events as they happened. The mote output data can be utilized to examine the motes' behavior and spot any irregularities.

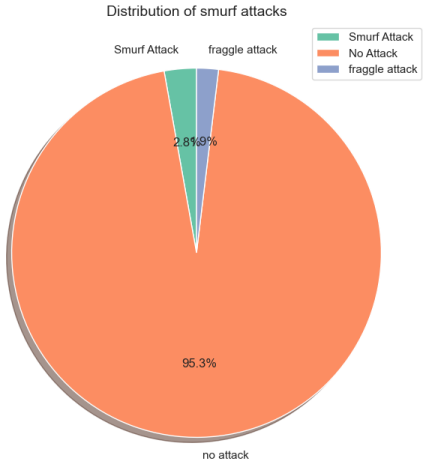

Fig 6: Percentage of DDOS Attacks

The distribution of Smurf attacks would typically involve capturing network traffic data during an attack scenario. The dataset would contain information such as the source IP addresses of the attackers, the victim's IP address, the timestamp of the attack, and other relevant network traffic characteristics. Analyzing this dataset would help researchers or security professionals understand the nature of Smurf attacks and Fraggle attacks, identify patterns, and develop effective defense mechanisms.

Table 1: This is the accuracy achieved by using the above algorithms

Name	Accuracy
KNN	97.378277
SVM	94.007491
Logistic Regression	91.760300
Naive Bayes	87.771883

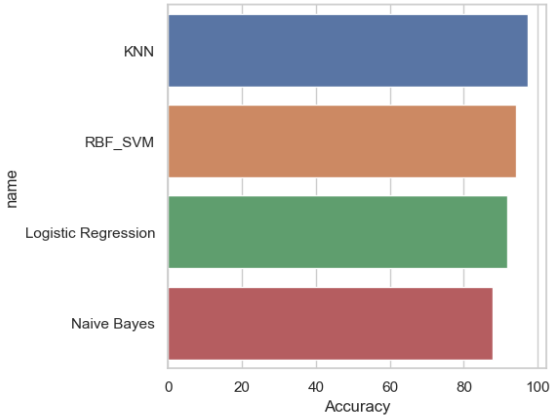

Fig7: Comparison Graph

The above figure shows the accuracy of KNN, SVM, logistic Regression, and Naïve Bayes machine learning algorithms

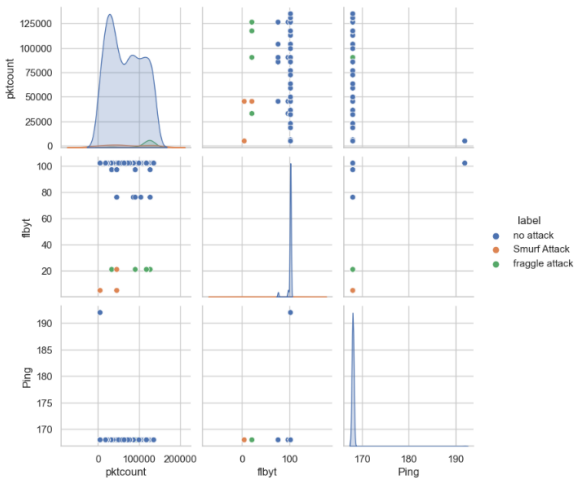

Fig 8: Attack based on parameters

Pair plot: The scatter plot matrix is like a picture that helps us see how things are related in a dataset. It uses dots on graphs to show connections between three measurements: "pktcount," "flbyt," and "Ping." Each graph compares two of these measurements. The colors of the dots tell us about different types of attacks: green is for Fraggle attacks, orange is for Smurf attacks, and blue is for no attacks. By looking at these colors and the patterns of dots, we can learn how the measurements are connected to different types of attacks.

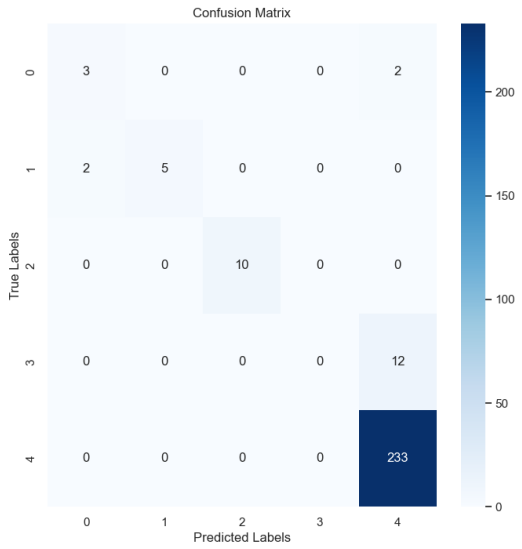

Fig 9: Confusion matrix plot

The matplotlib's heatmap function is employed to generate a graphical representation of the confusion matrix. This heatmap displays the matrix using colors and intensities, where each cell stands for a pairing of actual and predicted labels. The plot is titled "Confusion Matrix," with axis labels "Predicted Labels" and "True Labels." The heatmap is presented in shades of blue, employing color gradients to visualize patterns like misclassifications, high/low accuracy areas, thus assisting in comprehending model performance.

5. Conclusion

In conclusion, this research presents a multifaceted approach to fortify the security of Wireless Sensor Networks (WSNs) against malicious node behavior. By synergizing simulation-based data collection, advanced analysis techniques, and machine learning algorithms, the study makes significant strides in enhancing the network's resilience and integrity. The orchestrated creation of a controlled network environment, comprising

30 nodes and intentionally including 3 malicious nodes, provides a platform to comprehensively examine network behavior and responses. Through Wireshark analysis and subsequent feature extraction, distinctive attributes are identified, crucial for training machine learning models. The utilization of Support Vector Machines (SVM), Naive Bayes, Logistic Regression, and k-nearest Neighbors (KNN) underscores the efficacy of machine learning in distinguishing normal from malicious behaviors. The decision tree model's ability to classify incoming packets in real time demonstrates its potential as an adaptive intrusion detection and prevention mechanism. By intercepting and thwarting potential threats at the packet level, the prevention mechanism contributes to the network's robust defense against evolving attacks. The continuous monitoring and feedback loop ensures adaptability and effectiveness over time.

This research not only advances the understanding of WSN security but also presents a tangible solution to mitigate the risks posed by malicious nodes. By addressing both familiar attack vectors and potential emerging threats, this approach fortifies WSNs, fostering secure and resilient communication in the face of evolving challenges. The fusion of simulation, analysis, and machine learning strategies paves the way for a new era of WSN security, standing as a testament to the potential of interdisciplinary approaches in shaping a safer digital landscape.

Future Work

Future work could explore dynamic threat modeling, integrating anomaly detection, and refining machine learning models for better accuracy. Additionally, investigating edge computing integration, blockchain technology, and scalability considerations could further enhance the security of Wireless Sensor Networks. Human-in-the-loop systems, cross-layer defense mechanisms, and real-world deployment could validate and extend the research's effectiveness in practical scenarios, fostering more resilient and adaptable network security solutions.

References

[1] Kundrapu Bharathi, Dr Varanasi Usha Bala, Nandikota Dimple Sai Keerthana “Intrusion Detection System with Machine Learning Algorithms and Comparison Analysis” (IRJET), Volume 7, Issue: 04, April 2020, Pages 405-408 https://doi.org/10.1016/j.cose.2021.102540.

[2] ADITI PAUL, Somnath Sinha, SAUMYA MISHRA et al. Machine Learning based Hybrid Intrusion Detection System for detecting Cross-layer DoS attacks in IoT, 13 April 2023, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs2250467/v1]

[3] A. H. Farea and K. Küçük, “Detections of IoT Attacks via Machine Learning-Based Approaches with Cooja”, EAI Endorsed Trans IoT, vol. 7, no. 28, p. e1, Apr. 2022.

[4] Lakshmi HN, Santosh Anand, Somnath Sinha “Flooding Attack in Wireless Sensor Network-Analysis and Prevention”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019

[5] Nagarjuna S, Santosh Anand, Somnath Sinha “A Research on the Malicious Node Detection in Wireless Sensor Network” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019

[6] B. J. Santhosh Kumar and S. Sinha, "An Intrusion Detection and Prevention System against DOS Attacks for Internet-Integrated WSN," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 793-797, doi: 10.1109/ICCES54183.2022.9835838.

[7] M. Osman, J. He, F. M. M. Mokbal, N. Zhu and S. Qureshi, "ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks," in IEEE Access, vol. 9, pp. 83654-83665, 2021, doi: 10.1109/ACCESS.2021.3087175.

[8] Chandan, S. Kumar and S. Sinha, "Machine Learning based Robust Techniques to Detect DDoS Attacks in WSN," 2022 International Conference on Intelligent Innovations in Engineering and Technology (ICIIET), Coimbatore, India, 2022, pp. 294-300, doi: 10.1109/ICIIET55458.2022.9967543.

[9] B. J. Santhosh Kumar and K. R. Karthik Gowda, "Detection and Prevention of TCP SYN Flooding Attack in WSN Using Protocol Dependent Detection and Classification System," 2022 IEEE International

Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-6, doi: 10.1109/ICDSIS55133.2022.9915949.
[10] Z. Shang, Q. He, H. Guo, and Z. Li, "Malicious node detection in wireless sensor networks using power consumption patterns," 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-6. doi: 10.1109/ICC.2017.7996475
[11] X. Li, Y. Zhang, Z. Chen, and Y. Li, "A Power Consumption-Based Malicious Node Detection Method for Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 56861-56868, 2020. doi: 10.1109/ACCESS.2020.2980649
[12] M. K. Rasheed and M. H. Rehmani, "Power Consumption Based Malicious Node Detection in Wireless Sensor Networks: A Review," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 525-553, First Quarter 2019. doi: 10.1109/COMST.2018.2877873
[13] W. Song, Y. Zhang, Q. Liu, and H. Zhang, "An Efficient and Reliable Malicious Node Detection Approach Based on Power Consumption Patterns in Wireless Sensor Networks," in Sensors (Basel, Switzerland), vol. 19, no. 4, p. 878, 2019. doi: 10.3390/s19040878
[14] J. Sahoo and D. Kumar, "A Power Consumption-Based Malicious Node Detection Technique in Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, vol. 14, no. 7, pp. 1-10, 2018. doi: 10.1177/1550147718782262
[15] K.Q. Yan, S.C. Wang, C.W. Liu (2009), “A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks”, Proceedings of the International Multi-Conference of Engineers and Computer Scientists 2009, Vol IIMECS 2009, Hong Kong.
[16] Prof.Srinivasan, M. Vidhya (2015),” Cross-Layer Based Anomaly Intrusion Detection In Wireless Sensor Network” Advances in Natural and Applied Sciences, 9(6) Special, pp. 607- 613.
[17] S. Ansari, Rajeev S.G. and Chandrasekhar H.S(2003), “Packet Sniffing: A Brief Introduction”, IEEE Potentials, Dec 2002-, Volume:21, Issue:5, pp:17 – 19
[18] M.Vidhya, Prof.Srinivasan, R, Sudha, ” MULTI-LAYER INTRUSION DETECTION AND PREVENTION IN WSNs USING SELF HEALING MODULE(2015)” International Journal of Science, Engineering, and Technology Research (IJSETR Volume 4, Issue 3, pp. 424-429, ISSN:2278-7798.
[19] L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry and S. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," in IEEE Access, vol. 9, pp. 128765-128785, 2021, doi: 10.1109/ACCESS.2021.3111923.
[20] B. Jaint, S. Indu, N. Pandey and K. Pahwa, "Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine," 2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), Noida, India, 2019, pp. 247-252, doi: 10.1109/RDCAPE47089.2019.8979125.