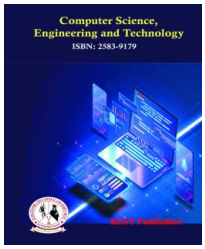
Computer Science, Engineering and Technology

Vol: 1(1), March 2025

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/1/1/11



Mitigating Malicious Attack in Manet Using Machine Learning Method

P. Balashanmuga Vadivu, M. Shanmugam, N. Indhumathi, G. Sripathi

Mahendra Engineering College, Namakkal, Tamil Nadu, India.

*Corresponding Author Email: shanmugavadivup@mahendra.info

Abstract. Mobile Ad Hoc Networks (MANETs) are distributed, self-configuring systems of mobile devices that interact with the use of permanent infrastructure. Because of their unsecured and constantly changing behavior, MANETs are extremely sensitive to a variety of security concerns, especially malicious assaults such as spoofing, Sybil and black hole. Traditional security mechanisms often fail to provide adequate protection due to the lack of centralized control and the unpredictable topology of these networks. In recent years, Machine Learning (ML) techniques have shown promising potential in enhancing security within MANETs by enabling the discovery and extenuation of malicious activities in real-time. This paper explores the application of ML methods to mitigate malicious attacks in MANETs. We propose an approach where various ML algorithms are used to identify and classify malicious behavior based on network traffic patterns and node interactions. The model is qualified on a dataset of normal and malicious network behaviors to progress its ability to recognize attacks with high accuracy. Furthermore, we discuss the integration of anomaly detection and supervised learning techniques to adapt to the self-motivated and evolving nature of the network. Experimental results demonstrate that ML-based methods significantly improve the detection and mitigation of common MANET attacks, offering a robust security solution for these vulnerable networks.

Keywords: MANETs, ML, attack, malicious, topology

1. INTRODUCTION

MANETs are a type of self-configuring, scattered wireless network in which nodes connect immediately to one another without the use of a permanent infrastructure or central authority. These networks are dynamic in nature, with the topology constantly changing as nodes move and form new communication links. This unique characteristic allows MANETs to be highly adaptable and flexible, making them appropriate for an extensive range of applications, such as emergency response [1], military operations, and remote area communications. However, despite these advantages, MANETs are also prone to a variety of security vulnerabilities due to their inherent features, making them an attractive target for malicious attacks.

The nonappearance of a central expert, combined with the open nature of communication channels, creates a fertile environment for various types of malicious activities. Since nodes in MANETs often rely on peer-to-peer communication, attackers can exploit this trust by masquerading as legitimate nodes, intercepting, altering, or dropping data packets, and disrupting the network's functionality [2]. Among the most prevalent security threats are Sybil attacks, where a malicious node presents multiple fake identities to gain control over the network, black hole attacks, where a malicious node falsely advertises itself as the best route for forwarding data but instead drops the data packets, and spoofing attacks, where an attacker impersonates a legitimate node to deceive other nodes into sharing sensitive information [3]. These malicious activities can severely degrade the performance of the network, cause data loss, reduce reliability, and compromise the confidentiality and integrity of the transmitted information.

The challenges presented by these attacks are compounded by the flexibility of the nodes and the self-motivated nature of MANETs. Traditional refuge mechanisms, such as centralized authentication, encryption, and access control protocols, are often ineffective in this environment due to the lack of centralized control and the unpredictable, constantly changing topology. For instance, traditional

intrusion detection systems (IDS) might not perform well in MANETs, as they rely on a fixed network structure and may fail to detect threats in real-time. As a result, there is an increasing demand for adaptable and scalable security systems that can respond dynamically to ever-changing network conditions.

ML techniques have received a lot of interest as a viable solution for improving MANET security. Unlike traditional security methods, ML models can be programmed to detect malicious conduct by analyzing communication patterns, node interactions, and past data. These models can classify network activities as normal or malicious, identify potential security breaches, and adapt to new, previously unseen attack patterns. Furthermore, machine learning can help reduce the reliance on predefined rules and signatures, which may not always account for the variety and complexity of attacks in MANETs [4]. By employing methods such as supervised learning, unsupervised learning, anomaly detection, classification, and clustering, ML techniques can identify subtle irregularities in the network that may indicate malicious behavior. These methods can detect attacks in real-time, allowing for swift countermeasures to be deployed, thereby minimizing the influence of the occurrences on the network.

The use of ML in MANET security has several potential advantages. First, it can provide a more accurate and efficient means of detecting complex and previously unknown attacks by analyzing large capacities of network data and identifying designs that might otherwise go unnoticed. Second, machine learning models can familiarize to the developing nature of the network, making them capable of detecting new attack strategies that emerge over time. Additionally, ML techniques can be integrated into distributed systems [5], allowing for decentralized security solutions that are well-suited to the architecture of MANETs. By reducing the need for centralized control, ML-based security systems can enhance the scalability and resilience of the network.

This paper aims to explore the potential of ML techniques in mitigating malicious attacks in MANETs. We will discuss various ML algorithms and how these can be applied to the discovery and deterrence of common attacks in MANETs. The paper will also review the trials related with applying ML in these networks, including the issues of data collection, model training, and real-time processing. Finally, the paper will examine the performance and effectiveness of ML-based security solutions [6] in MANETs, drawing comparisons to traditional security approaches and highlighting the benefits of using ML in these dynamic, decentralized environments.

The frequency and sophistication of malicious attacks on MANETs continue to grow, traditional security mechanisms are proving to be insufficient. Machine learning presents a promising alternative by offering adaptive, scalable, and real-time security events capable of detecting and mitigating a wide range of attacks [7]. This research aims to provide a comprehensive understanding of how machine learning can be leveraged to secure MANETs and ensure their reliable operation in the face of evolving threats.

2. LITERATURE SURVEY

The use of NN in mitigating malicious attacks in MANETs through ML has gained considerable attention in recent research due to their ability to learn multifaceted designs in data [8]. These models are particularly effective in distinguishing between normal network behaviors and malicious activities by analyzing network traffic. The methodology typically involves several key steps, each with its own challenges and solutions.

Data Collection and Preprocessing: The first step in utilizing Neural Networks for attack detection in MANETs involves data collection. Data is gathered from the network traffic, which could include packet headers, routing information, hop count, delay, packet size, and more. These features are essential for identifying normal patterns of network operation and recognizing deviations that could indicate an attack. Since MANETs are highly dynamic [9], the data needs to capture network characteristics under different conditions such as varying network topologies, node mobility, and environmental factors. Data may need to be normalized, transformed, or encoded to prepare it for training Neural Network models [10]. Feature extraction is also critical, as it helps identify the most important variables for detecting attacks. Techniques like **P**rincipal **C**omponent **A**nalysis (PCA) may be employed to reduce dimensionality and highlight the most relevant features.

Supervised vs. Unsupervised Learning (SL vs USL): Once the data is prepared, the next step is to choose the appropriate learning method. Supervised learning is commonly applied when labeled data (data where the attack types or behaviors are already known) is available [11]. In SL, the NN is trained using this labeled dataset to classify incoming network traffic as either normal or malicious. The model learns the underlying patterns associated with different types of attacks, such as blackhole, Sybil, DoS, and wormhole attacks.

Though, in numerous real-world situations, labeled data may be sparse or unavailable, especially for newer, unknown attack types. In such cases, unsupervised learning methods like anomaly detection or clustering are applied. Anomaly detection focuses on identifying deviations from established network norms [12]. For instance, if network behavior suddenly diverges from the established "normal" patterns—such as a spike in traffic, unusual packet loss, or unauthorized routing behavior, the model flags this as a potential attack. Clustering algorithms like K-means or DBSCAN group similar network behaviors together, and anything that falls outside these clusters can be flagged as anomalous. These unsupervised approaches are beneficial when the system must detect unknown or zero-day attacks for which labeled data is not yet available.

Training the NN: Training the Neural Network involves adjusting its parameters (such as weights and biases) using optimization algorithms like Gradient Descent. The model is trained to minimize a loss function that measures the difference between the predicted and actual outputs. Back propagation is used to update the weights based on the error. Neural Networks are particularly compatible for this task because they can learn highly complex, non-linear relations between the topographies in the data [13]. For example, they can capture intricate patterns that might be indicative of sophisticated attacks, such as botnet activity or routing manipulations. In more advanced approaches, **D**eep **N**eural **N**etworks (DNNs), which comprise manifold hidden layers, may be used to perceive more complex attacks. The depth of the network allows it to recognize hierarchical patterns and interactions among different features of the network data [14], which are often required for identifying subtle or highly sophisticated malicious behavior.

Model Evaluation: Following training, the model must be assessed to guarantee that it can apply generalization effectively to new, previously unseen data. The outcome indicators used in the assessment. These metrics let us determine how successfully the model detects malicious threats while minimizing FP and FN. Accuracy is the percentage of right predictions, however it can be misleading when dealing with imbalanced datasets (for example, if hostile attacks are far less common than normal traffic). Precision measures how many projected malicious instances were actually malicious. Recall measures how many genuine harmful instances were discovered by the model [15]. F1-score provides a balance between precision and recall, particularly significant in scenarios where both FP and FN have significant consequences. In the case of MANETs, where real-time detection is often critical, the model must balance detection performance with low latency to avoid introducing delays into the network. This requires optimizing the model to process data efficiently and quickly.

The ultimate goal of using NN and ML in MANETs is to deploy lightweight, adaptive, and scalable security solutions that can efficiently detect and alleviate malicious attacks in highly dynamic and resource-constrained environments. While there are significant challenges, such as data sparsity, computational limitations, and scalability issues [11], ongoing research continues to develop innovative techniques that address these problems. The combination of efficient data preprocessing, model optimization, hybrid methods, and real-time learning holds great promise for creating robust security systems capable of defending MANETs against a wide range of malicious activities.

3. RESEARCH METHODOLOGIES

Mitigating malicious attacks in MANETs using ML methods.

Security Solutions Based on ML Packets and routing: The protocols must be safe in order to perform successfully on a network. When developing sensitive apps, it is critical to consider security on the network. Forecasting models can be created using ML methodologies that leverage training data for specific attack trends and test information for the rest data [16] [17][3]. The learning model's accuracy is measured by its ability to recognise new assault patterns. There are a wide variety of assaults that may target MANET nodes, including flooding, **d**enial-**o**f-**s**ervice (DoS) attacks and other forms that take advantage of the network's openness. In a MANET, multi-hop transmission means that a data packet is routed from one node to another before arriving at its final destination. Transmission relies on the partnership of all nodes in an individual network. As a result, establishing the reliability of nodes is crucial for network security, because packets ought not to be routed to any unreliable or hostile node [18]. If you wish to improve the security of your network, there are several trust evaluation methodologies accessible. As shown in Figure 1, MANET security techniques can be categorized into the categories listed below. ML improves the security of MANET. A variety of ML techniques can be used to detect invasions and specific patterns of attacks in MANETs. Nonetheless, several reliable strategies for improving network security have been published in the literature. Three specific security vulnerabilities in MANETs have been fixed with ML-based techniques.

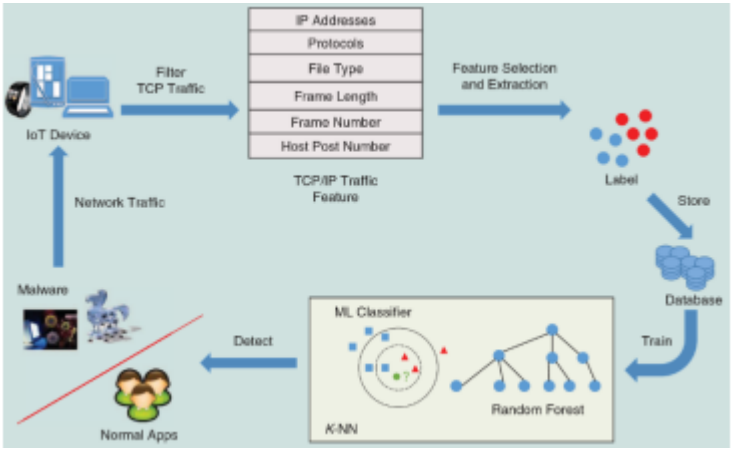


FIGURE 1. Classification of Protection Methods in MANET

Support Vector Machine (SVM): It is a type of supervised ML that employs a hyperplane structure to classify every data point in a particular set of data. SVM is more suitable for large datasets because it can deal with both linear and nonlinear situations [18]. SVM is used in WSNs to address a range of issues, including routing, localization, fault detection, handling congestion, and messaging.

Decision Trees (DT): Several algorithms use it together with additional requirements to improve the readability of their results. In DT, there are two sorts of trees to select from. One is the leaf node, and the other is the decision node. DT creates a training model using training data and forecasts a class or target based on the judgment parameters. DT give a variety of advantages, including openness, brevity, and thoroughness [17]. DT are commonly used in WSNs to address a variety of connectivity and data aggregating challenges, as well as handling mobile devices.

Convolutional Neural Network (CNN): Most often used for deep learning and neural networks with huge datasets such as photographs and videos are the CNN. Using cortical neurobiology, we were able to build a multilevel NN Using cortical neuroscience, we were able to build a multilevel NN. This structure includes both a convolution and a fully linked layer. Between these two levels, there could be subsampling layers. With the number and complexity of DNNs in well-scaled and holistically localized input data [19], they achieve the best DNNs. As a consequence, CNN is quickly applied in datasets with a large number of vertices and elements to train. Using these approaches, the researchers want to create

ML-based solutions that can successfully detect and neutralize harmful assaults in MANETs, guaranteeing the safety and endurance of these systems in dynamic and restricted by resources contexts.

4. RESULT AND DISCUSSION

In a study focused on mitigating malicious attacks in MANETs using ML methods, the result discussion typically involves analyzing how well the ML models achieve in detecting and mitigating numerous types of attacks in comparison to existing methods [20]. The results are usually evaluated based on several presentation metrics, such as accuracy, precision, recall, F1-score, and latency. The discussion may highlight strengths, weaknesses, and potential improvements for each model.

Evaluation Metrics and Performance Analysis

Accuracy: Events the general correctness of the model. High accuracy implies that the model correctly classifies both normal and malicious traffic.
Precision: Indicates how many of the identified malicious instances are actual attacks (reduces false positives).
Recall: Shows how numerous of the actual malicious instances were detected by the model (reduces false negatives).
F1-score: A sympathetic mean of precision and recall, if a stable measure when the classes (normal and malicious) are imbalanced.

Below is a chart showing the performance of three ML models DT, RF, and NN in detecting malicious attacks like blackhole, Sybil, and DoS in a MANET environment.

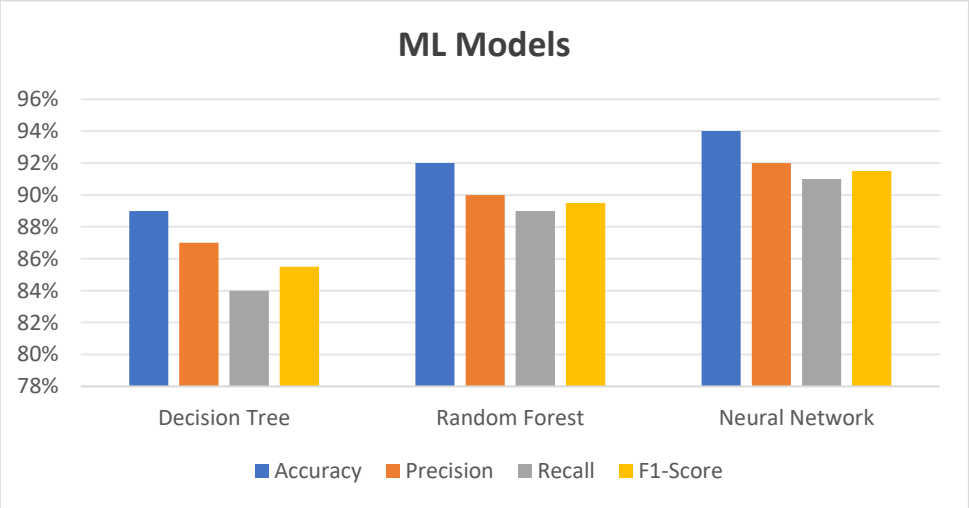


FIGURE 2. Performance of ML Models

Figure 2 illustrates the performance of ML approaches. The **NN** model performs the best in terms of overall **accuracy** and **precision**, with an **F1-score** of 91.5%. This indicates that the Neural Network is highly effective at both correctly identifying malicious attacks and minimalizing FP and FN. **Random Forest** follows closely with an F1-score of 89.5%, and the **Decision Tree** model has the lowermost performance across all metrics.

Discussion of Results

The results show that Neural Networks outperform other models in detecting malicious attacks in MANETs [21]. This is likely due to the network's ability to learn complex, non-linear relationships and generalize better across different attack scenarios. Neural Networks are capable of handling high-dimensional data, which is common in MANETs where various network features can vary drastically.

Accuracy: The high accuracy across all models suggests that the machine learning methods are effective at distinguishing between normal and malicious traffic in MANETs[22][3]. However, accuracy alone is not enough because it may not fully account for imbalanced datasets, where malicious traffic is much lower than normal traffic.

Precision and Recall: While precision is crucial for diminishing false alarms (i.e., flagging normal behavior as malicious), recall ensures that most actual attacks are detected. The results indicate that all models perform well in recall [23], meaning they are effective at detecting malicious behavior, but there is a trade-off among precision and recall. The Neural Network offers a balanced approach with both high precision and recall.

F1-Score: The F1-score is a key metric that provides a balanced measure of the model's ability to detect attacks while minimizing false positives and negatives. The Neural Network model's higher F1-score indicates that it provides the best trade-off between precision and recall[24], making it the most reliable model for real-world deployment.

In terms of real-time detection, the models' latency (processing time for each data packet) is also crucial. While Neural Networks may provide higher detection accuracy, they often require more computational resources and longer training times. However, once trained, they can be optimized for faster inference. Random Forest and Decision Trees may be more computationally efficient but might not achieve the same level of accuracy or adaptability to evolving attack patterns. The results of this study indicate that Neural Networks offer a robust and effective solution for detecting malicious attacks in MANETs, outperforming other traditional ML models [24]. However, encounters related to scalability, real-time processing, and resource limitations need to be addressed to make these solutions viable for large-scale, real-world MANET applications.

5. CONCLUSION

In conclusion, mitigating malicious attacks in MANETs using ML methods proves to be an effective and promising approach. The study highlights that ML techniques, especially NN, can significantly enhance the detection of various malicious attacks, such as blackhole, Sybil, and DoS attacks, by learning patterns in network traffic. The results demonstrate that ML models, particularly Neural Networks, offer high accuracy, precision, and recall, making them effective at identifying and mitigating attacks while minimizing FP and FN.

However, several challenges remain, counting the shortage of labeled data, the dynamic nature of MANETs, and the resource constraints of mobile devices in these networks. Addressing these challenges requires optimizing models to be lightweight and adaptive. Techniques such as model optimization, distributed learning, and edge computing will play a crucial role in overcoming these limitations and ensuring that ML-based solutions can operate efficiently in real-time and on resource-constrained devices.

The future of this research lies in improving the scalability and real-time flexibility of ML models, as well as incorporating more sophisticated approaches like reinforcement learning and hybrid models to improve detection competences. Overall, ML-based solutions have the potential to significantly recover the security of MANETs, providing robust, scalable, and efficient methods to defend against evolving and sophisticated malicious attacks.

REFERENCES

[1] Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2004). Mobile ad hoc networking. John Wiley & Sons.
[2] Goyal, N., & Gaba, A. (2013). A new approach of location aided routing protocol using minimum bandwidth in mobile ad-hoc network. International Journal of Computer Technology and Applications, 4(4), 653.
[3] Popli, R., Garg, K., & Batra, S. (2016, March). SECHAM: Secure and efficient cluster head selection algorithm for MANET. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIA Com) (pp. 1776-1779). IEEE.
[4] Kamboj, P., & Goyal, N. (2015). Survey of various keys management techniques in MANET. International Journal of Emerging Research in Management & Technology, 4(6).

[5] Zapata, M. G., & Asokan, N. (2002, September). Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security .
[6] Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. IEEE network, 13(6), 24-30.
[7] Hubaux, J. P., Buttyán, L., & Capkun, S. (2001, October). The quest for security in mobile ad hoc networks. In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing.
[8] Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping mis behavior in multihop wireless ad hoc networks. Journal of Network and Computer Applications, 35(3), 1130- 1139.
[9] Karpijoki, V. (2000). Security in ad hoc networks. In Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland.
[10] Lundberg, J. (2000). Routing security in ad hoc networks. Helsinki University of Technology, http://citeseer. nj. nec. com/400961. html.
[11] Papadimitratos, P., & Haas, Z. (2002). Secure routing for mobile ad hoc networks. In Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002) (No. CONF). SCS.
[12] Bandyopadhyay, A., Vuppala, S., & Choudhury, P. (2011, February). A simulation analysis of flooding attack in MANET using NS-3. In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE) (pp. 1-5). IEEE.
[13] Prasad, M., Tripathi, S., & Dahal, K. (2022). An enhanced detection system against routing attacks in mobile ad-hoc network. Wireless Networks, 1-18.
[14] Mondal, B., & Singh, S. K. (2022). A Comparative Analysis of Network Intrusion Detection System for IoT Using Machine Learning. In Internet of Things and Its Applications (pp. 211- 221). Springer, Singapore.
[15] Popli, R., Sethi, M., Kansal, I., Garg, A., & Goyal, N. (2021, August). Machine Learning Based Security Solutions in MANETs: State of the art approaches. In Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012070). IOP Publishing.
[16] Pachhala, N., Jothilakshmi, S., & Battula, B. P. (2021, October). A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1207-1214). IEEE.
[17] Zardari, Z. A., He, J., Pathan, M. S., Qureshi, S., Hussain, M. I., Razaque, F., ... & Zhu, N. (2021). Detection and prevention of Jellyfish attacks using kNN algorithm and trusted routing scheme in MANET. International Journal of Network Security, 23(1), 77-87.
[18] Laqtib, S., El Yassini, K., & Hasnaoui, M. L. (2020). A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. International Journal of Electrical and Computer Engineering, 10(3), 2701.
[19] Muratchaev, S. S., Volkov, A. S., Martynov, V. S., & Zhuravlev, I. A. (2020, January). Application of clustering methods in MANET. In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EI Con Rus) (pp. 1711-1714). IEEE.
[20] Ravi, N., & Ramachandran, G. (2020). A robust intrusion detection system using machine learning techniques for MANET. International Journal of Knowledge-based and Intelligent Engineering Systems, 24(3), 253-260
[21] Eid, M. M., & Hikal, N. A. (2020, October). Enhanced Technique for Detecting Active and Passive Black-Hole Attacks in MANET. In International Conference on Advanced Intelligent Systems and Informatics (pp. 247-260). Springer, Cham.
[22] Duraipandian, M. (2019). Performance evaluation of routing algorithm for Manet based on the machine learning techniques. Journal of trends in Computer Science and Smart technology (TCSST), 1(01), 25-38.
[23] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine, 35, 41-49.
[24] Sharma, Samiksha & Shekhawat, Hema & Pokharana, Anchal. (2018). Analysis & study of Routing protocols for Authentication of MANETs.

