International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

SMART SECURITY PROTOCOL FOR MANET'S USING MACHINE LEARNING ALGORITHM

Muhunthan E, Navaneethan S, Harish B, Dinesh Ram P.
Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology,
Sathyamangalam.

---***---

Abstract - *Machine learning (ML) techniques allow systems to learn based on many logical and statistical operations, helping them adapt to the environment. The main goal of ML is to recognize complex patterns and make decisions based on the results. There are various ML algorithms that have been implemented to secure mobile ad-hoc networks. The infrastructure less environment of MANETs poses great challenges in implementing security systems. Security approaches in MANETs are primarily focused on intrusion detection, countering malicious attacks, eliminating outliers/misbehaving/selfish nodes, and protecting routing paths. Researchers use state-of-the-art technologies to provide efficient security solutions considering the dynamic environment of MANETs. These technologies include machine learning, artificial intelligence (AI), genetic algorithm-based techniques, biologically inspired algorithms, etc. In this article, we present a comprehensive and systematic study of various state-of-the-art approaches to enhance the security of MANETs.*

Key Words*: *Machine Learning (ML), Mobile Ad-Hoc Networks (MANETs), Intrusion Detection Systems (IDS), Malicious Attacks, Routing Security

1. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are decentralized wireless networks where nodes communicate directly without relying on fixed infrastructure, making them highly flexible and scalable. However, this infrastructure-less nature poses several security challenges, including the risk of malicious attacks, selfish or misbehaving nodes, and insecure routing. Due to the dynamic and unpredictable topology of MANETs, traditional security measures are often ineffective. Machine learning (ML) techniques have emerged as a promising solution to enhance security in these networks by enabling systems to automatically detect patterns of normal and malicious behavior. ML models can identify intrusions, prevent attacks, detect misbehaving nodes, and optimize routing decisions based on real-time data. Supervised, unsupervised and reinforcement learning algorithms allow the system to adapt to new threats and improve the overall security of the network. In this paper, we present a comprehensive study of state-of-the-art ML approaches that address the key security challenges in MANETs, focusing on intrusion detection, attack prevention and secure routing.

2. Security Approaches in MANET'S

The unique characteristics of MANETs such as decentralization, autonomy, etc., make them attractive for various attacks on the network. Over the last decade, various security mechanisms have been proposed to detect attacks and mitigate their impact. A rough classification of these approaches is as follows: The first security protocols for MANETs were based on cryptographic approaches. In 1999, a key management system for authentication in ad-hoc networks using threshold encryption was implemented. In the proposed system, some nodes assume the role of servers and some nodes assume the role of administrators. A secure version of AODV called SAODV has also been proposed. The proposed method implements digital signatures and hash chains for cryptographic security in ad-hoc networks. Many cryptographic mechanisms were based on a central authority that issues certificates for authentication purposes. In summary, in the past, many cryptographic mechanisms have been used to introduce security features in MANETs, but the last decade has seen a paradigm shift in the networking field due to new technologies such as machine learning, deep learning, AI, and genetics. Algorithms have become an important choice for researchers in finding effective and optimized solutions to MANET security. Therefore, in this paper, we present state-of-the-art technologies that have proven to be highly effective in providing security solutions. These include detection, prevention, prediction, and containment of compromised nodes as well as various secure routing protocols based on machine learning.

Mobile **ad-hoc networks** (MANETs) face significant security challenges due to their **distributed** and dynamic nature. Unlike traditional networks, MANETs have **no** fixed infrastructure, making them more vulnerable to various attacks and malicious **behavior.** Security in MANETs is **critical** to ensure reliable communication, prevent unauthorized access, and protect sensitive **data.**

3. Security Solution Based on Machine Learning

Security is an essential requirement for all network operations such as packet and routing protocols. When developing sensitive applications, the important security features of the network must be taken into account. Machine learning techniques help in developing predictive models. They are trained using training data for specific attack patterns and tested using the remaining test data. The accuracy of a learning model is judged by its accuracy in identifying new attack patterns. Due to the open environment of the network, nodes in MANET are more vulnerable to various types of attacks. Attacks such as black holes, wormholes, grey holes, flooding, and DoS attacks. Furthermore, nodes in MANETs feature multi-hop communication, which means that a source node forwards a packet to a series of intermediate nodes before reaching the destination node. All communication relies on cooperation between nodes. Therefore, for security reasons, it is important to verify the trustworthiness of nodes to prevent packets from being forwarded to untrusted or malicious nodes in the network. To achieve this goal, there are many trust evaluation methods in the literature that have been proposed to improve the security of networks. Therefore, security mechanisms in MANETs can be classified into the following categories as shown in (Fig-1): Moreover, ML plays a vital role in improving the security of mobile ad-hoc networks. Various ML algorithms can be successfully applied in MANETs to identify intruders and specific attack patterns. Nevertheless, various trustworthy systems have also been proposed in the literature to improve security features in the network. Hence, ML-based approaches are elaborated for three specific security areas in MANETs as follows:

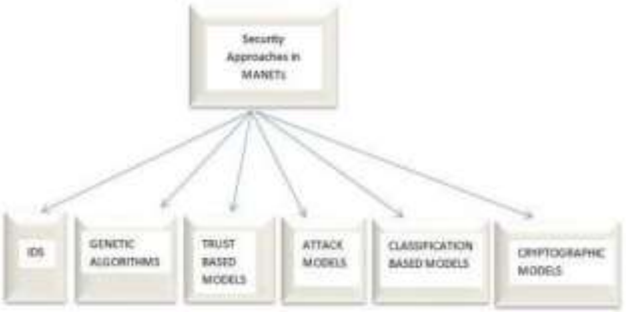

Figure 1. Classification of Security Approaches in MANETs

3.1. Machine Learning Based Intrusion Detection System

IDS (Intrusion Detection System) correspond to the defense mechanism used in MANET to monitor and investigate suspicious events. It contains various mechanisms to identify different types of anomalies in the network. In MANET, due to its open nature, nodes can join and leave at any time, making the network more vulnerable to different types of attacks. The main objective of an IDS is to identify malicious activities before they cause damage to the network. Hence, each node in a MANET is equipped with an IDS(Fig-2) to filter unauthorized access. Implementing an IDS in real-world scenarios is a big challenge since nodes in MANETs have limited resources. Machine learning techniques help in identifying various new threats and vulnerabilities. IDS can be based on various machine learning techniques such as fuzzy logic, genetic algorithms, Bayesian theory, and neural networks. IDS can be broadly divided into three categories: anomaly detection systems, abuse detection systems, and signature-based detection systems. Anomaly detection systems can filter out fraudulent or outlier nodes by comparing the actions of nodes with normal healthy patterns. If a node is found to be behaving abnormally, it is flagged as an intruder. In contrast, misbehavior detection systems and signature-based systems cannot detect new attacks because they rely on stored signatures or behavior patterns. Anomaly detection systems are therefore better at identifying unknown vulnerabilities because they assume that intruders do not follow normal attack patterns. However, they suffer from the drawback of having a high number of false positives. ML-based IDSs have become an interesting option for researchers to employ several methods to mitigate true and false negatives in the system and improve the security of MANETs. Various classification approaches in ML can be applied to classify normal and intruder nodes. Two new IDSs based on hierarchical and distributed architectures were introduced in 2003 . The proposed framework used SVM classification techniques and was primarily designed to protect the network layer. Later, another classification-based IDS was proposed, in which the authors developed a hybrid model based on Bayesian classifiers, Markov chain rules, and association rule mining to introduce security in MANETs. The proposed method ensured security at different levels, such as MAC level, routing level, and application level. Then, the characteristics of nodes at different levels were evaluated to identify the impostor nodes. Furthermore, considering the construction of an ensemble classifier for IDS, a multi-level hierarchical model was introduced to collect and process data using the ensemble classification method. Clustering techniques were tested to handle the anomaly index. Testing of the ensemble model was performed using two different routing protocols and a multi-attack model.

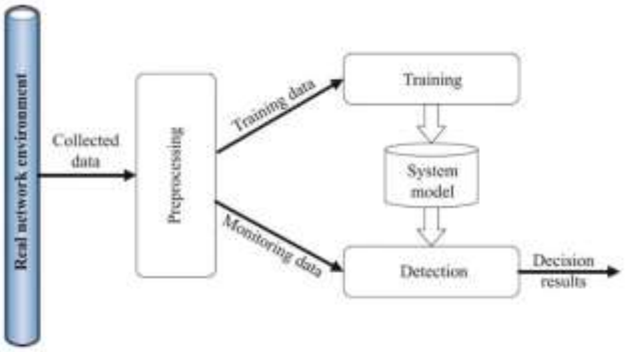

Figure 2. Machine Learning Based Intrusion Detection System

3.2 Detection of Compromised or Outlier Nodes in MANETs using Machine Learning

The main problem with the way MANETs work is the complexity in identifying and mitigating different types of attacks. Nodes in MANETs are highly insecure due to the open wireless nature of the network. Due to this, several researchers have started to take an interest in ensuring security using modern technologies, some of which have been discussed in the previous section. A flooding attack detection model using SVM classification algorithm was proposed [20]. The authors trained the SVM on different attack patterns, including flooding attacks, and the model was tested in a simulated environment. Results show that the model can successfully identify flooding attacks but fails to provide satisfactory results in case of multiple attack models. Improved K Nearest Neighbors (KNN) attack classification model for wireless networks. It classifies healthy and faulty nodes based on their behavioral patterns. It highlights differences in message forwarding speed, number of destinations when sending messages, etc. This implementation gives accurate results but does not provide a mechanism to generate a dataset. Furthermore, another model was defined to classify misbehaving and healthy nodes in MANETs . The authors applied an SVM model with an ad-hoc on-demand routing protocol and the classification was performed based on the packet loss behavior of the nodes. The performance of this approach was evaluated by calculating packet delivery ratio, packet modification, and misrouting rate.

3.3 Machine Learning Based Trusted System for Enhancement of Security in MANETs

Nodes in MANET operate in an unreliable environment and cooperate to forward data packets. To secure the network, each node is assigned a trust value. Many researchers are working on these security aspects to ensure the reliability of the network. In 2004, a trust system was proposed using the K-nearest neighbor approach, in which the trust value was evaluated based on the opinions of K trusted entities in a given period [8]. The value of K depends on the current state of the network and the number of valid neighbors. However, this may cause conflicts on the network. Due to the dynamic, complex and fuzzy nature of trust metrics, various trust methods based on fuzzy logic have been defined. A global approach was provided to assess trust based on aggregated trust scores. In the defined approach, the trust model relied on a defined function to calculate the trust level. Similarly, a trust approach based on Bayesian theory was introduced by researchers. Another approach implemented enhanced machine learning algorithms in the dynamic environment of MANETs. The authors claim that the algorithm does not rely on past data and can predict the behavior of new nodes in the network. Also, due to the physical distribution of MANET information, when selecting the optimal algorithm, it is necessary to choose an algorithm that can be distributed across the nodes. Instead of considering direct and indirect trust separately, it is recommended to apply a hybrid trust approach that aggregates trust scores. Furthermore, an improved trust model based on reinforcement learning and deep learning techniques in MANETs has been proposed [30]. The authors implemented the model using the AODV protocol and classified nodes into trusted and untrusted nodes by feeding simulated data into a recurrent neural network (RNN).

4. PROTOCOL PRPOSED

4.1. Anomaly Detection Using Supervised Learning

Data Collection: We collect traffic data such as packet delivery ratio, latency, packet loss rate, and energy consumption from the network.

Feature Extraction: Important features are extracted from the traffic data, including packet size, inter-arrival time, and routing paths.

Model Training: Using labeled data (normal and attack scenarios), we train a supervised machine learning model (e.g., Random Forest or Support Vector Machine).

Anomaly Detection: Once the model is trained, it is deployed on each node to detect any deviations from normal behavior that may indicate an attack.

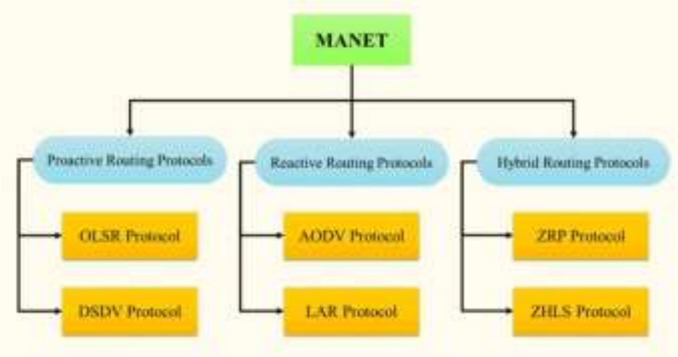

Figure 3. Routing Protocol

4.2. Adaptive Routing Using Reinforcement Learning

Q-learning algorithm: Nodes use Q-learning to dynamically adjust their routing decisions based on feedback from the network. The Q-value is updated based on the current network state (e.g. congestion, battery levels) and security state (e.g. attack detected).

State and action space: The state space represents the state of the network, and the action space consists of possible routing decisions.

Reward function: The reward function is designed to maximize secure and efficient routing, penalizing routing on compromised nodes or attacked paths.

5. SIMULATIONS AND RESLUTS

We use simulation tools like NS-3 to assess the suggested protocol's performance. Fifty mobile nodes with different network topologies and speeds make up the simulation environment.

5.1. Evaluation Metrics

The performance of the proposed protocol is evaluated based on:

Detection Rate: The proportion of attacks that were successfully identified.

False Positive Rate: The percentage of benign behavior that is mistakenly categorized as malevolent.

Packet Delivery Ratio (PDR): The proportion of successfully delivered data packets.

End-to-End Delay: The duration of a packet's journey from its origin to its final destination

Energy Consumption: The amount of energy used by nodes while the network is operating.

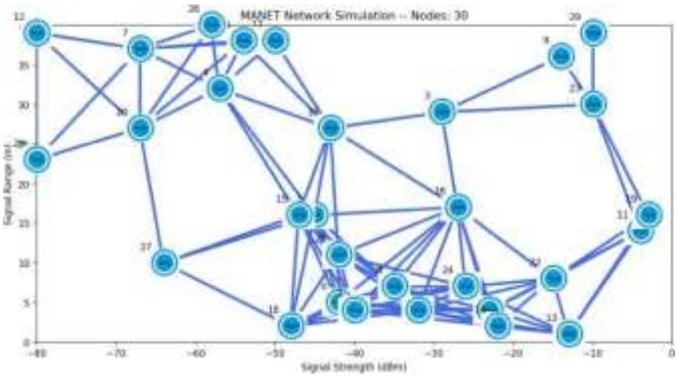

Figure 4. Simulation And Results

5.2. Results

According to the simulation results, the machine learning-based protocol performs noticeably better than conventional security measures. While the reinforcement learning-based routing offers more secure and effective routes, the anomaly detection system achieves a high detection rate with a low false positive rate.

6. CONCLUSION

Using machine learning techniques, this paper suggests a novel smart security protocol for MANETs with an emphasis on adaptive routing and anomaly detection. According to the results of our simulation, the suggested protocol efficiently reduces common security risks while maintaining optimal network performance. Future research will concentrate on enhancing the protocol's scalability even more and incorporating more machine learning models for all-encompassing threat mitigation.

ACKNOWLEDGEMENT

The Authors thanks the Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, for providing the resources and infrastructures. We extend our graduate to our Guide, Dr. ARULMURUGAN L, For their valuable guidance and support throughout this project. Special thanks to the laboratory staff for their assistance with the Synopsys tools and to our peers and family for their continuous encouragement

REFERENCES

[1] **S. K. Sharma, P. Singh**, "Security in Mobile Ad Hoc Networks: Issues and Challenges," *Journal of Wireless Communication and Networking*, vol. 2019, pp. 1-15, 2019.

[2] **H. K. Nguyen, M. M. Aziz**, "A Survey on Machine Learning for Security in Mobile Ad Hoc Networks," *IEEE Access*, vol. 8, pp.93721-93739,2020.

[3] **L. A. Tang, L. Xu**, "Q-Learning for Secure Routing in MANETs," *International Conference on Mobile Ad Hoc and Sensor Systems*, 2018, pp. 102-107.

[4] **P. Verma, A. Choudhary, B. S. Chaurasia**, "Artificial Intelligence for Security in MANETs: A Review," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 990-1015, 2021.