https://doi.org/10.48047/AFJBS.6.14.2024.1116-1122

AFJBS
African Journal of Biological Sciences
Journal homepage: http://www.afjbs.com
Research Paper
Open Access

Utilizing Machine Learning to Mitigate Attack Risks in MANET

Pratiksha Nigam
School of computer science and IT,DAVV,Indore-452001
M.P. India
Dr.Ajay Tiwari
Associate Professor
School of computer science and IT,DAVV,Indore-452001
Email. [1]nigampratikshaa@gmail.com, [2]tiwariajay8@gmail.com

Article History
Volume 6, Issue 14, 2024
Received: 30 June 2024
Accepted: 20 July 2024
Doi:
10.48047/AFJBS.6.14.2024.1116-1122

Abstract

Mobile Ad-hoc Networks (MANETs) are inherently vulnerable due to its dynamic, decentralized structure and requirement for advanced solutions for security risk mitigation. It is suggested to use a machine learning (ML)-based strategy for effective attack detection and mitigation. Important characteristics are identified and standardized from the network traffic data, such as the time it takes to respond, how frequently replies occur, and the rates at which packets are dropped. The efficacy of six Machine Learning classifiers—Support Vector, Naïve Bayes, K-Nearest Neighbour, Logistic Regression, Machine, Multilayer Perceptron, and Extreme Gradient Boosting—in identifying black hole attacks is assessed through training. The mentioned outcomes exhibit the efficiency and efficacy of the recommended machine learning strategy in limiting black hole attack risks in MANNETs. These results are based totally on numerous factors including Packet shipping Ratio (PDR), overall time, accuracy and energy usage.

Keywords: MANETs, ML, Security, Black holeAttacks, Identification of Attack. ,

Introduction

MANETs are wireless ad-hoc networks that allow unbiased motion and organization of mobile devices because they don't rely on fixed infrastructure (A. Abdelhamid, et. al. 2023). They share the wireless medium and communicate over multi-hop pathways (S. V Simpson and G. Nagarajan 2021). The MANET applications utilized decide the density and quantity of nodes. Before widespread business deployment is predicted, there are a number of issues associated with MANETs or mobile ad-hoc Networks that want to be thoroughly examined. Additionally necessary for programmed optimized route selection is device discovery. Compared to hardwired links, wireless networks have a much smaller capacity, and some nodes may get their energy from batteries or other finite sources. Due to flaws including neighbour relaying packets, a short wireless transmission range, and their broadcast nature, MANETs have security and dependability issues. Physical security risks such as denial-of-service attacks, spoofing, and eavesdropping needs to be taken into account (M. V. D. S. K. Murty and D. L. Rajamani et. al. 2023). Protection in the MANET is not easier to establish because of things like inadequate physical assurance of each node, irregular connectivity, no certification authority, and no centralised management unit (S. K. Prashanth et. al. 2023).

2.Related Work

A light-weight Support Vector Machine detecting framework was designed by (Abdelhamid et. al. 2023) to identify black hole attacks in networks, while a Secure SEAL was proposed by Simpson et al. to manage interruptions to IoT networks. Using a trust metrics (Makani et al. 2022) enhanced detection of threats and data throughput. (Younas et al. 2022) developed a neutral network-based method for detecting and mitigating black and gray whole attacks in vehicular networks, offering enhanced detection rates. V. Hamza et al. 2023) introduced the emperor penguin optimization fuzzy genetic algorithm (EPO-FGA) for energy-efficient cluster head selection, prolonging network lifetime and reducing energy consumption in simulations. (Sebopelo et al. 2019) introduce a machine learning (ML)-based security mechanism for real-time detection of malicious attacks in MANETs, classifying packet data as either normal or abnormal. Additionally, (Michael et al. 2022) explore probabilistic ML strategies to determine the preliminary threat Profile of MANETs, supplementing existing methodologies for threat evaluation. (Poongothai et al. 2014) suggest a new structure with the usage of ML to maximise detection accuracy, combining RST and SVM for improved overall performance and accuracy.

3.Proposed Approach

The network's availability, authorization, and authenticity is appreciably compromised by means of the black hole threats in MANETs. The service availability is disrupted by means of these attacks with the assistance of maliciously dropping packets, separating sections of the network, and overburdening sources. Additionally they violate authorization protocols by using enabling unauthorized access to sensitive statistics through misrepresenting malicious nodes as trustworthy. Furthermore, the authenticity of the network is undermined as blackhole attacks allow malicious nodes to impersonate legitimate ones, facilitating data tampering and eroding the network's trust mechanisms. Addressing these security challenges necessitates advanced detection and mitigation techniques, where Machine Learning can offer valuable contributions due to its adaptive and analytical capabilities. The detailed flowchart is presented in Fig. 1. The entire working is explained in below sub-sections.

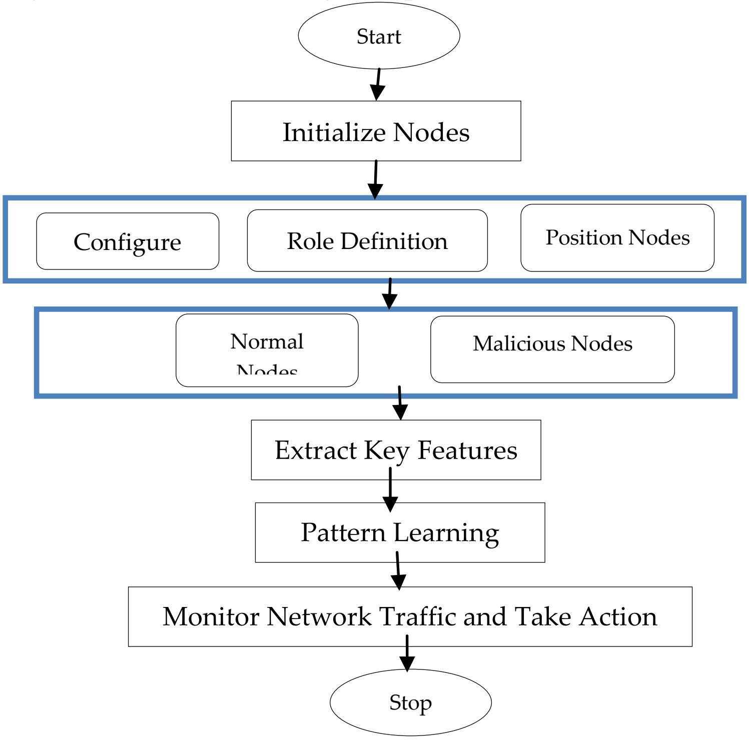

Figure 2 Working flowchart of the proposed model

1.1 Model Training

Nodes Initialization: This includes setting up their configurations, defining their roles (e.g., source, relay, destination), and positioning them if relevant (e.g., in wireless networks). Deployment of Normal Nodes: Nodes that follow standard protocol operations without any malicious intent are deployed in the network. Deployment of Malicious Node (blackhole attack): A node or set of nodes are configured to behave maliciously, mimicking the blackhole attack. Data Feature Extraction: Essential features include the total number of active nodes, frequencies of routing requests (RREQ) and replies (RREP), the data forwarding rate, and the packet drop rate. These features, when processed through a machine learning classifier, enable accurate Blackhole attack detection. Pattern Learning: The proposed method aids in detecting malicious activities of blackhole attack in an ad hoc network. The system differentiates between normal and malicious nodes. According to this, a labelled dataset is prepared based on a prominent node address. This data is then categorized into normal and malicious classes using six machine learning classifiers

1.2 Attack Detection

The trained machine learning model, which has been trained on a dataset containing instances of normal network behaviour and blackhole attacks, is deployed in the live network environment. Then as mitigation step, the system can temporarily halt any data transmission through the suspected route.

4.Result Analysis

In this section, the result is presented for black hole attack detection and avoidance using machine learning approach. In this approach preventive measure is not implemented. The entire working was implemented on MATLAB platform using following parameters.

$$Accuracy = \frac{TruePositive + TrueNegative}{TruePositive + TrueNegative + FalsePositive + FalseNegativ} \quad (1)$$

$$PacketDeliveryRatio(PDR) = \frac{SuccessfulReceptionofPackets}{TotalPacketsTransmitted} * 100 \quad (2)$$

$$TotalTime = \sum_{i=1}^{N} t_i \quad (3)$$

Where, t_i represents the total time taken to transmit n packets from source to destination.

$$TotalEnergy = \sum_{i=1}^{N} e_i \quad (4)$$

Where, e_i represents the total energy consumed by network while transmit n packets from source to destination.

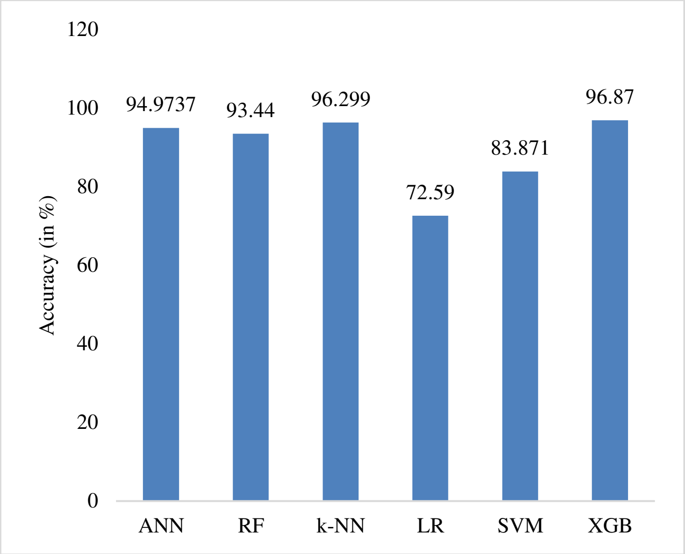

Figure 3. Accuracy Analysis of ML Techniques for Blackhole Detection

Fig 3 presents a graphical representation for comparing the accuracy of different ML models when applied to the problem of blackhole detection. Fig. 4 shows the time analysis with varying packet size with 100 nodes. For packet sizes ranging from 100 to 300, there's a direct and near-linear relationship between packet size and total time. As the packet size increases, the total time taken also increases proportionally. Beyond a packet size of 300, the growth rate of total time starts to slow down. Fig. 5 shows the energy analysis with varying packet size with 100 nodes. The total energy consumption seems to grow exponentially with the increase in packet size. Between packet sizes of 300 and 500, there's a significant jump in energy consumption. This suggests that transmitting larger packets requires considerably more energy, especially as the packet size exceeds 300. The exponential growth indicates that as the packet size increases, the energy required for transmission grows at a much faster rate.

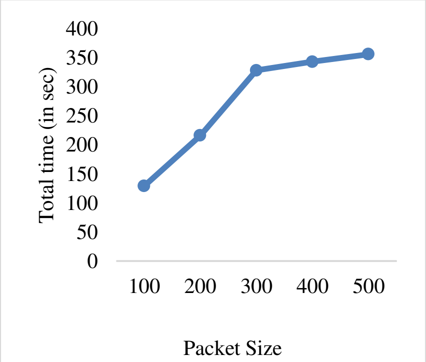

Figure 4. Time Analysis with Varying Packet Size with 100 nodes

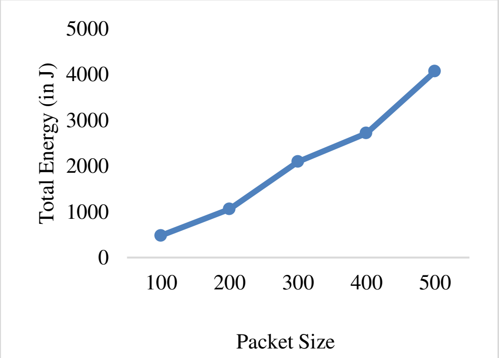

Figure 5. Total Energy Analysis with Varying Packet Size with 100 nodes

Fig. 6 shows the PDR analysis with varying packet size with 100 nodes. As the packet size increases, the Packet Delivery Rate (PDR) generally decreases. There's a notable drop in PDR when transitioning from packet sizes of 100 to 400.

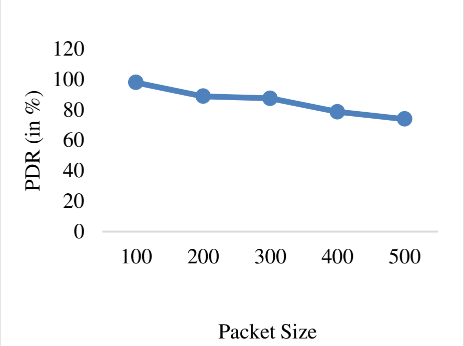

Figure 6. PDR Analysis with Varying Packet Size with 100 nodes

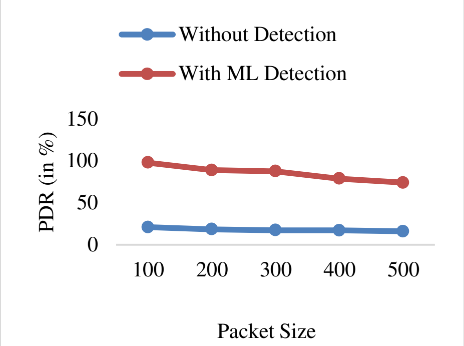

Figure 7. PDR analysis with and without ML Detection

This suggests that as packets grow in size, the likelihood of successful delivery reduces. While the PDR decreases with increasing packet size, the rate of decrease appears to slow down slightly after a packet size of 400. The fig 7 provided describes the Packet Delivery Ratio (PDR) analysis with and without Machine Learning (ML) Detection for various packet sizes. For both scenarios (with and without ML Detection), as the packet size increases, the PDR tends to decrease.

5. Conclusion

The research explored the potential of utilizing machine learning to enhance security within Mobile Ad-hoc Networks (MANETs), with a focus on mitigating risks associated with blackhole attacks. The empirical analysis, conducted using MATLAB, demonstrated that the Extreme Gradient Boosting Algorithm outperformed other classifiers in terms of accuracy in detecting blackhole attacks. Furthermore, the study found a significant improvement in Packet Delivery Ratio (PDR) when machine learning detection was employed, emphasis was put on effectiveness of the proposed approach. However, the research also observed that larger packet sizes were co-related with higher energy consumption and lower Packet Delivery Ratio (PDR), indicating areas for future optimization and investigation.

References

[1] Abdelhamid, A., Elsayed, M. S., Jurcut, A. D., &Azer, M. A. (2023). A Lightweight Anomaly Detection System for Black Hole Attack. Electronics, 12(6): 1294. doi: 10.3390/electronics12061294.

[2] S. V Simpson and G. Nagarajan, (2021). A fuzzy based Co-Operative Blackmailing Attack detection scheme for Edge Computing nodes in MANET-IOT environment, Futur. Gener. Comput. Syst., 125: 544–563,

doi: https://doi.org/10.1016/j.future.2021.06.052.

[3] M. V. D. S. K. Murty and D. L. Rajamani, (2023). Secure and Light Weight Aodv (Slw- Aodv) Routing Protocol for Resilience Against Blackhole Attack in Manets, Int. J. Soft Comput. Eng., 13: 1, 1–9. doi: 10.35940/ijsce.a3592.0313123.

[4] R. Alkanhel, A. A. Abdelhamid, and A. Ibrahim, (2023). Dipper Throated Optimization for Detecting Black-Hole Attacks in MANETs Dipper Throated Optimization for Detecting Black-Hole Attacks in MANETs, doi: 10.32604/cmc.2023.032157.

[5] S. K. Prashanth, H. Iqbal, and B. Illuri, (2023). An Enhanced Grey Wolf Optimisation–Deterministic Convolutional Neural Network (GWO–DCNN) Model-Based IDS in MANET, https://doi.org/10.1142/S0219649223500107,doi: 10.1142/S0219649223500107.

[6] Sebopelo, Rodney, Bassey Isong, and NaisonGasela. (2019). Identification of compromised nodes in MANETs using machine learning technique. International Journal of Computer Network and Information Security 11: 1, 1.

[7] Michael, Hosein, and Aqui Jedidiah. (2022). Mobile Adhoc networks-an overview of risk identification, intrusion detection and machine learning techniques used. 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE.

[8] Poongothai, T., and K. Duraiswamy. (2014). Intrusion detection in mobile AdHoc networks using machine learning approach. International Conference on Information Communication and Embedded Systems (ICICES2014). IEEE, 2014.