Journal of Industrial and Systems Engineering
Vol. 17, No. 1, pp. 204-216
Winter (January) 2025

JISE

Enhancing the Security of Mobile Ad-hoc Networks: A Black Hole Attack Mitigation Approach Using Response Time and Machine Learning Models

Fatimah Jasim Mohammed[1], Azam Andalib[2*], Hossein Azgomi[3], Seyed Ali Sharifi[4]

[1] *Computer Engineering Department, Urmia University, Urmia, Iran*

[2] *Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran*

[3] *Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran*

[4] *Department of Computer Engineering, Bon.C., Islamic Azad University, Bonab, Iran*

Abstract

As a type of wireless network, mobile ad-hoc networks (MANETs) consist of mobile nodes that are able to move freely and independently in any direction and operate in a self-configurable and self-organizing manner, especially in situations such as natural disasters, military operations, or large social events that require rapid setup without the need for fixed infrastructure. are absolutely vital. However, these networks face numerous challenges and are naturally vulnerable due to the limited resources of nodes, such as energy, processing, and memory, as well as the lack of pre-designed infrastructure. This vulnerability can lead to a variety of attacks and security threats, one of which is One of the most common is black hole attacks. In these types of attacks, attackers attract network traffic by luring other nodes and then ignore or eliminate it entirely, which can seriously affect network performance. In this paper, a new approach to detect black hole attacks through anomaly detection techniques using response generation time and machine learning models is proposed. It continuously monitors the activities of nodes and examines and analyzes real-time network traffic, and uses machine learning algorithms to identify behavioral characteristics, irregularities, and abnormal activities and differentiate them from other nodes. Analysis of the results of the nightshades shows increased accuracy in detecting black hole attacks and ensuring the security of mobile Ad-hoc networks. This approach not

[*] Corresponding Author
ISSN: 1735-8272,

only helps to detect attacks faster, but also increases the overall efficiency of the system.

Keywords: Mobile Ad-hoc Networks, Routing, Black Hole Attack, Destructive Node, Deep Learning and Response Time

1- Introduction

In today's world, with the increasing expansion of communication and information technologies, mobile ad-hoc networks (MANETs) are recognized as one of the important innovations in the field of wireless communications. These networks are used in many applications such as military, relief, and self-propelled timing due to their special features, such as the absence of the need for fixed infrastructure and the ability to self-time. and the Internet of Things (IoT) (Cirillo et al., 2019). However, these networks are highly vulnerable to security threats due to their decentralized and dynamic nature. One of the major challenges in this regard is black hole attacks, which can seriously affect the performance and security of mobile ad-hoc networks. As a type of attack in ad-hoc networks, black hole attacks are designed to redirect data traffic to a malicious node and disrupt communication between healthy nodes. This type of attack can have detrimental effects, especially when the network is extremely dense and the nodes are constantly moving. As a result, detecting and mitigating these types of attacks has become one of the main priorities in the design and implementation of mobile ad-hoc networks (Younas et al., 2022).

In this regard, the use of machine learning models has been considered as an innovative approach to increase the security of mobile ad hoc networks. Machine learning, as a branch of artificial intelligence, is able to identify complex patterns in data and automatically learn and improve its performance. Using these techniques, it is possible to detect black hole attacks as well as predict when to generate responses to these attacks. This can help reduce reaction time and increase network efficiency.

The use of machine learning models such as artificial neural networks, CNN, GRU, and GAN has enabled space-time relationships in node movements and accurate predictions without human intervention, and has performed much better in learning from larger data sets and understanding meaningful patterns to predict node positions (Cirillo et al., 2023; Movahed et al., 2023, Nozari et al., 2022).

The present study investigates different approaches to reduce black hole attacks in mobile ad-hoc networks and focuses on response generation time and machine learning models. The main purpose of this study is to provide effective solutions to identify and mitigate these types of attacks and improve the overall security of mobile ad-hoc networks.

Since mobile ad-hoc networks are also very vulnerable to insider attacks, a trust management system can be used as one of the most effective ways to deal with attacks within the network. To calculate the trust value of nodes, in addition to measures of communication behavior, energy behavior, and data behavior. Combinedly, the quality of communication is also of particular importance. For this purpose, in this paper, in order to validate and evaluate trust in order to reduce the risks of internal attacks and increase information security, a beta-based trust and credibility assessment system (BTRES) with the characteristics of loss rate, transmission frequency, reception frequency, energy consumption rate, and node power measurement has been used (Abdulhammed et al., 2019; Fallah et al., 2021, Fallah & Nozari, 2021).

In mobile ad-hoc networks, malicious nodes try to disrupt the routing process by using attacks such as denial-of-service and fake messages. Thus, to prevent network failures and increase security, intrusion detection acts as a second wall of defense (Chou and Jiang, 2021; Kalogeras et al., 2022; Nozari et al., 2024). A black hole attack is one of the most dangerous attacks in mobile ad-hoc networks, which receives packets and removes them from the network by responding to all requests and pretending to have the best

route. In this paper, a new approach to detect and prevent a black hole attack by malicious nodes with the help of data mining techniques and two-step encryption verification Based on the first node, the next step in the reverse path is proposed using the time required to generate the route request packet. This approach provides better results with minimal computations and routing overhead.

2- Previous Works

The security of mobile adversarial network networks (MANETs) as an important research topic has attracted a lot of attention, especially in the field of reducing attacks of black holes and gray holes. Traditional detection methods are known as the gateway to security in these networks, and one of the first approaches is the guardian mechanism (Sharifi and Babamir, 2016). Sajjad et al. (2022) introduced a method that detects malicious activity by continuously monitoring the behavior of neighboring nodes. Although this method is efficient in some scenarios, it may encounter false positives when the network is dynamic and vulnerable to collusion attacks. Therefore, in order to provide and increase the overall security of the network and deal with internal and external threats, it is necessary to develop and improve security methods in mobile ad-hoc networks. Rani et al. (2022) proposed a new approach using digital signatures and hash chains to protect against pathway manipulation called SAODV in order to increase resistance to attacks. The results of its simulation show that this method has a significant computational and communication overhead.

A variety of different techniques for detecting anomalies, activities, and abnormal behaviors of nodes by intrusion detection systems in mobile ad-hoc networks include anomaly-based detection, signature-based detection, and specification-based detection (Pedroso et al., 2024). One of the most important challenges in the implementation of these systems is the creation of the optimal balance between detection accuracy and computational efficiency is in mobile ad-hoc networks with limited resources. For this purpose, statistical techniques, artificial intelligence, neural networks, and data mining can be combined (Amalia et al., 2023). Venkatasubramanian et al. (2022) proposed a new approach adapted to dynamic network conditions to detect anomalies and abnormal behaviors of nodes, in which statistical modeling of normal network behavior and machine learning algorithms is used to detect and identify patterns. This method has a high overhead due to the possibility of large numbers of alerts.

Adeel et al. (2022) proposed the use of K-means clustering algorithms and decision trees to better understand the behavior of nodes, categorize their behaviors, and detect malicious nodes. This method also requires a lot of computational resources. Arulkumaran and Gnanamurthy (2017) and Panos et al. (2017), proposed a novel approach for developing an intrusion detection system and enhancing performance using machine learning algorithms and neural networks in mobile ad-hoc networks, that could predict the next actions of malicious nodes and reduce the delay in the optimization process.

Gurung and Chauhan (2018) proposed a new approach to increase the detection accuracy and packet delivery rate and reduce the false positive rate called demand-based multipath vector routing. The authors looked at the effects of malicious node activity on multi-step routing protocols in mobile ad-hoc networks they concluded that in high-mobility networks, attack-resistant protocols are needed. Tiruvakadu and Pallapa (2018) used a combination of intrusion detection systems and digital signatures to detect black hole attacks, improving packet delivery rates, latency, and routing overhead.

Khamayseh et al. (2018) proposed a distributed multipath interval vector for secure data transmission with reliability under black hole attacks, in which encrypted packet transmission takes place over several different paths. This method has improved network throughput and packet delivery rate compared to previous similar methods. Hammamouche et al. (2018) proposed a two-step approach in mobile ad-hoc networks, including They proposed identifying and sending data and predicting the safe route. In this approach, secure data transmission is largely satisfied but has high energy consumption. In Hamamoto et al. (2018) proposed a new approach to reduce the effects of black hole attack through detection and surveillance techniques. In this approach, the processing of the number of sequences of receptors is based on the value of the threshold number. are high receptor sequence numbers. In Goswami et al. (2020) proposed an effective and secure validation mechanism for authentication through digital signature in

mobile ad-hoc networks, which can improve computational overhead, end-to-end latency, and packet delivery ratio compared to other algorithms. In Moudni et al. (2019), have considered a new trust-based approach to two-factor authentication in mobile ad-hoc networks. This approach has been able to separate healthy nodes from destructive nodes by processing the estimation of the trust of nodes. In this method, the old packages of the origin node are used to send to the destination node. In Arulkumaran and Gnanamurthy (2019) a multi-black hole attack detection approach is introduced, which deals with the detection of single, cooperative black hole attacks. This approach includes three key elements: the first element is an additional path request that is sent without the use of a public broadcast address; the second element is the threshold value that represents the average destination sequence number of all malicious path requests; and the third element consists of two lists: BH† and CBH‡ Is. Updating this list is done when each of the nodes receives fake response packets and requests with the wrong target address. Investigations show that this approach reduces routing overhead and computational overhead but does not provide improvements in storage overhead.

Khan et al. (2020) proposed an approach to detect and eliminate black hole attacks in the path discovery phase, which involves a slight change by adding a bit of validity to the path response packet. This bit is only tuned by a node that has a legitimate path or destination node itself. And when the closed black hole node generates the path response, this bit will be invalidated. Each of the intermediate nodes that receive the path response packet must check the bit validity before sending it to the next node, and if it is not valid, delete that path response. This results in a reduction in processing and memory costs. In Arappali and Rajendran (2021) with the introduction of rules for identifying malicious nodes and increasing the security of the AODV protocol proposed a new approach in which two components of the number of sequences and the number of jumps have been used to identify malicious nodes. In this way, the node whose request packet has the highest number of sequences and the lowest number of jumps, or the number of packets received is high and the number of packets sent is low, or after receiving Packets do not send them to their neighbors is likely to be a destructive node. The simulation results of this approach show an increase in throughput, a decrease in the number of abandoned packets, and end-to-end latency in the network.

Riaz et al. (2019) presented a comprehensive assessment of the overall process of trust in nodes andproposed a new approach including direct and indirect evaluations of validity, synthesis and conversion of validity and trust to node behavior based on beta distribution and Bayesian formula in mobile ad-hoc networks. Sattaru et al. (2022) proposed a new approach to calculate trust and credibility in mobile ad-hoc networks based on the multivariate Gaussian distribution and Bayesian theorem and the combination of direct and indirect validity information. which can detect malicious nodes effectively. Atia et al. (2022) proposed an improved framework for establishing and managing trust dynamics in mobile ad-hoc networks using the previous trust and credit management system and some new measurements in the current trust and credibility management system. Subha and Anandakumar (2022) proposed an efficient distributed trust model for mobile ad-hoc networks, in which the calculation of direct trust, recommendation trust, energy trust, and data trust is done selectively according to the number of packets received. Bhatia et al. (2022) proposed a flexible rating-based trust and credibility framework model in mobile ad-hoc networks.

To counter Byzantine attacks on mobile ad-hoc networks in Sauer et al. (2022) a clustering approach based on trust and credibility with or without the use of a spare anchor node was proposed. According to the studies, this approach has a high computational complexity and requires special information and assumptions. A new approach based on beta distribution has been proposed to manage credit and elastic trust based on time window distribution. By analyzing the behaviors of nodes at risk for a specific period of time and comparing the differences in these behaviors, the abnormal validity value of the nodes is identified and eliminated. Saba Farheen and Jain (2022) proposed an intrusion detection approach based on fuzzy algorithms and an adaptive fuzzy neural inference system including the implementation of a neural inference system and optimization of the initial framework with a genetic algorithm in mobile ad-hoc networks.

† Black Hole

‡ Collaborative Black Hole

3- Proposed Approach

Nowadays, with the expansion and development of mobile ad-hoc networks and the increasing dependence on this technology, the security of these networks has become one of the most important challenges for researchers. One of the most serious threats in this field is black hole attacks, which can significantly affect network performance and data security. In this paper, in order to increase the security of mobile ad-hoc networks, a new approach to detect and mitigate black hole attacks using a combination of learning techniques the machine and time-generation analysis of nodal responses are proposed with the aim of identifying abnormal behavior patterns and predicting the mobility of nodes in six steps. In addition to quickly identifying and diagnosing malicious nodes, it also improves the overall security of the network by assessing the trust and analyzing the behavior of nodes. These steps include: identifying and analyzing the behavior patterns of nodes, modeling response generation time, designing a trust assessment system based on beta distribution, phase inference for decision-making, predicting nodal mobility, and identifying abnormal behaviors using deep learning models and evaluation and optimization. In the figure 1, the steps to detect and mitigate black hole attacks using the proposed approach are shown.

- **Identifying and analyzing the behavior patterns of the nodes**
  - Investigating the behaviors of nodes under different conditions.
  - Data Labeling and Identification of Attack Patterns Based on Nodes and Behavioral Characteristics Using Nearest Neighbor K Algorithm (KNN) and Determination of Node Similarity as Cluster Weight to Calculate the Euclidean Distance of Nodes from Each Other
- **Modeling Production Time Answer:**
  - Collect data on the response time of nodes in different conditions, including traffic load, number of active nodes, and energy status.
  - Predictive modeling using the GRU deep learning technique to predict response generation time based on the first node and the next step in the reverse path based on the different characteristics of the nodes.
  - To investigate the effect of various characteristics such as residual energy, number of packets received and sent, and previous behaviors of nodes on response generation time.

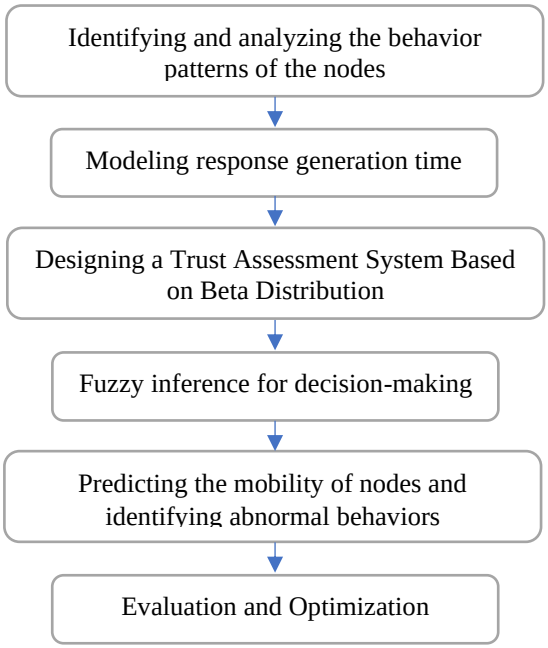

Figure 1. Steps to detect and mitigate black hole attacks using the proposed approach

❖ **Designing a Trust Assessment System Based on Beta Distribution**

- Trust evaluation based on a beta distribution that dynamically calculates the trust of nodes based on their interactions with other nodes according to relationship 1. This distribution has two parameters, α and β, which represent the parameter α positive interactions and the parameter β negative interactions.

$$P(\sigma) = (Bin(\alpha+\beta,\alpha) * Beta(1,1)) \,/\, (\alpha+\beta+1) = Beta(\alpha+1,\beta+1) \quad (1)$$

- Calculating the trust value of malicious nodes according to Relationship 2 using various trust criteria including calculating Communication TrustCT (number of collaborations) according to Relationship 3, calculating energy ETtrust (energy consumption) according to Relationship 4, and calculating DTdata trust (quality of transmitted data) according to Relationship 5.

$$dir_{Trst} = (w_1 * CT) + (w_2 * ET) + (w_3 * DT) \quad (2)$$

$$CT = E(Beta(\alpha_c+1,\beta_c+1)) = (\alpha_c+1) \,/\, (\alpha_c+\beta_c+2) \quad (3)$$

$$ET = E(Beta(\alpha_e+1,\beta_e+1)) = (\alpha_e+1) \,/\, (\alpha_e+\beta_e+2) \quad (4)$$

$$DT = E(Beta(\alpha_d+1,\beta_d+1)) = (\alpha_d+1) \,/\, (\alpha_d+\beta_d+2) \quad (5)$$

- where α_c the number of cooperative connections, β_c the number of non-cooperative connections, the α_e number of times normal energy is consumed, the number of times $\beta_e$abnormal energy is consumed, w_1 and $w_2 w_3$, respectively, the weight of communication trusts is energy and data. The update of the trust values of the nodes is done by the sliding time window in each time interval according to the relationship 6.

$$int_{Trst}(i+1)_{up} = \varphi_i int_{Trst}(i) + \varphi_{i+1} int_{Trst}(i+1) \quad (6)$$

In this regard, φ_i the value of prior trust and φ_{i+1} the value of current trust is presented.

❖ **Fuzzy inference for decision-making**

- Designing a fuzzy inference system that receives inputs such as the amount of energy remaining, the level of confidence and the response generation time, and calculates the amount of suspicion of the nodes. If the level of suspicion of each node is closer to the threshold of being destructive, it indicates that the node must be destructive and should be removed.
- Formulation of fuzzy rules for behavioral analysis of nodes and management of uncertainty and decision-making in complex situations.

❖ **Predicting the mobility of nodes and identifying abnormal behaviors**

- Using Deep Learning Models to Predict Nodal Mobility and Identify Abnormal Behaviors
- Designing an algorithm for isolating malicious nodes based on calculating response generation time and suspicious level of nodes. The response time is calculated by each of the nodes that are on the way back to the origin in the next first step and then compared with the average time of the predicted threshold. If the calculated time is less than the average predicted threshold time, that node is identified as a malicious node, because malicious nodes send the packet response immediately, without checking and updating the routing table, and in a short period of time.

❖ **Evaluation and Optimization**

- Evaluating the performance of the proposed approach in different conditions and comparing it with the existing methods.
- Optimizing the parameters of models and algorithms to achieve the best results in mitigating black hole attacks.

4- Simulation of the proposed approach and evaluation of the results

In order to simulate and evaluate the effectiveness of the combined method of mitigating black hole attacks using response generation time and machine learning models to increase the security of mobile ad-hoc networks, a series of experiments were conducted in a nocturnal environment using the NS-3 network simulator. Simulation network settings for the proposed approach are shown in the table 1.

Table 1. Simulation Parameters

Parameter	Value
Network Area	1000m*1000m
Number of Nodes	50-100
Pause time	10-50s
Speed	1-20m/s
Mobility model	Random
Simulation time	1000s
Packet size	512 bytes
Distance between packages	0.1s
Transmission range	250m
Maximum speed (m/s)	10

To evaluate the performance effectiveness of the proposed approach, the following criteria have been measured.

1. Accuracy: The correct percentage of predictions in identifying destructive and non-destructive nodes. This criterion indicates the model's ability to correctly distinguish between healthy nodes and suspicious nodes.
2. Sensitivity or Positive Detection Rate: The percentage of malicious nodes that have been correctly identified. This metric indicates the system's ability to detect actual attacks.
3. Specificity: The percentage of non-malicious nodes that have been correctly identified. This metric is important in reducing false alarms.
4. False Positive Rate: The percentage of non-destructive nodes that have been incorrectly identified as malicious. This metric is also important in reducing false alarms.
5. False Negative Rate: The percentage of malicious nodes that have been incorrectly identified as non-destructive. This metric represents the risks posed by undetected attacks.
6. Response Time: The amount of time the system spends detecting and responding to attacks. This metric refers to the efficiency and speed of the system in responding to threats.
7. Parcel Delivery Ratio (PDR): The average number of parcels successfully delivered to the destination relative to the total number of parcels shipped.
8. Packet Loss Ratio (PLR): The average number of packets lost relative to the total number of packets sent.
9. End-to-end delay: The average time it takes for packages to reach their destination.

Figure 2 shows the accuracy of black hole attack detection for TBT, ANN+SVM, ANFIS+PSO, Watchdog, Bi-LSTM, RNN, DSR, ReNN algorithms and the proposed approach. Among a large number of methods described in previous research, these methods have a more almost acceptable attack detection

percentage, which indicates an increase in network security against Black hole attacks. The results of the simulation show that the proposed approach has the highest average accuracy with 98% and the Watchdog method with 83% has the lowest average detection accuracy.

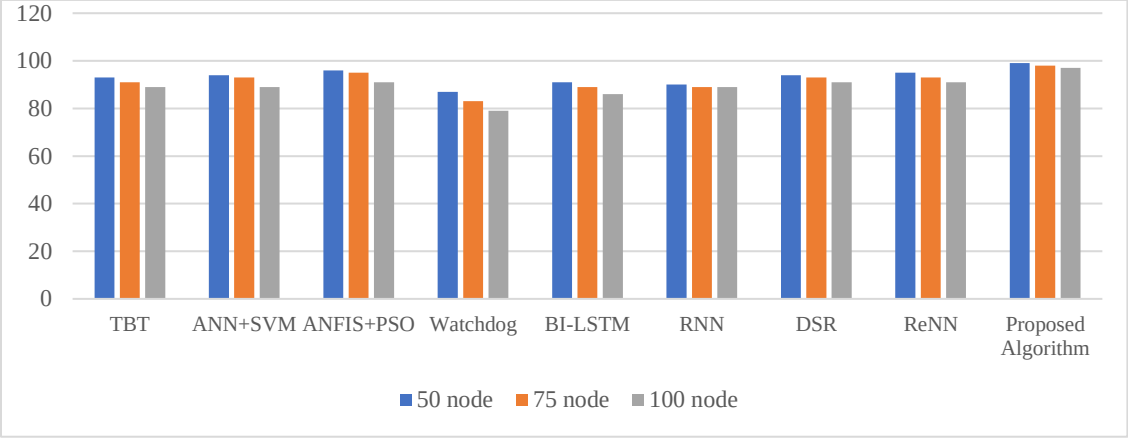

Figure 2. Comparison of the black hole attack detection accuracy of the proposed approach and other methods with the number of nodes 50, 75, and 100

The percentage of nodes that are incorrectly identified as destructive nodes is called the false positive rate. The lower the value of this parameter, the better the algorithm's performance. In Figure 3, the false positive rate of black hole attacks for the TBT, ANN+SVM, ANFIS+PSO, Watchdog, Bi-LSTM, RNN, DSR, ReNN algorithms and the proposed approach with the number of nodes of 50, 75 and 100 nodes is shown.

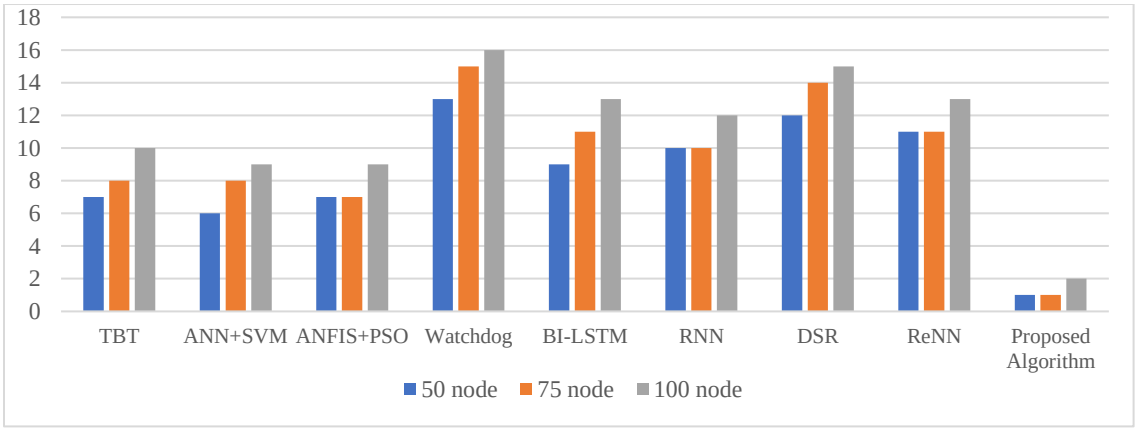

Figure 3. Comparison of false positive rate of black hole attacks of the proposed approach and other methods with the number of nodes 50, 75 and 100

As shown in the figure, the Watchdog algorithm with an average of about 14%, it has the highest value of false positive rate and the worst performance, and the proposed approach with an average of about 1% has the lowest value of false positive rate and the best performance among the compared algorithms. Therefore, it is concluded that the proposed approach increases the accuracy and reliability of attack detection.

In Figure 4, the packet delivery rate is shown in scenarios under black hole attack and without black hole attack with a number of nodes of 50, 75, and 100 for TBT, ANN+SVM, ANFIS+PSO, Watchdog, Bi-LSTM, RNN, DSR, ReNN and the proposed approach. As also shown in Figure Watchdog and DSR

algorithms It performed the worst in the successful delivery of packages and the suggested approach had the best performance in the package delivery rate compared to other algorithms.

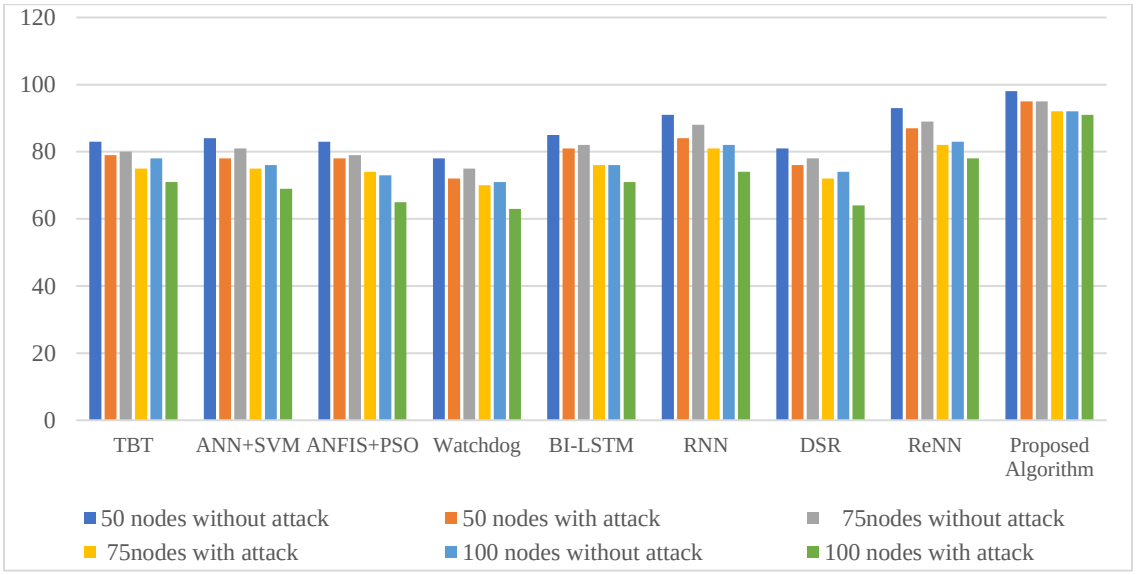

Figure 4. Comparison of the packet delivery rate of the proposed approach with other methods in scenarios under black hole attack and without black hole attack with the number of nodes of 50, 75 and 100

To increase the speed of data transmission in the network, it is necessary to reduce network latency. This will lead to improved network performance. In Figure 5, network latency in milliseconds in black hole attack and non-black hole attack scenarios with 50, 75, and 100 nodes for TBT, ANN+SVM, ANFIS+PSO, Watchdog, Bi-LSTM, RNN algorithms, DSR, ReNN and the proposed approach are shown. As expected, the latency of the whole network in the non-attack black hole state is at its lowest value for all algorithms compared to the situation with the black hole attack.

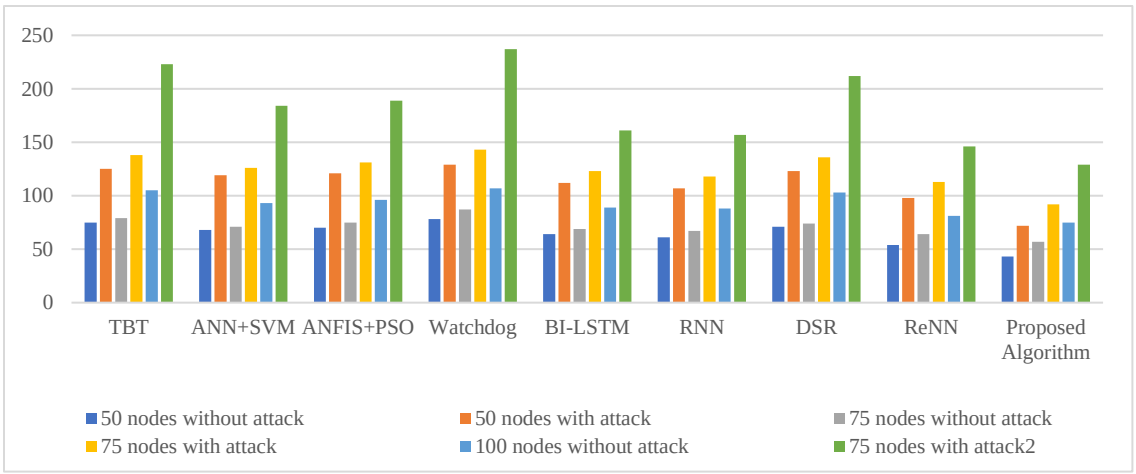

Figure 5. Comparison of the overall network latency of the proposed approach with other methods in scenarios under black hole attack and without black hole attack with the number of nodes of 50, 75 and 100

The results of the simulation show that the latency of the RNN algorithms and ReNN is lower than the other algorithms compared to the other algorithms in the scenarios without black hole attack and under

black hole attack in different nodes regardless of the proposed approach. While the proposed approach to these two algorithms has also been improved. This indicates an increase in the speed of data transfer.

Routing overhead is caused by additional resources such as computing power and bandwidth, and the routing process is reduced when the routing tables are less variable in the nodes, in which case the network time and resources are spent on closed transport instead of sequential routing, and the network is more stable. In Figure 6, the routing overhead of TBT, ANN+SVM algorithms, ANFIS+PSO, Watchdog, Bi-LSTM, RNN, DSR, ReNN and the proposed approach are shown in scenarios under black hole attack and without black hole attack with a number of 50, 75 and 100 nodes. According to the results of all algorithms, the routing overhead in the network when no attack occurred, is at its minimum, but with the occurrence of an attack, the overhead of routing also increases. According to the figure of the proposed approach, in the event of a black hole attack, it has a better performance than the algorithms compared.

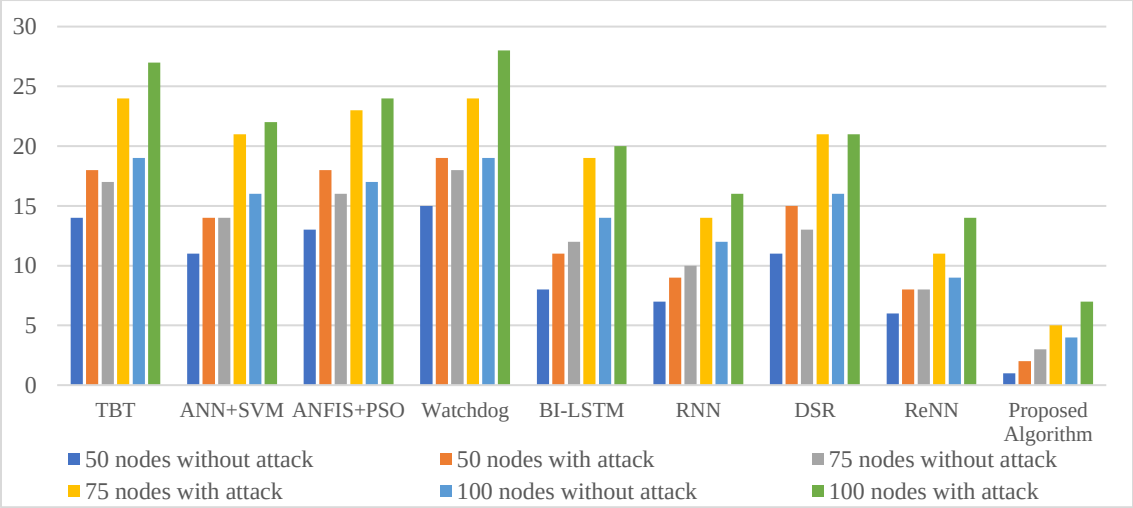

Figure 6. Comparison of routing overhead of the proposed approach with other methods in scenarios under black hole attack and without black hole attack with the number of nodes 50, 75 and 100

5- Conclusion

In this paper, the security challenges posed by black hole attacks in mobile ad-hoc networks are investigated and a new hybrid approach to reduce black hole attacks in order to increase security using response generation time and machine learning models with the aim of identifying abnormal behavior patterns and predicting node mobility in six steps: Identifying and analyzing the behavior patterns of nodes, modeling response generation time, designing a trust assessment system based on beta distribution, phase inference for decision-making, predicting the mobility of nodes, and identifying abnormal behaviors using deep learning models and evaluation and optimization were proposed. In addition to identifying and quickly detecting destructive nodes, it also improves the overall security of the network by assessing trust and analyzing the behavior of nodes.

The proposed approach was simulated in scenarios under black hole attack and without black hole attack with 50, 75 and 100 nodes and compared with TBT, ANN+SVM, ANFIS+PSO, Watchdog, Bi-LSTM, RNN, DSR, and ReNN algorithms. The results of the simulation show that the proposed approach is used in most of the evaluation criteria It has an edge compared to other algorithms. In other words, the identification of malicious nodes using the proposed hybrid approach has improved the detection accuracy, reduced false positives, increased packet delivery rate, decreased overall network latency, and reduced routing overhead.

References

Abdulhammed, R., Faezipour, M., Abuzneid, A. S., & Abumallouh, A. (2019). Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. *IEEE Sensors Letters*, *3*(1), 1–4. https://doi.org/10.1109/LSENS.2018.2880195

Adeel, A., Ali, M., Khan, A. N., Khalid, T., Rehman, F., Jararweh, Y., & Shuja, J. (2022). A multi-attack resilient lightweight IoT authentication scheme. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3676. https://doi.org/10.1002/ett.3676

Amalia, A., Pramitarini, Y., Perdana, R. H. Y., Shim, K., & An, B. (2023). A deep learning-based secure routing protocol to avoid Blackhole attacks in VANETs. *Sensors*, *23*(20), 8224. https://doi.org/10.3390/s23208224

Arappali, N., & Rajendran, G. B. (2021). MANET security routing protocols based on a machine learning technique. *Journal of Ambient Intelligence and Humanized Computing*, *12*(16), 6317–6331. https://doi.org/10.1007/s12652-020-02211-8

Arulkumaran, G., & Gnanamurthy, R. K. (2019). Fuzzy trust approach for detecting Blackhole attack in mobile ad hoc network. *Mobile Networks and Applications*, *24*(2), 386–393. https://doi.org/10.1007/s11036-017-0923-9

Atia, M. R. A., Mokhtar, M., & Khalil, J. (2022). An ANN parametric approach for the estimation of total production operation time. *Ain Shams Engineering Journal*, *13*(2), 101579. https://doi.org/10.1016/j.asej.2021.09.006

Bhatia, A., Kumar, A., Jain, A., Kumar, A., Verma, C., & Illes, Z. (2022). Networked control system with MANET communication and AODV routing. *Heliyon*, *8*(8), e11678. https://doi.org/10.1016/j.heliyon.2022.e11678

Chou, D., & Jiang, M. (2021). A survey on data-driven network intrusion detection. *ACM Computing Surveys (CSUR)*, *54*(1), 1–36. https://doi.org/10.1145/3423163

Cirillo, S., Desiato, D., & Breve, B. (2019). CHRAVAT—Chronology awareness visual analytic tool. In *Proceedings of the 2019 23rd International Conference Information Visualisation (IV)* (pp. 255–260). IEEE. https://doi.org/10.1109/IV.2019.00052

Cirillo, S., Desiato, D., Scalera, M., & Solimando, G. (2023). A visual privacy tool to help users in preserving social network data. In *Proceedings of the IS-EUD Workshops*. Cagliari, Italy.

Fallah, M., & Nozari, H. (2021). Quantitative analysis of cyber risks in IoT-based supply chain (FMCG industries). Journal of Decisions and Operations Research, 5(4), 510-521.

Fallah, M., Sadeghi, M. E., & Nozari, H. (2021). Quantitative analysis of the applied parts of Internet of Things technology in Iran: an opportunity for economic leapfrogging through technological development. Science and technology policy Letters, 11(4), 45-61.

Goswami, M., Sharma, P., & Bhargava, A. (2020). Black hole attack detection in MANETs using trust-based technique. *International Journal of Innovative Technology and Exploring Engineering*, *9*(4), 1446–1451.

Gurung, S., & Chauhan, S. (2018). A dynamic threshold-based approach for mitigating Blackhole attack in MANET. *Wireless Networks*, *24*(8), 2957–2971. https://doi.org/10.1007/s11276-017-1512-3

Hamamoto, A. H., Carvalho, L. F., Sampaio, L. D. H., Abrão, T., & Proença, M. L. (2018). Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications*, *92*, 390–402. https://doi.org/10.1016/j.eswa.2017.09.030

Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative Blackhole attacks for MANET. *Journal of Information Security and Applications*, *43*, 12–20. https://doi.org/10.1016/j.jisa.2018.10.002

Kalogeras, S., Mejri, S., & Efthimiou, F. (2022). The neuroscience of student engagement: Case studies in narrative pedagogies in mathematics, science, and technology. International Journal of Online Pedagogy and Course Design (IJOPCD), 12(1), 1-19.

Khamayseh, Y. M., Aljawarneh, S. A., & Asaad, A. E. (2018). Ensuring survivability against Blackhole attacks in MANETs for preserving energy efficiency. *Sustainable Computing: Informatics and Systems*, *18*, 90–100. https://doi.org/10.1016/j.suscom.2018.01.008

Khan, A. U., Abbas, G., Abbas, Z. H., Waqas, M., & Hassan, A. K. (2020). Spectrum utilization efficiency in the cognitive radio-enabled 5G-based IoT. *Journal of Network and Computer Applications*, *164*, 102686. https://doi.org/10.1016/j.jnca.2020.102686

Moudni, H., Er-rouidi, M., Mouncif, H., & Hadadi, B. E. (2019). Black hole attack detection using fuzzy-based intrusion detection systems in MANET. *Procedia Computer Science*, *151*, 1176–1181. https://doi.org/10.1016/j.procs.2019.04.168

Movahed, A. B., Aliahmadi, A., Parsanejad, M., & Nozari, H. (2023). A systematic review of collaboration in supply chain 4.0 with meta-synthesis method. Supply Chain Analytics, 4, 100052.

Nozari, H., & Chobar, A. P. (2024). The Dimensions and Components of Marketing 5.0: Introduction to Marketing 6.0. In Advanced Businesses in Industry 6.0 (pp. 75-86). IGI Global.

Nozari, H., & Szmelter-Jarosz, A. (2022). IoT-based supply chain for smart business. ISNet.

Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, quantifying, and detecting the Blackhole attack in infrastructure-less networks. *Computer Networks*, *113*, 94–110. https://doi.org/10.1016/j.comnet.2016.12.012

Pedroso, C., Batista, A. de S., Brisio, S., & Santos, A. (2024). A direct collaborative network intrusion detection system for IoT networks integration. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*. SBC.

Rani, P., Kavita, Verma, S., Kaur, N., Wozniak, M., Shafi, J., & Ijaz, M. F. (2022). Robust and secure data transmission using artificial intelligence techniques in ad-hoc networks. *Sensors*, *22*(1), 251. https://doi.org/10.3390/s22010251

Riaz, M. K., Yangyu, F., & Akhtar, I. (2019). A multidimensional trust inference model for the mobile Ad-Hoc networks. In *28th Wireless and Optical Communications Conference (WOCC)* (pp. 1–5). IEEE. https://doi.org/10.1109/WOCC.2019.8770587

Saba Farheen, N.S., & Jain, A. (2022). Adaptive fuzzy logic inspired path longevity factor-based forecasting model reliable routing in MANETs. *Sensors International*, *3*, 100201. https://doi.org/10.1016/j.sintl.2022.100201

Sajjad, S. M., Mufti, M. R., Yousaf, M., Aslam, W., Alshahrani, R., Nemri, N., Afzal, H., Khan, M. A., & Chen, C. M. (2022). Detection and blockchain-based collaborative mitigation of Internet of Things botnets. *Wireless Communications and Mobile Computing*, *2022*, 1194899. https://doi.org/10.1155/2022/1194899

Sattaru, N. C., Baker, M. R., Umrao, D., Pandey, U. K., Tiwari, M., & Chakravarthi, M. K. (2022). Heart Attack Anxiety Disorder using Machine Learning and Artificial Neural Networks (ANN) Approaches. In *2022 2nd International Conference on Advanced Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 680–683). IEEE. https://doi.org/10.1109/ICACITE53722.2022.9823697

Sauer, C., Lyczkowski, E., Schmidt, M., Nüchter, A., & Hoßfeld, T. (2022). Testing AGV mobility control method for MANET coverage optimization using procedural simulation. *Computer Communications*, *194*, 189–201. https://doi.org/10.1016/j.comcom.2022.07.033

Sharifi, S. A., & Babamir, S. M. (2016). A new approach to detecting and preventing the wormhole attacks for secure routing in mobile ad-hoc networks based on the SPR protocol. In *2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICAICT.2016.7991672

Tiruvakadu, D. S. K., & Pallapa, V. (2018). Honeypot-based Blackhole attack confirmation in a MANET. *International Journal of Wireless Information Networks*, *25*(4), 434–448. https://doi.org/10.1007/s10776-018-0415-2

Venkatasubramanian, S., Suhasini, A., & Hariprasath, S. (2022). Detection of Black and Grey Hole attacks using hybrid cat with PSO-based deep learning algorithm in MANET. *International Journal of Computer Networks and Applications (IJCNA)*, *9*(3), 724–735.

Younas, S., Rehman, F., Maqsood, T., Mustafa, S., Akhunzada, A., & Gani, A. (2022). Collaborative detection of Black Hole and Gray Hole attacks for secure data communication in VANETs. *Applied Sciences*, *12*(24), 12448. https://doi.org/10.3390/app122412448