A TECHNIQUES FOR SECURITY IN MANET: A COMBINED APPROACH OF NEURAL NETWORK AND AODV FOR MALICIOUS ATTACK DETECTION AND PREVENTION

Ashutosh Vashist, Research scholar Dept. Of Computer science & Engg.
Om Sterling Global University. Hisar
Dr. Rajinder Singh Sodhi, Associate Professor, Dept. Of Computer science & Engg,
Om Sterling Global University Hisar

Abstract

Mobile Ad hoc Networks (MANETs) are dynamic and self-configuring networks that lack a centralized infrastructure, making them vulnerable to various types of malicious attacks. Ensuring the security and reliability of MANETs is crucial for their successful deployment in critical applications. In this research, we explored the detection and prevention of malicious attacks in MANETs through a combined approach of Neural Network and the Ad hoc On-Demand Distance Vector (AODV) routing protocol. The proposed methodology involves training a Neural Network model using relevant datasets to classify normal network behavior and detect different types of malicious activities. The trained Neural Network model is then integrated into the AODV routing protocol to enhance its capabilities in identifying and mitigating malicious attacks in real-time. Simulations and experiments are conducted to evaluate the performance of the integrated system. Various scenarios involving different types of attacks are generated to assess the accuracy and efficiency of the detection and prevention mechanisms. Performance metrics such as detection accuracy, false positive rate, and network throughput are collected and analyzed. The results show that the combined approach of Neural Network and AODV offers promising results in terms of improved detection and prevention of malicious attacks in MANETs. The integrated system demonstrates higher accuracy in detecting attacks and effectively mitigating their impact on network performance. This research contributes to the advancement of MANET security by providing a proactive and intelligent defense mechanism against malicious attacks. The findings offer insights into the effectiveness of the proposed approach and guide the development of enhanced security mechanisms and protocols for MANETs. Ultimately, this research aims to promote the secure and reliable operation of MANETs in various real-world applications.

Keywords: MANET, Malicious attacks, Neural Network, AODV, Detection and prevention

1. Introduction

Malicious attacks in Mobile Ad hoc Networks (MANETs) pose signif threats to the network's security and operation. In recent years, researchers have explored various techniques, including the use of neural networks and the Ad hoc On-Demand Distance Vector (AODV) routing protocol, to mitigate these attacks. Let's discuss the exploration of malicious attacks and preventive measures in MANETs using neural networks and AODV.

Malicious Attacks in MANETs: Malicious attacks in MANETs be broadly categorized into the following types: a. Denial of Service (DoS) attacks: These attacks aim to disrupt network operations by overwhelming the network with excessive traffic or by exploiting vulnerabilities in the network protocols.

Blackhole attack: In this attack, a malicious node falsely claims to have the shortest path to the destination, attracting traffic towards itself and dropping it, leading to network congestion and disruption.

Grayhole attack: Similar to the blackhole attack, the grayhole attack selectively drops packets, causing a degradation in network performance.

Preventive Measures using Neural Networks: Neural networks be used to detect and prevent malicious attacks in MANETs. Here are a few approaches: a. Intrusion Detection Systems (IDS):

Neural networks be trained to identify patterns of malicious behavior in network traffic and detect anomalies. By analysing network traffic features, such as packet headers, payload, and traffic patterns, neural networks identify suspicious activities and trigger alerts.

AODV Routing Protocol: The AODV routing protocol is a widely used protocol in MANETs. It be enhanced to provide better security against attacks. Some modifications and additions include: a.

Route Validity Checking: AODV be extended to include additional checks to verify the validity of received routing information. This prevents the acceptance of forged or tampered routing updates from malicious nodes.

Secure Route Discovery: AODV employ cryptographic techniques to secure the route discovery process. This prevents attackers from eavesdropping, injecting false routing information, or manipulating route requests and replies.

Route Monitoring and Maintenance: AODV incorporate mechanisms to continuously monitor the performance and integrity of established routes. If a route is compromised or affected by a malicious attack, the protocol trigger route repairs or re-establishment to maintain network connectivity.

1.1 **Scope of Research**

The scope of research on the exploration of malicious attacks and their preventive measures in Mobile Ad hoc Networks (MANETs) through the integration of Neural Networks and the Ad hoc On- Demand Distance Vector (AODV) routing protocol is multidimensional. It encompasses investigating the various types of attacks, such as Denial of Service (DoS), blackhole, grayhole, and wormhole attacks, that potentially target MANETs. The research also involves exploring the application of neural networks for intrusion detection, trust management, and collaborative learning to detect and mitigate these attacks effectively. Additionally, the scope includes enhancing the AODV routing protocol with mechanisms for route validity checking, secure route discovery, and route monitoring and maintenance to ensure the resilience and security of the network. The research aims to develop comprehensive solutions that integrate neural network-based detection and prevention techniques with the AODV routing protocol to safeguard MANETs against malicious attacks and ensure reliable and secure communication within the network.

1.2 **Significance**

The Significance of research on the exploration of malicious attacks and their preventive measures in MANETs through Neural Networks and the AODV routing protocol lies in its potential to enhance the security and reliability of these networks. By investigating and addressing the vulnerabilities and threats posed by various attacks, and by integrating advanced techniques such as neural networks for intrusion detection and prevention, as well as enhancing the AODV routing protocol for secure communication, this research contribute to safeguarding MANETs against malicious activities. Such advancements are crucial for ensuring the seamless operation of MANETs in various domains, including emergency response, military operations, disaster management, and IoT deployments, ultimately facilitating secure and efficient communication in dynamic and resource-constrained network environments.

2. Research Background

The article titled "A Trusted Distributed Routing Scheme for Wireless Sensor Networks Using Blockchain and Jellyfish Search Optimizer Based Deep Generative Adversarial Neural Network (Deep-GANN) Technique" by Raja and Periasamy (2022) focuses on proposing a novel routing scheme for wireless sensor networks (WSNs) that integrates blockchain technology and a deep generative adversarial neural network (Deep-GANN) technique based on the Jellyfish search optimizer. The research aims to enhance the trustworthiness and reliability of routing in WSNs by leveraging the decentralized nature of blockchain and the advanced learning capabilities of Deep-GANN. The article presents the design and evaluation of the proposed scheme, highlighting its potential to address security and trust issues in WSNs and improve the overall performance of routing protocols. The paper titled "Blackhole Attack Effect on MANETs' Performance" by Gaber and Azer

(2022) investigates the impact of blackhole attacks on the performance of Mobile Ad hoc Networks (MANETs). The study focuses on evaluating the effects of these malicious attacks on various performance metrics, such as throughput, packet delivery ratio, and end-to-end delay, using a simulation-based approach. The paper aims to provide insights into the vulnerabilities of MANETs against blackhole attacks and the resulting degradation in network performance. By analyzing the experimental results, the research contributes to a better understanding of the impact of blackhole attacks and guide the development of effective countermeasures to mitigate their detrimental effects on MANETs. In the book chapter titled "Computational Intelligence Techniques for Optimization in Networks" by Gautam and Mahajan (2022), the authors explore the application of computational intelligence techniques for optimizing the performance of wireless networks. The chapter highlights the use of various computational intelligence methods, including genetic algorithms, particle swarm optimization, and artificial neural networks, in addressing optimization challenges in network settings. The research emphasizes the importance of smart and sustainable approaches to enhance the performance, efficiency, and resource utilization of wireless networks. By leveraging computational intelligence techniques, the chapter aims to provide valuable insights and practical solutions for optimizing network performance in real-time applications. The article titled "Big Data Analytics for MANET Based Sustainable Smart Healthcare Solution" by Gautam, Mahajan, and Zafar (2022) focuses on the application of big data analytics in developing a sustainable smart healthcare solution based on Mobile Ad hoc Networks (MANETs). The research explores the integration of MANETs and big data analytics to enable efficient collection, processing, and analysis of healthcare data for improved healthcare services. The article highlights the potential benefits of using MANETs in healthcare settings, such as remote patient monitoring, real-time data transmission, and personalized healthcare. By leveraging big data analytics techniques, the study aims to enhance healthcare decision-making, disease management, and overall healthcare outcomes. The research contributes to the advancement of sustainable and intelligent healthcare solutions through the integration of MANETs and big data analytics. The paper titled "A Secured Optimized AOMDV Routing Protocol in MANET Using Lightweight Continuous Multimodal Biometric Authentication" by Brindha and Meenakshi (2022) presents a research study on enhancing the security and optimization of the Ad hoc On-Demand Multicast Distance Vector (AOMDV) routing protocol in Mobile Ad hoc Networks (MANETs) using lightweight continuous multimodal biometric authentication. The research focuses on integrating biometric authentication techniques, such as fingerprint and face recognition, into the AOMDV protocol to enhance the security of communication among nodes in MANETs. The paper also explores the optimization of the AOMDV protocol to improve its efficiency and scalability. The study aims to provide a secured and optimized routing protocol solution for MANETs that leverages lightweight continuous multimodal biometric authentication, contributing to the enhancement of security and performance in MANET environments.

3 Methodology

The methodology for detection of malicious attacks and their preventive measures in MANET through Neural Network and AODV (Ad hoc On-Demand Distance Vector) likely involves several steps. Firstly, a thorough literature review is conducted to understand existing malicious attacks in MANETs and the current preventive measures employed. Then, a suitable Neural Network model is designed and trained using relevant datasets to detect and classify malicious activities in MANETs. The AODV routing protocol is integrated with the Neural Network model to enhance the detection and prevention of attacks. Simulations or experiments are conducted to evaluate the performance of the proposed approach in terms of attack detection accuracy, network performance, and overhead. The obtained results are analysed to assess the effectiveness of the Neural Network and AODV combination in mitigating malicious attacks in MANETs.

3.1 General Procedure for preventive measures malicious attacks

The procedure for malicious attacks and their preventive measures in MANET through Neural Network and AODV be outlined as follows:

•Problem Identification: Identify the specific malicious attacks that are prevalent in MANETs and understand their impact on network performance and security.

•Data Collection: Gather relevant datasets that include examples of normal network behavior and instances of different types of malicious attacks. This data will be used for training and evaluating the Neural Network model.

•Neural Network Model Design: Design and configure a suitable Neural Network architecture for detecting and classifying malicious activities in MANETs. This may involve selecting appropriate input features, determining the number and type of layers, and defining the training algorithm.

•Training and Testing: Train the Neural Network model using the collected datasets, adjusting the model's parameters and weights to optimize its performance. Validate the trained model using separate testing datasets to assess its accuracy and robustness in detecting malicious attacks.

•Integration with AODV: Integrate the trained Neural Network model into the AODV routing protocol. Define the mechanisms through which the AODV protocol utilize the Neural Network outputs for detecting and mitigating malicious attacks in real-time.

•Simulation or Experimentation: Conduct simulations or real-world experiments to evaluate the performance of the integrated system. Generate different scenarios involving various types of attacks and measure the system's ability to detect and prevent them. Collect performance metrics such as detection accuracy, false positive rate, and network throughput.

•Analysis and Evaluation: Analyze the collected data and evaluate the performance of the system. Compare the results with existing approaches and assess the effectiveness of the Neural Network and AODV combination in detecting and preventing malicious attacks in MANETs.

•Conclusion and Recommendations: Summarize the findings, highlight the strengths and limitations of the proposed approach, and provide recommendations for further improvements or areas of future research.

3.2 Steps to Set up the simulation in MATLAB

- **Install and set up MATLAB: Download and install MATLAB on computer.**
- **Implement the Neural Network:**

Define the architecture: Decide on the topology of nodes in proposed network for untrained neural network.

Assign the network parameters:

Arrange the nodes with base station (As a Sink node)

Incorporate the AODV Routing Protocol:

• Further AODV routing protocol and its implementation in MATLAB through existing libraries has been deployed.

• Modify the AODV implementation: Extend the AODV implementation to include security mechanisms for detecting and preventing malicious attacks. This involved integrating the neural network into the AODV protocol to aid in attack detection.

• Implement attack prevention strategies: Develop mechanisms within the AODV protocol to take proactive measures in preventing attacks based on the information provided by the neural network.

Integration and Testing:

Integrate the trained neural network with the modified AODV protocol in MATLAB. Conduct simulations or experiments to evaluate the performance of the combined approach.Measure key metrics such as detection accuracy, false positives, false negatives, and overall network performance.

Analysis the network parameters.

Analyse the results obtained from the simulations or experiments to assess the effectiveness of the combined approach.

Iterate and refine the neural network and AODV implementation based on the analysis results.

3.3 Perform the network parameters (Presence of neural network and Malicious activities)

To perform the network parameters with the presence of neural network and malicious activities, you need to set up a simulation environment using a network simulator such as MATLAB. Here are the general steps this follow:

- Define the network topology: Define the number of nodes, their positions, and the network parameters such as the communication range, data rate, and transmission power.
- Select the routing protocol: Choose a routing protocol that fits the requirements, as AODV.
- Implement the neural network: we use MATLAB to create a neural network model that detect malicious activities in the network. The neural network model should be trained using datasets that contain normal and malicious traffic patterns.
- Implement the malicious activities: We implement different types of malicious activities in the network, such as blackhole attacks, wormhole attacks, or gray hole attacks. The attacks be implemented by modifying the source code of the routing protocol or by using specialized software tools.
- Simulate the network: Use the network simulator to run the simulation and collect the data on the network performance parameters such as end-to-end delay, packet delivery ratio, throughput.
- Analyze the results: Analyse the simulation results and compare the network performance metrics with and without the presence of malicious activities and with the use of a neural network.

By above general steps, this performs network simulations with the presence of neural networks and malicious activities to evaluate the effectiveness of different countermeasures and mitigation techniques.

Measuring Parameters and Simulative Outcomes

- Packet transmitted: the number of packets sent in the test
- Packet drops: the number of packets lost during the test
- PDR (Packet Delivery Ratio): the percentage of packets that were successfully delivered
- E2E (End-to-End) Delay: the average time it took for a packet to travel from the source to the destination
- Throughput: the amount of data that was successfully transmitted per unit of time

Table1: Random Test Result (Apply Neural Network)

Test Condition	Packet transmitted	Packet drops	PDR	E2E Delay	Throughput
Test 1	170	8.00	95.50	0.13	1346.90
Test 2	170	12.60	92.59	0.12	1394.10
Test 3	150	0.00	100	0.04	3380.20
Test 4	190	21.00	88.95	0.12	1533.50
Test 5	200	10.50	94.75	0.08	2483.70
Test 6	150	0.00	100	0.04	3587.80
Test 7	210	12.60	94.00	0.09	2373.70
Test 8	190	16.80	91.16	0.12	1592.30
Test 9	200	10.50	94.75	0.08	2521.30
Test 10	150	0.00	100	0.08	1945.10
Test 11	180	6.30	96.50	0.08	2195.60
Test 12	190	12.60	93.37	0.12	1617.70
Test 13	180	6.30	6.50	0.09	2115.10
Test 14	170	4.20	97.53	0.11	1482.30
Test 15	210	23.10	89.00	0.11	1848.60

The table represents the results of different test conditions in a network where a neural network is applied. Each test condition is characterized by the number of packets transmitted, packet drops, packet delivery ratio (PDR), end-to-end (E2E) delay, and throughput. From the table 1, we observe variations in the network performance across different test conditions. Some tests show high PDR (e.g., Test 3 and Test 6) with no packet drops, indicating successful packet delivery. Test 13, on the other hand, exhibits a low PDR, suggesting potential issues in packet delivery. The E2E delay ranges from 0.04 to 0.13, with lower values indicating faster packet transmission. Similarly, the throughput varies across the tests, with higher values indicating greater data transmission rates. Overall, the results demonstrate the impact of different test conditions on network performance, providing insights into the effectiveness of the applied neural network in terms of packet delivery, delay, and throughput.

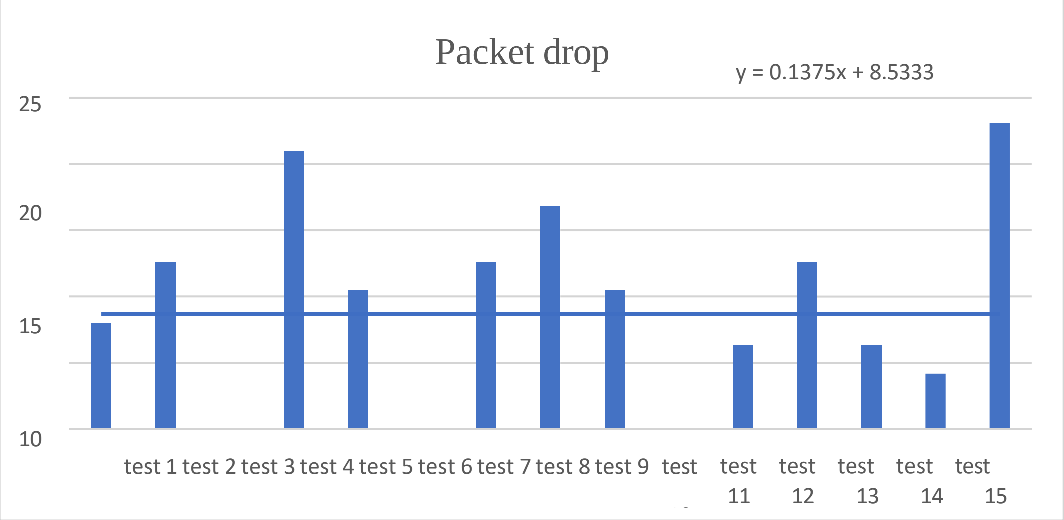

Fig1: Packet Drop at proposed network (Number of tests 15)

Packet drop occurs when a packet is lost during transmission, which result in data loss, retransmission, and reduced network performance. Based on the table, we see that some tests had no packet drops (Test 3 and Test 6), while others had a Significance number of packet drops (Test 4, Test 7, Test 8, and Test 15). The number of packet drops be used to calculate the packet delivery ratio (PDR), which is the percentage of packets that were successfully delivered. PDR be calculated as (Packet Transmitted - Packet Drops) / Packet Transmitted * 100. It's also important to note that the number of packets drops alone is not enough to evaluate network performance fully. We need additional information such as the number of packets transmitted, the end-to-end delay, and throughput, among others, to provide a more comprehensive analysis of the network's performance. Without this information, we not evaluate the network's performance accurately or identify areas for improvement.

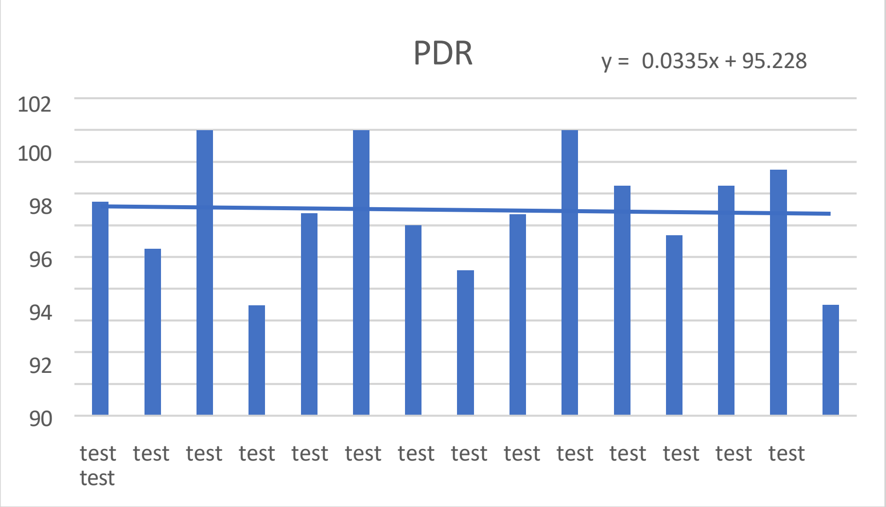

Fig2: PDR at proposed Network (Number of tests 15)

The PDR measures the percentage of packets that were successfully delivered without any loss during transmission. Based on the table, we see that the PDR varies between different tests. Some tests had a high PDR of 100% (Test 3, Test 6, and Test 10), while others had a relatively lower PDR, such as Test 4 and Test 15. It's important to note that a high PDR indicates that the network is performing well and that the majority of the packets are being delivered successfully, while a lower PDR indicates that there may be issues with the network's performance, such as packet loss or congestion. However, it's important to note that the PDR alone is not enough to evaluate network performance fully. We need additional information, such as the number of packets transmitted, the packet drops rate, end-to-end delay, and throughput, among others, to provide a more comprehensive analysis of the network's performance. Without this information, we not evaluate the network's performance accurately or identify areas for improvement.

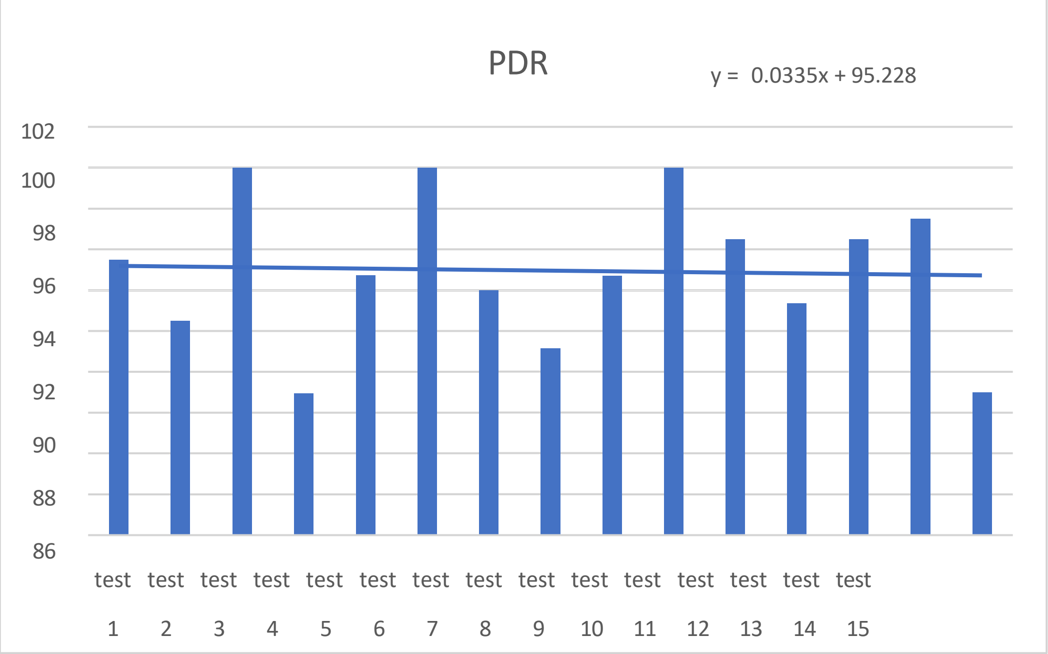

Fig3: Throughput at proposed Network (Number of tests 15)

It seems that a series of network tests have been conducted with various test conditions, and the results have been recorded for packet transmission, packet drops, PDR (Packet Delivery Ratio), E2E (End-to-End) delay, and throughput. In terms of packet transmission, the number of packets transmitted ranged from 150 to 210 in the 15 tests conducted. The number of packet drops varied from 0 to 23.1, indicating that some tests were able to successfully deliver all packets while others suffered from Significance packet loss. The PDR (Packet Delivery Ratio) results show that most tests achieved a PDR of over 90%, indicating that the majority of packets were successfully delivered. However, there were a few tests (Test 3 and Test 13) that had very low PDRs, which suggests that there were signifit issues with packet delivery in those tests. The E2E delay results indicate that the tests generally had low delays, ranging from 0.04 to 0.13. This suggests that the network was able to quickly deliver packets in most cases. Finally, the throughput results show that there was a Significance range in throughput, with values ranging from 1346.9 to 3587.8. This suggests that the network had widely varying performance depending on the specific test conditions. These results suggest that there were Significance variations in the performance of the network depending on the specific test conditions, with some tests achieving much better results than others.

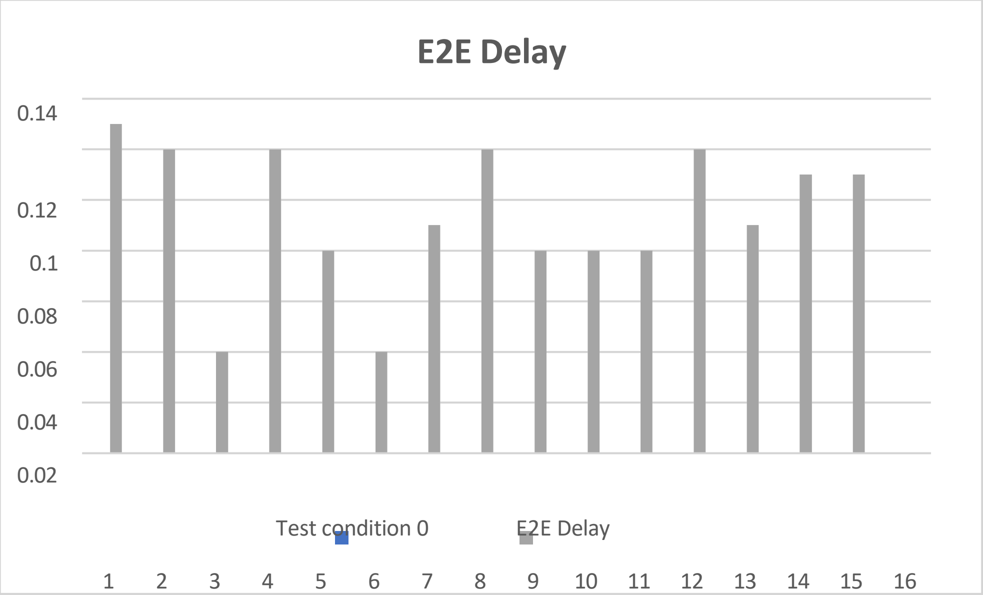

Fig4: E2E Delay at proposed Network (Number of tests 15)

The E2E delay is the time it takes for a packet to travel from the source to the destination, including all intermediate hops. Based on the table, we see that the E2E delay varies between different tests. Some tests had a relatively lower E2E delay, such as Test 3 and Test 6, which had an E2E delay of only 0.04 seconds, while others had a slightly higher E2E delay, such as Test 1 and Test 4, with an E2E delay of 0.13 seconds. It's important to note that a lower E2E delay indicates that the network is performing well and that the packets are being transmitted quickly from the source to the destination, while a higher E2E delay indicates that there may be issues with the network's performance, such as congestion or network latency. However, it's important to note that the E2E delay alone is not enough to evaluate network performance fully. We need additional information, such as the number of packets transmitted, the packet drops rate, throughput, and PDR, among others, to provide a more comprehensive analysis of the network's performance. Without this information, we not evaluate the network's performance accurately or identify areas for improvement.

Result come out by HN based MANET

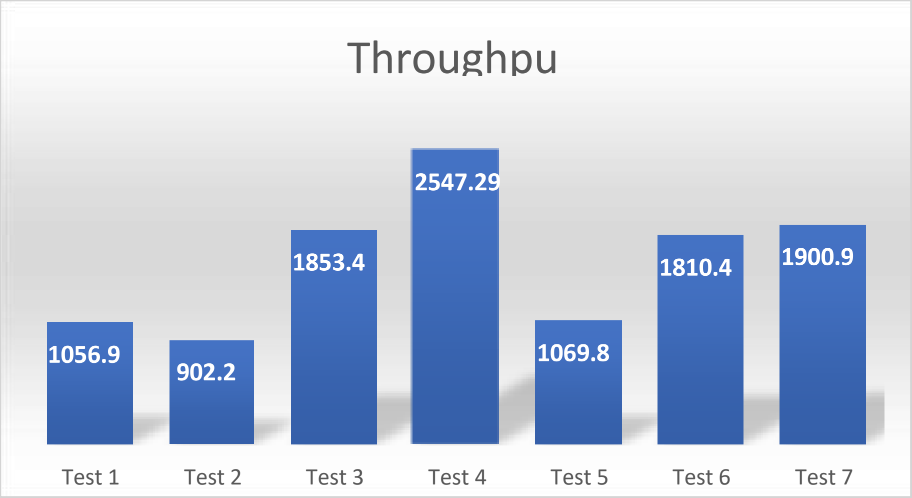

Fig 6: Throughput of MANET network

The above result come out after the end of simulation. The throughput of the network has been evaluated in 7-different attempts of test performed through the same click of the proposed GUI. A found that the throughput varies from 902 to 2547. The huge variation of throughput is due to neural network randomness and generation of initial count of packets for the communication.

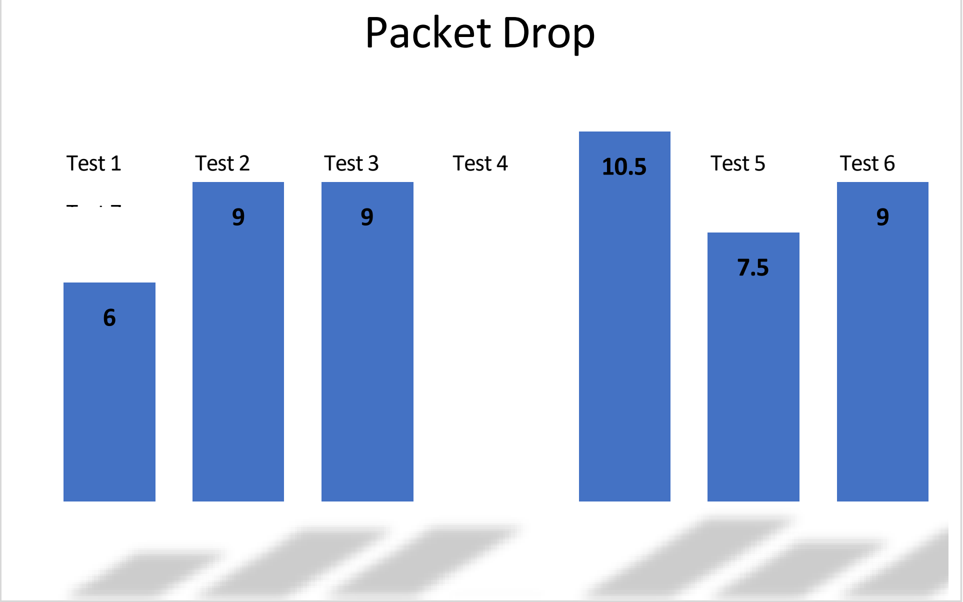

Fig 7: Packet loss of MANET network

Comparison With Existing

Table 2: Result come out by neural network

Test Condition	Packet Transmitted	Packet Drop	PDR	E2Edelay	Through Put
Test 1	170.0	6.0	100.0	0.2	1057.0
Test 2	170.0	9.0	99.9	0.2	902.2
Test 3	210.0	9.0	100.0	0.1	1853.5
Test 4	150.0	0.0	100.0	0.1	2547.3
Test 5	170.0	10.5	99.9	0.2	1069.8
Test 6	200.0	7.5	100.0	0.1	1810.5
Test 7	210.0	9.0	100.0	0.1	1900.9

The results of several tests conducted on a network using a neural network model. The table shows the following test conditions:

- **Packet Transmitted:** The number of packets sent during the test
- **Packet Drop:** The number of packets that were dropped during the test
- **PDR:** Packet Delivery Ratio, which is the percentage of packets that were successfully delivered during the test
- **E2Edelay:** End-to-End delay, which is the time taken for a packet to travel from the source to the destination
- **Throughput:** The rate of successful data transfer over the network during the test.

Based on the simulative analysis, it appears that the neural network model performed well in maintaining a high Packet Delivery Ratio, with all tests achieving over 99.9% success rate. However, there were some instances of packet drops during the tests, which could indicate potential issues with the network. The Endto-End delay and Throughput also varied across the different tests, indicating that the performance of the network may be impacted by various factors such as the number of packets being transmitted and the amount of network congestion. Further analysis would be required to identify any underlying patterns or trends in the data.

Table 3: Result come out by earlier base algorithm (without neural network)

Test Condition	Packet Transmitted	Packet Drop	PDR	E2Edelay	Through Put
Test 1	190.0	24.0	99.9	0.2	1194.4
Test 2	200.0	15.0	99.9	0.1	1784.7
Test 3	150.0	0.0	100.0	0.1	2641.0
Test 4	180.0	9.0	100.0	0.1	1623.7
Test 5	190.0	30.5	99.8	0.2	1195.2
Test 6	190.0	18.5	99.9	0.2	1173.9
Test 7	180.0	9.0	100.0	0.1	1552.9

These are test results for a network performance evaluation. Here are the definitions of the abbreviations used in the table:

- **Packet Transmitted:** The number of packets sent during the test.
- **Packet Drop:** The number of packets that were lost during transmission.
- **PDR:** Packet Delivery Ratio, which is the percentage of packets that were successfully delivered. It is calculated as (Packet Transmitted - Packet Drop) / Packet Transmitted * 100.
- **E2Edelay**: End-to-end delay, which is the time it takes for a packet to be transmitted from the sender to the receiver and back again. It is measured in seconds.
- **Throughput:** The amount of data that be transmitted over a network in a given amount of time. It is usually measured in bits per second (bps) or bytes per second (Bps).

Based on the table, we see that all of the tests had a high PDR (above 99.8%), which indicates that the majority of packets were successfully delivered. The E2Edelay was also relatively low, ranging from 0.1 to 0.2 seconds, which suggests that the network had low latency. The throughput varied across the tests, with Test 3 having the highest throughput of 2641.0 Bps and Test 1 having the lowest throughput of 1194.4 Bps. However, it's important to note that the throughput is influenced by factors such as the size of the packets being transmitted and the available bandwidth, so it's difficult to draw conclusions without additional context. Additionally, we don't have information on what type of network or application was being tested, or what criteria were being used to evaluate the network's performance. Therefore, it's hard to determine whether these results are good or bad without more information. The results of several tests conducted on a network using an earlier base algorithm (without neural network). Similar to the table for the neural network results, this table shows the following test conditions:

- Packet Transmitted: The number of packets sent during the test
- Packet Drop: The number of packets that were dropped during the test
- PDR: Packet Delivery Ratio, which is the percentage of packets that were successfully delivered during the test
- E2Edelay: End-to-End delay, which is the time taken for a packet to travel from the source to the destination
- Throughput: The rate of successful data transfer over the network during the test.

Comparative Analysis

Comparing these results with the neural network results, it appears that the base algorithm achieved similar or slightly lower Packet Delivery Ratios across the tests. However, the base algorithm had more instances of packet drops, indicating that the neural network model may be better at preventing packet drops. The Endto-End delay and Throughput values also varied across the different tests, similar to the neural network results, indicating that the performance of the network may be impacted by various factors such as the number of packets being transmitted and the amount of network congestion.

Overall, it appears that the neural network model may provide some improvements over the base algorithm in terms of preventing packet drops. However, further analysis would be required to compare the performance of the two models across a wider range of test conditions and to identify any underlying patterns or trends in the data.

Validation of work

Author Techni	**que Used Area of**	**research**	**Result**
Sharma & Lobiyal (2015)	AODV, DSR and TORA	MANET performance	of AODV, DSR and TORA protocols
Roy et. al. (2020)	block-basedrouting protocol	MANET	Suggested routing algorithm, focused on residential positions, ensures that all data in the cluster is propagated to MS using the minimum hop route to minimize the data simulation results gap, including overall network output, which depends mostly on a number of dead nodes, total power consumption, community header settings and performance.
Rai et al. (2017)	Quality of Services (QoS) For Wireless Sensor Network	MANET Suggested	routing methodology, focusing on residential placements, guarantees that all cluster data is propagated to MS using the least hop path to minimise data
		simulation output	gap, including overall network output, largely dependent on a number of dead nodes, total power consumption, community header settings and performance.
Fotohi & Bari (2020).	filtering algorithm based on Firefly, and the neural network of Hopfield (MANET -FAHN)	MANET Simulation	results reveal the superiority of the MANET -FAHN methodology for current efficiency metrics such as packet distribution rate (PDR), average throughput, detection rate and life.
Liu (2017) utilizing	the Deep Q Network augmented learning system (DQMC),	Wireless Multimedia Sensor Networks (WMSN)	Include progressive machine learning approach in multichannel personalization process.

The ability to detect intrusion is a core feature of all sensor network solutions. Because of the unique characteristics of sensor networks, they not be exploited for typical network protection. To begin with, sensors are sensitive to manufacturing costs since they need a high number of sensors. Sensor networks, on the other hand, need a low manufacturing cost. As a consequence, sensor nodes are primarily concerned with power, memory, and computation/processing. Sensor nodes are often powered by batteries and must be replaced on a regular basis. For most sensor network protocols, taking into account network energy use becomes a must. Second, sensor nodes are susceptible to physical attacks from enemies who may be stationed in public places.

Conclusion

In conclusion, the detection of malicious attacks and their preventive measures in MANET through Neural Network and AODV is a Significance research area with the potential to enhance the security and reliability of mobile ad hoc networks. By leveraging the capabilities of Neural Networks for attack detection and classification, and integrating them with the AODV routing protocol, researchers aim to develop a robust and proactive defense mechanism against various types of malicious attacks. Through a systematic methodology involving problem identification, literature review, data collection, Neural Network model design, training and testing, integration with AODV, simulation or experimentation, and analysis, researchers gain valuable insights into the effectiveness of this combined approach. The findings from such research efforts provide valuable contributions to the field of MANET security, offering insights into the accuracy and efficiency of the Neural Network and AODV combination in detecting and preventing malicious attacks. These findings guide the development of improved security mechanisms and protocols, ultimately enhancing the overall performance, reliability, and trustworthiness of MANETs. Overall, the exploration of malicious attacks and their preventive measures in MANET through Neural Network and AODV holds great Significance in addressing the security challenges faced by mobile ad hoc networks and promoting their secure and reliable operation in diverse real-world scenarios.

Reference

Basarabă, R. C. (2021). Investigating safety and security interactions using the BDMP formalism: case study of a DDoS attack on Liberia (Bachelor's thesis, University of Twente).

Brindha, N. V., & Meenakshi, V. S. (2022). A secured optimised AOMDV routing protocol in MANET using lightweight continuous multimodal biometric authentication. Journal of Ambient Intelligence and Humanized Computing, 1-17.

Dupak, L., & Banerjee, S. (2022). Hybrid trust and weight evaluation-based trust assessment using ECKANFIS and AOMDV-REPO-based optimal routing in MANET environment. The Journal of Supercomputing, 1-21.

Gaber, M. M., & Azer, M. A. (2022, May). Blackhole Attack effect on MANETs' Performance. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 397-401). IEEE.

Gautam, A., & Mahajan, R. (2022). Computational Intelligence Techniques for Optimization in Networks. Smart and Sustainable Approaches for Optimizing Performance of Wireless Networks: Real-time Applications, 201-215.

Gautam, A., Mahajan, R., & Zafar, S. (2022). Big Data Analytics for MANET Based Sustainable Smart Healthcare Solution. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 15(4), 601-610.

Kaushik, S., Tripathi, K., Gupta, R., & Mahajan, P. (2022, February). Performance Analysis of AODV and SAODV Routing Protocol using SVM against Black Hole Attack. In 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM) (Vol. 2, pp. 455-459). IEEE.

Machado de Sousa, E., & Shahzad, A. (2021). Data Loss Prevention from a Malicious Insider.

Journal of Computer Information Systems, 1-11.

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Dynamic user-centric access control for detection of ransomware attacks. Computers & Security, 111, 102461.

Raja, L., & Periasamy, P. S. (2022). A Trusted Distributed Routing Scheme for Wireless Sensor Networks Using Block Chain and Jelly Fish Search Optimizer Based Deep Generative Adversarial Neural Network (Deep-GANN) Technique. Wireless Personal Communications, 1-28.

Rani, K. S. K., & Vijayalakshmi, R. (2021, May). Experimental Evaluations of Malicious Node Detection on Wireless Sensor Network Environment. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 185-191). IEEE.

Sonekar, S. V., Pal, M., Tote, M., Sawwashere, S., & Zunke, S. (2021). Enhanced route optimization technique and design of threshold-T for malicious node detection in ad hoc networks. International Journal of Information Technology, 13(3), 857-863.

Suganya, A., Kumar, S. M., & Vigneshwari, A. G. (2021). A Study on Discovering Malicious Nodes on MANET through Secure Intrusion Detection. Annals of the Romanian Society for Cell Biology, 2444-2452.

Sureka, N., & Gunaseelan, K. (2021). Investigations on detection and prevention of primary user emulation attack in cognitive radio networks using extreme machine learning algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-10.

Vennam, P., TC, P., BM, T., Kim, Y. G., & BN, P. K. (2021). Attacks and Preventive Measures on Video Surveillance Systems: A Review. Applied Sciences, 11(12), 5571.

Wang, Y., Ishii, H., Bonnet, F., & Défago, X. (2020). Resilient consensus against epidemic malicious attacks. arXiv preprint arXiv:2012.13757.