https://doi.org/10.48047/AFJBS.6.5.2024.10592-10603

African Journal of Biological Sciences

Hybrid Secure Clustering Multi-Threat Prevention Mitigation Technique for Intrusion Detection in Manet

Ms. Jasdeep Kaur [1*] and Prof. Vijay Dhir [2]

[1] Research Scholar, Department of Computer Applications, Sant Baba Bhag Singh University, Jalandhar, Punjab 144030, India, jasdeep.edu@gmail.com ,

[2] Professor, Department of Computer Science and Engineering, Sant Baba Bhag Singh University, Jalandhar, Punjab 144030, India, drvijaydhir@gmail.com

Article History

Volume 6, Issue 5, 2024
Received: 22 May 2024
Accepted: 03Jun 2024
doi:*10.48047/AFJBS.6.5.2024.10592-10603*

Abstract:

MANETs are more exposed to intrusion vulnerabilities as compared to wired networks depending on factors such as dynamic network architecture, mobility of nodes, a compromised operating environment, and various additional other elements. MANET can be safeguarded via data encryption, reliable routing algorithms, intrusion detection systems (IDS), or a mixture of these technologies. Although there are many different routing protocols readily available that enhance network acceleration, only a few of them target security-related issues. This research proposes an I-AODV routing protocol for routing the data that implementing K-means. The whale optimization approach with artificial neural network has been employed in preventing launched attacks called "Hybrid Secure Clustering Multi-Threat Prevention and Mitigation technique (HSCMM)". This approach can identify threat such as black holes, flooding, and selective packet dropping. The Proposed method generates Throughput 12730, E2E delay 0.018 to 0.5, packet dropping rate 0% to 3%, and PDR 97% to 100%.

Keywords: Intrusion Detection System, AODV, WOA, Artificial Neural Network, Black Hole Attack.

1. Introduction

Since the mobile nodes in a MANET create temporary pathways for packet transmission among themselves, it is known as an infrastructure-less system. In a MANET, nodes could communicate explicitly with each other. when the nodes are located outside of each other's reach, but within the wireless connectivity ranges of each other must rely on nodes to relay messages.

Security in MANET is the main critical agreement against the essential usefulness of the system. To defend MANET from assault, a few sorts of authentication schemes must be developed. Therefore, in the past decade, scholars have started working to create additional security methods or adapt existing ones could be used with MANETs [1]. The safety objectives of MANET, namely Confidentiality, Integrity, Availability, Authenticity, are the same as those of other systems. Intrusion detection is required as an additional barrier to safeguard computer devices. IDS has been recognized as a vital element of defensive security measures since it preserves networks and computer systems against malicious activities [2]. Analyzing systems or networks for unauthorized entry, action, or file alteration is a technique of intrusion prevention.

Intrusion detection systems are invented to recognize prohibited attempts to exploit networks of computers for illicit uses of resources to be safeguarded in a target network, which included system kernels, user accounts, file systems, etc.

For secure information delivery, MANET transmission security is essential. MANET is highly susceptible to digital/cyberattacks than a wired connection because it has an inadequate centrally coordinated response as well as a shared wireless channel. Attacks can be categorized based on their point of origin, whether internal or external or their mode of operation, whether passive or active. IPS in MANETs is used to minimize the probability of assaults and respond with real-time automated security against known threats is the top priority. For effective network functionality, you need to respond quickly to intrusions and when manual observation and intervention are restricted. To provide a layered security strategy within a MANET, a mix of both IDS and IPS can be used, with IDS offering monitoring and detection abilities and IPS offering immediate threat prevention. Such an approach could help in attaining an equilibrium between network performance and security. The current research work aims to develop an intrusion detection system for MANETs.The system's purpose is to examine & mitigate the consequences of separate attacks on the system. The system then assesses every attack's impact on network performance. This technique used ANN-based IDS systems to identify attacks by studying and imitating typical network behavior and discovering deviations from it. Conventional IDS systems are prone to problems recognizing new or quickly evolving attacks. This research article is organized into six sections. Section 1 discusses the significance of security in a mobile ad hoc network. Section 2 represents a review of the literature. Section 3 discusses the suggested I-AODV and IDS approach that adopt WOA and ANN. Section 4 describes the simulation findings and various parameters. Section 5 Comparative analysis and Section 6 wrap up the paper.

2. Literature survey

Umar et al. (2018) propose enhanced CBDS, a method that adds an RSA public key cryptosystem.With a current CBDS, for mitigating and minimizing allied gray hole and black hole assaults in mobile ad-hoc networks. That used network simulator version 2 and an analogous system was built with 50 connected devices where some devices serve as black hole intruders and snoopers, much like CBDS. User Datagram Protocol (UDP) was utilized to simulate the source and target links. With the aid of CBR, traffic was generated utilizing ongoing packets over the UDP link. [3]

Aliady et al. (2019) developed a potential energy-saving secure method relying on network connectivity preventing the wormhole attack using Network Simulator 3 and applied it to the AODV routing approach. Only when a wormhole attack is prevented and uses a tunnel for four or even more hop does this technique focus on energy consumption, and the node remains static during the transmission, which is impossible in MANETs.[4]

Khan et al. (2018) A MAC authentication structure that relies on a light-weight encryption approach is described to protect against black hole and DDoS attacks. NS2 evaluates the proposed approach, and the findings demonstrate that it provides quick route evaluation with increased throughput while lowering the routing overhead & preventing BH assaults, but only avoids the black hole attack.[5]

Neeraj et al. (2018) showcase their ideas for the application of the aforementioned principles for altering the number of hubs in two different ranges (placing the hubs in an irregular shape) in a variety of specifically

constructed platforms (MANETs). The NS-2 test apparatus is used to perform several replications by the authors. The study discovered that although throughput and E2E delay vary in two separate reaches as the number of hubs rises, standardized steering load, parcel thickness division, and energy used stay constant.[6]
Ankome et al. (2021) presented a hierarchical cooperative intrusion detection system for MANET. Using NS 2.35, HCIDM was programmed. 50 regular MN and 5 BH nodes migrated dynamically within a framework of 4000 square meters as an element of the simulation. Throughput, packet drop and PDR are used as measures to assess the HCIDM's efficiency. The bandwidth attained by HCIDM may be the reason why the system with HCIDM had an average packet loss of 26.92 compared to CCIDM's median of 19.85. During a black hole attack, the network's average total throughput with HCIDM is 23.23 Mbps.[7]

RashmiandSeehra. (2014) discussed the MANET and its security threats and proposed a clustering approach in AODV (Adaptive on Demand Protocol) routing protocols for diagnosis and mitigation over BH attacks for MANET based on PDR, detection rate and throughput. In this approach, every node within the cluster will ping once to the cluster's prime node and detect deviations between no. of packets sent and no. of packets obtained in the system to diagnose the misbehaving node. For simulation of the outcomes, the author used NS2. This approach, is compared with the modified DSR (Dynamic Source Routing) protocol approach and the detection rate is higher in the proposed approach.[8]

Ansari and Waheed. (2017) describes about flooding attack, which is a kind of DDOS attack and a major threat to the MANET Security. They presented a novel cross-layer mechanism for the detection of flooding attack where nodes in MAC (media access control) layer analyze the noise signal properties and list them into routing tables by MAC layer/network interface and marked the flooding node as malicious. The malicious node was blacklisted in the routing table. This approach, yields optimal results where SNR (signal noise ratio) is high, but performance degrades where SNR was low.[10]

Sumit et al. (2014) employed a clustering method to distinguish between invasive or typical behavior on the nodes. This approach, which was inspired by k-means clustering, was given the term efficient k-means clustering. They suggested installing an IDS on each MANET node that used the ZRP for packet flow. They then separated the malicious nodes from the system using efficient k-means. As a result, the Ad-Hoc system was free of any malicious behavior, packets can transit normally; however, the cost may rise as the amount of nodes rises.[11]

Abdelhaq et al. (2011) For the purpose of detecting BH Attacks through the AODV routing protocol in MANETs, a Local Intrusion Detection security routing method has been developed. Rather than performing ID via the source node, like in the SID security routing method, the ID detection is performed directly using the prior node of the malicious nodes in LID security routing method. The security protocol overhead was decreased by using LID security route. The E2E delay & routing overhead was reduced completely as well as the ratio of throughput enhancement provided by the LID protected routing technique was simulated using the GloMoSim simulator. If the attacker's prior node's link is broken, this approach would be useless.[12]

Indirani et al. (2014) suggested a decentralized MANET intrusion detection system that is effective and based on swarms. Swarm agents were employed in this method to choose the nodes that had the greatest trust values, energy and unlimited bandwidth for active nodes. The trust value of all the detected nodes is assigned to all nodes currently active and keeps track of its nearby neighbors within its range. Depending on the trust levels, the operational nodes adjust. On the other side, if an operational node discovers any network node that is less than a minimum trust threshold during the related exchange of the identified trust values of the nodes among the nodes currently active, the node is flagged as malicious. A defending strategy is used to remove the malignant node in the network when the source obtains an alarm signal about it. Focusing on the use of energy, throughput, packet delivery ratio, and dropped packets this method is compared to Digital Telephony Using Goertzel Algorithm (DTMF). They demonstrated through simulation results how effective the suggested technique is as a MANET intrusion detection tool. The packet drop ratio rises linearly with network growth. [13]

Zant and Yasin. (2019) outlined the various flooding attack types and proposed improved AODV protocols called AIF AODV that rely on two algorithms to recognize and avoid flooding attacks. Both algorithms has been applied to avoid flooding attacks and identify attacker nodes from the network. When compared to standard ADOV protocols, the proposed AIF AODV turns out better than average when it comes to of

residual energy, Throughput, PDR, Normalized Routing & End-to-End Delay. The simulation of the findings was done using the load under the low mobility scenario of NS 2.35.[14]
Sivanesh and Dhulipala. (2020) presented as an intrusion detection system named Accurate and Cognitive Intrusion Detection System (ACID) for the network's black hole attack detection. The recommended mechanism has been evaluated against standard AODV routing protocols and outperformed AODV on the basis of PDR and Throughput. It simply addresses packet loss only. NS 2 simulator was used to simulate outcomes.[15]

Ashutosh Vashist, Dr. Rajinder Singh Sodhi (2023) investigated attacks that are malicious in MANETs through a mixed approach comprising a Neural Network and the Ad hoc On-Demand Distance Vector (AODV) routing protocol. The trained Neural Network model will be incorporated into the AODV routing protocol to further enhance its immediate identification and protection of harmful threats. To measure the efficiency of the entire system, simulations and tests are carried out. To test the accuracy and efficacy of prevention and identification procedures, many scenarios involving various sorts of assaults are put together. Performance indicators are detection accuracy, network throughput and false positive rate are gathered and analyzed. As the network grows in size the packet drop ratio also rise and there is a fall in packet delivery ratio.[18]

Mohamad T Sultan et, al (2023) The primary objective of the research experiment is is to analyze, and employing machine learning artificial neural networks (ANNs), develop an intrusion detection determining Technique to implement ad hoc networks on mobile devices. An evaluation utilizing simulation and a structure of deep ANNs for identifying and restricting a Denial-of-Service attack are being addressed. in order that will enhance the general degree of security for Mobile ad hoc networks. It detects only DDos Attack and few parameters are tested as the no. of connection increases the performance of proposed technique decreases.[19]

A. S. Q. Syed et. Al (2024), discuss about the improvements to security for mobile ad hoc networks (MANETs). RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography) are commonly employed for security and mentioned about their limitations. They suggested Chaos algorithms facilitate swifter validation and provide protection from the false behaviour black hole attacks but this technique only works for authentication for black hole attack other types of attacks and various performance parameters were ignored. [24]

3.Methodology

In this research, an improved AODV routing using K-meansand for IDS WOA & ANN is employed for MANET named “Hybrid Secure Clustering Multi Threat Prevention Mitigation” (HSCMM). WOA and ANN are utilized with I-AODV protocols for optimal performance of the parameters while K means is employed for cluster formation.ANNs are implemented by this method to categorize the attacks. Matlab 2016a was used to simulate each and every intrusion detection system that is shown here [20]. Three steps constitute the algorithm's process: (A) Formation of clusters and slection of Cluster head (B) I-AODV used for route creation. (C) Identification and mitigation of Flooding attack, selective packet drop and Black hole attack.
The otherphase uses the WOA to train the ANN to recognize differences between attacks and normal network phenomena. Under the suggested WOA-ANN approach, every search agent is set up to maximize the ability of the neural network. Vectors of the biased and weighted parameters found in an MLP (Multi Layer Perception) network show the connections between different layers that are input, hidden and output layer.

3.1 Whale Optimization approach (WOA)

The Whale Optimization Technique (WOA), an optimization technique that mimics how humpback whales hunt and fight utilizing bubble net, in order to model their hunting behavior [7]. The three major components of the WOA method are roundup, net bubble attack, & prey search. By shifting its location vector, the whale in this method hunts in a single or multidimensional space. The variables for solving the issues are represented by the position or evaluation of the candidate answer along with the whale itself, which stands in for the solution space. WOA developed a helix mechanism to direct individuals in seeking an optimal solution to the problem.The whale optimization algorithm can yield better outcomes in the environment of moving devices, to discovering the position of every node in the MANET and to determine the optimal and appropriate path for data delivery.
There are three phases to the WOA algorithm:
1)Searching and encircling the Prey

2) Spiral upgrading position: A novel spot that is compatible with the spinning motion can be obtained by applying the spiral-based updating position procedure

3. Look for prey: While other whales will move to their most advantageous individual places to attain balance, the current community of whales will be picked at random as the existing optimal choice for the entire population.

Each individual whale in the WOA technique begins at a random location and then moves in accordance with either when specific whale position was ascertained for each and then repeat or each whale that was randomly

Fitness Function (FF)

Fitness function is utilized for the detection of attacks, whose value depends upon the average value. The average value will be calculated automatically depending upon the number of nodes entered. In WOA, FF is essential for the best solution and it is calculated as;

$$f(x_{1,}\ldots.. ,x_n) = \sum_{i=1}^{n} x^2 \qquad (1)$$

where n=size of Population, i= no. of iterations, x=Position of vectors of the best Solution and f(X)= Best Solution.The value of the fitness function is (0,0) as the key objective of the WOA is to reduce the FF for better optimization [21].

Here we use 100 search agents (Whales) and 0 lower bound and 1000 upper bound with Dim 100 and maximum number of iterations are 100.

3.2 Artificial Neural Network

Artificial neural networks (ANNs), essentially imitate the framework of the human brain, comprise a set of input, hidden, and output layers with interconnected neurons (nodes). It presented an important capacity to predict engineering application performance and undertake challenging, linear, and nonlinear work. ANN designs, comprising GRNN, RBF, and MLP, have been extensively used in various applications. ANN combines backpropagation (BP) with a Levenberg-Marquardt (LM) training algorithm. The currently operational nodes evaluate the incoming nodes and deliver input signals to them. ANNs are complex interaction-based nonlinear classification designs. A physical cellular network that can gather, store, and apply experimental information is called artificial neural network (ANN). ANNs might be programmed to recognize and classify objects intricate patterns because they are modelled after the framework and functions of neurons in the human brain as shown in figure 1.

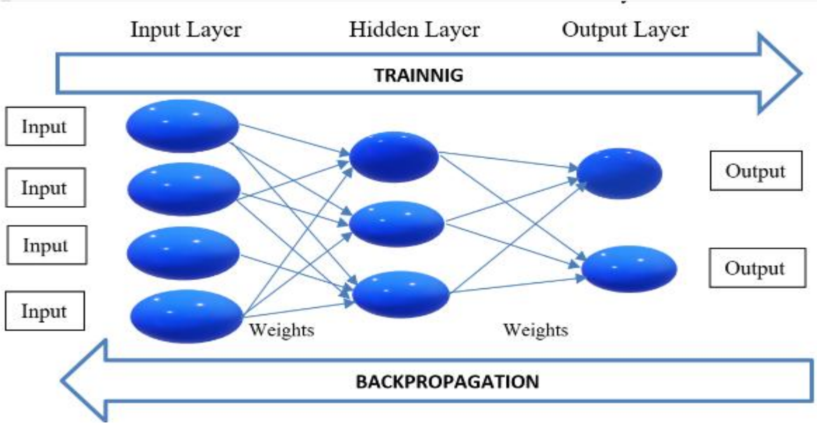

Fig 1: ANN Structure

The idea of improving a reactive protocol for routing is came up withMANET-based IDS (HSCMM) to provide a path for data packet's transmission.In this research experiment, the main objective is to develop a better routing algorithm for IDS to identify and mitigate the attacks by combining the idea of K-means with WOA and ANN. In order to distinguish it from other or solely AODV routing mechanisms, it is termed to as a I-AODV routing protocol. We required a network simulator, in order to simulate and evaluate the suggested model. We employ the Graphical User Interface (GUI) idea in the MATLAB 2016 a programme with the I-AODV routing mechanism to develop this simulator where Training Rate is 70%, Value Rate is 15% and Test Rate is 15%. Here, we use the network height and breadth in accordance with the supplied equation to simulate the suggested MANET-based IDS model on an area of 1000m^2:

$$\mathbf{Area\ of\ IDS, A_{IDS} = H_{IDS}\ X\ W_{IDS}}$$

Where, H_{IDS} → Height of the MANET-based IDS Simulator and

W_{IDS}→ Width is the MANET-based IDS Simulator

Deployment of mobile sensor nodes in IDS Simulator, total 100 nodes has been set up within the area of simulator and all nodes assign a unique ID such as N_1, N_2, N_3….N_N. Here, nodes deployment is based on the random mechanism with the range of 0 to 1000m^2 equal to the area of simulator.

After that, nodes have been organized into clusters using the concept of K-means as a clustering mechanism and in accordance with the likelihood that there are live nodes within the network at the initialization, clusters are formed. Clusters having a cluster head with same color and their names are CH1, CH2…CHn. All CHs are responsible to receive and monitor the nodes within region and then assist with the creation of a route from T_X-Node to R_X-Node via Base Station and CHs. So, after that, we deploy a base station (BS) at the center of network having coordinates x=500 and y=500 interconnected to every CH within the network to keep track while receiving data packets from CHs or nodes.Then, we assign a node as source (T_X-Node) and a node as destination node (R_X-Node).

Once the route discovery is completed, the data packets have been sent across CH and BS from TX to RX node the fundamental setup and nodes are deployed in the MANET-based IDS simulator. The I-AODV route discovery process works by having the TX node send packets of data to the head of the cluster CH, who then chooses which of the node will serve as the next hop or intermediate node as well in the route. The found route is hence termed to as RIDS in the MANET-based IDSbut at this point security is not consider. So, after that the concept of WOA and ANN is employed to recognize the intruder's node based on their characteristics and three types of attacks were considered; flooding attack, Black Hole (BH) attack and Selective Packet Drop (SPD) attack.

3.3 For Detection and Prevention

To detection and prevent the proposed Hybrid Secure clustering multi attack Prevention and Mitigation Method is the combination of WOA and ANN is used along with I-AODV routing protocol. For detection, Whale Optimization Algorithm (WOA) is used on the key idea of consumption of energy. If a node consumes more energy than the average energy, then it is marked as abnormal node. For preventions, the route is havingabnormal nodes will be ignored for data transmission. The algorithm of an intrusion detection WOA-based ANN is written as:

Intrusion Detection WOA-based ANN Algorithm

Input: R_{IDS}←Ideal Route from MD_S to MS_D in MANET-based IDS

Output: OR_{IDS}← Optimize Ideal Route from MD_S to MS_D in MANET-based IDS

```
Start route optimization
To optimized the $R_{IDS}$, WOA-based ANN is used
Index = Using the WOA, locate the RIDS node index.
Apply WOA
If the index of the route is normal then
    O $R_{IDS}$ = $R_{IDS}$ (index)
Else
    Mark as faulty route
End – If
Call and initialize the ANN with the ORIDS properties as the training data (T), the number of nodes as the group (G), and the neurons (N)
Initialize, IDS-Model = NEWFF (T, Group, N)
IDS-Model = TRAIN (IDS-Model, T, G)
Current Sensor Nodes, NC = Properties of current node in MANET-based IDS Model
Characteristics of Sensor Nodes = SIM (IDS-Model, NC)
If Sensor Nodes Characteristics is accurate then
    $OR_{IDS}$ = Validated
Else
    $OR_{IDS}$ = Attacker Nodes
End – If
Returns:RIDS as Ideal and Verified Route with Attacker Nodes from TX to RX.
End – Function
```

4. Results and Discussions

The proposed HSCMM IDS uses random data of nodes in communication toolbox in MATLAB 2016a. Here, a specific area of simulation is considered using height and width of $1000m^2$ in MALTAB environment because it has been highly validated simulation software by the community of networking research, Neural network model and the validated performance as implied in figure 2 and figure 3. We use 10 hidden layers to train weigh and basis and minimum value of MSE (mean square error) will be calculated shown in figure 3. Table1 shows the parameters for simulation needed to simulate a network environment.

Table 1. Simulation Setup and Parameters

Software	MATLAB 2016a
Hardware	Keyword, Mouse, 4GB RAM and minimum 120GB HDD
Number of Nodes	100
Simulation Round	5 to 100
Simulation Time	0,10, 20, 30, 40, 50 secs
Mobility Model	Random
Packet Size	512
No. of Iterations	6
Routing Mechanism	I-AODV with K-means
Attack detection	Artificial Neural Network (ANN) with WOA (whale optimization Algorithm)
Types of Attacks	Flooding Attack, Black Hole Attack and Selective Packet Drop Attack
Parameters	Throughput, Packet Delivery Ratio, End-to-End delay, and Packet Drop Ratio

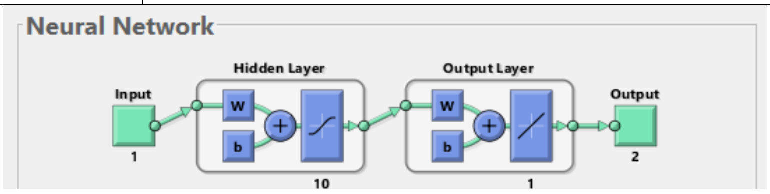

Fig.2: Neural Network

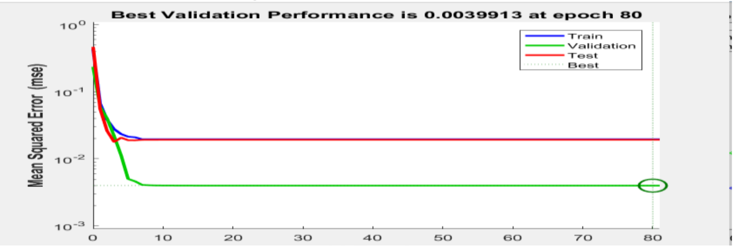

Fig.3: TRAINING, VALIDATION AND TESTING WITH WOA+ANN

4.1 Throughput

Throughput is the rate at which packets are delivered accurately in a given amount of time via the communication connection. Figure 4 comparison of the throughput figures for various methods demonstrates this.

$$T = \frac{P_r/P_s}{T} \tag{2}$$

source delivered the packet Ps, the volume of received packets at the final destination is Pr, and the processing time is T. The protocol performs better when the throughput value is higher. This study compares the throughput of transmitted and discarded packets. Kilobytes per second is used to measure it (Kbps). In other words, the percentage of all packets delivered to total packets arrived at the final destination is known as throughput.

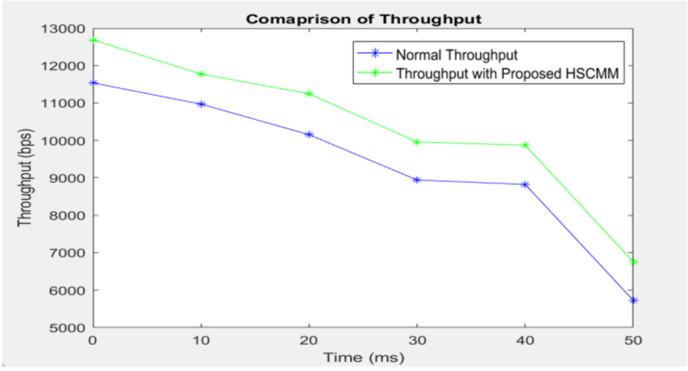

Fig.4: Throughput with and Without Proposed HSCMM

Figure 4 shows the throughput obtained with the same scenario. Throughput is compared with and without Proposed HSCMM. Throughput with the proposed technique range from 6996 to 12730 but Normal throughput without any security measure is significantly lower than the proposed HSCMM.

4.2 End-to-end delay

The time that it requires for a data packet to be transmitted from a source to the final destination via a network is recognized as the delay.

EED= (arrive time − send time) number of connections (3)

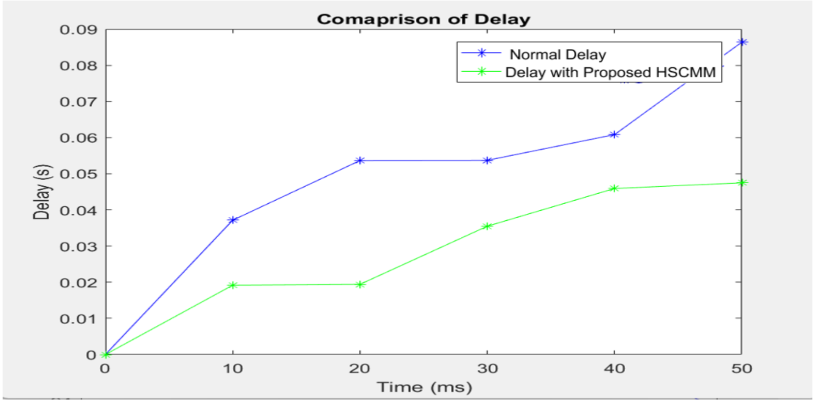

Fig. 5: Delay with and without Proposed HSCMM

Figure 5 shows the Delay obtained with the same scenario. Normal end to end delay is compared with Delay with Proposed HSCMM. Delay with Proposed HSCMM is within the range of 0 and below 0.0417. But Delay without any security measure is above 0.08 which is very much higher as compare to Proposed HSCMM.

4.3 PDR

The quantity of packets that actually make it all from root to the destination is determined by the Packet Delivery Ratio (PDR) inside the network, may be calculated. The comparative analysis of PDR is shown in Figure 6 to demonstrate the comparison.

$$PDR = \frac{No.of\ PacketReceived}{No.of\ Packet\ sent} \quad (4)$$

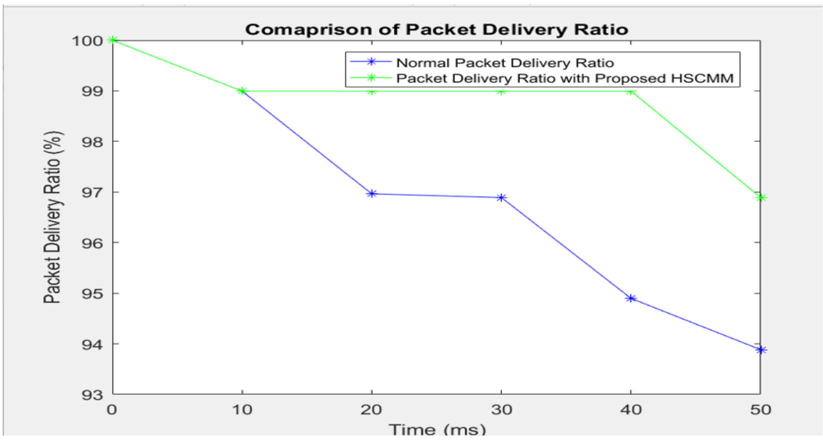

Fig: 6: PDR with and without Proposed HSCMM

Figure 6 illustrated the PDR obtained with the same scenario. PDR with Proposed HSCMM is in comparison with Normal PDR. The proposed HSCMM demonstrate 100% PDR as compared to normal PDR with any security measure.

4.4 Packet Drop Ratio

The percentage of data packets lost while being sent via the network is known as the packet drop ratio.

$$S_N = \sum_{k=1}^{N} a_k \quad (5)$$

For instance, the cumulative sum of the sequence "a, b, c,.." is "a," "a+b," "a+b+c," and so on. In a simulation, the overall node-by-node count for packets lost and the number of dropped packets at the malicious or self-centered node are considered to determine the extent of harm, they do to the present routing protocol.

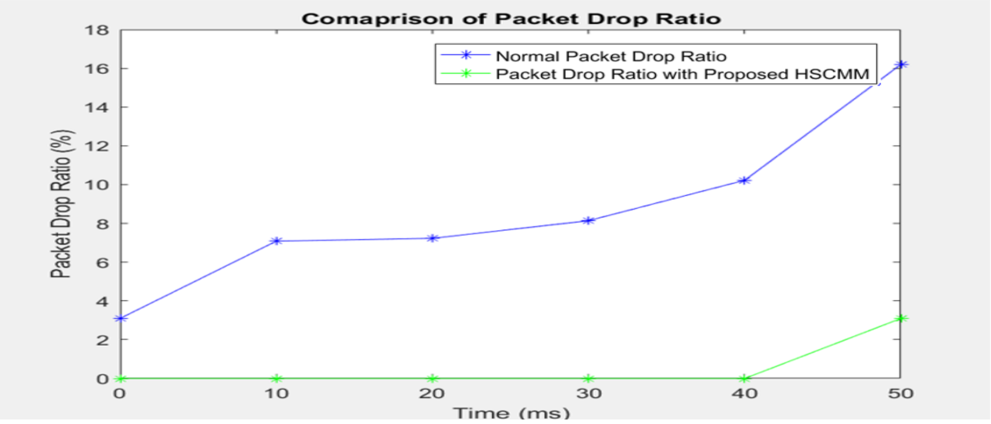

Fig: 7: Packet Drop Ratio with and without Proposed HSCMM

Figure 7 shows the Packet drop ratio obtained with the same scenario. PDR with Proposed HSCMM is compared with Packet drop ratio without Proposed HSCMM. With the Proposed HSCMM Packet Drop Ratio is within the range of 0% to 3%. But Packet drop ratio without any security measure is above 16%.

5.HSCMM is compared to the work proposed by Himani Yadav*, Umesh Lithore and Nitin Agrawal on the basis of simulation time [23].

This section explains the experimental results on the basis of simulation time for these results are analyzed with normal WOA, M-WOA and with proposed HSCMM technique in terms of different QoS parameters i.e., throughput, Packet Drop Ratio, Delay and Packet Delivery Ratio (PDR). In Table 2,3 and 4 the comparative analysis of simulation results of proposed MANET-based IDS simulator (HSCMM) with the combination of WOA and ANN and design an I-AODV routing protocol is compared with WOA and M-WOA_ANN is given.

Table 2: Packet Drop Ratio Comparison

Simulation Time (seconds)	WOA	M-WOA_ANN	HSCM
10	0	42	0
20	84	12	0
30	60	98	0
40	22	70	0
50	72	18	3
60	62	26	5

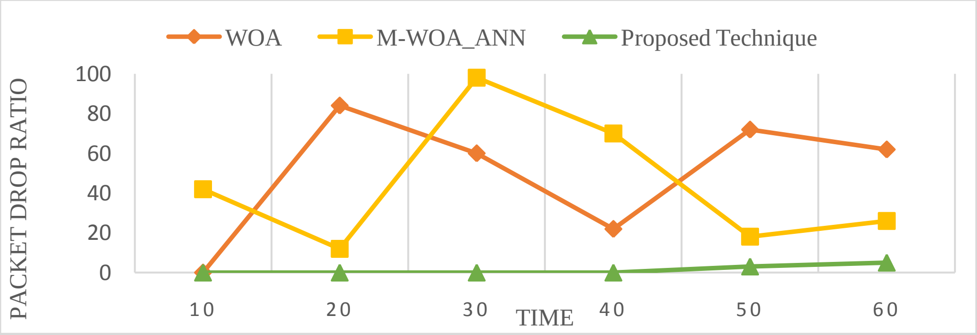

Figure 8: Comparison of Packet Drop Ratio

Figure 8 shows the performance efficiency of three different techniques across various simulation time which demonstrate that in normal WOA Packet Drop Ratio ranges from 0 to 62, in M-WOA_ANN Packet Drop Ratio ranges from 42 to 26 and in proposed HSCMM it ranges from 0 to 5 which is much lower than other two techniques so proposed HSCMM performs better.

Table 3: End to End Delay Comparison

Simulation Time (seconds)	**WOA**	**M-WOA_ANN**	**HSCM**
10	0	1.2	0.018
20	2.26	2.9	0.018
30	3.03	2.6	0.0315
40	2.85	1.22	0.0413
50	2.01	1.79	0.0417
60	2.34	1.77	0.05

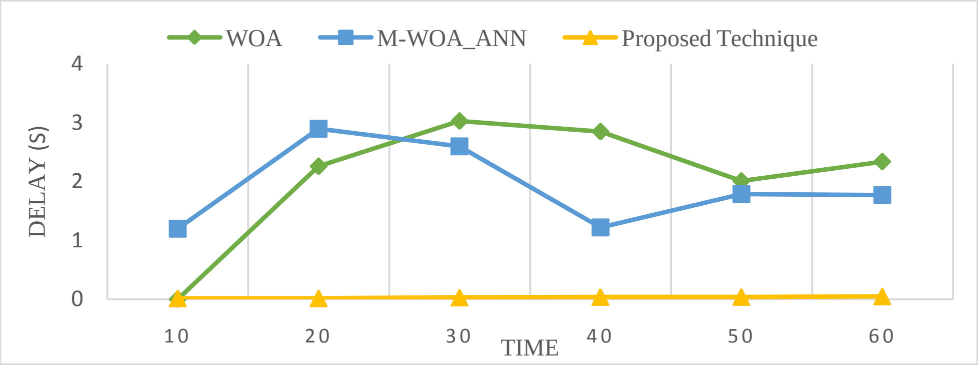

Figure 9: Comparison of Delay

Figure 9 shows the performance efficiency of three different techniques across various simulation time which demonstrate that in normal WOA Delay ranges from 0 to 2.3, in M-WOA_ANN Delay ranges from 1.2 to 1.77 and in proposed HSCMM it ranges from 0.018 to 0.05 which is much lower than other two techniques so proposed HSCMM more efficient than others.

Table 4: Throughput Comparison

Simulation Time (seconds)	**WOA**	**M-WOA_ANN**	**HSCM**
10	0	5875	11815
20	3427	3264	11500
30	3019	3182	10282
40	3182	5548	10000
50	3508	5222	6875
60	3672	3998	6996

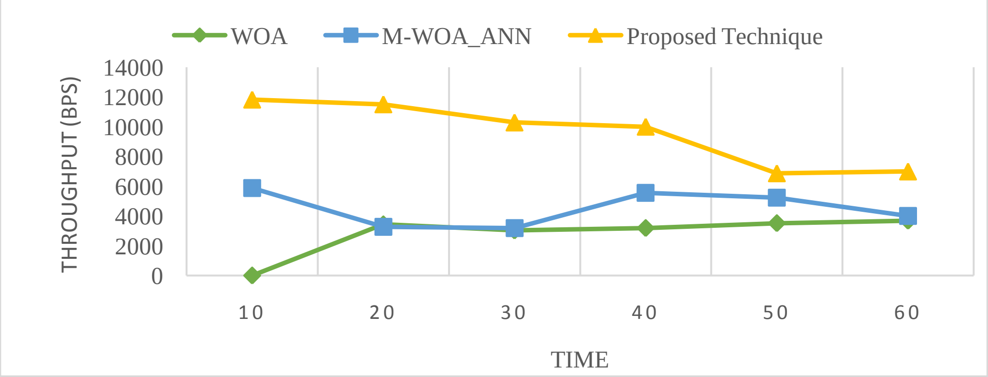

Figure 10: Comparison of Throughput

Figure 10 shows the performance efficiency of three different techniques across various simulation time which demonstrate that in normal WOA, Throughput ranges from 0 to 3672 and performs better at 60 secs, in M-WOA_ANN Throughput ranges from 3182 to 5875 and performs better at10 secs. In proposed HSCMM it ranges from 6875 to 11815 which is significantly higher than other two techniques so proposed HSCMM performs better at 10 secs but it out performs at initial point that is 12730.

6. Conclusion

This research offered an improved AODV routing approach with the whale Optimization Algorithm which is used to create solutions to identify the best possible route from the root terminal to the desired destination node, routing challenges related to bandwidth, throughput, and power consumption has been resolved. ANN is employed to identify attacks for preventing launched assaults using an intrusion detection system. A comparative analysis of the suggested HSCMM technique against conventional WOA and M-WOA_ANN indicates that the proposed technique excels andgenerates higher values. It is the most efficient technique for cyber security. Further investigation and tests could confirm or elaborate on these outcomes by considering other performance parameters which possibly offering helpful information for future development of models and optimization.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Author Contributions

Jasdeep Kaur:The first author drafted the manuscript and contributed to the research work methodology and programming. The second author Prof. Vijay Dhir supervised the entire research work.

RERENCES

[1] Amouri, Amar; Morgera, Salvatore; Bencherif, Mohamed; Manthena, Raju, “A Cross-Layer, Anomaly-Based IDS for WSN and MANET,” Sensors, vol. 18, no. 2, pp. 1-17, doi:10.3390/s18020651

[2] Mafra, P.M.; Fraga, J.S.; Santin, A.O, “Algorithms for a distributed IDS in MANETs,” Journal of Computer and System Sciences, vol. 80, no. 3, pp. 554–570, doi: 10.1016/j.jcss.2013.06.011, .(2014)

[3] Umar, M., Sabo, A., & Tata, A, “Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET”, International Conference on Networking and Network Applications (NaNA), (2018)

[4] Aliady, W. A., & Al-Ahmadi, S., “Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks”, IEEE Access, Vol. 7, pp. 84132–84141. (2019)

[5] Khan, S., Hashim, F., Rasid, M. F. A., & Perumal, T, “Reducing the Severity of Black Hole and DDoS Attacks in MANETs by Modifying AODV Protocol using MAC Authentication and Symmetric Encryption”, 2nd International Conference on Telematics and Future Generation Networks (TAFGEN). (2018)

[6] Neeraj, K., Yedupati, K., SOUMYA, A. S., & KRISHNA, S, “Performance Analysis Of Different Routing Protocols In Manet Using Different Parameters In Different Ranges”, 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2nd International Conference On. (2018)

[7] Ankome, T., & Lusilao Zodi, G.-A., “Hierarchical Cooperative Intrusion Detection Method for MANETs (HCIDM)”, 15th International Conference on Ubiquitous Information Management and Communication (IMCOM). (2021)

[8] Rashmi and AmeetaSeehra ,“ Detection and Prevention of Black-Hole Attack in MANET”, International Journal of Computer Science Trends and Technology(JICT), vol. 2, no. 4. (2014)

[9] Ashok Koujalangi ,“Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocols in MANET(Mobile Ad Hoc Network)”, American Journal of Computer Science and Information Technology, pp 2349-3917. (2018)

[10] Afroze Ansari,Dr.Mohammed Abdul Waheed ,"Flooding Attack Detection and Prevention in MANET Based on Cross layer Link Quality Assessment"International Conference on Intelligent Computing and Control Systems, ICICCS. (2017)

[11] Sumit, S., D. Mitra, and D. Gupta. Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining. IEEE. (2014)

[12] Abdelhaq, M., et al, "A local intrusion detection routing security over MANET network" International Conference on Electrical Engineering and Informatics, IEEE. (2011)

[13] Indirani, G. and K. Selvakumar, "A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)." International Journal of Parallel, Emergent and Distributed Systems. 29(1): Pp. 90-103. (2014)

[14] Mahmoud AbuZantandAdwanYasin,, "Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)" Hindawi Security and Communication Networks , Article ID 8249108, Pp.. (2019)

[15] S. Sivanesh and V. R. Sarma Dhulipala, "Accurate and Cognitive Intrusion Detection System (ACIDS): a Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks" Springer Science+Business Media, LLC, part of Springer Nature. ,(2020)

[16] Tamil Selvi, P.; Suresh GhanaDhas, C., "A Novel Algorithm for Enhancement of Energy Efficient Zone Based Routing Protocol for MANET," Mobile Networks and Applications, vol. 24, pp. 307-317. ,(2018)

[17] Veeraiah, N., & Krishna, B. T, "An approach for optimal-secure multi-path routing and intrusion detection in MANET." Evolutionary Intelligence. doi:10.1007/s12065-020-00388-7. (2020)

[18] Ashutosh Vashist, Dr. Rajinder Singh Sodhi "A TECHNIQUES FOR SECURITY IN MANET: A COMBINED APPROACH OF NEURAL NETWORK AND AODV FOR MALICIOUS ATTACK DETECTION AND PREVENTION" Industrial Engineering Journal ISSN: 0970-2555 Volume: 52, Issue 8, No. 1, August: 2023.

[19] Mohamad T Sultan et al " AN INTRUSION DETECTION MECHANISM FOR MANETS BASED ON DEEP LEARNING ARTIFICIAL NEURAL NETWORKS (ANNS)" International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.1, January 2023.

[20] Mathworks®, Matlab® Neural Network & Deep Learning toolboxes. Available: https://uk.mathworks.com/products

[21] Seyed Reza Nabavi "An Optimal Routing Protocol Using Multi-Objective Whale Optimization Algorithm for Wireless Sensor Networks" International Journal of Smart Electrical Engineering, Vol.10, No.2, Spring 2021.

[22] Mahadeva, R., Kumar, M., Gupta, V. et al. Modified Whale Optimization Algorithm based ANN: a novel predictive model for RO desalination plant. Sci Rep 13, 2901 https://doi.org/10.1038/s41598-023-30099-9. (2023).

[23] Himani Yadav*, Umesh Lithore and Nitin Agrawal "An enhancement of whale optimization algorithm using ANN for routing optimization in Ad-hoc network" International Journal of Advanced Technology and Engineering Exploration, Vol 4(36) ISSN (Print): 2394-5443 ISSN (Online): 2394-7454(2017).

[24] A. S. Q. Syed, C. Atheeq, L. Ali, and M. T. Quasim, "A Chaotic Map-based Approach to Reduce Black Hole Attacks and Authentication Computational Time in MANETs", Eng. Technol. Appl. Sci. Res., vol. 14, no. 3, pp. 13909–13915, Jun. 2024.