HPSGNN: A Hybrid of Particle Swarm and Genetic Neural Network System to Defense against Blackhole Attack Targeting MANETs

Tuka Kareem Jebur
Al-Mustansiriyah University, College of Management and Economic, Baghdad, Iraq

Keywords: Particle Swarm Optimization, Blackhole Attack, Mobile Ad-Hoc Networks (MANETs), Clustering.

Abstract: In this paper, propose a Hybrid of Particle Swarm and Genetic Neural Network system to the Defense Against Blackhole attack Targeting MANETs. Detection and Prevention System black hole attack in MANETs for this purpose two-stage applying the first stage using PSO to find an optimal cluster head this reduces power consumption, conjunction, the second stage using the genetic algorithm to find optimal path then used a neural network to detect and prevent malicious node in MANETs network with some criteria nodes. Therefore, by isolated all data forms from the network, the Blackhole node is eliminated.

1 INTRODUCTION

When a router is affected by different causes. The packet drop attack is very difficult to detect and avoid because packets are regularly dropped from the losses network (Vimal Kumar & Kumar, 2015). MANET considers significant kinds in wireless ad hoc network used in many fields but has a challenge such as dynamic topology, no preexisting infrastructure, packet drop, power consume introducible change of device (node) can be moved in any direction another drawbacks security issues (Chaubey, 2015).

There is numerous protection to secure the network from black hole attacks, such as a firewall, to prevent unsafe activities. Such protections do not however guarantee complete network security. The second line of defense is therefore required that will be capable of detecting new vulnerabilities every day (K. Dalasaniya & N. Dutta, 2014).

Several systems have already been built for this purpose, first used method splits the entire network into interconnected structures called clustering the continuous amount of nodes known as the (cluster) CH responsible to aggregate data from the node and send it to another CH or distention node so it reduces cognition and power consume. Hence, when using clustering in MANET reduces power consumption and conjugation and another advantage of the clustering method (N. J. Patel, 2015).

Unique routing protocols are used for this purpose that can specify the route between nodes not within each other's transmission range. particle swarm optimization (PSO) consider one of the types of computer algorithms based on the principle of finding the value of the best solution among the possible solutions to the problem depending on the principle of experimentation and repetition. This algorithm originated on the principle of the presence of a swarm of elements. This squadron is spread in a limited research area in the (problem space) and moves randomly in the region to discover the best of all solution in this region. The larger the number of squadron elements and the smaller the search area, the easier it is to find the perfect solution faster and vice versa (A. Omidvar & K. Mohammadi, 2015) genetic algorithm used in many research to prevention Blackhole the attack, it can be defined as one of the types of research methods can be classified as an evolutionary algorithm .This algorithm uses Darwin's revolutionary technology, which includes inheritance, mutation, cross crossover, and the production of the best solutions by repeating the genetic cycle that is progressively improved after each crossover, As a result of these characteristics, are to find the best solution between several solutions and the production of new solutions have been used to solve some of the problems facing the process of transfer or confidentiality of data in wireless networks. (K. Nikhil, S. Agarwal, and P. Sharma, 2012).

The research paper deliberates the concept of detecting black hole attack and studied some of the major detection methods such as the type of attacks addressed and architecture in MANET. Furthermore, artificial intelligence methodology called Neural network considers an important method that can be used to detect this attack paradigm attempts towards mimic biological neural network structure and functionality. The neuron takes the basic construction block into account; the model includes three easy rules: summing, multiplying, and activation (A. Krenker, J. Bešter, & A. Kos, 2011).

In this type of attack, there are usually two cases in which the data packet is obtained using a malicious node; one where a malicious node uses the routing protocol such as the AODV protocol, to send route reaction control message (RREP) immediately to the source node upon receipt of the route request control node (RREQ). This RREQ overflow causes unnecessary overhead that leads to reduced network performance such as the delivery of packets and latency. The success of the RREQ broadcast will suffer from a hidden node problem. So it drops the data directly. Therefore, the source node became un incapable to send its data to the destination node which disturbs the influence of the network and its connectivity (L. Prajapati & A. S. Tomar, 2015). A method to detect and prevention black hole attacks in MANETs is proposed in this paper.

Moreover, by monitoring their neighbor's actions, the system detects malicious nodes. If a suspicious behavioral anode is found, declare the suspicious node and send a threatening message. By refusing all data forms, the black hole nodes are isolated from the network. In the Network Simulator, MATLAB simulations are performed to test the performance of the technology proposed. The results show that all types of black hole nodes are identified and isolated by a proposed mechanism.

In this paper, focus on security challenges when designing security schemes for MANETs, hence in this work proposed a hybrid of PSO and GNN to defense against Blackhole attack that targeting the MANTs. The rest of the paper is organized in section 2 are provided the relevant research. Section 3 outlines the scheme we are proposing while being discussed in Section 3. 4, results, and desiccations are shown. Last but not least, Section.5 is the conclusion paper.

2 THEORETICAL AND PREVIOUS STUDIES

Generally, the main assumption considered in the MANET is that each node is a trusted node. However, in a real scenario, some unreliable nodes misbehave and launch the attack in a network like Blackhole in which the misbehaving nodes attract all the traffic towards itself by giving false information of having the shortest path towards the destination with a very high destination sequence number. This section discussed different methods to detect or prevent Blackhole attacks.

2.1 MANETs

MANETs have many users in many fields as such as the modern technology revolution and its great development, has a dynamic topology, no need for infrastructure.

On MANETS, PSO and GNN algorithms were suggested, each offering an effective implementation technique. However, several investigators have suggested various approaches to the black hole attacks in MANETs. Most of these methods can be classified into various categories such as the following: In the work of (Omidvar & Mohammadi, 2014) the PSO algorithm has been suggested which use the maximum flow objective to decide best node locations for each network operation step, this method adds some delay in the process time discovery as intermediate nodes, computation time. Presented technique by (Prajapati & Tomar, 2015) this technique is called PSO of the AODV protocol to find a solution for many network attacker nodes. PSO tracks nodes by changing ad hoc values, if the node converges then it switches node value to endless and prevents the node from sending a packet. This method has a drawback such as a delay packed drop. However, the scheme needs to be further analyzed, since values are modified after a specific time period. Therefore, shorter update time requires more overhead processing if accuracy of detection decreases.

In the previous work of (A. Kaur, P. Kaur, & H. Aggarwal, 2017) suggested using GA and PSO for AODV routing protocols to detect the Blackhole in WSN. By using this approach, it reduces power consumption and finds the best bath from the source to the destination suggested used genetic algorithm (R. Garg & V. Mongia, 2018) with one type of routing protocol called AODV for preventing the Blackhole attack these methods need time toward finding intruder node equal 13.2 whether suggestion algorithm takes 0.64 times with 200 node The scheme needs to be further analyzed, since values are modified after a specific time period. So the shorter update period requires more overhead, otherwise the accuracy of detection will be reduced.

The used technique called clustering by Sanjeev et al. (S. Gangwar, K. Kumar & M. Mittal, 2013) to portion network to the region and using AODV to opt node called a cluster head this method reduce power consume in MANETs. (A. Augustine & M. James,2015) present a method to extending and butter performing network lifetime they suggested a method based on ANN to detect the attack and using AODV protocol to find path this method does not prevent attack There is still the question of delay in path exploration. In the work of (V. Kumar,2018) presented a technique based Neural networks to find malicious nodes in a Blackhole where a group of nodes is examined according to the amount of energy consumption, and the results are stored in a table and updated periodically The results showed that it's difficult to apply this approach in large networks where nodes rapidly change positions.

The approach used in (F. Tseng, et al,2018) present a method called GA was used to find intruder nodes in a black hole attack A set of data has been trained to identify this type of attack and not to prevent the attack in minimum time.

As well (Kaur et al., 2017) proposed a safe route discovery mechanism called GA to build the IDS for black hole attacks in MANET. (Patel, 2015)The author uses GA for intrusion detection. The GA-based IDS proposed analyses the behavior of a node and identify black hole nodes based on network parameters, e.g. packet drops, transmission rate requests, and receipt rate requests, GA requires time for evolution that is not suitable to detect malignant nodes in MANET.

The present method by (Omidvar & Mohammadi, 2014) it's focused on a forecast of links and node lifetime algorithms in MANET. Path recovery with PSO, this approach adds extra traffic and allows more messages to prolong the discovery process.

All of these and other works are aimed at finding a route or finding a blackhole node for attack or prevention. However, improved implementation in MANETs.

3 THE RESEARCH METHODS

This section introduces the research methods which consists of the system design, testing dataset, and the evaluation methods, and it is described as the following:

3.1 Testing Dataset

Several types of datasets have been used to evaluate the performance of the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) such as KDD, CAIDA, BDD, and DARPA (Patel, 2015).

Among these different types of datasets, the Berkeley Deep Drive (BDD) dataset is selected due to its variety of features that could be suitable to evaluate the performance of our proposed model. The available BDD dataset in (Yassein, Khamayseh, & Abujazoh, 2016) was utilized to evaluate the HPSGNN system in this study. It is involving feature selection to select the main as well as the most appropriate features for detecting and preventing Blackhole attack, the selection and the removal of a redundant, non-relevant feature from the data, to achieve an efficient and effective selection process. A big behavioral feature of the black-hole node that it presents itself as an intermediate node with the best route towards the target node, it sends an RREP message to the destination node with a high destination sequence number and a low number of hops. Thus, to determine the "High Report Sequence Number," "Number of low hop number to destination" characteristics, the thresholds for destination and hop count are determined before the preliminary characteristics are obtained. These thresholds are determined by collecting the RREP data that each network node transmits and recalculates, Moreover, features are selected as relevant features for the Blackhole attack.

3.2 The HPSGNN System Design

In this section, the system design has been described. There are many types of attacks targeting MANETs such as Routing Attacks, Black Hole Attacks, Grey Hole attacks, Rushing Attacks (Tseng et al., 2018). Furthermore, a blackhole Attack is the most common type of attack targeting MANETs (Gurung & Chauhan, 2019). In this work, we attempt to overcome the Black Hole Attack and protect the MANETs by proposing the HPSGNN system. The HPSGNN system is implemented by using MATLAB software, and 64 bit Windows 8. The used computer has specifications of Intel CPU core i7 @ 2.10 GHz with RAM of 4 GB. The performance of the system is computed by analyzing the results of the tested NAME Dataset. However, the HPSGNN is consisting of a hybrid of (a) Particle Swarm Optimization (PSO) algorithm, (b) Genetic Algorithm, and (c) Neural Network as the following:

3.3 Particle Swarm Optimization (PSO) Algorithm

It is a technology of evolution using a population of candidate solutions to create an optimal solution to the problem. A fitness function is used to calculate the degree of optimality. It is motivated by collective actions in societies with organized communities and evolving intelligence. It uses several nodes (particles) that make a swarm in the search area in search of the best solution. This technique is used here for the global optimization of the node values. By converging the values using the shortest route of the network nodes, PSO optimizes the values (Preetha & Chitra, 2017). This article suggests a solution by using the PSO-algorithm to optimize ad hoc network numbers of clusters and energy dissipation in nodes to provide an energy-saving solution and minimize network traffic. This method searching for a more effective and reliable solution. Inter-cluster and intra- cluster traffic is handled by cluster heads in the proposed solution. The algorithm proposed takes into account node volume, transmission power, and the mobile node battery power consumption. This approach provides a variety of options at a time (Kaur et al., 2017). The main benefit of this algorithm provides a solution with appropriate clusters and this method takes into account various parameters such as ideal degree, mobility, transmission power, and node capacity. The CH is chosen on this basis and this CH is responsible for interacting with the cluster nodes and the neighboring CHs (Fahad et al., 2018). This method has the main benefit of offering a series of solutions simultaneously to the algorithm to find optimal CH.

3.4 Genetic Algorithm (GA)

It is one type of machine learning, accompanied by its operation as an example of nature's creation cycle. In a population system, chromosomes show a set of characteristics identical to base-4 chromosomes, which completes the creation. This algorithm has 5 components.1. Population size: 2. No. of variables: 3. Mutation 4. Crossover: how much mutation happens is described. 5. Fitness: this role ultimately decides the condom (Kukreja, Dhurandher, & Reddy, 2018). To find the optimal path GA takes the variety of PSO nodes from the previous phase in a population recognized as chromosomes. Growing chromosome is shown as 0s or 1s bits. The selection is determined on each route according to the maximum fitness value. If the whole route has the highest fitness value, new chromosomes will be picked using crossover from this point. Crossover is also known as recombination of two route path and finds a new path. Then here also fitness is estimated and fewer Hops to hop count distance nodes path is chosen as first. Here if the node doesn't satisfy the blackhole attack then those nodes are well-thought-out as normal, Mutation adjusts new chromosomes by changing two bits in the node's position. A chromosome picked for the mutation will have an arbitrarily picked bit different from 0 to 1, or vice versa (Dalasaniya & Dutta, 2014).

3.5 Neural Network (NN)

ANN is used for the detection of the node in the suggested work. MATLAB's neural network is initially trained according to the characteristics of the network's nodes. ANN consists primarily of 3 layers, input, output, and hidden layer. The weights are modified in the hidden layer to increasing the variance between the input and the produced output and therefore the desired output (Krenker et al., n.d.)The function activation is used for weighted and input based outputs. If the result is consistent with the actual output, the input is right therefore the output would be modified to weight. The output is compared to the target; when the route is discovered between the source and destination node then the attacker or intruders in the set route using the ANN are being checked and if the attacker is being found then their identification is saved. On the behalf of the attacker‟s activities, the types of attackers have been checked and the presentation from the attacker is being checked to achieve better results (Preetha & Chitra, 2017).

4 EVALUATION METHODS

In this analytical study, the performance of our system is evaluated using eminent metrics, such as packet delivery ratio (PDR), Detection Rate (DR), and Throughput. PDR: calculate how much data can be succeeding is reached to the recipient if send it. DR represents the total number of detected nodes (whether these are black hole nodes or not) from the overall network traffics. Whereas, the Throughput represents the process of calculating the number of delivered data in seconds. Where in the PDR was calculated as by Eq. 1:

$$\mathrm{PDR} = \frac{\sum \text{number of packet receive}}{\sum \text{number of packet send}} \quad (1)$$

Where in the DR was calculated as by Eq. 2:

$$\mathrm{DR} = \frac{\text{number of true positive}}{\text{number of true postive} + \text{number of false negative}} \quad (2)$$

Where in the Throughput was calculated as by Eq. 3:

$$\text{Throughput} = \frac{\sum \text{packets sent}}{\text{Total data packets}} \quad (3)$$

One-way delay: processing of calculating the time to send data from the sender to the recipient over the network

One way delay = NL/R + (P-1) L/R = (N+P-1)L/R (4) N = link ,L = packet length ,R = transmission rate

5 SIMULATION AND RESULTS

The suggestion proposed methods Applying PSO and Genetic Artificial Neural Resource Networks (G-ANN) for the defense of Blackhole attacks is discussed in this section. Step I. Build a network simulator environment with some basic dimensions and important data set called DBB In the first case, N nodes are generated within the MANET for simulation to deploy the ad hoc mobile network. Step 2. The source and destination nodes from the N nodes have been described with their location after simulator creation. Step III. Use the PSO algorithm as the Cluster algorithm to find optimum no. of CH. Every node scope, including source and destination, was then initialized. Step IV. A code is generated to define the path between source and target node for the GA routing protocol. Step V-The GA algorithm for the discovery of the route and the best selection of the route by the scope is initialized. Step VI. The fitness function of the GA algorithm is calculated according to the information requested. Step VII. When a route is discovered between source and destination node then the attacker or intruders in the set route using the ANN is being checked and if the attacker is being found then their identification in the routing table is saved. Step VIII. The types of attackers have been tested and the presence of the attacker is tested to achieve better results for the operation of the attacker.

The GA and NN also reduce in comparison with an attack the effect of the black-hole assault within the. The parameter count used is energy use, packet delivery ratio by changing the value of nodes, pause time, location. Genetic algorithms have been successfully applied for black hole avoidance and optimization.

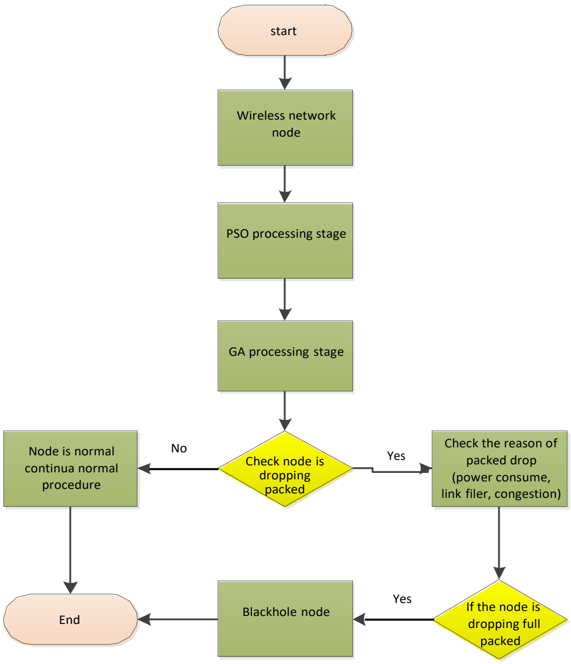
start
Wireless network node
PSO processing stage
GA processing stage
Check node is dropping packed
No
Yes
Node is normal continua normal procedure
Check the reason of packed drop (power consume, link filer, congestion)
If the node is dropping full packed
Yes
Blackhole node
End

Figure 1: Simulation Model.

1 First phase finding the optimal number of CH in MANETs network by using PSO where this method portion network to the region and then choosing CH node responsible to aggregate data then forward it to destination.

2 The second phase takes the output from the first phase and using Genetic find optimal path and neural network algorithm to detect and prevent attack with the number of parameters that have been taken place in the network using such as Throughput, Delay and the dropped packets, delivery of the packet.

This section explains the findings achieved after the proposed study was simulated. In the presence of malicious nodes, the output of the proposed method (AODV) is evaluated with GA. the method proposed compared ADOV to our simulation findings and the HPSO- GA (Kukreja, D, 2018, Thanuja, R, 2018). The main reason to choose these methods is that they are the most recent strategies in the scientific literature used and are close to our methodology, i.e. the set of nodes. The results also rely on measures of performance such as detection rate of, packets drop, throughput, and average delay. For every output metric individually, the outcomes analysis is further discussed.

- Detection Rate

Table 1 shows the results of the detection rate are described in the approach suggested. The identification rate is an important item for the precise evaluation of malicious nodes in the status packet. The reason to choose this measure is that the proposed approach demonstrates the capacity of the network to recognize the malicious nodes. On the x-axis in figure 3, the number of nodes is shown, and the y-axis indicates the detection rates (research accuracy) of the AODV, GA, and HPSO-GA. This indicates that the HPSO- GNN detection rate is the highest (98%). This is because of the reaction from every legitimate node to our proposed technology, while the malicious nodes did not respond correctly or drop down the status packet. The HPSO-GNN strategy proposed would become more likely to recognize malicious nodes as soon as the number of malicious nodes increases in the network, the proposed technology thus identifies malicious nodes faster than other nodes and therefore improves the detection rate with an increasing number of nodes, which is the highest detection rate at 98.25%.

Table 1: The detection rate evaluation values with 200 nodes.

NUMBER OF nodes	(HPSO-GA)	(AODV)	GA	Proposed HPSO-GNN
10	93.21%	85.32%	87.97%	95.40%
50	93.65%	86.28%	88.18%	96.12%
100	93.91%	86.94%	88.29%	96.99%
150	94.58%	87.15%	88.63%	97.62%
200	95.13%	87.63%	89.35%	98.25%

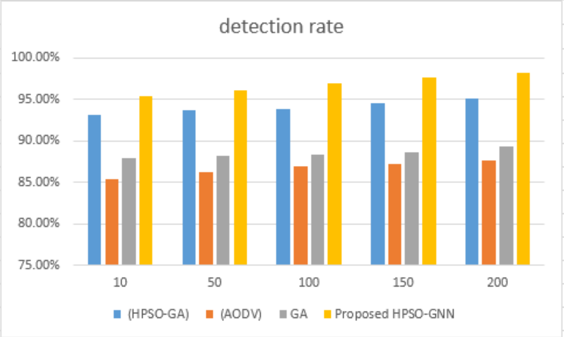

Figure 2: Detection rate.

- Packed Delivery Ratio

Table 2 and Figure 3 show the PDR of AODV, GA, HPSO-GA, and HPSO-GNN.

The PDR of HPSO-GNN is the maximum recorded (97.98%) because, after the detection of malicious nodes, packets are simply delivered more rapidly to the destination node. however, the malicious nodes increase, certainly they will cover the greatest of the network and will interrupt the communication by sending fake replies and not delivering data packets to the destination appropriately. However, after the distribution of the proposed technique, it was detected that the PDR is considerably increased, as it blacklists the malicious nodes with a status packet for a short amount of time. Nevertheless, the PDR is much better when compared to the other three protocols. Furthermore, the result investigation of packet delivery shown indicates that the proposed method outperforms AODV, GA, and HPSO-GA.

Table 2: The packet delivery ratio evaluation values with 200 nodes.

NUMBER OF nodes	(HPSO-GA)	(AODV)	GA	Proposed HPSO-GNN
10	92.28%	81.12%	83.93%	95.56%
50	92.96%	82.85%	86.53%	96.52%
100	93.15%	84.16%	87.28%	97.32%
150	93.68%	84.63%	90.15%	97.42%
200	93.96%	86.24%	90.028%	97.98%

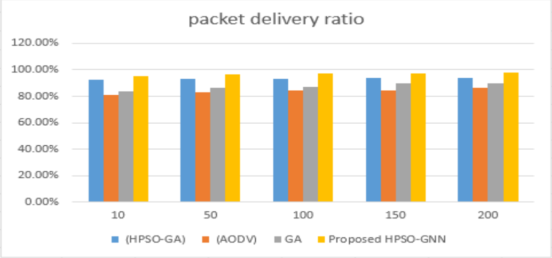

Figure 3: Packed delivery ratio.

Table 3: The one-way delay(s) with 200 nodes.

<table>
<tr><th>NUMBER OF nodes</th><th>(HPSO-GA)</th><th>(AODV)</th><th colspan="2">GA</th><th>Proposed HPSO-GNN</th></tr>
<tr><td>10</td><td>0.09</td><td>0.34</td><td colspan="2">0.21</td><td>0.05</td></tr>
<tr><td>50</td><td>0.08</td><td>0.35</td><td colspan="2">0.23</td><td>0.055</td></tr>
<tr><td>100</td><td>0.1</td><td>0.39</td><td colspan="2">0.238</td><td>0.06</td></tr>
<tr><td>150</td><td>0.16</td><td>0.16</td><td>0.43</td><td>0.2</td><td>0.075</td></tr>
<tr><td>200</td><td>0.19</td><td>0.19</td><td>0.468</td><td>0.2</td><td>0.043</td></tr>
</table>

- Throughput

Table 3 and Figure 4 showed the throughput of the network when node is translation. However, in the presence of malicious nodes in the network, as shown in the figure the proposed technique and AODV are compared. If there are two normal nodes and any malicious nodes send the false routing information claiming that there is a correct route when the data packets actually are dropped, the output is reduced. The mobility of the nodes also has a direct impact on the network's efficiency, as the movement of the nodes causes a breakdown in the connection and results in a lower network output. Table 4 demonstrates better results based on the technology's efficiency (kbps). As in HPSO- GNN, every node sends status packets to which each node responds positively. When a node does not satisfy the predefined criteria, then the node labels it as a malicious node and the other nodes cease communicating with it.

Table 4: The throughput evaluation values.

NUMBER OF nodes	(HPSO-GA)	(AODV)	GA	Proposed HPSO-GNN
10	69.16	59.23	66.288	73.122
50	70.21	60.18	66.97	74.44
100	71.76	62.42	67.71	75.91
150	72.63	63.12	68.55	76.61
200	72.34	63.78	68.75	77.33

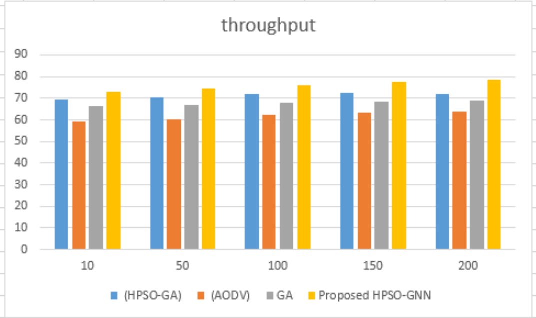

Figure 4: Throughput with 200 node.

- One-way Delay

Table 4 shows the one-way delay with a varying number of nodes. Figure 5 shows the delay in the results of the AODV and the proposed HPSO-GNN using the nodes time to forward packets on time to the intended node. The results show that the AODV network delay is high because, during transmission, the malicious node drops the data packets. In our technique suggested, the delay at meager points is slightly higher because the number of nodes continuously sends packets to regular status nodes. In MANETs, the connection failure was likewise obvious, which implies that the nodes were to retransmit the data packets back to the destination node, so that time required could cause the delay It can be seen that at meager points, in particular, The HPSO- GNN proposed is more efficient than other approaches.

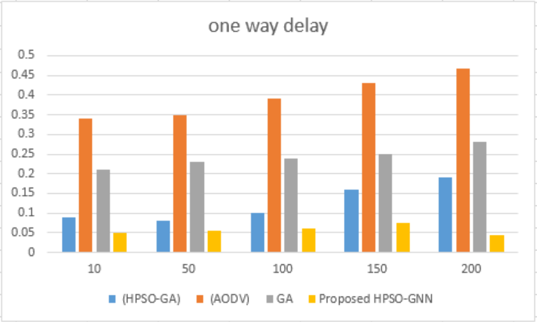

Figure 5: One-way delay.

- Packed Drop

Table 5 and Figure 6 show the results of a packet drop in the network, with no. of nodes (200) the packet drop rate proposed approach with puss time (5-15) sec and No. of black hole nodes (1-3). in which the AODV and the Proposed HPSO-GNN can be compared. It can be seen in the proposed technique that their Isa slight lag at a point, as the number of nodes is decreased; the reason for this is that the nodes end packets periodically. When a packet has broadcasted the node, it takes less time to reach every node in the set rather than the whole network. Despite sending broadcast status packets occasionally, the packed drop of the proposed technique decreases. The overall performance of the proposed method in terms of the packed drop is decreased more than other methods.

Table 5: Comparative packet drop rate.

NUMBER OF nodes	(HPSO-GA)	(AODV)	GA	Proposed HPSO-GNN
10	1.10	3.12	4.11	0.01
50	2.11	3.98	4.5	0.10
100	3.12	4.55	4.89	0.19
150	4.13	5.32	5.28	0.28
200	5.14	5. 87	5.67	0.37

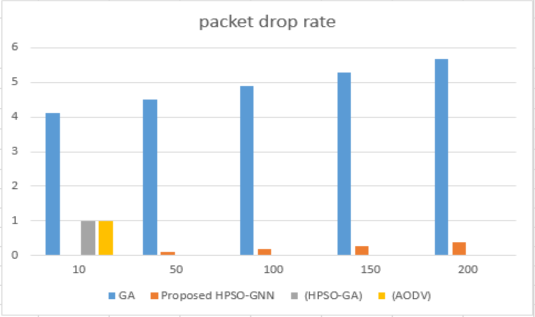

Figure 6: Packed drop rate with 200 node.

Table 6: Comparison of the proposed method with existing techniques.

Related work	No. of CH	Delay	Computation Time	Throughput	Packed Drop	Find Blackhole node
Preeti and Sumita .	✓	✓	✓	x	✓	No
ShivaniI and Pooja .	x	x	✓	x	✓	✓
Kaural et al.	x	✓	x	x	x	✓
Garg and Mongia.	x	✓	✓	x	✓	✓
Gangwar et al.	✓	✓	x	x	✓	x
Augusti and James.	x	✓	✓	✓	x	x
Kumar .	x	✓	x	✓	✓	✓
Tseng et al.	x	✓	x	x	✓	✓
Fan-Hsun et al .	x	x	✓	x	✓	✓
Shruti and Rakesh .	x	x	x	✓	✓	x
Proposed method	✓	**x**	**x**	✓	**x**	✓

6 CONCLUSIONS AND FUTURE WORK

In this paper, the proposed method to detect and prevent black hole attack in MANET, it is capable of delivering packets to the destinations even in the presence of malicious node while increasing network size decreases the packet loss and increase the security. End to end time taken to deliver the packet take smaller than another approach (with 200 nodes). To make the result more accurate the performance of these two and detection rate as compared to GA, HPSO-GA, and AODV. Future work will include increasing the number of parameters such as accuracy and routing overhead measured by the number of packets required for the communication in the network. Used approaches GA, HPSO-GA, and AODV the simulation result. Besides, for cooperative black-hole attacks, the proposed approach is equally successful. The MATLAB 2016 simulation findings indicate that all real black hole was found by the proposed method. This improves network efficiency by reducing the rate of decline, with low false-positive efficiency. This method its better performance in almost all parameters: throughput, end to end delay, packet drop rate for performance measurement will provide a more reliable and accurate result. Integrating the genetic ANN with Fuzzy Logic can result in a more efficient and faster Blackhole detection and prevention mechanism.

ACKNOWLEDGMENTS

This work has not received any financial support from any scientific institution.

REFERENCES

Augustine, A., & James, M. (2015).
ANN to Detect Network under Black Hole Attack, (Ideas), 15–18.

Chaubey, N. (2015). Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size, (i). https://doi.org/10.1109/ACCT.2015.62

Dalasaniya, K., & Dutta, N. (2014). A Survey of Cluster Management Techniques in MANETs, *IV*(December), 7–13. https://doi.org/10.1109/COMST.2005.1423333

Fahad, M., Aadil, F., Rehman, Z. ur, Khan, S., Shah, P. A., Muhammad, K., Mehmood, I. (2018). Grey wolf optimization based clustering algorithm for vehicular ad-hoc networks. *Computers and Electrical Engineering*, *70*, 853–870. https://doi.org/10.1016/ j.compeleceng.2018.01.002

Gangwar, S., Kumar, K., & Mittal, M. (2015). Cluster Head Selection in Mobile Ad-hoc Network (MANET) Using ART1 Neural Network Cluster Head Selection in Mobile Ad-hoc Network (MANET) Using ART1 Neural Network, (April).

Garg, R., & Mongia, V. (2018). Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence Technique, *3*(1), 1168–1174. https://doi.org/10.1109/ ACCESS.2020.3004692

Gurung, S., & Chauhan, S. (2019). Performance analysis of black-hole attack mitigation protocols under grayhole attacks in MANET. *Wireless Networks*, *25*(3), 975– 988. https://doi.org/10.1007/s11276-017-1639-2

Kaur, A., Kaur, P., & Aggarwal, H. (2017). Implementation of Blackhole attacks in WSN using Genetic Algorithm and PSO, *10*(4), 717–726.

Krenker, A., Bešter, J., & Kos, A. (n.d.). Introduction to the Artificial Neural Networks.

Kukreja, D., Dhurandher, S. K., & Reddy, B. V. R. (2018). Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 941–956. https://doi.org/10.1007/s12652-017-0496-2

Kumar, Vimal, & Kumar, R. (2015). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc. *Procedia - Procedia Computer Science*, *48*(Iccc), 472– 479. https://doi.org/10.1016/ j.procs.2015.04.122

Kumar, Vinod. (2018). A Review on Detection of Black hole Attack Techniques in MANET International Journal of Advanced Research in A Review on Detection of Blackhole Attack Techniques in MANET, (April 2014).

Nikhil, K., Agarwal, S., & Sharma, P. (2012). Application of Genetic Algorithm In Designing A Security Model For Mobile, 181– 187. doi : 10.5121/csit.2012.2116

Omidvar, A., & Mohammadi, K. (2014). Particle swarm optimization in intelligent routing of delay-tolerant network routing, 1–8. https://doi.org/10.1186/1687-1499-2014-147

Patel, N. J. (2015). Detecting pack et dropping nodes using machine learning techniqques in Mobile ad-hoc network : n, 468–472. doi: 10.1109/SPACES.2015.70 58308

Prajapati, L., & Tomar, A. S. (2015). Detection of Black Hole Attack with Improved AODV Protocol in Manet, 3535–3540. https://doi.org/10.15680/IJIRSET.2015.04050119 Preetha, V., & Chitra, K. (2017). Soft Computing Techniques in Mobile Adhoc network : A Technical Overview. *International Journal of Current Research and Review*, *9*(14), 23–25. https://doi.org/10.7324/ ijcrr.2017.9146

Tseng, F., Chiang, H., & Chao, H. (2018). Black Hole along with Other Attacks in MANETs : A Survey, *14*(1), 56–78. https://doi.org/10.3745/JIPS.03.0090

Yassein, M., Khamayseh, Y., & Abujazoh, M. (2016). Feature selection for black hole attacks. *Journal of Universal Computer Science*, *22*(4), 521–536.