NEURAL NETWORK APPROACH FOR DETECTING BLACK HOLE ATTACK IN MANET

Nidhi Dahiya[1], Devesh Kumar[2]

[1]Student, [2]Faculty, ECE Department, Amity University,U.P., (India)

ABSTRACT

At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious. So, this proposed work tries to design and implement neural network protocol with Black hole attack in AODV and prevent the system for threat using this hybridization.

Keywords: Neural Network, MANET, Security, AODV protocol, Black Hole attack.

I. INTRODUCTION

MANETs are very vulnerable to security sensitive applications [1]. In MANETs security is the main concern and challenge due to various vulnerabilities [2].

Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks. In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network [3]. As a matter of fact, the boundary of the network is not properly defined. Nodes can intermittently come into the network or leave it. Moreover malicious nodes can flood the network with junk packets hampering the network service or intentionally drop packets. But these nodes can but these nodes can subtly manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious [4].

In the previous couple of decades the world has turn into a worldwide town by prudence IT sector. Information Technology (IT) is developing step by step. Organizations have a tendency to utilize more difficult system situations. Regardless of the endeavors of system heads and IT merchants to secure the computing situations, the dangers posed to individual protection, organization security and different resources by attacks upon systems and PCs. The Mobile Ad hoc Networks (MANETs) are unquestionably a piece of this revolution [5]. A MANET is an accumulation of wireless devices or hubs that impart by dispatching packets to each other or for another device/hub, without having any framework controlling information for routing. MANET hubs have boundless network and versatility to different hubs. Having a secured transmission and correspondence in MANET is a key issue because of the way that there are different sorts of attacks that the mobile system is interested in [6]. To secure correspondence in such systems, understanding the at risk security attacks to MANET is an extraordinary task and concern. MANETs experience the ill effects of a mixed bag of security attacks and dangers, for example, Denial of Service (DoS), flooding attack, mimic attack, wormhole attack, black hole attack, etc.

Past studies demonstrate that there are distinctive classifications of attacks on MANET, for example, Passive and Active attacks, Internal and External attacks and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are alluded to as attacks on numerous hubs and are noxious.

1.1 Security in MANET

In MANET, every single systems administration capacity, for example, routing and packet forwarding, are performed by hubs themselves in a self-arranging way. Hence, securing a MANET is exceptionally difficult. The objectives to attack if portable specially appointed system is secure or not are as per the following [9]:

- Availability: Availability implies the benefits are available to approved gatherings at proper times. Accessibility applies both to information and to administrations. It guarantees the survivability of system administration in spite of disavowal of administration attack.
- Confidentiality: Confidentiality guarantees that PC related resources are gotten to just by approved gatherings. Assurance of data which is trading through a MANET. It ought to be secured against any divulgence attacks like eavesdropping in unapproved perusing of message.
- Integrity: Integrity implies that benefits can be altered just by approved gatherings or just in approved way.
- Authentication: Authentication is basically affirmation that members in correspondence are verified and not impersonators. The recourses of system ought to be gotten to by the validated hubs.
- Authorization: This property relegates distinctive access rights to diverse sorts of clients.
- Resilience to attacks: It is obliged to maintain the system functionalities when a bit of hubs is traded off or devastated.
- Freshness: It guarantees that malicious hub does not resend previously captured packets.

1.1.1AODV Protocol: The Ad hoc On-Demand Distance Vector (AODV) is a routing protocol that is basically used by mobile node in MANET. It utilizes the destination number to send the packets from source to destination. Utilization of destination number leads to avoiding various problems like classical distance vector protocols [10].

1.1.2 Black Hole Attack: In black hole attack, the malicious nodes use its routing irrespective of shortest path routing. In this attack no checking of routing table is done so the attack mainly happens in which malicious node tries to reply the route request message and then retains its data [7]. In this getting actual reply from actual node, dos not happen but reply from malicious node occurs [7]. Now dropping of all the packets is done to an unknown address.

Following figure describes the process of the black hole attack in the network. Suppose node A wants to send data to node C. Then irrespective of node C data will be sent to node B. Node B is the malicious node in the network. It starts sending packets to itself by showing that it is the destination and actual node. In this way lots of data gets lost or dropped [8].

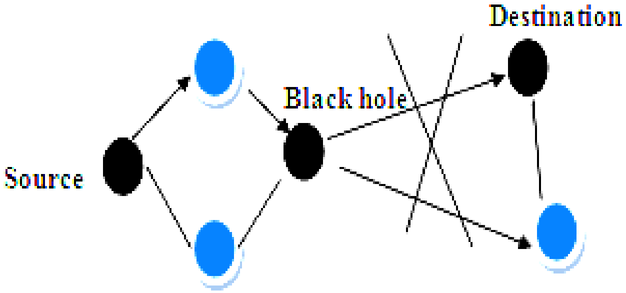

Fig.1. Black Hole Attack

1.1.2.1 Basic Strategy to mitigate Black Hole Attack: The malicious nodes in this attack acts as Black hole that drop all the data packets passed by it. If the attacking node acts as a connecting node of two components, the separation of network in two disconnected components wound taken place. The main strategies to mitigate the problem [9]:

- To collect the number of RREP messages.
- Hope the varied redundant paths to destination node.
- A buffering process need to be taken place till the safe route is found.
- With the previous sequence number, a table needs to be maintaining in increasing order.
- RREQ request would be send by the sender node to its neighbor.
- When the RREQ reaches the destination, the RREP reply was sent with last packet sequence number.
- If some problem occurs, then the RREP contains a wrong sequence number.

1.1.3 Neural Network: The main goal of neural network is to work like human brains consists of neurons. Neural network has various numbers of neurons and it works like human brain neurons. There are basically two types of NN model as shown below [17]:

- Cyclic;
- Acyclic

The normal Back propagation is the mainly applied to train Multilayer FNN. The linear and nonlinear outputs are correspondingly given by:

The net input has given by:

$$n1^{k1+1}(i) = \sum$$

The unit i is given by

This recurrence relation is executed at the final layer

II. RELATED WORK

[10] Mariappan Kadarkarainadar Marichelvam et.al (2014) proposed firefly algorithm to take care of half flowshop planning issues with two targets. Makespan and mean flow time is the target functions considered

here. Computational experiments have been done to assess the execution of the proposed method. The results demonstrate that the proposed calculation beats numerous different metaheuristics in the literature.

[11] Manoj Jhuria et.al (2014) proposed a mobile based technique to deal with overcome it. Mobile agents was generally another approach in which rather than specifically getting to a hub a project is exchanged to that system and the system executes on a system hub by using their resources and sends the obliged data back to home made. This theory shows a mobile agent based method to enhance the execution of the DSR protocol. The dynamic source Routing protocol (DSR) is a basic and effective routing protocol planned particularly for utilization in multihop remote specially appointed systems. DSR license the system to be totally self-arranging and selfconfiguring, without the requirement for any subsisting system infrastructure or administration.

[12] Mohamed Dyabi et. al (2014) proposed a new algorithm hat was basically based on clustering. The process of clustering is being done to get the nodes in terms of average memory, energy and speed. This method can also be used to solve the problem of steganography in MANET. From simulation results it has been seen that proposed clustering algorithm is better than other clustering algorithms.

[13] Istikmal (2013) utilized the routing algorithm in MANET and the improvement is done on the DSR (Dynamic Source Routing) which is routing protocol utilizing ACO algorithm. At that point they investigates and assessed the execution of this routing algorithm in different situation and contrasted the outcome and standard DSR routing protocol.

[14] K. Amjad (2013) analyzed the execution of a Mobile Ad-hoc Network (MANET) utilizing the Dynamic Source Routing (DSR) protocol with gatherings of hubs moving as indicated by the Reference Point Group Mobility (RPGM) model. Four diverse arbitrary versatility models, Levy-Walk, Probabilistic Random Waypoint, Random Direction and Random Walk were chosen for gathering pioneer's portability and the impacts of changing correspondence burden and transmission reaches were explored. The outcomes demonstrate that the execution of DSR is better if bunch pioneers take after Levy-Walk portability design paying little respect to load and reach. The execution of DSR is more terrible if the pioneer's versatility carries on like Rand-Dir or Rand Walk portability models.

[15] K.Naidu et.al (2013) presented the firefly Algorithm- FA in terms of frequency control optimization technique. FA is the type of algorithm similar to swarm optimization algorithm. The proposed work analysis the efficiency and robustness of the FA in terms of optimization. In this work comparison of FA-PID and traditional PID has been done and it has been concluded that FA-PID operates better to get high efficiency.

[16] Mohammed Wazid et.al (2013) presented that the Wireless Sensor Networks (WSNs) are inclined to different attacks in which Blackhole a sort of Denial of Service (DoS) attack is extremely hard to recognize and guard. In blackhole attack, the intruder catches and re-programs an arrangement of hubs in the system to obstruct the data they get as opposed to sending them towards the base station. Accordingly any data that enters the blackhole locale is caught and not ready to achieve destination bringing on top of the line to-end postpone and low throughput. Beforehand little measure of work is done only for identification and counteractive action of the Blackhole attack in the WSN making its discovery and avoidance extremely essential according to network execution is concerned. In this paper at first the influence of Blackhole attack was measured on the system parameters took after by the proposition of a novel method for the recognition and counteractive action of Blackhole attack in WSN.

III. PROPOSED WORK

The whole implementation is done using neural network to mitigate black hole attack in network.

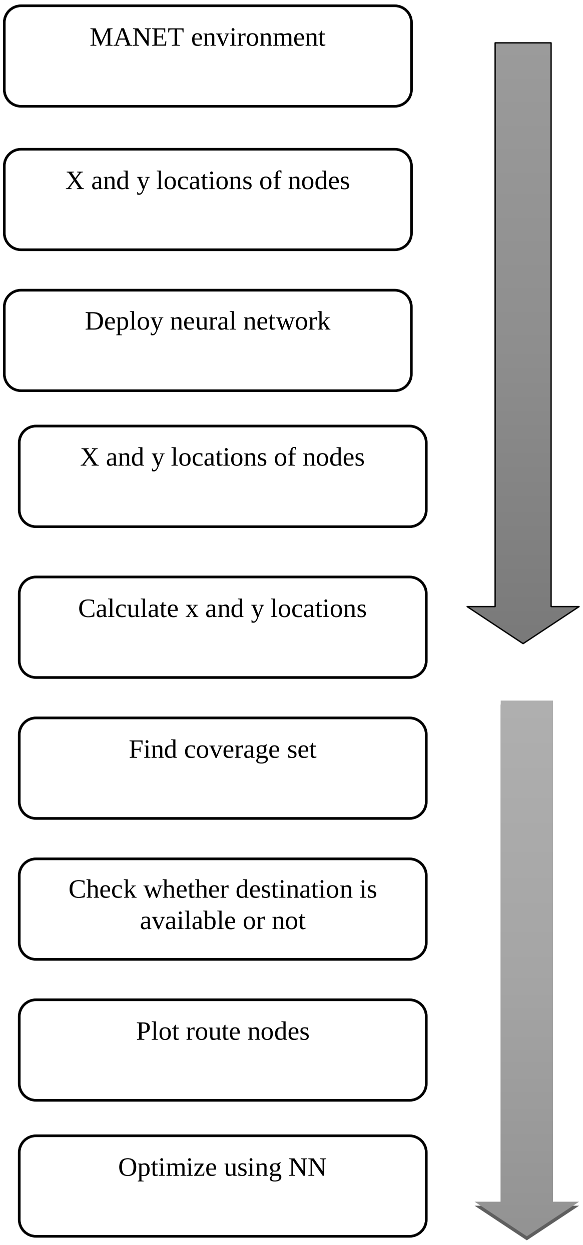
MANET environment
X and y locations of nodes
Deploy neural network
X and y locations of nodes
Calculate x and y locations
Find coverage set
Check whether destination is available or not
Plot route nodes
Optimize using NN

Fig.2. Proposed Flowchart

```
Manet Environment Deloyment
X and y locations of the nodes
Load neural network
{
Training_data=energynormal;
group=1:numel(energynormal);
net=newff(energynormal,group,10);
net.trainparam.epochs=100;
net=train(net,training_data,group);
save('neuralarchitecture','net');
grid on;
save('networknode','node_count');
%net_area=net_length*net_width;
no_nodes=node_count;
generalized_error_rate=2*rand;
clear wavelenght_substance;
}
calculate the xloc y loc and time_stamp of each nodes
Select the clusetr head by considering the time_stamp of the curren block with avg time_stamp
measure of x and y location distance
find the coverage set of each node from others
check that whether destination is available or not
selecting any node from the coverage set of the current node
plot the the source and destination in the same figure where the other nodes are already plotted
plottting the route nodes
Identify black node
Optimize using trained NN
Calculate parameters.
```

IV. RESULTS AND ANALYSIS

The whole simulation is being done in MATLAB using various parameters.

4.1Throughput

It is the rate of the data transfer from source to destination in given interval of time.

4.2 Packet Delivery ratio

It is the ratio of total number of packets transferred from total data packets.

4.3 Mac Collision

Mac Collision is defined as the total time taken to reach the destination from source and it also includes the all delays that occurs during transmission.

$$\text{Avg. EED}=S/N$$

S is the amount of the time spends to bring packet for each destination, and N is the number of packets received by the all destination nodes.

4.4 Routing overhead

It is the ratio between the numbers of sent routing packets over the number of received data packets.

4.5 Bit Error rate

The bit error rate (BER) is the numeral of bit errors per unit time. BER is a unit less calculation, frequently taken as percentage.

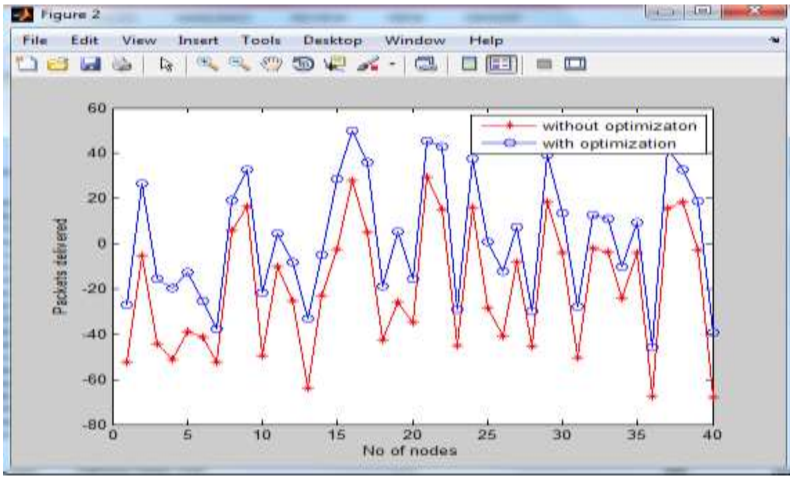

Fig.3. Packet Delivery Ratio

Above figure shows the packet delivery ratio graphical representation with and without optimization using neural network. From graph it can be seen that PDR with optimization has 40 value and without NN it is 20.

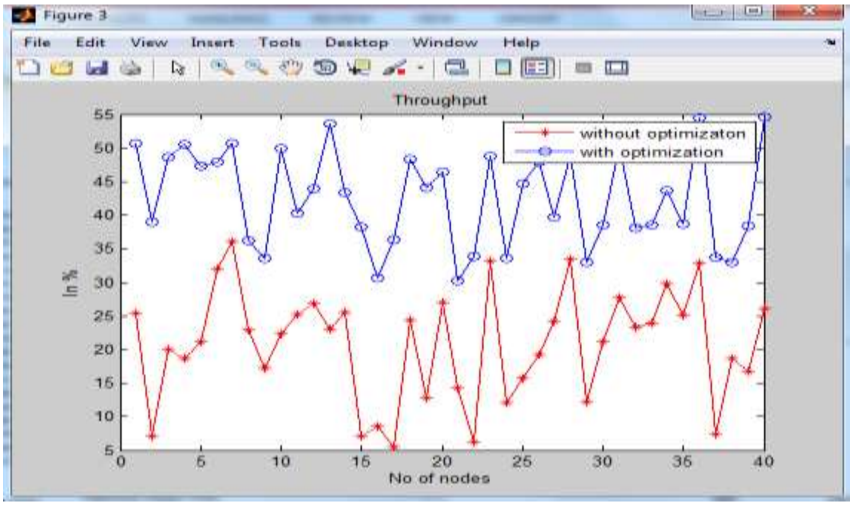

Fig.4. Throughput

Above figure shows the throughput graphical representation with and without optimization using neural network. From graph it can be seen that throughput with optimization has 50 values and without NN it is 35.

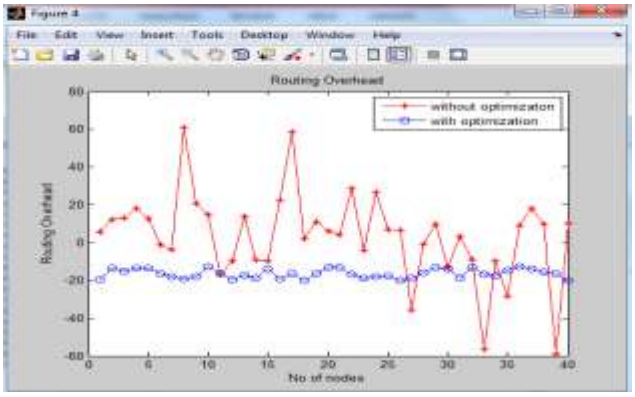

Fig.5. Routing Overhead

Above figure shows the routing overhead graphical representation with and without optimization using neural network. From graph it can be seen that routing overhead with optimization has -20 value and without NN it is 20.

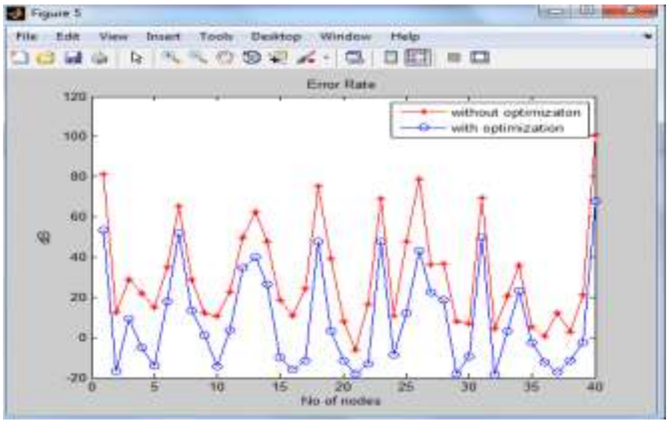

Fig.6. Error rate

Above figure shows the error rate graphical representation with and without optimization using neural network. From graph it can be seen that error rate with optimization has 40 value and without NN it is 80.

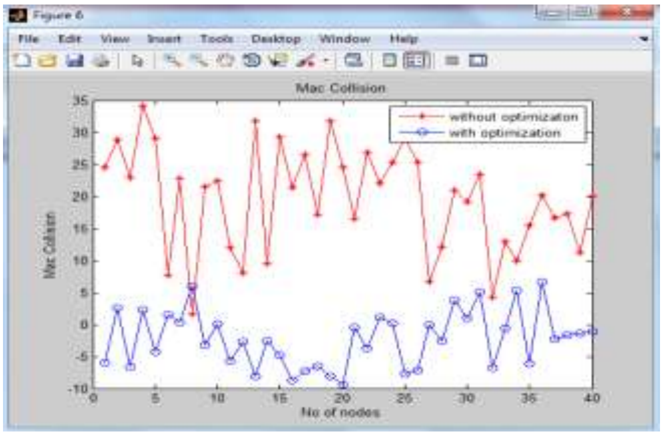

Fig.7. Mac Collision

Above figure shows the mac collision graphical representation with and without optimization using neural network. From graph it can be seen that mac collision with optimization has 35 values and without NN it is 5.

V. CONCLUSION

In this proposal, we have analyzed the effect of black hole attack in MANET using neural network algorithm. The simulation has been done in MATLAB 2010 a environment and from simulation results it has been seen that throughput with and without optimization using neural network. From graph it can be seen that throughput with optimization has 50 value and without NN it is 35, routing overhead with optimization has -20 value and without NN it is 20, error rate with optimization has 40 value and without NN it is 80 and mac collision with optimization has 35 value and without NN it is 5. So, it has been concluded that neural netwok has good rate of performance.

REFERENCES

[1] Meenakshi Tripathi,M.S.Gaur,V.Laxmi, Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN ,The 8th International Symposium on Intelligent Systems Technique, Procedia Computer Science. pp.1101 – 1107, 2013.

[2] M. Mohanapriya, Ilango Krishnamurthi, Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers and Electrical Engineering, 2013.

[3] Ting Lu and Jie Zhu, Genetic Algorithm for Energy-Efficient QoS Multicast Routing, IEEE Communications Letters, Vo.17, pp. 31-35, 2013.

[4] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad, Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks, Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN). IEEE, pp.1-5, 2012.

[5] K.S.Sujatha, Vydeki Dharmar, R.S.Bhuvaneswaran, Design of Genetic Algorithm based IDS for MANET, IEEE. pp. 28-35, 2012.

[6] M. H. Sulaiman, M. W. Mustafa, Z. N. Zakaria, O. Aliman, S. R. Abdul Rahim, Firefly Algorithm Technique for Solving Economic Dispatch Problem. Power Engineering and Optimization Conference (PEDCO) Melaka, IEEE, 2012.

[7] Sabrina Merkel, Christian Werner Becker, Hartmut Schmeck, Firefly-Inspired Synchronization for Energy-Efficient Distance Estimation in Mobile Ad-hoc Networks, IEEE, pp.205-212, 2012.

[8] V.K Taksande, A Simulation Comparison among AODV, DSDV, DSR Protocol with IEEE 802.11 MAC for Grid Topology in MANET, Computational Intelligence and Communication Networks (CICN), IEEE, 2011.

[9] Bharat Bhushan, Sarath S. Pillai, Particle Swarm Optimization and Firefly Algorithm: Performance Analysis. 978-1-4673-4529-3/12/$31.00, IEEE, 2012.

[10] Chang, J. M, Defending against collaborative attacks by malicious nodes in MANETs, A cooperative bait detection approach. Systems Journal, IEEE, 9(1), 65-75, 2015.

[11] Mariappan Kadarkarainadar Marichelvam, Thirumoorthy Prabaharan, and Xin She Yang, A Discrete Firefly Algorithm for the Multi-Objective Hybrid Flowshop Scheduling Problem, IEEE transactions on evolutionary computation, vol. 18. , 2014.

[12] Manoj Jhuria, Improve Perfomance DSR Protocol by Application of Mobile Agent, 2014 Fourth International Conference on Communication Systems and Network Technologies, IEEE, pp 336-341, 2014

[13] Mohammed Dyabi, A new MANETs clustering algorithm based on nodes performances. Next Generation Networks and Services (NGNS) , IEEE, pp. 22-29, 2014.

[14] Istikmal, Analysis And Evaluation Optimization Dynamic Source Routing (DSR) Protocol in Mobile Adhoc Network Based on Ant Algorithm, Information and Communication Technology (ICoICT), IEEE, pp. 400-404,2013.

[15] K.Amjad, Performance analysis of DSR protocol under the influence of RPGM model in mobile ad-hoc networks. 31st International Conference on Distributed Computing Systems Workshops, IEEE, 2013.

[16] K. Naidua, H. Mokhli, A. H. A. Bakar, Application of Firefly Algorithm (FA) based optimization in load frequency control for interconnected reheat thermal power system, IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), IEEE, 2013.

[17] Mohammad Wazid, Avita Katal, Detection and Prevention Mechanism for Black hole Attack in Wireless Sensor Network. International conference on Communication and Signal Processing, IEEE, pp. 576- 581, 2013.

[18] Liu Shaohui, et al, Neural Network based Steganalysis in Still Images, Proceedings of IEEE ICME, 2003.