ANN to Detect Network under Black Hole Attack

Alfy Augustine
PG scholar
Department of ECE
SJCET, Palai

Manju James
Assistant Professor
Department of ECE
SJCET, Palai

ABSTRACT
Security related issues are of serious concern in MANET. Lack of central administration and shared wireless medium makes MANET more vulnerable to security threats. An intruder passes an intermediate node into the MANET and introduces several kinds of attacks on the data transfer occurring between nodes. In this paper we consider Black hole attack in mobile ad hoc network, where all data packets are absorbed by the malicious nodes. A mechanism based on Artificial Neural Network (ANN) to detect the network under Black hole attack employing AODV routing protocol has been designed.

General Terms
MANET

Keywords
Ad hoc network, Black hole attack, Artificial Neural Network

1. INTRODUCTION
Mobile Ad hoc Network is a system in which the communication between mobile nodes takes place via radio waves. They are capable of operating without the aid of any fixed infrastructure. The mobile nodes that are in radio range of each other can communicate directly whereas others need the help of intermediate nodes which serve as routers. These networks are fully distributed and can be built at any place. Each node can send traffic and hence the node can act as both a router and a host. Due to Dynamic topology, autonomous terminal, multi hop routing, and self organization MANET find applications in several areas particularly in military tactical, disaster area network and instant conferences [1].

Availability, confidentiality, integrity, authentication and non-repudiation are the five major security goals required to maintain a reliable, better and secure ad hoc network environment [2]. Due to their inbuilt characteristics of dynamic topology, lack of central administration and shared wireless medium make MANET susceptible to various security threats. Attacks in MANET are mainly classified into two types : passive attack and active attack. Passive attack does not alter the data transmitted within the network whereas active attack prevent the message flow between the network. Eavesdropping, traffic analysis and monitoring are the different types of passive attacks. Active attacks include wormhole attack, black hole attack, greyhole, Dos attack, sybil and rushing attack.

In this paper, the Black hole attack in MANET is discussed and analysed. Our aim is to design a mechanism based on Artificial Neural Network (ANN) to detect network under black hole attack. ANN is one of the artificial intelligence methods with high computation rate and learning ability through pattern presentation.

This paper is organized as follows: Section 2 provides a brief detail on Black Hole attack. Section 3 describes about the survey made on various techniques of black hole attack detection and avoidance in MANET. Detection method is given in section 4. Conclusion on detection mechanism and future scope is described under section 5.

2. BLACK HOLE ATTACK
Black Hole attack is a kind of Denial of Service attack in mobile ad hoc network, in which all data packets are absorbed by the malicious node [3]. Black hole attack is introduced in the route discovery process of AODV routing protocol.

Ad hoc On Demand Distance Vector (AODV) is a reactive routing protocol which establish route only when it is needed. When a source node needs a route to the destination, it generates a Route Request (RREQ) packet across the network. Neighbouring nodes rebroadcast this RREQ packet to the network. Once the RREQ reach the destination, it returns a Route Reply (RREP) packet to the source via the same path. When the source node receives the Route Reply, it may begin to forward packet to the destination [4].

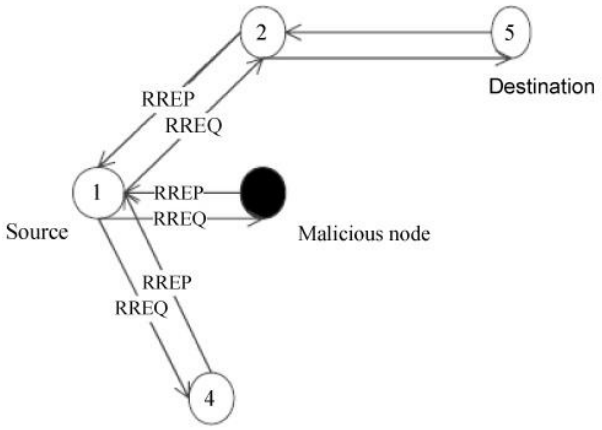

Fig 1: Black Hole attack

Figure 1 shows the black hole attack. Here 1 is source node and 5 is destination node. Node 1 wants to send a packet to node 5. So node 1 starts with route discovery process by broadcasting a Route Request message across the network. Hearing this malicious node claims it has the shortest route to the destination. Since the Route Reply message from the malicious node is more likely to reach the source node first, source node ignore all other reply messages and begin to send data packets to the malicious node, thinking that the route discovery process is complete. As a result all the data packets are absorbed by malicious node.Black hole attacks are of two types: Single Black hole attack and Cooperative Black hole attack. In single black hole attack, one node advertises itself having the shortest route to the destination and intercepts the

packet. In cooperative black hole attack, malicious nodes act in groups.

3. RELATED WORK

B. Sun et. al. in 2003 [5] proposed a neighbourhood based method to detect the existence of a black hole attack and a routing recovery protocol to mitigate the effect of black hole attack. The proposed model improved the packet throughput by at least 15 percent.Gerhards et. al. in 2007 [6] proposed a method using topology graphs to detect nodes trying to create a black hole. In this system the node generating fake information is considered as malicious node and the system triggered an alarm if plausibility check fails. The proposed system detected any attempts trying to create black hole before the actual impact occurred.Jagpreet Sing et. al. in 2011 [7] proposed Fuzzy logic based Intrusion Detection System Against Black Hole Attack on AODV in MANET. The system detected black hole in the network and this information is passed to other nodes also. The proposed algorithm improved the performance of AODV routing protocol.

Poonam Yadav et. al. in 2012 [8] proposed a fuzzy based approach to detect black hole in MANET. The system detected blackhole node using fuzzy rule which was implemented on response time of node communication.Vipin Khandelwal et. al. in 2013 [9] proposed a black hole detection method for AODV routing protocol. The proposed system introduced additional delay due to pre process in AODV routing protocol without causing any change in the functioning of AODV.Ramanpreet Karur et. al. in 2014 [1] proposed a black hole detection in MANET using Artificial Neural Network. Ann's modelling for detecting black hole attack was investigated in this paper. Throughput, Packet Delivery Ratio, End-to-End Delay and Average Jitter were given as input data for training Neural Network.

4. BLACK HOLE ATTACK DETECTION METHOD

In this system we use ANN to detect network under black hole. It is one of the artificial intelligence methods. Neural networks are organised in layers which are made up of a number of interconnected nodes that contain an activation function [9]. The basic structure of neural network consists of input layer, hidden layer and output layer. In this paper we consider the following four metrics to evaluate black hole attack:

I. Packet Delivery Ratio : It is the ratio of the packets that are successfully delivered to the destination.

$$\text{Packet Delivery Ratio} = \text{Number of packet sreceived} / \text{Number of packets send}$$

II. End-to-End Delay: It is the average time taken by the packets to pass through the network.

$$\text{E2E delay [packet id]} = \text{received time[packet id]} - \text{sent time[packet id]}$$

III. Throughput: It is the amount of data transferred over the period of time expressed in bits per second.

$$throughput(bits\ per\ second) = \frac{No.of\ delivered\ packets * Packet\ size * 8}{Simulation\ time}$$

IV. Routing Overhead: It is the number of control packets generated by each routing protocol

4.1 Implementation Methodology

Simulation was carried out using Network Simulator-2. We have performed the attack on AODV routing protocol. The network is constructed with 10 nodes. The configuration of MANET in NS-2 is shown in Table 1.

Table 1. MANET Configuration in NS2

Protocol	AODV
Mac layer	IEEE 802.11
Transmission range	250m
Node placement	Random
Area	500m X 500m
Size of data packets	512 bytes
No. of nodes	10
Traffic type	CBR
Simulation time	200sc

Using the trace files the performance metrics are calculated. Simulation results are shown in table 2.

Table 2. Simulation Results

Parameter	Packet Delivery Ratio	End-to-End Delay	Throughput	Routing Overhead
Without Black hole	6.4197	0.0192	41.62	0.13128
With Black hole	4.9653	0.0158	31.23	0.16223

4.2 ANN's Modelling

Neural Network toolbox of Matlab is used for modelling. The network consist of 3 input neurons, 2 hidden layer and 1 output layer and Feed Forward Back Propagation is selected as network type. The learning algorithm used here are TRAINLM and LEARNGDM. Packet Delivery Ratio, End-to-End Delay and Throughput are used as input data for training the neural network. Fig.2 shows the considered ANNs topology. The output parameters are shown in table 3.

Table 3. Output Parameter

Output Parameter	Status of Network
q = 1	Normal
q = 0	Network under attack

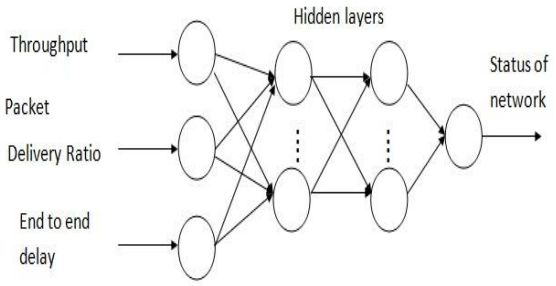

Fig 2: ANNs Topology

4.3 Simulation Results and Analysis

The analysed results are to be plotted as X-Graphs and the results are to be compared. Fig. 3 and 4 respectively shows the end-to-end delay and packet delivery ratio of normal AODV protocol and in the presence of black hole attack.

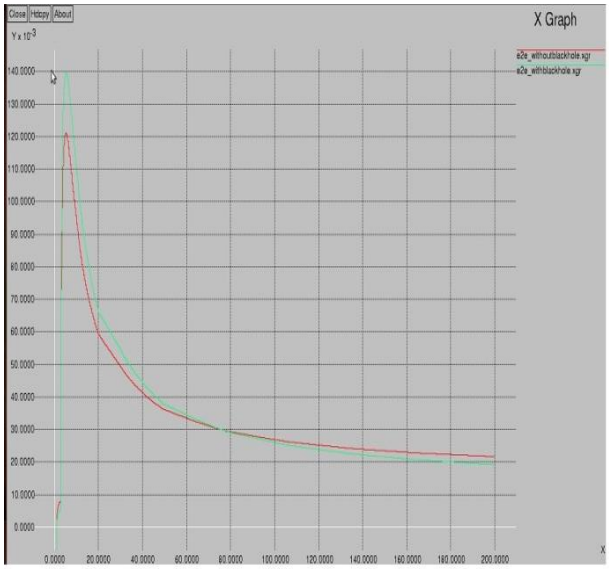

Fig 3: End-to-End delay

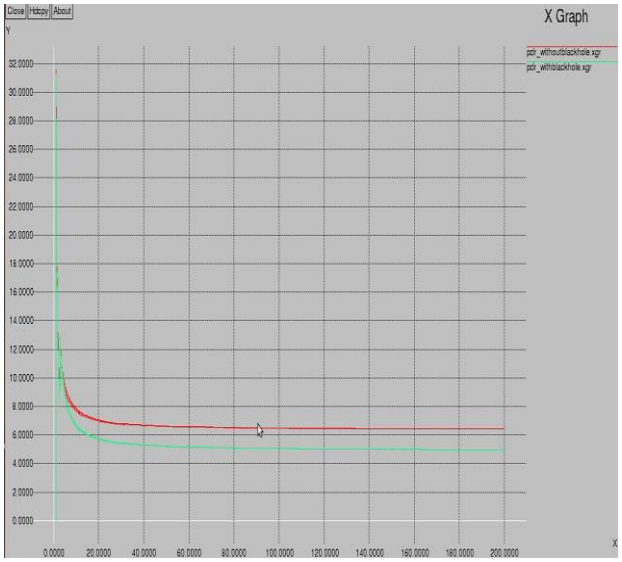

Fig 4: Packet Delivery Ratio

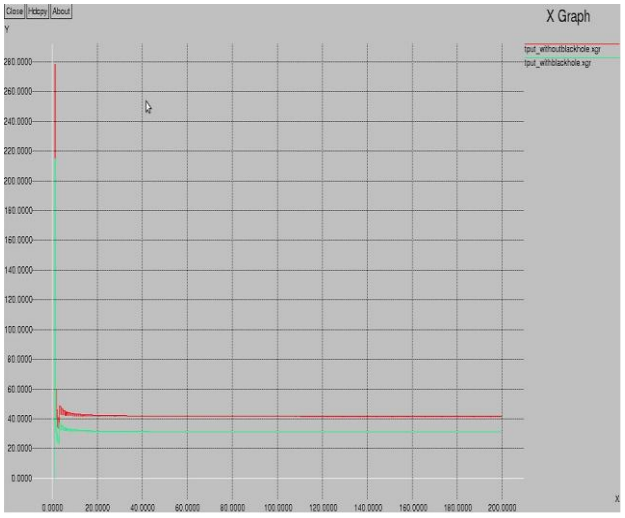

Fig 5: Throughput

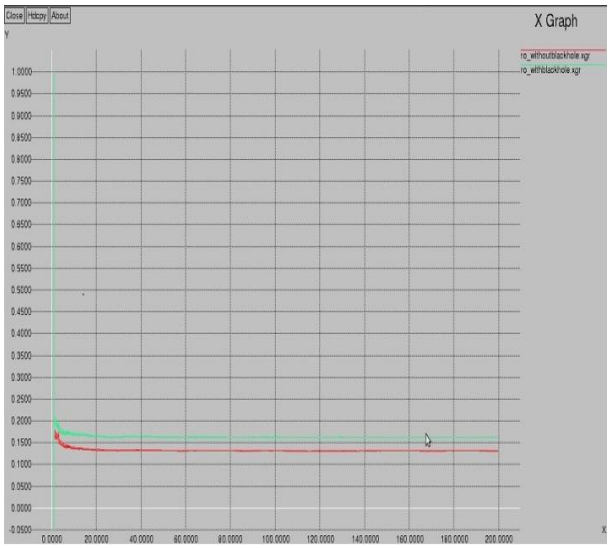

Fig 6: Routing Overhead

From fig. 3 and 4 it is clear that when the malicious node is present in the network, it reduce the end-to-end delay and the

packet delivery to destination. It can also be observed that from fig. 5 and fig. 6, when black hole attack initiates in network, there is a decrease in throughput and increase in Routing Overhead. Performance plot after the training is shown in fig. 7.

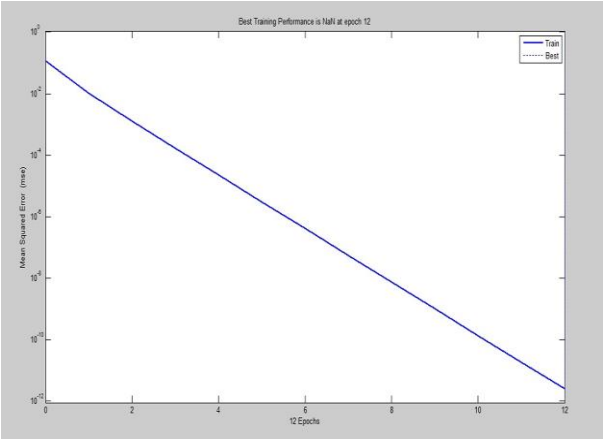

Fig 7: Performance Plot

From the plot it is clear that the mean square error decreases as the epochs increases. The values of training parameters can be changed. With the trained network random data as well as simulated data can be tested for black hole attack. If the value of q is 0, then the network is under black hole attack.

5. CONCLUSION AND FUTURE SCOPE

A mechanism based on ANN for detecting black hole attack was investigated in this paper. Throughput, packet delivery ratio and end-to-end delay were used as input data for training the neural network. It is shown that the model can be utilized for detecting up to 14 nodes under black hole attack effectively. Increasing the number of parameters used for performance measurement will provide more reliable and accurate result. Integrating the ANN with Fuzzy Logic can result in a more efficient and faster black hole detection mechanism.

6. ACKNOWLEDGMENTS

We thank our colleagues from St. Joseph's College of Engineering and Technology, who provided insight and expertise that greatly assisted the research.

7. REFERENCES

[1] Ramanpreet Kaur, Anantdeep Kaur, "Blackhole Detection in MANET Using Artificial Neural Network", International Journal for Technological Research in Engineering , Vol . 1, No. 9, 2014.

[2] Magnus Frodigh, Per Johansson and Peter Larsson, "Wireless ad hoc networking the art of networking without a network", Ericsson Review, No. 4

[3] Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre, "Securing Blackhole attack in Routing Protocol AODV in MANET with watchdog mechanisms", Word Research Journal of Computer Architecture, Vol.1, issue 1, 2012

[4] Elizabeth M Royer and Charles E Perkins, "An implementation study of the aodv routing protocol", wireless communications and networking conference, WCNC, IEEE Vol.3

[5] Bo Sun Yong Guan Jian Chen Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks" , EPMCC, 2003.

[6] Gerhardss-Padilla,E., Aschenbruck N. ,Martini, P. , Jahnke, M. , Tolle,J., " Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", IEEE Trans. 2007.

[7] Jagpreet Singh, Kulbhushan, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET", IEEE Trans.Comput. 2011.

[8] Yadav Poonam, Kumar Naveen, Gill R.K, "A Fuzzy Based Approach to Detect Black Hole Attack", International Journal of Soft Computing And Engineering (IJSCE), ISSN: 2231-2306, Vol. 2, No. 3, July 2012.

[9] Vipin Khandel, Dinesh Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs", IJARCET, April 2013, Vol 2, No 4.

[10] Moradi Zahra, Teshnehlab M., Rahmani A. M,, "Implementation of Neural Networks for Intrusion Detection in MANET" , IEEE Trans. 2011.

[11] Demuth, H.B. and M. Beale, "Neural Network Toolbox, Users Guide", The Math Work, Inc., Natick, MA, 2002.

[12] Vipan Chand Sharma, Atul Gupta, Vivek Dimri, "Detection of Black Hole Attack in MANET under AODV Routing Protocol" , IJARCSSE, Vol 3, No. 6 , June 2013.

[13] A. Mitra, R. Ghosh, A. Chakraborty, D. Srivastva," AN Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network" , IJARCSSE , 2013.

[14] J.Ramkumar, R.Murugeswari, "Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network", IJIRSET, Vol. 3, No. 3, March 2014.

[15] Y. Zhang, W. Lee, Y. Huang, "Intrusion detection techniques for mobile wireless networks", Wireless Networks , Vol 9, No. 5, Pp.545-556, March 2003.