BLACKHOLE DETECTION IN MANETS USING ARTIFICIAL NEURAL NETWORKS

Ramanpreet Kaur[1], Anantdeep Kaur[2] (Assistant Professor)
DCE, Punjabi University
Patiala, India.

Abstract: Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. A MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. Some characteristics of MANETs such as communication via wireless links, resource constraints (such as bandwidth and battery power), cooperation between the nodes due to communication protocols and dynamic topologies make it more vulnerable to attacks. Black hole attack is a well-known security threat in mobile ad hoc networks. A black hole attack node attracts all packets by falsely claiming a fresh route to the destination node and absorbs them without forwarding them to destination. In recent years, different approaches have been implemented to improve the security of MANETs. The aim of this paper is to design a mechanism of blackhole detection based on artificial neural networks (ANNs). Using a simulated MANET environment, ANNs modelling for detecting the blackhole attack is investigated and it is showed that mopdel can detect nodes under blackhole attack effectively.

Keywords: MANETs, ANNs, Intrusion detection, Blackhole Attack, FFBP.

I. INTRODUCTION

A MANET is a collection of mobile nodes that organize themselves into a network without any predefined infrastructure or centralized operation management. MANET is an IP based network consisting of a number of wireless and mobile machine nodes linked with radio. In MANET, nodes within the radio range communicate with each other directly via wireless links, while nodes out of the radio range need an intermediate node to forward their messages.[11] All the nodes in network participate in network management task. Hence network management is done in distributed manner. Each node in the network works both as router and host. As all nodes are movable so this changes topology of the network dynamically, that brings more challenges in security of Ad hoc network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. Dynamic network topology, fluctuating link bandwidth, multi-hop routing, self-organization, self-adaptive and self-configurable make it an attractive option for broad area of networking, particularly in military tactical, personal area, instant conferences and disaster area networks.

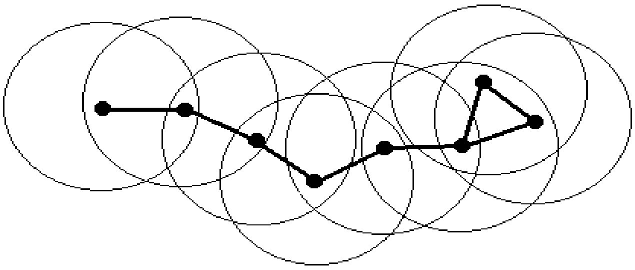

Fig. 1: A MANET

Different characteristics of MANETs include autonomous terminal, fast deployment, dynamic topology, fluctuating bandwidth, resource constraints, lack of fixed infrastructure, self-organization, distributed operation and lack of physical security. There are five major security goals that maintain a reliable and secure ad-hoc network environment. They are confidentiality, integrity, availability, authentication and non-repudiation. Attacks in MANETs can be classified into two main categories: passive attacks and active attacks. Different types of passive attacks are: eavesdropping, location disclosure and traffic analysis. Active attacks include sleep deprivation, warmhole attack, blackhole attack, sinkhole, greyhole, rushing attack, Sybil attack and DDoS attack. The aim of this paper is to design a mechanism to detect blackhole attack in MANETs on the basis of artificial neural networks (ANNs). ANNs are one of the artificial intelligence methods that can provide a strong tool for detecting malicious nodes in MANETs. High computation rate, learning ability through pattern presentation, prediction of unknown patterns and flexibility affronts the noisy patterns are the main advantages of ANNs.[14] In this paper, we present a blackhole attack simulated in the MATLAB software and introduce an ANN designed to detect that attack. Finally, the conclusion is presented.

II. RELATED WORK

In recent years different approaches have been implemented to detect blackhole attack and improve security of MANETs.

B. Sun *et al.* in 2003[1] proposed a neighbourhood based method to detect whether there exists a blackhole attack and a route recovery protocol to set up a correct path to the true destination. This method has a remarkable advantage that the number of encryption/decryption operations for authentication is much reduced compared to those methods completely relying on cryptography based authentication which can save many system resources.

S. Ramaswamy *et. al. in* 2003[2] proposed an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

M. Shurman *et al. in* 2004[3] proposed two different approaches to solve the black hole attack. The first solution, the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination.The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

Gerhards *et al.* in 2007[4] proposed a centralised approach, using topology graphs to identify nodes attempting to create a black hole. Well-established techniques are used to gain knowledge about the network topology and this knowledge is used to perform plausibility checks of the routing information propagated by the nodes in the network. A node generating fake routing information is considered as malicious. Therefore, we trigger an alarm if the plausibility check fails. With this approach, it is possible to already detect the attempt to create a black hole before the actual impact occurs.

Poonam Yadav *et al* in 2012[5] proposed a mechanism based on fuzzy logic to check a node is infected by black hole attack or not. The given research provides the solution of packet loss in case of blackhole attack over the network. Firstly the blackhole node is detected using fuzzy rule. The fuzzy rule is implemented on response time of node communication. Instead of transferring data on this node, it will be passing on from surrounding nodes: it will only handle the transmission that is directed to it only.

A. Mitra *et al* in 2013[6] proposed an Artificial Neural Network (ANN) based automated Black Hole node detection tactic. Proposed ANN based system is dynamic in nature. Implemented intercommunication methodology for detecting the presence of Black Hole node helps to update routing table more dynamically as it is working at both ends: at CRC side and TTR side.

G. Wahane *et al.* in 2014[7] proposed the modification of Ad Hoc on Demand Distance Vector Routing Protocol. The proposed work suggests two new concepts, Maintenance of Data Routing Information Table and cross checking of a node. A security protocol has been proposed that can be utilized to identify multiple blackhole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the blackhole nodes.

III. METHODOLOGY

To design the mechanism, following steps are taken [14]:

- Blackhole attack definition and parameters selection
- MATLAB simulation
- Data Extraction
- ANNs Modelling
- Result Analysis

A. Blackhole Definition and Parameters Selection

A black hole attack is a kind of denial of service attack in mobile ad hoc networks. In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the destination node of the packet that was intercepted. This attack can be easily implemented in AODV during the routing discovery process. Once the forged route has been established the malicious node is able to become a member of the active route and intercept the communication packets. The outcomes of this attack can vary. The malicious node can either stop after inserting the false route information in the network and aim in creating instability and unnecessary network traffic or drop all incoming application packet for the specific destination. [5]

Blackhole attacks can be classified into two categories: Single blackhole attack and Cooperative blackhole attack.

Figure 2 shows a black hole attack.

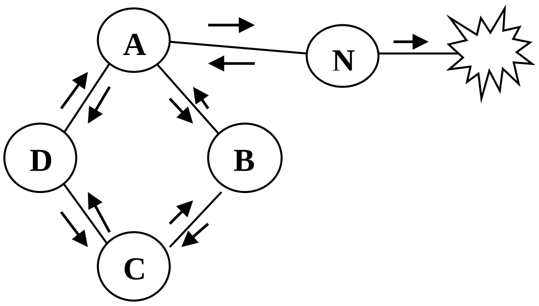

Fig. 2: Blackhole Attack

Here, A is the source node D is the destination node and N is the malicious node. Node A starts with the route discovery process then the node N advertises itself as having a valid shortest route to the destination, even though the route is false with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost.

Blackhole attack can be detected using the parameters that are affected by this type of attack.

Four critical parameters considered in this paper are given below:

a) Throughput: It is defined as the total number of packets delivered over the total simulation time. It is represented in packets per second or bits per second.

Throughput (bits per second) = (No. of delivered packets * Packet Size * 8) /Simulation Time

b) Packet Delivery Ratio: Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source.
Packet delivery ratio= Number of packets received/ Number of packets sent

c) End-to-End Delay: The average time taken by the packets to pass through the network is called end-to-end delay.
E-2-E delay [packet_ id] = received time [packet_ id]– sent time [packet_ id]
Average Delay= $\sum_{i=1}^{n} d_i / n$
Where, di= average end to end delay of node of ith application and n=number of application.

d) Average Jitter: Jitter is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source.

B. Simulation Environment for MANETS
Simulation was carried out using MATLAB. MATLAB provides a simple platform for simulation. The number of nodes is unlimited i.e., a node can be connected to any no. of other nodes in range (say 20, 50, 100, 200,...).

C. Data Extraction
Using analysis log files, the parameters were extracted. Configuration of MANETs is shown in table below:

Parameter	Value
Area Size	1000m*1000m
Number of Nodes	50,100,150,200,250,
Simulation Time	6.45 sec
Packet Size	8 bits
Number of Packets	100*Number of Nodes
Communication Range	250m
Number of Connections	1775

Table. 1: Configuration of MANETs

The input and output parameters are shown below in tables 2 and 3 respectively.

Parameters	Throughput	Packet Delivery Ratio	End-to-End Delay	Avg. Jitter
Without blackhole	1.1733	1.2911	0.0026	0.0478
With blackhole	0.5711	0.7511	0.0019	0.0183

Table. 2: Input Parameters

Output Parameter	Status of Node
c <= 1	Normal
c > 1	Node under Attack

Table 3. Output Parameters

D. ANNs Modeling
Neural network MATLAB toolbox is used for the modeling. Neural network model is trained by applying test data given in as inputs to ANN. In this research, Feed Forward BackPropagation (FFBP) is selected for network type. Backpropagation learning algorithm is used to train the network.
Artificial neural network is one of the artificial intelligence methods. The goal of ANNs is to discover the inherent relationship between input and output data. The basic architecture consists of three types of neuron layers: input, hidden and output layers in ANNs that process data and tries to reduce the differences between actual and predicted output by changing the connection weights between layers. Reaching this desired outcome, results trained ANNs that its knowledge is saved in weights between layers and could be used to predict the output of any new input with the same pattern.

E. Result Analysis
A Graphical User Interface (GUI) is generated that contains buttons for different options: Train, Result and Simulation Result. Random data as well as simulated data can be tested for blackhole attack. If the value of counter c is greater than 1, then the node is under blackhole attack.
Figure 3 shows packet delivery ratio of nodes without blackhole and with blackhole. Figure 4 and Figure 5 show throughput and end-to-end delay of nodes without blackhole and with blackhole respectively.

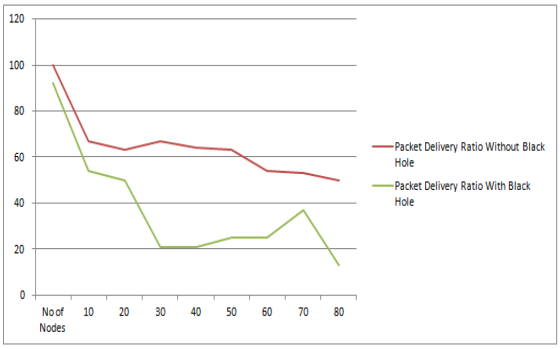

Fig. 3: Packet Delivery Ratio

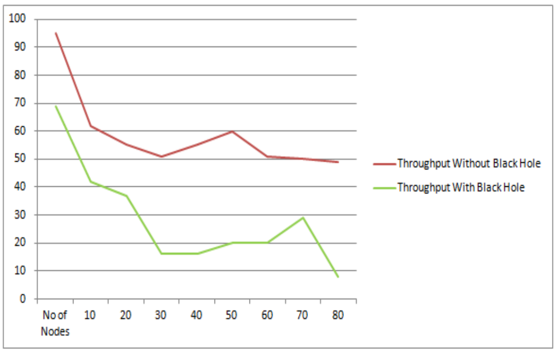

Fig. 4: Throughput

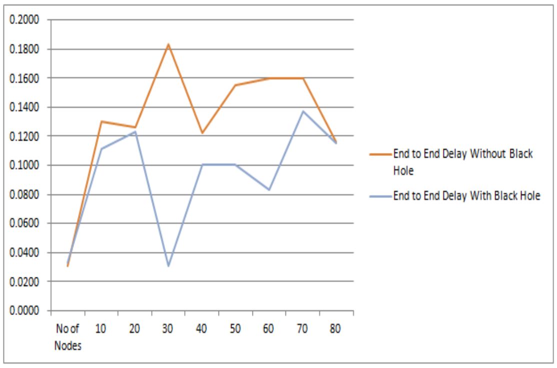

Fig. 5: End to End Delay

IV. CONCLUSION

ANNs modelling for detecting blackhole attack was investigated in this paper. Throughput, packet delivery ratio, end-to-end delay and average jitter were used as input data for training the neural network. The values of training and testing parameters can be changed. Using simulation, it is shown that the proposed model can be utilized for detecting nodes under blackhole attack effectively.

V. FUTURE SCOPE

Artificial neural networks are one of the artificial intelligence methods which have been least explored. ANNs have a wide scope of research in future. In blackhole detection mechanism, the number of parameters can be increased. Greater number of parameters will give more accurate results. Artificial neural networks can be collaborated with various techniques like Fuzzy logic, Genetic algorithm, Classification algorithms, etc to develop mechanisms that can detect blackhole attacks in MANETs with more speed, more ease and more efficiency.

REFERENCES

[1] B. Sun, Y. Guan, J.Chan,U.W. Pooch, “Detecting Black-hole Attack In Mobile adhoc Networks” in EPMCC, 2003.

[2] S. Ramaswamy, Huirong Fu, M. Sreekantaradhya, John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” in Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.

[3] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park,” Black Hole Attack in Mobile Ad Hoc Networks” in ACMSE’04, April 2-3,2004, Huntsville, AL,USA.

[4] Gerhardss-Padilla,E., Aschenbruck N. ,Martini, P. , Jahnke, M. , Tolle, J., “Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs” in IEEE, 2007, pp.1043-1052.

[5] Yadav Poonam, Kumar Naveen, Gill R.K., “A Fuzzy Based Approach to Detect Black Hole Attack” in International Journal of Soft Computing And Engineering (IJSCE), ISSN: 2231-2306, Volume-2, Issue-3, July 2012.

[6] A. Mitra, R. Ghosh, A. Chakraborty, D. Srivastva, “An Alternative Approach to Detect Presence of Black HoleNodes in Mobile Ad-Hoc Network Using Artificial Neural Network” in IJARCSSE, 2013.

[7] G. Wahane, A. Kanthe, s”Techniques for detection of cooperative Black hole Attack in MANET” in IOSR-JCE, 2014.

[8] N. Komninos, D. Vergados, C. Douligeris,”Detecting unauthorised and compromised nodes in mobile adhoc networks” in Adhoc Networks 5, 2007, pp. 289-298.

[9] Mitrokotsa A, Komninos Nikos, Douligeris Christos, “Intrusion Detection with Neural Networks and Watermarking Techniques for MANET” in IEEE, 2007.

[10] Sujatha K.S. , Dharmar V. , Bhuvaneswaran R.S., “Design of genetic algorithm based IDS for MANET”, IEEE (2012), pp.28-33.

[11] Y. Li, J. Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET”, Commodore Perry, 2004

[12] Y. Zhang, W. Lee, and Y. Huang, “Intrusion detection techniques for mobile wireless networks” in Wireless Networks, vol. 9 no. 5, pp. 545- 556., 2003.

[13] Zhou, L. and Z.J. Haas, 1999, “Securing ad hoc networks” in IEEE Network, 13(6), pp 24-30.

[14] Moradi Zahra, Teshnehlab M., Rahmani A. M., “Implementation of Neural Networks for Intrusion Detection in MANET”, (IEEE), 2011.