International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence Technique

Rajni Garg, Vikas Mongia
Computer Engineering Department, Guru Nanak College, Moga, Punjab, India

ABSTRACT

This research has dealt with the detection and mitigation of black hole attack in MANET. Generally, the black hole attack can be easily deployed with an adversary. It is one of the known security threats in the network. Black hole occurs because of the malicious nodes that draw the data packet with the false route. In this research, AODV routing protocol is being used. Genetic algorithm for the optimization of the route from the source to the destination has been used with the neural network that detects and prevents the network from the black hole attack. The simulation has been carried out in MATLAB environment and the performance is being calculated with the number of parameters, like, Throughput, PDR, Delay and energy consumption.

Keywords : MANET, AODV routing protocol, GA (Genetic algorithm), NN (neural network).

I. INTRODUCTION

MANET (Mobile ad hoc network) is known as infrastructure less IP (internet protocol) network for wireless and mobile machine nodes integrated with the nodes [1]. In the experiment, the MANET nodes do not contain a mechanism of centralized administration. MANET is considered for the routable network in which every node behaves as a router for forwarding the traffic to another particular network node [2].

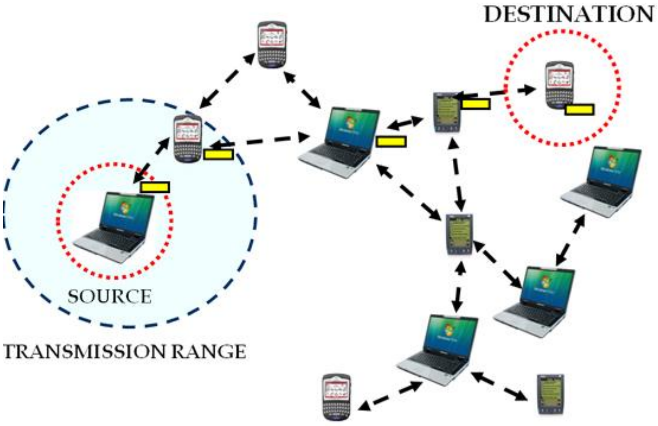

Figure 1 : MANET (Mobile ad hoc network)

Generally, MANET is consisted of three types, termed as InVANET (Intelligent Vehicular ad hoc network), VANET (Vehicular ad hoc network) and iMANET (Internet based MANET) [3].

InVANET has AI (Artificial intelligence) for tackling the unanticipated circumstances such as vehicle accident and collision.

VANET let the efficient communication with other vehicle and assists for the communication with roadside equipments.

iMANET support to link static and the mobile nodes.

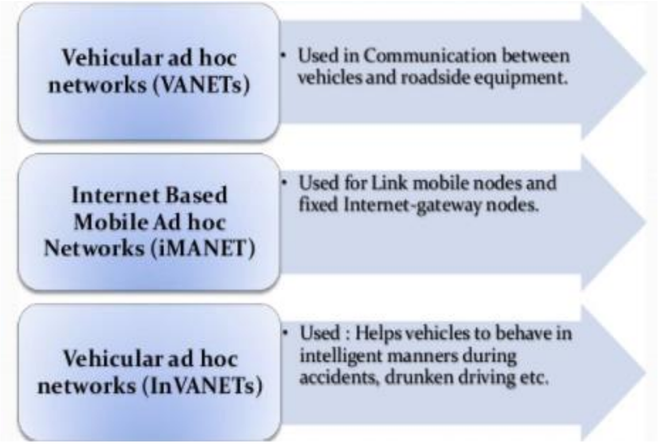
Vehicular ad hoc networks (VANETs)
Used in Communication between vehicles and roadside equipment.
Internet Based Mobile Ad hoc Networks (iMANET)
Used for Link mobile nodes and fixed Internet-gateway nodes.
Vehicular ad hoc networks (InVANETs)
Used : Helps vehicles to behave in intelligent manners during accidents, drunken driving etc.

Figure 2 : MANET types

MANET communication is consisted of two phases, route discovery and data transmission. These phases are susceptible for number of attacks. Initially, the rival might interrupt the route discovery by copying the control traffic being forged. Accordingly, the attackers may block the legitimate route control traffic propagation and wrongly manipulate the benign nodes general knowledge [4].

For providing the complete security, the discussed MANET phase communication should be guarded safe. It is to be notice that the secure routing protocols guarantee that the accuracy of the information of discovered topology cannot by itself sure the safety and the undisrupted transmitted data delivery [5]. The approach to secure the network at the network layer is by securing the routing protocol for the prevention of probable attacks. In concise, the routing protocol task discovers the topology for ensuring that every node can obtain a recent network topology map to develop the routes.

Routing in MANET could be categorized in three categories, namely, Reactive protocols [for instance, DSR and AODV], Proactive Protocols [for instance, OLSR and TBRPF], Hybrid protocols [for instance, ZRP]. The existing works in MANET security research [for instance, ARAN, SAODV and SEAD] have determine the preventive methods for protecting the routing protocol. Significant work is dependent on the key management/encryption methods for preventing the unauthorized nodes from network joining. Though, the methods cannot prevent the attacks being launched by the nodes with the valid key. So, response system and intrusion detection schemes are needed for countering the attacks as protection of second line. For designing an efficient scheme, in depth knowledge of how the nodes may attacks the network is essential [6].

The objective of the research is the prevention of black hole attack by utilizing the AODV routing protocol. GA (Genetic algorithm) optimization and ANN (Artificial bee colony) algorithm has been utilized for the mitigation of the black hole attack. Metrics, namely, Delay, throughput, BER and energy consumption are used for the calculation of the performance.

II. AODV ROUTING PROTOCOL OVERVIEW

AODV (Ad Hoc On-Demand Distance Vector) routing protocol has been used widely and is known as the reactive protocol in which the routes are developed only when required. The network nodes exchange the routing packets among them when the communication is required and sustain only the established routes [7]. This is the one that adjusts the DSDV (Destination sequenced distance vector) protocol for having dynamic link situations. When the node requires transferring the data packet to other node, it checks its routing table. If the node has fresh route then it utilizes that route for sending the data packets [8]. Route discovery process initializes only when the node doesn’t have the route or doesn’t have the novel route. Therefore, it transfers the RREQ (route request message) to its subsequent neighbours. The intermediate node verifies while it has the destination nodes or the fresh route towards the destination node. If it is accessible, than the intermediate send the RREP (Route reply message) back to the source node [9].

Or, it transfers the RREQ message towards the neighbours by utilizing the flooding method. This procedure is constant till the destination node is being found/ node with the fresh route towards the destination has been found. When the route discovery process is finished, source node and the destination node could communicate and transfer the packets among them. When some know identifies the failure or break, RERR (route error) message is transferred to another node for lost link notification. The ‘HELLO’ message is utilized for the detection and monitoring the links to the neighbours [10].

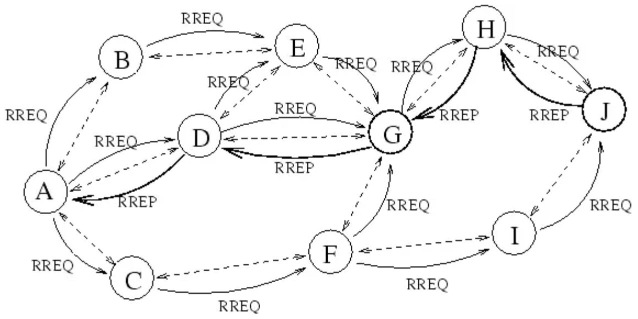

Figure 3 : AODV illustration

Consider an example in which AODV checks the probable route to RREP from the destination to the source. In the example, node A requires to set up the route to the node J. Following conditions are taken place while the establishment of the route [11].

i. For the establishment of the route, node A requires to send RREQ packet to another neighboring network nodes.

ii. When the node J has the RREQ packet, it transfers back to RREP packet.

iii. The packet is being unicasted to the A node (sender node) by another neighboring node.

III. BLACK HOLE ATTACK

In MANET, with AODV protocol, the black hole node assume to have fresh enough route towards the destination demanded by the nodes and takes up the network traffic. When the source node transfers the RREQ message to some destination, the black node instantly responds with RREP message with the highest sequence number and the message is taken as it is impending from the destination or from the node with the fresh towards the destination. The source node then initializes by sending the data packets to the black hole node with the trust that the packets would reach the destination [12].

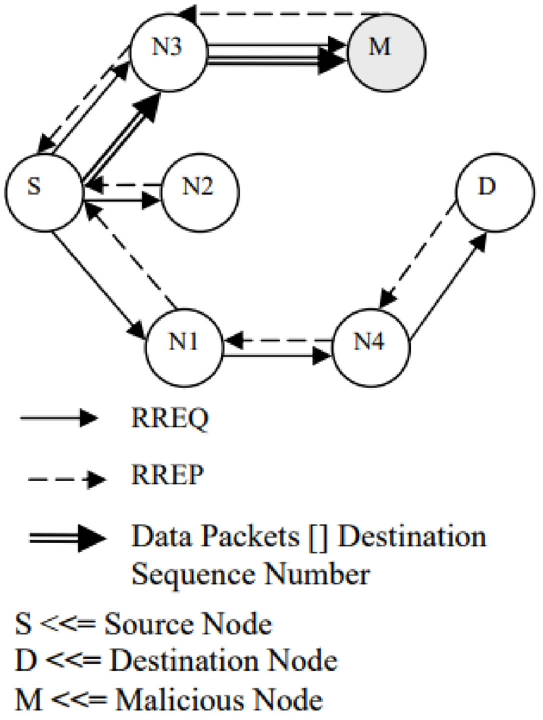

Figure 4: Black hole attack

As shown in the above figure, the destination sequence number be 32 bit integer being connected with each route and is utilized for deciding the exact route freshness. The node N3 would transfers that to the node. As the node N1 with the node N2 doesn't have the route towards the node D, it will again send the RREQ control message. RREQ control message has been send the Node N3 being expected to be taken by node M. Therefore, the node M produces the false RREP control message and transfers it to the node N3 with enhanced destination sequence number transferred to node S. Though, in AODV, as the destination sequence number is more, the route from the node would be taken be fresh and therefore, node S will start transferring the data packets to node N3 [13].

IV.SIMULATION MODEL

This section defines the work being proposed for the detection and mitigation of black hole attack. AODV routing protocol has been used with GA optimization algorithm and ANN (Artificial neural network) in MANET network. The algorithms for the same are defined below:

Genetic algorithm

```
function GA ()
{
        Initialize population;
        Calculate fitness function;
        While(fitness value != termination criteria)
{
        Selection;
        Crossover;
        Mutation;
        Calculate fitness function;
        }
}
end
```

Artificial Neural Network Algorithm

```
Initialize the ANN
Net= newff (Training_data, Ggroup, Neurons)
Where, Training_data=All data
Ggroup= No. of categories
Neurons=50
Initialize the training parameters
Epoch=1000
Levenberg marquardt
Performance= MSE, gradient, mutation, & validation checks
Net= Train (Net, Training_data, Group)
Return Net as output of ANN
```

The steps followed for the simulation of the proposed work are defined below:

i. Development of a simulator with 1000*1000 as height and width has been taken place. Firstly, n number of nodes are executed in MANET for the simulation with x as well as y co-ordinates.

ii. The source and the destination are introduced with the creation of the simulator with N number of nodes with the usage of co-ordinates.

iii. Coverage area is initiated with each node with source and the destination. The coverage area for the network is 20% for total network area.

iv. AODV routing protocol is developed for the route discovery for source and the destination node.

v. GA algorithm is considered for route discovery and for searching the best route selection with the coverage set.

vi. Fitness function has been described for GA as per network requirements.

vii. When the route discovery takes place, the performance parameters are calculated and if the performance is being degraded, then the classification of the attack would be done by using NN.

viii. According to attacker's activity, the attacker kind is measured and the performance of the attacker is measured to have the better results.

ix. Metrics, such as, throughput, delay, energy consumption and BER are measured for checking the proposed work performance.

V. SIMULATION RESULTS

The results being obtained after the simulation of the proposed work are defined in this section. The explanations of the parameters are described below:

i. Throughput

It is defined as the amount of packets send in the simulation time. It is the addition of the transmitted data from the source towards the destination in exact time span. The throughput could be measured in Kbps, Mbps, and Gbps and commonly defines in percentage (%). Throughput can be defined as:

$$\text{Throughput}= \frac{\sum \text{Packets sent}}{\text{Total data packets}}$$

ii. Delay

It is the time taken for the transfer of data packet in the network from the source to the destination. So, generally, the routes are utilized in the network with few probability of delay for enhanced performance. It can be defined mathematically as:

$$Dend - end = Dtrans + Dprop + Dproc$$
$$Where\ Dend - end = End - To - End\ Delay$$

As depicted, Dtrans= Transmission Delay (Dprop= Propagation Delay and Dproc= Processing Delay

iii. BER (Bit Error rate)

It is defined as the rate at which the errors present in the transmission system. It might be explicitly translated in the string with the required number of bits. It can be defined as:

$$\text{BER} = \frac{\text{number of errors}}{\text{number of packets sent}}$$

iv. Energy Consumption

It is described as the energy being consumed by the network while transferring the packets. It can be described as:

$$\text{Energy consumption} = E_{Tx} + E_{Rx} + E_{Amp} + E_{Agg} + E_{Prop}$$

As defined, E_{Tx} is the transmission energy , E_{Rx} is the receiving energy, E_{Amp} is the amplification energy, E_{Agg} is the aggregation enegy and E_{Prop} is the propagation energy

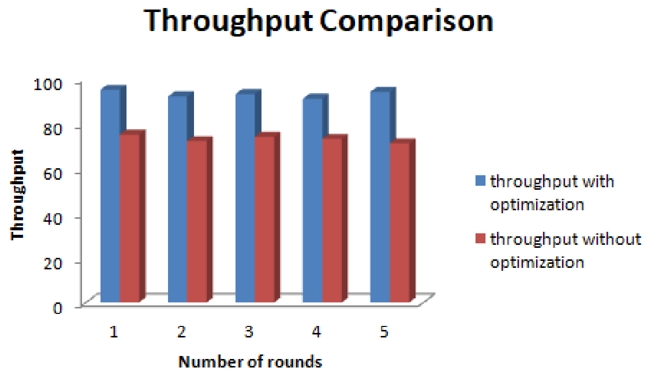

Figure 5 : Comparison of throughput for with and without optimization

The comparison of throughput with and without optimization is depicted in the above figure. As shown, the X-axis is the number of rounds and Y-axis is for throughput. The blue bar defines the value of throughput with optimization that is with Genetic Algorithm and ANN. The average value of throughput with optimization is 93 and without optimization, it is 73.

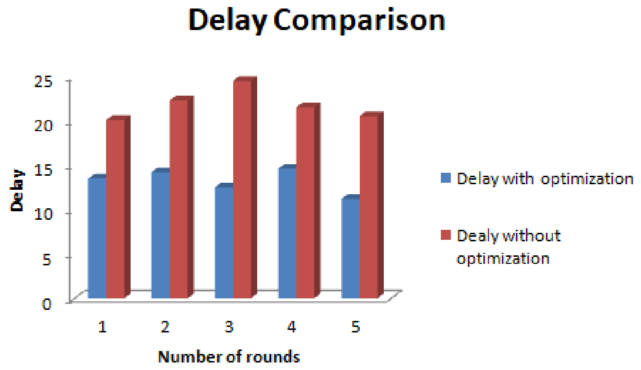

Figure 6 : Comparison of Delay for with and without optimization

The comparison of delay with and without optimization is depicted in the above figure. As shown, the X-axis is the number of rounds and Y-axis is for delay. The blue bar defines the value of delay with optimization that is with Genetic Algorithm and ANN. The average value of delay with optimization is 13.2 and without optimization, it is 21.78.

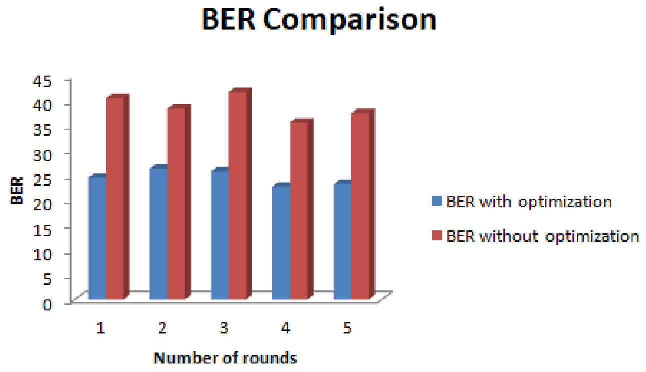

Figure 7 : Comparison of BER for with and without optimization

The comparison of BER with and without optimization is depicted in the above figure. As shown, the X-axis is the number of rounds and Y-axis is for BER. The blue bar defines the value of BER with optimization that is with Genetic Algorithm and ANN. The average value of BER with optimization is 24.5 and without optimization, it is 38.74.

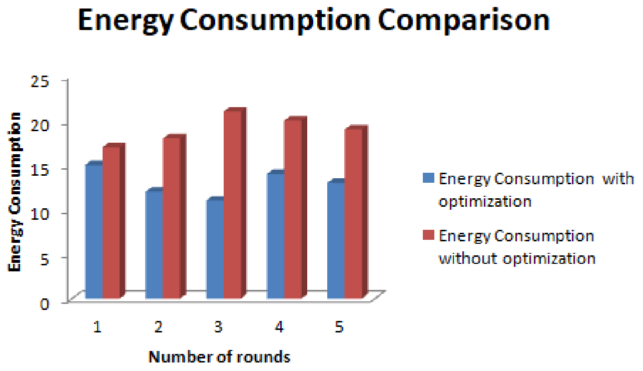

Figure 8 : Comparison of Energy Consumption for with and without optimization

The comparison of energy consumption with and without optimization is depicted in the above figure. As shown, the X-axis is the number of rounds and Y-axis is for energy consumption. The blue bar defines the value of energy consumption with optimization that is with Genetic Algorithm and ANN. The average value of energy consumption with optimization is 13 and without optimization, it is 19.

VI.CONCLUSION

The research has analyzed and mitigated black hole attack in MANET. GA is being used for the reduction of delay, BER and for the enhancement of throughput. ANN as a classifier has been used. A variety of work has been done for the detection of black hole attack but did not utilize routing protocol for the betterment of the results. This research has used AODV routing protocol with the optimization and the classification algorithm. Parameters, like, throughput, BER, Delay and energy consumption has been utilized for the performance calculation. The average value of throughput with optimization is 93 and without optimization, it is 73. The average value of delay with optimization is 13.2 and without optimization, it is 21.78. The average value of BER with optimization is 24.5 and without optimization, it is 38.74. The average value of energy consumption with optimization is 13 and without optimization, it is 19. It can be said that with the usage of GA and NN, enhanced results are obtained.

VII. REFERENCES

[1]. Tønnesen, A. (2004). Mobile ad-hoc networks. Courtesy of http://www. olsr. org/docs/wos3-olsr. pdf.

[2]. Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1), 1-22.

[3]. Subbaiah, K. V., & Naidu, M. M. (2010). Mobile Ad Hoc Network. Simulation, 1(04), 246-251.

[4]. Royer, E. M., & Perkins, C. E. (2000). An implementation study of the AODV routing protocol. In Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE (Vol. 3, pp. 1003-1008). IEEE.

[5]. Chakeres, I. D., & Belding-Royer, E. M. (2004, March). AODV routing protocol implementation design. In Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on (pp. 698-703). IEEE.

[6]. Royer, E. M., & Perkins, C. E. (2000). An implementation study of the AODV routing protocol. In Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE (Vol. 3, pp. 1003-1008). IEEE.

[7]. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks, 22(5), 1505-1511.

[8]. Abdelshafy, M. A., & King, P. J. (2016, January). Resisting blackhole attacks on MANETs. In Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual(pp. 1048-1053). IEEE.

[9]. Biswas, S., Nag, T., & Neogy, S. (2014, February). Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In Applications and Innovations in Mobile Computing (AIMoC), 2014 (pp. 157-164). IEEE.

[10]. Yen, Y. S., Chan, Y. K., Chao, H. C., & Park, J. H. (2008). A genetic algorithm for energy-efficient based multicast routing on MANETs. Computer Communications, 31(10), 2632-2641.

[11]. Sahin, C. S., Urrea, E., Uyar, M. U., Conner, M., Hokelek, I., Conner, M., ... & Pizzo, C. (2008, July). Genetic algorithms for self-spreading nodes in MANETs. In Proceedings of the 10th annual conference on Genetic and evolutionary computation(pp. 1141-1142). ACM.

[12]. Sahin, C. S., Urrea, E., Uyar, M. U., Conner, M., Hokelek, I., Conner, M., ... & Pizzo, C. (2008, July). Genetic algorithms for self-spreading nodes in MANETs. In Proceedings of the 10th annual conference on Genetic and evolutionary computation(pp. 1141-1142). ACM.

[13]. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5).