Mitigation of Blackhole Attack on MANETs using ABC and ANN Algorithm

Tanmaya Kharyal, C. Rama Krishna

Abstract: Mobile ad hoc network (MANET) is an important field of research that comprises of moveable nodes. These nodes communicate with each other through wireless links. Therefore, it becomes essential to design a secure network as it finds applications in different fields where data and communication are important like that in defense areas and disaster rescue operations. This paper focuses on detecting Blackhole nodes in MANETs and preventing it from the same. In this work, Ad hoc On-Demand Distance Vector (AODV) is employed as a routing mechanism and a secure network is established using Artificial Bee Colony (ABC) algorithm as an optimization technique in combination with Artificial Neural Network (ANN) as a classification algorithm to identify the Blackhole nodes. Simulations are carried out in MATLAB and the efficiency of the network in terms of Throughput, Packet Delivery Ratio (PDR), End-to-End Delay and Energy Consumption are measured. Throughput and PDR have been increased by 11.11%, 4.9 %, whereas end- to- end delay has been reduced by 4.93% as compared to existing work proposed by Ashish et al.[6].

***Index Terms*: MANET, Blackhole node, AODV, ABC, ANN.**

I. INTRODUCTION

MANET is a peer-to-peer (p2p), a self-motivated, autonomous, multi-hop network [1] which performs operation by sharing their information among the network nodes [2]. These operations require competing nodes to participate in a trusted manner. The data is transmitted from source node to destination node using routing protocols. In MANET routing can be performed in three different ways (i) Proactive (ii) Reactive and (iii) Hybrid. In this paper, the route is formed using a reactive routing protocol i.e. AODV. The advantage of using the AODV routing protocol is that it utilizes the less congested path instead of the shortest path [3]. AODV selects the path through the node that consumes less energy and has higher capacity. Since in MANET the nodes are mobile, there is a frequent change in topology due to which finding the route becomes a complex process. AODV responds well in this situation. It works well for longer traffic as compared to other existing routing protocols. The created route might be expired due to the mobile nature of nodes [4]. As the network size increases, different performance metrics begin to decline. AODV is based on the likelihood that the nodes are co-operating and based on their co-operation, AODV establishes the route. That is why AODV is exposed to various types of attacks as it is designed without security mechanism. The general description of AODV and Blackhole attack is described in the subsequent section.

Revised Manuscript Received on July 05, 2019.

Tanmaya Kharyal, Department of Computer Science and Engineering, NITTTR, Chandigarh, India.

C. Rama Krishna, Department of Computer Science and Engineering, NITTTR, Chandigarh, India.

A. AODV

AODV is an on-demand routing mechanism that establishes route when communication begins. In case of a change in the communication link, the sequence number of each node is auto incremented by 1 unit. Sequence number helps to determine the data type whether it is new or old. The route discovery process is displayed in figure 1.

Source node 'S' starts broadcasting RREQ message when it wants to communicate with the destination node. The nearby nodes denoted by node 1 and node 3 depicted in figure 1 receive the RREQ data. Node 1 and Node 3 check for the new route as well as check for the repeated RREQ. If the request already exists, then it is discarded. In case if node 1 and node 3 have a valid route to the destination then the nodes send RREP to the source node. In case if the route is not found in the neighbouring node route table, the neighbouring node again broadcasts RREQ message. In this way, the route between source and destination is created. In case if a node receives a number of RREQ, then it selects those RREQ which has the highest sequence number. In the case of identical RREQ, the node selects the RREQ with the lowest hop count [13].

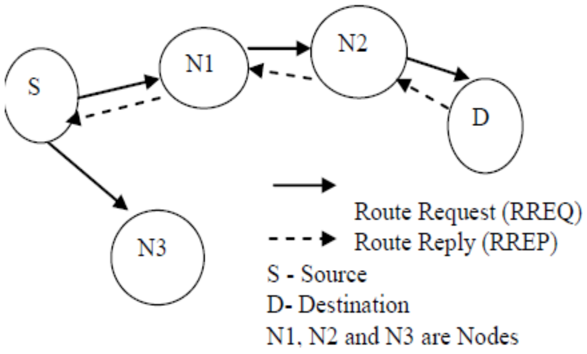


Fig. 1 AODV Routing Mechanism

B. Blackhole Attack

It is the most common attack present in MANET. When the network is under this attack, the Blackhole node also receives RREQ message broadcasted in AODV routing protocol. After receiving RREQ, it instantly sends back an RREP message with the highest sequence number. On receiving RREP message, legitimate node considers it as a neighbouring node to create the route and sends all data through this node. In this way, the Blackhole node absorbs all the packets and drops the throughput of the network.

Figure 2 shows the scenario in the presence of the Blackhole attack. Here 'B' represents the Blackhole node with the highest sequence number i.e. 4929200 and lowest hop count. In response to RREQ request from the source node, 'B' sends RREP acknowledgement to the source node and takes the control of data transmission by creating a route between source node S and node N3 through node B which in return drop all the data packets [4].

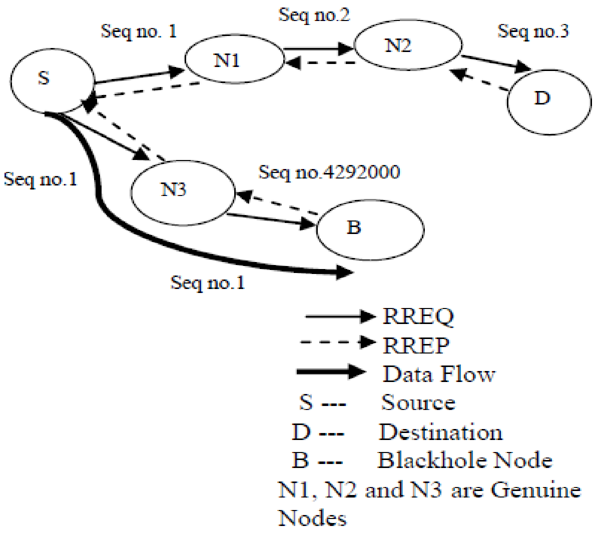


Fig. 2 Illustration of Blackhole Attack

The Blackhole node can distort the network and decrease the data transmission rate. The node affected by the Blackhole attack consists of the highest sequence number with shortest path information and behaves like a genuine node. It attracts the data traffic and drops the packet delivery rate [5]. This research work presents an artificial intelligence technique with an optimization scheme to secure MANET from Blackhole attack.

This paper presents a basic introduction required for the proposed work in section I, the related work is discussed in section II, the techniques used for the prevention of Blackhole attack is demonstrated in section III. The proposed work is described in section IV. Section V includes the description of simulation work along with the comparative analysis. The concluding remarks are presented in section VI.

II. RELATED WORK

This section illustrates the existing work done in the field of detection and mitigation of Blackhole attack in MANET. It highlights the survey, mechanism, working, benefits and limitations of existing literature.

Ashish et al. [6] introduced a Fuzzy model which is based on the weighted binary relationship to lessen the consequence of Blackhole attack in MANET that used AODV routing protocol. Fuzzy logic as a classifier has been used to differentiate between the genuine node and attacker node. The major drawback of Fuzzy Logic is that it works on a rule set. Therefore, if we have a network comprising of large number of nodes, then we need to define large number of rules which are impossible to create and becomes complex for the developer. Chhabra et al. [7] designed a secure fuzzy potential threat protocol that utilized to fight against Blackhole attack in OppNets. In this scheme, a rank list of nodes has been created to make a decision regarding as to which node the data has to be transmitted. However, this process is very much time consuming as well as requires more storage space. To enhance the speed as well as the detection rate, Abdel-Azim et al. [8] proposed a model by utilizing the GA based optimization algorithm in addition with two classifiers named as Fuzzy and Neural Network. The test result has been demonstrated that the PDR of the network is increased when optimization and classification techniques are used in combination than that of the PDR without any technique.

Author Rao et al. [9] has focused on the reduction of false replies that came from the malevolent nodes by using the cache algorithm. The above-mentioned existing works have focused on only for the detection of Blackhole attack node. Panda et al. [10] have worked for the detection as well as to minimize the side effect of the gray hole and Blackhole attack in MANET by implementing a new technique named as Ant Colony Optimization (ACO). The purpose of this technique is to determine the shortest route from transmitting node to the target node based on the energy consumption rate. In the same field, the effect of clustering has been presented by Patel et al. [11] that helps to form a cluster head which controls over the whole network. The authors have used 32 numbers of nodes that are divided into three clusters based on energy absorbed by every communicating node. The node that has a maximum level of energy is used as Cluster Head (CH). To enhance efficiency of the network in case of malicious node a trust value has been generated that helps to boost the throughput of the network.

After studying the above papers in the field of detection and mitigation of Blackhole attack in MANET, it has been observed that the various researchers have used fuzzy logic method to detect the Blackhole attack or other attacks present in the mobile network. Since the fuzzy logic works on the rule set theory, therefore, to detect malicious node in a large network area it becomes difficult to create a number of rules, which further requires large memory space to store these rules. ACO technique is used as an optimization algorithm to reduce the effect of attacks (gray hole and Blackhole) in the network. After applying this technique in the network it has been determined that, the coverage time is large for the large network area. Hence, in this paper, the concept of Artificial Intelligence i.e. ANN along with ABC is used to classify the attacker nodes and as optimization algorithm respectively. The detailed description is provided in the following section.

III. TECHNIQUES USED

In this research to mitigate the effects of Blackhole attack ANN as a classification algorithm and ABC as an optimization algorithm is used. The detail description is provided in the following.

A. ABC Algorithm

To enhance the data transmission rate and detect the Blackhole node, an optimization scheme ABC is used. The ABC algorithm is a swarm inspired meta heuristic-based algorithm that has been developed by Dervis Karaboga in 2005 [14] and was used to resolve complex numeric problems. This algorithm works on a similar model as introduced by "Tereshko & Loengarov" in 2005 [14]. This model replicates the collection and selection of food as done by honeybee colonies. ABC algorithm mainly consists of three important components: employed foraging bees, unemployed foraging bees, and food sources. In the initial phase, the location of the food source is found out by scout bees, after that the quality of gathered food is analyzed by comparing it with the food already collected by the onlooker bee. If the quality of food is good compared to the existing food then that food is considered otherwise rejected [14]. In this work, the optimal nodes of the network (based on energy consumption and delay) would act as Employed Bees.

B. ANN

ANN is an artificial intelligence technique that is used to resolve the complex pattern problem by using the concept of the human brain. ANN includes different elements that work in parallel mode. ANN mainly works with weight. Initially, ANN generates a random guess for the present problem. Then the network searches for the desired result and makes adjustment of weight accordingly [15]. In this work, the optimized features of the nodes are provided as an input to the input layer of ANN, which the neural network learns through epochs in order to classify the Blackhole nodes from genuine nodes.

IV. PROPOSED WORK USING ABC AND ANN ALGORITHM (AB_NN)

It is observed that previous researches have mostly used fuzzy logic, which works on the rule set theory. Due to which it becomes tedious and difficult to create a number of rules for larger network area. Hence, the proposed methodology has used an on-demand based AODV routing protocol in combination with ABC and ANN approach. The AODV routing protocol only recommends the route for the data transmission without knowing about the nature of node i.e. genuine or attacker node. Therefore, for the detection of the nature of node ANN is used. In ANN, the optimal features of the nodes are provided as input in order to find out the attacker node. To separate the properties of the nodes ABC algorithm is applied which uses a fitness function that creates a list of features of the genuine node. These lists of features are the input to the ANN. This approach helps to identify and remove the Blackhole nodes that exist during the communication process. The steps followed are explained in the following:

i. Initially, the mobile network with height and width of 1000m ×1000m is designed using data acquisition tool in MATLAB.
ii. Initialize *n* number of sensor nodes within the mobile network that is moving with particular velocity.
iii. The coverage areas of each node to which the mobile nodes are able to exchange information with other nodes are specified along with the transmitting and receiving nodes.
iv. Create a path between source nodes and sink node by using AODV as a routing protocol.
v. Examine the efficiency of the network based on computation parameters. If the performance of the network is significantly low, it indicates the presence of the Blackhole attack in the mobile network.
vi. Apply ABC as an optimization algorithm to optimize the route by using following fitness function:

$$FitnessFunction, fit(x) = \begin{cases} True\ (E_{bee}), & E_{bee} > O_{bee} \\ False\ (O_{bee}), & E_{bee} \leq O_{bee} \end{cases}$$

ABC extracts the features of each node based on energy absorbed by the node and delay. These optimized features are provided as an input to the neural network, which compares these extracted features with the genuine node features. If the features are not matched, then it indicates that the node as an attacker node and change the path between the source and destination node.
vii. At last, the performance is measured in terms of computation parameters and compared with the existing work performed by author Ashish et al. [6].

The proposed algorithm AB_NN, which is a combination of ABC with ANN algorithms, is described in the following section. The input to the proposed algorithm is the node properties (energy consumption, delay, co-ordinates) based on which nodes are distinguished as genuine or attacker nodes. The output of this algorithm is the detected Blackhole nodes. The functions of ABC, such as employee bee, onlooker bee and scout bee are defined. These bees are actually the information related to the node. The node that consumes less energy with minimum delay is selected by the onlooker bees. The node with best features are stored into an array. The process is repeated for the entire communicating nodes within the network and hence a list of optimized nodes (that satisfies the fitness function) or the attacker nodes (do not satisfy the fitness function) is created. Based on these properties ANN is trained along with other parameters such as epoch, neurons, Mean Square Error (MSE) and Mutation. If the properties of the node are matched with the stored properties in ANN then the node is considered as genuine node otherwise considered as attacker node.

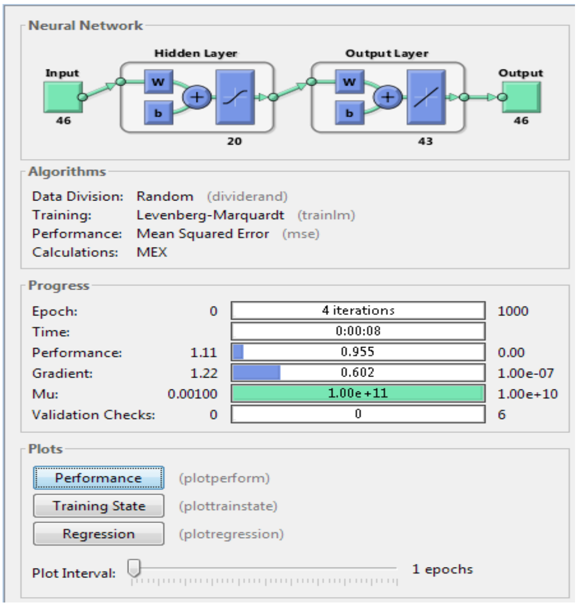
Algorithm: AB_NN

```
ABC:
Input: Properties of nodes (energy consumption, delay, co-ordinates)
Output: Optimized nodes feature
Initialize algorithm with their function – Employ Bee ($E_{bee}$), Onlooker Bee ($O_{bee}$), and Scout Bee ($S_{bee}$)

Define the fitness function,
$FitnessFunction, fit(x) = \begin{cases} True\ (E_{bee}), & E_{bee} > O_{bee} \\ False\ (O_{bee}), & E_{bee} \leq O_{bee} \end{cases}$

Create empty array for storing optimized feature, $ABC_{data}$ = []
Count = 0
Feature = Nodes properties
Calculate rows (R) and columns (C) = Size ($E_{bee}$)
For i = 1 to R
    For j =1 to C
        $E_{bee}$ = Feature (i, j)
        $O_{bee}$ = Average (Feature)
        Fit_bee = $fit(E_{bee}, O_{bee})$
    $ABC_{data}$ (i, j) = Fit_bee
    End
End
ANN:
Training Data (T) = $ABC_{data}$
Initialize ANN with parameters;
        – Epochs (E)
        – Neurons (N)
        – Performance parameters: MSE, Gradient, Mutation
        and Validation Points
        – Training Techniques: Levenberg-Marquardt
        (Trainlm)
Training data= Optimize_data
Group = Real and Attacker node
Epoch=1000
Neurons=50
Net=newff(Trainingdta, group, neuron)
Net= Train (net, training data, group)
Classification= considered as Blackhole node if properties are not matched
                                Otherwise genuine node
  Return Blackhole node
```

The optimized features of nodes (energy consumption, location x and y co-ordinates, delay) that are optimized by the ABC algorithm are used to train ANN. In this research, ANN is used to classify the Blackhole node from the legitimate node and hence secure the network. Figure 3 represents the structure of ANN used for the detection of Blackhole attack. The ANN structure used in this paper comprises of three layers with different neurons: the input layer (46 input), hidden layer (20 neurons), and the output layer (43 neurons). The number of neurons in hidden layer are selected in such a way (hit and trial) so that no overfitting and underfitting occurs in the neural network. Further, the number of neurons in the output layer get adjusted automatically according to that in hidden layer. The neurons are adjusted at the hidden layer by applying a bias voltage. The bias is applied in such a way so that the desired output can be obtained.



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	4 iterations	1000
Time:		0:00:08	
Performance:	1.11	0.955	0.00
Gradient:	1.22	0.602	1.00e-07
Mu:	0.00100	1.00e+11	1.00e+10
Validation Checks:	0	0	6

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)

Plot Interval: 1 epochs

Fig. 3 Structure of ANN

V. RESULTS AND DISCUSSIONS

The network is designed with 50 numbers of nodes and the experiments are conducted in a MATLAB tool with the input as listed in table 1. To analyze the results appropriately, simulations are done a number of times where Blackhole nodes are selected randomly. Due to the random selection, Blackhole nodes varied between 10% to 80%.

Table 1 Input Parameters

Area	1000 m^2
Total number of Nodes	50
Transmission Range	250m
Packet Size	1000
Number of Malicious Nodes	Random Selection

In this work Neural Network Toolbox is used in MATLAB to construct and train ANN in order to classify the genuine and Blackhole nodes.

The parameters that are measured during the simulation process are defined below:

i. Throughput: It is defined as the total number of packets delivered to the receiver side with respect to the total simulation period.

ii. End- to-end delay: It is defined as the time required by the transmitted message to reach the receiver side. The delay includes the time like buffering time, route discovery time and transmission time.

iii. Energy Consumption: The energy like utilization of battery during the transmission of data, processing of data as well as when the nodes are idle with respect to the initial energy provided to the nodes. This must be small for a successful communication network.

iv. Packet delivery ratio (PDR): It is the ratio of delivering the data packet to the receiver to that of total packets generated by the source node.

Figure 4 demonstrates the average throughput computed during simulation of 50 number of sensor nodes within the network. The throughput in the simulation work has been measured in the presence of the attack and when the network is prevented from the Blackhole attack. The percentage increase in the throughput measured after preventing the network from Blackhole attack using the proposed algorithm AB_NN is11.11% as compared to Fuzzy interface used by Ashish et al. [6] network. From Figure 4, it is seen when the Blackhole nodes are in the range 10% - 50 %, the throughput of the proposed AB_NN model is increased with a very small variation as compared to the existing work presented by Ashish et al.[6] Model. With the increase in the percentage of Blackhole nodes, the throughput has been increased significantly and the largest difference is determined at 70% of Blackhole nodes.

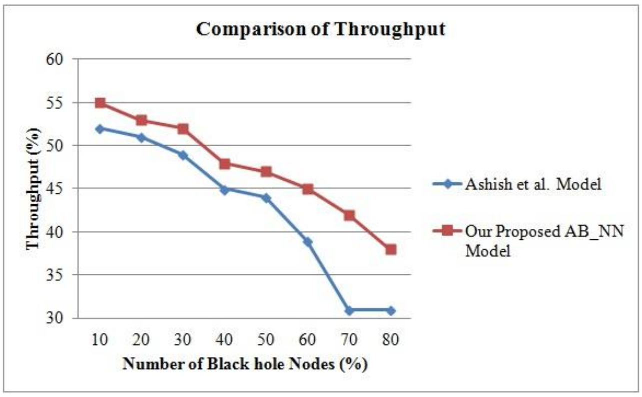


Fig. 4 Throughput Comparison of AB_NN with Ashish et al. Model

The PDR of the proposed work along with existing work proposed by Ashish et al. is depicted in fig. 5. The graph plotted between PDR and the number of Blackhole nodes represent that with the increase in the percentage of Blackhole nodes the packets delivered to the network decreases. The average value of PDR for the AB_NN model as well as for the existing work measured is 63.87 % and 67% respectively. Thus, there is an enhancement of 4.67 % while AB_NN algorithm is used. From the fig., it is clear that PDR remains constant up to 20% of Blackhole node and then decreases sharply above 20% of Blackhole nodes within the network. This is due to the rigorous dropping of data packet done by the Blackhole nodes.

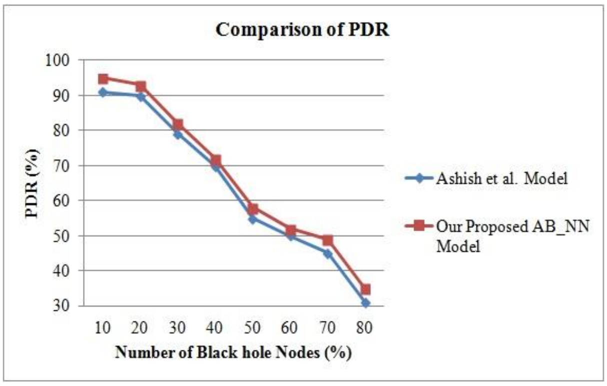


Fig. 5 PDR Comparison of AB_NN with Ashish et al. Model

Fig. 6 represents the graphical illustration of end-to-end delay measured for AB_NN model and existing work. From the graph, it is observed that as the percentage of Blackhole nodes increases the delay in the data packet delivery also increases. The average percentage of end-to-end delay measured during the experiment for the AB_NN model as well as for the existing work is 31.25% and 32.87% respectively. Therefore, the delay has been reduced by 4.93 % of the existing work. The delay analyzed from (10% to 30%) of Blackhole node is less, and from 30 % to 70 % of the Blackhole node the delay is similar to that of Ashish et al. model. This reflects that end-to-end delay remains more or less the same as compared to Ashish et al. model.

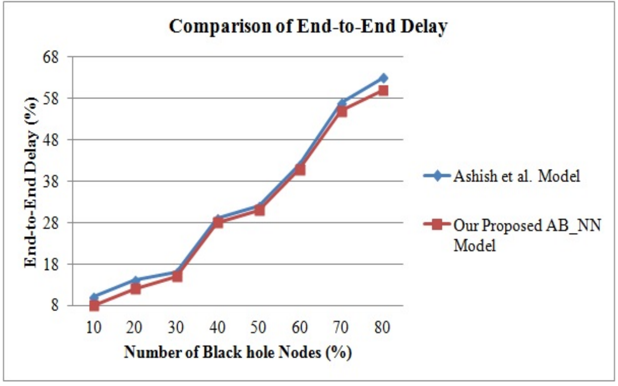


Fig. 6 End-to-End Delay of AB_NN with Ashish et al. Model

The additional parameter of energy consumption is measured by simulating the AB_NN model in five rounds. The values of energy consumption measured with and without prevention algorithm are shown in figure 7. The average value of energy consumed by nodes without prevention algorithm and with prevention algorithm is 53.37 J and 44.91 J respectively, which is an enhancement of 15.85 % while preventing the network from Blackhole attack. This signifies that Blackhole nodes when present in the network consumes lot of energy and hence preventing the network from Blackhole attack, energy is also saved.

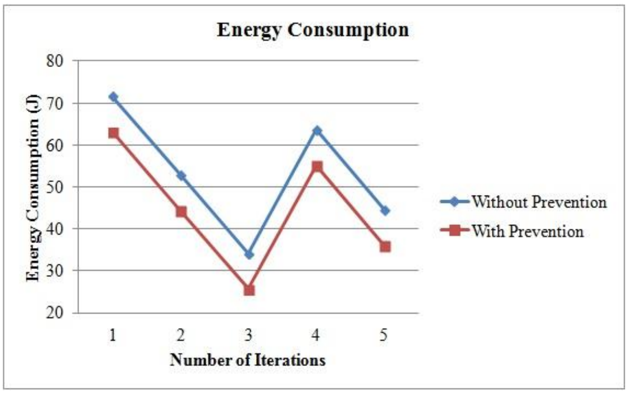


Fig. 7 Energy consumption of AB_NN model

VI. CONCLUSIONS

Secure communication is a key requirement for any communication network. The communication through air medium (wireless communication) creates additional security threats. MANETs being self-configuring with mobile devices increases the security threats on the network.With huge increase in cyber-attacks, security of MANETS are at an indispensable stage. Blackhole attack is one of the most notorious attacks present in MANETs. To prevent the network from Blackhole attack a security system has been presented by utilizing the concept of artificial intelligence (ABC and ANN). In existing research, it was observed that most of the authors have used fuzzy logic as a machine learning technique that results in the heavy calculation, as it requires number of rule sets and large storage space. To overcome these problems and to provide a secure network from the Blackhole attack, ABC along with ANN is used (AB_NN model). ABC optimizes the route created using AODV routing protocol and ANN classifies the node as genuine or malicious one. From the experiment, it has been analyzed that AB_NN performs well in terms of PDR (%), throughout (%) and end-to-end delay(%). The percentage increase in the PDR and Throughput from the existing work is about 4.9% and 11.11% respectively, while the percentage reduction in end-to-end delay of about 4.93%. Hence, resulting in a significant increase in the throughput of the network.

REFERENCES

1. Z. Li and Y. Wu, “Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs,” in *IEEE Communications Letters*, vol. 21, no. 7, pp. 1529-1532, July 2017.
2. Y. Fang, Y. Zhou, X. Jiang and Y. Zhang, “Practical Performance of MANETs Under Limited Buffer and Packet Lifetime,” in *IEEE Systems Journal*, vol. 11, no. 2, pp. 995-1005, June 2017.
3. L. Wang and S. Olariu, “A Two-Zone Hybrid Routing Protocol for Mobile Ad hoc networks,” in *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 12, pp. 1105-1116, Dec. 2004.
4. B. Singla, A. K. Verma, and L. R. Raheja, “Preventing Blackhole Attack in AODV Routing Protocol using Dynamic Trust Handshake-based Malicious Behavior Detection”, *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*, 258, 2019.

5. Q. M. Yaseen, and M. Aldwairi, “An Enhanced AODV Protocol for Avoiding Blackholes in MANET”, *Procedia Computer Science*, vol. 134, pp. 371-376, 2019.
6. Ashish., Tokekar V. and Shrivastava S., “Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Blackhole Attacks”, in *Information and Communication Technology*, pp. 39-47, Springer, Singapore, 2018.
7. A. Chhabra, V. Vashishth, and D. K. Sharma, “A fuzzy logic and Game Theory based Adaptive Approach for Securing Opportunistic Networks Against Blackhole Attacks”, *International Journal of Communication Systems*, vol. 31, no. 4, pp. 3487-3510, 2018.
8. M. Abdel-Azim, H. E. D. Salah, and Eissa, “IDS Against Black-Hole Attack for MANET”, *International Journal of Network Security*, vol. 20 no. 3, pp. 585-592, 2018.
9. R. L. Rao, B. Satyanarayana, and Kondaiah, “Performance of CBIDS on AODV Routing Protocol against Blackhole attacks in MANET”, *International Journal of Scientific Research in Computer Science and Information Technology*, vol. 3, no. 3, pp. 1637-1644, 2018.
10. N. Panda, and B. K. Pattanayak, “Energy aware detection and prevention of blackhole attack in MANET”, in *International Journal of Engineering and Technology (UAE)*, vol. *7,* no. 26, pp. 135-140, 2018.
11. N. J. K., Patel, and K.. Tripathi, “Trust Value based Algorithm to Identify and Defence Gray-Hole and Black-Hole attack present in MANET using Clustering Method”, *IJSRET*, vol. 4, no.4, pp. 281-288, 2018.
12. P. Priya, S. Reddy, H. D. Sushma, S. Vaishnavi, and M. M. Nayak, “Enhanced Performance and Security for Manet’s Against Blackhole Attack Blackhole Attacks”, in *3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics*, pp. 80-87, 2018.
13. P. Gupta, P. Goel, P. Varshney, and N. Tyagi, “Reliability Factor Based AODV Protocol: Prevention of Blackhole Attack in MANET”, in *Smart Innovations in Communication and Computational Sciences*, pp. 271-279). Springer, Singapore, 2019.
14. M. V. Anand & S. Hariharan, “Bee-mimetic DSR Based Secure Routing in MANET using Artificial Bee Colony Optimization”, *International Journal of Pure and Applied Mathematics*, vol. 119, no. 17, pp.1337-1350, 2018.
15. R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, & K. M. Koumadi, “Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)”,Journal of Computer Networks and Communications, 2019.

AUTHORS PROFILE

Tanmaya Kharyal , M.E, Department of Computer Science, NITTTR, Chandigarh

Dr. C Rama Krishna, Ph.D. from IIT Kharagpur, M.Tech. from CUSAT, Cochin B.Tech. from JNTU Govt. College of Engg., Anantapur