A SECURED SYSTEM AGAINST BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK USING ARTIFICIAL INTELLIGENCE TECHNIQUE

Arpit Bakshi

Assistant Professor Department of Computer Science & Engineering ,
Vedant College of Engineering & Technology ,Bundi, Rajasthan (India)

ABSTRACT

This research deals with a common approach for the detection and mitigation of black hole attack in MANET that because of the mobility and nature broadcasting are generally susceptible for the attacks as compared to the existing wired network. Particularly, black hole attack could be easily be deployed by an adversary. Black hole attack is one of the well known security threat occurs in MANET. A black hole attack occurs due to malicious nodes that attract the data packet by addressing a false route. In the research work, AODV (Ad hoc network) routing protocol has been used. Cuckoo search optimization algorithm has been used for optimizing the route from source to destination. ANN (Artificial neural network) is used for the detecting and preventing the network from black hole attack. The simulation is being carried in MATLAB simulator and the performance has been calculated by means of performance parameters, namely, Throughput, Delay, BER (Bit error rate) and energy consumption.

Keywords: ANN (Artificial neural network), AODV routing protocol, black hole attack, Cuckoo search algorithm, MANET

I. INTRODUCTION

Mobile Ad-hoc system is known as a system, in which the communication happens in remote medium utilizing an access point. Restricted to the framework of remote systems where every client straightforwardly corresponds with base station or access point, mobile specially appointed system namely, MANET, which is a type of remote Ad-hoc network [1]. It is a system of self-arrangement of movable routers connected by remote connections with no entrance point. Each movable device in a system is self-governing as the presence of no middle authority is there in the MANET. Each device can move separately freely in all the directions. The main aim in developing a MANET is carrying each device for continuously maintaining the information required to accurately route the traffic [2]. Mainly two topologies are used in MANET named as Ad-Hoc topology and Infrastructure topology. Ad-hoc network is a compilation of nodes or routers which exists dynamically with no utilization of existing network. Ad-hoc wireless network can also be regarded as more decentralized wireless network. It is one of the simplest forms of wireless communication network. In the Ad Hoc network, the router can smoothly performs network standard that results to change topology quickly and are hard to predict. In this topology, the devices are connected through wireless LAN named as Service Set Identifier (SSID).

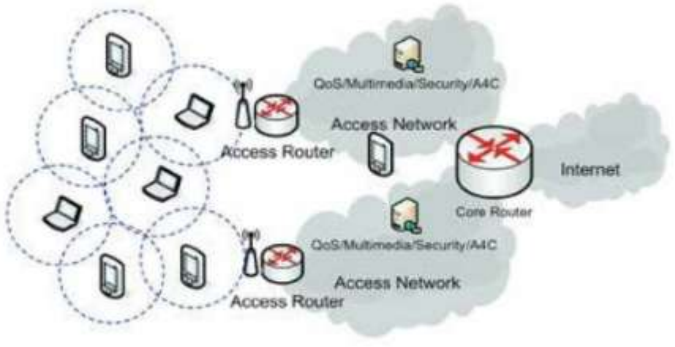

Fig.1: MANET (Mobile Ad hoc network)

All the computers or the communicating devices are connected to the same SSID then formed a network known as infrastructure network. The network topology formed by the infrastructure network is star topology [3].

The aim of this research work is to analyze and mitigate the black hole attack using AODV routing protocol. Cuckoo search optimization algorithm and ANN (Artificial neural network) has been used for the same. The performance of the research work has been calculated by different parameters, like, throughput, BER (bit error rate), delay and PDR (Packet delivery ratio).

II. MATERIAL AND METHODS

This research has developed a novel algorithm using trust model and cuckoo search algorithm. For the mitigation the effects of black hole attack, fuzzy logic has been used.

2.1 Cuckoo Search Algorithm

Cuckoo search algorithm is developed as a Meta-heuristic approach with an inspiration of bird cuckoo. This bird never makes its nest and usually lays the eggs in other bird's nest. Few host birds may engage straight with the intruding cuckoo [4]. If the host bird finds the eggs which are not even their egg than it throw the eggs from the nest or relieve its nest or make a new nest. In the nest, every egg shows a solution and cuckoo egg depicts a novel and better solution. The solution being obtained is a novel solution on the basis of existing solution with some amendments in the characteristics. Cuckoo search is utilized for solving the scheduling issues and for solving the design optimization issues in structural engineering. Cuckoo search admires the breeding behaviour and may be developed for different optimization problems as mentioned below [5]:

i. Every cuckoo lays single egg at one time and deposits it to an arbitrarily selected nest.

ii. The better nests having high egg quality would take to the subsequent generation.

iii. There are fixed number of accessible host nest and if a host birds finds the cuckoo egg having probability of pa=[0,1] then the bird may throw or abandon them and generate a novel nest.

Cuckoo search Algorithm

```
Begin
Objective function g(x), x=(x1, x2 ... xt) M
Produce initial population for n number of host nest xi (i=1, 2... n)
While (m<Max Generation) or (halt criteria)
        Obtain a cuckoo arbitrarily
        Execute its fitness Gi
        Decide a nest between n arbitrarily
                If (Gi< Gj)
                Change j with novel solution
                End if
A fraction of inferior nest is discarded and novel ones are developed
Keep the better solutions
Rank the solution and evaluate the solution and existing best
End while
        Post process results
End begin
```

2.2 Fuzzy logic

Fuzzy logic is based on the standard form of right or wrong, realism rather than modern computers based (1 or 0) Boolean logic calculations. Natural language (like most other life activities or even the universe) is not readily converted to the absolute value of 0 and 1 [6]. This can be useful as a way to see the fuzzy logic inference real job, binary or Boolean logic is a special case. Fuzzy logic as 0 and 1, includes an extreme case of truth (or 'state of things' or 'truth'), but also includes a variety of real estate in the middle, so that, for example, the comparison results between the two things cannot be ‘high or 'short’, but ‘high’. Fuzzy logic works as the human brain works. Fuzzy logic is for the development of human capabilities with AI (Artificial Intelligence) requirements and generates the representation of human cognitive abilities in software [7].

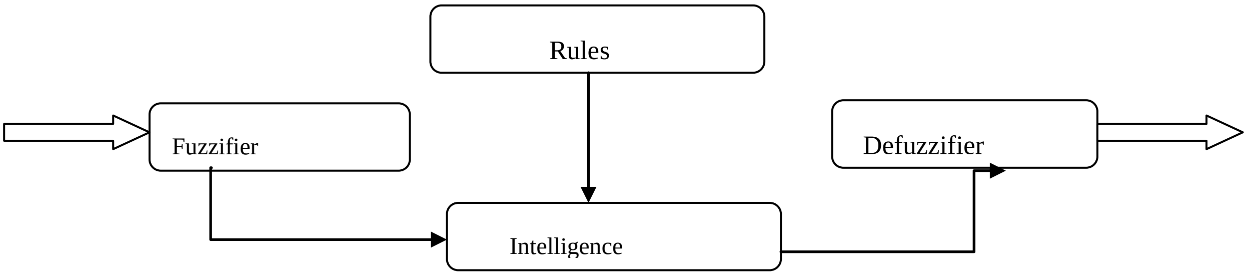

Fig.2: Fuzzy logic system

Fuzzy logic algorithm

```
Describe the linguistic terms and variables (Initialization)
Develop the membership function (initialization)
```

Develop the rule base (initialization)

Change the crisp input data to fuzzy value by utilizing membership function (fuzzification)

Calculate the rules in the rule base (Inference)

Integrate the outcome of every rule (Inference)

Change the output data to non-fuzzy values (de-fuzzification)

III. BLACK HOLE ATTACK

Black hole attack is considered as a type of DoS (Denial of Service) attack in which a malicious node may attract the packets by wrongly claiming a new route to the destination and later absorbs the nodes without sending them towards the destination [8].

On the below figure, a malicious node has been imagined named as ‘MN’. When a node B sends a RREQ packet, the node D, A, MN accepts it. Node MN as a malicious node doesn’t verify with the routing table for the requested route towards node C. Therefore, it abruptly transfer back RREP packet, maintaining RREP from MN ahead of RREP from D and A.

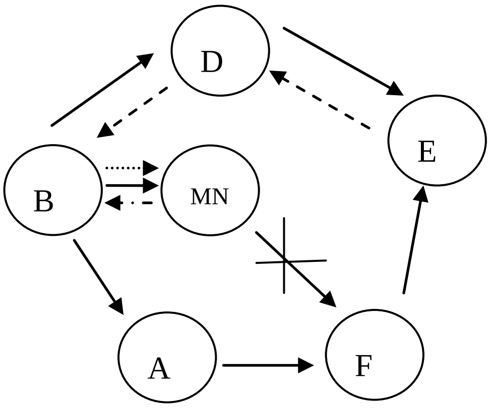

Fig.3: Black hole attack

In the above figure, node B assumes that the route via MN is the shortest route and transfers some packet towards the destination. When the node B transfers the data to MN, it takes the data and therefore, behaves as a black hole. The researchers have presented solutions for identifying a single black hole node. Though, in that solution next hop also act as a malicious node that cannot be identified [9].

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 Cuckoo search optimization algorithm and ANN (Artificial neural network) in MANET network.

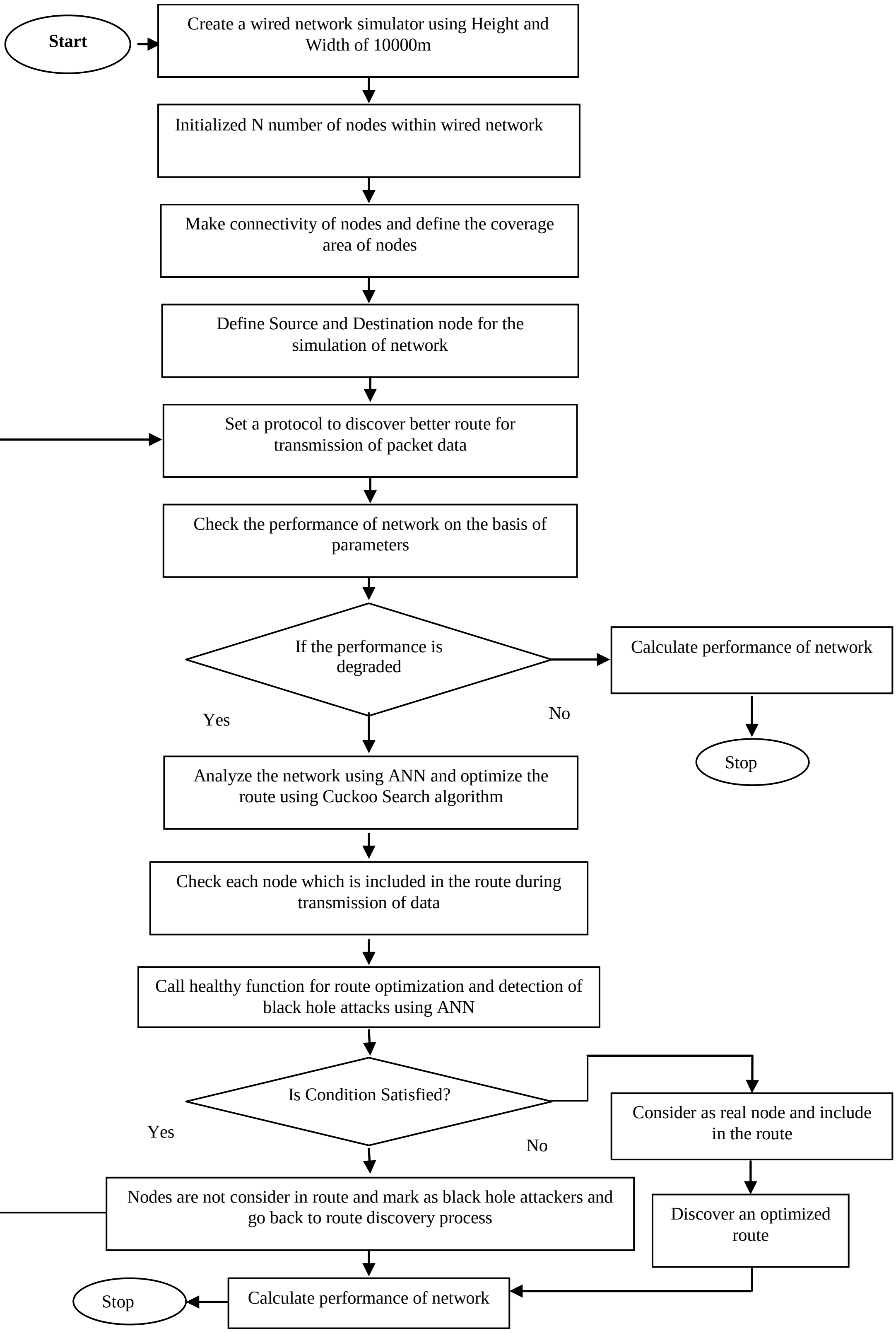
Start
Create a wired network simulator using Height and Width of 10000m
Initialized N number of nodes within wired network
Make connectivity of nodes and define the coverage area of nodes
Define Source and Destination node for the simulation of network
Set a protocol to discover better route for transmission of packet data
Check the performance of network on the basis of parameters
If the performance is degraded
Yes
No
Calculate performance of network
Stop
Analyze the network using ANN and optimize the route using Cuckoo Search algorithm
Check each node which is included in the route during transmission of data
Call healthy function for route optimization and detection of black hole attacks using ANN
Is Condition Satisfied?
Yes
No
Consider as real node and include in the route
Nodes are not consider in route and mark as black hole attackers and go back to route discovery process
Discover an optimized route
Stop
Calculate performance of network

Fig.4: Simulation Model

Step 1 : Then, Cuckoo search optimization algorithm is initialized for route discovery and for finding the better route selection as per the coverage set.

Step 2 : The healthy function has been defined for cuckoo search algorithm according to the requirement of networks.

Step 3 : After the discovery of route from the source and the destination calculated the performance parameter of the network and if the parameters id degraded then classify the attacker using ANN.

Step 4 : On the basis of attacker's activities, the kind of attacker is being checked and the attacker performance is being calculated for achieving the best results.

Step 5 : Parameters, namely, Delay, throughput, BER and energy consumption has been calculated to check the performance of the proposed work and compare with the existing work to verify the proposed work.

V. SIMULATION RESULTS

This section describes the results obtained after the simulation of the proposed work. Parameters, Delay, throughput, BER and energy consumption have been calculated. The explanation for the same is given below:

i. Throughput

It is described as the total number of packets transferred in the simulation time. It is the sum of total data transmitted from source to destination in an appropriate time span. Throughput can be calculated in terms of Mbps, Kbps and Gbps and generally denotes in percentage (%). Throughput can be described as:

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

ii. Delay

It is referred as the time taken for a packet data to be transferred over a network from source node towards destination node. Therefore, usually those routes are used in the network that has less probability of delay for the better performance of the proposed work. Mathematically, delay can be explained as below:

$$Dend - end = Dtrans + Dprop + Dproc$$

$$Where\ Dend - end = End - To - End\ Delay$$

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

iii. BER (Bit Error rate)

It is described as the rate via which the errors exist in the transmission system. This may be explicitly translated occur in the string with the mentioned number of bits. It can be explained mathematically as shown below:

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

iv. Energy Consumption

It is defined in as total energy consumed by a network during the transmission of packet data from the source node to the destination node. It can be calculated in Joules. Mathematically, it can be defined as:

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

Where, 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

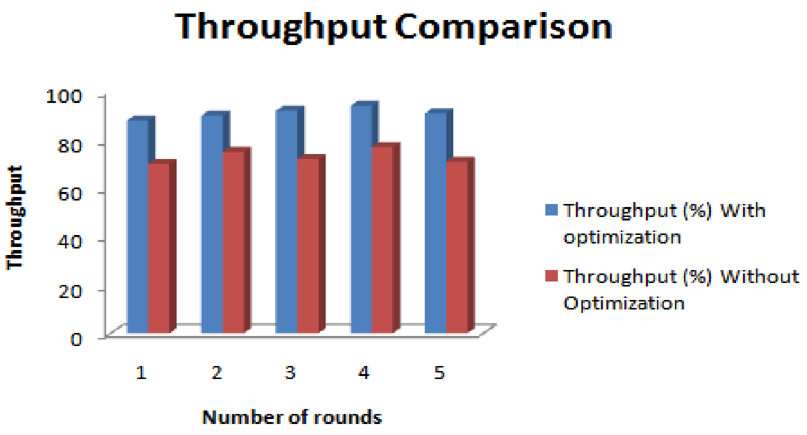

Fig.4 Comparison of throughput for with and without optimization

Above figure represents the comparison for throughput for with (Cuckoo and ANN) and without optimization. X-axis in the above graph is for number of rounds and Y-axis represents throughput values obtained. Blue bar in the graph is for throughput with optimization and red bar represents the values without optimization. The average value obtained for with optimization is 91 and for without optimization it is 73. Throughput has been measured in percentage.

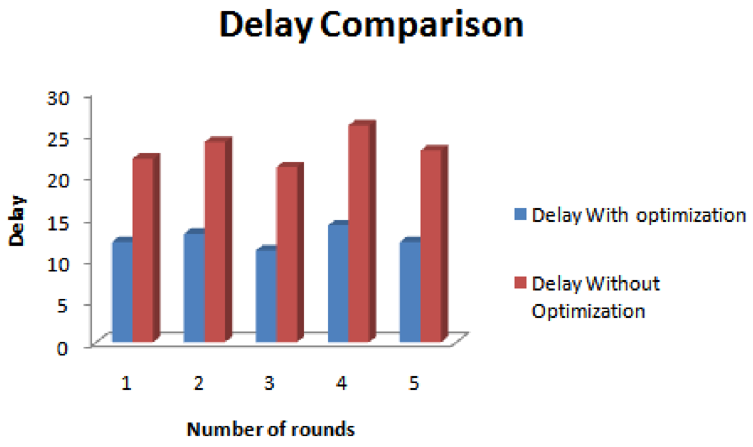

Fig.5 Comparison of Delay for with and without optimization

The comparison of delay has been shown in above graph for with and without optimization. Numbers of rounds are shown in X-axis in the graph where the values obtained for delay are shown in y-axis. The average value for delay in case of with optimization is 12.4 while in case of without optimization, it is 23.2.

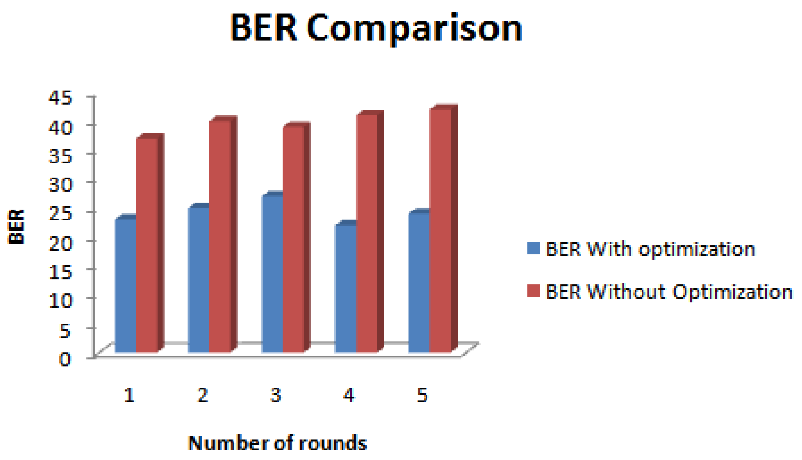

Fig.6 Comparison of BER for with and without optimization

The comparison of BER is shown in above figure with respect to the rounds. Red bar depicts the values obtained for without optimization while blue bar is for with optimization case. X-axis defines the number of rounds and Y-axis defines the BER values obtained after the simulation of the work. The average value obtained for with optimization is 24.2 and for without optimization, it is 39.8.

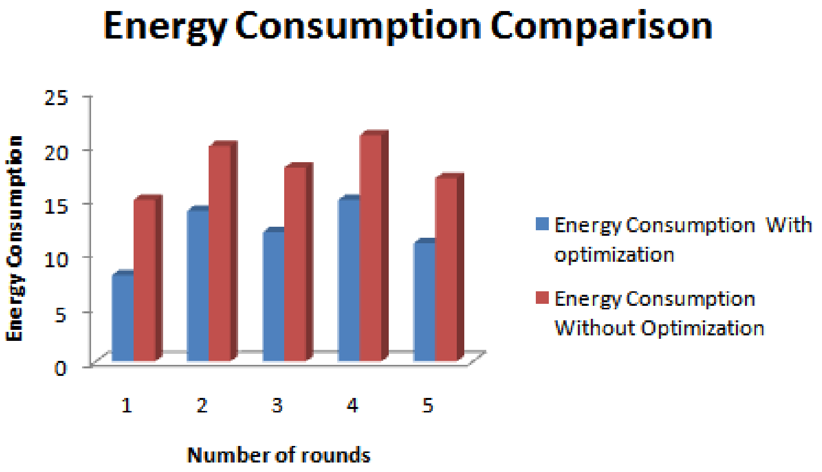

Fig.7 Comparison of Energy Consumption for with and without optimization

The comparison of energy consumption for with and without optimization is depicted in above figure. X-Axis defines the number of rounds and Y-axis shows the value obtained for energy consumption after the simulation. The blue bar in the graph is for with optimization case and red bar shows the result of the without optimization. The average value for with optimization for energy consumption is 12 and for without optimization, it is 18.2.

VI. CONCLUSION

This research has dealt with the detection and mitigation of black hole attack in MANET. Cuckoo search optimization algorithm has been used for the optimization for reducing the delay, bit error rate and for increasing the throughput of the simulated work. ANN as a classification algorithm is used as a classifier. Number of researchers has proposed a number of prevention techniques for the mitigation of black hole attack as only routing protocol cannot give better results. So, the performance can be increased by using optimization as well as classification algorithms. Parameters, like, throughput, BER, Delay and energy consumption has been used for the calculation of the performance. The average value obtained for with optimization is 91 and for without optimization it is 73 for throughput. The average value for delay in case of with optimization is 12.4 while in case of without optimization, it is 23.2. The average value obtained for with optimization is 24.2 and for without optimization, it is 39.8 for BER. The average value for with optimization for energy consumption is 12 and for without optimization, it is 18.2. It is being concluded that with the usage of optimization techniques (ANN and Cuckoo search), enhanced results has been obtained.

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.] Harjeet Kaur, VarshaSahni, Dr.ManjuBala, “A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review”, *International Journal of Computer Science and Information Technologies, (IJCSIT)*, Vol. 4 (3), pp. 498-500, 2013.

[4.] N. Schweitzer, A. Stulman, A. Shabtai and R. D. Margalit, “Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes,” in *IEEE Transactions on Mobile Computing*, vol. 15, no. 1, pp. 163-172, Jan. 1 2016.

[5.] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach,” in *IEEE Systems Journal*, vol. 9, no. 1, pp. 65-75, March 2015.

[6.] S. K. Shah and D. D. Vishwakarma, “FPGA implementation of ANN for reactive routing protocols in MANET,” *2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)*, Bali, 2012, pp. 11-14.

[7.] Wang, Sun-Chong. “Artificial neural network.” *Interdisciplinary computing in java programming*. Springer US, 2003. 81-100.

[8.] L. Tamilselvan and V. Sankaranarayanan, “Prevention of Blackhole Attack in MANET,” *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, Sydney, NSW, 2007, pp. 21-21.

[9.] M. Mohanapriya , Ilango Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET,” Computers & Electrical Engineering 40, no. 2,2014,pp. 530-538

[10.] Anuj K Gupta., Harsh Sadawarti, and Anil K. Verma. "A review of routing protocols for mobile ad hoc networks." SEAS Transactions on Communications 10, no. 11 ,2011, pp. 331-340.

[11.] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," in *IEEE Access*, vol. 5, no. , pp. 10369-10381, 2017.

[12.] Cheng, Hui, and Jiannong Cao. "A design framework and taxonomy for hybrid routing protocols in mobile ad hoc networks." IEEE Communications Surveys & Tutorials 10, no. 3 (2008).

[13.] S. Sarkar and R. Datta, " mobile ad hoc networks," in *IET Wireless Sensor Systems*, vol. 7, no. 3, pp. 55-64, 6 2017.

[14.] Siddharth Dhama, Sandeep Sharma, and Mukul Saini, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks," In Computing for Sustainable Global Development (INDIACom), 2016, pp. 2993-2996. IEEE, 2016

[15.] D. C. Karia and V. V. Godbole, "New approach for routing in mobile ad-hoc networks based on ant colony optimisation with global positioning system," in *IET Networks*, vol. 2, no. 3, pp. 171-180, Sept. 2013.

[16.] M. Sheikhan and E. Hemmati, "High reliable disjoint path set selection in mobile ad-hoc network using hopfield neural network," in *IET Communications*, vol. 5, no. 11, pp. 1566-1576, July 22 2011.