Volume 6, Issue 10, October – 2021 International Journal of Innovative Science and Research Technology

ISSN No:-2456-2165

An Improved Black Hole Detection and Prevention Mechanism in MANET using Firefly and Neural Network

Priyanka Kaushik
Sri Sukhmani Institute of Engineering & Technology

Abstract:- A MANET is a set of wireless hosts that form a temporary network without the use of a dedicated infrastructure or centralised management. Since the nodes in the network are mobile, they self-organize and configure themselves. They send and receive data from other nodes in the network. To find unique paths between the source and the destination in MANETs, route protocols are needed. In which sensor node can moves freely as well as each node acts as the host node or router. In this paper, the best path with efficient Ad-Hoc on Demand Distance Vector (AODV) routing protocol is selected as the routing approach. Firefly algorithm is discovered as a metaheuristic algorithm which is inspired by the flashing behaviour of fireflies and the bioluminescent communication approach to get the optimized route. The Artificial Neural Network (ANN) is used to identify and detect the black hole node inside the network so that the data transmitted from source to destination in secured manner.

***Keywords**:- AODV, MANET, Firefly, ANN, Black Hole Attack.*

I. INTRODUCTION

Each mobile device in a scheme is self-governing since the MANET does not have a central authority. The secured transmission of data in MANET is very challenging. An example MANET is illustrated in Figure 1, demonstrates the network formed by different mobile devices like mobile phones and laptop Every message requires to be identified by which the message can be passed to the correct destination. And we need to find the optimal route to reach at the destination node. Since the links between the nodes are dynamic, it may get broken at any time when the movement of node is carried out apart from ranges of communication. Also new links will be formed when new node comes under the communication range. And these information needs to be updated to all the nodes by which routing can be perfect (Veerasamy et al. [1]).

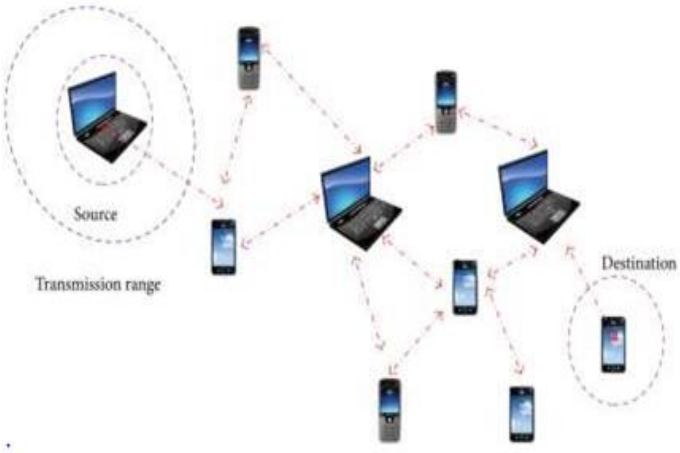

Figure 1. MANET

1.1 Routing in MANET

In MANET, a particular device work as a host as well as a router. Routing refers to an information transfer mechanism from the source towards communication network. A routing algorithm's goal is to create a device that can transport a packet from one node to another. Generally, the existing routing protocols can be categorized into proactive or as reactive and integration of both. In this work, we focused on ad-hoc on demand distance vector (AODV), which is a reactive routing protocol. the MANET routing protocols are very susceptible to a different type of attacks, particularly balck hole based detection approch is implemted. AODV has traditional routing tables and sequence number of destination for the identification of new route from destination with the creation of routing loops. AODV comprises of three types of control messages in order to maintain the route such as; RREQ (Route Request, RREP (Route Reply) and RRER (Route Error Message) (Dhenakaran and Parvathavarthini, [2]).

1.2 Black Hole attack in MANET

In this attack, the malicious node considers one of the routing protocols for presenting that it owns the shortest route towards the destination node or the data that a malicious node wants for the interruption. This node broadcast the availability of recent route without confirming the route within the routing table. According to this, the malicious node would always be available for replying the routing request and hence intercept the packet and keep it. Figure 2 depicts an example of black hole attack in which node 1 and node 4 are the source node and destination node respectively. Node 3 represented by the red colour is the malicious node that respond to the RREQ request sent from the source node.

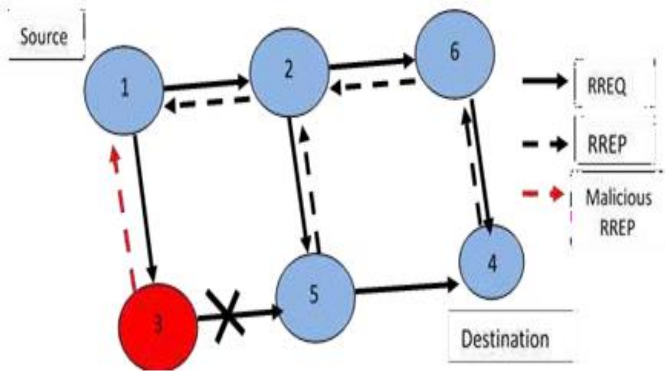

Figure 2. Black hole attack

Source node finds the route using route discovery process through the node 3 and sent data to node 3. In this way node 3 drop the packet and degrades the performance of the network. This problem is consequently known as black hole problem in MANET (Zhang et al. [3]).

II. RELATED WORK

Chadha and Jain [4] proposed preventive measures for black hole attacks in MANET. Black hole attacks leads to a serious security challenges for services of routing through attacking reactive routing protocols, resulting in a sharp drop in data packets. AODV (Ad hoc on-demand distance vector) routing is one of many protocols and is often an easy victim of such attacks. **Chhabra et al. [5]** designed a secure fuzzy Potential Threat (PT) protocol that is utilized to fight against "Black Hole attack" in OppNets. The proposed technique delivers packet in time with a minor overhead and mitigates the rate of dropped data packet. The energy consumption rate also decreases. **Jain et al. [6]** introduced a fuzzy model which is based on the weighted binary relationship to lessen the consequence of "Black Hole attack" in MANET that used AODV routing protocol. The network has been designed using NS-2 simulator tool. The network comprises of 50 number of nodes moving in the 1 km ×1 km area along with 2 to 80 % of malicious nodes. **Panda et al. [7]** proposed an Ant Colony Optimization (ACO) scheme to minimize the side effect of "Gray Hole" and "Black Hole" attack in MANETs. This technique has been used to determine the shortest route from transmitting node to target node on the basis of energy consumption rate. It has been seen that AODV routing protocol perform better with less energy consumption rate and with high throughput. **Su, M.Y. [8]** proposed IDS known as AMB (Anti-black hole mechanism) which has been implemented in the nodes group in the network for the detection of black hole attacks. ABS helps to identify the malicious node with the identification of uncertain importance of the node which is obtained by evaluating the difference RREQ and RREP packet sending from the mobile nodes. **Khan et al. [9]** have studied regarding the implementation of Ant Colony optimization (ACO) technique along with repetitive route configuration through reactive routing protocol mainly for the obstruction of black hole attack in MANET. It has to be clear from the obtained outcomes of this study, the result with highly valuable throughput and enhanced prevention from black hole attack by using ACO including reactive routing protocol. They have accomplished 10% more throughput and 27% less packet loss over least cost path protocol.

III. FIREFLY ALGORITHM

The optimization problem is to find a solution in the feasible region that has the objective function's minimum, or maximum value. The routes can be identified by AODV routing protocol but it does not have information about the nodes authorization means, whether it is an actual or fake node. So solve this challenge, the node features are determined according to the fitness function of the Firefly Algorithm (Yang, X.S., [10]).

IV. ANN

ANN is biologically inspired computing systems. These systems are based on the interconnected nodes or units that are also known as artificial neurons that roughly equivalent to the neuron of the biological nervous system. The signals are processed through the neurons connections that are equivalent to the synapses found in brain. ANN can be considered as a weighted directed graph, in which artificial neurons are nodes. According to the architecture of connections, ANNs can be grouped into two classes.

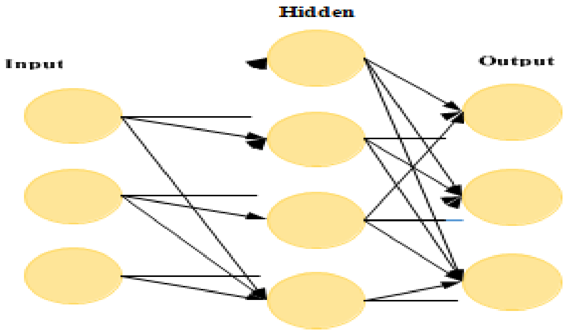

Figure 3. FFBPNN

Feed forward networks, in which graphs do not have loops, and recurrent networks, or networks with feedbacks. Figure 2 shows typical networks of feedforward back propagation neural network (FFBPNN). A typical neural network consists of input layer, hidden layer and output layer with connections (Bajpai et al. [11]).

V. METHODOLOGY

The methodology can be well explained using the following flow diagram. First, Initialization of the network with number of nodes as shown in figure 4.

The designed network for 50 numbers of nodes as depicted in figure 5, depicts the simulator in the range of 1000 × 1000 corresponds to X-axis and Y-axis. The graph along both axes represents the height and weight correspondingly.

Then identify the source node and destination node. After that apply AODV routing protocol to determine the route between source and destination node. As given in figure.

1. Node 26 is consider as the source node as well as node 41 is the destination node. For the data transmission, a route is created using AODV routing protocol. Node 26 sends "hello" packet or RREQ message to its nearby nodes. Hello message includes source address, destination address and hope count. In such scenario, Node 19, node 23 and node 4 receives Hello packet. All nodes except node 4 deny that the destination is not in its zone and next RREQ message has been sent by node 4, as destination node is in its range.

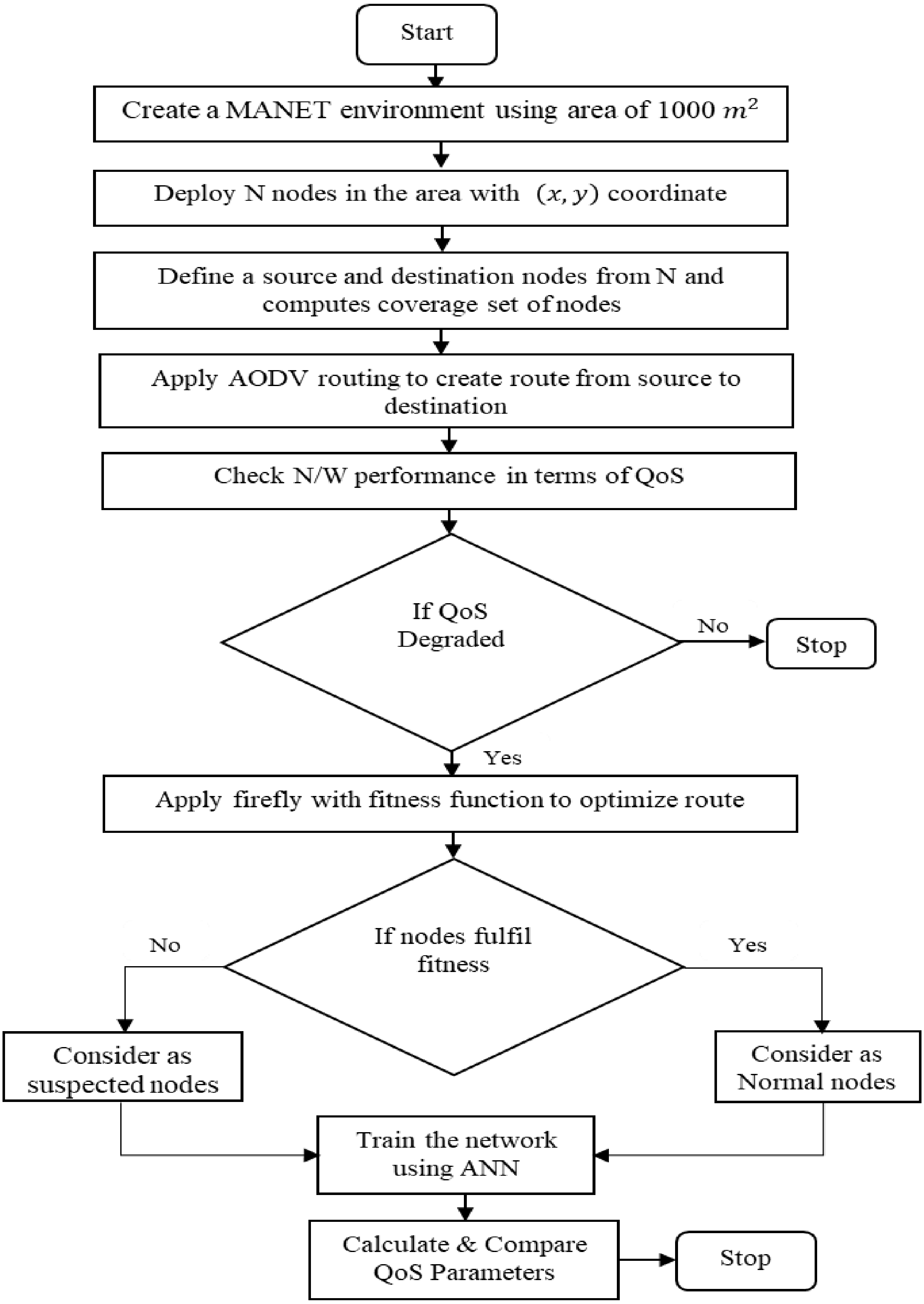
Start
Create a MANET environment using area of 1000 m^2
Deploy N nodes in the area with (x, y) coordinate
Define a source and destination nodes from N and computes coverage set of nodes
Apply AODV routing to create route from source to destination
Check N/W performance in terms of QoS
If QoS Degraded
No
Stop
Yes
Apply firefly with fitness function to optimize route
If nodes fulfil fitness
No
Yes
Consider as suspected nodes
Consider as Normal nodes
Train the network using ANN
Calculate & Compare QoS Parameters
Stop

Figure 4. Proposed Flow of Work

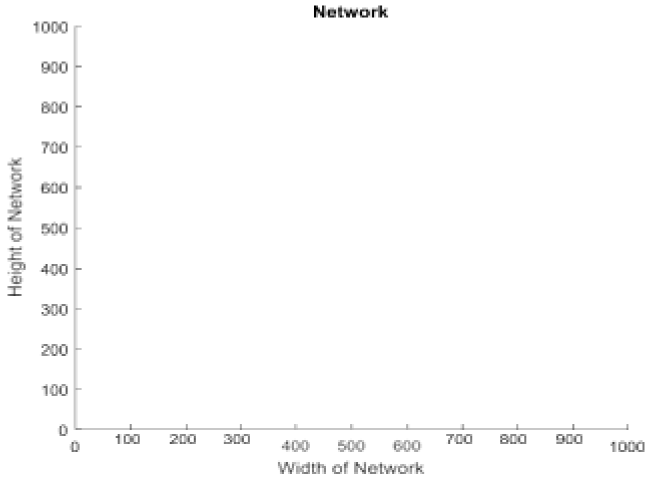

Figure 5. Network Simulator

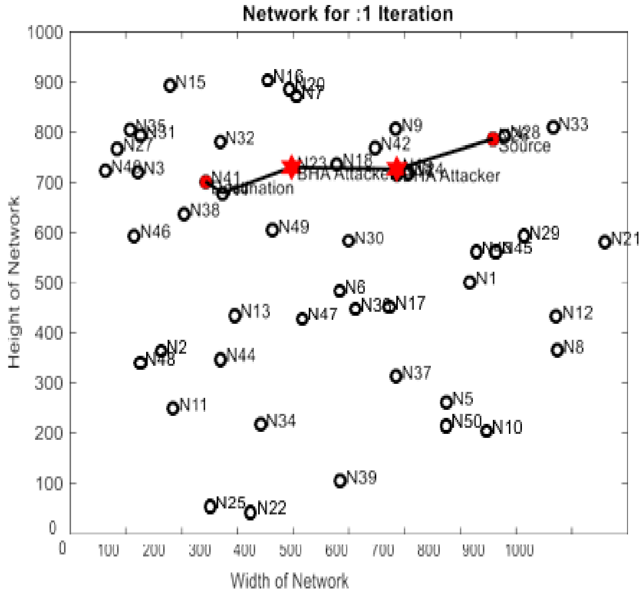

Figure 6. Designed Network

A similar process is repeated until the destination is not determined. After the detection of the destination node, the source node starts data transmission. In this network node 23 and node 19 are the attacker nodes but behave like as genuine node and starts dropping data packets. To get the optimize path, firefly algorithm is applied by using an appropriate fitness function. Then check if the fitness function of Firefly algorithm is not satisfied then apply neural network to find the suspected node otherwise repeat the process. Finally after determining different parameter compare these with the existing work.

a. RESULTS AND SIMULATION

To observe the enhanced performance of proposed work, in the presence of black hole attack using prevention algorithm and without any prevention is demonstrated in this section. The experimental result has been evaluated in terms of Throughput, Packet Loss Rate, Delay and Energy Consumption as discussed below;

i. Throughput

The throughput can be defined to the degree in which the message is successfully transmitted to the destination. Generally, its measurement is done in Bits Per Second (bps).

ii. Packet Loss Rate

It can be described as the amount of data packets that are arrived at the destination to the complete amount of data packets transmitted from the sender side. In a transmission interval, the mathematical expression of PLR can be provided as;

$$PLR = \frac{n^{tr}-n^{rc}}{n^{tr}} \times 100\%$$

Where $n^{tr}$and n^{rc} are the total number of transmitted and received packets, respectively.

iii. Delay

The time consumed in average by the data packet to arrives at the destination that includes all delays caused by buffering, duringroute discovery, latency and queuing at the interface queue. Its description is provided in mathematical form as

$$Delay = delay\ (Normal) + delay\ (Blackhole\, attack)$$

iv. Energy Consumption

It is the amount of energy consumed by the mobile nodes. A node should ideally function, by consuming less energy. This is the main parameter of the network as the lifetime of the network depends upon the battery life and life of battery depends upon the rate of energy consumed by the communicating nodes. The evaluated values of considered are provided in Table 1 in two scenarios such as; without prevention and with prevention technique.

Table 1. Evaluated Parameters

Number of Rounds	Without Prevention				With Prevention			
	Throughput	PLR	Delay	Energy Consumption	Throughput	PLR	Delay	Energy Consumption
1	0.9932	0.0134	0	3.1594	0.9951	0.0127	2.0012	8.1743
2	0.9903	0.0113	2.0022	2.0558	0.9924	0.0102	3.0124	8.5392
3	0.9887	0.0203	4.0156	5.5410	0.9904	0. 0187	6.1152	7.9369
4	0.9841	0.0198	6.7523	8.7125	0.9873	0.0184	6.7523	8.1144
5	0.9801	0.0223	8.4315	12.5431	0.9882	0.0199	7.5613	10.5824
6	0.9789	0.0412	60.7891	56.3263	0.9837	0.0211	10.0052	10.2544
7	0.9679	0.1045	60.9205	60.0124	0.9816	0.0212	19.1325	37.9687
8	0.9168	0.1231	61.7093	84.2317	0.9801	0.0451	26.1304	59.2623
9	0.9145	0.1463	97.6832	87.2087	0.9467	0.1425	42.7521	75.3842
10	0.8104	0.1892	178.4579	119.2276	0.8866	0.1407	120.7652	102.2563

For identifying the network from black hole as well as increase the throughput ANN is used. From the given table, it is understandable that the throughput while utilizing the ANN algorithm is high as contrast to the throughput obtained without any prevention algorithm. An enhancement of 2.39% in terms of throughput has been analysed because of the utilization of ANN as a classification approach for differentiating the normal and attacker node. The significant amount of reduction is observed by applying prevention approach with respect to rate of packet loss, end-to-end delay and energy consumption by 30%, 49.16% and 33.06%, respectively.

Comparison of proposed work with Khan et al. [9, 2020]

In 2020, a research work to prevent the black hole attack utilization of Firefly optimization presented by Khan et al. [9]. In that research the authors achieved the 513 throughputs and 237 packets loss with 10 number of nodes by using Reactive Routing Protocol.

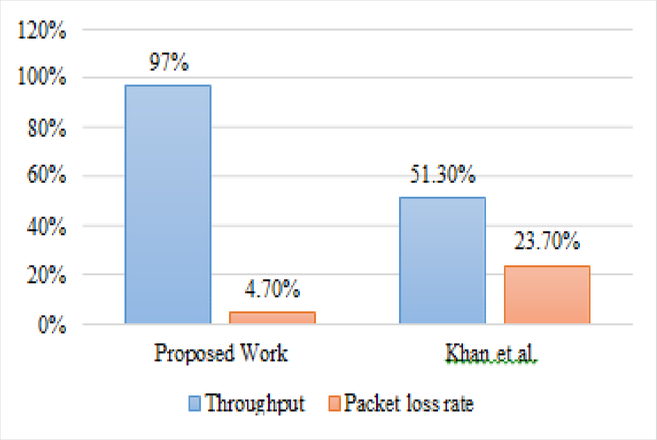

Figure 7. Comparison of Proposed and Existing work

From the graph (see figure 7) it has to be clear that using NN the throughput has been increased by 24% and the percentage reduction in loss of packet using NN has been obtained at about 20.7%. It has been examined that the throughput has been increased by using ANN. Hence, Because of the proper selection of route as FFBPNN helps to distinguish among attacker node and genuine node. Therefore, we conclude that firefly algorithm with AODV Routing Protocol with ANN classifier produces better throughput and provide better prevention from black hole attack.

b. CONCLUSION

In this paper, we have designed a black hole attack detection and prevention system by utilizing the machine learning approach. The route between source and destination node has been discovered by utilizing a table driven route discovery mechanism (AODV) routing protocol. The NN is trained on the basis of the node's properties like energy consumption and delay. Also, the performance parameters has been computed and compared with the existing work to show the efficiency of the proposed work. From the experiment, it has been analysed that the throughput has been increased by 2.39% as well as reduction is observed in terms of packet loss rate, delay, and energy consumption has 30%, 49.16% and 33.06%, respectively. The comparative analysis with existing Khan et al. (2020) has been done in terms of two parameters; and analysed that throughput has been increased by 24%, the percentage reduction in loss of packet using NN has been obtained at about 20.7%.4.

REFERENCES

[1]. Veerasamy, A., Madane, S. R., Sivakumar, K., & Sivaraman, A. (2016). Angle and context free grammar based precarious node detection and secure data transmission in MANETs. *The Scientific World Journal*, *2016*.

[2]. Dhenakaran, S.S. and Parvathavarthini, A., 2013. An overview of routing protocols in mobile ad-hoc network. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(2).

[3]. Zhang, X., Sekiya, Y., & Wakahara, Y. (2009, March). Proposal of a method to detect black hole attack in MANET. In *2009 International Symposium on Autonomous Decentralized Systems* (pp. 1-6). IEEE.

[4]. Chadha, K. and Jain, S., 2014, May. Impact of black hole and gray hole attack in AODV protocol. In *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)* (pp. 1-7). IEEE.

[5]. Chhabra, A., Vashishth, V. and Sharma, D.K., 2018. A fuzzy logic and game theory based adaptive approach for securing opportunistic networks against black hole attacks. *International Journal of Communication Systems*, *31*(4), p.e3487.

[6]. Jain, A.K., Tokekar, V. and Shrivastava, S., 2018. Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks. In *Information and Communication Technology* (pp. 39-47). Springer, Singapore.

[7]. Panda, N., & Pattanayak B. K., “Energy aware detection and prevention of black hole attack in MANET”, *International Journal of Engineering and Technology (UAE)*, vol. *7* no. 26, pp. 135-140, 2018.

[8]. Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, *34*(1), pp.107-117.

[9]. Khan, D.M., Aslam, T., Akhtar, N., Qadri, S., Rabbani, I.M. and Aslam, M., 2020. Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique. *Information Technology and Control*, *49*(3), pp.308-319.

[10]. Yang, X.S., 2009, October. Firefly algorithms for multimodal optimization. In *International symposium on stochastic algorithms* (pp. 169-178). Springer, Berlin, Heidelberg.

[11]. Bajpai, S., Jain, K., & Jain, N. (2011). Artificial neural networks. *International Journal of Soft Computing and Engineering (IJSCE)*, *1*(NCAI2011).