IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 3, 2020, accepted June 22, 2020, date of publication June 25, 2020, date of current version July 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004692

Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network

POOJA RANI[1], KAVITA[1], (Member, IEEE), SAHIL VERMA[1], (Member, IEEE), AND GIA NHU NGUYEN[2,3], (Member, IEEE)

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara 134112, India
[2]Graduate School, Duy Tan University, Da Nang 550000, Vietnam
[3]Faculty of Information Technology, Duy Tan University, Da Nang 550000, Vietnam

Corresponding author: Gia Nhu Nguyen (nguyengianhu@duytan.edu.vn)

ABSTRACT Wireless technology and the latest developments in a mobile object, has led to a Mobile Ad Hoc network (MANET), which is a collection of mobile nodes that are communicating with each other without requiring any fixed infrastructure. Due to the dynamic nature with a decentralized system, these networks are susceptible to different attacks such as Black Hole Attack (BHA), Gray Hole Attack (GHA), Sink Hole Attack (SHA) and many more. Several researchers have worked for the detection and mitigation of individual attacks, either GHA or BHA nodes. But the protection of MANET against a dual-threat is scarce. In this paper, the protection against dual attacks has been presented for BHA and GHA by using the concept of Artificial Neural Network (ANN) as a deep learning algorithm along with the swarm-based Artificial Bee Colony (ABC) optimization technique. The performance of the system has been increased by the selection of appropriate and best nodes for data packets transmission which is explained in the result section of this paper. For the network designing and simulation purposes, MATLAB software is used with communication and neural network toolboxes. The examined results show that the presented protocol performs better in contrast to the existing work under black hole as well as gray hole attack condition. A mobile ad hoc network (MANET) is a collection of mobile nodes that dynamically form a temporary network without using any existing network infrastructure.

INDEX TERMS ABC, ANN, AODV, black hole attack, gray hole attack, MANET.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a self-tuning network that does not have a dedicated router; since there is no centralized node, and each node behaves as a router (Singh *et al.* [1]). Each node has a limited range for data transmission in the network, and the data transmission occurs from one node to another node. The routing in MANET assumes the entire nodes in the network as normal unless there is no modification in the data and router direction is found. MANET finds applications in various fields like disaster management (Martín-Campillo *et al.* [2], Military (Plesse *et al.* [3]), vehicle computing (Toor *et al.* [4]), and more (Poongodi and Karthikeyan [5]). For data transmission, routing mechanisms such as proactive (Chavan *et al.* [6]), reactive (Ochola *et al.* [7] and El-Semary and Diab [8]), and hybrid routing protocol is employed. In a dynamic routing protocol, the routing information of nodes is store into the table and is modified whenever the route is changed. In a reactive routing protocol, as the node suggests, the path is created whenever the source node wants to send data to the destination node that is, it works on-demand (Han and Lee [9]). The last protocol is formed by combining the advantages of the above-defined routing protocol that is named as a hybrid routing protocol in MANET (Wang *et al.* [10]).

Due to the free or the mobile nature of nodes, the network is vulnerable to different attacks such as the gray hole, black hole attack, and selective packet drop attack (Mohanapriya and Krishnamurthi [11]).

Blackhole (Arunmozhi and Venkataramani [12]) and the gray hole attack (Schweitzer *et al.* [13]) are also termed

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Fu Cheng.

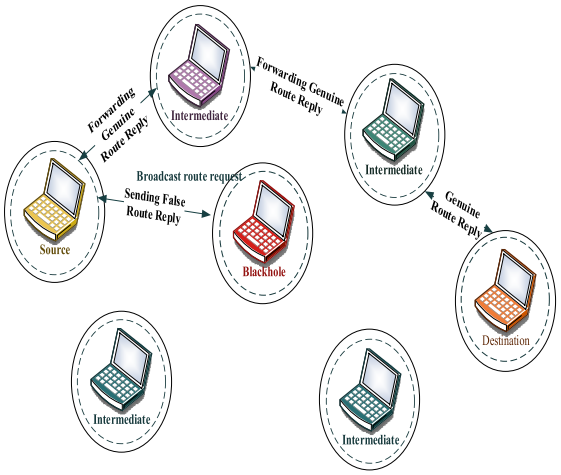


FIGURE 1. Sending FRREP by black hole node.

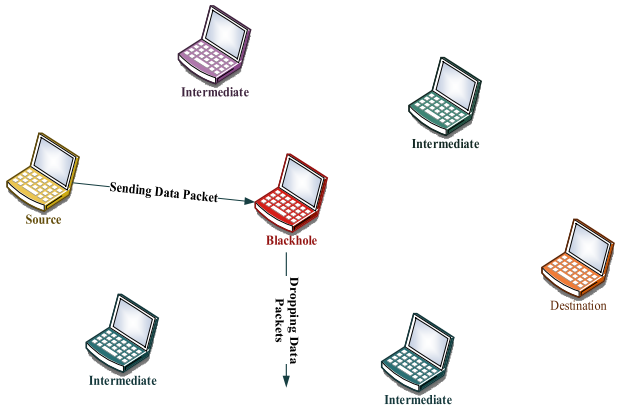


FIGURE 2. Packet drop by black hole node.

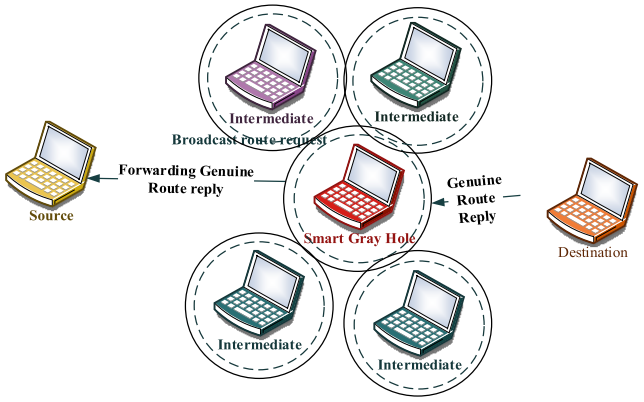


FIGURE 3. Participation of gray hole attack as a normal node during route discovery process.

as packet drop attacks and result in packet drop during the communication process.

A. BLACK HOLE ATTACK

It is a kind of Denial of Service (DoS) attack (Gupta *et al.* [14]) and sometimes known as a full packet drop attack (Djahel *et al.* [15]). BHA node tries to attract data traffic towards itself by sending FRREQ with minimum count and maximum destination sequence number.

The presence of an attacker node can be sensed during the route discovery phase (Jain *et al.* [16]). There is no static route in the network. Therefore, whenever the nodes want to communicate a dynamic route is created using any of the routing mechanisms (Ochola [7]). In this research, the route formation has been performed using AODV is an on-demand routing protocol along with DSR. Using this protocol, the source node sends the RREQ packet to the nearby node, which contains the address of the destination node. If the adjacent node is not the destination node (not found its address) in the RREQ packet, then forward the packet to the next node, which comes in its communication range (Shashwat *et al.* [17]). After receiving the RREQ packet by the black hole node, the affected node instantly sends an RREP packet towards the source node with a higher hop count to win the request known as fake routing response (FRREP) (Mohammadani *et al.* [20]). The route is established from the source to the destination node through the black hole node, and hence the entire data packets are dropped by the black hole as an intermediate node, which in return decrease the throughput of the network (Li *et al.* [19] and (Kumari *et al.* [20]). The process of dropping the packet through the black hole node is shown in Fig. 2.

The MANET topology composed of seven modes besides the source and the destination node represented by the yellow and the orange laptop, the red color laptop as black hole node, and left is the intermediate nodes. RREQ message is being broadcasted by the source node (Gurung and Chauhan [21]). After reaching the RREQ packet to the destination node, the destination regenerates the RREP packet. The regenerated RREP packet along with the FRREP with the highest hop count is sent by the black hole node towards the source node (Taranum and Khan [22]). As the source node received the packet with the highest hope count then it starts sending data towards the black hole node by believing that it is a destination node (Majumder and Bhattacharyya [23]). The black hole node drops the data instead of forwarding it to the destination node (see Fig.2).

B. GRAY HOLE ATTACK

It is a continuation of a black hole attack (Sandhya Venu and Avula [24]), which drops selective data packet during the data transmission process and is also termed as a partial packet drop attack (Gurung and Chauhan [25]).

In the initial stage, the gray hole node does not show its appearance as a malignant node because they behave like a normal node during the route discovery process. After some time, when the method of communication/ data transmission starts, these nodes turn into malignant nodes. The participation of the gray hole attack as a genuine node during the process of route discovery and the partial drop of data during the data communication process is shown in Fig. 3 and Fig. 4, respectively (Gurung and Chauhan [26]).

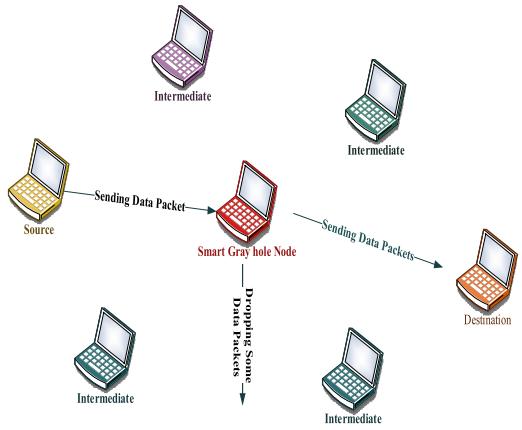


FIGURE 4. Partial packet drop by GHA.

Therefore, it becomes very challenging for the researchers to identify the gray hole attack (Schweitzer *et al.* [13]) in MANET. Most of the scholars have offered different solutions to overcome the problem of a black hole along with gray hole attacks in MANETs (Djahel *et al.* [15]). Most of the solutions are provided only for a single attack that might be a black hole, warm hole, gray hole attack another one. It is very difficult to identify the presence of gray hole attacks, as GHA node participated normally during the route discovery process, attracts traffic, and drops selective data. Sometimes, it is known as a smart gray hole.

C. ORGANIZATION OF THE PAPE

The remaining article is organized as follows. The work related to the detection and prevention of black hole and gray hole attack in MANET using different techniques is discussed along with the limitations. In section III, the entire flow of work with the algorithm used is presented along with the pictorial representation. Section IV explained the simulation parameters examined using MATLAB tool in the presence and absence of BHA and GHA. Finally, the conclusion has been provided in section V followed by the references used.

II. RELATED WORD

From the last couple of years, several researchers have worked to secure MANET against different types of internal as well as external attacks. Several Intrusion Detection System (IDS) has been developed by (Shams and Rizaner [27], Nadeem and Howarth [28], Marchang *et al.* [29], and Bu *et al.* [30]) that worked as a safeguard against threats. IDS aims to detect malicious nodes and improve network performance. (Shi *et al.* [31]) has presented a clustering-based approach to protect the network against the BHA. Clustering is a supervised approach, through which the entire system is divided into subareas, and each sub-area is monitored by a Cluster Head (CH) that helps to detect the presence of BHA node in the network. The main drawback through which this research lacks is that with the various CH formation, the overhead increases and also requires high maintenance. (Chang *et al.* [32]) have utilized cooperative bait detection methods for the identification of malicious nodes. Based on this mechanism, the next hope node has been selected by the transmitting node so that the source node could be assisted to provide the data to the receiving node along with sending an acknowledgment to the malicious node. The drawback of this work is that only the nearby node has been selected as a bait address, which might be an affected node and hence pass data to that node and thus degrade the network performance. A few researchers such as (Singh *et al.* [11] and Nurcahyani and Hartadi [34])have worked on DSR protocol to protect the data transmitted using it. Using this protocol, the node's behavior has been analyzed based on the packet received and sent. The nodes have been defined as a malicious node if the value of nodes has been exceeded the specified threshold (Mohanapriya and Krishnamurthi [11]). Also, a model has been presented to protect the network against a black hole attack based on the trust mechanism. The trust of the node has been evaluated based on the node's stability, mobility, power remaining, and the pause time (Biswas *et al.* [35]). Also, an attempt has been made by (Dhaka *et al.* [36]) to protect MANET against GHA in combination with the BHA node by using the controlled packet. The control packet has been sent by the source node to its nearby node and based on its response the activity of the node such as normal and malicious has been determined. A smart gray hole attack has been identified by using a novel protection mechanism named as Mitigating Gray hole Attack Mechanism (MGAM). This mechanism worked by analyzing the gray hole node based on the concept of the threshold value. That is the case when the packet drop by the nearby node increases more than the threshold value an Alert has been broadcasted, which declared that the gray hole node has appeared in the network. A dual-threat detection approach precisely for GHA and BHA has been presented by (Ali Zardari *et al.* [37]) for MANET. The attacker has been identified based on two features of nodes such as energy and its presence in the blacklist. If it is present in the blacklist then the data is not passed to that node. Existing work only applicable for small network because they only use the concept of energy consumption by nodes as a feature sets to differentiate between normal or malicious node, that means if network size is large, then identification of malicious nodes becomes complicated due to the involvement of similar types nodes and need an optimization approach to segregate the nodes based on the energy consumption, transmission delay, and packet transfer rate according to the fitness function.

To overcome this, a novel fitness function has been designed for the ABC algorithm based on which the nodes are segregated. Based on the segregated node list, the ANN structure is trained, which helps to delivered data with a small delay and high PDR.

III. MATERIAL AND METHODS

This research aims to protect the network against two types of attacks named a BHA and GHA. The detection process

TABLE 1. Ordinary measure.

Matrix	Range
Node Range	50-100
Area of Network	1000 × 1000 mm2
Coverage Range	25% of the total area
Type of Model	Heterogeneous

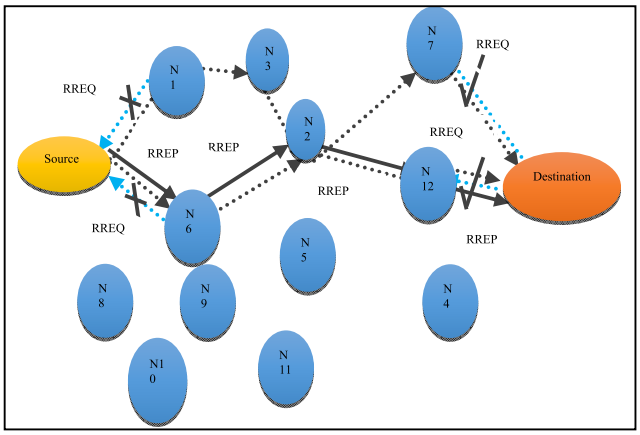


FIGURE 5. Route discovery using AODV.

of these malicious nodes has been performed using ABC (Tareq *et al.* [38]) as an optimization algorithm along with the ANN (Canêdo and Romariz [39]) approach. The step by step description is provided below.

Initially, a network of certain length and width is designed by deploying the N number of nodes within the system (N = 50 and 100). The requirement for the network is listed in Table 1.

The network is designed for a simulated area of 1000 × 1000 mm^2, and each node can communicate within its 25 % of the total area, means that if a node is located with a position of (x,y) = (500,500), then the node can communicate with neighboring nodes up to having maximum position lies in between (525, 525) in both x and y-direction.

Also, a heterogeneous model means that the nodes' communication capacity range is decided based on different parameters like packet delay, co-ordinates, and energy consumption.

After deploying nodes, the source and the destination nodes are defined. Then, using the AODV routing algorithm, the process of data transmission has been performed. The routing concept is shown in Fig. 5.

In AODV, the route is formed only when the data needs to be transmitted. The process is carried out in two steps that are Route request (RREQ) and Route Reply (RREP). Whenever the source node wants to communicate with the destination node, a data packet that consists of the RREQ message is broadcasted within the source's coverage range of (25 %). After receiving the data packet by the nearby node, it stores data into its routing table and also matches it with the previous data store, if the data is not matched then forward to

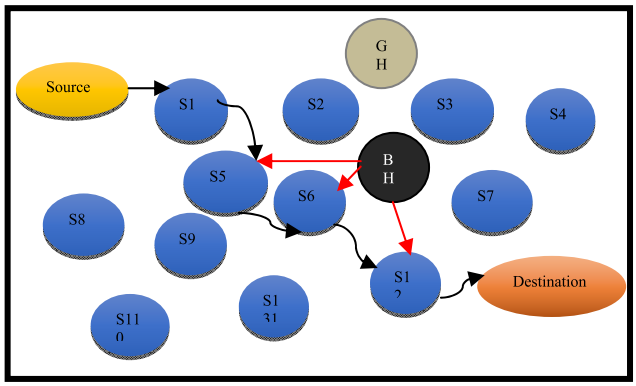


FIGURE 6. Network with black hole and gray hole attack.

its nearby node (Taha *et al.* [40] and Abusalah *et al.* [41]). In this way, the data packet is reached at the destination node by following multiple paths. In the AODV protocol, one of the best suitable routes is considered for data transmission among numerous possible routes based on distance measurement (Nakayama *et al.* [42]). After the data packet is received, the destination node sends back a route response packet towards the transmitting node through the shortest path. The route discovery mechanism is depicted in Fig. 5. The blue dotted line represents the Route Request sent by the nearby node. The dotted black color line represents the possible route, whereas the solid black color line represents the appropriate route formed between the source and the destination node (Gharavi [43]). The cross clicks represent that the nods that receive the RREQ packet are not the destination node. The right-click represents that the desired destination is obtained, and it responds with the RREP packet (Fapojuwo *et al.* [44]). The designed algorithm for AODV as a routing mechanism is written below.

After route discovery, the next step is to deploy attacker nodes (a Blackhole and Gray hole) as indicated by the black and the gray color, respectively, in Fig. 6. The attacker nodes are marked based on their properties, such as if a malicious node behaves as a source node in route, and it is not a validated source, then it is defined as a BHA node. In other cases, if the node acts as an intermediate node in route and drops data partially, then it is considered as gray hole node. Based on the properties of the node, the nodes are differentiated into two categories typical and abnormal communicating nodes. Further, abnormal communicating nodes as separated into two subcategories named as a Blackhole and GHA nodes using ABC as an optimization technique with a novel fitness function. Those nodes that satisfy the ABC fitness function is considered as normal node otherwise considered as a malicious node.

A. ARTIFICIAL BEE COLONY (ABC)

ABC algorithm is motivated by the forging performance of honey bees that is a robust and swarm intelligence algorithm. It was firstly designed by Karaboga and has been improved by different researchers by combining with other approaches.

Algorithm 1 AODV Routing Protocol

Required Input: N_{SN} ← Number of Mobile Sensor Nodes
N_S ← Source Sensor Node
N_D ← Destination Sensor Node

Obtained Output: FR ← Final Route from N_S to N_D

1. Start Routing
2. Nodes (NSN) start broadcasting of RREQ messages to neighbor nodes
3. Defined a message for RREQ = [NS, Hop Count, ND], At initially Hop Count = 0
4. Route = [] // Initially Route is empty
5. Route(1^{st} Node) = N_S
6. While N_D not founded
7. 1^{st} Node Broadcast RREQ to Neighbors Sensor Nodes and Record Hop Count
8. Neighbor Nodes Receive RREQ and check requirements
9. If [NS, Hop Count, ND] == Neighbour Sensor Nodes [NS, Hop Count, VD]
10. Route = Neighbour NSN is an ND
11. Each node Send RREP to NS
12. Hop Count = 1
13. Else
14. Route = Neighbour NSN
15. Send RREP to NS
16. Hop Count = +1
17. End – If
18. Update and repeat step 3 to 13 until ND not founded
19. Possible Route, R = R1, R2, R3,.....RN
20. For r in range of R
21. Current Route, R = R(r)
22. Calculate to distance (D) from NS to ND
23. If D is minimum then
24. Final route, FR = R(r)
25. Else
26. Check next route condition
27. End – If
28. End – For
29. End – While
30. Returns: FR as a final route from NS to ND
31. End – Function

It mainly works by using three types of Bees such as (i) scout bee (ii) onlooker bee (iii) employed bee. The working steps are illustrated in (Kalucha and Goyal [45]).

The initial and foremost step of the ABC algorithm is to generate a population on a random basis and hence search for the solution in the search space. The search space that is found in its boundary range is determined by equation (1);

$$y_i^j = y_{iN_s}^j + S^j \times Rand(0, 1) \tag{1}$$

where, N_s is the source of nectar with i = 1……..N and j = 1……..M, where N, M represents the number of nectar sources and optimization parameters respectively. The minimum and maximum values in dimension j in search space is represented by y_{min}^j *and* y_{max}^j. Now the position of employed as well as onlooker bees are being updated using the equation (2);

$$y_i^j = y_i^j + (y_i^j - y_{neighbour}^j) \times rand \tag{2}$$

Here, a neighbor belongs to (1, N), which is being selected randomly and rand comprises of a real number range [-1,1] and is distributed uniformly. When some parameter values generated by this operation exceed the predefined limits in equation (3), the parameter is set to the appropriate limit (Karaboga *et al.* [46], and Keerthika and Malarvizhi [47]).

$$y_i = \begin{Bmatrix} y_1^i & if\ y_i < y_1^i \\ y_2^i & if\ y_i < y_2^i \end{Bmatrix} \tag{3}$$

The designed fitness function is given by equation (4);

$$F(f) = \begin{cases} 1; & if\ N_{PROP} < Threshold_{PROP} \\ 0; & Otherwise \end{cases} \tag{4}$$

In the fitness function, N_{PROP}: is properties of current sensor nodes which are in FR and $Threshold_{PROP}$ are the threshold properties of all communicating sensor nodes which are defined based on energy, transmission delay, and packet transfer rate. Based upon the fitness function segregated list of nodes (normal, attacker) is created. Those nodes who satisfy the fitness function are considered in the normal list and those who not are considered in the abnormal list.

The algorithm for ABC is written below:

Based on the above properties, the network is trained using Artificial Neural Network (ANN). During the simulation process, based on the trained architecture of ANN, the system can classify normal, BHA, and GHA nodes and create an optimized and secure route from the transmitting node to the receiving node. The developed trained structure along with the designed algorithm for the ANN approach is written below;

The trained structure for 50 numbers of nodes and 100 nodes is represented in Fig. 7 (a) and Fig. 7 (b) respectively.

From Fig. 7 (a) it is seen that the input layer comprises 50 numbers of nodes as input data, the information of which such as delay, energy consumption is being carried by10 number of neurons as depicted under the hidden layer of Fig. 7. At the output layer, there are 47 numbers of nodes has been attained, which demonstrates the class of communicating nodes. The network has been trained on energy consumption and the delay produced by the nodes. Later on, these parameters are used to decide that to which node the data is forwarded.

After clicking on the performance button shown under ANN trained structure as depicted in Fig. 7, the Mean Squared Error (MSE) graph has been analyzed. From the graph shown in Fig. 8, MSE value measured at which the ANN structure is trained for 50 numbers of nodes and 100

Algorithm 2 ABC

Required Input: N_{PROP} ← Mobile Sensor Nodes Properties in terms of Energy Consumption, Transmission Delay, Packet Transfer Rate, etc.
$F(f)$ ← Fitness function
FR ← Final Route using AODV between Source to Destination

Obtained Output: ON_{PROP} ← Optimized Mobile Sensor Nodes Properties

1. Start
2. To optimized the FR, ABC Algorithm is used
3. Set up basic parameters of ABC: Population of Bee (B) – Number of Sensor Nodes
   Final Route (FR) – Route from NS to ND
   Fitness Function using equation 4
4. Calculate Length of Route in terms of R Length
5. Set a variable to store optimized nodes properties, ONPROP = []
6. For i in rang of R Length
7. EBEE = FR (i) = N_{PROP} // Current Bee from B
8. OBEE = $Threshold_{PROP}$ // // Mean of all B
9. $F(f) = Fit\ Fun(E_{BEE}, O_{BEE})$
10. ONPROP = ABC (F(f), FR (i))
11. End – For
12. Returns: ONPROP as an optimized mobile sensor node property
13. End – Function

TABLE 2. Parameters used for ANN.

Parameter	Value
Input layer	neurons=50/100
Hidden layer	neurons=10
Number of hidden layers	1
Output layer	neurons=47/92
Epoch	3

number of nodes is 0.4834 and 0.63463 respectively, which is obtained at the 3rd epoch. For better training, it is desired that the MSE value should by low and near to zero.

Using ANN, the network learns the behavior of participating nodes, which further helps to detect node as a normal and malicious node.

IV. RESULT AND DISCUSSION

After the simulation, the performance has been evaluated using AODV (Under Threat), ABC with ANN (After Prevention), and the comparison with the existing approach presented by Ali Zardari *et al.* 2019 has been shown to show the better performance of the proposed work. The entire work has been conducted in MATLAB simulator Fig. 9 represents the values examined for the PDR parameter for four different conditions, such as under threat (GHA and BHA) node, AODV, AODV with ABC, and after network prevention using

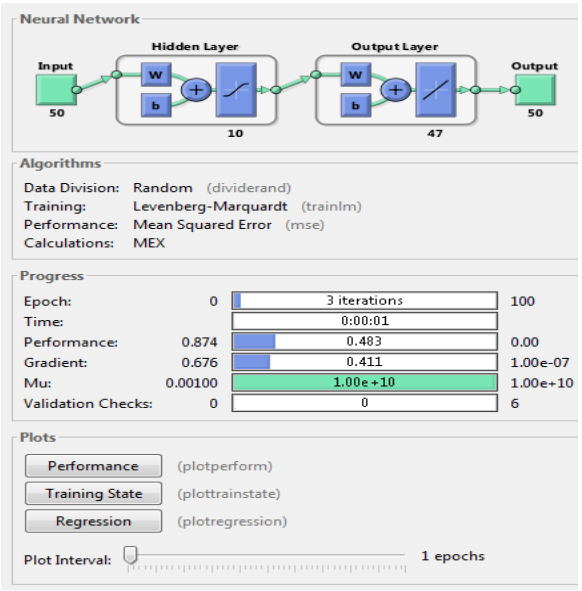
Algorithm 3 ANN

Required Input: N_{SN} ← Number of Mobile Sensor Nodes
ON_{PROP} ← Optimized Mobile Sensor Nodes Properties in terms of Energy Consumption, Transmission Delay, Packet Transfer Rate, etc. concerning the node behavior
Cat ← Target/Category in terms of Normal and Abnormal Sensor Nodes
N ← Carrier Neurons Number

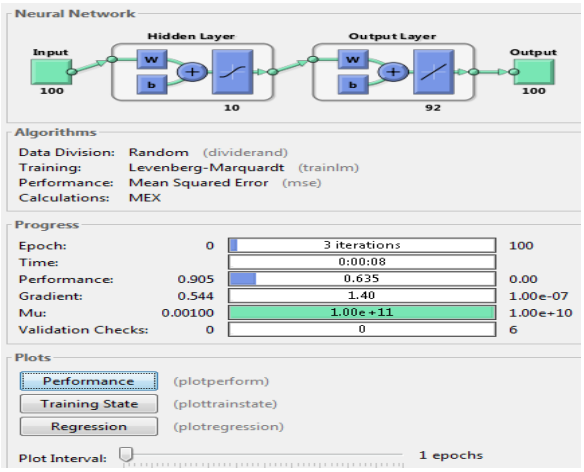
Obtained Output: OR and BHA/GHA ← Optimized and Validated Route from N_S to N_D with Black Hole and Gray Hole Nodes// if node behave like GH and BH node in route, then ANN identify them and discard that nodes from route

1. Start Routing
2. Call and set the ANN using ONPROP properties as training data (T), number of NSN as a group (G) and Neurons (N)
3. Initialize the ANN: 10 numbers of neurons Epoch
   Parameters: MSE, Gradient, Mutation, and Validation
   Training Algorithm: Levenberg-Marquardt
4. Set, MANET_Structure = NEWFF (T, Group, N)
5. MANET_Structure = TRAIN (MANET_Structure, T, G) // To train the network based on nodes properties
6. Current Sensor Nodes, NC = Properties of the current node in MANET // Current sensor node means which are considered in route during routing and their properties are denoted as NC
7. Sensor Nodes Characteristics = SIM (MANET_Structure, NC) // To match nodes nature with training structure of ANN
8. If Sensor Nodes Characteristics is valid then
9. OR = Validated
10. Else
11. OR = Need Correction or mark as BHA and GHA Nodes
12. If the drop rate is maximum
13. Marked as BHA
14. Else if drop some and transmit some data packets
15. Marked as GHA
16. End – If
17. End – If
18. Returns: OR as an Optimized and Validated Route from NS to ND with Black Hole and Gray Hole Nodes
19. End – Function

AODV with ABC & ANN. From the Figure, the highest PDR of about 98.66 % has been examined for 2000 nodes. This is because, after preventing the MANET against BHA and

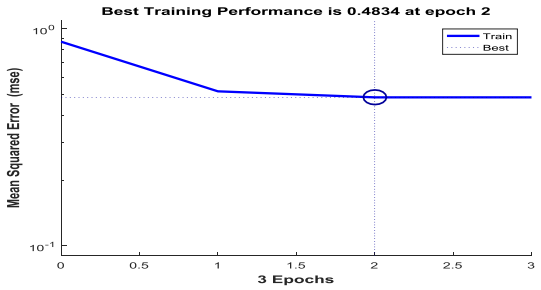


(a)

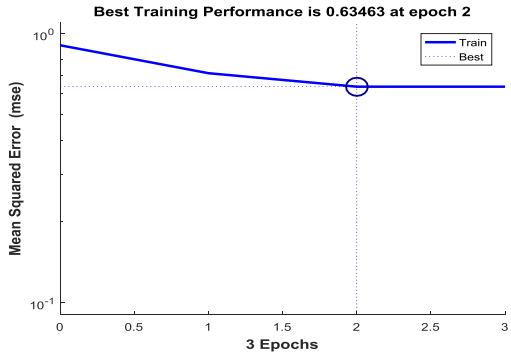


(b)

FIGURE 7. (a) Training structure for 50 nodes. (b) Training structure for 100 nodes.



(a) MSE for 50 Nodes



(b) MSE for 100 Nodes

FIGURE 8. (a) MSE for 50 nodes. (b) MSE for 100 nodes.

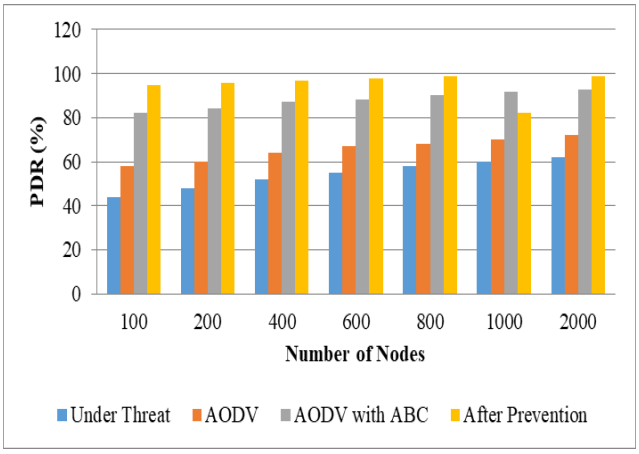


FIGURE 9. PDR.

TABLE 3. PDR (%).

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention
100	44	58	82	94.7
200	48	60	84	95.8
400	52	64	87	96.9
600	55	67	88	97.1
800	58	68	90	97.7
1000	60	70	92	98.24
2000	62	72	93	98.66

GHA node, packets are delivered efficiently and with a higher speed to the destination node. After the implementation of the proposed algorithm in hybridization that is AODV with ABC and ANN approach, the PDR rate has been increased slightly compared to the remaining three conditions, as indicated by the blue, the red, and the green color respectively. Also, the observed values of PDR are indexed in table 3.

The throughput values analyzed under threat, after prevention from (GHA and BHA), AODV, AODV with ABC as well as the values observed by proposed work (after prevention) has been depicted in Fig. 10. The case when the nodes are usually communicating, and their communication is disturbed by the attacker node by sending the false request or by claiming that the route through the attacker node is the exact route or the shortest path, the throughput gets degraded. The performance has been increased after the detection of the malicious node. The data is then passed to a normal intermediate node that is being selected using ABC with the ANN approach. The values examined using the proposed

TABLE 4. Throughput (Kbps).

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention
100	58.97	68.02	80.25	85.64
200	60.25	72.94	82.59	86.98
400	62.57	75.36	85.25	88.02
600	63.87	78.75	87.94	89.64
800	65.94	79.25	88.92	90.57
1000	66.32	80.25	89.25	91.89
2000	67.85	82.67	90.04	92.96

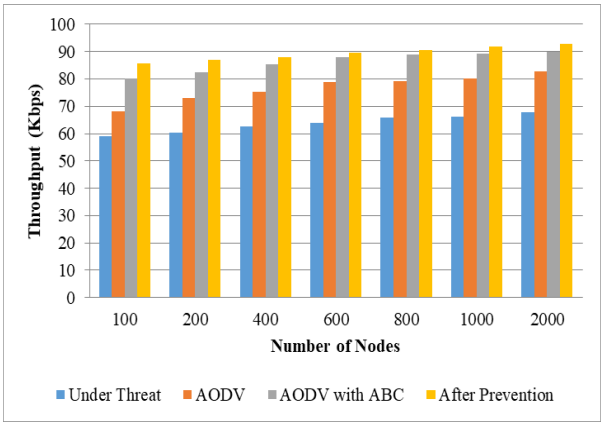


FIGURE 10. Throughput.

TABLE 5. Average delay (S).

Number of Nodes	Under Threat	AODV	AODV with ABC	After Prevention	Ali Zardari et al. 2019
100	0.13	0.11	0.099	0.059	0.071
200	0.19	0.13	0.12	0.062	0.075
400	0.22	0.145	0.133	0.065	0.080
600	0.26	0.159	0.142	0.068	0.081
800	0.28	0.167	0.151	0.075	0.092
1000	0.29	0.174	0.158	0.18	
2000	0.30	0.179	0.162	0.22	

technique after prevention, under threat, and AODV, AODV with ABC are listed in table 4.

Delay represents the time interval taken by the communicating nodes to send the data packet from the source node to the destination node successfully within the time frame. From the Figure, it has been observed that the delay analyzed under the malicious node (BHA and GHA) nodes is high as indicated by the blue bar because of the drop-down of a data packet during the communication process. From the graph shown in Fig. 11, there is a constant increase in the delay that has been observed with the amplification of deployed nodes. Also, it is observed that the delay followed by ABC with the ANN approach performs better in contrast to existing work.

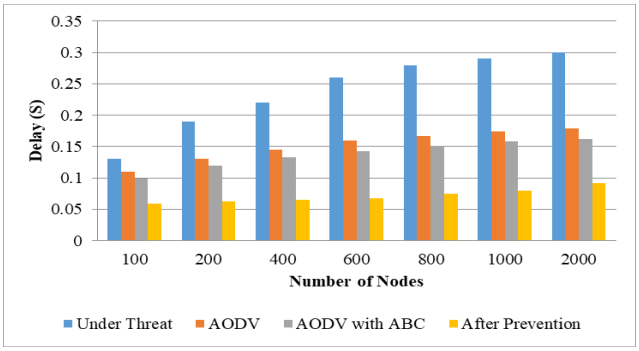


FIGURE 11. Delay.

TABLE 6. Comparative analysis for examined parameters.

PDR (%)		Throughput (Kbps)		Delay (s)	
Proposed	**[40]**	**Proposed**	**[40]**	**Proposed**	**[40]**
97.55	96.94	89.38	79.08	0.071	0.087

A. COMPARISON OF PROPOSED WORK WITH EXISTING WORK

To show the efficiency of the designed secure MANET system, a comparison has been made with the existing work presented by Ali Zardari *et al.* 2019. The comparison has been made based on average values examined for PDR, Throughput, and delay as depicted in Table 6.

The PDR of the proposed work has an enhancement of about 0.63 % while using ANN with the ABC algorithm. This is because in [37], the authors have used a traditional approach named CDS (connected Discriminant Set) approach, in which a set of nodes has been created based on their energy. The authorization of the node has been checked based on the energy. During this process, the chances of packet drop increase because each node contains a data packet for a long time. To overcome this problem, we create a model using the concept of AI for detection of intrusion in the network automatically and the achieved average PDR is 97.55%.

Using AI technique, intermediate nodes transmit a data packet to other nodes without any delay then the rate of data delivery as well as the speed of data delivery rate increases, which is represented in terms of the throughput parameter.

The comparison of average throughput examines by deploying nodes (N = 100, 200, 400, 600, 800, 1000, 2000) in the proposed work against the existing work [37]. The throughput examined by the proposed work is better compared to [37]. Also, there is an enhancement of $\{(\frac{89.38-79.08}{79.08}) \times 100\} = 13.02\%$ has been observed compared to the [37] work. The comparison of throughput (Kbps) is shown in Table 6.

The comparison of delay produced during the communication process in [37] and the proposed work is shown is presented in Table 6. Using a swarm-based approach in combination with the AI approach the speed of data transmission has been increased and the percentage reduction in

the data transmission observed compared to the [37] work is calculated as; $[(\frac{0.087-0.071}{0.071} \times 100)] = 18.39\%$. This is because the list of affected nodes and the normal node is created by an ABC algorithm based on which accurate route is selected by the ANN algorithm. This process helps to enhance the speed and hence reduce the delay.

V. CONCLUSION

The performance of MANET has been affected by many attacker nodes, which becomes a great concern for the research. The identification of multiple threats in the network is a necessary job to enhance the lifetime of the network. Therefore, to improve the performance of the network in the presence of malicious nodes, specifically BHA & GHA nodes, a security mechanism using ABC as a swarm-based approach and ANN as a machine learning technique has been used. ABC utilized the intelligent behavior of honeybees, which has been used to segregates the nodes based on their properties, such as into two lists named healthy and affected nodes lists.

Furthermore, the attacker nodes list is subdivided into BHA nodes and the GHA nodes list. Using these properties, ANN trains the network. The performance has been analyzed based on PDR, throughput, and delay. The improvement against PDR, throughput, and delay compared to existing work such as 0.63 % 13.02 %, and 18.39 % has been attained compared to existing work.

REFERENCES

[1] T. Singh, J. Singh, and S. Sharma, "Energy efficient secured routing protocol for MANETs," *Wireless Netw.*, vol. 23, no. 4, pp. 1001–1009, May 2017.

[2] A. Martín-Campillo, J. Crowcroft, E. Yoneki, and R. Martí, "Evaluating opportunistic networks in disaster scenarios," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 870–880, Mar. 2013.

[3] T. Plesse, C. Adjih, P. Minet, A. Laouiti, A. Plakoo, M. Badel, P. Muhlethaler, P. Jacquet, and J. Lecomte, "OLSR performance measurement in a military mobile ad hoc network," *Ad Hoc Netw.*, vol. 3, no. 5, pp. 575–588, Sep. 2005.

[4] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.

[5] T. Poongodi and M. Karthikeyan, "Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks," *Wireless Pers. Commun.*, vol. 90, no. 2, pp. 1039–1050, Sep. 2016.

[6] A. A. Chavan, D. S. Kurule, and P. U. Dere, "Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack," *Procedia Comput. Sci.*, vol. 79, pp. 835–844, Jan. 2016.

[7] E. O. Ochola, L. F. Mejaele, M. M. Eloff, and J. A. van der Poll, "MANET reactive routing protocols node mobility variation effect in analysing the impact of black hole attack," *SAIEE Afr. Res. J.*, vol. 108, no. 2, pp. 80–92, 2017.

[8] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95185–95199, 2019.

[9] S. Y. Han and D. Lee, "An adaptive hello messaging scheme for neighbor discovery in on-demand MANET routing protocols," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 1040–1043, May 2013.

[10] L. Wang and S. Olariu, "A two-zone hybrid routing protocol for mobile ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, no. 12, pp. 1105–1116, Dec. 2004.

[11] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Comput. Electr. Eng.*, vol. 40, no. 2, pp. 530–538, Feb. 2014.

[12] S. A. Arunmozhi and Y. Venkataramani, "Black hole attack detection and performance improvement in mobile *ad-hoc* network," *Inf. Secur. J., Global Perspective*, vol. 21, no. 3, pp. 150–158, 2012.

[13] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based gray-hole attack minimization for *ad-hoc* networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2174–2183, Aug. 2017.

[14] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks," in *Proc. MILCOM*, vol. 2, Oct. 2002, pp. 1118–1123.

[15] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 658–672, 4th Quart., 2010.

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

[17] Y. Shashwat, P. Pandey, K. V. Arya, and S. Kumar, "A modified AODV protocol for preventing blackhole attack in MANETs," *Inf. Secur. J., Global Perspective*, vol. 26, no. 5, pp. 240–248, 2020.

[18] K. H. Mohammadani, K. A. Memon, I. Memon, N. N. Hussaini, and H. Fazal, "Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 5, pp. 1–18, May 2020.

[19] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen, and C. Sun, "DAPV: Diagnosing anomalies in MANETs routing with provenance and verification," *IEEE Access*, vol. 7, pp. 35302–35316, 2019.

[20] A. Kumari, M. Singhal, and N. Yadav, "Blackhole attack implementation and its performance evaluation using AODV routing in MANET," in *Inventive Communication and Computational Technologies*. Singapore: Springer, 2020, pp. 431–438.

[21] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability," *Wireless Netw.*, vol. 26, no. 3, pp. 1981–2011, Apr. 2020.

[22] F. Taranum and K. U. R. Khan, "Maneuvering black-hole attack using different traffic generators in MANETs," in *Intelligent Systems, Technologies and Applications*. Singapore: Springer, 2020, pp. 101–115.

[23] S. Majumder and D. Bhattacharyya, "Improvement of packet delivery fraction due to discrete attacks in MANET using MAD statistical approach," in *Proc. Global AI Congr.* Singapore: Springer, 2020, pp. 187–196.

[24] V. S. Venu and D. Avula, "Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks," *Int. J. Commun. Syst.*, vol. 31, no. 6, p. e3518, Apr. 2018.

[25] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Netw.*, vol. 24, no. 2, pp. 565–579, Feb. 2018.

[26] S. Gurung and S. Chauhan, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," *Wireless Netw.*, vol. 25, no. 3, pp. 975–988, Apr. 2019.

[27] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Netw.*, vol. 24, no. 5, pp. 1821–1829, Jul. 2018.

[28] A. Nadeem and M. P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2027–2045, 4th Quart., 2013.

[29] N. Marchang, R. Datta, and S. K. Das, "A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1684–1695, Feb. 2016.

[30] S. Bu, F. R. Yu, X. P. Liu, P. Mason, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1025–1036, Mar. 2011.

[31] F. Shi, W. Liu, D. Jin, and J. Song, "A cluster-based countermeasure against blackhole attacks in MANETs," *Telecommun. Syst.*, vol. 57, no. 2, pp. 119–136, Oct. 2014.

[32] 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," *IEEE Syst. J.*, vol. 9, no. 1, pp. 65–75, Mar. 2015.

[33] M. M. Singh and J. K. Mandal, "Effect of black hole attack on MANET reliability in DSR routing protocol," in *Advanced Computing and Communication Technologies*. Singapore: Springer, 2018, pp. 275–283.

[34] I. Nurcahyani and H. Hartadi, "Performance analysis of *ad-hoc* on-demand distance vector (AODV) and dynamic source routing (DSR) under black hole attacks in mobile ad hoc network (MANET)," in *Proc. Int. Symp. Electron. Smart Devices (ISESD)*, Oct. 2018, pp. 1–5.

[35] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *Proc. Appl. Innov. Mobile Comput. (AIMoC)*, 2014, pp. 157–164.
[36] A. Dhaka, A. Nandal, and R. S. Dhaka, "Gray and black hole attack identification using control packets in MANETs," *Procedia Comput. Sci.*, vol. 54, pp. 83–91, Jan. 2015.
[37] Z. A. Zardari, J. He, N. Zhu, K. Mohammadani, M. Pathan, M. Hussain, and M. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet*, vol. 11, no. 3, p. 61, Mar. 2019.
[38] M. Tareq, R. Alsaqour, M. Abdelhaq, and M. Uddin, "Mobile ad hoc network energy cost algorithm based on artificial bee colony," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–14, Aug. 2017.
[39] D. R. C. Canedo and A. R. S. R. Romariz, "Intrusion detection system in ad hoc networks with artificial neural networks and algorithm K-means," *IEEE Latin Amer. Trans.*, vol. 17, no. 7, pp. 1109–1115, Jul. 2019.
[40] 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," *IEEE Access*, vol. 5, pp. 10369–10381, 2017.
[41] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, pp. 78–93, 4th Quart. 2008.
[42] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2471–2481, Jun. 2009.
[43] H. Gharavi, "Multichannel mobile ad hoc links for multimedia communications," *Proc. IEEE*, vol. 96, no. 1, pp. 77–96, Jan. 2008.
[44] A. O. Fapojuwo, O. Salazar, and A. B. Sesay, "Perfor mance of a QoS-based multiple-route ad hoc on-demand distance vector protocol for mobile ad hoc networks," *Can. J. Electr. Comput. Eng.*, vol. 29, nos. 1–2, pp. 149–155. 2004.
[45] R. Kalucha and D. Goyal, "A review on artificial bee colony in MANET," *Int. J. Comput. Sci. Mobile Comput.*, vol. 3, no. 7, pp. 34–40, 2014.
[46] D. Karaboga, S. Okdem, and C. Ozturk, "Cluster based wireless sensor network routing using artificial bee colony algorithm," *Wireless Netw.*, vol. 18, no. 7, pp. 847–860, 2012.
[47] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt AODV in MANET," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 621–632, May 2019.

POOJA RANI received the B.Tech. and M.Tech. degrees from Guru Nanak Dev University, Amritsar. She is currently pursuing the Ph.D. degree with Lovely Professional University, Phagwara, India. She has guided many students for various projects at graduation level, and she has also successfully guided many M.Tech. degree thesis in the areas of *ad-hoc* networks, MANETs, and VANETs. She is currently working as an Associate Professor with Rayat Bahra University, Mohali. Her research interests include security, privacy, MANETs, and VANETs. She has a keen interest in security and *ad-hoc* networks.

KAVITA (Member, IEEE) received the B.Tech. and M.Tech. degrees from Maharishi Markandeshwar University at Mullana, Ambala, India, in 2012, and the Ph.D. degree from Jaipur National University, Jaipur, India, in 2018, all in computer science and engineering. She is guiding six Ph.D. degree students. She has visited many universities out of these two are international universities in Italy and Czech Republic. She is currently working as an Associate Professor with Lovely Professional University, Phagwara, India. She has many research contributions in the areas of cloud computing, the Internet of Things, vehicular *ad-hoc* networks, WSNs, and MANETs. Some of her research findings are published in top-cited journals, such as the IEEE and Wiley, and various reputed international conferences. She is a member of the ACM and IAENG, and an editorial board member of many international journals. She has chaired many sessions in reputed international conferences in abroad and India.

SAHIL VERMA (Member, IEEE) received the B.Tech. and M.Tech. degrees from Maharishi Markandeshwar University at Mullana, Ambala, India, in 2012, and the Ph.D. degree from Jaipur National University, Jaipur, India, in 2017, all in computer science and engineering. He is currently working as an Associate Professor with Lovely Professional University, Phagwara, India. He has many research contributions in the areas of cloud computing, the Internet of Things, vehicular *ad-hoc* networks, WSNs, and MANETs. Some of his research findings are published in top-cited journals, such as the IEEE and Wiley, and various reputed international conferences. He is a member of the ACM and IAENG, and an editorial board member of many international journals. He has chaired many sessions in reputed international conferences in abroad and India. He has guided 14 master's degree students and three Ph.D. degree students and six are ongoing. He has visited many universities in abroad and India.

GIA NHU NGUYEN (Member, IEEE) received the Ph.D. degree in computer science from the Hanoi University of Science, Vietnam National University, Vietnam. He is currently the Dean of the Graduate School, Duy Tan University, Vietnam. He has a total academic teaching experience of 20 years with more than 50 publications in reputed international conferences, journals, and online book chapter contributions (indexed by SCI, SCIE, SSCI, and Scopus). His research interests include network communication, security and vulnerability, network performance analysis and simulation, cloud computing, and biomedical image processing. He is currently an Associate Editor of the *International Journal of Synthetic Emotions* (IJSE).