ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Detection and mitigation of Black hole attack in MANET using Artificial intelligence technique

[1] Saurabh Kumar, [2] Anjani Garg
[1] M.tech (Scholar,CSE), [2] AP (CSE)

***Abstract*— MANET (Mobile ad hoc network) is a self-governing network that comprises of moveable nodes that communicates with each other through wireless links. To find the route from source to destination, different routing protocols named as proactive, reactive and hybrid routing protocols are used. In the proposed work, AODV (Ad-hoc on demand) routing protocol is used. It is a packet routing protocol which is designed to use in MANET. Every node maintains a routing table that contains information about the destination node. In MANET, normally, numbers of attacks are routing protocol attacks. This research has dealt in detecting and mitigating black hole attack. The 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 proposed work, ABC (Artificial Bee Colony) algorithm is used to optimize the route from source to destination. ANN (Artificial Neural network) is used to detect and prevent the network from black hole attack. The simulation is carried out in MATLAB simulator and the performance parameters, namely, throughput, packet delivery ratio, delay are measured..**

Keywords: **MANET (Mobile Ad-hoc network), AODV (Ad-hoc on demand), ABC (Artificial Bee Colony), ANN (Artificial Neural network)**

I. INTRODUCTION

Ad Hoc networks do not have any access point to network accessibility. In MANET the wireless devices such as laptop, cell phones and notepads forms a network through which they can communicate with each other. To make communication successful, the nodes within the network follow some rules along with some trust algorithms. All the nodes in the network behave as a host as well as router that forward packets to another node. As the nodes are not stable, therefore, they work on variable topologies. In MANET to find the route between source and destination, different routing protocols are used. In the proposed research work, AODV (Ad-hoc on demand) routing protocol is used [1]

A. Ad Hoc On-Demand Distance Vector Routing (AODV)

It is a reactive routing protocol which is also known as On-demand routing protocol. In this type of protocol, whenever nodes needs the route to send data only then the route is discovered. A route is discovered by the initiation of a route discovery process by the source node [2]. The routing protocol mainly comprises of two components named as Route discovery and route maintenance.In route discovery process, RREQ request is initiated to find the route. RREQ message is forwarded inside the network until it discovers the intermediate node having recent route information for the destination

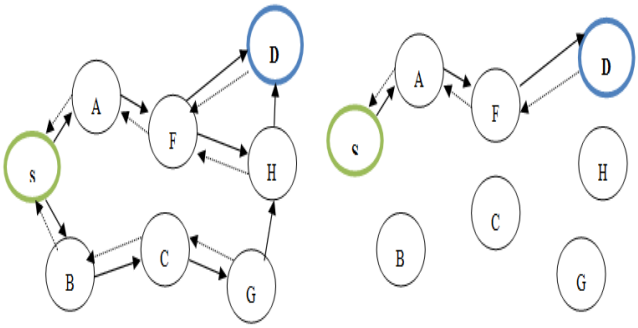


Fig.1. (a) Propagation of PREQ (b) Route determination from source to destination

The RREQ request contains sequence numbers for ensuring that the routes are loop free and reply contains latest information only. When the RREQ request is moving from one node to other node, each node keeps the records in their tables and the table further is used for constructing the reverse path for the RREQ [3]. When the request came back to source, the nodes upgrade the table accordingly. If any of the intermediate nodes change their position then the neighboring node realizes that a link failure occurs and link failure information is being transmitted to its upstream nearby node until it reaches to the source. For overcoming broken links Route error packets are used [4]. In the figure above 'S' represents the source in the network and 'D' represents destination in the network. Solid arrow represents propagation of PREQ and dotted arrow represents reverse route entry

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

Table I Characteristics of AODV routing protocol [5]

Control message	Features	Advantages
Route Request	The route that is not used for a long time deleted from the route table, thus, saves memory	AODV give response very quickly to the topological changes
Route Reply	As the nodes in the MANET are mobile so the bandwidth is constrained	Uni-cast as well as multicast data transmission is possible
Route Error	Route discovery broadcasts	Do not put any overhead as it does not uses source routing
Hello Message	AODV uses PREQ and uni-cast RREP messages to transfer packet	Do not require any central control system to handle the routing process.
		Decreases congestion.
		Robustness and scalability is better.

Security has become the main issue in the computer network. Security in ad hoc networks is a difficult issue. Thus, to provide security to the network, one must know about the types of attacks in MANET. Deficiency of any method for detection of attacks makes mobile networks more unprotected than wired network. Attacks are mainly divided into two types namely external and internal Attack.

i. External attack

An external attack is carried by the node and does not belong to the network. These kinds of attacks attempts to bring about congestion situation in the system, denial of service (DOS), and promotes wrongly routing data and so forth. Outer attacks keep the system from typical communication and delivers extra overhead to the system.

ii. Internal Attacks

Internal attacks are particularly prompts the attacks on nodes shows in system and associates interface between them [6].

II. BLACK HOLE ATTACK IN MANET

Attacker in the network has mainly two purposes, first one is to block the packet by changing the actual route of the packet and second one is to change the sequence number and hop count. In a black hole attack, the malicious node usually waits for the root node or one of the nodes to send RREQ messages to the network. When a node receives a broadcast message, it presents a new route to the destination, that is, it has the highest order number and provides a RREP message. Once the source receives the response message, it pretends to receive a response from a trusted node and it starts sending the packet to the destination. At first, it can pass the packet to its destination, and over time it will continue to throw the packet and start acting incorrectly [7].

Black hole attack is mainly divided into two types namely, single black hole attack and collaborated black hole attack. In single black hole attack, the attacker affects only one node in the network whereas in Collaborated black hole attack more than one nodes are affected by the attacker.

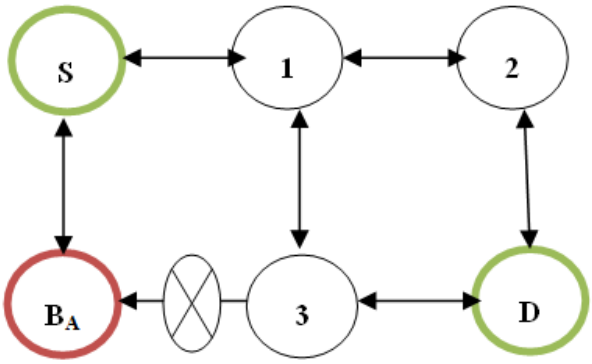


Fig. 2. Single black hole attack

The above figure has discussed how the black hole problem arises in the network. In the figure above, Source node 'S' wants to transmit data to destination node 'D'. Therefore, the route discovery process is being initiated. Here, BA is the black hole node and claims that it is an active node by receiving the PREQ packet from the source node. In response to PREQ request, BA node sends RREQ packet to the S node and in response to RREQ request node, S give the control of route by ignoring all other request and it starts sending data to node BA. In this way, black hole attack node consume all the data packets [8].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

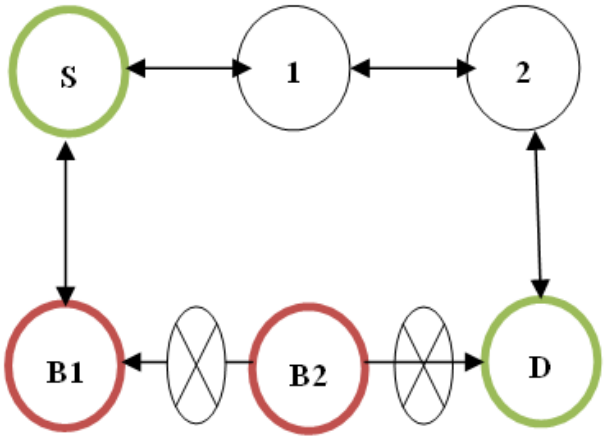


Fig. 3. Collaborated black hole attack

In the figure above, more than one node, namely, B1 and B2 are affected by the attacker and drops the packets came from source node 'S'.

III. RELATED WORK

In this section, the methods used for detecting and detecting and mitigating black hole attack in MANET are discussed. Comparison of different existing routing protocols such as AODV, DSR, DSDV along with their outcomes are discussed.

References	Proposed Work	Outcome
[10]	Black hole attack detection with prevention method for MANET utilizing AODV routing protocol.	Performance of QOS parameters is being calculated and has proposed AODV routing protocol for the prevention of network from black hole attacks but the detection and prevention rate is not acceptable.
		To improve the result of proposed work, a classifier can be used for prevention of network from attackers.
[11]	A comprehensive review of routing protocols like AODV, DSDV, DSR, SRP, TORA, and ZRP with their security aspects.	The work has focussed on the routing protocols for supporting effective communications among nodes in Ad hoc network but has not considered other topics like Scalability, Security, Traffic and Power.
[11]	A framework has been designed for hybrid routing protocols in MANET.	In this work, hybrid routes are valid and extensible based on hybridization of topology routing and geographic routing.
		The authors has used three design schemes, geographic information, routing areas, and routing structures, but the efficiency can be improved by using space technology.
[12]	A novel approach for routing in MANET on the basis of ACO (Ant colony optimization) using global positioning system and QOS parameters.	This work has focussed on the problem of ANTNET protocol and proposed a new routing protocol, OANTGPS for ad-hoc networks.
		By using the OANTGPS routing protocol, only route

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

		discovery process is accelerated but cannot simulate with mobile hosts.
[13]	A mobility-aware route selected technique for MANET on the basis of AODV and DSR.	A routing metric called mobility factor which is computed on the direction, pause time and velocity of a mobile node basis has been calculated.
		From the simulation; the performance of proposed routing protocols are significantly influenced due to nodes' mobility.
[14]	A Modified DSR protocol for the removal and detection of selective black hole attack in MANET with dynamic routing protocols.	An intrusion detection system (IDS) is proposed for detecting black hole attacks only.
		When the number of nodes in the network increases, the rate packet transmission is reduced.
[15]	FF-AOMDV with fitness function is designed by Ad Hoc On Demand Multipath Distance Vector (AOMDV). The energy-efficient multipath routing protocol of MANET with fitness function is proposed.	A new energy-saving multipath routing algorithm called FF-AOMDV is proposed in three different scenarios.
		The node speed, packet size and simulation time are different.
		Energy consumption and network lifetime are unacceptable and can be improved by using an optimization algorithm with a new fitness function
[16]	A simulator for collaborative black hole attack detection using a true link crosses check for MANET is proposed.	In the proposed work, the modified AODV is used to detect the cooperative black hole attack using cross-detection of the True-Link concept, but True-Link is a timing-based countermeasure against collaborative black hole attacks.
		In the proposed work, with more security and timestamps in link verification, routing overhead has been increased.
[17]	A simulator for risk awareness mitigation using MANET routing attacks using adaptive decision concepts.	The authors have proposed a risk response solution to reduce MANET routing attacks.
		The performance of the proposed work has been investigated, and the effectiveness and scalability of the use of risk awareness approaches are inappropriate and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

		acceptable from an observational perspective.

IV. MATERIALS AND METHODS

In this research work, for identifying and mitigating the Black hole attack in MANET, ABC (Artificial Bee colony) algorithm is used with neural network as a classifier. ABC algorithm is an optimization algorithm that is used to optimize the route and ANN is utilized for classifying the black hole attack that affects the route.

A. Artificial Bee Colony (ABC)

ABC is considered as one of the mostly utilized algorithms by author Dervis Karaboga in 2005, stimulated by the intelligent honey bees' behaviour. ABC is known as an optimization tool that gives a procedure of population based searching by which the individual call the food positions and are altered by artificial bees by time with an objective of discovering the food source places with more nectar amount [18]. In ABC system, the artificial bees flied among the multi-dimensional searching space with few of onlooker and employed bees and adopt the food sources as per the experience of itself, nest mates and correct the positions. Few of the scouts fly and determine the food sources arbitrarily without some experience. If the amount of nectar is as more as compared to existing one in the memory than the bees remember the novel position and forgets the previous one. Therefore, ABC integrates the method of local searches by onlooker and employed bees by global search methods by scouts and onlookers and later balances the exploitation and exploration

process. It works in four phases; namely, initialization phase, Employed Bee phase, Onlooker Bee and Scout Bee phase [19].

i. Initialization Phase

The food sources initially are produced arbitrarily by the following expression:

$$y_m = k_i + rand\ (0,1) * (v_i - k_i) \quad (1)$$

As defined in the above equation, v_i and k_i are the lower and upper bound for objective function solution space, rand [0,1] is a random number in a range of [0,1].

ii. Employed Bee Phase

The food sources u_{mi} is calculated and determined by the below equation:

$$u_{mi} = y_{mi} + \emptyset_{mi}(y_{mi} - y_{li}) \quad (2)$$

In the above equation, y_{mi} is an arbitrarily index of selected parameter, y_l is an arbitrarily chosen food source, $\emptyset_{mi}$is an arbitrarily number in a range of [-1 to 1]. The fitness is measured by below formula, and later on a greedy selection is being taken among y_m andu_m.

$$fit_m(y_m) = \frac{1}{1+fm(y_m)}, fm(y_m) > 0; fit_m(y_m) = 1 +; fm(y_m), fm(y_m) < 0 \quad (3)$$

In the above equation, $fm(y_m)$ is an objective function value of (y_m).

iii. Onlooker Bee Phase

The food source quantity is calculated by its profitability of food sources and itself.

$$P_m = \frac{fit_m(y_m)}{\sum_{n=1}^{SM} fit_m(y_m)} \quad (4)$$

In the above equation, $fit_m(y_m)$ is the fitness of (y_m). The onlooker bees find the food sources neighbourhood as per the below expression:

$$u_{mi} = y_m + \emptyset_{mi}(y_{mi} - y_{li}) \quad (5)$$

iv. Scout Phase

The novel solutions are arbitrarily found out by scout bees. The novel solution y_m would be designed by the scouts by utilizing the below equation:

$$y_m = k_i + rand\ (0,1) * (v_i - k_i) \quad (6)$$

As defined in the above equation, $rand\ (0,1)$ is an arbitrary number in a range of 0 to 1, v_i And k_i are the lower and upper bound of objective function solution space.

ABC Algorithm

Initialize the total bee= Total data
Initialize the bee categories- **Employed bee**
- Onlookers bee and
- Scouts bee

Set threshold of properties=f_t
Defined f_s as scout bee
For i=1 → node in route
Call objective function j

$$ABC_{obj} = \begin{cases} E_{Bee} > O_{Bee} \text{ then j True} \\ \text{E}_{\text{Bee}} \leq O_{Bee} \text{ then j false} \end{cases}$$

Return $S_{Bee}j$
Optimize_data = $ABC\ (ABC_{obj}, f_s, f_t)$
End
$S_{Bee} = optimize\_data$
Return optimize_data and prevent the node using properties of node.

A. Artificial Neural network (ANN)

The artificial neural network consists of simple elements of parallel operation. The artificial neural network is basically used with weight. When an artificial

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

neural network initially presents a pattern, it produces a random 'guess' for it [20]. Then, it will see how far it is with the actual answer and make the appropriate adjustments to its connection weights. In the proposed work, ANN is used to detect the malicious node. Neural network in MATLAB is initially trained according to the properties of the nodes used in the network. ANN is mainly comprises of three layers, input, output and hidden layer. In the hidden layer, the weights are adjusted in such a way that the difference between the input and the generated output is reduced and thus, obtaining the desired output.

In the above figure, Activation function is used to generate related outputs from weighted and input. The output is compared with the target; if the output produced is compatible with actual output then the input is correct otherwise that output will be adjusted according to the weight [21].

ANN algorithm

Load optimize properties of nodes
Initialize the ANN
Define parameters
Training data= optimize_data
Group = Real and Attacker node
Epoch=1000
Training algo=LM
Performance parameters=MSE
Neurons=50
Net= neuro $f_t(\ Training\ dta, group, neuron)$
Net= Train (net, training data, group)

Classification=$\begin{Bmatrix} Attacker; if\ properties\ not\ match \\ Real\ node; if\ match \end{Bmatrix}$

Return $\{Classified\ node\ as\ a\ attacker\}$

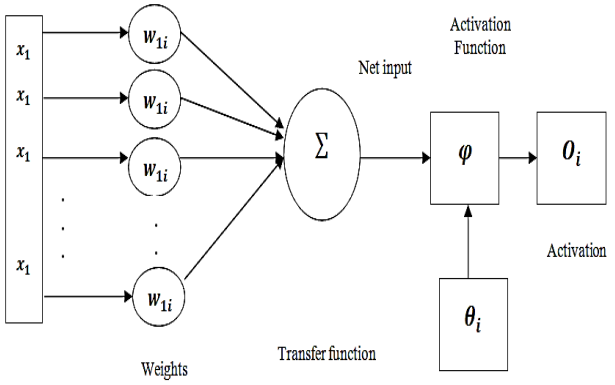


Fig. 4. Artificial Neural network

V. PROPOSED METHODOLOGY

The methods of proposed work used for preventing the network from black hole attack by using Artificial Bee Colony (ABC) and Artificial Neural network (ANN) in form of steps are discussed in this section.

Step I. Create a simulator to simulate the proposed network using the some specific dimension. To deploy the mobile ad hoc network, we have considered height of 1000m and width of 1000m. Firstly, N no. of nodes has been generated within the MANET for simulation with the help of x co-ordinates and y co-ordinates of nodes.

Step II. After the creation of simulator, the source and destination node has been described from the N nodes by using their co ordinates.

Step III. The coverage area of each node has been initialized including source and destination.

Step IV. A code is being developed for the AODV routing protocol to discover the route between source and destination node.

Step V. The ABC optimization algorithm is being initialized for the route discovery and best route selection according to the coverage set.

Step VI. For ABC optimization algorithm, the fitness function is defined according to the required information.

Step VII. If route is discovered between source and destination node then the attacker or intruders in the set route using the ANN is being checked and if attacker is being found then their identification in the cache routing table is saved.

Step VIII. On the behalf of the attacker's activities, the types of attacker have been checked and presentation from the attacker is being checked to achieve the better results.

Step IX. To check the accuracy and efficiency of the proposed simulation work we calculate the QOS parameters like Throughput, Delay, and Packet Delivery Ratio etc.

The parameters used for calculating the performance of the proposed work are:

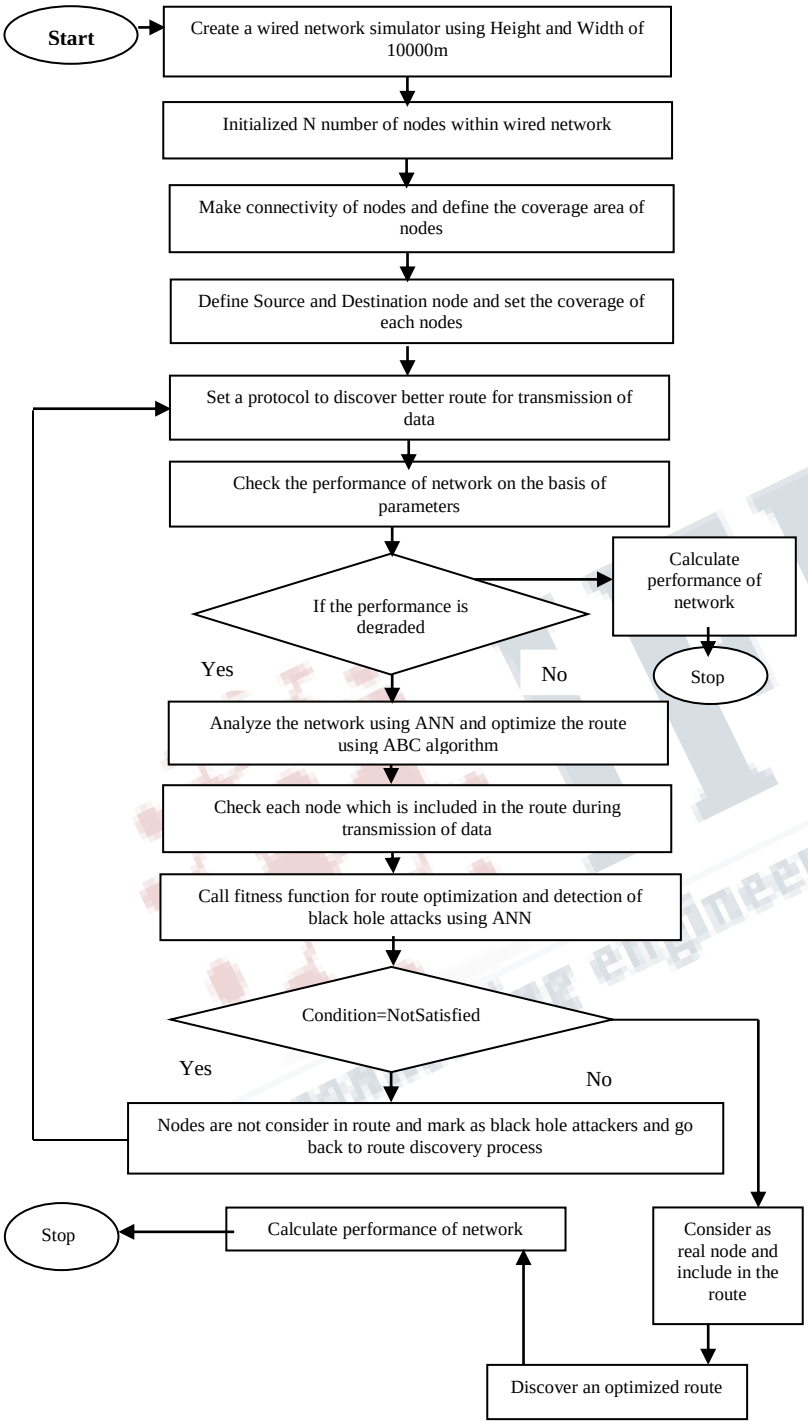
A. Throughput

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 (%).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

Fig. 5. Flowchart of proposed work



Throughput can be described as:

$$\text{Throughput} = \frac{\sum \text{Packets sent}}{\text{Total data packets}} \quad (7)$$

B. 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:

$$D_{end\text{-}end} = D_{trans} + D_{prop} + D_{proc} \quad (8)$$

Where $D_{end\text{-}end}$= End-To-End Delay (9)

As shown, D_{trans}= Transmission Delay (D_{prop}= Propagation Delay and D_{proc}= Processing Delay

C. 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:

$$\text{Energy consumption} = E_{Tx} + E_{Rx} + E_{Amp} + E_{Agg} + E_{Prop} \quad (10)$$

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

D.PDR (Packet Deliver rate)

It is defined as the ratio of packets that are effectively delivered to the destination as compared to the packets that are transferred by the sender.

$$\text{PDR} = \frac{\text{number of packets delivered}}{\text{number of packets sent}} \quad (11)$$

VI. SIMULATION RESULTS

The proposed work is executed in MATLAB simulator. MATLAB is a simulating tool used for manipulating matrix and solving linear algebra. MATLAB is abbreviation for Matrix laboratory. The performance parameters like throughput, delay, Bit error rate (BER), energy consumption, Packet delivery ratio (PDR) are calculated. The size of network area of 1000×1000 having 50 numbers of nodes is simulated in MATLAB.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

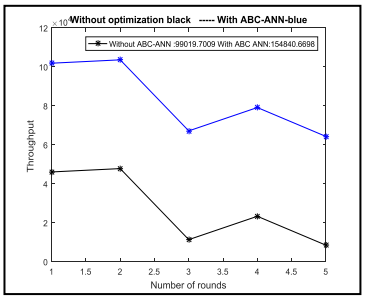


Fig. 6. Throughput values with optimization and without optimization of the network

The performance of throughput is shown in figure 6. In the figure, the black colour line indicates the throughput values obtained in case of without optimization i.e. no algorithm or protocol is used to reach the packet at the destination node. The blue line indicates the throughput values obtained for the MANET with optimization i.e. ABC and ANN are used to find the accurate path and the packet has to reach at exact destination. The process is repeated five times to have the accurate results. The average throughput values obtained for the network without optimization is $3.11*10^4$ whereas the throughput values obtained for network with ABC and ANN is $8.59*10^4$.Therefore, it is clear that the average value obtained for network with optimization is better as compared to without optimization.

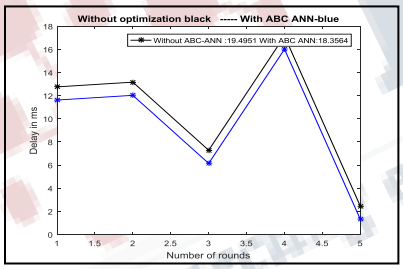


Fig.7. Delay in network with and without optimization

Above figure is depicting the result of the delay obtained. In the above figure, black line shows the delay occurred in case of without optimization and blue line is indicating the delay with optimization. It is being seen that the delay value obtained for network with optimization is less than the value obtained for without optimization which means that in without optimization case, the data packets takes more time to reach at the destination than with optimization case. The average value of delay obtained with and without optimization are 9.36ms and 10.64ms respectively.

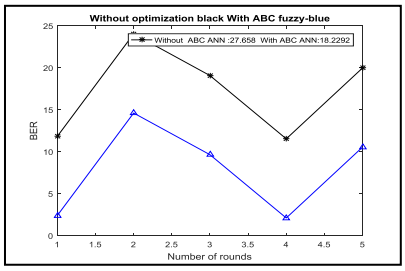


Fig. 8. BER in network with and without optimization

The result obtained for Bit error rate is shown in above figure. When ABC and ANN are applied to the network, Bit error rate came out to be less as compared to the BER obtained for the network without ABC and Fuzzy. Therefore, the results obtained for the network using optimization are better than without optimization. The average value obtained for BER with and without optimization in MANET are 7.6 and 17.2 respectively.

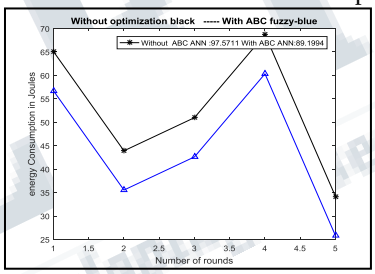


Fig. 9. Energy consumption (Joule) in network with and without optimization

Above figure is for energy consumption. It is being seen that more energy is consumed without optimization algorithm than with optimization algorithm being applied to the network. In case of without optimization, the energy consumption is 52.2 whereas; in case of with optimization, the energy consumption is 43.6 which is less as compared to without optimization. Thus, there is an improvement of 19.72% of the total power consumed when optimization algorithm has been applied.

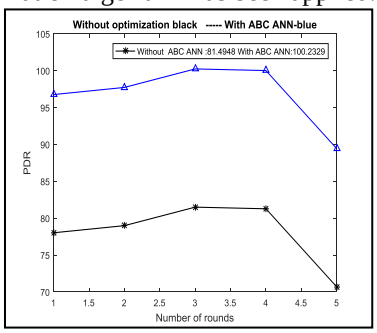


Fig. 10. PDR in network with and without optimization

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

From the above Figure 10, it is concluded that with AODV routing protocol, the packet delivery rate is less whereas when optimization algorithm (ABC) along with classification algorithm (ANN) has been applied. The average value of PDR obtained with optimization and without optimization are 96.4 and 78.4 respectively.

A. Comparison of Proposed Work With Existing Work

In this section, the comparison of existing work with the proposed work is depicted. The comparison has been drawn on the basis of delay and PDR. The work of [22] has been used for the comparison. Below figure represents the comparison of delay. Red line indicates the delay values of existing work and blue line indicates the delay values of proposed work. In the proposed work, delay has been calculated when AODV routing protocol is applied in MANET.

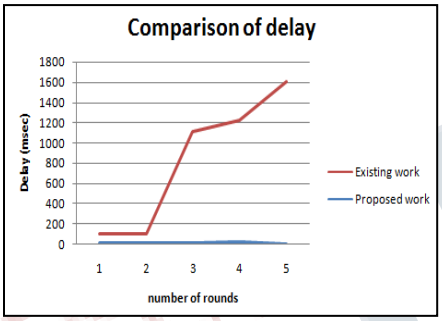


Fig. 11. Delay of proposed work and existing work

When ABC along with ANN is applied, delay is being reduced and approximately become zero. It can be seen that delay for the proposed work is almost negligible as compared to the delay for existing work.

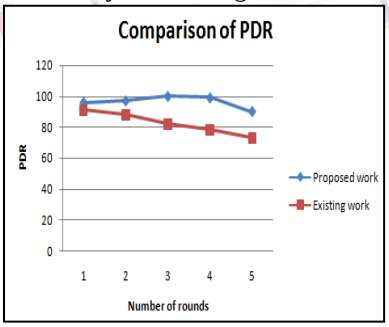


Fig.12. Comparison of PDR

The comparison of packet delivery ratio for proposed work and existing work is shown in the above figure. The blue line represents the PDR values obtained for the proposed work and red line indicates the PDR value obtained for the existing work. It is concluded that the average value PDR for the proposed work and existing work are 96.4% and 82% respectively. Thus, there is an increment of 14.4% when ABC-ANN is used in the network. Therefore, it is being concluded that PDR for proposed work is better as compared to the existing work.

VII. CONCLUSION

Ad hoc network comprises of number of nodes being that are interconnected with each other for communication purpose. The concept of Ad hoc network is not that familiar to end users who have a typical router for sending the wireless signals. For deploying the network in Ad hoc network, configuration of network is considered. MANETs are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the black hole attack as there is no centralized security management. In the proposed work, mitigation of the black hole attack in MANET is considered using Artificial Bee Colony (ABC) along with Artificial Neural Network (ANN) as a classifier. Route from source to destination has been created using AODV routing protocol. Many researchers have proposed a number of prevention techniques for black hole attack because only routing protocols cannot enhance the performance. Therefore, the performance of AODV routing protocol has been increased by using optimization and classification algorithms. The performance parameters like throughput, bit error rate, Packet delivery ratio, and delay have been improved using optimization and classification algorithms. Throughput is being increased by 54.8 % when ABC and ANN have been applied, BER decreases by 9.6msec, PDR increases by 18%, and delay decreases by 12.8 msec. A comparison of proposed with existing work has been done and it is concluded that ABC along with ANN has performed well as compared to existing techniques. In future work, for classification neural network can be used along with fuzzy logic and for optimization Artificial Bee Colony (ABC) can be used in hybridization with Genetic algorithm. Thus, the detection and prevention of black hole attack can be improved and hence, can increase the accuracy of the network.

REFERENCES

1. Tseng, F. H., Chou, L. D., & Chao, H. C, “A survey of black hole attacks in wireless mobile

ad hoc networks," Human-centric Computing and Information Sciences, vol.1, issue 1, 2011

2. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," IJ Network Security, vol. 5, issue 3, pp. 338-346, 2007.
3. Keerthika, V., & Malarvizhi, N, "Mitigate black hole attack using trust with AODV in MANET," Computing for Sustainable Global Development (INDIACom), pp. 470-474), 2016.
4. Woungang, I., Dhurandher, S. K., Koo, V., & Traore, I, " Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad Hoc networks, Globecom Workshops (GC Wkshps), IEEE, pp. 1037-1041,2012.
5. Mukherjee, S., Chattopadhyay, M., & Chattopadhyay, S, "A novel encounter based trust evaluation for AODV routing in MANET," Applications and Innovations in Mobile Computing (AIMoC), IEEE, pp. 141-145, 2015.
6. Lupia, A., & De Rango, F, "Performance evaluation of secure AODV with trust management under an energy aware perspective," Performance Evaluation of Computer and Telecommunication Systems, IEEE, pp. 599-606, 2014.
7. Abdelhaq, M., Serhan, S., Alsaqour, R., & Satria, A., "Security routing mechanism for black hole attack over AODV MANET routing protocol," Australian Journal of Basic and Applied Sciences, vol. 5, issue 10, pp.1137-1145,2011.
8. Lo, N. W., & Liu, F. L, "A secure routing protocol to prevent cooperative black hole attack in MANET," Intelligent technologies and engineering systems, Springer, pp. 59-65, 2013.
9. Dhama, S., Sharma, S., & Saini, M, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks," Computing for Sustainable Global Development (INDIACom), IEEE, pp. 2993-2996, 2016.
10. Gupta, A. K., Sadawarti, H., & Verma, A. K, " A review of routing protocols for mobile ad hoc networks," SEAS Transactions on Communications, vol. 10, issue 11,pp. 331-340,2011.
11. Cheng, H., & Cao, J, "A design framework and taxonomy for hybrid routing protocols in mobile ad hoc networks," IEEE Communications Surveys & Tutorials, vol. 10, issue 3, 2008.
12. Karia, D. C., & Godbole, V. V, "New approach for routing in mobile ad-hoc networks based on ant colony optimisation with global positioning system," IET networks, vol. 2, issue 3, pp.171-180,2013.
13. Sarkar, S., & Datta, R, "Mobility-aware route selection technique for mobile ad hoc networks," IET Wireless Sensor Systems, vol. 7, issue 3, pp55-64,2017.
14. Mohanapriya, M., & Krishnamurthi, I, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," Computers & Electrical Engineering, vol. 40, issue 2, pp. 530-538, 2014.
15. Taha, A., Alsaqour, R., Uddin, M., Abdelhaq, M., & Saba, T, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," IEEE Access, vol. 5, pp.10369-10381,2017.
16. Wahane, G., Kanthe, A. M., & Simunic, D, "Detection of cooperative black hole attack using crosschecking with truelink in MANET," Computational Intelligence and Computing Research, IEEE International Conference ,pp. 1-6,2014.
17. Zhao, Z., Hu, H., Ahn, G. J., & Wu, R., "Risk-aware mitigation for MANET routing attacks," IEEE Transactions on dependable and secure computing, vol. 9, issue 2, pp.250-260,2012.
18. Mohan, B. C., & Baskaran, R, "Energy aware and energy efficient routing protocol for adhoc

network using restructured artificial bee colony system. High Performance Architecture and Grid Computing," pp. 473-484,2011.

19. Barani, F., & Abadi, M, "BeeID: intrusion detection in AODV-based MANETs using artificial bee colony and negative selection algorithms," ISC international journal of information security, vol. 4, issue 1, pp.25-39,2012.

20. Kaur, R., & Kaur, A. (2014). Blackhole Detection In Manets Using Artificial Neural Networks. International Journal For Technological Research In Engineering, 1(9), 959-962.

21. Singh, J. P., Dutta, P., & Pal, A, "Delay prediction in mobile ad hoc network using artificial neural network," Procedia Technology, vol. 4, pp.201-206, 2012.

22. Poongodi, T., & Karthikeyan, M, "Localized secure routing architecture against cooperative black hole attack in mobile Ad hoc networks," Wireless Personal Communications, vol. 90, issue 2, pp. 1039-1050,2016.