INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Mitigation of Sinkhole Attack in MANET Using ACO

Saurbh Sharma
Research Scholar
L.R. Institute of Engineering & Technology, Solan, Himachal
er.saurabhsharma64@gmail.com

Kanchan Bala Jaswak
Assistant Professor
L.R. Institute of Engineering & Technology, Solan, Himachal
t.kanchan103@gmail.com

Abstract: ***MANET (Mobile ad hoc network) is the emerging and most demanding technology of wireless network. Because of self-deliberate property, the network points behave as router or source and the nodes keep moving freely in the network area. MANET plays a significant role in connection less infrastructure. Securing a network is the fundamental issue in MANET for securing the susceptible information from hackers. MANET has different attacks that are routing protocol attacks. The sink hole is known as the severe one from all the attacks in MANET. It generally attracts the neighbour's nodes towards itself and transmits the bogus or fake routing path. This attack decreases the network lifetime and increases the network overhead by boosting energy consumption and later destroys the network. In the proposed work, the routing protocol is being optimized by utilizing ACO (Ant Colony Optimization) with NN (Neural Network) for achieving enhanced performance as compared to existing work. Different parameters, namely, Bit error rate, throughput, an end to end delay and energy consumption are used for calculating the performance of the proposed wok in MANET or to check the effect of Sinkhole attack. The environment created by simulating the work has 50 to 100 nodes. The width and height of the network is 1000 nodes***

Keyword: MANET, Neural Network, Ant Colony Optimization, Error Rate, Energy Consumption, Throughput, Delay.

I. INTRODUCTION

MANET (Mobile Ad hoc Network) is a self-arranging system of movable routers joined by remote connections with no entrance point. Each movable device in a system is self-governing as there is no central authority in the MANET. The movable devices are allowed to shift freely and compose themselves subjectively. It performs a significant role with its dynamic nature. It permits the mobile nodes to either connect or disconnect from the network freely. The mobile nodes capability for communication is not limited. The data may lose in a case when the connection is established in ad hoc network and the nodes of mobile are out of radio range area. The architecture of MANET is shown in figure 1.

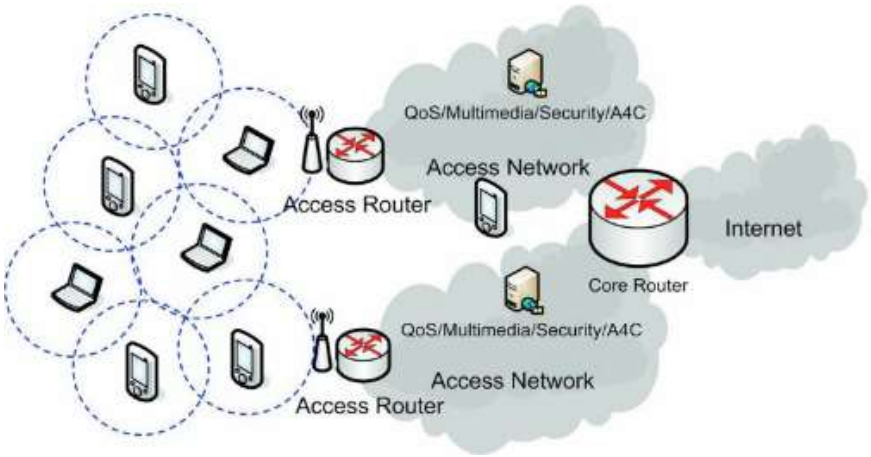

Figure 1: Mobile ad hoc Network Architecture

The security concern is a general concern for ad hoc network for securing the communication among mobile hops intended in the antagonistic network. The validated networks, as well as the intruder attackers, usually connect the wireless channel. The attacks are characterized by two types of attacks, namely, active and passive attacks. There is no modification of data in passive attacks, though it only listens and the active attack, the data is being directed to the network area, like alteration, duplication and exchange data removal. Ad hoc network is susceptible to some attacks. The sink hole is considered as one of the risky attacks in the network.

II. SINK HOLE ATTACK

Sinkhole attack is one of the risky and dangerous attacks in MANET. In this attack, an intruder hop transfers the immoral message of routing for generating itself as definite hop and considers the volume of the network for transferring the data. When the whole network is entertained, the private data get moderated like a variation of data packets or packet may drop for making the network complex.

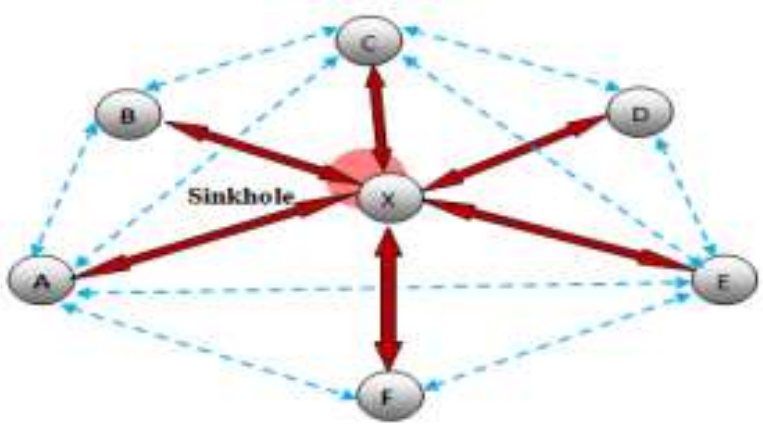

Figure 2: Sink Hole attack in MANET

The evil node tries to focus on the information or the protected data from the nearest hops. The sinkhole attack usually distresses ad hoc network functioning of protocols, namely, DSR, AODV and ZRP and so on. This is done by utilizing traffic with an enlargement of the sequence number or by lessening the hop count among routers. The route presented by the intruder is taken as a healthier path.

III. SIMULATION ALGORITHMS

In the proposed work, the routing protocol has been optimized by using an ant colony optimization (ACO) with artificial intelligence concept to achieve better performance than other techniques.

3.1 Neural network

Neural networks are composed of simple elements which operate in parallel. A neural network can be trained to perform a particular function by adjusting the values of the weights between elements. Network function is determined by the connections between elements. There is activation function used to produce relevant output. A Neural Network Classifier is based on neural networks consisting of interconnected neurons. From a simplified perspective, a neuron takes positive and negative stimuli (numerical values) from other neurons and when the weighted sum of the stimuli is greater than a given threshold value, it activates itself. The output value of the neuron is usually a non-linear transformation of the sum of stimuli.

3.2 Ant Colony Optimization (ACO)

Ant colony optimization is an optimization algorithm class that are inspired by the managed collaborative ant behaviours. Ants are the individuals of nature with less intelligence looking for the nests to search for food. ACO defines the concepts of net building, food foraging, cooperative support, labour division, cemetery organization and self-assembly of actual ants for the approaches of meta-heuristic. Algorithm for ACO is defined below:

Input: An instance y of integrated optimization problem

While termination condition not achieved do

Schedule Activities
Ant dependent solution construction ( )

Pheromone update ( )

Daemon actions ( )

End Scheduled Activities

S_{best}→enhanced solution in population of solutions

End while

Output: S_{best} candidate to enhanced solution for x

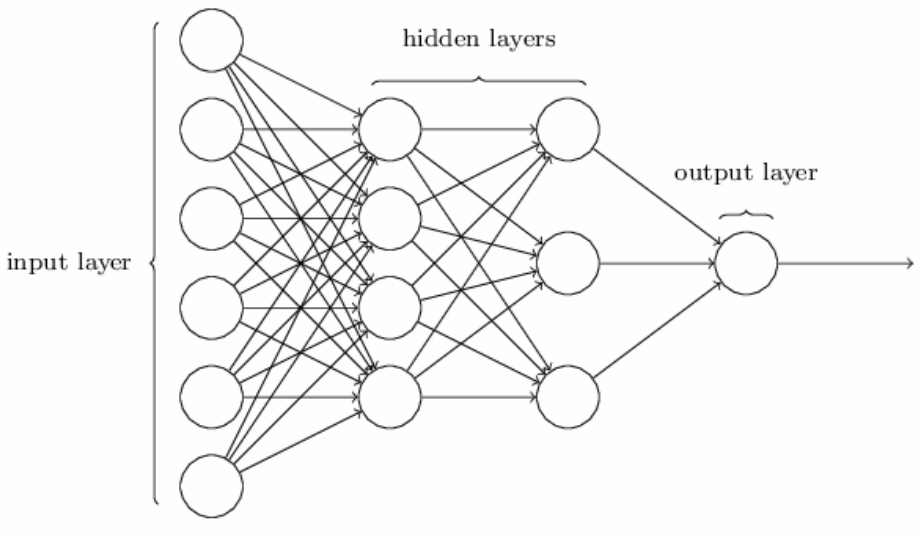

Figure 3: Neural Network Architecture

IV. PROPOSED MODEL

This work has dealt with the detection and prevention of Sink Hole attack. For the optimization purpose, optimization algorithm, ACO with classification algorithm, NN has been used. Parameters, namely, throughput, Bit error rate, delay, and energy consumption are used for calculating performance and are defined below:

i. Throughput

It is defined as the total number of packets transmitted in the whole simulation time. The amount of packet data transferred from one place (source) to another place (destination) in a specified amount of time. Packet data transfer rates for networks are measured in terms of throughput. Typically, throughputs are measured in Kbps, Mbps, and Gbps and we denote in the percentage. Mathematically, it can be defined as:

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

Throughput= N / 1000

Where N is the number of successfully received bits.

ii. End to end delay

End-to-end delay refers to the time taken for a packet data to be transmitted across a network from source node to destination node. So, in the network, we use those routes in which the probability of end to end delay is less so that the performance of the proposed work can be better. In the mathematical term, we can say that the end to end delay is the total amount of time which is elapsed during the transmission of packet data.

$D_{end\text{-}end} = D_{trans} + D_{prop} + D_{proc}$

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

D_{trans}= Transmission Delay

D_{prop}= Propagation Delay

iii. Bit error rate

It is described as the rate at which the error takes place in the transmission system. It can be normally transferred in a number of errors that exists in the string of different bits. Mathematically, it can be defined as:

$$BER = \frac{Number\ of\ errors}{Total\ number\ of\ bits\ sent}$$

Bit Error Rate is the main parameter which is utilized in assessing systems for transmitting the digital data from one location to another location.

iv. Energy Consumption

Energy consumption is described as the amount of unit needed for the key transmission during the simulation process. The energy consumption is concerned with optimal path selection that needs less energy for routing the data from source to destination.

The model for simulating the work is defined below:

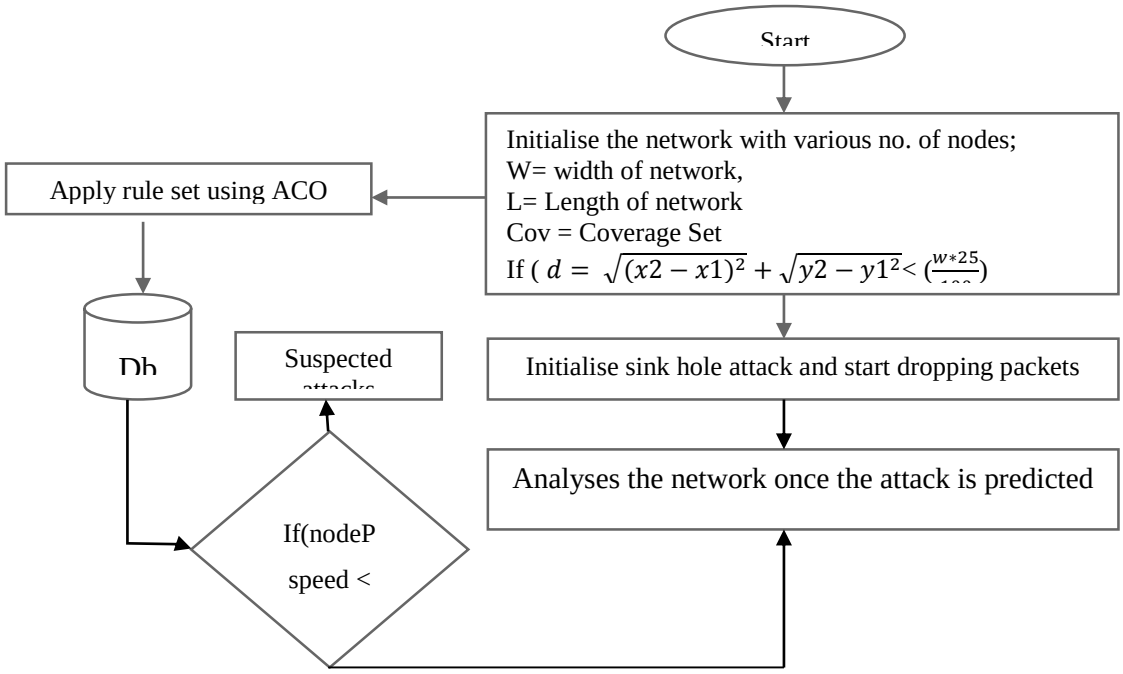

Figure 4: Proposed Model

Step I. Start
Step II. Initialize the network with various no. of nodes.
Step III. Enter width and length of the network to implement the network.
Step IV. Calculation of X and Y location of nodes
Step V. Deployment of sensor nodes in network
Step VI. Plotting of source and destination
Step VII. Find source and destination
Step VIII. Find coverage set, and then find the distance and then request HELLO message.
Step IX. Optimize using ACO and Neural Network to find an attack.Each layer represents a path which consists of sequences of positive integers that represent the IDs of nodes through which a routing path passes with the source node followed by intermediate nodes (via nodes), and the last node indicating the destination, which is the goal. Evaluate optimal route selection.
Step X. End

V. SIMULATION RESULTS

This section shows the result obtained after the simulation of the proposed mode. The following results in MATLAB with 50-100 nodes have been obtained.

Below diagram is describing the environment of simulation showing the number of nodes that are being considered for running the network and is taken 50. The width of the network is taken as 1000 and the height is also taken as 1000.

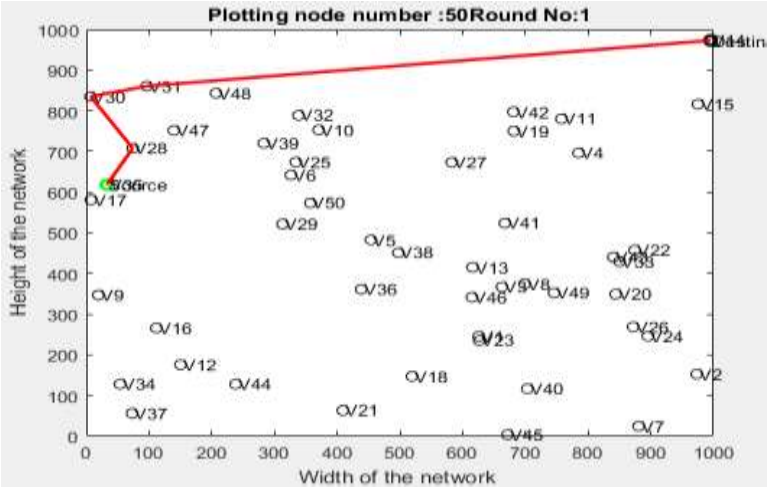

Figure 5: Route between Source and Destination

Above figure is describing the route between the source and the destination. The route is being used for transferring the data. The green colour is describing the source while dark black is defining the destination. Red line is the route from source to destination using coverage area.

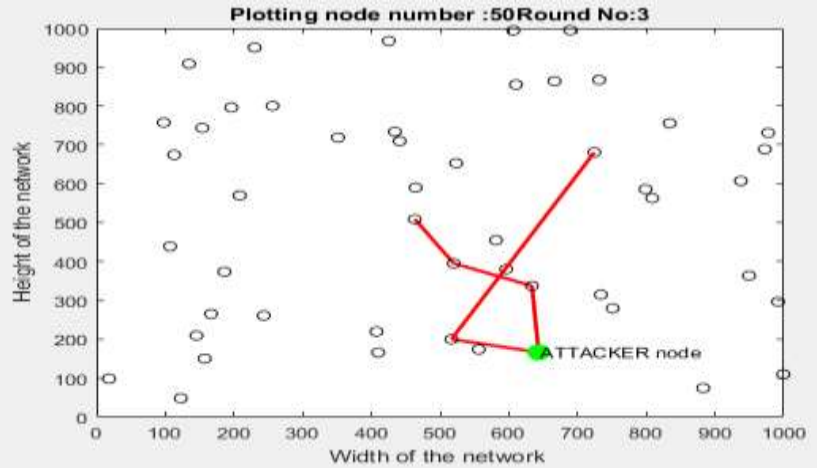

Figure 6: Initialization of Attacker

Above figure is defining the transmission of data from the source node to destination node with attackers. When packet data travels from source to destination via the route, then attacker initializes in the route. Green color node is attacker node as shown above that creates a problem. Due to the attacker, the efficiency of proposed work affects. Therefore, to remove this, NN with ACO is being used in the work.

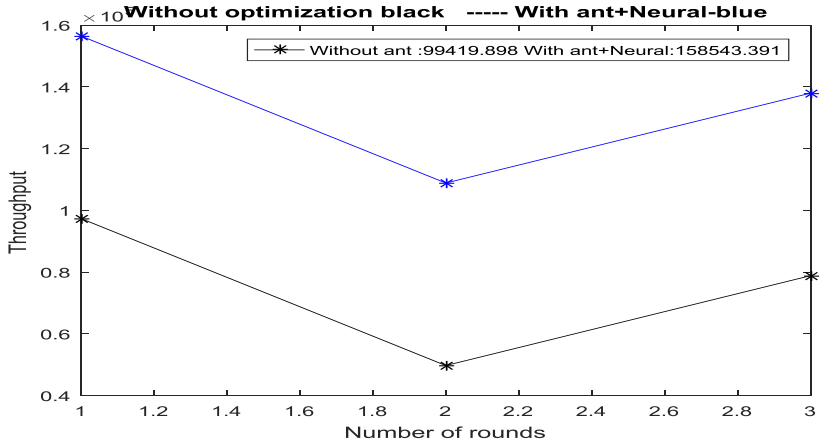

Figure 7: Throughput Comparison

Above figure shows the comparison of throughput between without ACO and with ACO technique. The black colour is defining the results obtained by without optimization and the blue line is defining the results obtained by with optimization that is with ACO and NN. The maximum throughput obtained without optimization is 99419.898 whereas the maximum throughput obtained with optimization is 158543.391.

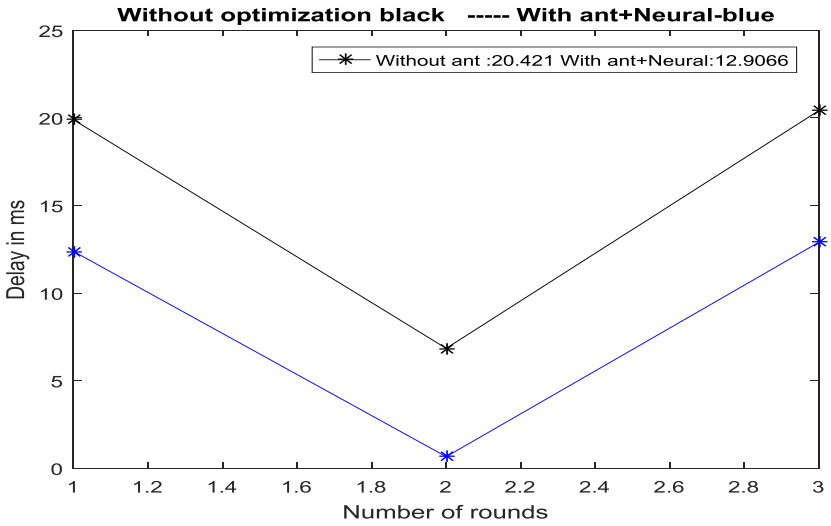

Figure 8: Delay Comparison

Above figure is defining the comparison of delay for with and without optimization. The blue line indicates the results obtained with optimization with a maximum value near about the 12.91 seconds. Black colour line graph represents the delay value without optimization and the maximum value of delay without optimization is near about the 20.42 seconds. From the above observation, it is concluded that the delivery time of packets from the source node to the destination node is better.

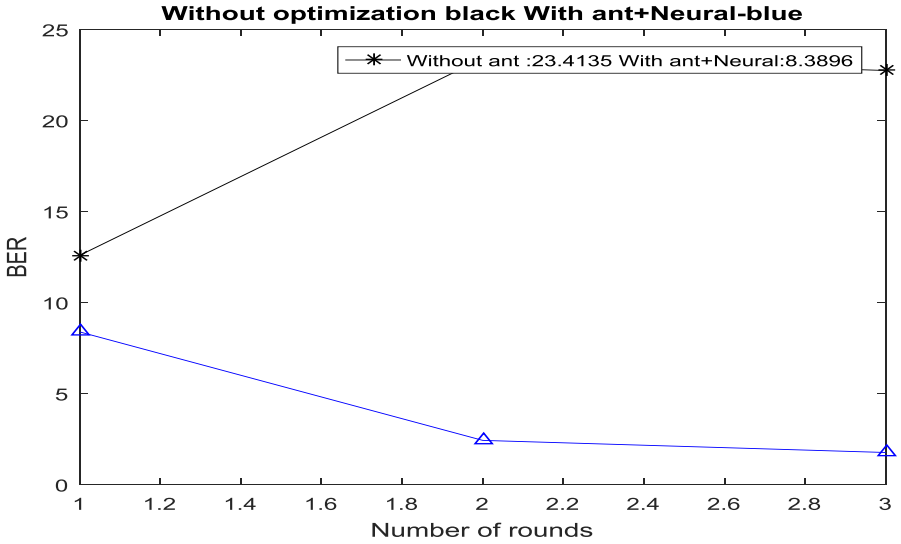

Figure 9: BER Comparison

Above figure is defining the comparison of BER for with and without optimization. The blue line indicates the result obtained with optimization and the maximum value of BER is near about the 8.38. Black colour line graph represents the BER value without optimization and the maximum value of BER without optimization is near about the 23.41. We can clearly say that the rate of error during the transmission of packets from the source node to the destination node is better.

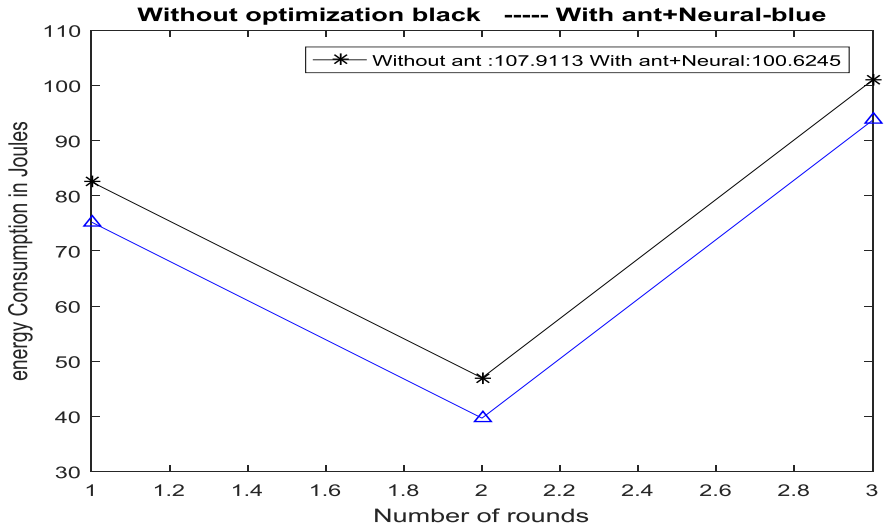

Figure 10: Energy Consumption Comparison

Above figure is defining the comparison of energy consumption for with and without optimization. The blue line indicates the result obtained with optimization and the maximum value of energy consumption is near about the 100.62J. Black colour line graph represents the energy consumption value without optimization and the maximum value of energy consumption without optimization is near about the 107.91. From the above observation, the rate of energy consumption during the transmission of packets from the source node to the destination node with optimization is less.

VI. CONCLUSION

Ad hoc network consists of individual devices for the communication purpose with each other. The concept of Ad hoc network is not that familiar to end users that have a typical router for sending the wireless signals. For deploying the network in Ad hoc network, the configuration of the network is considered. MANET is the known as a popular network that is utilized mostly because of its dynamic nature. Such networks detect sinkhole attack because of negligible security management and considered as the severe attacks and make the trustable nodes to the malicious nodes and even can result in loss of information. In this thesis, Detection and mitigation of sinkhole attack are considered. ACO (Ant colony optimization) has been used for the optimization and the rule sets are applied by using the same. The neural network is used for the detection of sinkhole attack. Parameters like Throughput, End to end delay, Bit error rate and energy consumption are used for detecting the attack. From the results, it is being seen that the when the comparison of throughput is considered for with and without optimization, throughput came out to be better when with optimization case is considered means when ACO is used. It came out to be 158543.391 in case of with optimization. While considering the case of Delay, with ACO, it came out to be 12.91 sec whereas, without optimization, it is 20.42 sec. Therefore, it can be said that delay is less when optimization is considered. BER should be less for the reliable system. In the proposed work, BER in case of optimization is 8.38 whereas, without optimization, it is 23.41. Thus, it is clear from the values that BER is less in the proposed work. The energy consumption while packets transmission from the source node to destination node should be less. In the proposed work, in case of ACO, it is 100.62 J whereas, without optimization, it came out to be 107.91 J. Therefore, on an all, it is clear that as compared to the existing work, the proposed work has performed better.

REFERENCES

[1] Nasipuri, A. (2004). Mobile ad hoc networks. *Handbook of RF and Wireless Technologies*, 59-100.

[2] Singh, Suresh, Mike Woo, and Cauligi S. Raghavendra. "Power-aware routing in mobile ad hoc networks." *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998.

[3] Subbaiah, K. Venkata, and M. M. Naidu. "Mobile Ad Hoc Network." *Simulation* 1.04 (2010): 246-251.

[4] Gandhewar, Nisarg, and Rahila Patel. "Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network." *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on*. IEEE, 2012.

[5] Jathe, Sonal R., and Dhananjay M. Dakhane. "Indicators for detecting Sinkhole Attack in MANET." *International Journal of Emerging Technology and Advanced Engineering* 2.1 (2012).

[6] Culpepper, Benjamin Jack, and H. Chris Tseng. "Sinkhole intrusion indicators in DSR MANETs." *Broadband Networks, 2004. BroadNets 2004. Proceedings. First International Conference on*. IEEE, 2004.

[7] Mitrokotsa, Aikaterini, Nikos Komninos, and Christos Douligeris. "Intrusion detection with neural networks and watermarking techniques for MANET." *Pervasive Services, IEEE International Conference on*. IEEE, 2007.

[8] Shah, Satish K., and Dharmistha D. Vishwakarma. "Development and Simulation of Artificial Neural Network based the decision on parametric values for Performance Optimization of Reactive Routing Protocol for MANET using Qualnet." *Computational Intelligence and Communication Networks (CICN), 2010 International Conference on*. IEEE, 2010.

[9] Baskaran, R., P. Victer Paul, and P. Dhavachelvan. "Ant colony optimization for data cache technique in MANET." *Proceedings of International Conference on Advances in Computing*. Springer, New Delhi, 2013.

[10] Kumar, Lalan. "Performance evaluation of ACO based on demand routing algorithm for mobile ad hoc networks." *International Journal of Engineering Science & Technology* 3.3 (2011): 1809-1815.

[11] Arif, Mohammad, and Tara Rani. "ACO based routing for MANETS." *arXiv preprint arXiv: 1205.1604* (2012).

[12] Macker, Joseph. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).

[13] Al-Ani, Razan. "Simulation and performance analysis evaluation for variant MANET routing protocols." *International Journal of Advancements in Computing Technology* 3.1 (2011): 1-12.

[14] Sharma, Parul, Arvind Kalia, and Jawahar Thakur. "Performance analysis of AODV, DSR AND DSDV routing protocols in the mobile ad-hoc network (MANET)." *Journal of Information Systems and Communication* 3.1 (2012): 322.

