iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Improvisation of QOS Parameters by Detecting and Preventing the Black Hole Attacks using Artificial Intelligence Techniques

Meenanshu Gupta[1], Mr. Varun Jasuja[2]
[1]*Student,* [2]*Assistant Professor, Guru Nanak Institute of Technology, Mullana Kurukshetra University, Kurukshetra*

Abstract: ***Mobile ad hoc networks (MANETs) are the integration of number of freely moving nodes that are used to transfer information from one node to other node within the network. MANET finds the applications in different areas like in medical field, military area, battlefield, home applications etc. But the performance of these networks are degraded by different attackers named as Black hole attack, gray hole attack, sink hole attack etc. In this research work, we have proposed an efficient method to detect and prevent Black hole attack in mobile ad hoc network (MANET). Cuckoo search algorithm is used for optimizing the properties of the nodes according to the objective functions and then the optimized properties of the nodes are trained by using a classifier known as artificial neural network (ANN). By using ANN, Black hole attack is identified and removed from the route. Afterwards, performance parameters like throughput, delay, energy consumption and bit Error Rate are determined.***
Keyword: MANET, Cuckoo Search (CS), Artificial Neural Network (ANN), Black Hole Attack, AODV.

I. INTRODUCTION

A mobile ad –hoc network is an integration of electronic devices like cell phones, laptops, PCs, satellites etc. In this network, all the communicating devices are connecting wirelessly through radio links. All the devices are free to move in any direction and thus, make communicating links to other devices quickly [1]. Due to independent nature, the Ad hoc networks find the application in the fields like in military, battlefield. In Military, ad-hoc networks are used to connect soldiers or other military units to each other. In battlefield, sensor nodes gather the information about soldiers and the environment of the field [2]. These networks are used in the places where creating the infrastructure is impossible and expensive. In MANET, every device acts as a host when requesting or providing information to or from the nodes within the network. Nodes in the network also act as a router whenever route maintenance/discovering are required within the network.

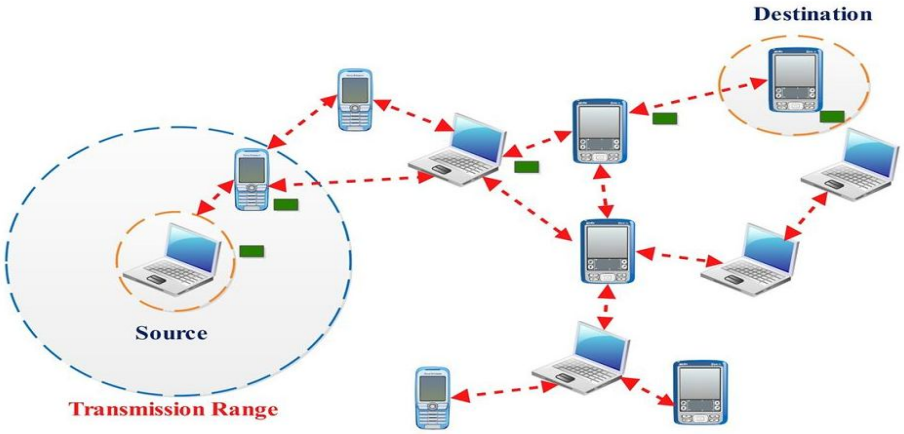


Fig. 1 MANET

Mainly, three protocols, namely, Destination Sequenced Distance Vector routing (DSDV), Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) are used in the network to discover the best possible route [3]. DSDV is a table driven routing protocol in which every node in the network keeps a routing table in which the address of destination node along with the

number of hopes are controlled. For maintaining consistency, the routing table has been updated whenever route in the network is changed. DSDV routing protocol is a not applicable in large area network because as the network grows, the overhead also increases. DSR is an On-demand routing protocol and it saves the routing address in cache memory [4]. By using DSR routing protocol, every data packet contains the complete information along with the destination of the node. AODV is an On -demand routing protocol that will generate route only when the source nodes are required. Whenever source node wants to transmit data to destination node, it firstly search for the free route and if route is not available then it broadcasts Route Request (RREQ) message to their nearby nodes, which travels from one node to other node until a fresh node has been determined. Every node has maintained RREQ message in their routing table when a route has been discovered. The Route Response (RREP) message is being unicasted to the neighboring node from which the RREP message has been obtained. When RREP message is received by the source node, it will start transmitting the data to the destination node [5].AODV routing protocol is susceptible to the Black hole attack. The node with black hole responds to the RREQ message being generated by the source node and sends a RREP message falsely. Source node assumed that black hole node is the destination node and starts transmitting packets to black hole node. Thus, the packets reached at the black hole node dropped by it rather than forwarding to the destination node [6].In this paper, we have proposed a method to identify black hole node by using cuckoo search technique and neural network. The rest of the paper is organized as follows: In section 2 single and cooperative black hole attack has been discussed. Next, in section 3, the methods used to optimize and classify the black hole attack are discussed. In section 4, related work followed by section 5 that contains methodology, results and finally conclusion and future scope has been discussed.

II. BLACK HOLE ATTACK

A black hole attack is a dangerous attack occurred in MANET. A black hole consists of two types, namely, single black hole attack and a multiple black hole attack. In single black hole attack, only one node is suffered whereas in multiple black hole attacks, a number of malicious nodes are present in the network. An example of single black hole attack is described below;

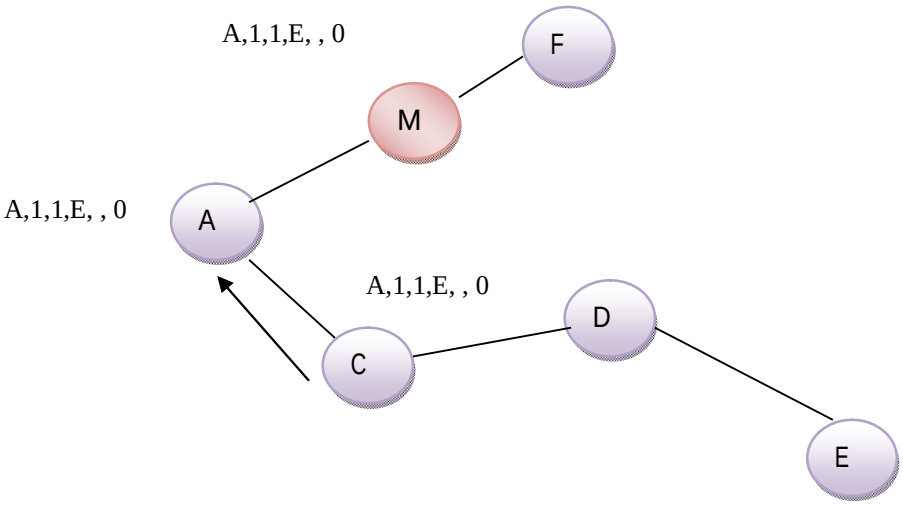


Fig.2 Black hole attack

As shown in the figure above, a network is formed with 6 nodes. Here, M is the malicious node. Let us consider that A is a source node that wants to transmit the data. To transmit data from node A to E. A is having no idea to transmit data to node E. So, for transmitting the data, node A searches for the route. So 'A' send RREQ request. That contains a source address, sequence number, broadcast ID, destination address, destination sequence number, hope count [7]. A starts broadcast this packet to node M and C node. If the node has path to reach at node E then the nodes will reply other for the message. Node M has no information to connect node A to node E and create a fake route packet and assist that it has a shorter route to node E. The generated packet contains (E,A,120, 2>). When A receive this packet it store into its routing table. So, in future A wants to send data to node E then it will follow the routing table that contains the false information [8]. In the research work, we are using the Ad hoc on demand distance vector (AODV) routing protocol. The safety of this protocol is effected by the a number of attacks such as warm hole attack, gray

hole attack, Sybil attack etc. In the proposed work, we are considering the effect of black hole attack. As we know that AODV has not any security mechanism, thus a number of attacks may affect nodes. So in this paper,
we are proving a security mechanism to the AODV routing protocol by eliminating the threat of Black Hole attack.

III. CUCKOO SEARCH (CS) ALGORITHM

The cuckoo search algorithm is based on the idea that how cuckoos lay their eggs in the host nests, if the eggs are not distorted then the eggs are hatched to chicks by the hosts. If the host bird find that the eggs in the host are not their own, they will throw them out or either leave the nest and create a new one. The algorithm can be used MANET that contains a number of nodes. In the proposed work, Cuckoo search is used to optimize the properties of each node according to their objective function [9, 10].
For defining CS algorithm, below three set of rules are considered that are defined below:
Every cuckoo lays one egg at a time, and dumps it in an arbitrarily chosen nest
The best nests with high-quality eggs will be carried over to the next generations.
The number of available host nests is fixed and the egg laid by a cuckoo may be discovered by the host bird with a probability pa ∈ (0, 1). In this case, the host bird can either get rid of the egg, or simply abandon the nest and build a completely new nest.
Cuckoo search algorithm is used in this research work, to discover a safe route by avoiding cooperative black hole attack. Cuckoo search algorithm is initiated in case when the performance of the network is degraded. In the research work, cuckoo search is used to optimize the properties of all nodes which involves in the routing process. On the basis of objective function, we design a optimize property list of all node along with their properties of real and attacker nodes. Thus in order to discover route from source to destination, if there is any attacker present in the route then the performance like energy consumption, execution time, packet delivery time increased and also the performance of the network decreased. For example, if the black hole attack occurs in the path.

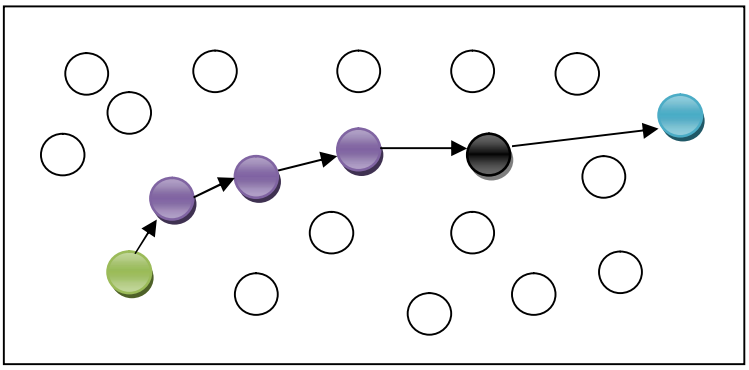


Fig.3: Network area

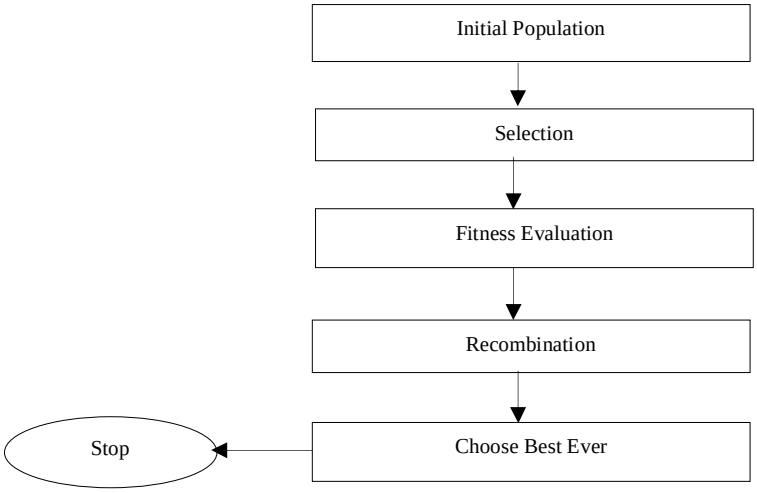


Fig.4 Cuckoo Search Flowchart

In figure 3, green circle represents' the source node, blue circle represents the destination node, violt circle represents the intermediate node and black circle represents the node suffered from black hole attack. As we discussed above that CS is used to optimize the features of each node and stored into the routing table. Thus if black hole attack come into the network, then to differentiate between black hole node and actual nodes, we are using ANN.

A. Artificial Neural Network

Artificial neural network is a computational model that is inspired by the biological neurons. Neuron in brain has been organized in such a manner that they perform some computation task. It has the capability to learn fastly such that of brain. This function is used to produce relevant output from weighted sum of inputs. 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 adjust according to with weight [11].
Training of ANN is dependent on certain learning processes. Using learning method, a network to yield a particular response to a specific input has been considered. It becomes necessary when the information about input is unknown or incomplete.

B. Supervised Learning

In this system, we have assumed that at each instant of time when the input is applied, the desired response of system is obtained. It tries to predict the outcomes for known examples. Such a system compares its predications with the known results and learns from its mistakes.

C. Unsupervised Learning

In this mode, desired response is not known, thus, explicitly error information cannot be used to improve network behavior. Since no information is available for correctness or incorrectness of responses, learning somehow is accomplished based on observations of response to inputs.

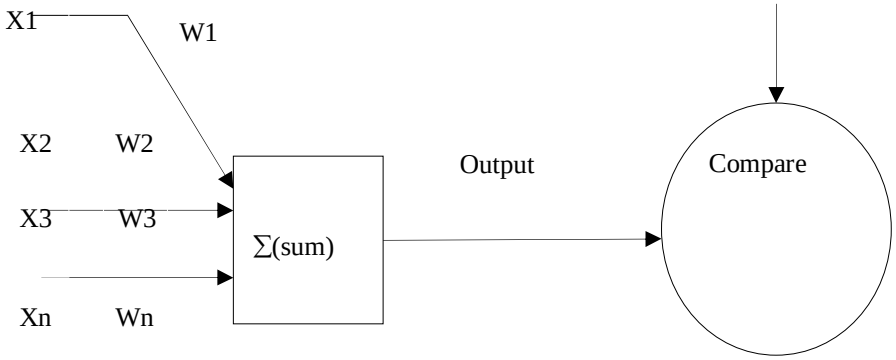


Fig.5 Artificial neural network

In this research paper, ANN is used to classify between the real and attacker nodes. By using ANN we are generating two classes. In class I the properties of real nodes are stored whereas in Class II the properties of attacker nodes are stores. As shown in figure 3. The nodes represented by green, violet, and blue color are having same properties thus comes in class I and the black node is having different property thus ANN stored the properties of this node into class-II. In this way ANN classify that black node is an attacker and pass the data to the neighboring node instead of black node. Hence the performance of the network is increased.

IV. RELATED WORK

Al-Shurman et al. [12, 2004] proposed a technique to solve the problem of attacks occur in Mobile Ad Hoc networks. In first solution, more than one route has been discovered and in second case packet sequence number is added to packet header. AODV routing protocol has been used and concluded that second solution perform having accuracy up to 98 %. Tamilselvan et al. [13, 2008] discussed routing security problems that are being occurred due to black hole attack. The black hole attack has been deployed by using a fidelity tables. In this method, fidelity levels have been assigned to each and every node that takes part in communication. Packet drop has been reduced and the whole process is carried out in Global Mobile Simulator (GloMoSim). Kansal, Puneet et al. [14, 2013] described a black hole attack in MANET along with a routing protocol. The authors has discussed that in a network, more than one black hole can occur that degrade the performance of the network by dropping the packet. Ramaswamy e al. [15,

2003] identified multiple black hole attack occurred in the network and discovered a secure route from source to destination. S. Lu et al. [16, 2005] proposed and implemented AODV routing protocol in the network in which black hole attack has been occurred. The protocol is named as Secure Ad on demand vector (SAODV) routing protocol that is able to handle black hole attack in the network. Augustine et al. [17, 2015] used artificial neural network for securing the network from Black Hole Attack along with AODV routing protocol. Kaur et al. [18, 2014] designed a mobile ad hoc network (MANET) and identify black hole attack using artificial neural network (ANN). The network has been simulated for varying nodes ranges from 20-250 with an area of 1000*1000m.

V. METHODOLOGY

A. The Steps That Are Performed During The Research Work Are Described Below

1) Create a simulation environment for MANET using height and width of 1000m
2) Initialize N number of nodes within the network.
3) Defined the coverage area of each node
4) Defined a Source and a destination node
5) Route is discovered by using AODV routing protocol to find the route between source and destination node.
6) Check the performance of network. If the performance of the network is degraded then initialize Cuckoo search algorithm using their objective function otherwise evaluate parameters.
7) Optimize the properties of the nodes according to the objective function.
8) If the properties of the nodes are satisfactory then train them using ANN otherwise reject that property
9) Classify the attacker present in the route.
10) If node is real then create a new route and evaluate the performance parameters like throughput, delay, BER, and Energy consumption. Otherwise, consider as attacker and remove from the route.

VI. SIMULATED RESULTS

The simulation has been carried out in MATLAB 2010 environment and the performance of the network has been examined with and without optimization and classification techniques.

A. Simulation profile

The simulation profile is listed in table below

Table 1 Simulation profile

PROPERTY	VALUE
Number of nodes	50
Simulation Time	20 Sec
Mobility	Varies between 20-40 Sec
Coverage area	1000m×1000m

The performance parameters that have been measured are described below:1000m×1000m

B. Throughput

Throughput means how many data packets is transmitted form source node to destination node in the total simulation time. In the figure below black line indicates the throughput value obtained when no optimization algorithm has been applied whereas blue line indicates the throughput values with optimization algorithm. Maximum throughput value without optimization and with optimization are 99019.7009, 154840.637 respectively. So it is concluded that when cuckoo search and NN are applied to the network throughput increased.

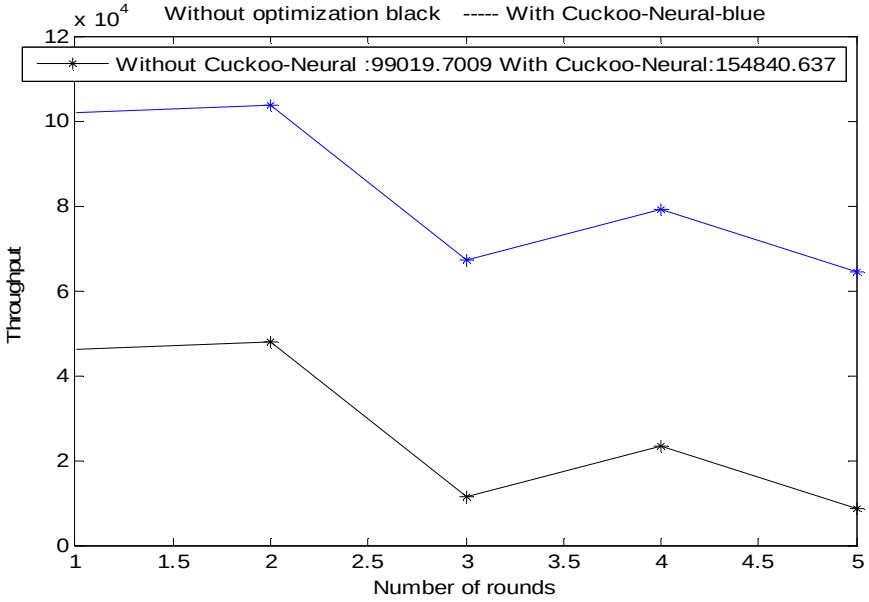


Fig.4 Throughput

C. Delay

Delay is the average time a network takes to send data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

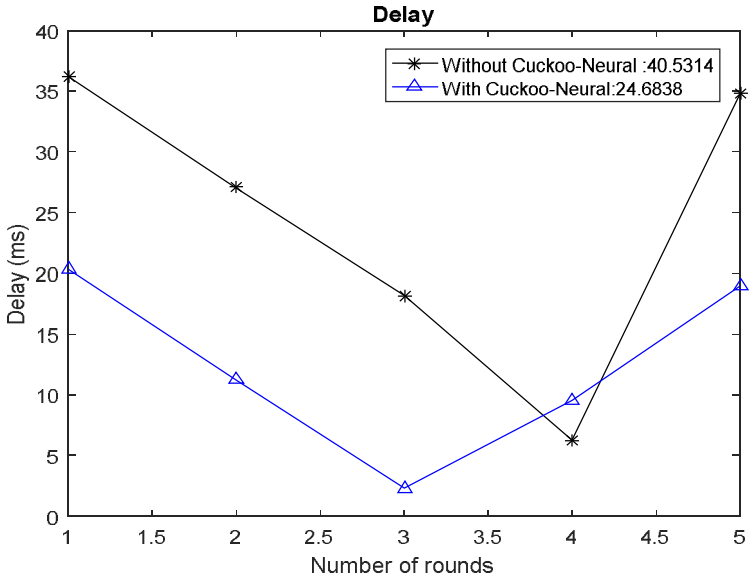


Fig.6 Delay

From the above figure, it is concluded that maximum value of delay without any optimization technique is 40.5314 m sec that is obtained at 4th iteration. When optimization algorithm is applied delay value decreased and value obtained is 24.6838 at the 3rd iteration.

D. Bit Error Rate (BER)

It is defined as the total numbers of bit errors occur in transmitting data bits from any source node to any destination node within the network. It is observed that without optimization and with optimization maximum value of BER 20.9729 and 15.1324.

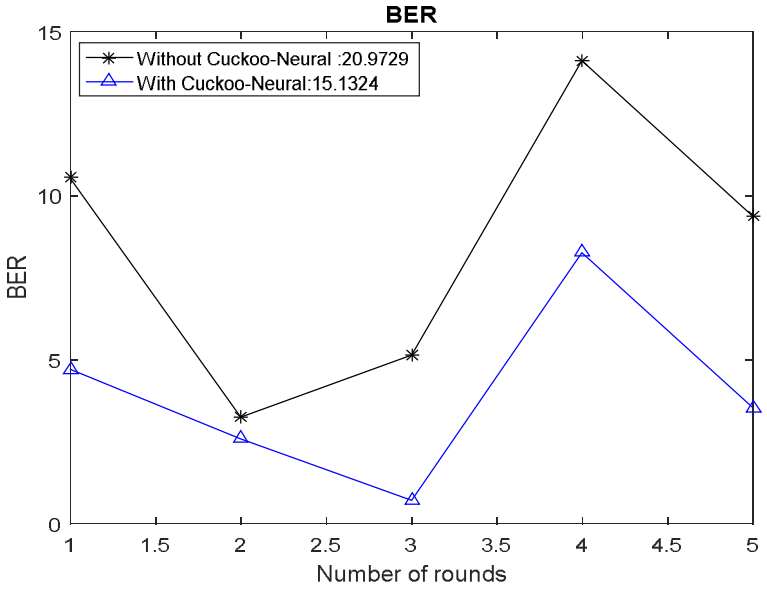


Fig. 7 BER

E. Energy Consumption

When data packet is transmitted form source node to destination node, it goes through different intermediate nodes and each node consumes some energy. Thus, it become essential to discover a route that consume less energy.

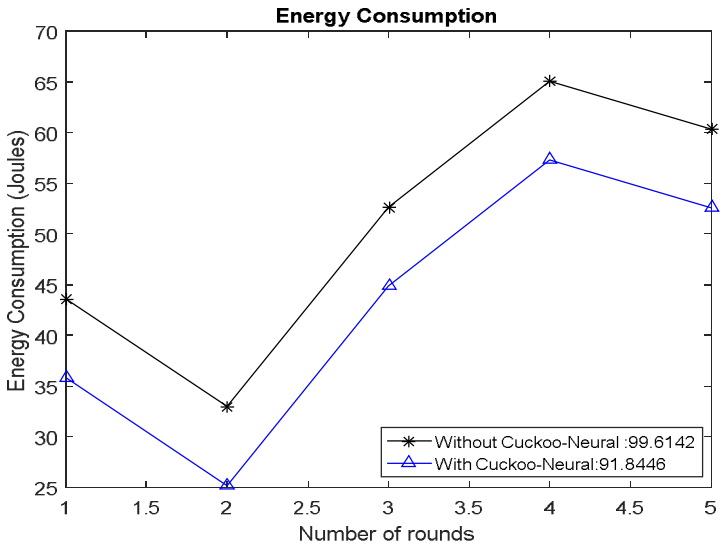


Fig.8 Energy consumption

The energy consumed measured with and without optimization is listed in figure below. From the figure, it is clear that without optimization more power is consumed which is maximum at 4^{th} iteration and the value is 99.6142 whereas with optimization algorithms energy consumption decreased and become 91.8446.

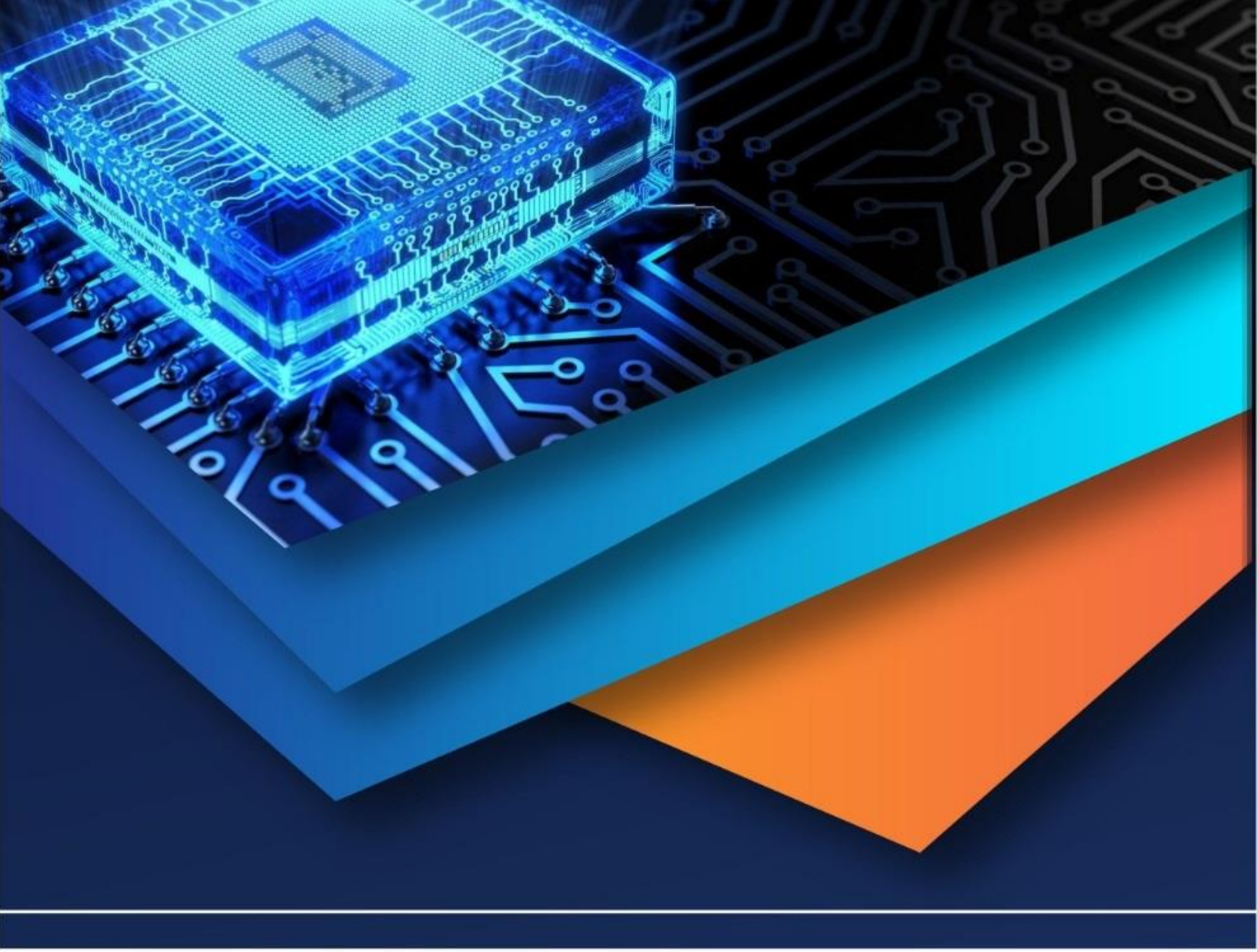
VII. CONCLUSION

In this research work, Black hole attack has been identified and removed from the route within the Mobile Ad Hoc Network (MANET). The route between source and destination has been discovered by using AODV routing protocol. If the black hole attack occurs in the network then the performance of the network like through put, delay, BER, Energy Consumption have been degraded. To improve the performance and reduce the packet drop discovered route has been optimized by using optimization algorithm

named as Cuckoo search. This algorithm finds the nodes having the same properties and thus trains the network using ANN. If a Black Hole attack occurs in the network then the route has been removed from the network and parameters are calculated. By using these techniques a secure and efficient network has been designed. The comparison graph with and without optimization algorithms has also been discussed and it is find that with optimization network performed better than that of without performance.In future, this network can be used to detect and prevent other attacks like gray hole attack, warm hole attack. The performance of the network can be increased by using other optimization techniques like Genetic algorithm (GA), Artificial Bee Colony (ABC) algorithms. For classification Fuzzy logic, SVM can be applied.

REFERENCES

[1] K. Madhuri, N. K. Viswanath and P. U. Gayatri, "Performance evaluation of AODV under Black hole attack in MANET using *NS2*," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-3.
[2] P. S. Hiremath, Anuradha T and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," 2016 International Conference on Information Science (ICIS), Kochi, 2016, pp. 245-251.
[3] Balachandra and N. P. Shetty, "Interception of black-hole attacks in mobile AD-HOC networks," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-5.
[4] K. A. A. Kumar, "Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA," 2016 International Conference on Communication Systems and Networks (ComNet), Thiruvananthapuram, 2016, pp. 93-98.
[5] L. Mejaele and E. Oketch Ochola, "Effect of varying node mobility in the analysis of black hole attack on MANET reactive routing protocols," 2016 Information Security for South Africa (ISSA), Johannesburg, 2016, pp. 62-68.
[6] N. Sharma and A. S. Bisen, "Detection as well as removal of black hole and gray hole attack in MANET," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 3736-3739.
[7] S. Dhama, S. Sharma and M. Saini, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2993-2996.
[8] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using trust with AODV in MANET," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 470-474.
[9] Yang, Xin-She, and Suash Deb. "Cuckoo search: recent advances and applications." Neural Computing and Applications vol.24, 2014, pp. 169-174.
[10] Gandomi, Amir Hossein, Xin-She Yang, and Amir Hossein Alavi. "Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems." Engineering with computers vol.29, 2013, pp. 17-35.
[11] Kaur, Ramanpreet, and Anantdeep Kaur. "Blackhole Detection In Manets Using Artificial Neural Networks." International Journal For Technological Research In Engineering vol.1, 2014, pp. 959-962.
[12] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. ACM, 2004.
[13] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." JNW vol. 3, 2008, pp.13-20.
[14] Kansal, Puneet, Nishant Prabhat, and Amit Rathee. "Black hole attack in Manet." International Journal of Advanced Research in Computer Science and Software Engineering vol.3, 2013.
[15] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., & Nygard, K. E. (2003, June). Prevention of cooperative black hole attack in wireless ad hoc networks. In International conference on wireless networks , vol. 2003, pp. 570-575.
[16] S. Lu, L. Li, K. Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," 2009 International Conference on Computational Intelligence and Security, Beijing, 2009, pp. 421-425.
[17] Augustine, Alfy, and Manju James, "ANN to detect network under Black Hole attack." Journal of Computer Applications , 2015, pp. 15-18.
[18] Kaur, Ramanpreet, and Anantdeep Kaur, "Blackhole Detection In Manets Using Artificial Neural Networks," International Journal For Technological Research In Engineering vol.1, 2014, pp. 959-962



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY