4th International Conference on Science, Technology and Management
India International Centre, New Delhi (ICSTM-16)
15th May 2016, www.conferenceworld.in ISBN: 978-81-932074-8-2

A MECHANISM OF PREVENTING SYBIL ATTACK IN MANET USING BACTERIAL FORAGING OPTIMIZATION

Sonam Mahajan[1], Devesh Kumar Sachin[2], K. Rajput[3]

[1]Student, [2,3] Faculty of ECE Department,
Amity University,U.P., (India)

ABSTRACT

Every author seeks to optimize the QOS in MANET network through routing. Essentially, Qos optimization is used to enhance the life time so that less energy can be consumed, additional packets should be distributed with less Bit Error Ratio and less routing overhead. In this research, the performance analysis of DSR routing protocol is evaluated. Firstly the optimization technique i.e. Bacterial Foraging optimization is applied individually on DSR routing protocol and then compare the performance analysis of DSR routing protocol through BFO approach and without BFO approach that performs better to increase the lifetime of the MANET network so that packets will be transferred in an efficient manner and with less error rate so that the chance of node failure will be less and prolong the lifetime of the network for the realization of routing optimization.

Keywords: MANET, Security, Routing, BFO, BER, Throughput.

I. INTRODUCTION

Security is one of the most common issues in the wireless sensor network and black hole attack is one of those security attacks that mainly occur in mobile ad-hoc networks (MANETs). In Ad-hoc Networks (MANET) each node works like a router [1]. In this network each node acts as neighbor nod to find the path for transmission of data. Various characteristics like dynamic topology, lack of defense features, open medium etc. made MANET more vulnerable. In MANET routing mostly gets affected by Sybil attack in which fake route reply gets occurred for transmission of data. It is the type of attack in which it is assumed that relay packets has been supposed but actual it gets discarded. Because wireless networks architecture is different than typical wired network architecture and any host, either original or fake, can broadcast that it can provide the shortest path for reaching the destination. So, there is lot of chance of injection for the malicious or fake route which contains malicious nodes. Then there, is requirement of optimization through which we can secure the network from Sybil attack [2] [3].

Routing Protocol is second hand to find suitable routes between communicate nodes. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link. As the nodes are changing timely, so the topology of the network gets changed [4]. MANETS basically consists of three routing protocols i. reactive, proactive and hybrid protocol.

1.1 Dynamic Source Routing (DSR)

DSR stands for Dynamic Source Routing that is basically designed for WSN, Adhoc networks. The DSR contains two terms [2] [4] [5].

1.1.2 Route Discovery Process When source A wants to deliver data packet to destination D, then destination address can be obtained from header. Header also consists of the source node that contains the each routing node id [6] [7] [8] [9] [10] [11].

Node A sends route request then in response the receiving node replies the route reply so that to confirm that communication can takes place between them. Send buffer contains the copy of each packet that cannot get transmitted to the destination [12] [13] [14].

1.1.3 Route Maintenance Process: When data packet moves from source to destination, then it is responsibility of each node to take care that right packet has been moved from source to destination [15]. Example in figure 1.3 Node A passes packet from Node B, Node C, and Node D to Node E, the destination.

1.2 Bacterial Foraging Optimization

BFO algorithm is first projected by Passino in 2002 [2] [4]. It is motivated by the foraging and Chemo tactic behaviors of bacteria, especially the Escherichia coli (E. coli). Locomotion can be achieved during the process of real bacteria forging through

the tensile flagella set. In this algorithm, we evaluate total bacteria present on that specific by multiplying rows with column. Then we check if the first bacteria (1,j) is less than checo matic complexity then training features is obtained. If this does not verify the condition such that bacteria value is greater than checo matic complexity then training features is obtained by deducting first bacteria from one and further divided by 16 to obtain trained features and in this further increment is applied so that we can get trained features for every bacteria as well as to increase bacteria sequence up to total bacteria i.e. change count is equal to previous change count and add 1 increment. Then they reproduce using training features [21]. In reproduction process, the least healthy bacteria eventually eliminated or die while each of the healthier bacteria asexually split into two bacteria, which are then

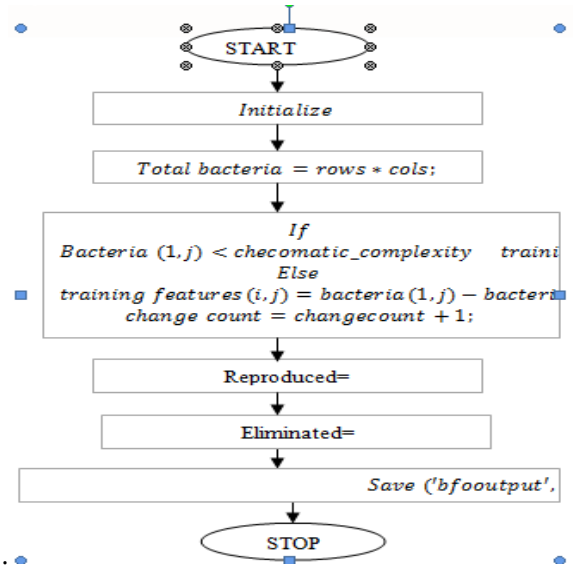

Fig. 1.BFO Flowchart

placed in the same location

Then after this we move towards elimination step, in which eliminated bacteria count is evaluated by deducting total reproduced

bacteria from total bacteria. Afterwards this step, we will save all the parameters value such that BFO output, total bacteria, reproduced, eliminated and change count. And the process will stop on completion process [22, 23].

II. RELATED WORK

Wang Yunwu,(2009), proposed fuzzy based genetic algorithm for the detection of attack in network [16]. Wei Li, (2010), has presented the genetic algorithm for the detection of attack in network and it is then tested with TCP/IP networks [17].Anup Goyal and Chetan Kumar, (2010), presented the optimization algorithm that is called genetic algorithm to enhance the security of the network. The experiment was applied on KDD cup 99 to produce rules for the classification of attacks [18].Yuteng Guo, (2010), discussed a method to improve detection accuracy and efficiency, a new Feature Selection method based on Rough Sets and improved Genetic Algorithms is proposed for Network Intrusion Detection. The effectiveness of the algorithm is tested on the classical KDD CUP 99 data sets, using the SVM classifier for performance evaluation. [19]

2.1 Contribution

The main contribution of this proposed work will be to detect the Sybil attack in network and that will help out to secure various network systems.

2.2 Organization of Paper

The paper is organized as Section 1 discussed the brief introduction of security attack, Section 3 discussed the proposed algorithm, and Section 4 showed the results and analysis and in the end conclusion is described.

III. PROPOSED WORK

The network is established and there are two nodes that are one source and one destination and when one node connects with the other the edge set is formed i.e. the total energy of the nodes. The path which is optimized by genetic algorithm depends on the number of iterations. Length of the path is defined for every node. The initialization of Bacteria Foraging Algorithm begins by defining the path. Tumbling of nodes added to the path from source to destination. For every node, the fitness value is defined. The sorting of the fitness value array is done by defining destination (I.D.) of every node.

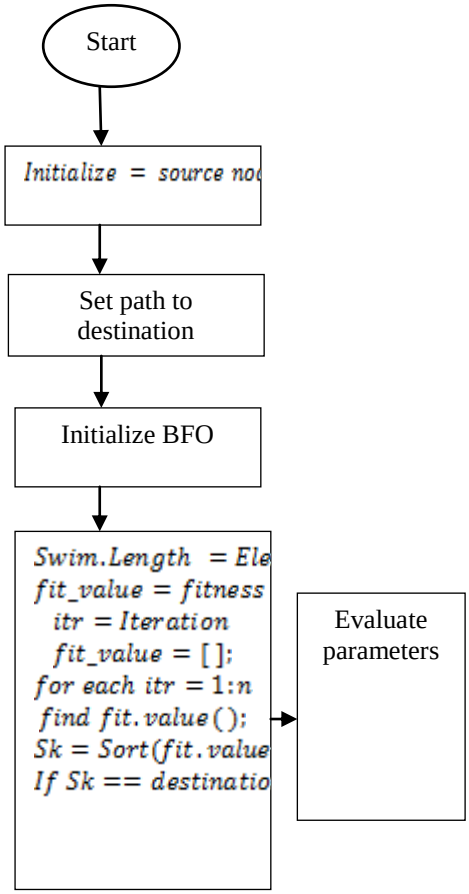

Fig.2. Proposed Flowchart

START

S=Source Node, D=Destination Node.

G (V, E) where V is the vertex or Node set and E is the Edge set between Vi and Vj.

E = Energy set of the nodes.

P = Path of source to destination

for each k in P

Initialize BFO

Swim.Length =Element Count.Path

fit_value=fitness fn BFO(x,S));

itr=Iteration

fit_value=[ ];

for each itr=1:n

find fit.value( );

Sk=Sort(fit.value)

If Sk==destination

End

STOP

IV. SIMULATION RESULTS

The demonstration tries to find out the best performance by using MANET for QOS optimization through routing. So, each part we evaluate the impact of one of the following parameters on the performance of routing protocols:

4.1 Average End-to-End Delay

It is defined as the time takes for the transmission of packets from source to destination. Following formula is for average E2E delay in network.

$$E = \frac{1}{np}\sum_{u=1}^{np}\frac{dn_u}{pckdn_u}$$

4.2 Throughput

It is the total amount of data that has been transferred from source to destination in given interval of time.

$$T = \frac{1}{np}\sum_{u=1}^{np}\frac{td_u}{t_u}$$

4.3 Bit Error rate

The bit error rate (BER) is the numeral of bit errors per unit time. BER is a unit less calculation, frequently taken as percentage.

4.4 Energy Consumption

Energy consumption has become one of the greatest challenges in the field of high performance computing and it is defines as the total energy consumed in running of parallel tasks

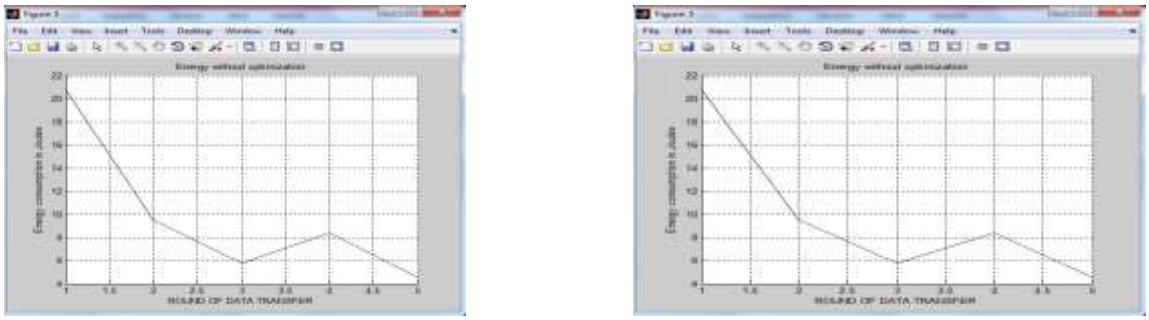

Fig.3. Throughput without Optimization and Energy without Optimization

Throughput is the number of nodes sent over the network in given time without congestion. The above figure.2 shows the throughput value without optimization. It has been seen that value of throughput is being reduced in

the figure. 2. Energy optimization is the energy consumption by the nodes during transmission in network. Its value must be low in the network to have good performance. Above figure.3 shows the high energy consumption.

Fig.4. Error rate without Optimization and End 2 End Delay without Optimization

Error rate is the number of errors present over the network in given time during transmission. The above figure. 4 shows the error rate value without optimization. It has been seen that value of error rate is being enhanced in the figure. Delay is the Minimis able delay in the network during packet transmission. The above figure.5 shows the delay value without optimization. It has been seen that value of overhead is being enhanced in the figure.

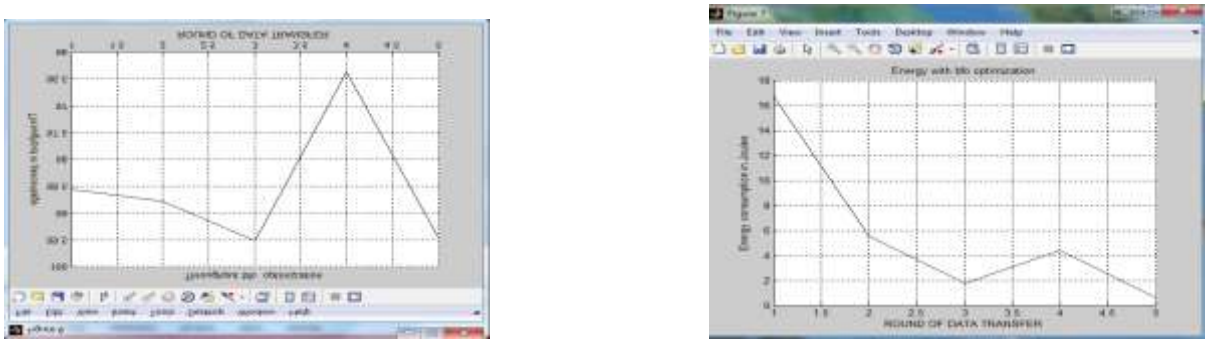

Fig.5. Throughput with Optimization and Energy with Optimization

Throughput is the number of nodes sent over the network in given time without doing congestion. The above figure.6 shows the throughput value after comparison through BFO. It has been seen that value of throughput is being enhanced in the figure to 95.1. Energy optimization is the energy consumption by the nodes during transmission in network. Its value must be low in the network to have good performance. Above figure.7 shows the low energy consumption having values = 2 J.

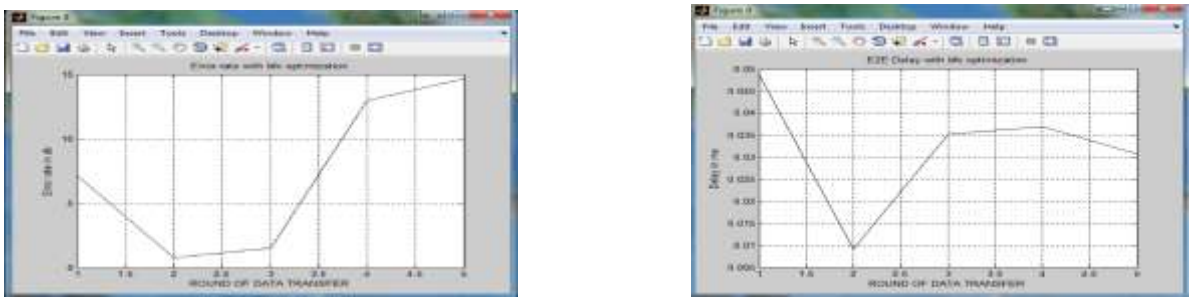

Fig.6. Error rate with Optimization and E2E with Optimization

The bit error rate (BER) is the numeral of bit errors per unit time. The above figure.8 shows the error value after comparison through BFO. It has been seen that value of errors is being reduced here. It is the average time taken by data packet to reach the destination and includes all delays caused by buffering during route discovery latency, queuing at the interface queue. The above figure.9 shows the delay value after comparison through BFO. It has been seen that value of delay is being reduced here.

V. CONCLUSION

MANET are very emerging technology these days and are used in wide applications. The main aim of this proposed work deals with the study of the DSR routing protocol. We find that the DSR with BFO optimization technique performs better than applying just DSR routing protocol so that the packets should reach from source to the destination with less packet drop rates and high data rates to extend the network lifetime. As the energy conservation is one of the main issue in MANET network so for efficient working of the network, energy consumption should be less. High energy consumption is one of the main reasons of the node failure.

REFERENCES

[1] Mariappan Kadarkarainadar Marichelvam, Thirumoorthy Prabaharan, and Xin She Yang, A Discrete Firefly Algorithm for the Multi-Objective Hybrid Flowshop Scheduling Problems, IEEE transactions on evolutionary computation, 2014, vol. 18.

[2] Manoj Jhuria. : Improve Perfomance, DSR Protocol by Application of Mobile Agent, Fourth International Conference on Communication Systems and Network Technologies, IEEE, 2014, pp 336-341.

[3] Mohammed Dyabi, A New MANETS Clustering Algorithm Based On Nodes Performances, Next Generation Networks And Services (Ngns), IEEE, 2014, pp. 22-29.

[4] Istikmal, Analysis And Evaluation Optimization Dynamic Source Routing (DSR) Protocol in Mobile Adhoc Network Based on Ant Algorithm, Information and Communication Technology (ICoICT), IEEE, 2013, pp. 400-404.

[5] K.Amjad, Performance analysis of DSR protocol under the influence of RPGM model in mobile ad-hoc networks, International Conference on Distributed Computing Systems0 Workshops, IEEE, 2013.

[6] K. Naidua, H. Mokhli, A. H. A. Bakar, Application of Firefly Algorithm (FA) based optimization in load frequency control for interconnected reheat thermal power system, iEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT),2013, IEEE.

[7] Mohammad Wazid, Avita Katal, Detection and Prevention Mechanism for Black hole Attack in Wireless Sensor Network, International conference on Communication and Signal Processing, IEEE,2013, pp. 576-581.2013.

[8] Meenakshi Tripathi,M.S.Gaur,V.Laxmi, Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN, The 8th International Symposium on Intelligent Systems Technique, Procedia Computer Science,2013, pp.1101 – 1107.

[9] M. Mohanapriya, Ilango Krishnamurthi., Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers and Electrical Engineering, 2013.

[10] Ting Lu and Jie Zhu, Genetic Algorithm for Energy-Efficient QoS Multicast Routing. IEEE Communications Letters, Vo.17,2013, pp. 31-35.

[11] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad., Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Network, Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN),2012, IEEE, pp.1-5.

[12] K.S.Sujatha, Vydeki Dharmar, R.S.Bhuvaneswaran., Design of Genetic Algorithm based IDS for MANET.IEEE,2012, pp. 28-35.

[13] M. H. Sulaiman, M. W. Mustafa, Z. N. Zakaria, O. Aliman, S. R. Abdul Rahim., Firefly Algorithm Technique for Solving Economic Dispatch Problem, Power Engineering and Optimization Conference (PEDCO) Melaka,2012, IEEE.

[14] Sabrina Merkel, Christian Werner Becker, Hartmut Schmeck, Firefly-Inspired Synchronization for Energy-Efficient Distance Estimation in Mobile Ad-hoc Networks, IEEE,2012, pp.205-212.

[15] Wang. Yu, Using Fuzzy Expert System based on Genetic Algorithm for Intrusion Detection System, IEEE, 2009, pp. 201-224.

[16] Wei Li, Using Genetic Algorithm for Network Intrusion Detection, IEEE, 2010, pp.1-8.

[17] Crosbie, Mark, and Gene Spafford., Applying Genetic Programming to Intrusion Detection., In Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8.,1995, Cambridge, Massachusetts.

[18] Yuteng Guo, Beizeng Wang, Xingxing Zhao, Xiaobiao Xie, Lida lin and Qinda Zhou., Feature Selection based on Rough Set and modified Genetic programming for Intrusion Detection, In 33 ICRTIT-2012 proceedings of 5th International Conference of Computer Science and Education, IEEE, 2012.

[19] Kwashie A. Anang, Lawal Bello, Titus. I. Eneh, Panos Bakalis and Predrag B. Rpajic , The Performance of Dynamic Source Routing Protocol to Path Loss Models At Carrier Frequencies Above 2 GHz. Communication Technology (ICCT), IEEE, 2011, pp151-155.

[20] Pengfei Guo Xuezhi Wang, The Enhanced Genetic Algorithms for the Optimization Design, IEEE, 2010.

[21] Yong-Feng Dong, Jun-Hua Gu. , Combination of Genetic Algorithm and Ant Colony Algorithm For Distribution Network Planning, IEEE, 2010.

[22] Chang Wook, R. S. Ramakrishna.,A Genetic Algorithm for Shortest Path Routing Problem and the Sizing of Populations, IEEE,2002.