International Journal of
ADVANCED COMPUTRONICS
AND MANAGEMENT STUDIES

Prevention of Gray Hole Attack in MANET using Fuzzy Logic

Niharika Gupta[1], Pradeep Singh[2]

[1]M.Tech (Scholar, CSE), [2]M.Tech (Assistant Professor, CSE)

[1]SR Group of Institutions, Jhansi, India, [2] SR Group of Institutions, Jhansi, India

[1]er.niharika2009@gmail.com,[2] pradeepusingh@gmail.com

Abstract- In recent years, MANET (Mobile ad-hoc network) has turn out into an interesting research area among a variety of researchers because of their flexibility as well as independence of network infrastructures, like base stations. In the presence of malicious nodes, the network becomes penetrable to different kind of attacks. In MANET, routing-attacks are relatively serious. It has number of potential-applications that are in completely un-predictable in dynamic environment. Routing protocol utilized here are in a form of reactive-routing protocol known as OLSR. This routing protocol route is based on demand. In specification based IDS, specific characteristics of vital-objects are being investigated with the detection of any abnormality. The proposed work has designed and implemented MANET in OLSR routing protocol. The gray hole attack is mitigated using Fuzzy Logic based on rule sets to have better routing process and ABC (Artificial Bee Colony) algorithm at superior rate for optimizing the route set at novel objective function. The results would be evaluated using Parameters, namely, Throughput, BIT (Bit Error Rate), Energy consumption and PDR (Packet Delivery Ratio).

Keywords: MANET, OLSR, Fuzzy Logic, Gray hole attack, ABC

1. Introduction

A network is a group of two or more computer systems which are linked together to communicate with one another. It is a telecommunication network that allows computers to exchange data. The connections between nodes are established using either cable media or wireless media [1]. Computer networks differ on the basis of physical media used to transmit their signals, the communication protocols used to organize network traffic, the size of the network, topology used in the network [2]. MANET is a mobile ad-hoc network. It is self-configuring network which is infrastructure-less in nature. In MANET, different mobile nodes are connected through wireless links. Each node is free to move i.e. no central controller available. The infrastructure less network does not need any infrastructure to complete its job. In such network, every single node could possibly interconnect straight forwardly through several other hubs/nodes [5]. So, in such kind of network, not a single access point is obligatory which used for directing medium access.

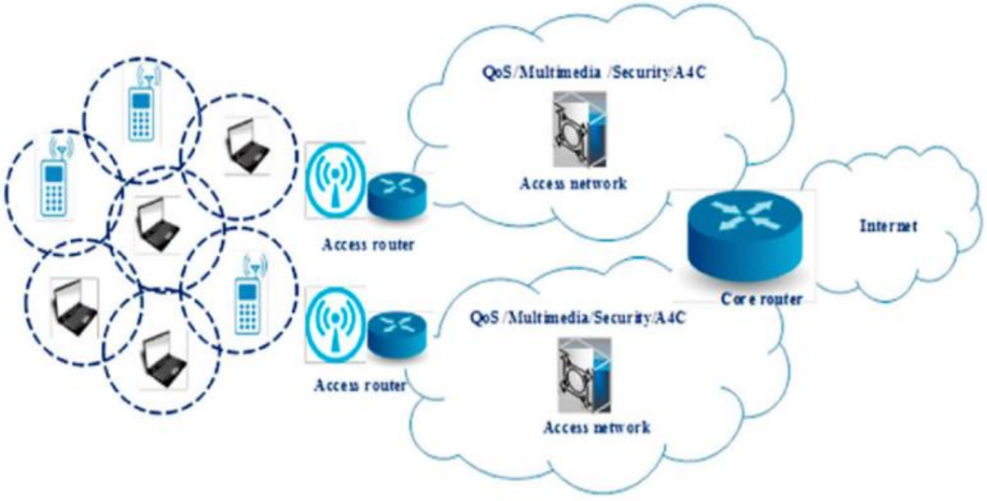

Figure 1: Basic architecture of MANET

Mobile Ad hoc network is one of most advanced network system for any type of routing or communication. It is not only fast but quite accurate also. Increasing demands of the recent trends have increased level of theft as well. Hacking of Ad hoc network path discovery process or affecting the search algorithm can be seen often in this contrast. Attacks like DDOS, Sybil attack were assumed to be very dangerous for Ad hoc networks but these days more risky security threats have come up in a surprising manner. This research work discuss major and one of the most advanced security threats in the Ad hoc routing and enhancement namely GRAY HOLE ATTACK that was primarily given by Chris Karlof and David Wagner in 1990s. In this attack, the nasty or malicious node acts as normal node and even drops the packets or message that are passed through them, therefore, the concept of hiding the important data to transfer to the next node or destiny node. This research work also aims to mitigate the effects of this attack by designing a unique fitness function which is applied over fuzzy logic provides the human reasoning capabilities. Fuzzy logic starts with and builds on a set of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. This simplifies the job of the system designer and the computer, and results in much more accurate representations of the way systems behave in the real world and

ABC method which is one of the most recently defined algorithms by Dervis Karabogain 2005, motivated by the intelligent behaviour of honey bees. ABC as an optimization tool provides a population-based search procedure in which individuals called foods positions are modified by the artificial bees with time and the bee's aim is to discover the places of food sources with high nectar amount and finally the one with the highest nectar.

2. Related Work

Yong-Feng Dong, Jun-Hua Gu (2007) anticipated a combinational algorithm that derive since the qualities of Genetic Algorithm and Ant Colony Algorithm toward solving sharing system preparation difficulty. The simulation shows that the novel algorithm is efficient in solving division system preparation difficulty. Kwashie A. Anang et al (2011) proposed the implementation result of Dynamic Source Routing- DSR protocol in wireless channel. From the implementation results, it has been concluded that there are some propagation parameters like end to end delay, SNR, power ratio that also affects the performance of the DSR protocol. .B Chikha et al (2011) assessed routing protocol in MANET e.g. AODV and dynamic source routing protocol (DSR's) exhibitions for IEEE 8o2.15.4/ZigBee. The assessment is in terms of packet loss, packet delivery ratio, system throughput, and end delay and energy consumption. The authors have examined different reproduction situations, changing system and activity densities and utilized the system test system Ns2. Ashok M.Kanthe et al (2012) presented the performance examination of the Dynamic Source Routing- DSR and Ad hoc on-demand routing protocol- AODV protocol in terms of end to end delay, packet ratio and throughput. From the simulation results, it has found that AODV performs better than DSR in terms of packet drop ratio and end to end delay in comparison to DSR and the whole simulation is done in Network Simulator (NS)-2 environments. Bharat Bhushan and Sarath S. Pillai (2012) listed out a comparative study of Particle Swarm Optimization (PSO) and Firefly Algorithm (FFA) with simulation results approved on a number of normal benchmark function. By means of evolutionary methods and performance of biotic mechanism of nature, a lot of optimization algorithms were made. Istikmal (2013) utilized the routing algorithm in MANET and the improvement is done on the DSR (Dynamic Source Routing) which is routing protocol utilizing ACO algorithm. At that point, the author has investigated and assessed the execution of this routing algorithm in different situation and contrasted the outcome and standard DSR routing protocol. Ting Lu et al (2013) presented the energy efficient GA algorithm to determine the nature of quality of service (QoS) issue, which is NP-complete. The proposed GA optimization algorithm relies upon limited end-to-end delay and less energy consumption of the multicast tree. Experiment results demonstrate that the proposed algorithm is viable and effective. Ahmed Shariff et al (2013), showed Mobile Ad-Hoc Networks (MANETs) bein characterized by the lack of infrastructure, dynamic topology, and their use of the open wireless medium. Black-hole attack represents a major threat for such type of networks. The author has presented an extensive survey of the known black-hole detection with the prevention approaches with the presentation of new dimensions for their classification. Mariappan Kadarkarainadar Marichelvam et al (2014) proposed firefly algorithm to take care of half flowshop planning issues with two targets. Makespan and mean flow time as the target functions are considered. Computational experiments have been done to assess the execution of the proposed method. The results have demonstrated the proposed calculation beats numerous different meta-heuristics in the literature.

3. Simulation Model

Gray hole attack is one of the most common attacks made against the reactive routing protocol in MANETs. It involves malicious node(s) fabricating the sequence number, hence, pretending to have the shortest and freshest route to the destination. Numerous studies have attempted to devise effective detection methods for this attack. The aim of this research is to investigate gray hole detection methods within the scope of OLSR reactive routing protocol. In proposed work, we have focused on OLSR routing protocol with ABC to identify gray hole attack in MANET using fuzzy logic based on rule sets and then classification of active nodes is done. The fuzzy rule sets overcome the problem which was not solved by existing techniques. The fuzzy logic technique is very easy to implement and produce precise output by removing various ambiguities and ABC has optimised the results. In the end, the parameter evaluation is done using Throughput, Bit Error Rate, Energy Consumption and Packet delivery ratio.

Below are the steps taken for the implementation of the work:

Step: 1 Start

Step: 2 Deploy MANET with width and height.

Step: 3 Initialise the nodes within network.

Step: 4 Find source to destination from the nodes.

Step: 5 Define the coverage set of each node including source and destination.

Step: 6 Discover route from source node to destination node using LSR routing protocol.

Step: 7 Set the fuzzy rule set in the MANET.

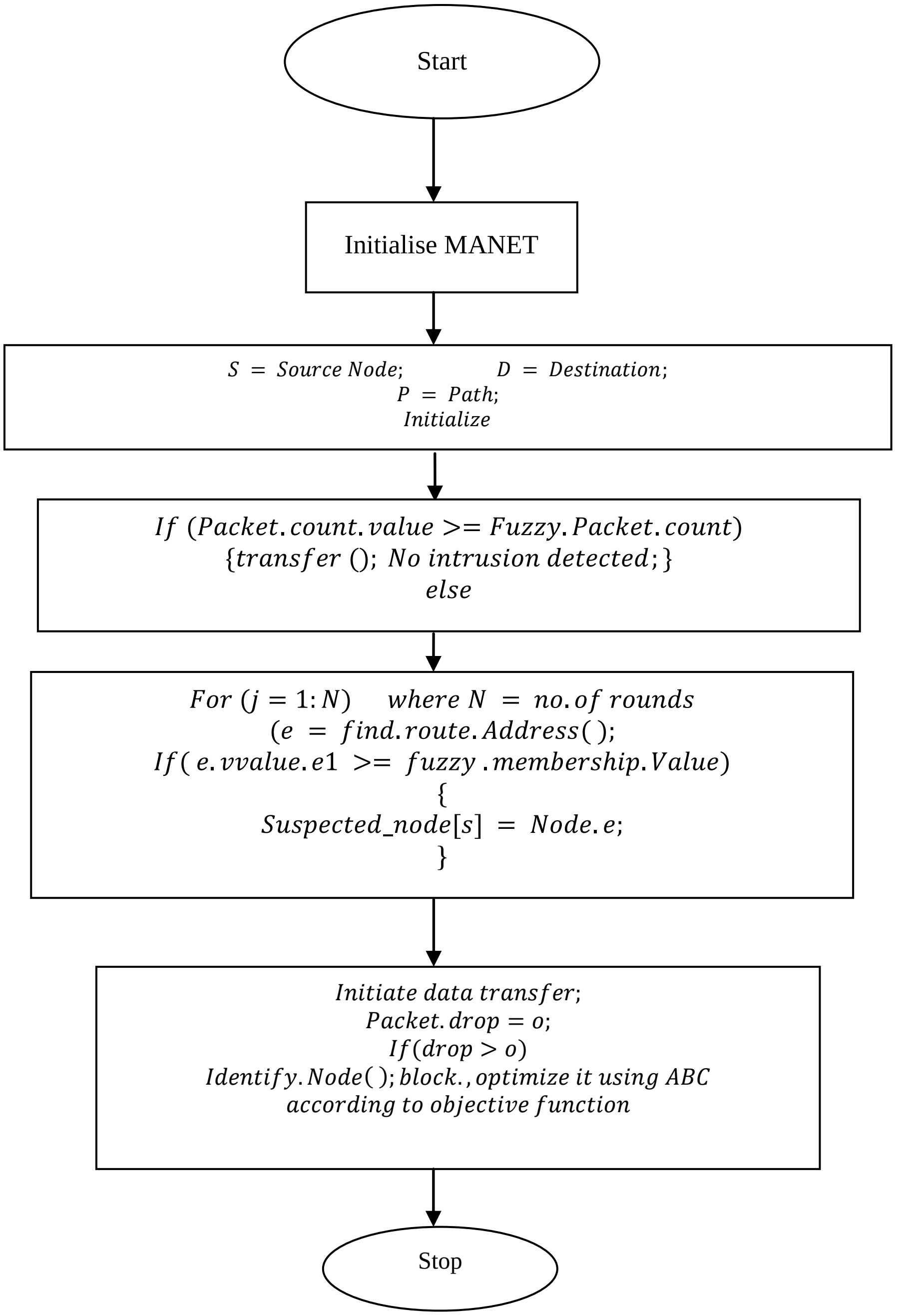
Start
Initialise MANET
$S = Source\ Node;$ $D = Destination;$
$P = Path;$
$Initialize$
$If\ (Packet.count.value >= Fuzzy.Packet.count)$
$\{transfer\ ();\ No\ intrusion\ detected;\}$
$else$
$For\ (j = 1{:}N)$ $where\ N = no.of\ rounds$
$(e = find.route.Address(\,);$
$If(\,e.vvalue.e1 >= fuzzy\ .membership.Value)$
$\{$
$Suspected\_node[s] = Node.e;$
$\}$
$Initiate\ data\ transfer;$
$Packet.drop = o;$
$If(drop > o)$
$Identify.Node(\,); block., optimize\ it\ using\ ABC$
$according\ to\ objective\ function$
Stop

Figure 2: Proposed work flowchart

Step: 8 Evaluate parameters i.e. Throughput, Bit Error Rate, Energy Consumption and Packet delivery ratio.

Step: 9 Analyze the parameters and if needed then use optimization.

Step: 10 Find gray hole node using optimization with ABC technique.

Step: 11 If a malicious node is node is detected, then fuzzy logic mechanism is activated by setting the node against malicious node. The fuzzy mechanism changes the path of data packet once the malicious node is detected; this is done by OLSR which modifies the path in order to provide secure data communication. In the end, ABC will classify between the gray hole nodes.

Step: 12 Again, evaluate parameters i.e. Throughput, Bit Error Rate, Energy Consumption and Packet delivery ratio

Step: 13 End

4. Simulation Results

The whole simulation is being done in MATLAB using various parameters as defined below:

i. Throughput

Throughput is defined as the total number of packets transmitted n the whole simulation time. Mathematically, it is defined as:

$$\text{Throughput} = \frac{\sum Packtssent}{Totaldatapackets}$$

ii. Bit Error rate

Bit Error rate (BER) is defined as the number of bits per unit time. It is the division of bit errors by the total number of transferred bits during time interval. It is often defined in the form of percentage and it is a measure of unit less performance.

iii. Energy Consumption

Energy consumption is the defined as the total amount of energy being consumed by each node in MANET at different network layers. It is obtained by energy consumed summation in every operation mode during simulation time. It is defined mathematically as below:

$$Energy\ Consumption = \sum_{i=0}^{n-1} (Energy\_consumed\_by\_node(i))$$

iv. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the ratio among the number of packets transferred by a traffic source and the number of packets being received by a traffic sink. It calculated the loss rate as seen by transport protocols and as such, it characterized correctness as well as efficiency. PDR is defined as the ratio of the data packets anticipated by the destination for those produced vua different sources. Mathematically, it is defined as:

$$PDR = S1 \div S2$$

Where, $S1$ is the sum of data packages being received by the every specific destination and $S2$ is the sum of data packages that are produced by each single source.

Table 1: Parameter values with and without Optimization

Parameters	Without Optimization	With Optimization
Throughput	72.4	96.6
Packet Delivery Ratio	91.7	94.3
-Bit Error Rate	16.8	7.3
Energy Consumption	54.4	28.4

Above table is describing the values of parameters, namely, Throughput, Packet Delivery ratio, Bit error rate and energy consumption. These values are obtained as per the rounds taken. The values for various parameters have been taken for with and without optimization.

Table 2: Throughput with and without Optimization

THROUGHPUT		
Number of rounds	Without Optimization	With Optimization
1	72.4	96.6
2	71.9	98.4
3	68.47	94.5
4	74.6	96.2
5	73.5	97.3

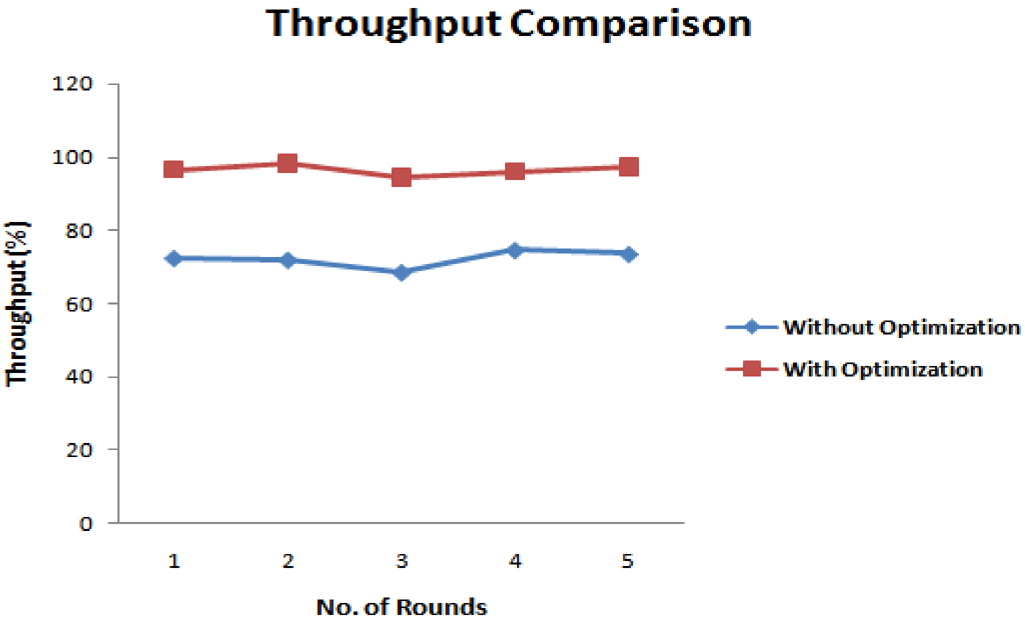

Figure 3: Throughput Comparison

Above figure describes the graph obtained for throughput with respect to number of rounds. In the graph, five rounds as shown in the X-axis have been taken for execution of proposed work and Y-axis is showing throughput. The average value for throughput is 72.174 in case of without optimization and 96.6 is the average value taken for with optimization. Therefore, it is clear from the result that in case of with optimization, the value of throughout is better.

Table 3: Packet Delivery Ratio with and without Optimization

PACKET DELIVERY RATIO		
Number of rounds	Without Optimization	With Optimization

1	91.7	94.3
2	89.3	92.5
3	90.5	93.4
4	91.5	92.7
5	92.7	94.2

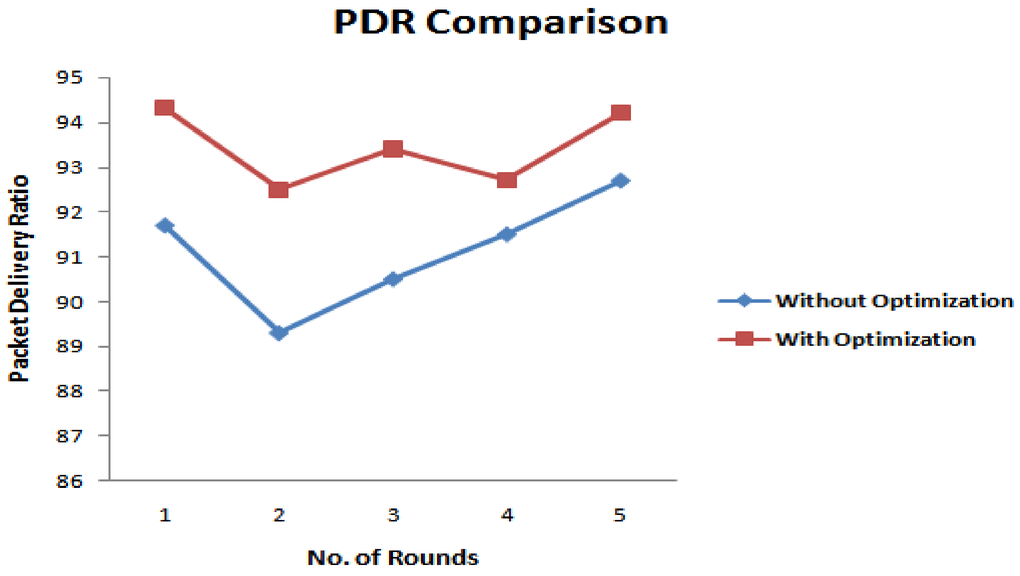

Figure 4: Packet Deliver Ratio Comparison

Above diagram shows the graph of packet delivery ratio for with and without optimization. It is defined as the ratio of data packets expected by the generated through sources. X-axis is defining the number of rounds taken and Y-axis is defining the packet delivery ratio. Red line is defining PDR for with optimization and blue line is defining the results obtained for without optimization. The average value of PDR for without optimization is 93.4 and for with optimization, the average value is 91.14.

Table 4: Bit Error Rate with and without Optimization

BIT ERROR RATE		
Number of rounds	Without Optimization	With Optimization
1	16.8	7.3
2	15.7	6.9
3	14.9	7.1
4	16.2	6.7
5	16.5	7.2

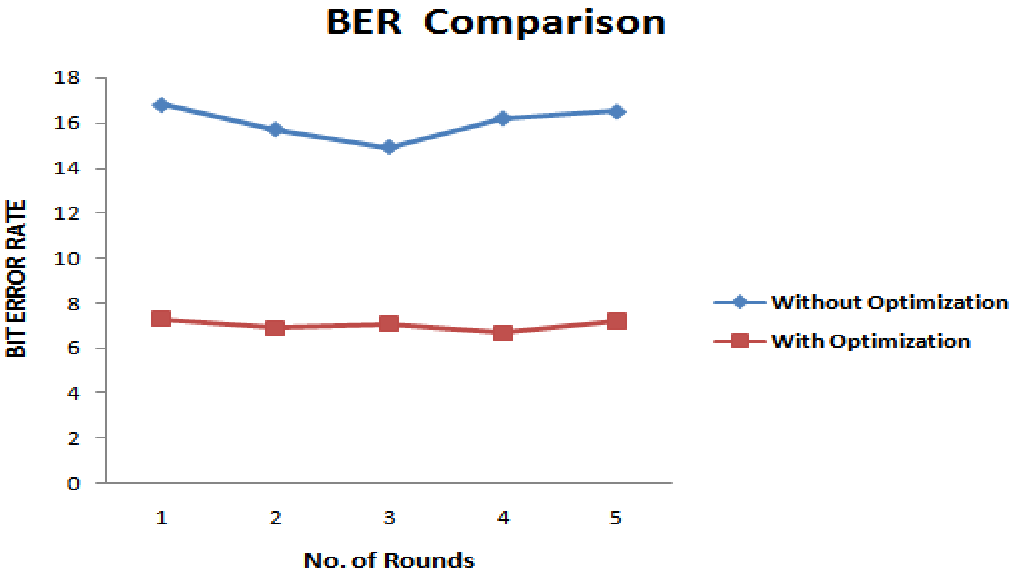

Figure 5: Bit Error Rate Comparison

In the above figure, the graph of Bit Error Rate (BER) is shown for with and without optimization. X-axis is defining the number of rounds taken and Y-axis is defining bit error rate. Blue line is defining the results for without Optimization and red line is for with optimization. The average value of Bit Error Rate for without optimization is 16.02 and for with optimization, the average value is 7.04. It can be seen from the graph that the result value of BER has been improved after applying ABC optimization algorithm.

Table 5: Energy Consumption with and without Optimization

ENERGY CONSUMPTION		
Number of rounds	Without Optimization	With Optimization
1	54.4	28.4
2	52.6	27.5
3	53.5	28.1
4	54.2	26.9
5	53.8	27.9

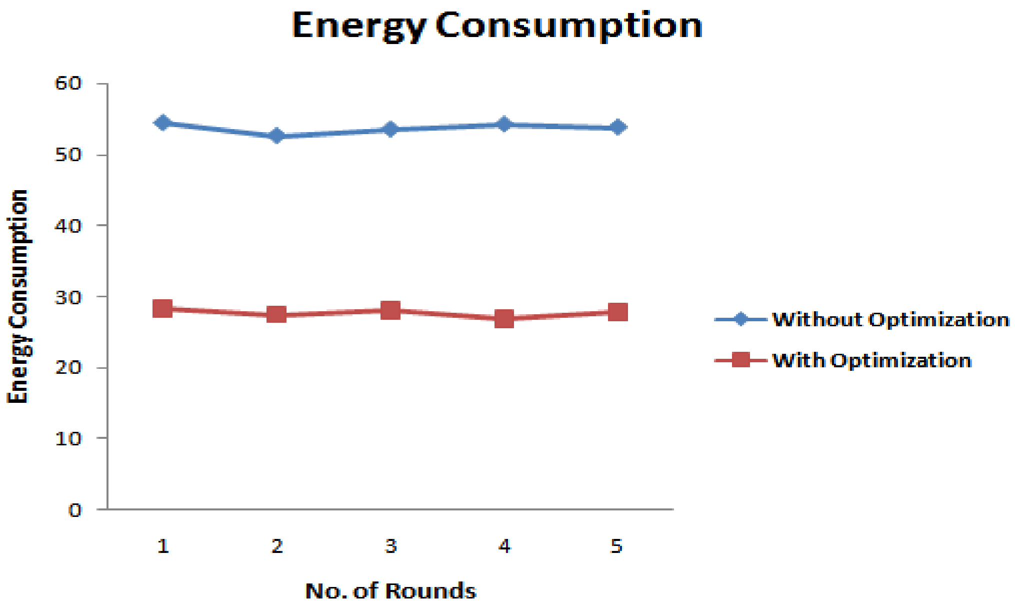

Figure 6: Energy Consumption Comparison

Above graph is for energy consumption for with and without optimization. Consumption of nodes wisely and effectively is considered as one of the important feature. As wireless sensor nodes are prepared with non-chargeable batteries by inadequate energy supply, a sensor network cannot works well after a fraction of nodes run out of energy. In the graph above, it is being concluded that in case of with optimization, the energy consumption is less while in case of without optimization, energy consumption is more. The average for Energy consumption with respect to without optimization is 53.7 and in case of with optimization, the average for energy consumption is 27.6.

5. Conclusion

In this proposed work, we have analyzed the effect of Gray hole attack in the performance of OLSR routing protocol. This routing protocol set route based on demand for analyzing the attacker, and for that Fuzzy Logic is used as a classifier. It works on the basis of rule sets which can help to find whether the attack is present or not. Through fuzzy logic technique, the rules are being set as per OLSR routing protocol. The simulation has been executed using the MATLAB. The simulation results has shown that when the gray hole node exists in the network, the performance of the network is being affected and decreased and can be optimized by using ABC algorithm with fuzzy rule sets. A hypothetical network was constructed for the simulation purpose and then monitored for number of parameters. We simulate our model for various nodes. Initial position for the node is specified in a movement scenario file created for the simulation using a MATLAB. The nodes move randomly among the simulation area. So, the detection and prevention of gray hole attack in the network exists as a challenging task. In proposed work, throughput (more than 96%) and packet delivery ratio (more than 94%) values have been increased when Optimization is being used while bit error rate and energy consumption are decreased in the case of with optimization.

In future work, we can design and implement Mobile Ad-hoc Networks in OLSR protocol with neural network classifier using the hybrid optimization for detection and prevention form different types of attackers. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. When the route is classified using neural network, the attack can be accurately detected so that more appropriate performance can be achieved.

References

[1]. Perkins C. and Royer E, "Ad hoc on-demand distance vector routing", In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100,1999.

[2]. Padmini Misra, "Routing Protocols for Ad Hoc Mobile Wireless Networks", [online], Available: http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing,2000.

[3]. Papadimitratos P. and Haas Z. J, "Secure routing for mobile ad hoc networks", In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (2002)

[4]. Hu Y.-C., Johnson D. B. and Perrig A., "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13 (2002).

[5]. W. Stallings, "Data Communication", in Data and Computer Communication, 7th Ed., Prentice Hall, 2003, ch. 1, pp. 10-14.

[6]. Y.-C. Hu, A. Perrig, and D. B. Johnson. " Packet leashes: A defense against wormhole attacks in wireless networks", IEEE INFoCoM, Mar 2003.

[7]. S. Capkun, L. Butty´an, and J.-P. Hubaux. "SECToR: secure tracking of node encounters in multi-hop wireless networks.",In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 21–32, oct 2003.

[8]. J. Zhen and S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks", In ADHoC-NoW, LNCS 2865, pages 140–150, 2003.

[9]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, "An overview of Mobile Adhoc Networks: Applications and challenges", Sint Pietersnieuwstraat 41, Belgium, 2005.

[10]. R.E.Kassi, A.Chehab, and Z. Dway, "DAWWSEN: A Defence Mechanism against Wormhole Attacks in Wireless Sensor Networks", in proceeding of the second International conference on innovations in information Technology (ITT' 05), UAE, September 2005.

[11]. B. Forouzan, "ICMP", in Data Communication and Networking, Fourth Ed., McGraw-Hill, 2oo6, ch.21, pp. 621-637.

[12]. Tamilselvan L. and Sankaranarayanan D. V, "Prevention of impersonation attack in wireless mobile ad hoc Networks", International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 3, p.118–123 (2007)

[13]. Yong-Feng Dong, Jun-Hua Gu, "Combination Of Genetic Algorithm And Ant Colony Algorithm For Distribution Network Planning,". 4244-0973-x/07/$25.00 ©2007 IEEE.

[14]. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks", In International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201, pp.78-86.

[15]. Pengfei Guo Xuezhi Wang, "The Enhanced Genetic Algorithms for the Optimization Design," 978-1-4244-6498-2/10/$26.00 ©2010 IEEE.

[16]. K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama and K. Thilagam, "Modified AoDV Protocol against Black hole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010.

[17]. S Upadhyay and B.K Chaurasia, "Impact of Wormhole Attacks on MANETs", International Journal of Computer Science & Emerging Technologies, Vol. 2, Issue 1, pp. 77-82 (2010)

[18]. R. Maulik and N. Chaki, "A Comprehensive Review on Wormhole Attacks in MANET", In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010

[19]. CaimuTang, and Dapengoilver, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE, 2011.

[20]. V.K Taksande, "A Simulation Comparison Among AODV, DSDV, DSR Protocol with IEEE 8o2.11 MAC for Grid Topology in MANET", Computational

Intelligence and Communication Networks (CICN), IEEE, 2011.

[21]. Haithem Ben Chikha, Amira Makhlouf and Wiem Ghazel, "Performance Analysis of AODV and DSR Routing Protocols for IEEE 8o2.15.4/ZigBee", IEEE, 2011.

[22]. 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, pp151-155, 2011.

[23]. Perkins.C.E, " Ad hoc Networking, Boston", Addison Wesley (2011)

[24]. Harris Simaremare and Riri Fitri Sari , "Performance Evaluation of AODV variants on DDoS, Blackhole and Malicious Attacks", International Journal of Computer Science and Network Security, VoL-11, June 2011, pp.6.

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

[26]. K.S.Sujatha1, Vydeki Dharmar, R.S.Bhuvaneswaran, "Design of Genetic Algorithm based IDS for MANET", IEEE, pp. 28-35, 2o12.

[27]. 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, IEEE, 2012.

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

[29]. Bharat Bhushan, Sarath S. Pillai, "Particle Swarm Optimization and Firefly Algorithm: Performance Analysis", 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.

[30]. M. H. Sulaiman, M. W. Mustafa, "Firefly Algorithm Technique for Solving Economic Dispatch Problem,"978-1-4673-0662-1/31.0002012IEEE.

[31]. Isaac Woungang et.al, "Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1-4673-1550-0/12/$31.0 ©2012 IEEE.

[32]. Yang, Bo, Ryo Yamamoto, and Yoshiaki Tanaka, "Historical evidence based trust management strategy against black hole attacks in MANET", Advanced Communication Technology (ICACT), 2012 14th International Conference on. IEEE, 2o12.

[33]. Perkins C. and Bhagwat P, "Highly dynamic destination-sequence distance-vector routing (DSDV) for mobile computers", In Proceedings of ACM Conference on Communications Architectures, Protocols and Applications (ACM SIGCoMM

[34]. Kyriaki Gkoutioudi, Helen D. Karatza, "A simulation study of multi-criteria scheduling in grid based on genetic algorithms," 978-0-7695-4701-5/12 $26.00 © 2012 IEEE DOI 10.1109/ISPA.2012.48.

[35]. Chang Wook, R. S. Ramakrishna, "A Genetic Algorithm for Shortest Path Routing Problem and the Sizing of Populations," 1089-778X/02$17.00© 0002 IEEE.0

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

[37]. K.Amjad, "Performance analysis of DSR protocol under the influence of RPGM model in mobile ad-hoc networks", 2011 31st International Conference on Distributed Computing Systems Workshops, IEEE, 2013.

[38]. 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", 2013 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), IEEE, 2013.

[39]. Rooshabh Kothari, Deepak Dembla, "Implementation of Black Hole Security Attack Using Malicious Node for Enhanced-DSA Routing Protocol of MANET", International journal of computer applications (IJCA).Vo.64-No.18, 2013.

[40]. Kaur, Harjeet, Manju Bala, and Varsha Sahni, "Study of Black hole Attack Using 2 Detection Techniques in Mobile

Ad-hoc Network (MANET)", IEEE, pp: 346-352, 2013.

[41]. Mohammad Wazid, Avita Katal, "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", International conference on Communication and Signal Processing, IEEE, pp. 576- 581, 2013.

[42]. 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 Techniq, Procedia Computer Science, pp.1101 – 11o7, 2013.

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

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

[45]. Tan, Seryvuth, and Keecheon Kim, "Secure Route Discovery for preventing black hole attacks on AoDV-based MANETs", ICT Convergence (ICTC), 2o13 International Conference on. IEEE, 2013.

[46]. Rooshabh Kothari, Deepak Dembla, "Implementation of Black Hole Security Attack Using Malicious Node for Enhanced-DSA Routing Protocol of MANET", International journal of computer applications (IJCA).Vo.64-No.18, 2013.

[47]. 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, vol. 18, 2014.

[48]. Manoj Jhuria, "Improve Perfomance DSR Protocol by Application of Mobile Agent", 2o14 Fourth International Conference on Communication Systems and Network Technologies, IEEE, pp 336-341, 2014.

[49]. Mohammed Dyabi, "A new MANETs clustering algorithm based on nodes performances", Next Generation Networks and Services (NGNS),, IEEE, pp. 22-29, 2014.

[50]. G.Vennila, Dr.D.Arivazhagan, N .Manickasankari "Prevention of Co-operative Black Hole Attack in MANET on DSR Protocol Using Cryptographic Algorithm" International Journal of Engineering, Volume 6 No 5 oct-Nov 2014.

[51]. Wahane, Gayatri, and Savita Lonare. "Technique for detection of cooperative black hole attack in MANET." 2o13 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.

[52]. Zhu Xialonget. Al, "A location privacy preserving solution to resist passive and active attacks in VANET", IEEE, Vol.11, pp. 60-67, 2014.