Mody University International Journal of Computing and Engineering Research
Vol. 1 Issue 2, 2017, pp.75-82
ISSN: 2456-9607 (Print) 2456-8333(Online)

The Evaluation and Detection of Sinkhole Attack by Implementing Genetic Algorithm in MANET

Vikas Raina, Sulekha Kumari, Partha Pratim Bhattacharya and V. K. Jain

Department of Electronics and Communication Engineering,
College of Engineering and Technology,
Mody University of Science and Technology, Lakshmangarh, India

vikasraina.cet@modyuniversity.ac.in

Received 15 Sept. 2017, Published 05 Nov. 2017

Abstract: In a mobile ad-hoc network (MANET), there is a temporary network setup by wireless nodes which randomly move and communicate in the absence of proper infrastructure of network. MANETS are prone to various kinds of attacks due to its various features of dynamic changing topology, limited battery life and distributed nature. One of the attacks which affect the network is sinkhole attack. This paper mainly includes the optimization of data packets and data route for sinkhole attack using weight function over the network based on genetic algorithm and compare the results with and without optimization of sinkhole attack in the network.

Keywords: *MANET, Sinkhole Attack, AODV Routing Protocol, Genetic Algorithm, Energy Consumption, Packet Delivery Ratio, Throughput*.**.**

1. INTRODUCTION

MANET is the self- organizing network in which links are attached via wireless medium. As due to wireless communication, the infrastructure is de-centralized, so security issues are very common. Reliability of the system is very important for security criteria. Various routing protocols have been established for enhancing the accuracy of the system. However it is very important to choose the best routing algorithm. Each node in the network can independently move in any direction and continuously keeps changing its links to other nodes in the network. Therefore, the nodes keep moving in and out of the network thus the control of the network is distributed among the nodes. MANETS are non-centralized system which is robust in nature with ease in access of resources. Also the network is scalable and the node work as host as well as routers. On the other hand, there are some serious issues in MANETS due to its random topology it is difficult to find the malicious nodes in the network [1-4].

A. Sinkhole attack and routing protocol

In a sinkhole attack, the nodes which are adversary and compromised have a goal to trick all the traffic of that particular area and make a sinkhole. The intruder node announces to all the neighboring nodes in the network that it has the optimum routing path to the base station for the transfer of data packets. Thus the good nodes in the network pass the data packets through the malicious nodes and it results in dropping off of the packets. Therefore the successful delivery of data packets to the destination is prevented.

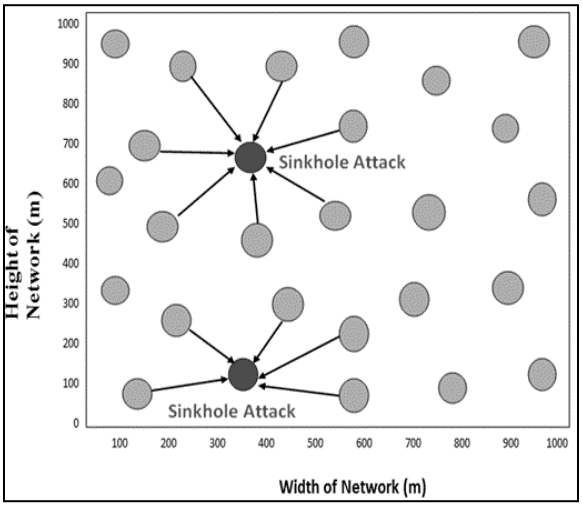

Fig. 1. *Sinkhole attack*

In MANETS different routing protocols are used [5-9]. Ad-hoc on demand distance vector (AODV) is used for outing purpose. To connect to neighbors HELLO messages are used. This message is broadcasted by one node and all other nodes receive this message. If a node does not receive the message and reject it, that means the nodes are disconnected.

When a message is sent to unknown destination Route Request (RREQ) message is sent. If the source node receives the message, the message is Route Reply (RREP) [10-14].

2. RELATED WORK

In 2014, Mariappan Kadarkarainadar Marichelvam et al. [15] proposed firefly algorithm to take care of half flow shop planning issues with two targets. Make span and mean flow time is the target functions considered here. Computational experiments have been done to assess the execution of the proposed method. The results demonstrate that the proposed calculation beats numerous different mathematics in the literature. In 2014, Manoj Jhuria et al. [16] proposed a mobile based technique to deal with overcome it. Mobile agents was generally another approach in which rather than specifically getting to a hub a project is exchanged to that system and the system executes on a system hub by using their resources and sends the obliged data back to home made. This theory shows a mobile agent based method to enhance the execution of the DSR protocol. The dynamic source Routing protocol (DSR) is a basic and effective routing protocol planned particularly for utilization in multi hop remote specially appointed systems. DSR license the system to be totally self-arranging and self-configuring, without the requirement for any subsisting system infrastructure or administration. In 2014, Mohamed Dyabi et al. [17] proposed a new algorithm in MANET that was based on clustering. The use of clustering is being done to get the best node from the network in terms of energy, memory and speed, so that cluster head selection can be done easily. Also this solution can be used to handle cryptographic keys in MANET. From the simulation results it has been concluded that performance of the proposed algorithm is good in comparison to other clustering algorithms in MANET. In 2013, Istikmal [18] 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 they investigate and assessed the execution of this routing algorithm in different situation and contrasted the outcome and standard DSR routing protocol. In 2013, K. Amjad [19] analyzed the execution of a Mobile Ad-hoc Network (MANET) utilizing the Dynamic Source Routing (DSR) protocol with gatherings of hubs moving as indicated by the Reference Point Group Mobility (RPGM) model. Four diverse arbitrary versatility models, Levy-Walk, Probabilistic Random Waypoint, Random Direction and Random Walk were chosen for gathering pioneer's portability and the impacts of changing correspondence burden and transmission reaches were explored. The outcomes demonstrate that the execution of DSR is better if bunch pioneers take after Levy-Walk portability design paying little respect to load and reach. The execution of DSR is more terrible if the pioneer's versatility carries on like Rand-Dir or Rand Walk portability models. In 2013, K. Naidu et al. [20] presented the firefly Algorithm- FA in terms of frequency control optimization technique. FA is the type of algorithm similar to swarm optimization algorithm. The proposed work analysis the efficiency and robustness of the FA in terms of optimization. In this work comparison of FA-PID and traditional PID has been done and it has been concluded that FA-PID operates better to get high efficiency.

In 2013, Mohammed Wazid et al. [21] presented that the Wireless Sensor Networks (WSNs) are inclined to different attacks in which Black hole a sort of Denial of Service (DoS) attack is extremely hard to recognize and guard. In black hole attack, the intruder catches and re-programs an arrangement of hubs in the system to obstruct the data they get as opposed to sending them towards the base station. Accordingly any data that enters the black hole locale is caught and not ready to achieve destination bringing on top of the line to-end postpone and low throughput. Beforehand little measure of work is done only for identification and counteractive action of the Black hole attack in the WSN making its discovery and avoidance extremely essential according to network execution is concerned. In this paper at first the influence of Black hole attack was measured on the system parameters took after by the proposition of a novel method for the recognition and counteractive action of Black hole attack in WSN. In 2013, Meenakshi Tripathi et al. [22] gives a description of LEACH, the most famous clustering algorithm of WSN and how LEACH can be traded off by Black Hole and Gray Hole attack. High Energy limit" idea is utilized to recreate these attacks on NS-2. The execution of WSN under these attacks was completely examined, by applying it on different system parameters with different hub densities. It is watched that the impact of the Black Hole attack is all the more on the system execution when contrasted with the Gray Hole attack. In 2013, Mohan Priya et al. [23] proposed an Intrusion Detection System (IDS) where the IDS hubs are situated in unbridled mode just when needed, to distinguish the abnormal contrast in the number of information data being sent by a hub. At the point when any anomaly is distinguished, the adjacent IDS hub telecast the message, advising all hubs on the system to helpfully disengage the malicious node from the system. In

2013, Ting Lu et al. [24] presented the energy efficient GA algorithm to determine 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. In 2012, Ashok M. Kanthe et al. [25] 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 to be 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 environment.

In 2012, K.S Sujhatha et al. [26] proposed an IDS system based on Ad hoc on-demand routing protocol –AODV protocol to mitigate the black hole attack using Genetic Algorithm- GA. The simulation model analyses that behavior nodes affects the black hole attack and various rules like Request Forwarding Rate, Reply Receive Rate has been used in AODV protocol. In the end performance of MANET has been analyzed. In 2012, M. H Sulaiman et al. [27] presented the usage of Firefly Algorithm (FA) in explaining the Economic Dispatch (ED) issue by minimizing the fuel cost and considering as far as possible and transmission misfortunes. ED is a standout amongst the most difficult issues of power system since it is hard to take care of the specific burden demand with the base fuel expense and transmission misfortune. FA is a meta-heuristic algorithm which was roused by the flashing behaviours of fireflies. The main role of firefly's flash is to go about as a sign framework to draw in different fireflies. In this paper, 26-bus system is used to demonstrate the adequacy of the FA in taking care of the ED issue. Lila Kari, Grzegorz Rozenberg [28] reviewed the many surface of Natural computers such as cellular automata, neural networks, genetic algorithms, swarm intelligence, computer membrane, intelligent water droplets, firefly algorithms, swarm optimization, based on biogeographic optimization, swarm optimization of particles, search cuckoo. X.S. Yang et al. [29] has created a New meta-heuristic algorithm, called cuckoo search (CS), used to solve optimization problems. This approach depends on the necessary action with several birds key cuckoo clutch several species of fruit flies, in addition to the flight operation fused Levy. They also demonstrate that the proposed technology and personnel test then in addition to particle swarm optimization through genetic algorithms to evaluate the performance of the above. In 2006, Rohit Gupta, Ravindra Singh, Sajal Kumar [30] A multi-tone synchronous collision resolution system permits communication nodes within a MANET to contend simultaneously for a plurality of available channels. The communication nodes contend for access using a synchronous signaling mechanism that utilizes multiple tones in a synchronous manner to resolve contentions. Contentions are arbitrated locally, and a surviving subset of communication nodes is selected. The communication nodes of the surviving subset then transmit data packets simultaneously across the available communication channels. In 2012, Subramanian Ramanathan et al. [31] described systems and methods including adaptive routing processes for packet-based wireless communication networks. This routing approach works both in MANETs (when a contemporaneous end-to-end path is available) and in DTNs (when a contemporaneous end to end path is not available, but one of formed over space and time). In particular, the methods include adaptively selecting a routing process for transmitting a packet through a node in the network based on available information on the network topology and/or the contents of the packet. In 2012, Dinesh Verma [32] systems and methods are provided for detecting malicious behavior in mobile ad-hoc wireless networks. The mobile ad-hoc network contains a plurality of actual nodes and a plurality of decoys that are derived from the actual nodes using duplicate instances of the operational software of the actual nodes in combination with a virtual interconnection topology created to make the decoys appear as actual nodes within the mobile ad-hoc network. The interconnection topology includes routing characteristics indicating that the most efficient path of communication to any given decoy is through at least one actual node in the network. The decoys are used to identify malicious behavior in the network and in particular to identify attempt to communicate directly with decoys in contradiction to the created interconnection topology. When the malicious behavior is associated with an identifiable node, corrective action is taken that includes quarantining that node from the other nodes in the network. In 2006, Thomas Jay Billhartz [33] apprise that mobile ad-hoc network (MANET) may include a plurality of nodes for transmitting data there between using a media access layer (MAC), where each of the nodes has a respective MAC address associated therewith. The MANET may also include a policing node for detecting intrusions into the MANET by monitoring transmissions among the plurality of nodes to detect frame check sequence (FCS) errors from a MAC address, and generating an intrusion alert based upon detecting a number of FCS errors for the MAC address exceeding a threshold. The policing

node may also detect intrusions based upon one or more of failed MAC addresses authentications, illegal network allocation vector (NAV) values, and unexpected contention or contention-free operation.

3. PRILIMINARIES

An attempt is made to study the significance of the application of the neural network for the prevention of sinkhole attack method. We get the parameters like node id, no. of nodes, network width, network length etc. The simulations will carry out by using MATLAB as the language that we use to develop the proposed framework. We used the AODV protocol to modify the network parameters that we added to the simulator and evaluate our proposed framework based on it. We assume that N number of sensor nodes are deployed in the field randomly and form the connected network. Each node has its unique identity. We further assume that, each sensor nodes generate and send data at B bits per unit time. The initial energy of sensor node is θ where θ > 0.The result evaluation will be done using following parameters:

Energy Consumption**:** The total energy consumed in the network due to running of tasks.

$E_{consum}=E_{loss(normal)}+E_{loss(sinkhole)}$ (1)

E_{consum} is the total energy consumed which is the sum of energy loss when the network is normal ($E_{loss(normal)}$) and the energy loss when the sinkhole nodes are present ($E_{loss(sinkhole)}$).

Throughput**:** It is the rate at which the data packets are delivered successfully over a communication channel. First calculate the total packet loss in the network with and without sinkhole attack. Let us denote it by ϕ.

Φ = Total packet drop (normal) + Total packet drop (sinkhole) (2)

Throughput here is represented by α and given by:

$$\alpha = \frac{[\beta - \phi]}{t} \quad (3)$$

Where β is the total no. of packets and t is the total time taken by the packets to reach the destination.

Delay**:** It is the time taken for the transmission of packets from source to destination. Delay is given by:

Delay= Delay (normal) + Delay (sinkhole) (4)

Where Delay (normal) is the delay when the network is not sinkhole attacked and Delay (sinkhole) is the delay when the network is sinkhole attacked.

Packet Delivery Ratio: PDR is the ratio of total no. of packets delivered (P_d) out to the total number of packets sent over network (P_t).

$$PDR = P_d / P_t \quad (5)$$

First the parameters are evaluated when the network is free from sinkhole attack then the parameters are evaluated when the network is attacked b sinkhole attack. Then at the end the parameters are compared. The various parameters are evaluated and the network is optimized using genetic algorithm.

4. GENETIC ALGORITHMS

In this paper, Genetic algorithm is used to link the nodes and establish the network. It is a strategy for delicate figuring which utilizes the laws of choice and advancement. The Genetic algorithm starts from distinguishing the information set called population. These are bits which are utilized and encoded exclusively. These are characters or whole numbers which shape a chromosome. Now the Assessment Function is utilized to decide the honest chromosome. At each step, the process selects individuals randomly from the current population and then the selected individuals are used as parents to produce the next generation. Over the successive generation, the population is evolved to achieve an optimal solution at the best point. There are three steps involved in this process-

1. Create a populace of arbitrary hopefuls arrangements named pop.
2. Until the calculation end conditions are met, do the accompanying (every emphasis is known as an era):
(a) Create an unfilled populace named new-pop.
(b) As new-pop is not occupied, perform the accompanying:
(i). Choose two people aimlessly since pop so that people that are extra fit will probably be chosen.
(ii). Cross-over the two people towards delivering two new people.
(c) Let every person in new-pop contain an irregular opportunity to transform.

Choose the human being from pop by the highest fitness as the answer to the difficulty. The selection process is analogous to the survival of the fittest in the natural world. Individuals are selected for "breeding" (or cross-over) based upon their fitness

values-the fitter the individual, the more likely that individual will be able to reproduce.

Selection rule-In this process, individual are selected called parents which contribute to the population at the next generation.

Selection operator
Wheel path selection algorithm can be used to select the initial size of the population. It can be as follows:
Algorithm: Pseudo algorithms of Roulette wheel selection
For M=1 to L
Do
Merge fitness function values
From population of each populace
End
For m=1 to l population
Find likelihood until new selection has been obtained
end
There is another method called tournament method can also be used to select a population.
Algorithm: Pseudo algorithms of tournament selection
Choose initial population
From left population, select individual chromosomes.
Choose best selected chromosomes.
Do crossover
Do repetition
End
Crossover rule- In this process, the parent is combined to form children for the upcoming generation.
Crossover Operator
The crossover operator is mainly used to change chromosome programming so that a new generation can occur.
Algorithm: Pseudo algorithms of crossover operation
For o= 0 to crossover point do
child S _gene[o] = parent S_ gene[o]
child S _gene[o] = parent S_ gene[o]
end
for o= crossover point to chromosome length do
child S _gene[o] = parent S_ gene[o]
child S _gene[o] = parent S_ gene[o]
end

Mutation rule- The random changes are applied to the individual parents to form children.

Mutation Operator
Mutation operators are used to differ the generation of GA (Genetic Algorithm).
Operator by mutant chromosome form a randomly selected collection of genes then reverses its value.

Before Mutation	0	1	1	0	1	1	1
After mutation	0	0	1	1	1	1	1

The calculation establishes a "populace" of imaginable answer for the matter and provides them "a chance to advance" above a variety of eras to determine improved actions [15-17]. Steps required in GA are as per the following:

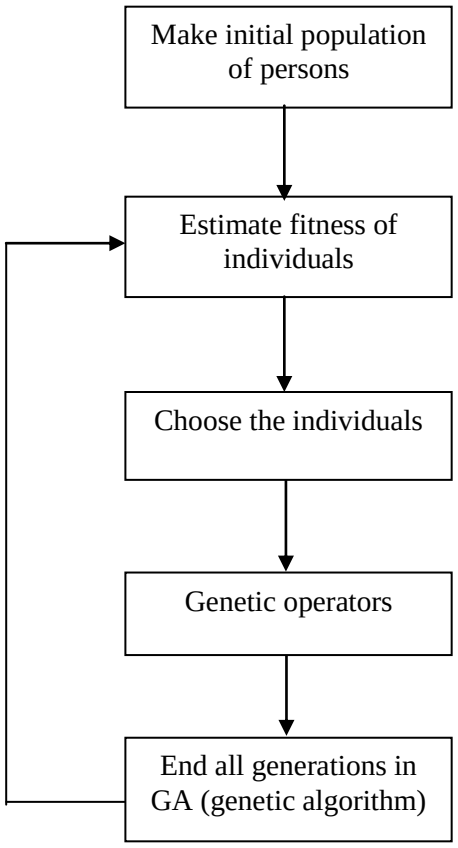

Fig. 2. *Genetic algorithm*

5. SIMULATION SCENARIO

BBO A simulation is performed using MATLAB and AODV protocol is used to modify the network parameters. In the simulation, firstly the number of nodes is entered and then simulation area. Now enter the cluster heads and number of rounds to run for the network then the cluster head is plotted. Sinkhole node is not found, the sinkhole attack detection takes place which produces the number of multiple copies in the network which increases the load in the network. The various parameters are evaluated like energy consumption, throughput, and delay and

packet delivery ratio. Network is optimized using Genetic algorithm using weight function. The parameters are evaluated again in the end like energy consumption, throughput, and delay and packet delivery ratio. The proposed work is compared with the previous one. The following parameters are taken for the simulation given in table below:

TABLE I. PARAMETER SETTING

Parameters	Values
Simulation Area	1000mX1000m
Total Number of sensor nodes	50
Routing Protocol	AODV
Total Number of Rounds	5
Total Number of Packets	1000
Communication Protocol	IEEE 802.15.4
Node Deployment	Random
Battery Model	Linear
Energy Model	Generic
Battery (mAh)	300
Application	Traffic Generator

The following steps are required during the simulation:

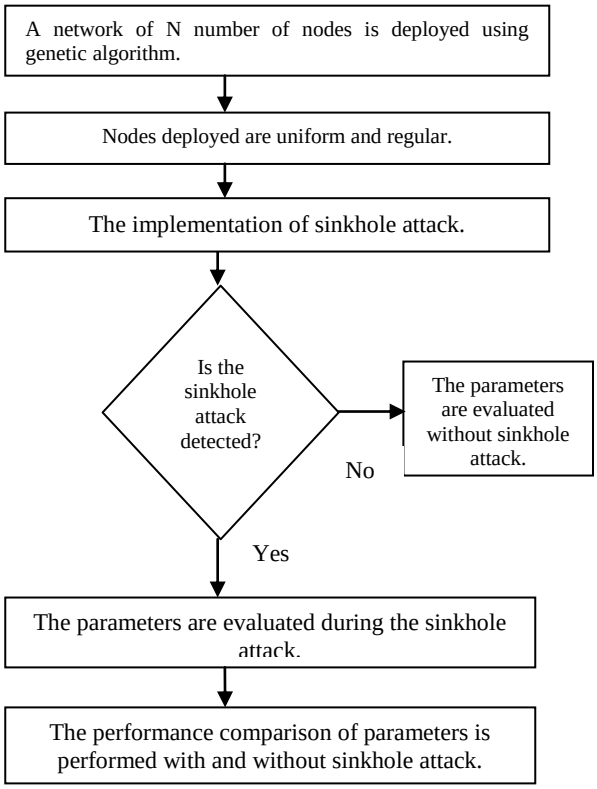

Fig. 3. *Steps for evaluation of parameters with and without sinkhole attack*

TABLE II.COMPARISON OF METRICS w.r.t ROUND 1

Parameters	With attack	Without Attack
Throughput(bits/sec)	400	420
Delay (secs)	12	5.8
PDR	91.6	92.8
Energy consumption(J)	53	50

6. RESULTS AND DISCUSSIONS

The network is setup for 1000 m^2 area as shown in Fig. 4, sinkhole nodes are detected in the network. The Table II shows the comparison of parameters with attack and without attack of sinkhole attack in the network when the round is 1.The parameters are Throughput, Delay, PDR (Packet Delivery Ratio) and Energy Consumption. Fig.5. shows the impact on energy consumption.

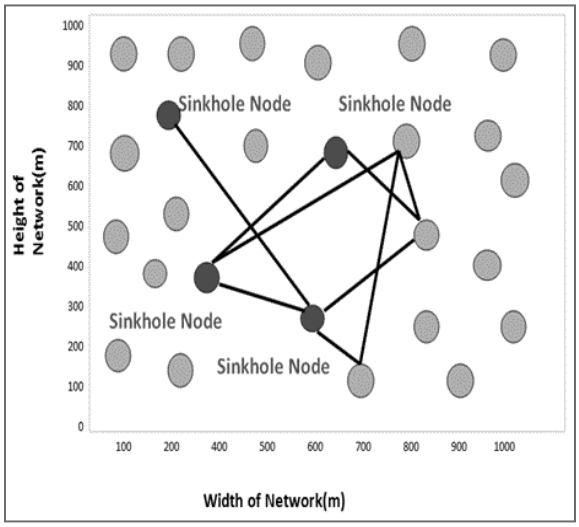

Fig. 4. *Detection of sinkhole attack*

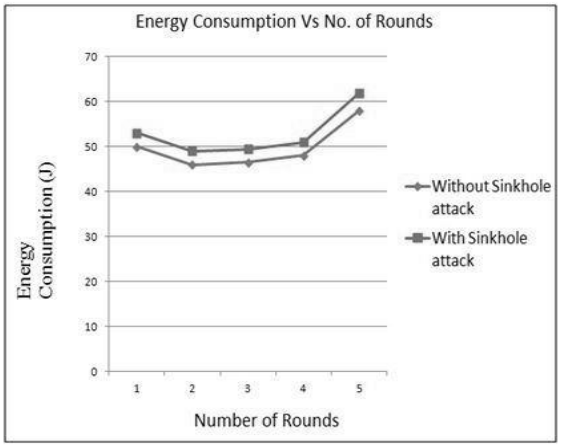

Fig. 5. *Energy Consumption Vs No. Of Rounds*

When the network is free from any attacks, the energy consumption is 50 J in round 1, i.e. the packets are utilizing the energy in transferring of nodes from source to destination.
But when the network is attacked with sinkhole, the malicious nodes increases in the network and thus the load of the network increases .When the load increases the malicious nodes consume energy and thus energy consumption increases. So in the round 1, energy consumption significantly increases to 53 J.
Fig.6. shows the impact on Throughput:

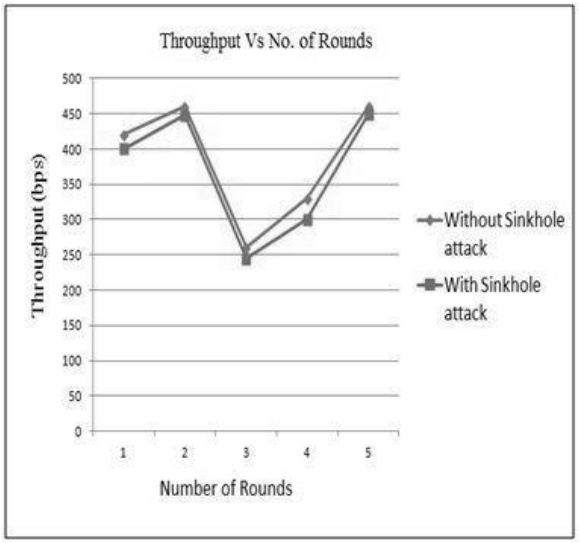

Fig. 6. *Throughput vs no. of rounds*

When the network is healthy and free from any attacks then the throughput is 420 bit/sec. While when the network is attacked with sinkhole, the malicious nodes either don't forward the packets or drops the packets. Thus the throughput significantly decreases in round 1 which is 400 bit/sec.
Fig.7. shows the impact on Packet Delivery Ratio:

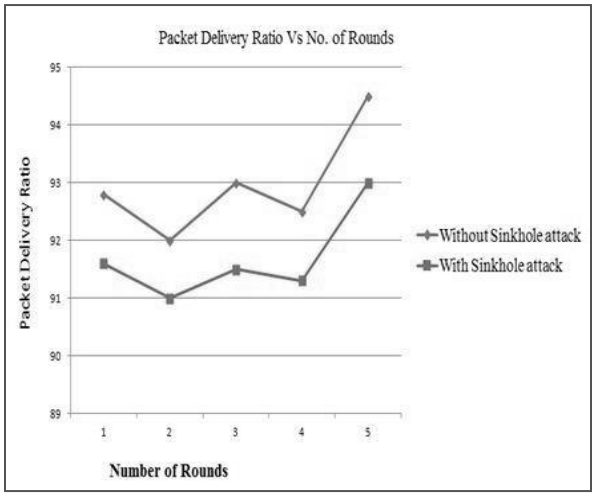

Fig. 7. *PDR vs no. of rounds*

Due to increase in the malicious nodes in the network, the packet delivery ratio significantly decreases from 92.8 (without attack) to 91.6 (when the network is attacked with sinkhole).This decrease in the packet delivery ratio is due to packet drops by malicious nodes in the network.
Fig.8. shows the impact on Delay:

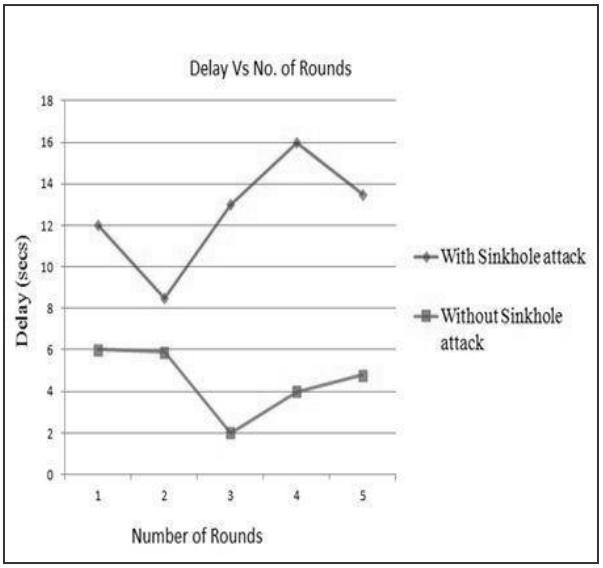

Fig. 8. *Delay vs no. of rounds*

Similarly, the delay increases from 6 secs (when the network is free from any attack) to 12 secs (with sinkhole attack).This delay occurs because the malicious nodes sends the wrong information to the network nodes that it has the shortest path and when the malicious nodes get the information it consumes the data and drops it . Thus the time taken to reach the information from source to destination is more as the network has to initialize the packet transfer from the source once again.

7. Conclusion And Future Work

MANET is very susceptible to various attacks in the network, as it is dependable network. It is flexible in nature and utilizes various routing protocols for transmission of packets from source to destination. AODV is one type of routing protocol that is less prone to attacks and hence is utilized in proposed work. Among various attacks, sinkhole attack is an actual threat in contradiction of AODV protocol in MANET. The malicious nodes generally target the routing controller messages interrelated to routing data. It has been concluded that the Genetic algorithm works well by optimizing the sinkhole network and it has been measured that various metrics are optimized when evaluated after preventing the attack i.e. delay, packet delivery ratio, energy consumption and throughput.

REFERENCES

[1] Caimu Tang, and Dapengoilver, "An Efficient Mobile Authentication Scheme for Wireless Networks, " IEEE, 2011.

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

[3] B. Forouzan,"ICMP", In: Data Communication and Networking, Fourth Ed., McGraw-Hill, ch.21, 2006, pp. 621-637.

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

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

[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), Oct, 2003, pp. 21–32.

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

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

[10] 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)

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

[12] Perkins.C.E, "Ad hoc Networking, " Boston, Addison Wesley (2001).

[13] 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, pp.6, June 2011.

[14] 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, 2007, pp.118–123.

[15] 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.

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

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

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

[19] 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.

[20] 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.

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

[22] 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, 2013, pp. 1101 – 1107.

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

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

[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, 2012, pp.1-5.

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

[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] Lila Kari, GrzegorzRozenberg, "The Many Facets of Natural Computing," Communication of the ACM,vol. 51, no.10, 2008.

[29] X.S. Yang, S. Deb, "Cuckoo Search via Lévy Flights," Proceedings of World Congress on Nature & Biologically Inspired Computing (NaBIC 2009, India), IEEE Publications, 2009, pp. 210-214.

[30] Rohit Gupta, Ravindra Singh, Sajal Kumar, **"**Multi-channel MAC protocol using multi-tone synchronous collision resolution in a mobile ad hoc network," US7466676, May 31, 2006.

[31] Subramanian Ramanathan , Prithwish Basu, Richard Earl Hansen, Christine Elaine Jones, Rajesh Krishnan, Regina Rosales Hain, "Systems and methods for adaptive routing inmobile ad-hoc networks and disruption tolerant networks ," US 8149716 B2, Apr 3, 2012.

[32] Dinesh Verma , "Method and apparatus for detection of malicious behavior in mobile ad-hoc networks ,"US 8122505 B2, Feb 21, 2012.

[33] Thomas Jay Billhartz ,"Mobile ad-hoc network with intrusion detection features and related methods ," US 7082117 B2, Jul 25, 2006.