2nd International Conference on Science, Technology and Management
University of Delhi (DU), Conference Centre, New Delhi (India)
27 September 2015, www.conferenceworld.in, www.icstmdu.com
978-81-931039-6-8

GENETIC OPTIMIZATION BASED ADAPTIVE APPROACH FOR THE DETERMINATION OF BLACK HOLE ATTACK IN AODV PROTOCOL

Chandeep Singh[1], Vishal Walia[2], Dr.Rahul Malhotra[3]

[1]ECE Department, RIEIT, Railamjra

[2]Associate Prof.ECE Department, Dean Acdemic, RIEIT, Railmajra

[3]Prof.ECE Department, Director GTBKIET, Malout

ABSTRACT

MANET is a self-configuring infrastructure less network. The lacks of an infrastructure in ad hoc networks pose large challenges in the functionality of these networks. Mobile Ad Hoc Network has number of security problems that exists due to the self-configuring nature of nodes. The black hole attack is one of the well known security intimidation in wireless mobile ad hoc networks. The intruders use the loophole to take out their malicious behaviors because the route discovery process is essential and inevitable. Many researchers have conducted dissimilar detection techniques to suggest different types of detection schemes. More focus is on the study of black hole attack in MANET after analyze the effects of black hole attack by means of network load, throughput and end to end delay. The black hole attack is prevented with the genetic algorithm.

Index Terms: MANET, Black hole attack, AODV, Genetic Algorithm, Throughput.

I. INTRODUCTION

Mobile ad hoc networks have mainly been used for tactical network related applications to recover battlefield communications and survivability. Present ad hoc network are measured the third generation [3] [5]. The first generation ad hoc network came into limelight in 1970s. In 1970‟s, these are called Packet Radio Network (PRNET) [9]. The Defense Advanced Research Project Agency (DARPA) initiated investigates of using packet-switched radio communication to provide consistent communication between computers and urbanized PRNET. The PRNET is then evolve into the Survivable Adaptive Radio Network (SURAN) in the early 1980‟s. SURAN provides some payback by improving the radio performance. This is the basis MANET is one of the elementary research field.

978-81-931039-6-8

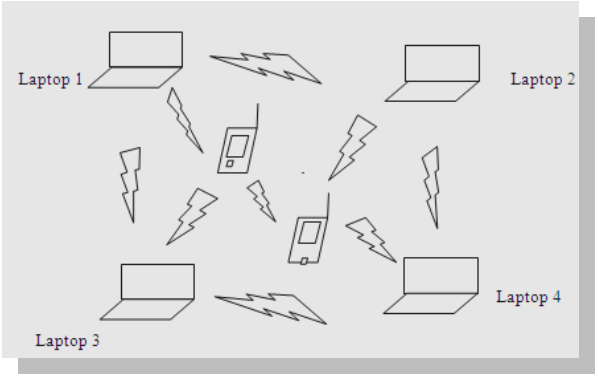

Figure 1: Mobile Ad hoc Network

MANET is the subset of various applications like static networks, large networks, ranges from large to small dynamic networks.

1.1 Routing in Manet

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 restriction wireless link. Since the nodes are mobile, the network topology may change randomly over time [10]. The network is de centralized and all the network activities like discover the topology and deliver messages must be complete by the nodes .They do not use any contact point to bond to other nodes .It must be able to switch high mobility of the nodes. MANET routing protocols could be broadly surreptitious into three major categories:

1.1.1 Proactive Routing Protocols

It possesses in order of the reason route before it is wanted for the routing of data to the reason. Routing tables are maintaining in this protocol. Update in the routes paths is swap among the nodes to replicate the topological changes. These routing protocols update the routing table in order either occasionally or in reply to alter in the network topology. These protocols repeatedly learn the topology of the network by replace topological information among the network nodes. The profit of these protocols is that a source node does not need route discovery actions to discover a route to a purpose node. Disadvantage of this protocol is it is slow as it has vast amount of traffic as these have to uphold a reliable and up-to-date routing table which requires substantial messaging overhead and thus uses large piece of the bandwidth to keep in order up to date [11].

1.1.2 Reactive Routing Protocols

A dissimilar proactive, reactive routing protocol does not create the nodes to start a route discovery process until a way to reason is required. The advantage of these protocols is that overhead messaging is reduced which consequences in less usage of bandwidth. Difficulty of these protocols is the delay in discover a new route which leads to higher latency [13].

1.1.3 Hybrid Routing Protocols

The hybrid routing protocols inhabit both reactive and proactive property by maintaining intra zone information pro-actively and inter zone information reactively. Often reactive or pro active feature of a particular routing protocol might not be enough; in its place a mixture might yield better solution.

978-81-931039-6-8

II.BLACK HOLE ATTACK

In black hole attack, a cruel node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to interrupt. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. That is why intruder has always accessibility [1]. In flooding before acknowledgment the reply node sends the packet but in wrong direction so its route gets forget [5]. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies [5]. Fig.2 shows how black hole problem arises, here node 1 want to send data packets to another node and initiate the route discovery process. So if 1 node is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. In this way that node will imagine that this is the active route and thus active route discovery is complete. Node 1 will disregard all other replies and will start seeding data packets to node n. In this way all the data packet will be lost extreme or lost [7].

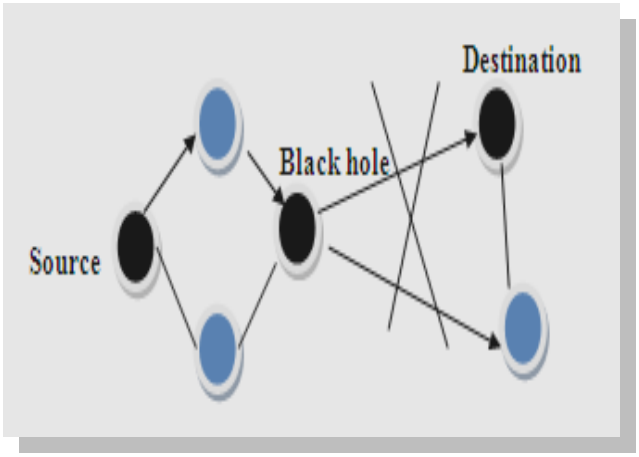

Figure 2: Black Hole Attack

2.1 Basic Strategies to Mitigate the Black Hole Attack

The malicious nodes in this attack acts as Black hole that drop all the data packets approved by it. If the attacking node acts as a linking node of two components, the severance of network in two severed components wound taken place. The main strategy to mitigate the problem [4] [8] [10]:

- To assemble the number of RREP messages.
- Hope the varied redundant paths to destination node.
- A buffering process need to be taken place till the safe route is found.
- With the previous sequence number, a table needs to be maintaining in increasing order.
- RREQ request would be send by the sender node to its neighbor.
- When the RREQ reaches the destination, the RREP reply was sent with last packet sequence number.
- If some trouble occurs, then the RREP contains a wrong sequence number.

III. GENETIC ALGORITHM

According to Goldberg et al., 1989, GA is commonly used in applications where search space is huge and the precise consequences are not very significant.

Genetic algorithms (GAs) are computer programs that take off the processes of biological growth in order to explain problems and to make evolutionary systems [2,6]. Specify the problem to be solved and a bit-string illustration for candidate solutions, the simple GA works as follows [20,22]:

Step 1: Set up a arbitrarily generated population of N L-bit chromosomes.

Step 2: Calculate the Fitness F(x) of each chromosome x in the population.

Step 3: Repeat the following steps until N offspring have been created:

(a) Choose a pair of parent chromosomes from the present population, with the probability of selection being an increasing function of fitness. The same chromosome can be selected more than once to become a parent.

(b) With probability pc (the crossover probability), cross over the pair at a arbitrarily chosen point to form two offspring or to make the copies of their parent's offspring.

(c) Change the two offspring at each locus with probability pm (the mutation probability) and put the resultant chromosomes in the original population.

4. Change the current population with the new population.

Every repetition of this process is known as Generation. A GA is usually iterated for wherever from 50 to 500 or more generations known as Run. With the ending, there are frequently one or more extremely fit chromosomes in the population. Since arbitrariness plays a huge role in every run, different behavior can be produced when the random number seeds.

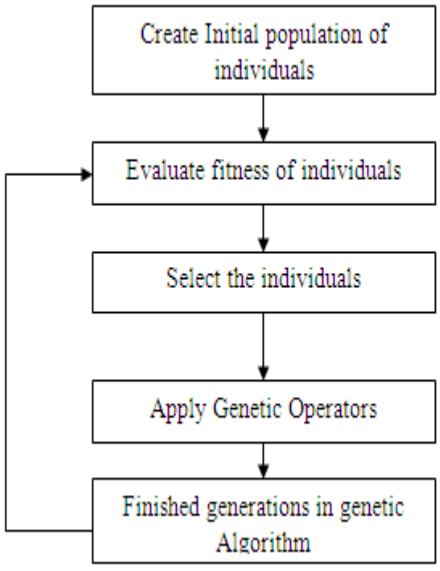

Figure 3: Flowchart of Genetic Algorithm

[Start] Generate irregular populace of n chromosomes (suitable answers for the issue) [12,14]

[Fitness] Evaluate the wellness f(x) of every chromosome x in the populace

[New population] Create another populace by rehashing after ventures until the new populace is finished.

[Selection] Select two guardian chromosomes from a populace as indicated by their wellness (the better wellness, the greater opportunity to be chosen)

[Crossover] with hybrid likelihood traverse the folks to shape posterity (kids). In the event that no hybrid was performed, posterity is a precise duplicate of folks.

[Mutation] with a transformation likely to change new posterity at every locus (position in chromosome).

[Accepting] Place new posterity in another populace

[Replace] Use new produced populace for a further run of calculation

[Test] if the end condition is fulfilled, stops, and returns the best arrangement in current population.

[Loop] Go to step 2

IV. AODV PROTOCOL

AODV stands for on demand routing. This protocol is like any other on demand routing protocol which facilitate an even adaptation to changes in the link conditions. In case when a link fails, messages are sent only to the pretentious nodes. With this information, it enables the affected nodes to undo all the routes through the failed link. AODV has low memory overhead, build uncast routes from source to the destination and network utilization is less. When two nodes in an ad hoc network wish to found a connection between each other, it will enable them to build multichip routes.

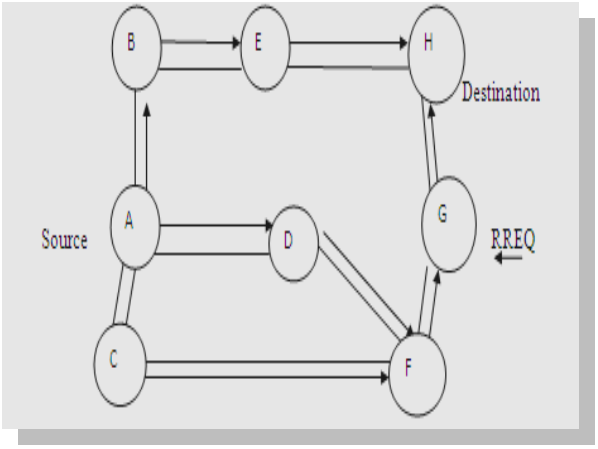

Figure 4: AODV Protocol

- DSR has less routing overhead than AODV.
- AODV has less normalized MAC overhead than DSR.
- DSR is based on a source routing apparatus whereas AODV uses a combination of DSR and DSDV mechanisms.
- Higher-mobility scenarios of AODV protocol.
- Less recurrent route discovery processes than AODV [19].

V. RELATED WORK

Adnan Nadeem and Michael Howarth (2009) have proposed that their approach not only secures the MANET from a wide assortment of routing attacks but also has the capability to detect new unforeseen attacks. Simulation results of a case study show that our proposed machine can successfully detect a various types of attacks. Simulation results show this implemented mechanism can secure MANETs from a wide variety of attacks with an affordable processing overhead. **Zhao Min and Zhou Jiliu (2009)** described the routing security issues and the problem of coordinated attack by multiple black holes acting in group in MANET. Two authentication mechanisms, based on the hash function, the Message Authentication Code (MAC) and the

Pseudo Random Function (PRF), are proposed to provide fast message verification and group identification, identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack. The methods above proposed improve the routing security in ad-hoc environment and avoid cooperative black hole, and also prevent the network form further malicious behavior. Two authentication mechanisms eliminate the need for a PKI or other forms of authentication infrastructure, which are usually not practical in MANET**. Noor M. Asraf (2010)** proposed a genetic algorithm that finds an optimal multicast tree that satisfies multiple QoS parameters. Simulation studies to verify the proposed approach in meeting the QoS objectives. It is noted that the optimal paths obtained by the proposed GA appear non-uniform with respect to the increase in the number of nodes. The performance and scalability results are presented and compared against a related algorithm. Based on these results, it is evident that the MOGA-based approach produces better performance results and demonstrates its ability to optimize multiple objectives simultaneously. Sunil **Taneja (2010)** shows that Mobile Ad-hoc Network is set of multi-hop wireless mobile nodes that converse with each other without central manage or recognized communications. The wireless relations in this network are very error horizontal and can go down often due to mobility of nodes, intrusion and less transportation. Therefore, routing in MANET is a grave task due to highly active environment. In recent years, some routing protocols have been planned for mobile ad-hoc networks and important among them are DSR, AODV and TORA. This research paper provide a summary of these protocols by present their characteristics, functionality, benefits and borders and then makes their relative analysis so to evaluate their show. The objective is to make notes about how the show of these protocols can be better. **Soufiene Djahel (2011),** made a comprehensive survey investigation on the state-of-the-art countermeasures to deal with the packet dropping attack. Furthermore, we examine the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a sophisticated attack. In this paper we have presented a survey of the state of the art on securing MANETs against packet dropping attack. The attack schemes, as well as prevention, detection and reaction mechanisms have been explored. They categorized them into three categories according to their goals and their specific strategies. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. **Fan-Hsu n Tseng (2011)** surveyed the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. It was expected to furnish more researchers with a detailed work in anticipation. In this paper, they first summary the pros and cons with popular routing protocol in wireless mobile ad-hoc networks. Then, the state of the art routing methods of existing solutions are categorized and discussed. The proposals are presented in a chronological order and divided into single black hole and collaborative black hole attack. **Shekhar Tandan (2011)** has shown a mechanism based on PDRR to detect the black hole attack in MANET with AODV protocol. This paper proposed detection of black hole attack using AODV protocol. **Shanmuganathan and Mr. T. Anand (2012)** described that Mobile Ad-hoc Network is used the majority generally all around the world, because it has the aptitude to converse each other lacking any set network. It has the leaning to take decision on its own that is independent state. MANET is generally known for transportation less. The bridge in the network is usually known as a base station. A united security solution is very a lot needed for networks to protect both route and data forward operation in the network layer. Refuge is an important requirement in MANET. Lacking any

proper safety solution, the hateful node in the network will act as a usual node which causes attic is tumbling and choosy forwarding attack normally known as gray whole attack. In this paper we survey about the diverse types of attacks occur in the network layer in MANET. Gray Hole attack is one of the attacks in net layer which comes under security active attacks in MANET. **Sapna Gambhir and Saurabh Sharma (2013)** discussed the routing security issues in MANETs and in particular the malicious node attack .A security protocol has been proposed that can be utilized to identify malicious nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the malicious nodes. As future work we intend to include that the proposed security mechanism may be extended so that it can defend against the malicious nodes which are present inside the clusters. The next step is to simulate more scenarios in which more complicated misbehaviours exist and other metrics need to be measured such as latency and end-to-end delay. **Ei Ei Khin and Thandar Phyu (2014**) analyzed the impact of black hole attack on Ad-hoc On-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are taken on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay. In this paper, we have analyzed the effect of black hole attack in the performance of AODV protocol. The simulation has been done using the network simulator (NS-2.34). The performance metrics like average end to end delay, packet delivery ratio and routing overhead has been detected and analyzed with the variable node mobility, pause time and number of transactions as shown in Figure 2-13. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. **Mahnaz Chishti (2014)** described that black hole attack is implemented on AODV protocol which reduce the performance parameters of network by exploiting the packet sequence number included in any packet header. The proposed mechanism of Intrusion Detection System (IDS) is also implemented to enhance the network performance. Simulation results using Network Simulator 2(NS2) shows that, in a high mobility environment, malicious node could be detected and the packet delivery ratio has been improved.

VII. RESULTS

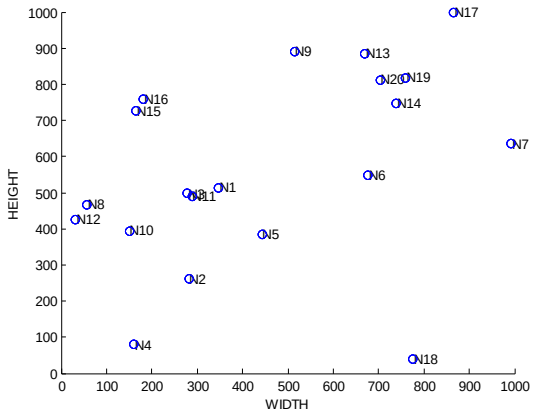

Figure 5:Number of Nodes in the Network

Above figure shows the network model of 1000*1000 length and width using 20 number of nodes. Above figure shows the data transmission from source to destination using red line. Here red line shows the path of data transmission. Blue circles show the nodes participating in the whole network.

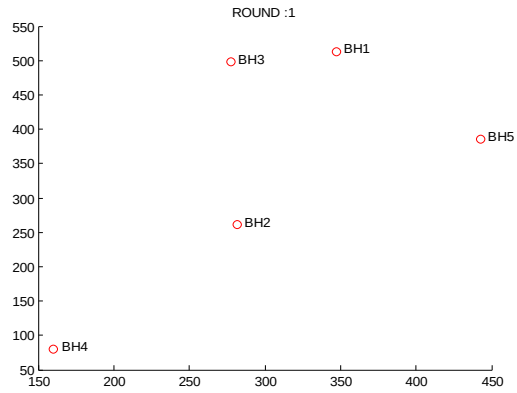

Figure 6: Round 1

In the round 1 of black hole node attacks, there are only five black hole nodes.

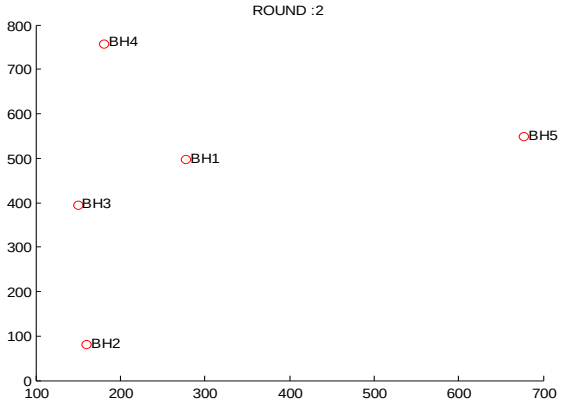

Figure 7: Round 2

In the round 2 of black hole node attacks, there are only five black hole nodes.

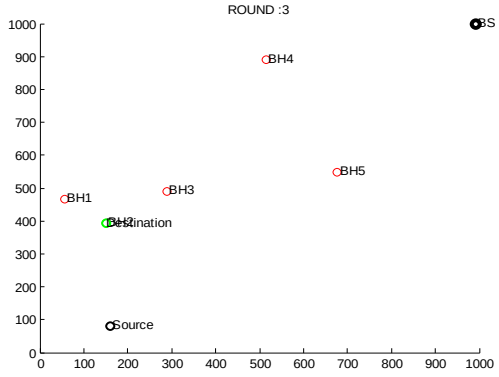

Figure 8: Round 3

In the round 3 of black hole node attacks, there are only five black hole nodes.

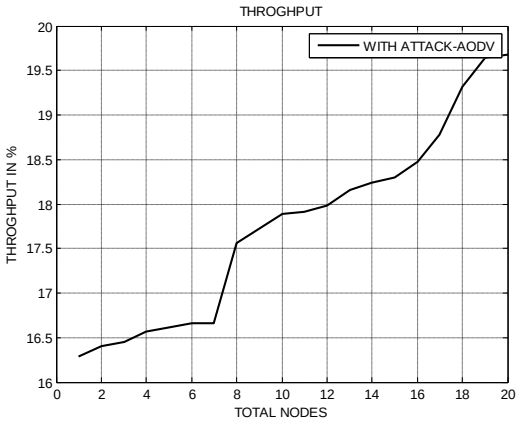

Figure 9: Throughput with attack

Throughput is the number of packets sent over the network in given time. Above figure shows the throughput value in attack in AODV without application of GA. It has been seen that value of throughput is being reduced in the figure on later stage.

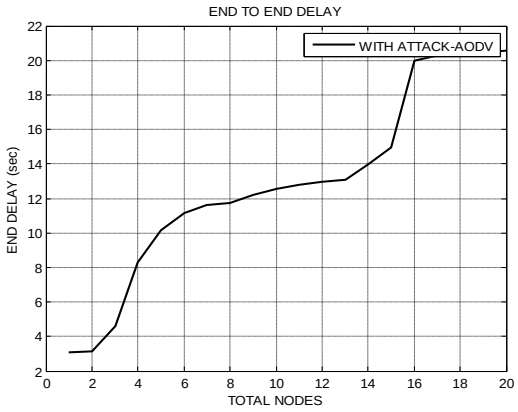

Figure 10: End to end delay with Attack

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows the end to end delay with AODV. It has been seen that end to end delay decrease in the end.

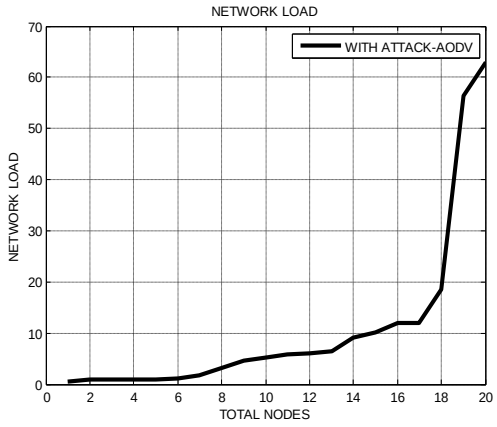

Figure 11: Network load with attack

Above figure shows the network load in AODV protocol without GA. It has been seen that network load decreases due to addition of GA, as it has been increased by black hole attack in network.

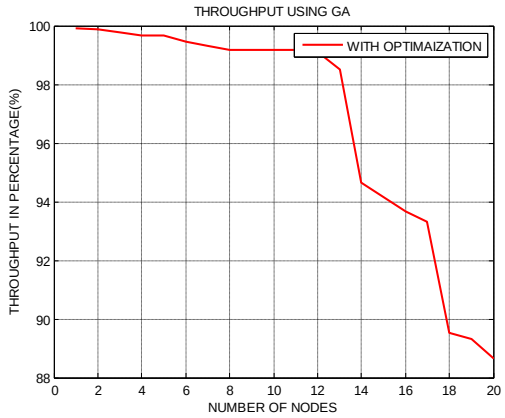

Figure 12: Throughput with optimization

The attacker nodes cause decrease in the throughput of the network. It is because number of collisions is more in system and it is optimized using GA algorithm as shown above in AODV network.

Above figure shows that throughput value with GA/DSDV. Total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity.

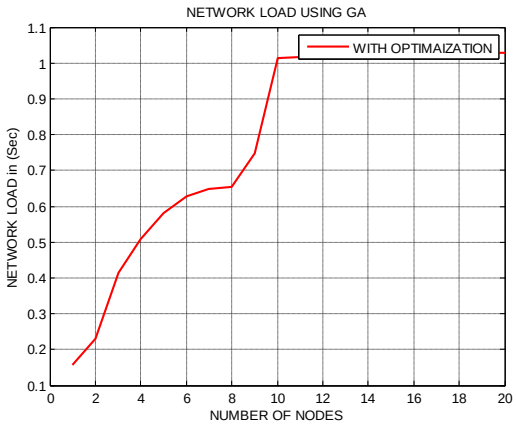

Figure 13: Network load with optimization

As the no nodes increases the network load increases leading to congestion which will Detroit the network performance since replicated nodes will act as the original nodes the source node will unable to choose the intermediate nodes which will ultimately create delay and the message carrying capacity will be decreased leading to congestion. Above figure shows the network load in AODV protocol in attack with the use of GA.

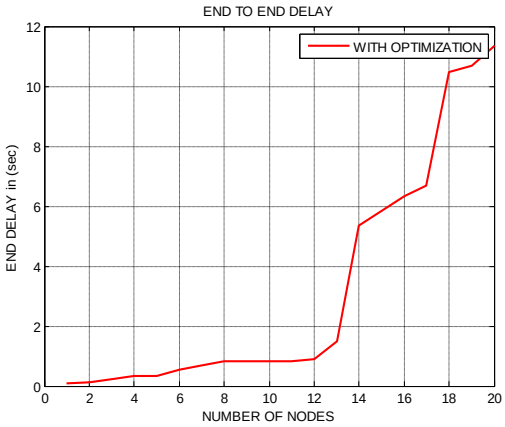

Figure 14: End to End delay with optimization

End to end delay is the time taken by the packet to reach from source to destination. It must be high in the network. Above figure shows the end to and delay in AODV protocol in attack without the application of GA. In starting it reduces but after some time it continues in straight line.

VIII. CONCLUSION

In Black hole attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding; no data will be transfer further. This will degrade the network lifetime and performance of the network. To solve this problem I have used genetic algorithm for enhance the network lifetime and performance of the network. In this research, we have analyzed the effect of black hole attack in the performance of GA in AODV protocol. From the simulation results it has been observed that AODV-GA is better than only AODV. So, the detection and prevention of black hole attack in the network exists as a challenging task. In the future, firefly optimization algorithm in case of Genetic algorithm for the black hole detection as well as black hole prevention can be used.

REFERENCES

[1] Ahmed Sherif, Maha Elsabrouty. Amin Shoukry, “A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)”, IEEE, pp: 346-352, 2013.

[2] Anup Goyal and Chetan Kumar, “GA-NIDS: A Genetic Algorithm based Intrusion Detection System”, 2010.

[3] 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.

[4] Isaac Woungang et.al, “Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks” 978-1-4673-1550-0/12/$31.00 ©2012 IEEE.

[5] Kaur, Harjeet, Manju Bala, and Varsha Sahni. "Study of Black hole Attack Using Different Routing Protocols in MANET." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering2.7 (2013): 3031-3039.

[6] K.S. Sujatha, V. Dharmar. R.S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET", Conference: Recent Trends in Information Technology (ICRTIT), IEEE, pp.28-33, 2012.

[7] Prachee N. Patil et al, "Black Hole Prevention in Mobile Ad Hoc Networks using Route Caching" 9781-4673-5999-3/13/$31.00 2013 IEEE.

[8] 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.

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

[10] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16.

[11] Wahane, Gayatri, and Savita Lonare. "Technique for detection of cooperative black hole attack in MANET." 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.Zhu Xialonget. Al, "A location privacy preserving solution to resist passive and active attacks in VANET", IEEE, Vol.11, pp. 60-67, 2014.

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

[13] 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, 2012.

[14] 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, August 2010, China.