PREVENTION OF BLACK HOLE ATTACK IN MANET USING GENETIC ALGORITHM

Arshdeep Kaur[1], Mandeep Kaur[2]

[1]Student, [2]Asst Prof, Guru Kashi University Talwandi Sabo, Bathinda (PB)

ABSTRACT

Recently, Wireless ad hoc networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Network Early work in MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious. So, this proposed work tries to design and implements GA algorithm with Black hole attack and prevent the system for threat using this DSR protocol.

Keywords: Mobile Ad Hoc Network, Genetic Algorithm, Dynamic Source Routing Protocol

I. INTRODUCTION

The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties [1]. However, similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself. In MANET, security is a challenging issue due to the vulnerabilities that are associated with it [2].

Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks. In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network [3]. As a matter of fact, the boundary of the network is not properly defined. Nodes can intermittently come into the network or leave it. Moreover malicious nodes can flood the network with junk packets hampering the network service or intentionally drop packets. But these nodes can but these nodes can subtly manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious [4].

This paper elaborates the ongoing research on intrusion detection systems for detecting network layer attacks in mobile Ad-hoc networks. Precisely, GA and BFO protocol has been adopted and specifically monitors the vulnerabilities in the network layer. A solution is proposed based on the GA and BFO IDS technique for the detection of vulnerabilities in MANET.

II. RELATED WORK

Dokurer et. al, (2007), investigated the effects of Black Hole attacks on the network performance. We simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network. [8].

Anup Goyal and Chetan Kumar, (2010), has suggested a systematic learning method known as Genetic Algorithm (GA), to identify illegitimate nodes. The algorithm considers the varied features in network connectivity like protocol type, network service to destination and connection status to generate a type based rules. This was experimented by implementing in GA and trained it on the KDD Cup 99 data set to generate rules that can be applied to the IDS to categorize based on the attack types.[5]

K.S. Sujatha et.al (2012) propose a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system is based on Genetic Algorithm, which analyzes the behaviors of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on. The performance of MANET is analyzed based on GAC.[7]

Ahmed Shariff et. al, (2013), showed Mobile Ad-Hoc Networks (MANETs) are 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 purpose of this paper is two folds. First, to present an extensive survey of the known black-hole detection and prevention approaches. Another objective is to present new dimensions for their classification.[6]

III. DSR AND AODV

3.1 AODV

AODV is an on-demand routing protocol used in ad-hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to changes in the link conditions. In case when a link fails, messages are sent only to the affected nodes. With this information, it enables the affected nodes to invalidate all the routes through the failed link. AODV has low memory overhead, builds unicast routes from source to the destination and network utilization is less. There is least routing traffic in the network since routes are built on demand. When two nodes in an ad hoc network wish to establish a connection between each other, it will enable them to build multichip routes.

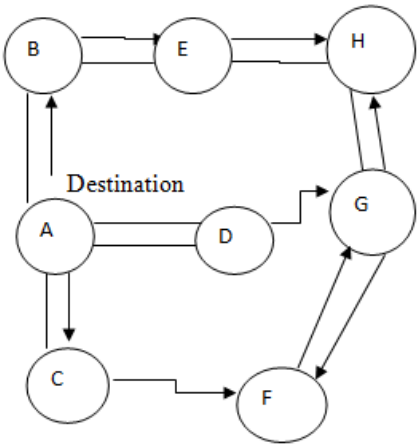

Fig 1.5: AODV Protocol

3.2 DSR

Dynamic Source Routing (DSR) is the very efficient protocol designed mainly for WSN, adhoc networks. Dynamic Source Routing (DSR allows network to be self- organizing as well as self- configured. The DSR contains two terms.

- Route Discovery
- Route Maintenance

Source routing helps to remove loops, packet forwarding etc. It is similar to AODV protocol in which demands are made on requirement. DSR also scales automatically, only when changes are needed. In DSR nodes forwards data packets from one node to another in order to enhance cooperation. AS sequence number is needed at destination, so rich topology is need like mesh, ring etc. Dynamic Source Routing (DSR protocol allows to search source node dynamically in whole network. Each data packet contains header that contains the information of destination as well as routing path. Thus there is no need to update regularly the routing table.

IV. COMPARISON BETWEEN DSR AND AODV

Dynamic Source Routing (DSR) and Ad-Hoc on Demand Distance Vector Routing (AODV) are both routing protocols for wireless mesh/ad hoc networks. Both the protocols employ different mechanisms that result in varied performance levels. DSR and AODV can be compared and evaluated based on the packet delivery ratio, normalized MAC load, normalized routing load, and average end-to-end delay by altering the number of sources, speed, and pause time.

1. DSR has less routing overhead than AODV.
2. AODV has less normalized MAC overhead than DSR.
3. DSR is based on a source routing mechanism whereas AODV uses a combination of DSR and DSDV mechanisms.
4. AODV has better performance than DSR in higher-mobility scenarios.
5. DSR has less frequent route discovery processes than AODV.

V. SIMULATION MODEL

A packet drop attack is also known as black hole attack in the network layer [9]. In black hole attack node drops packets at each step, then high loss of data takes place in the network. The node that drops the packet is malicious node. This attack can be viewed as following:

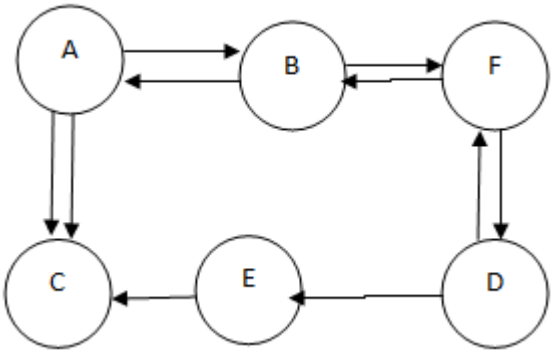

Figure. 1 Black Hole Attack/ Packet Drop Attack

Above figure shows that node A wants to send data to node D. So if node C is the shortest distance path from A to D, then it has to be followed. It will then receive the RREQ message from A node. As soon as node A starts to send the packet the node C drops packet in the middle of the data sending process [10].

Genetic Algorithm is a method of soft computing which uses the laws of selection and evolution. These algorithms are implemented by converting a problem in a particular field into a model a chromosome like structure. In computer network security, it is mainly used to find an optimal solution to a problem. The Genetic Algorithm starts by identifying a data set called population. Then these are individually encoded using bits, characters or integers and they form a chromosome. The next operation on them is an 'Evaluation Function' used to determine the genuine chromosome. During this process, two different operations namely, crossover and mutation are performed which is used to imitate the breeding and evolution. The selection of the chromosome is biased towards the fittest of the species. At last, the fit chromosome is selected once the optimization criterion is met. Below illustrates the basic functionality of Genetic Algorithm.

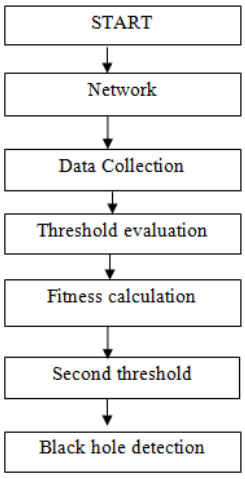

Figure 2 Black Hole Attack/ Packet Drop Attack Proposed Flowchart

The Figure elaborates on the functioning of Genetic Algorithm. The conditions for crossover if selected improperly will lead to the design of an illegal offspring. Hence identifying an optimal solution is not met if the finishing is slow or the convergence is premature. This is determined by means of selection of the fit condition to be either too large or too small.

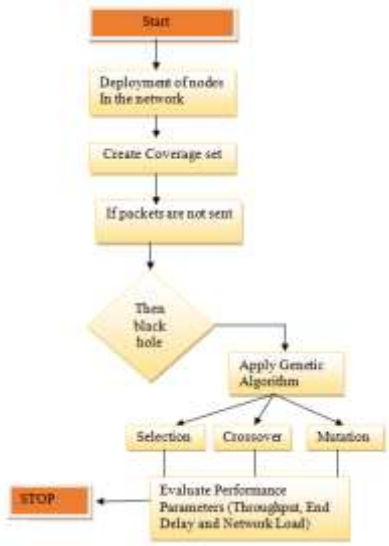

Figure 3 Genetic Algorithms Processing For Black Hole Attack/ Packet Drop Attack

VI. RESULTS AND IMPLEMENTATION

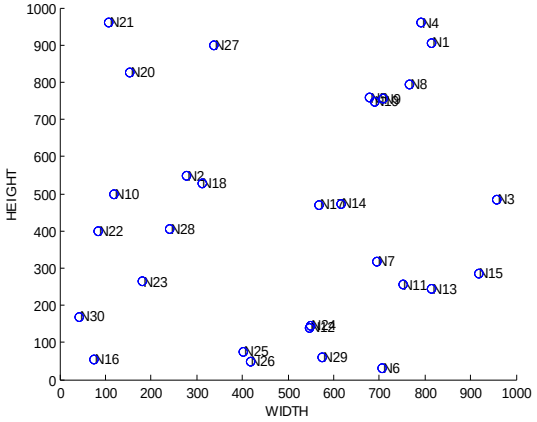

Figure 1 AODV Network

The above figure shows the AODV deployment of the nodes in the network. The area considered in 1000*1000 meters. The deployment of the nodes deals with the x locations and y location of the nodes.

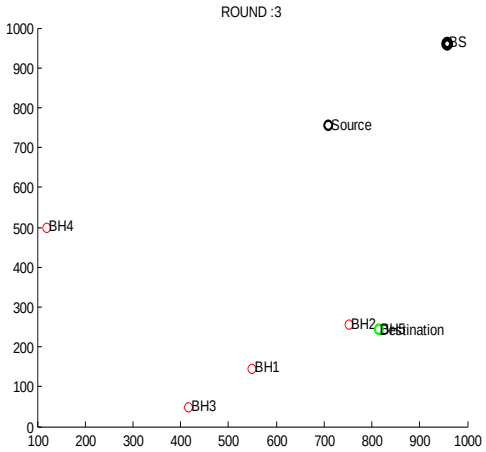

Figure 2 Black Hole Nodes

The above figure shows the black hole nodes at the end of the round because the nodes are the mobile nodes and their positions are changes according to the execution of rounds and the source in black color and destination in the green color is also plotted in the network

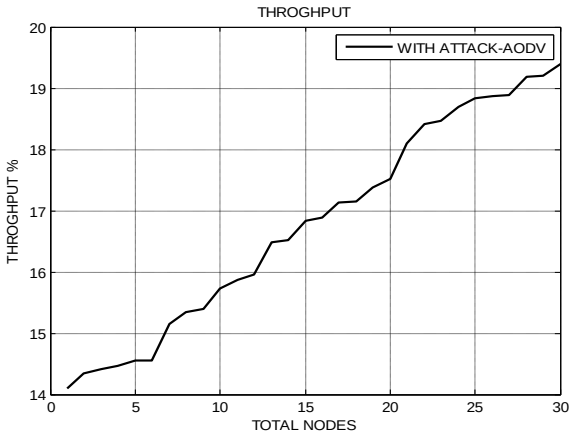

Figure 3 Throughput AODV

The above figure shows the Throughput with black hole attack using AODV and is having near about 19 percent which shows the effect of black hole attack in the overall performance of the network.

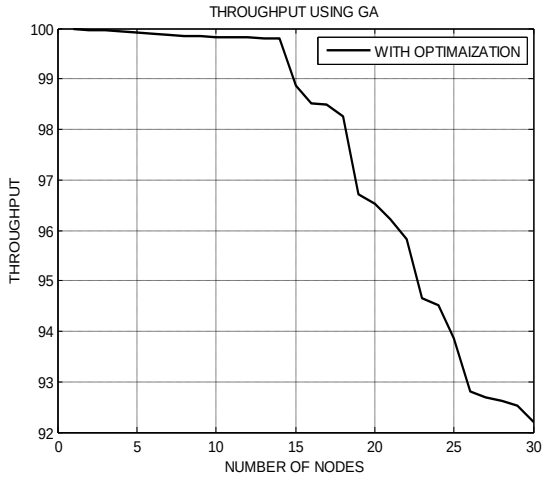

Figure 4 Throughput Using Genetic Approach

The above figure shows the throughput of the network using optimization approach using genetic algorithm which shows the overall performance of the network. This measure should be high for the efficient network. The graph shows the throughput 93.5% which is a sufficient measure to increase network lifetime.

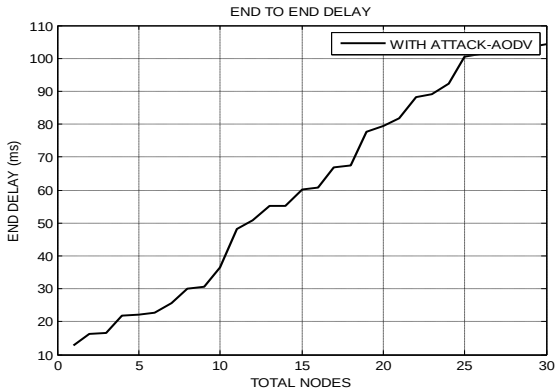

Figure 5 End Delay AODV

The above figure shows the End to end delay in milliseconds which is shows the successfully transmission with the particular time from source to the destination and shows 110 ms end delay to deliver packets from source to the destination

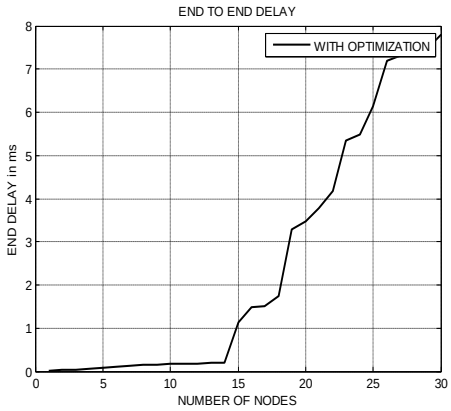

Figure 6 Delay using Genetic Algorithm

The above figure shows the end to end delay using genetic algorithm which is less as compared to the end delay with black hole attack. This measure should be low to successfully delivery of packets at particular time from source to the destination.

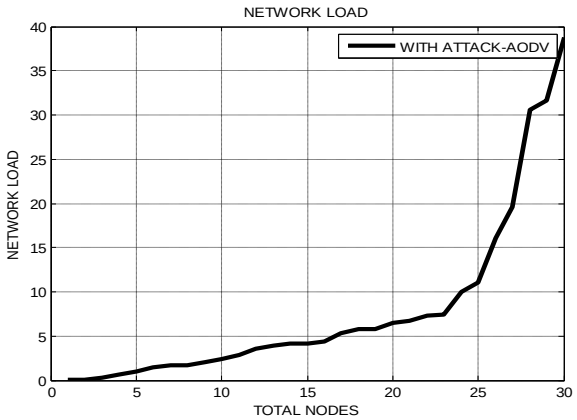

Figure 7 Network load with black hole attack

The above figure shows the black hole attack using AODV protocol in terms of network load which should be low for the efficient performance of the network

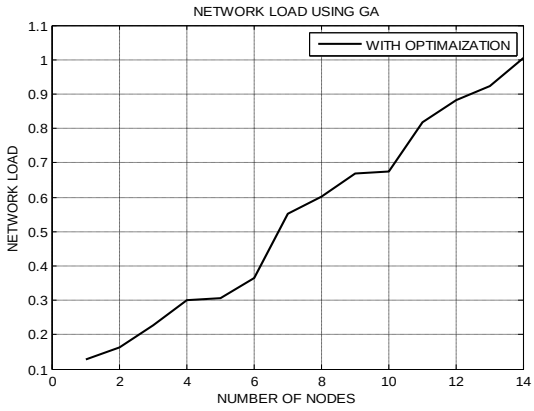

Figure 8 Network Load Using Optimization Approach

The above figure shows the network load using Genetic Algorithm which is used for the optimization and having less network load as compared to the AODV protocol in the presence of the black hole attack.

VII. DSR RESULTS ANALYSIS

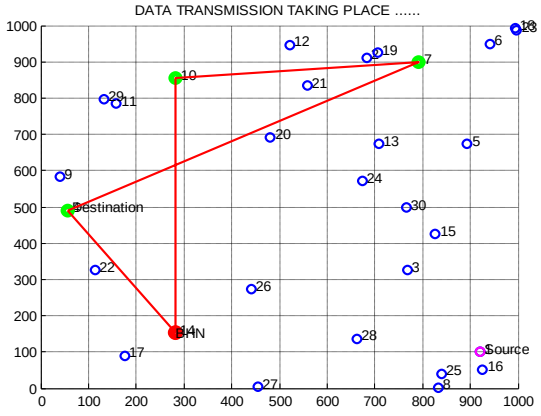

Figure 9 DSR Network

The above figure shows the DSR network architecture with deployment of the nodes in the network with source and destination plotted and transmission of the nodes are shown using black hole node in the network which is shows in red color in the above figure.

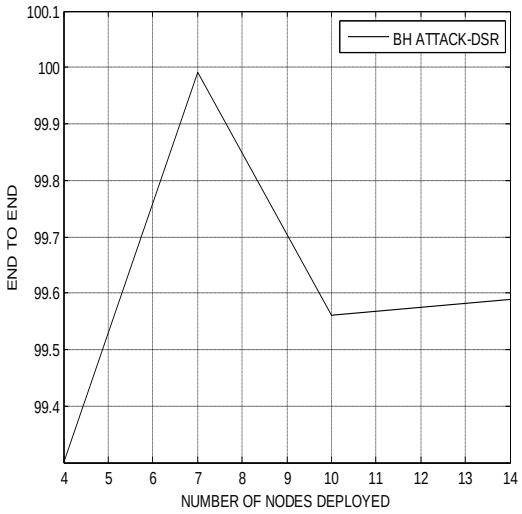

Figure 10 DSR End Delay

The above figure shows the End to end delay of Dynamic source routing in milliseconds which shows the successfully transmission within the particular time from source to the destination and shows 99.6 ms end delay to deliver packets from source to the destination

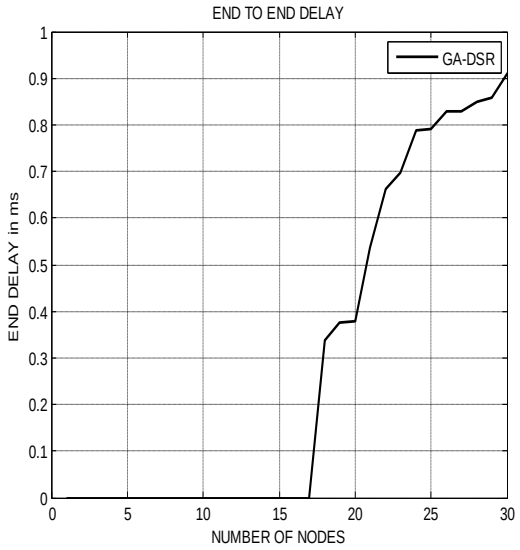

Figure 11 End Delay with Optimization

The above figure shows the end to end delay with optimization using Genetic algorithm and shows that the end delays less as compared to the DSR protocol in the presence of the black hole attack which is 0.9 ms.

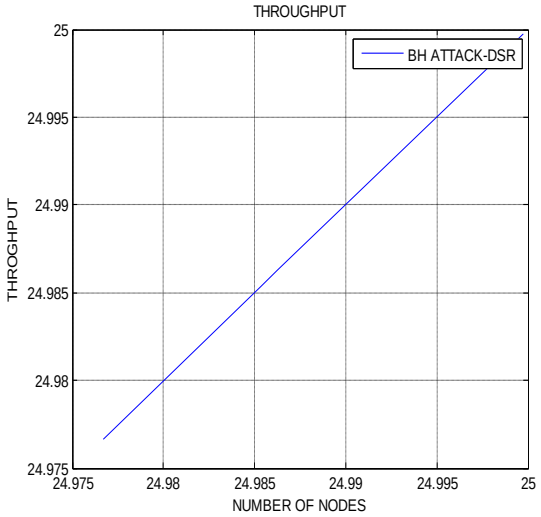

Figure 12 Throughputs with Attack

The above figure shows the throughput performance graph in the presence of the black hole nodes which is very less i.e. 25 % and should be high for the overall performance of the network

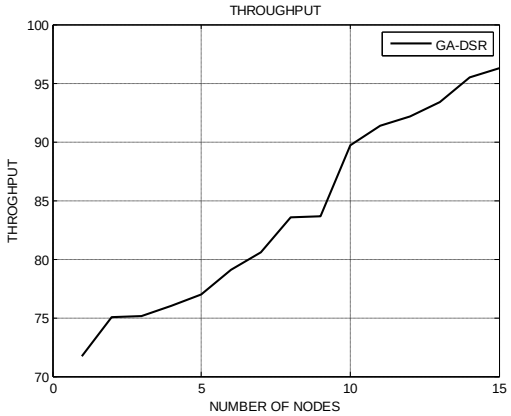

Figure 13 Throughputs with Optimization

The above figure shows the throughput performance graphs with genetic which is 97 % and is high to increase the network lifetime.

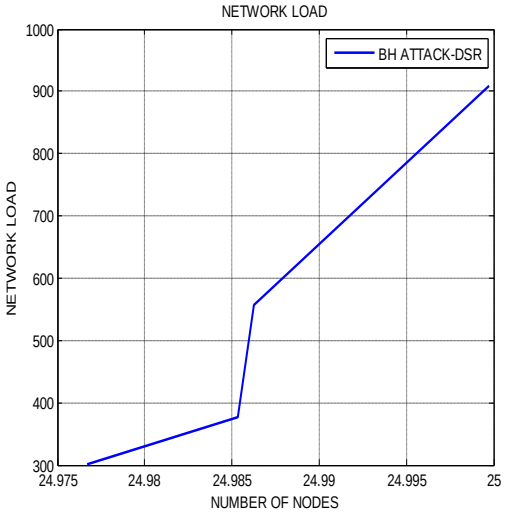

Figure 14 DSR Network Load

The above figure shows the network load in the presence of the black hole attack and is having very high value which degrades the performance of the network

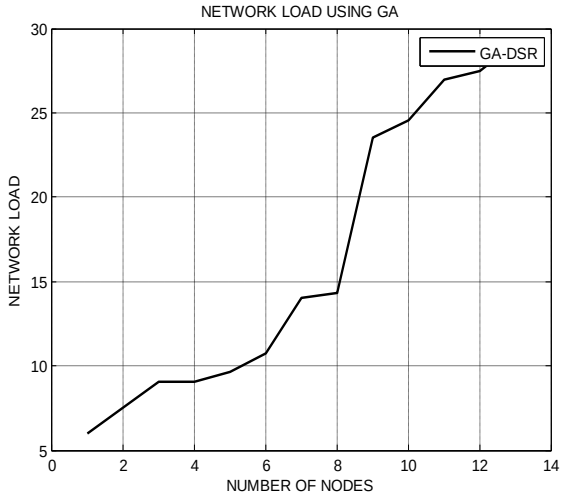

Figure 15 DSR Network Load with GA

The above figure shows the network load with genetic algorithm. Genetic algorithm optimizes the network load which is less as compared to the network load in the presence of the black hole attack.

VIII. CONCLUSION AND FUTURE SCOPE

In this proposal, we have analyzed the effect of black hole attack in the performance of GA. The simulation has been done using the MATLAB. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of network and it can be optimized by using GA optimization algorithm. A hypothetical network was constructed for the simulation purpose and then monitored for a 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 black hole attack in the network exists as a challenging task. As future work, we intend to simulate and analyze the effect of the black hole attack in other routing protocols and we intend to perform the solution for the black hole attack and compare its performance with the AODV protocol and DSR protocol.

REFERENCES

1. Sheenu Sharma and Roopam Gupta, “Simulation Study of Black hole Attack in Mobile Adhoc Networks”, In proceedings of Engineering Science and Technology. 2009.
2. Akansha Saini and Harish Kumar “Effect of Black hole attack on AODV Routing Protocol In MANET” , International Journal of Computer Technology, Volume1, Issue 2,December 2010.
3. Rajib Das, Dr.Bipul Syam Purkayastha and Dr.Pradipto Das “Security Measures for Black hole Attack in MANET: An Apporach” Internationsl Journal of Engineering Science and Technology, 2009.
4. P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.
5. Anup Goyal and Chetan Kumar, “GA-NIDS: A Genetic Algorithm based Intrusion Detection System”, 2010.

6. 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.
7. 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.
8. Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks".Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.
9. Wei Li, "Using Genetic Algorithm for Network Intrusion Detection", 2010.
10. Ganapathy S, Yogesh P and Kannan A "Intelligent agent based intrusion detection system using enhanced multiclass SVM", Hindawi Publishing Corporation, Computational Intelligence and Neuroscience, 2012.
11. Revathi B, Geetha D, „A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of Computer Science and Management Research, Vol 1, no 2, September 2012.
12. Vijayan R, Mareeswari V and Ramakrishna K "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic", International Journal of Research and review in computer science, vol.2 No.3, June 2011.