ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com

# Security Measures for Black Hole Attack and Develop a Intrusion Detection System based Genetic Algorithm in Mobile Ad-Hoc Network

[1]V. Senthil Murugan and [2]Dr. K. Selvakumar

[1]*Research scholar, Dept of Computer Science Engg., Annamalai University, Chidambaram , Tamilnadu , India.*
[2] *Associate Professor, Dept of Computer Science Engg ., Annamalai University, Chidambaram, Tamilnadu, India.*

**ARTICLE INFO**

***Article history:***
*Received 3 October 2015*
*Accepted 31 October 2015*

***Keywords:***
*MANET, AODV, Black Hole Attack, Genetic Algorithm, Fuzzy logic Control, KDD cup 99.*

**ABSTRACT**

A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Routing and security are the main issues for ad hoc networks due to dynamic topology as well as resource constraints. Routing protocol used here is a form of reactive routing called AODV. AODV (Adhoc On Demand Distance Vector) routes based on demand. The feature of AODV is minimum connection setup delay. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack. We Propose a technique to analyze the exposure to attacks in AODV, Black Hole Attack and to develop a Intrusion Detection system is based on Genetic Algorithm, Which analyzes the behaviors of each node and provides information about the attack. The features of AODV such as Request Forwarding Rate, Reply Receive Rate and performance of MANET is performed based on Genetic Algorithm.



**To Cite This Article:** V. Senthil Murugan and Dr. K. Selvakumar., Security Measures for Black Hole Attack and Develop a Intrusion Detection System based Genetic Algorithm in Mobile Ad-Hoc Network. ***Aust. J. Basic & Appl. Sci.,*** *9(33): 26-30, 2015*

## INTRODUCTION

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, every host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient. The communication between the nodes in the MANET is done either directly or through intermediate nodes acting as routers. Thus, the nodes act both as hosts and routers. Due to the limited range of transmission, various nodes may be needed to route a packet to its destination. Owing to the node mobility, the establishment of routing paths is altered by the inclusion and exclusion of nodes. The topology of the network changes rapidly and dynamically. The usage of MANET is augmented in various application environments which don't require any basic infrastructure support.

Any unauthorized access or non permitted attempt to access system or resource information is called intrusion. A device or software application that monitors network or system activities for malicious events is called intrusion detection system. One of these attacks is the Black Hole attack. Black hole attack be an active insider attack. Black hole has two main properties. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets. In this paper, we focus on the effect of Black Hole attack in MANET using AODV routing using Genetic Algorithm.

### *2. Literature Survey:*

Wei Li (2009) has proposed a Genetic Algorithm based intrusion detection system which was tested with TCP/IP networks. This made use of

**Corresponding Author:** V. Senthil Murugan, Research scholar, Dept of Computer Science Engg., Annamalai University, Chidambaram , Tamilnadu , India.
E-mail: senthilkmvs@gmail.com

Australian Journal of Basic and Applied Sciences, 9(33) October 2015, Pages: 26-30

spatial and temporal implementations of network based connections in encoding the network based rules. Anup Goyal et.al (2010) has proposed 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. Ahmed Shariff et. al, (2013) mentioned that 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. Dokurer,S et.al (2007)] has performed the analysis of ad-hoc networks under Black hole attack.

### *3.Introduction to AODV:*

The Ad-Hoc On-Demand Distance Vector routing protocol is a reactive routing protocol. AODV routing protocol uses on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets . In AODV, Route discovery process is initiated by the source node broadcasting a route request message (RREQ) to all its neighbor nodes. The Route request (RREQ) packet contains the following field:

- Source IP address
- Source sequence number,
- Broadcast id
- Destination IP address
- Destination sequence number,
- Next Hop

If the RREQ reaches the destination node or a node that has a route to the destination, the node sends a route reply message (RREP) to the source. If a node cannot satisfy the RREQ, it keeps track of the reverse path setup as well as forward path setup that will accompany the transmission of the eventual RREP . The Route reply (RREP) packet contains the following field:

- Destination IP address
- Source IP address
- Broadcast id
- Expiration time for reverse path route entry
- Source node's sequence number.

In case if a node realizes that the route is damaged or broken it transmits a route error (RERR) message to the source. The simulation of black hole attack in ad hoc wireless is carried out using AODV protocol.

### *4. Proposed Method:*

In this section, the proposed system presents Genetic algorithm based IDS method used to detect the black hole nodes (malicious nodes, misbehaving nodes) specifically the most common network layer hazard, Black Hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. in the mobile ad hoc network (MANET).The proposed system is divided into four modules.

- Attack Description
- Intrusion Detection system (IDS)
- Genetic Algorithm (GA)
- IDS based GA

### *4.1 Attack Description:*

Black hole problem in MANETS is a important security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

In the figure 1, consider a malicious node M. When node 1 broadcasts a RREQ packet; nodes 2, 4 and M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node 5 . Hence, it immediately sends back a false RREP packet, claiming a shortest route to the 1 Receives the RREP from M ahead of the RREP from 2 and 4. Node 1 assumes that the route through M is the shortest route and sends data packets to the destination through it. When the node 1 sends data to M, it absorbs all the data and drops this data . As this data cannot reach to the destination, it is called as a Black hole attack.

### *4.2 Intrusion Detection system (IDS):*

Intrusion Detection Systems (IDS) are designed to monitor a computer or a network to detect and prevent against invalid accessibility. IDS can monitor users, applications, networks, or combinations of the three, in order to detect well-known and unknown attacks. Intrusion Detection System has an major role in computer security, which differentiates an authorized entry from a malicious intrusion. Intrusion Detection Systems are software or hardware products that automate the process of monitoring and analyzing intrusion attempts. The goal of Intrusion Detection System is that to detect attacks and reduce false positives. False positive is when the system allows access to someone who is not authorized. False negative is when the system denies access to someone who is authorized.

Now a days, an organization faces security threats from all sides. All the networks and systems have many known vulnerabilities as described above.

Australian Journal of Basic and Applied Sciences, 9(33) October 2015, Pages: 26-30

Maintaining the security of an organization is getting tougher as more and more sophisticated tools are being developed by intruders which are freely and easily available on internet. Under such scenario, the need for detecting intrusions is of paramount importance.

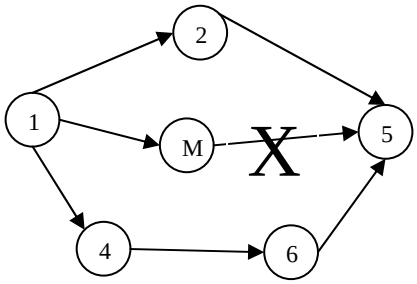


**Fig. 1:** Black-hole attack.

### *4.3 Genetic Algorithm (GA):*

Genetic Algorithm is a soft computing method 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 a best 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 original 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. Fig 2 illustrates the basic working flow of Genetic Algorithm.

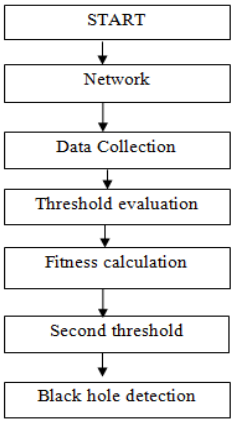


**Fig. 2:** Proposed Architecture.

### *4.4 IDS based GA:*

Genetic Algorithm can be used to concoct elementary principles for traffic in networks. These principles are used to distinguish between genuine connections against malicious ones. The malicious ones refers to the objects with illegitimacy. The rules follow the forthcoming syntax and they are selected only if a particular condition is met.

***If (Condition) then {act}:***

The condition specified in the above syntax is usually a single or multiple network parameters. The algorithm starts initially with the population of nodes. The number of nodes in the base network is varied and hence the initial population is also variable. Then the next step in this IDS is encoding, where the members of the initial population are encoded using binary values and they are called as chromosomes. Each chromosome is then evaluated for an objective function by considering the various network parameters like packet drop (PD), Request Forwarding Rate (RFR) , Request Receive Rate (RRR) etc. Then the threshold is determined by calculating the average of the individual network parameters. Then the fitness criterion for each every network parameter is determined based on Tournament Selection which includes Fitness remapping wherein the fit nodes are assigned '0' values and then the second threshold is determined as the weighted average of the network parameters. Then the surviving black hole nodes are the ones with the value of all the optimal parameters to be zero. Thus these nodes are determined and plotted versus their node identification number.

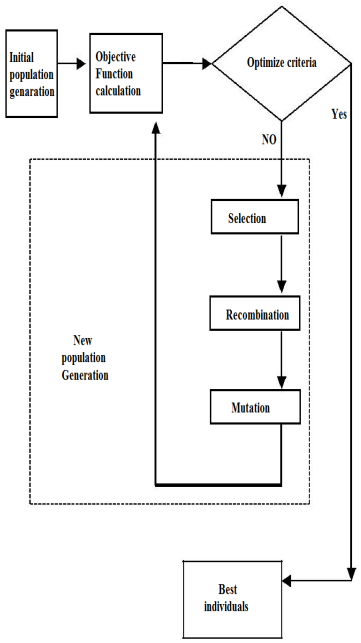


**Fig. 3:** Flow Algorithm of GA.

### *5. The GA Approach:*

The analysis of the Proposed GA based IDS was

analyzed in ns2. The proposed method is as follows wireless networks with 15,25 and 50 nodes were created in ns2. These networks are using AODV routing protocol. Then Black Holes were introduced making appropriate changes in routing protocol. The analysis of performance of the network was done in terms of various network parameters such data received, forwarded and dropped . Then Genetic Algorithm is applied using Fig.4 and by applying the different criterions, the Black Hole node is distinguished from the Genuine nodes. The algorithm of the proposed technique is as follows,

(i) Get the network parameters of the nodes (15, 25,50) in the network.

(ii)Get the parameters like packet drop, request forwarding rate, reply receive rate , node id.

(iii) Calculate the first threshold based on network parameters.-The threshold(TS1) is calculated as follows,

TS1 = Average ( NWPi)

Where, TS1 = First Threshold

NWPi = Network Parameter such as PD, RFR, RRR .

i = 1,2,3….N.

NW= Total no of nodes in the network

(iv) Encode the chromosomes based on threshold criterion. Determine the chromosomes greater than the threshold.

(v) Shortlist the chromosomes based on their fitness.- Calculate the optimum parameters value as follows,

If(NWPi<=TS1) then { NWPi-ov =1} else {NWPi =0}

This results in denoting the corresponding network parameter as either ‘0’ for fit nodes and ‘1’ for unfit ones. Here ‘ov’ represents the optimum value calculation.

(vi) Determine the second threshold.(TS2)-This is done by calculating the weighted average of the individual network parameters of the fit chromosomes.

(vii) Select the remainder based on selection and recombination criteria. – This requires an If loop to determine the node id with all the optimal parameters after the second threshold to be zero. The compatible node becomes the remainder “Black Hole” node and hence the compatible node id is displayed.

### *6. Simulated Results:*

The figure bellow shows the Black Holes detected in a 50 node network. The performance is evaluated based on the following metrics:

*1.* ***Packet Delivery Ratio****:*

It is the ratio of the number of packets received successfully and the total number of packets transmitted.

*2.* ***End to End delay****:*

It is the total time delay taken by the nodes to transmit the data to the receiver.

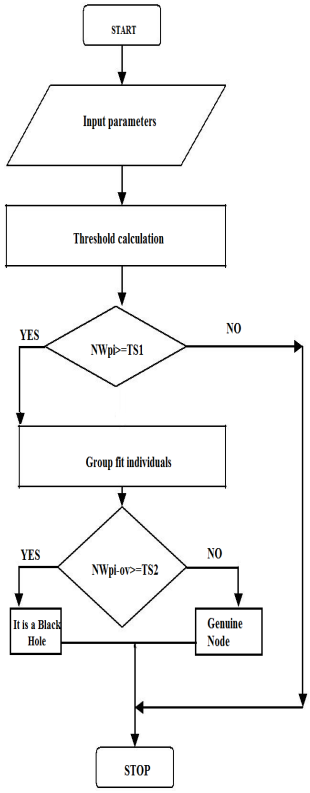


**Fig. 4:** Proposed technique Flow diagram.

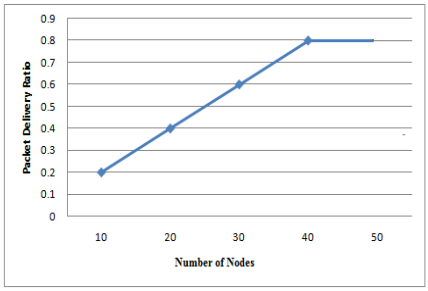


**Fig. 5:** Packet Delivery Ratio in 1 Black hole.

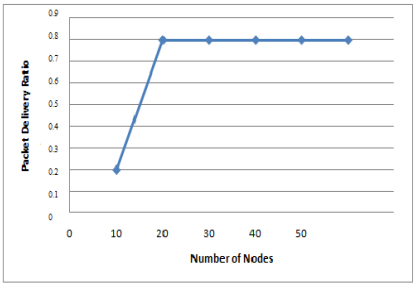


**Fig. 6:** Packet Delivery Ratio in 5 Black holes.

### *7.Conclusions and Future Work:*

In this paper , the issues related to security and loopholes of AODV protocol , has been studied specific to the network layer attacks such as packet drop Attack. An Intrusion Detection System (IDS) is implemented using Genetic Algorithm and tested

with networks of varied node configurations. The algorithm will be tested for more number of nodes and the performance analysis will be done in terms of execution time and efficiency of the algorithm as the node number is increased. This can be extended to DSDV protocol for detecting black hole to avoid routing through the attacker.

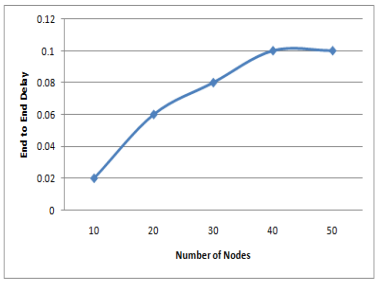


**Fig. 7:** End to End Delay in 1 Black hole.

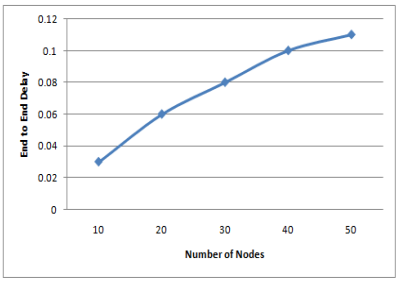


**Fig. 8:** End to End Delay in 5 Black holes.

## REFERENCES

Wei Li, 2010. “Using Genetic Algorithm for Network Intrusion Detection”.

Sheenu Sharma and Roopam Gupta, 2009. “Simulation Study of Black hole Attack in Mobile Adhoc Networks”,In proceedings of Engineering Science and Technology.

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

Akansha Saini and Harish Kumar, 2010. “Effect of Black hole attack on AODV Routing Protocol In MANET” ,International Journal of computer Technology, 1-2.

Perkins, C., E. Belding-Royer and S. Das, 2003. “Ad Hoc On demand Distance Vector (AODV) Routing,”IETF RFC 3561.

Rajib Das, Dr.Bipul Syam Purkayastha and Dr.Pradipto Das, 2009. “Security Measures for Black hole Attack in MANET: An Apporach” International Journal of Engineering Science and Technology.

Michiardi, P., R. Molva, 2002. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks".European Wireless Conference.

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

Bridges, Susan and Rayford B. Vaughn, 2000. “Intrusion Detection Via Fuzzy Data Mining.” In Proceedings of12th Annual Canadian Information Technology Security Symposium, 109-122. Ottawa, Canada.

Ganapathy, S., P. Yogesh and A. Kannan, 2012. “Intelligent agent based intrusion detection system using enhanced multiclass SVM”, Hindawi Publishing Corporation, Computational Intelligence and Neuroscience.

Revathi, B., D. Geetha, 2012. A Survey of Cooperative Black and Gray hole Attack in MANET‟‟, International Journal of Computer Science and Management Research, 1-2.

Vijayan, R., V. Mareeswari and K. Ramakrishna, 2011. “Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic”, International Journal of Research and review in computer science, 2-3.

McHugh, John, 2001. “Intrusion and Intrusion Detection.” Technical Report. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

Dokurer, S., Y.M. Erten, C.E. Acar, 2007. SoutheastCon Journal, “Performance analysis of ad-hoc networks under black hole attacks”.Proceedings IEEE, 22-25: 148 –153.