International Journal of Research in Advent Technology, Vol.3, No.11, November 2015
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Secure Intrusion Detection System in Ad hoc Wireless Network

Shrikant V. Sonekar[1], Dr. Mrs. M. M. Kshirsagar[2], Dr. Mrs. Latish Malik[3]
Research Scholar[1], *Research Guide*[2], *H.O.D*[3]
Department of CSE[1, 2, 3]
G. H. Raisoni College of Engineering, Nagpur[1, 2, 3]
srikantsonekar@gmail.com[1]
manali.kshirsagar@yahoo.com[2]

Abstract— MANET (Wireless Mobile Ad-hoc Network) is a technology which are used in society in daily life an activities such as in traffic surveillance, in building construction or its application is used in battlefield also. In MANET there is no control of any node here is no centralized controller that's why each node has its own routing capability. And each node act as device and its change its connection to other devices. The main problem of today's MANET is a security, because there is no any centralized controller. Our main aim is that we protect them from DDOS attack in terms of flooding through messages, packet drop, end to end delay and energy dropping etc. For that we are applying many techniques for saving energy of nodes and identifying malicious node and types of DDOS attack and in this paper we are discussing this technique.

Keywords— Security, algorithms, denial of attack, intrusion detection system, MANET.

1. Introduction

Mobile ad hoc network (MANET) is a combinations of two or more than two nodes which having a capacity to transfer a data to each other with a centralized system. It is an autonomous system in which nodes are connected using the wireless links in wireless communication and send data to each other. The communication system in MANET, there is no any centralized system (Controller), so the routing is established by itself node. Due to its ability of mobility and self routing there develops much kind of weaknesses in the security of nodal basis analysis. To solve the security issues in the wireless environment, an Intrusion detection system is adopted which is categorized into three models:

1. Signature Based. 2. Anomaly Based. 3. Misuse Anomaly Based.

1.1 Signature Based:-

In the first part of intrusion detection system there are some previously detected signature kinds of patrons which are stored into the data base of the Intrusion detection system if any kind of variations is found in the network by Intrusion detection system it matches it with the previously stored patrons or signature and if it is matched than intrusion detection system immediately comes to know that it has been attacked. But in some cases this is attack on its stored signature cannot be detected by the intrusion detection database system. For this periodic updating of database is compulsory.

1.2 Anomaly Based:-

To solve the previous drawbacks, IDS invented a new system called as anomaly based IDS system. In this IDS first creates a normal profile of the nodes and networks, and keep in the database of IDS and it checks and monitors. If it matches with monitoring profile then it is directly declared as attack. Its benefit is without pre-intimation of attack, it can capture an attack. MANET is also a part of wireless ad hoc network; in this they use routing tables for maintaining a network on a link layer of ad hoc network. This Ad hoc network consists of wireless sensor network and the same problem is also faced in MANET. The sensor network is not so affective because they may be corrupted by the environment and other things and because of this there is less chance of data recovery.

These attacks are applicable in MANET and DDoS also. In wireless network, Intrusion attack can more easily happen when compared to wired attack. In ad hoc network, DOS attack is considered to be very serious. In a DOS attack, a large bulk of data is thrown on a node simultaneously and is coordinated with the attack on the current node of a network. Actually in a DOS attack, one of the available node is captured and guilt node which is attacking the bulk of data on the available node. So much data is stored that it cannot receive any node data. It also captured its bandwidth through this attack.

In Anomaly based IDS, Researcher are detecting the behavior of nodes i.e. whether it is normal or anomalous on the basis of their behavior. Basically the division of any attack is always based on some proper rules or protocol of the system on behalf of the signature or any particular pattern. This attack is exactly opposed of signature based systems. This system can only analyze the attacks for which a signature has been stored in the database. In order to decide & analyze what is attack traffic, the system must be trained to detect normal system activity. This can be completed in different ways. The most occurring technique is an artificial intelligence type. A system also uses neural networks technique with great effect.

Anomaly-based Intrusion Detection has some limitations such as a high false positive rate and the ability to be fooled by a correctly delivered attack. Various attempts have been made to address the relevant issues with the help of many techniques. A wireless intrusion detection system (WIDS) analyzes and detects the radio spectrum in effect of positive assertions of unrecognized users, rogue access points and the use of various wireless attack tools. WIDS system check the network with the help of wireless LAN and if any malicious node is detected then it suddenly send the message alert to system administrator. With the help of MAC address wireless devices is compared and detected.

1.3 Misuse Anomaly Based:-

In Misuse Anomaly Based system (MABS), Sensors are installed and activated inside a private network. Server is hosted in secure & private data centre and is accessible on the Internet. Users can access the MABS Console anywhere using internet. A network implementation is not much secured than a hosted MABS. It is very much secure, because in between server and node, and between node to server console data flow is encrypted. In hosted MABS, sensor is present and it has some small configuration system in network and this sensor is always looking on a network over a secure SSL connection.

In a large organization, small network cannot handle the system. The organization who use large network host MABS. Hosted MABS uses a sensor in a network without special configuration requirement and it is on demand of subscription based software in a service network.

In a network MABS implementation, Server, Sensors and the Console are all placed inside a private network and are not accessible from the internet. Sensors & Server communicate with each other over a private network via private port. Since the Server hosted on the private network, users can allow access to the Console within the private network. A DoS attack normally consist of efforts to temporarily or shortly disturb or deactivate services of a node connected via internet. Perpetrators of DoS normally surrounded with the important sites or services hosted on money landed web servers like banks, credit card payment gateway as Well as with even root name servers. Internet Architecture Board (IBA) is provided some sort of protocol which should not be breakable to the DoS attack. So they are giving proper policy or rules to the all internet service providers, they are applicable to all the nations in the world.

From the above discussion, Researcher have seen that our project is based on Anomaly Based Intrusion System, because the second module which I have created function in the same manner. It also tracks down the attacking node in a flooding stage. And it also gives the information to the other nodes about attacking node what Researcher call as malicious node.

2. ATTACKs ON AD HOC NETWORK

a. Black Hole

In a black hole attack, a malicious node involved makes a fake route in the network and sends to the all the nodes of the network and spreads the message of a shortest path in a network. After receiving this message all the traffic moves on that fake path towards the malicious node with the help of eavesdropping or DoS attack through dropping the received packets.

b. Denial of Service

Denial of service attacks ultimate aim is to disturb the normal network and involve the malicious node in the network. In this technique they use a routing table overflow and sleep deprivation torture. Routing table overflow is a technique in which malicious node is attacks a bulky amount of data on a node in a network for which that node is busy for flooding and leaves the important data in the network. Through sleep deprivation torture attack, targeted nodes battery is totally consumed by this attack.

c. Wormhole

Wormhole is very powerful attack in this two infected nodes communicate with each other and diverts all the traffic of network. for e.g. node A is malicious node which builds a set up with other malicious node of B, in between they set up a tunnel and all the traffic of network is diverted to them.

d. Replay

A replay attack is performed when attacker listening to the conversation or transaction between two nodes and puts important messages like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender.

e. Location Disclosure

In a Location disclosure attack, the attacker targets the requirement of a network. They monitor or send probing messages to the network and searches the place of a targeted node.

f. Distributed Denial of Service

A DDoS attack is same as DoS attack but one of the differences is that in DoS attack performed on one node and DDoS attack is performed on many nodes. All nodes of an network is attacking at a time simultaneously on the targeted node or they send huge amount of data on that targeted node so the targeted node doesn’t have a bandwidth to receive other data and they will skip important information.

3. LITERATURE SURVEY

Prajeet sharma, Niresh sharma, Rajdeep singh. They have introduced types of attack and gave information about MANET and DDoS attacks.[1] The title of the paper is as follows "A Secure intrusion detection system against DDOS attack in Wireless Ad-hoc Network".

Douglas S. J. De Couto, Daniel Aguayo ,John Bicket, Robert Morris "A High Throughput Path Matric for Multi-Hop wireless Routing" This paper presents the expected transmission count metric (ETX), which finds high-throughput paths on multi-hop wireless networks. ETX minimizes the expected total number of packet transmissions (including retransmissions) required to successfully deliver a packet to the ultimate destination.[2]

Christos Douligeris and Aikaterini Mitrokotsa "DDOS Attack and Defence Mechanisms; a classifications". This paper presents the problem of DDoS attacks and develops a classification of DDoS defense systems. Important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined.[3]

ShabanaMehfuz, Doja,M.N introduced "Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs”. In this he proved that Researcher can reject transmissions of control packets and using this Researcher can reduce routing overhead and achieved stability of prominent routes[4].

Ya-an Haung, Wenke Lee provide the "A Co-Operative Detection system For Ad-hoc Network". They have developed the scheme to monitor and detect the traffic pattern to alleviate distributed denial of service attacks [5].

After referring the above papers Researcher are conclude that AODV is good routing protocol for various scenarios with high mobility using numerous genetic algorithm techniques and also conserve energy during transmission. Routing related to WSN is a contrivable task as global addressing mechanism are absent as well as data source from multiple paths to single source with the reason of data redundancy and also because of energy and computation constraints of the network. The traditional routing algorithms are not so effective when applied to WSNs. The performance of the existing routing algorithms for WSNs varies from domain to domain as there are diverse demands of different applications. There is a effective need for improvement of routing techniques that work well across enhanced range of applications.

In brief the routing protocols are divided into two categories first is based on the network structure as well as second is based on protocol operation. The networking structure is as flat network routing, hierarchal network routing and location based routing. The protocol estimation well based on negotiation based, multipath based, query based, QoS based and coherent based routing.

4. PROBLEM DEFINITION

In the Existing System, at present during the time of large traffic the malicious node consume the bandwidth does not allow any other important packet to reach the system and so in the proposed system attempts have been made normal time, Attack time and intrusion detection system module time through simulation modules. Researcher is using genetic-based mechanism and intrusion detection system.

It uses two intrusion detection parameters, packet reception rate (PRR) and inter arrival time (IAT). And Researcher is using AODV routing protocol in all normal module attack module and intrusion detection system for prevention through attack. Minimizing energy needed for data transmission. Improving Energy efficiency in MANET as Well as Ad-Hoc network.

5. RESEARCH METHODOLOGY

a. Formation of Cluster and CH

In this module, Researcher has form a Cluster of nodes and CH. A Cluster formation is done with the help of Cluster formation algorithm and CH formation is done with the help of CH formation algorithm. In Present work part Researcher has discuss on how cluster is form and how CH is selected.

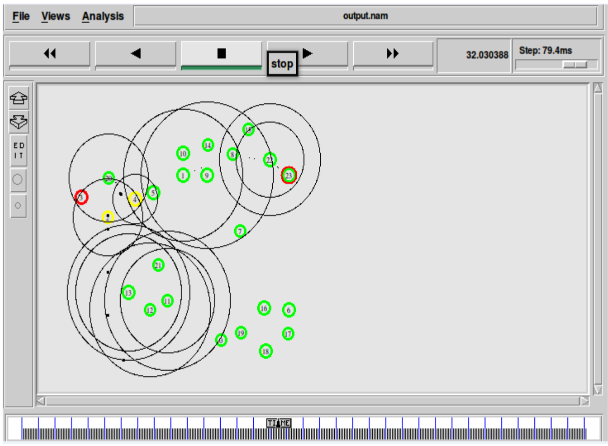


Fig.1 Formation of Cluster.

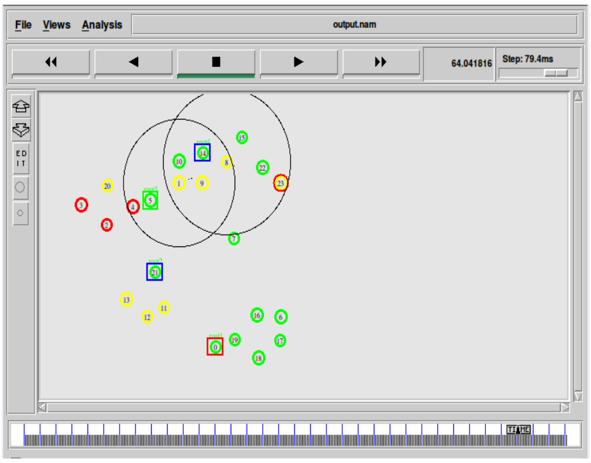


Fig.2 Formation of Cluster Head.

b. Node Energy

In this module, Researcher has calculated the energy of nodes. Researcher has also calculated the initial as well as residual energy of node. Colors of node according to energy of node are also involved in this module. This overall process is performing with the help of Node Energy Algorithm.

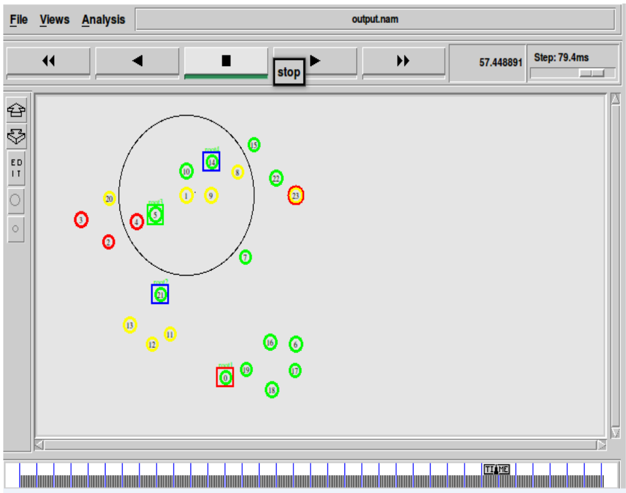
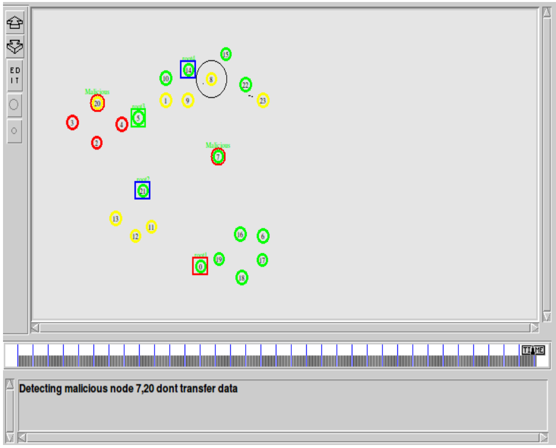


Fig.3 Node Energy

c Detection of Malicious Nodes.

In this module, Researcher has identified the malicious node with the help of some Threshold Parameter. Researcher calculates some parameter and gives some condition. On this result Researcher conclude that the node has malicious. And on the behavior of the malicious node, it also had shown in simulator malicious node do flooding in a communication. All the observation of nodes Researcher concludes that, the flooding nodes and their parameter values are greater than normal nodes. So, it is consider as malicious.



Detecting malicious node 7,20 dont transfer data

Fig.4 Detecting Malicious Node

6. RESULTS

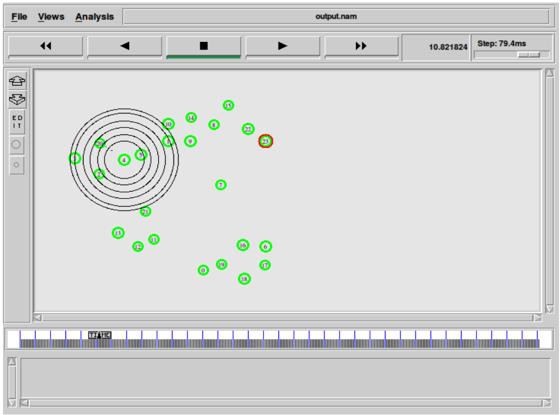


Fig. 5 Communication in nodes

Initially numbers of nodes are created and energy model with node configuration are inserted nodes. Nodes are allowed to communicate with different initial energy modes.

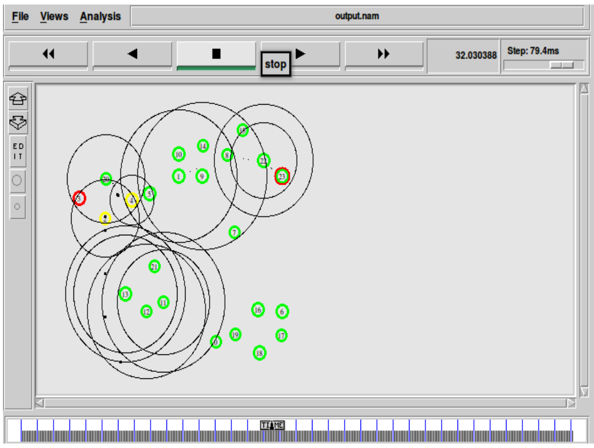


Fig. 6 Broadcasting information among all of nodes

In figure 2 nodes are broadcasting information their residual energy information along with their neighboring node configuration with distance in them. Based on residual energy they change their status

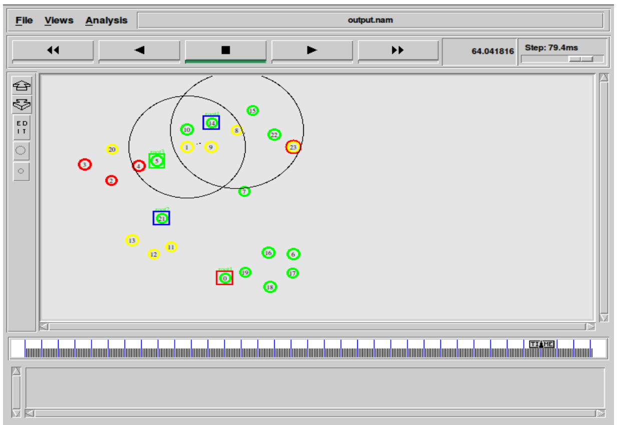


Fig. 7 Forming cluster heads

In the above screenshot the cluster heads are formed with their residual energy mode calculation. Figure 8 shows the residual energy graph against their number of nodes configuration

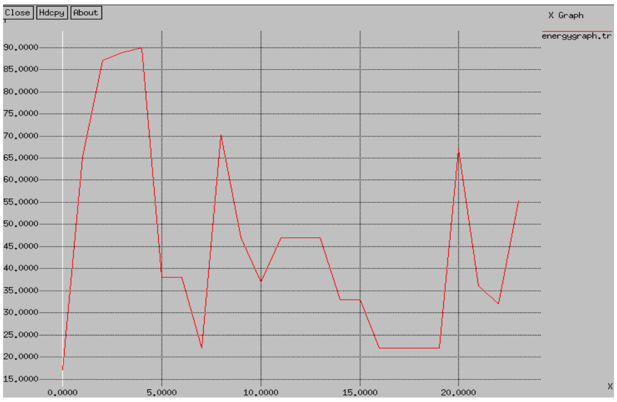


Fig. 8 Residual energy graph against number of nodes

Researcher has work on the efficiency of energy in a project and highlighted their energy through colors. Here Red color indicates node having a lowest energy, Yellow showing average energy and Green color showing a highest energy node in the simulator or in a network. Fig.5. shows all the scenario of energy of nodes.

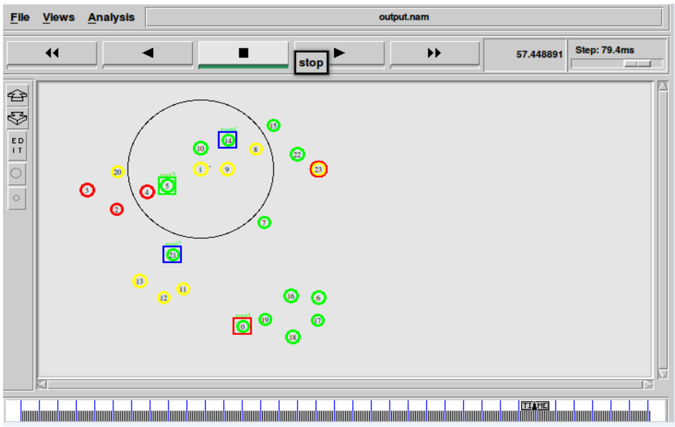


Fig. 9 Scenario of Energy of Nodes.

REFERENCES

[1] Prajeet sharma, Niresh sharma, Rajdeep singh ,A Secure intrusion detection system against DDOS attack in Wireless Ad-hoc Network " International Journal of Computer Applications (0975 – 8887), Volume 41– No.21, March 2012.

[2] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, Robert Morris, "A High Throughput Path Matric for Multi-Hop wireless Routing," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[3] Christos Douligeris and Aikaterini Mitrokotsa, "DDOS Attack and Defence Mechanisms; a classifications", International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008) .

[4] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent PoResearcherr-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008) .

[5] Ya-an Haung, Researchernke Lee : A Co-Operative Detection system For Ad-hoc Network", International Journal of Software Engineering and Its Applications, Vol. 3, No. 6, pp. 24-29 (2010)

[6] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008) .

[7] Song M., and Rajasekaran S., "A Transaction Mapping
Algorithm for Frequent Itemsets Mining," IEEE Transactions On Knowledge And Data Engineering, vol. 18, no. 4, April
2006.

[8] Sanjit Biswas and Robert Morris : "ExOR: Opportunistic MultiHop Routing for Wireless Networks ", IEEE Transactions On Knowledge And Data Engineering, vol. 22, no. 13, May 2010.

[9] X. Tan, B. Bhanu, and Y. Lin, "Fingerprint classification based on learned features," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. 35, 2005, pp. 287-300.

[10] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint classification by directional image partitioning," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 21, 1999, pp. 402-421.

[11] R. Cappelli, M. Ferrara, and D. Maltoni, "Fingerprint indexing based on minutia cylinder-code," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33, 2011, pp. 1051-1057.

[12] R. Cappelli, M. Ferrara, and D. Maio, "Candidate list reduction based on the analysis of fingerprint indexing scores," IEEE Transactions on Information Forensics and Security, Vol. 6, 2011, pp. 1160-1164.

[13] K. C. Leung and C. H. Leung, "Improvement of fingerprint retrieval by a statistical classifier," IEEE Transactions on Information Forensics and Security, Vol. 6, 2011, pp. 59-69.

[14] Lim E., Jiang X., and Yau W., "Fingerprint quality and validity analysis," ICIP, pp. 469-472, 2002.