Intrusion Detection and Prevention in MANET using Artificial Immune System

Ehteshaam Hussain[1], Mohd. Akbar[2]
[1]M.Tech , Final Year, Computer Science and Engineering, Integral University,U.P., India
[2]Assistant Professor, Dept. of Computer Science and Engineering, Integral University, U.P., India
[1]Email: ehteshaamhussain [AT] gmail.com
[2]Email: Akbar [AT] iul.ac.in

Abstract— **In the current scenario everything has become accessible with the growing of technology. If we see earlier we will find that it has been changed significantly. As the technology grows security concerns are being more challenging.**
A mobile ad hoc network (MANET) is a wireless and self-configured network. The node in the network is mobile in nature. So due to mobility in nature it is infrastructure less architecture because they are not stable in term of their positions. And that's why it is also topology less system due to undefined position of nodes in ad hoc network. It is a decentralised network.
In the absence of a permanent topology there are a lot of security concerns. Like there is no any secure physical boundary to define the network area. In the absence of a secure boundary it's vulnerable to different type of malicious attack.
In this paper we are proposing the use of IDS & Artificial Immune System for detection, prevention and self-healing for secure and fault tolerant and reliable system. The Artificial Immune System is originally derived by the biological immune system and now it's a part of artificial system too.

***KeyWords*: MANET, Wireless, Decentralised, Topology, IDS, Artificial Immune System**

I. INTRODUCTION

A mobile ad hoc network (MANET)is also known as wireless ad hoc network [1]
The Mobile Ad Hoc Networks (MANET) has the capacity of self-configuration and they can interconnect by wireless medium. In MANET a network can take place when no. of nodes are connected together.. There is no any centre administration who control this network, its mean it is a decentralized wireless network. We can use wireless technology to access information across the world…services can also be provided where it is not possible to reach physically. Today we are using wireless devices everywhere. It has become a part of our life. Due to wireless network the access of technology and information is available to everywhere and to everyone.
It is a type of ad hoc network that can change its locations and able to configure itself. It use wireless connections to

connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.
Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. Due to their dynamic nature MANETs are typically not very secure, so it is important to be cautious what data is sent over a MANET

II. CHARACTERISTICS OF MANET

I. Dynamic Network Topologies
II. Low Bandwidth:
III. Limited Battery Power
IV. Decentralized Control:
V. Unreliable Communications
VI. Weak Physical Protection:
VII. Scalability

III. ATTACKS

3.*1 Active*

Active attacks are the attacks that are performed by the malicious nodes. Moreover, these nodes consume some energy in order to perform the attacks. Active attacks involve some changes of data or creation of false information. The following attacks come under the category of active attacks:

3.1.1Sink holes

A compromised node tries to attract the data to it, from all neighbouring nodes. The node eavesdrops on all the data that is being communicated among its neighbouring nodes. Sinkhole attacks can also occur on ad hoc networks such as AODV by using techniques like maximizing the sequence number or minimizing the hop count.

3.1.2. Denial of Service

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users

by temporarily or indefinitely disrupting services of a host connected to the Internet. [2] The DOS attacks are performed by flooding some kind of network traffic to the target. This exhausts the processing power of the target and makes the services provided by the target unavailable. The distributed nature of the services makes it impractical. Also, the mobile ad hoc networks are more vulnerable than the wired networks. The interference-prone radio channel and the limited battery power is the reason behind the vulnerability.

3.1.3 Wormhole Attack

Wormhole attacks are severe threats to MANET routing protocols. When the attacker accords packet at a place, and redirects them to another location, routing is disrupted. This occurs because of the redirection. Such mishaps are nomenclature as Wormhole Attack.

3.1.4. Modification

It affects the integrity of data. The attacker alters the packet.

3.1.5. Spoofing

Spoofing occurs when a malicious node pretends as some other node. It does so to alter the vision of the network topology that an innocent node can gather. Spoofing is also called the man in the middle. The attacker achieves this, by showing it's IP as the IP of the node it wants to act as.

3.1.6. Fabrication

Attacks performed by generating false routing information, are fabrication. These are difficult to identify since they come as valid routing constructs, especially in the case of erroneous. They claim that a neighbour can no longer be contacted.

3.1.7. Sybil Attack

The Sybil attack in computer security is an attack in which a reputation system is subverted by forging identities in peer-to-peer networks.[3] When one node impersonates a group of nodes, it is known as Sybil attack. This is a complex attack as a node depends on many intermediate nodes for communication, and so there are redundant algorithms to ensure the delivery of data. However, if a single malicious nodes is able to represent many nodes, it becomes simpler for the attacker. Now, the destination nodes cannot interpret the change in packets. Fake recommendations about the integrity of a certain party can also be delivered, thus attracting more traffic to it.

3.2 PASSIVE

In passive attacks, the routing protocol is not disturbed. Valuable information like node hierarchy and network topology is obtained. The attacker's goal is to obtain information that is being transmitted. Passive attacks are very difficult to identify as they do not involve any modification of data. The following are passive attacks.

3.2.1 Eaves Dropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their permission.[4] The goal of eavesdropping is to obtain some confidential information during communication. The confidential information may include the location, public key, private key or even passwords of the nodes. It is crucial that such data are kept hidden from unauthorized people.

3.2.2. Traffic Analysis

In this attack, the attacker scrutinizes the traffic, determine the location, discover communicating hosts, and detect the frequency and length of message being exchanged. These information are used to predict the nature of communication. All incoming and outgoing traffic of network is not altered.

3*.2.3. Monitoring*

The nodes are monitored. The packet transactions and other activities of the nodes are verified and audited

IV. PROPOSED WORK

To detect the intrusion in a mobile Ad- Hoc network we are using pattern matching. The pattern matching will be based on the predefined parameter of a node in An Artificial immune system algorithm.

4.1 Native Search

We are using Native-Search (N[ ])to decide that a node has all the attributes of a healthy or not.

ALGORITHM

Native _Search (N [ ], F [ ])
F [1……m] –features
1. For i ← 0 to m
do
2. K ← 0
3. While K,m& F [K]= N [i+k] do
4. K K+1
5. If k = m
Return i. " Match"
Else
Return -1

Here in this algorithm F[ ] is the features of a healthy node. K is constant. N [ ] is the features of any node.

If all the attributes that is necessary for a healthy node are confirmed then communication process will be continue for further communication.
If any feature is found missing after Native - search Iteration then an AIS approach will be apply to this node.
In AIS approach we have to see the no. of missing features. If it is more than half according to algorithm then this node will be not recover, otherwise it can be recover by adding missing features .
In such a way the process will be continue.

4.2 AIS Algorithm

1. MF [ ] length of (N [ ])
2. for I = 0 to length (F)
If F [i] ≠ MF [i]
Then
MF[ ] ← F [i] – Nf. Length
If MF [I] > F [i]/ 2
Return " Not recover"
Else NF [i] ← F [i] – MF [i]
Return " recover"
Where M is the missing feature of any node

4.3 Implementation

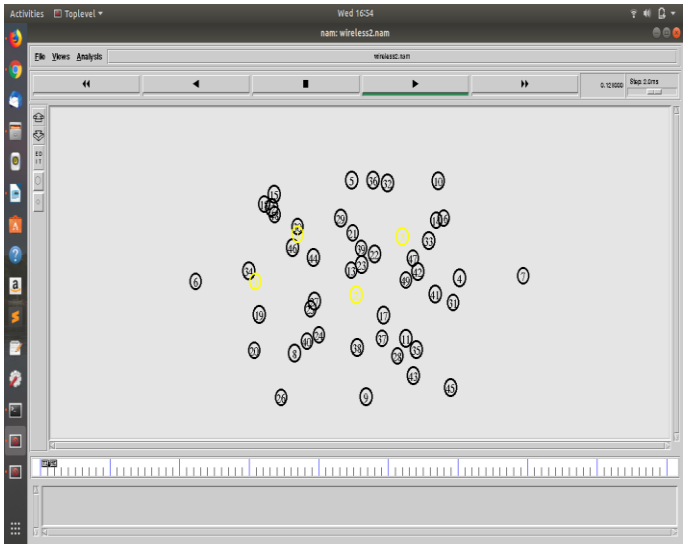

Fig -1: Pattern matching and detection of malicious nodes (Yellow Nodes)

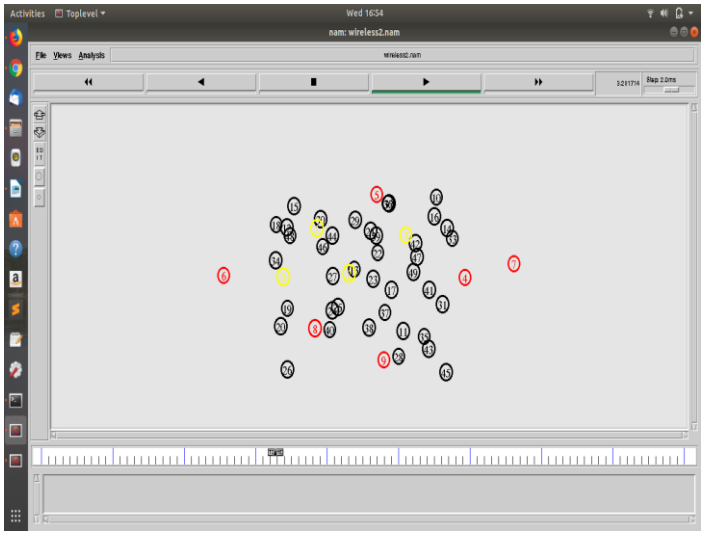

Fig -2 Detection of the nodes that cannot be recovered (RED NODES)

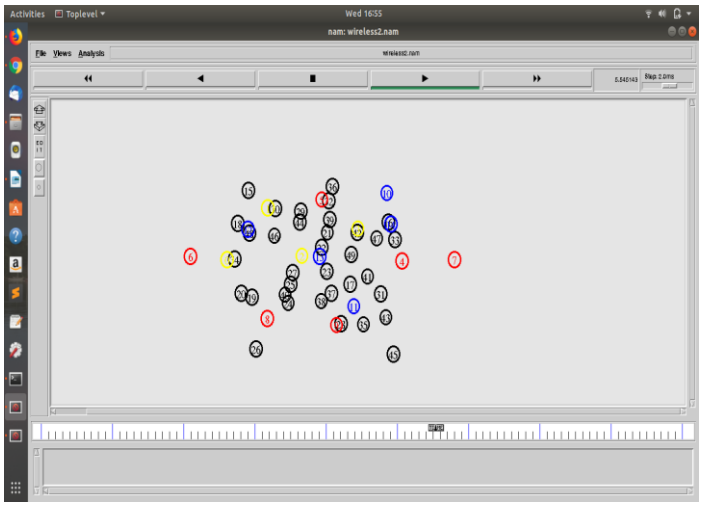

Fig -3 Recovered Nodes with the help of Artificial Immune System Algorithm (Blue Nodes)

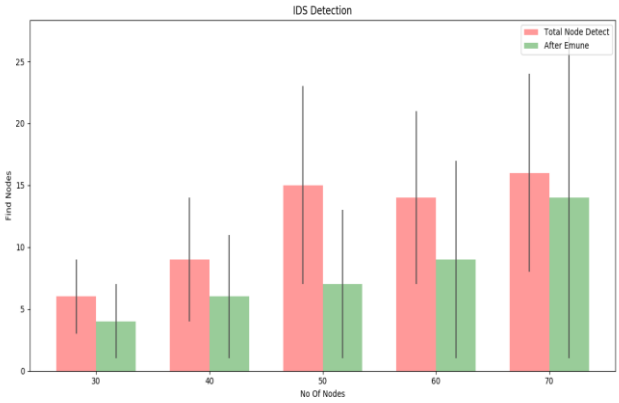

Fig -4 Total Nodes (Pink) and recovered Nodes (Green) comparison.

V. CONCLUSIONS

As we know the security is a major concern in an Ad- Hoc network and there are different strategies to cope with it.
In this research work we have presented an approach for detection of intrusion as well as a way for the recovery of the infected nodes with the help of Artificial Immune System.
For this purpose a virtual environment was created with the help of Network Simulator Tool "NS2" on Linux platform and a pattern matching approach was applied between a healthy node and a victim node.
With the help of a predefined health parameter in AIS , we find out the missing parameter or features of a victim node, that is necessary for a reliable communication with in network and then these features will be added in that node.
In this approach we have gain success to recover those nodes who have infected more than 50%.
In our future work we will try to recover those nodes who are infected more than fifty percent.

VI. REFERENCES

[1] Trifa, Zied; Khemakhem, Maher (2014). "Sybil Nodes as a Mitigation Strategy Against Sybil Attack". Procedia Computer Science. 32: 1135–40. doi:10.1016/j.procs.2014.05.544.

[2] Garner, p. 550[full citation needed]

[3] 1997. ISBN 9780792398226 Wireless ATM & Ad Hoc Networks. Kluwer Academic Press

[4] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.