ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.2

Intrusion Detection System using Mobile Ad-Hoc Network

V.R.Shashanthini
Department of CSE
RAAK College of Engineeering and Technology, India

Abstract:
MANET is very popular and efficient, easy and secure way of communication between two or more mobile user ends and we can send and receive data, information, updates and signals from one end to another known end securely by using Novel Intrusion Detection System technique and by blocking unknown nodes in MANET.In this paper ,implementation of Security in wireless mobile ad-hoc network by using Novel Intrusion Detection System in Aodv routing protocolis is shown. Aodv routing protocol is a distance vector routing protocol used for better performance, we are implementing the method of Intrusion Detection System, which is based on the principle of network, nodes or information misuse detection system, which can accurately compare the signatures of known attacks and has a low rate of packet dropout's alarms. We are bounding wireless mobile ad-hoc network nodes to getting updates from unknown or unwanted nodes on the same network through routing table; we are using a Novel intrusion detection technique with the help of routing protocols in MANET (mobile ad hoc network).

Keywords: Intrusion Detection System, MANET (Mobile ad-hoc network).

1. INTRODUCTION

Mobile ad-hoc network is an autonomous collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. Each node is free to move about arbitrarily.It is often said to be the "Stand Alone Network".

2. CHARACTERISTICS OF MANET:

1. Dynamic network topology configuration(Node can be moved anywhere).
2. Limited bandwidth power constraints for each operation(Link on a wireless networks tend to have low capacity than wired networks).
3. Low overheads.
4. Ability to handle packet loss.
5. Autonomy(Each node in MANET calculates its own route path that will be selected sequentially).

3. PARTS OF MANET:

The MANET network layer has two parts, namely the network layer and the transport layer.In the network layer of MANET is the IP (Internet protocol) and the ad hoc routing layer uses the AODV protocol (ad hoc on demand distance vector) This Wireless is a new technology that allows users to access information and services in spite of the geographic position. Now a day's people can easily access the things whenever and whatever they want from this technology. In general, wireless network are of two types: Infrastructure network and ad hoc network. Mobile ad hoc network (MANET) [3] is an autonomous group of mobile users who communicate with each other without any fixed infrastructure and centralized administration. Since the hosts are mobile, the network topology may change rapidly and unpredictably over time. Wireless Ad-hoc network is less secure network and open network to every node or intruder. Any node can easily get connected to our wireless mobile ad-hoc network and get updates. That's why we consider wireless ad-hoc network less secure and open network, wireless ad-hoc network does not require any physical topology or cabling media for communication. So it is important to secure this network from outsiders.

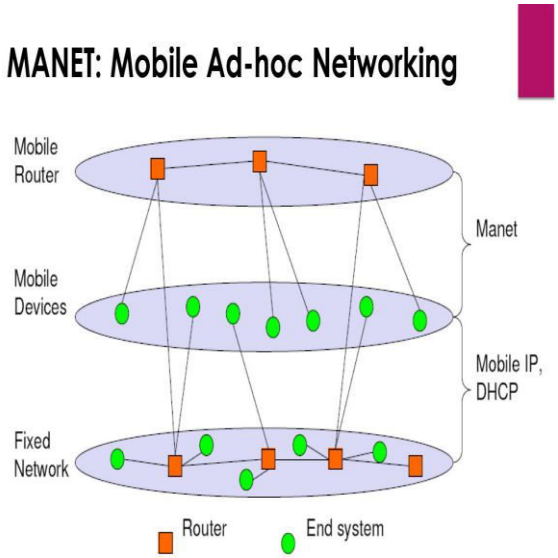


Figure.1. Infrastructure of MANET

4. LITERATURE SURVEY:

Existing surveys conclude that:
1. AODV is being implemented and modified under multimetrics.

2.The most predominant factor is the HOP COUNT which measures the number of Hops between the source and destination paths.

Example:
Initialize a first message, say "HI"
If a node didn't succeed to receive several HI messages from a neighbor, a link break arises

5. PROPOSED WORK:
Intrusion Detection System is purely based on the principle of network. Nodes or information misuse detection system can accurately compare the signatures of known attacks and has a low rate of packet dropout's alarms. In Our paper work we

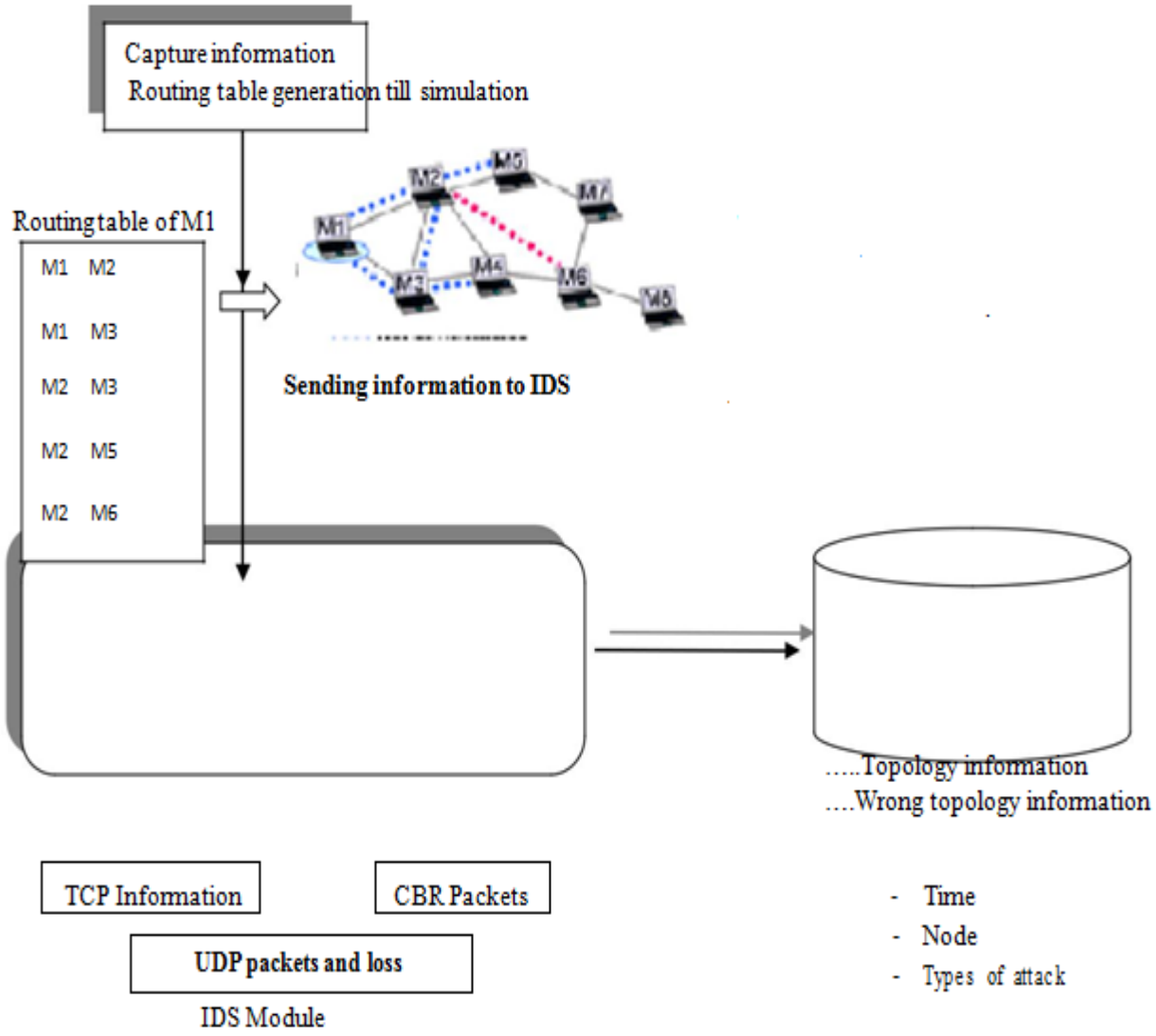


Figure.2. Novel Intrusion Detection system topology

Have focused on Ad-hoc on demand distance vector routing protocols, which are extensively used and trouble-free to implement. The general move towards taken at the same time as effectively implementing the scheme for AODV routing protocol which allows us to integrate it in several other MANET [4] routing protocol.

6. PROPOSED SOLUTION:

A.PARAMETERS INVOLVED:

1. **PDR (Packet Delivery Ratio)**: - It refers to the number of delivered data packets to the node. Higher the PDR, better is the performance

PDR= (Number of Packet's Transmitted)/ (Total Number of Incoming Packets)

2. **Control overhead**: It refers to the ratio of number of Control packets transmitted to the total number of data packets.

CO = (Number of Control Packet's Transmitted)/ (Total Number of Packets)

3. **PMIR (Packet Misroute Rate)**:A Misroute Data Packet is one which has been sent from a node to a wrong destination. PMIR is the ratio of number of misroute packet is delivered to the transmitted packets.

PMIR= (Number of Packet's Misrouted)/ (Total Number of Packets delivered)

In our paper work of the Novel intrusion detection system is included , it detects the misincident happens in the network, in our component we analyze the outcome from first to last number

of misincident comes on the network and after that after an Intrusion detection system we protect through miss incident.

B.ALGORITHM FOR SECURITY IN WIRELESS MOBILE AD-HOC NETWORK USING NOVEL INTRUSION DETECTION SYSTEM AND MAINTAINING TTL (TIME TO LEAVE) SYSTEM

I. Initialization

```
Set TTL_START = 5
Set TTL_THRESHOLD = 7
Set TTL_INCREMENT = 2
Set NETWORK_DIAMETER = 30
```

II. Calculation of TTL Time

```
rt->rt_req_last_ttl = max(rt->rt_req_last_ttl,rt->rt_last_hop_count);
```

III. Check Whether TTL is zero or not

```
if (0 == rt->rt_req_last_ttl) {
// first time query broadcast
   ih->ttl_ = TTL_START;}
else {
```

IV. Expanding ring search

```
if (rt->rt_req_last_ttl < TTL_THRESHOLD) ih->ttl_ = rt->rt_req_last_ttl + TTL_INCREMENT;
else {
```

V. Network-wide broadcast

```
   ih->ttl_ = NETWORK_DIAMETER; rt->rt_req_cnt += 1;
        }
}
```

C.ROLE OF INTRUSION DETECTION SYSTEM

1) Intrusion detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization

2) An intrusion-detection system (IDS) [9] can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity

Misuse Based Intrusion Detection Systems

1) Misuse based IDSs operate based on a database of known attack signatures and system vulnerabilities

AODV protocol based IDS

1) Intrusion detection and response model (IDRM) to enhance security in the **Ad Hoc on Demand Distance Vector (AODV**) routing protocol.

Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms

1) TIARA is a set of design techniques that strengthen MANETs against DoS attacks [5].

7. SIMULATIONS AND RESULTS:

We use NS3 as the simulation platform, and table I lists the parameters used in the simulation scenarios. We use three parameters PDER, CO and PMIR [7] to evaluate the correctness and efficiency of the behavior scheme. Overall, the research can be alienated into two phases - Behavior stage and classification stage. In behavior stage collect the behavior of every node through the simulation. After this pass to this behavior in the NS3[8] if the node cross the threshold limit they detect as a flooded node.

A) Result After Implementing Novel Intrusion Detection System And Maintaining Ttl (Time To Leave) System

We use NS-3 simulation platform and table 1 lists the parameter we used in this, we can use the following parameters PDER, CO, PMIR to evaluate the performance and efficiency of nodes. We have been doing research in two phases – Behavior phase and Classification phase .In the behavior stage we can collect the behavior of each and every node by simulation. After doing the behavior phase, we can check this behavior in the Novel intrusion detection system, which can detect the node that is unwanted or malicious.

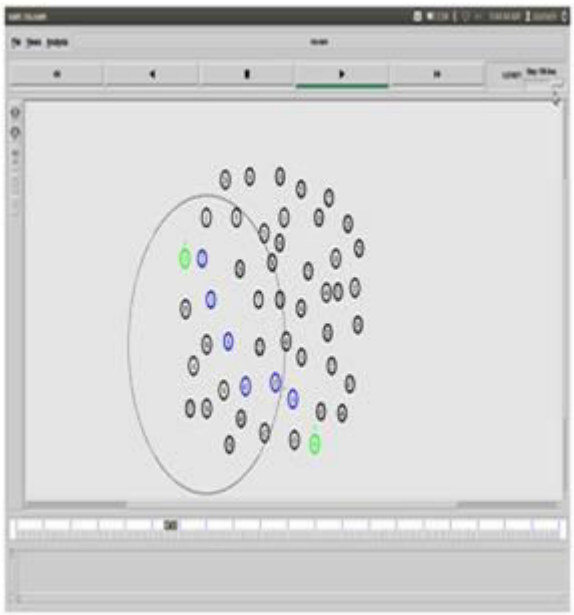
Table 1. Simulation parameters

Simulation Parameter	Value
Simulator	NS-3(v-3.14)
Protocol	AODV
Simulation time	100 seconds
Number of Nodes	70,80,90,100,120
Transmission Range	200m
Traffic Type	UDP
Simulation Area(m*m)	800*800

Here we compare the performance of different nodes and analyze the performance of the network after detection of unwanted and malicious nodes and also calculate the time of travelling of packets from one node to the other. we can calculate the threshold value which doesn't cross the limit that means it is flooded as soon as by Intrusion detection system .We can find out the malicious and unwanted node so we can prevent as well as detect the unknown attackers.

Table.2.Ids Nodes Detected By Ns3

No. of Nodes	Flooded nodes (by IDS in SVM)	IDS(intrusion detection system using NS3)
70	1	2
80	2	4
90	1	2
100	1	3
120	5	8

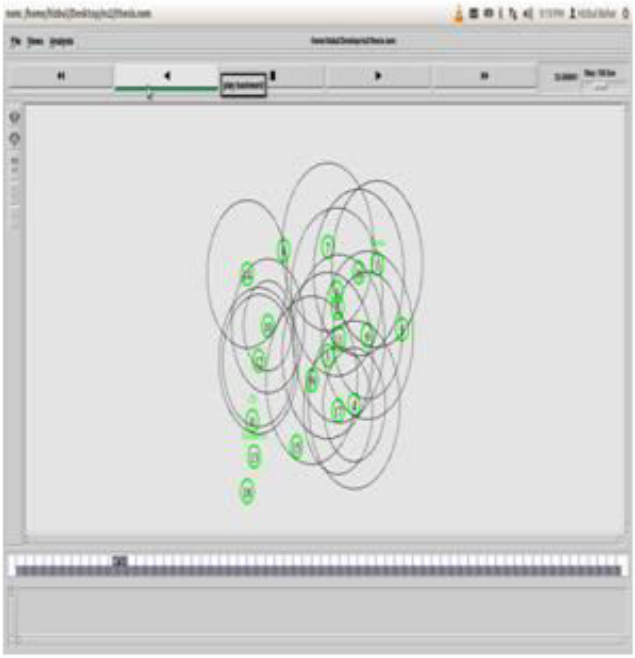


A. Previous result

The above table shows the total number of Intruder nodes in a given set of input nodes.It can compare the previous paper results to our results.

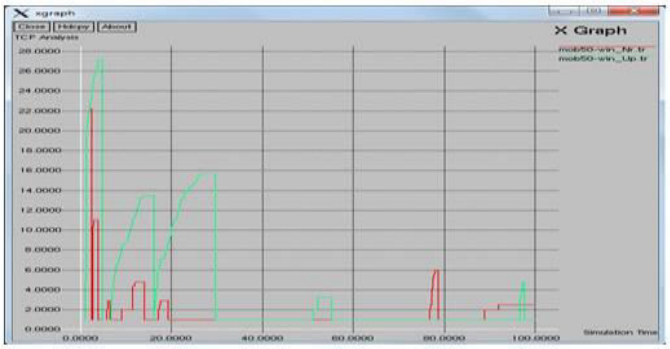
Overall Summary

SEND = 8405.00 pckts
RECV = 6050.00 pckts
ROUTING PKTS = 8144.00
PDF = 71.98
NRL = 1.35
AVERAGE E-E DELAY (MS) = 614.28ns
NO. OF DROPPED DATA (PACKETS) = 2277pckts NO. OF DROPPED DATA (BYTES) = 2325100 bytes



B. Updated result

We can see that nodes behavior the blue color nodes are malicious as it detected by previous method and prevented also but it cannot calculate the time of travelling of packets from one node to another .After implementing TTL field to that result, we can see in updating result, that there is no malicious node in it which shown by blue col



AODV ROUTING WITHOUT TTL FIELD USING SVM

8. CONCLUSION

Routing Protocols of Mobile Ad-hoc network are very useful and played a very important role in wireless Mobile Ad-hoc network Intrusion detection system after implementing above mentioned new algorithm for the Intrusion detection system, we can block or restrict unknown nodes from attacks and can establish a secure ad-hoc network and for result and coding we used Network Simulator 3 [8] software for getting better result and performance. We have also worked in TTL fields in MANET and we have implemented a Security in wireless mobile ad-hoc network using Novel Intrusion Detection System.

9. REFERENCES

[1]. V.D. Park, and M. S.Corson "A Highly Adaptive Distributed Routing Algorithm for Mobile WirelessNetworks", Proc. INFOCOM '97, April 1997

[2]. Alokparna Bandyopadhyay1, Satyanarayana Vuppala2, “A Simulation Analysis of Flooding Attack in MANET using NS-3” IEEE 2011

[3].Meenakshi Patel, Sanjay Sharma, “Detection of Malicious Attack in MANET A Behavioral Approach”, IEEE 2012

[4].Prasenjit Choudhury, Subrata Nandi, Anita Pal, Narayan C. Debnath, “Mitigating Route Request Flooding Attack in MANET using Node Reputation”, IEEE 2012.

[5]. S. Kanan, T. Kaliakikumaran, S. Karthik and V.P Arunachalam, ”A Review on Attack Prevention Method in MANET” Journal of Modern Mathematics and Statistics Year 2011/Volume :5 /Issues : 1 /Page no. 37-42.