Simulation of Intrusion Prevention System

S.S.CHOPADE[†] and Prof. Nitiket N.Mhala[††]

[†]DMIETR,Wardha,M.S.,India
[††]H.O.D. of Electronics Engg, Bapurao Deshmukh COE, Sevagram,Wardha,M.S.,India

ABSTRACT
The security of data becomes more important with the increased use of commercial application over wireless network environments; there were several problems of security in wireless networks due to different types of attack and intruders. There were better methods an intruding handling procedure available for fixed networks. But it was difficult to analyze attacks in the mobile ad-hoc environments. The reason is that there is no central point to control all the activities in the network and dynamically changing network topology and behavior and limited power level of mobile devices, attacked by intruders because unauthorized use of wireless network so that the whole network will be suffered from packet loses. With the help of intrusion detection system we detect attack after when attacker affect the network; we presented an approach to handle such type of internal attacks for wireless network from the beginning though attack is present in the network but because of our prevention system that attack not affect the network.. We report our progress in developing intrusion prevention capabilities for MANET with the use of CBR interval. The proposed work can be performed by modifying ad-hoc on demand distance vector routing protocol. The simulation experiments are conducted on NS-2 environment in Linux platform.

Keywords
MANET, CBR, INTRUSION PREVENTION SYSTEM.

1. Introduction

A MANET (Mobile Ad-hoc Networks) is an autonomous system of mobile nodes connected by wireless links. In MANET, each mobile node functions as both a host and a router. The MANET does not require any fix infrastructure such as base station. In recent years, with the rapid enhancement of wireless devices e.g. mobile laptops, computers, PDA and wireless telephone, the potential and importance of mobile ad-hoc networking has become apparent. Basically ad-hoc networks are temporary in nature. It usually has a group of stations communicating with each other and can be formed spontaneously.
Among all the research issues, security in mobile ad-hoc routing protocols is particularly challenging due to the nature of wireless communication and the lack of infrastructure supports. Several efforts (e.g., Security-aware AODV, ARAN, SRP, SEAD, CONFIDANT, Watchdog and Path rater) are underway to provide security services in ad-hoc routing protocols
In wireless network, with the help of intrusion detection system we can detect the attack and after we remove the attack by isolating the intruder from the topology and thus we will get a safe communication in the wireless network .but we are progressing our report by doing simulation of intrusion prevention system with the help of IPS we can prevent the network from the beginning though the number of attack was present in the network.
The proposed wireless intrusion detection system has been simulated using ns-2.29 environmental in Linux platform.

2. Related Network

[1] "An Approach for detecting attacks in mobile adhoc networks"by V.Madhu Viswanatham and A.A.Chari,AP,India
[2]"Evaluation of Wireless Sensor Network Simulators" by Miloš Jevtic, Nikola Zogovic, and Goran Dimic Serbia, Belgrade, November 24-26, 2009.
[3]ns-2 Tutorial Exercise ,Multimedia Networking Group, The Department of Computer Science,UVA Jianping Wang
[4]Nils Aschenbruck researched a project called MITE which funded by German armed forces. A distributed intrusion detection system for tactical MANETS has been developed.
[5]Nachiket R. Potlapally's work focuses on one important constraint of several devices battery life and examines how it is impacted by the use for various security mechanisms. He has studied the energy consumption requirement of the most popular transport - layer security protocol; secure socket layers. (SSL)
[6]Yu-Xi Lim, [6] member from IEEE studies an off the shelf wireless access point was modified by downloading a new lines operating system with non-standard wireless access point functionality in order to implement a wireless intrusion detection system that has the ability to actively respond to identified threats. Increasing no of organizations are deploying wireless networks, mostly utilizing the IEEE 802.11 b protocol.

Manuscript received September 5, 2011
Manuscript revised September 20, 2011

[7]S. Basagni. [8] Distributed clustering for ad hoc networks. In ISPAN-99, International Symposium on Parallel Architectures, Algorithms, and Networks

3. Intrusion Prevention System

Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking resources. Intrusion detection systems are widely used in wire network to protect network system. This intrusion detection techniques can not applied directly to wireless network. However, this wireless network has some disadvantages that there is no central point to control all the activities in the network; dynamically changing network topology and behavior limited power level of mobile devices

So there is a problem of security in wireless network. Hence, there is a need for efficient wireless network technology to provide safe network accesses to users and also the efficient wireless intrusion detection and prevention system that not only detects different possible attack but also to recover from them. we are progressing our report by doing simulation of intrusion prevention system. With the help of IPS we can prevent the network from the beginning though the number of attack was present in the network.

This section gives an overview of intrusion detection system-The main design goal is:

1) Though the attack is present in the network it will not affect the network

2)To propose a method for preventing network from attacks in MANET.

This work can be performed by modifying ad-hoc on demand distant vector protocol (AODV). The AODV routing protocol is one of several published reactive routing protocols for mobile ad-hoc networks, and is currently extensively researched. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source.

The overall system design includes different nodes. Each node can communicate with each other randomly and also based on communication range. The transfer of packets among different nodes could be easily visualized under the simulation environment. For each traffic flow a source/destination pair is randomly selected from the node set. Every nodes can move arbitrarily, the network topology from time to time at the communication links between mobile nodes break frequently.

As an example we are introducing the three attacks that is Node isolation, route disruption, Resource consumption. This attack is present in the network and detected by detection engine and in prevention engine we are trying to develop though this attack is present in the network but it will not affect the network.

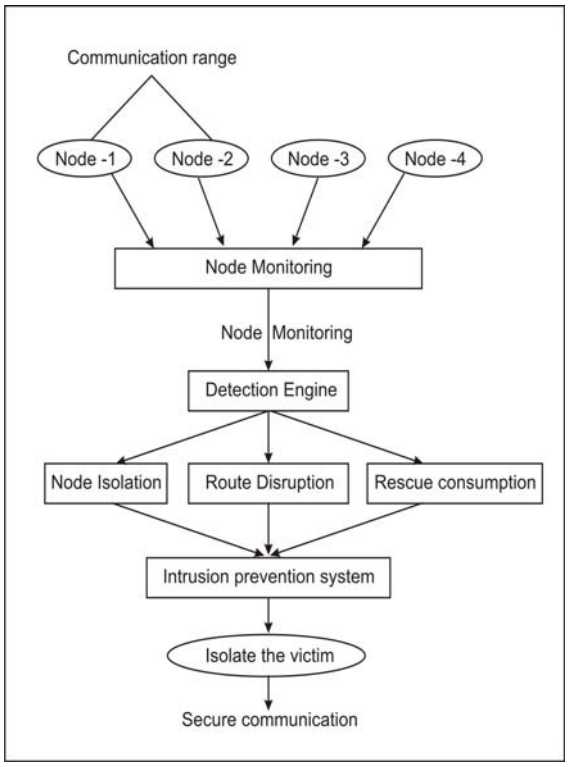

Table1: Simulation parameters

Parameters	Value
Simulation duration Topology Number of mobile Nodes Transmission range Node movement model Traffic type Data payload	100 sec 500m* 500m 08 1.5m Random way point model CBR(UDP) 50 bytes

5. Experimental Studies

We have conducted the following experiment using ns2.29 simulator on Fedora 9 in order to study the different types of internal attacks & their Intrusion prevention System.

5.1 Parameter Selection

We are to apply the random way-point model to emulate node mobility patterns with a topology of 500m by 500m. We use both TCP and UDP/CBR as underlying transport protocol. The maximum number of mobile nodes is set to be 8. Transmission range is 1.5m. All trace have a run

time of 100sec. some regarding simulation environment given in tables.
An important property of a mobile ad-hoc network is dynamic network topology. Since every node can move arbitrarily. Network topology changes time to time and the communication links between mobile nodes break frequently. This simulation parameters is shown in Table2

5.2 Simulated Attack

RESOURCE CONSUMPTION (RC)attack:
In resource consumption, an attacker might try to initiate large number of route requested to bogus destination in order to exhaust the resources of the network. Selective dropping of packet resulting in increased number of route requests from neighbor nodes .This attack introduced at 30sec.

NODE ISOLATION (NI) ATTACK
The action of node isolation attack is preventing a node from communicating with other node. Under this attack node gets isolated from the network topology due to action of attacker over the system. In our simulation experiment node0 send 3000packets towards the destination i.e. node3 but node 4 acts as an attacker and it isolates node 0. This attack introduced at 50sec

ROUTE DISRUPTION (RD) ATTACK
The action of route disruption is breaking of an existing root or preventing a new route from being established. In this attack under normal mode, node 5 transmits 3000 packets towards destination that is node 6, but node 7 tries to take message from node 5 and drops a number of packets. Under this attack, due to dropping of an existing route , dropping of packets occurs. Here, the result shows 3000packets are sent under normal mode while under attack mode 19000 packets are sent, which clearly distinguish the action of attacker from that normal mode. This attack starts at the moment of 65th sec.

5.3 Intrusions Prevention System

The node that highly drops the packet, the node which disrupts the existing routes and the one which consumes more packets are generally said to be attackers. These nodes are pointed as attacker in the simulation environment and isolated from the topology so that we get the safe communication.
In one network there should not be more than one CBR active at a given time. If it is so then network is under attack. So to remove the attack we need to remove the CBR which are attacking the network. CBR are the main components that control traffic in a system. If there are a number of packet losses at a node, the CBR has to be stopped so that the traffic is cut off from the node

If the CBRs which are found faulty, are given a higher CBR intervals (this can change as per the network traffic), the network would not respond to the fast changes in the packets as introduced by the attacker, thus preventing the network from these attacker from the beginning. This is the basic concept behind intrusion prevention system.

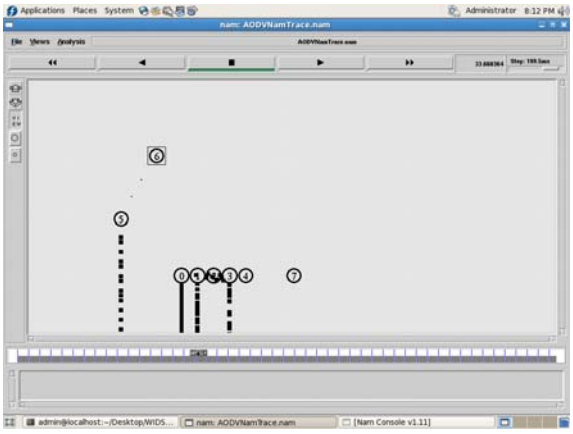

Figure1: Simulation setup of resource consumption attack

6. Experimental Result

In this section, we will see some few simulation scenarios to understand these network internal attacks in detail. NAM is tool with ns-2.It gives us a graphical representation of the network and packet traversing through the network. It helps to have cursory glance and deduce some events happening in the simulation. Figure 1 shows graphical representation of 8 mobile nodes where adjacent nodes are in range to one another.

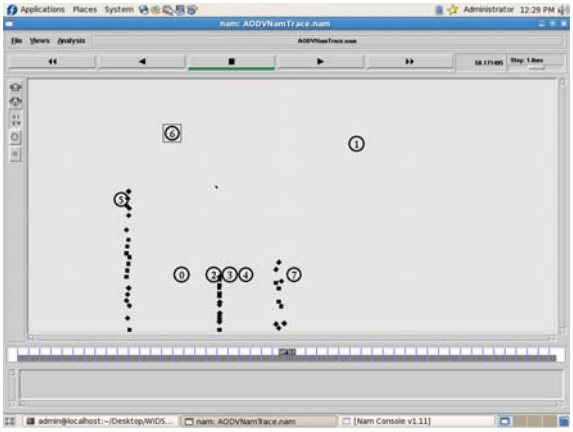

Figure2: Simulation setup of Node isolation attack

As shown in fig.1 Resource consumption attack starts at 30sec. node 0, node 1, node 2, and node 5 act as attackers and continuously drop the packets

Due to NI attack node 4 which act as a attacker isolate node1 from communicating with node 3.This attack starts at the moment of 50th sec.

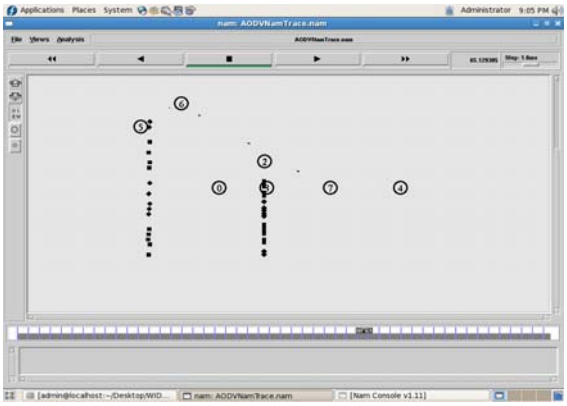

Figure3: Simulation setup of routing disruption attack

In the above result node 7 acts as a attacker and disturbs the main route which is from node 5 to node 6 This attack starts at the moment of 65th sec.

We are simulating the above attacks as an example; such type of number of attack is present in the network at different time. CBR are the main components that control traffic in a system. If there are a number of packet losses at a node, the CBR has to be stopped so that the traffic is cut off from the node. In one network there should not be more than one CBR active at a given time. If it is so then network is under attack. So to remove the attack we need to remove the CBR which are attacking the network If the CBRs which are found faulty, are given a higher CBR intervals (this can change as per the network traffic), the network would not respond to the fast changes in the packets as introduced by the attacker, thus preventing the attack in the network from the beginning.

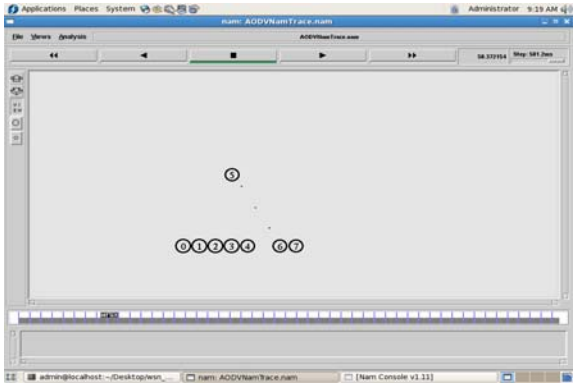

Figure4 Simulation result for IPS system

In our simulation experiment through observation if the CBR interval is 0.3, there is no packet drop at that juncture which we have discussed. As indicated in fig. 4, from the beginning there is a safe communication between node 5 and node 6 though the above attack is present at different time. This happened only due to proper CBR-interval.

Final tool that can be helpful in analyzing data from NS-2 is x-graph .Up to CBR interval at 0.3 the network is suffered from attacks; this is illustrated in Fig 5 where we have taken CBR intervals on x-axis and on y axis packet dropping at fixed time of 40sec. No attack is present after 0.3 in the network. Then With this observation, it is noted that if CBR interval is kept 0.3 attacks are prevented. But for security, we have taken the intervals on 0.5. where attack is completely wiped out.

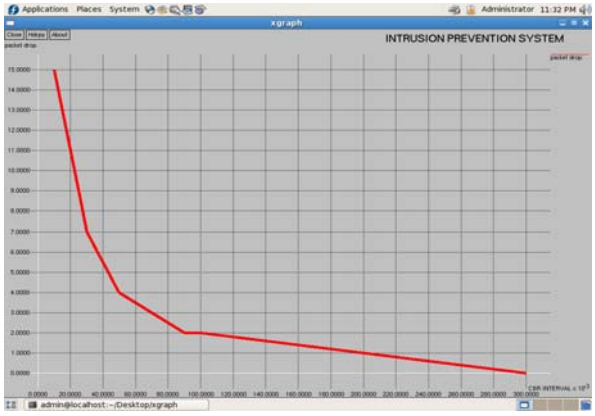

Figure 5 X-graph of IPS system

7. Conclusion

An approach for detecting and analyzing various attacks on MANET has been studied and performance is analyzed. In this paper the basic observation related in intrusion prevention system has been studied for the particular node dropping the packets, diverting the route and consuming more resources detected by the proposed systems.

In the future enhancement ,simulation can be performed for some complicated attack, also the action of attack can be reduced by using some sophisticated algorithmic techniques of intrusion prevention system, so as the future work ,the recovery phase can be more concentrated

References

[1] “An Approach for detecting attacks in mobile adhoc networks”by V.Madhu Viswanatham and A.A.Chari,AP,India

[2] Yi-an Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia, October 31, 2003.

[3] J. Wright, "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection 2002 Nov 8 (Online Document)
[4] 'A Co-operative Intrusion detection system for Ad-hoc Network'
[5] Peter Barron @ cs, tcd–ie, Stetan Weber, Siobhan Karke, and Vuinny Cahill. "Experiences Deploying an Ad-hoc Network in an Urban Environment" Stetan Weber 6) Yu-xi Lim, Tim Shemoyes, proceeding of the 2003
[6] "Intrusion Detection in Tactical Multi- Hop Networks' by Nils Aschenbrack, Marko Jahnke University of Bonn, Institute of Computer Sciences IV Roemerstr, 164, Germany (aschenbrack@cs.ani-bo, nnde)) 802,11ninja "802,11ninja.net," available http://802.11ninja.net
[7] Air Defense Inc, "Wireless LANSecurity for the Enterprise" Air Defense. Available http://airdefense.net e
[8] NS-2 manual
[9] A Cooperative Intrusion Detection System for Ad Hoc Networks Yi an Huang College of Computing Georgia Institute of Technology yian@cc.gatech.edu
Wenke Lee College of Computing Georgia Institute of Technology wenke@cc.gatech.edu