Open access Journal International journal of Emerging Trends in Science and Technology

Experimental Evaluation of Location attacks in Mobile ad hoc Networks Implementation with Linux based Real time Systems

Authors

M.Rajaram*, Dr. V. Sumathy, V.Ramasamy*****

*PARK college of Engineering & Technology, Kaniyur as Assistant Professor in Electronics & Communication department. Phone: 9894853715;
Email: *happyramm900@ gmail.com*

**Govt college of Technology, Coimbatore as Associate Professor in Electronics & Communication department.
Email: sumi_gct2001@ yahoo.com

***PARK college of Engineering & Technology, Kaniyur as Assistant Professor in Computer Science& Engineering department. Phone: 9894836977
Email: csrams@ gmail.com

Abstract—Mobile ad hoc networks will often be deployed in environments where the nodes of the networks are unattended and have little or no physical protection against tampering. The clients of mobile ad hoc networks are so susceptible to compromise. The nets are specially vulnerable to denial of service (DoS) attacks launched through compromised nodes or intruders. In this report, we investigated the effects of location attacks in Network Simulation 2 (NS-2) and measured the packet delivery ratio and packet delay under different Location frequency and different routine of attack modes. Simulation results indicate that with the increase the location, frequency and the number of attack modes, network performance drops. Meanwhile the packet delay firstly increases and then pass up to a value of constancy in the terminal. Simulate in NS-2 Existing statements are primarily focused on finding the malicious node, but they are hardware specific like directional antennas and synchronized clocks. Only the suggested algorithm is both software and hardware specific. An linux based RToS is included to create the ad hoc network a real time application.

Index Terms— Mobile ad hoc networks, security, routing protocol, Location attack ,Linux based RTOS,

INTRODUCTION

The mobile Ad hoc network is an independent organization of mobile nodes connected by wireless connections. Each node operates not just as an end-system, but also as a router to forward packets. The guests are free to go around and coordinate themselves into a mesh. Mobile ad hoc networks do not require any set up infrastructure such as base stations, therefore, it is an attractive networking option for linking mobile devices rapidly and spontaneously, such as military applications, emergent operations, personal electronic device networking, and civilian applications like an ad-hoc meeting or an ad-his classroom.

The mobile ad hoc networks have several salient characteristics, such as Dynamic topologies, Bandwidth constrained, variable capacity links, Energy-constrained operation, Limited physical security [1]. Due to these features, mobile ad hoc networks are especially vulnerable to denial of service attacks launched through the compromised node. In this report, examining the effect of location attack in mobile ad hoc networks is focused. The simulation a variety of location attack scene by using NS2 network simulation too is designed.

Alterations in the number of attack nodes and the frequency of attacks on the scene, the location attack on the full network operation is examined. Simulation experiment shows:

With the increase the Location frequency and the number of attack nodes, network performance drops. □

When the frequency of location attacks in less than a certain value (for example, 20 packet/s), network performance decreases in inverse proportion to the increasing frequency of Attempts. When the frequency of location attacks is greater than the value, the performance drop gets not obvious. The primary cause is that packets of location attacks overtake MAC Processing power and cannot be transported away. □

With the increasing frequency of location attacks, the first step-up in the packet delay and then fall. □

In the remainder of the paper, section 2 summarizes the literature. Part 3 briefly introduces the routing protocol and discusses location attack. In section 4, we present the simulation experiments. Finally, section 5 concludes the paper.

RELATED WORK

We have not found related papers on the effect of location attack in mobile ad hoc networks by far. Many papers study how to defend location attack.. In these papers, their research only relates to location attack Rather than concentrate on the issue of location attack in mobile ad hoc networks. In the paper [2], we present a location attack which results in denial of service. In this attempt, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks, or transmits a lot of DATA packets to use up the bandwidth so as to congest in links. In that theme, our contribution is to present the model of attack and the way to defend location attack. Only we do not consider the effect of location attack in mobile ad hoc networks. In the paper [3], S. Desilva and R. V. Boppana introduce a simple rate based control packet forwarding mechanism to mitigate malicious control packet locates. Yinghua Guo and Sylvie Perreau present a behavior-based trackback mechanism to identify location attack origins, and also propose an attack isolation scheme to alleviate the attack impact on the network [4]. Yinghua Guo et al investigates one type of DoS attacks [5], spoofing location attack non-address-spoofing location attack, and present a detailed example to qualify it. They design two flow based detection features, and utilize the cumulative sum algorithm to them to effectively and accurately detect such attack.

THE MODEL OF LOCATION ATTACK

A. Overview of DSR

The Dynamic Source Routing (DSR) [6] is an exclusively on demand ad hoc mesh routing protocol, which is composed of two parts: Route Discovery and Route Maintenance. In DSR, whenever a node needs to transmit a packet to some destination for which does not presently have a route to that address in its Route Cache, the node initiates Route Discovery to find a path. The initiator broadcast a ROUTE REQUEST packet to its neighbors, specifying the target and a unique identifier from the initiator. Each client receiving the ROUTE REQUEST, if it has recently examined this request identifier from the initiator, discards the REQUEST. Differently, it adds its own node address to a list in the REQUEST and rebroadcasts the REQUEST. When the ROUTE REQUEST reaches its target node, the object sends a ROUTE REPLY back to the initiator of the REQUEST, including a transcript of the compiled list of destinations from the REQUEST. When the REPLY reaches the initiator of the REQUEST, it caches the new path in its Route Cache. The intermediate node also sends a ROUTE REPLY, if it has a path to the terminus.

Route Maintenance is the mechanism by which a client transmitting a packet along a set route to some destination detects if that path has gone bad. If, after a limited act of local retransmissions of the package, a guest in the route is unable to make this confirmation, it returns a ROUTE ERROR to the original source of the packet, identifying the link from itself to the next node as broken. The sender then removes this broken connection from its Route Cache; for subsequent packets to this destination, the sender may use any other route to that address in its Cache, or it may seek a new Route Discovery for that mark if necessary.

Location based packets in the whole network will consume a lot of resources of a mesh. To reduce congestion in a net, the protocol takes over some methods. A guest can not initiate more than ROUTE REQUEST messages per minute. After broadcasting a ROUTE REQUEST, a node waits for a ROUTE REPLY. If a route is not received within round-trip milliseconds, the guest may attempt again to find a route by broadcasting another ROUTE REQUEST, up to a maximum of retry times at the maximum TTL value. Repeated attacks by a root node at route discovery for a single destination must utilize a binary exponential back off. The first time a source node broadcasts a ROUTE REQUEST, it waits round-trip time for the receipt of a ROUTE REPLY. If a ROUTE REPLY is not picked up within that time, the source node sends a new ROUTE REQUEST. When estimating the time to wait for the ROUTE REPLY after sending the second ROUTE REQUEST, the source node MUST use a binary exponential back off.

Hence, the waiting time for the ROUTE REPLY corresponding to the second ROUTE REQUEST is 2 * round-trip times. The ROUTE REQUEST packets are spread in an incrementing ring to cut the overhead caused by location the whole net. The packets are flooded in a low country (a closed chain) first defined by a starting TTL (time-to-live) in the IP headers. After RING TRAVERSAL TIME, if no ROUTE REPLY has been obtained, the flooded area is expanded by increasing the TTL by a specified value. The process is iterated until a ROUTE REPLY is received by the originator of the ROUTE REQUEST, i.e., the path has been set up.

B. Location Attack

In the location, Attack, the attack node violates the above rules to beat the network resource. Firstly, the attacker selects many IP addresses which are not in the networks if he recognizes the scope of IP address in the meshes. Because no client can answer ROUTE REPLY packets for these ROUTE REQUEST, the reverse route in the route table of the guest will be conserved for long. The attacker can select random IP addresses if he cannot recognize the scope of IP address. Secondly, the attacker successively originates mass ROUTE REQUEST messages for these void IP addresses. The attacker attempts to charge an excessive ROUTE REQUEST without considering ROUTE REQUEST_RATELIMIT in per sec. The attacker will resend the ROUTE REQUEST packets without waiting for the ROUTE REPLY or round-trip time, if he uses out these

IP addresses. The TTL of ROUTE REQUEST is set up to a maximum without using the expanding ring search method. In the Location Attacks, the whole network will be full of ROUTE REQUEST packets which the attacker sends. The communication bandwidth is consumed by the flooded ROUTE REQUEST packets and the resource of nodes is used up at the same time. For instance, the storehouse of the route table is defined. If mass ROUTE REQUEST packets are getting to the node in a little time, the storage of route table in the node will exhaust so that the client cannot receive new ROUTE REQUEST packet. As a consequence, the legitimate nodes can not fix up routes to transmit information.

SIMULATION EXPERIMENTAL AND RESULT ANALYSIS

A. Experimental setup

To examine the effect of location attack in mobile ad hoc networks, we have implemented Location attack in a network simulator and conducted a series of experiments to measure its strength. The wireless network simulation software, from Network Simulator NS-2 is used. It includes simulation for wireless ad-hoc network infrastructure, popular wireless adhoc routing protocols (DSR, DSDV, AODV and others), and mobility scenario and traffic pattern generation.

Our simulations are based on a 1000 by 1000 meter flat pace, spread with 50 wireless nodes. The nodes move from A random starting point to a random destination with a velocity that is randomly selected. The speed is uniformly distributed between 0-20m/Sec. As the address is reached, another random address is targeted after a pause time. The MAC layer used for the simulations is IEEE 802.11, which is included in the NS-2. The transport protocol used for our simulations is User Datagram Protocol (UDP). Each information packet is 512 bytes long. The traffic files are generated such that the source and destination pairs are randomly spread over the integral net. The scenario files to determine the mobility of the lymph glands. The mobility model used random way point model in a rectangular domain. Continuance of the simulations is 90 minutes.

We utilize the following metrics to assess the public presentation of location Attack. Packet delivery rate: the ratio between the number of packets originated by the application layer CBR (continuous bit rate) sources and the number of packets received by the concluding terminus. The packet delivery ratio is significant as it depicts the loss rate that will be picked up by the transport protocols, which in turn move the maximum throughput that the network can sustain. The metric characterizes both the completeness and rightness of the routing protocol. Average delay: this is the average of delays incurred by all the packages which are successfully sent. 29.6 % Efficiency obtained from our Research. Number of Packet forward: the amount of packets which all nodes forward.

B. Simulation results are presented

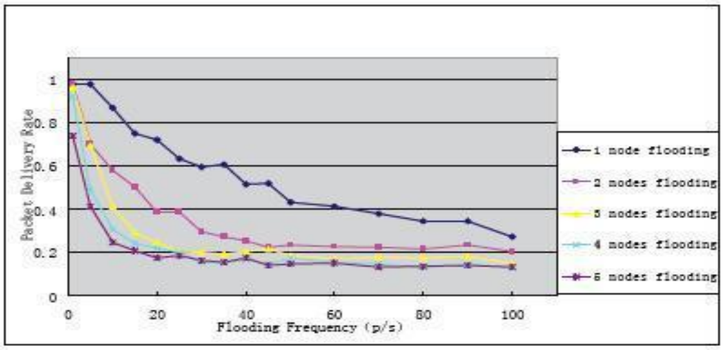

Figure 1: Packet delivery rate at different locate frequency

In Fig.1, simulation results show that the drop of packet delivery rate is relatively smooth under one location In pretending, the frequency of location attack changes from sending 0 packets/ per second to 100 packets/ per sec. Meanwhile, the measure of location nodes increase from 0 to 5.5.
Lymph gland, and when the location, frequency increases to 100 packets/ per second, packet delivery rate fall to 29%. With the growth in the number of location nodes and the frequency of location attack, the drop of packet delivery rate significantly speeds up. Under 5 location nodes and 21 attack packets/ per second, packet delivery rate fall to 17 %

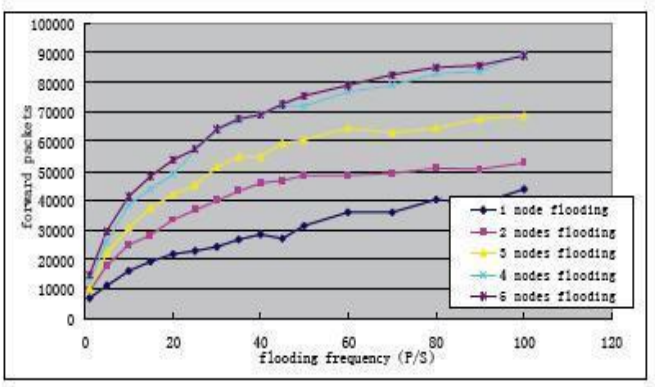

Figure 2: Number of forward packets at different location frequency

Number 2. The number of forward packets under different location, frequency In Fig.2, we can clearly see, with the increase in the number of nodes and the frequency of location attack, the number of forward packets significantly increases in contrast with the trend in Figure. It understands that location nodes have exhausted the communication bandwidth and node resource so that the valid communication can not be delivered.

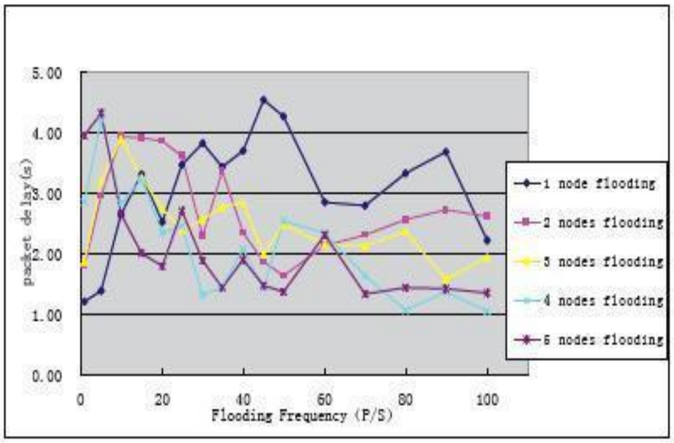

Figure3: Packet delay at different locate frequency

In fig. 3, with the increase of the frequency of location attack, the packet delay extends from 1.2 seconds to 4.5 seconds under one location node. Later, with the gain of the frequency of attack, the packet delay start to flow and get to 2.3 seconds under 100 location attack packets/per sec. Similarly, the circumstances under many nodes locations, the first packet delay goes up to a point and then pass up to a value of constancy in the terminal. For exemplar, the circumstances under 5 nodes location, first packet delay goes up to 4.2 seconds and then turn down to 1.4 seconds at the final stage. This phenomenon can be explained that before the communication bandwidth and node source are exhausted, the packet delay increases in direct ratio to the increasing frequency of attempts. All the same, when the network source has been exhausted, with increasing frequency of location attacks, nodes begin to throw out the congestion packets, especial in a long road. It results in shortening the delay that a batch of mail boats in long route have lost and some packets in the shortest route survive.

In parliamentary law to bring into account delay of lost packages, we will place a unified larger value for delay of lost packages. Fig.4 shows these re-calculated curves by this method. We can clearly see, with the increase in the number of location nodes and the frequency of location attack, the delay significantly increases.

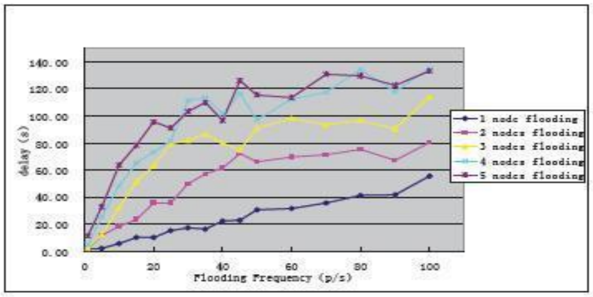

Figure 4 : The overall delay under different location frequency

REAL TIME OPERATING SYSTEM APPROACH

A. The Hardware Platform

Considering the focus of this paper, which is to evaluate the practicality of a Embedded Linux Platform for a relatively average speed computer network application, we thus opted for the The XPedite5502 is a high-performance, PrPMC/XMC, single board computer supporting Freescale QorIQ P1 and P2 processors. With dual PowerPC e500v2 cores running at upwards to 1.2 GHz, the P2020 delivers enhanced performance and efficiency for today's network information processing and other embedded computing applications. Complementing processor performance, the XPedite5502 features up to 8 GB of DDR3-800 ECC SDRAM. A configurable SerDes Interface (PCI Express or Serial RapidIO) to the XMC connector or a conventional PCI interface to the PMC connectors provide ample bandwidth to the P2020. Single Gigabit Ethernet port, a USB 2.0 port, and two RS-232/422/485 ports are routed to P14 or P16 for additional system flexibility. The front panel offers comfortable access to two Gigabitports Ethemet Ports and two RS-232 serial ports.The XPedite5502 provide a high performance.future rich soluation for current and future generation Embedded Diligences.Additionally,for customer seeking a maximum Power of just 8 W, the XPedite5502 can be made with the Freescale P1020 processor. Operating system support software systems for the XPedite5502 include Wind River VxWorks, QNX Neutrino, Green Hills INTEGRITY, and Linux 3.6.

FEATURES

I. Freescale QorIQ P2020 processor with dual PowerPC e500v2 cores at up to 1.2 GHz (alternate processors P1011, P1020, P2010)
II. Air-cooled
III. Upward to 8 GB of DDR3-800 ECC SDRAM
IV. Up to x4 PCI Express or Serial RapidIO
V. PCI PrPMC interface
VI. Three Gigabit Ethernet ports
VII. Two RS-232/422/485 serial ports
VIII. One USB 2.0 port
IX. Upward to 256 MB of NOR flash (with redundancy)
X. Upward to 16 GB of NAND flash
XI. Linux BSP
XII. Wind River VxWorks BSP
XIII. QNX Neutrino BSP
XIV. Green Hills INTEGRITY BSP

C. System Overview

The system is called Embedded Security Scan Detector (ESSD) and its task is to ensure security through incorporation of LOCATION. Sensing. The system is user programmable, meaning the user has the flexibility of choosing the ports that he/she would wish to peep into looking for any possible malicious attack activity. The SBC, which complies with the embedded PC standard, a commonly-used robotic development platform, has a main table of around 4 by 4 inches that houses a CPU, memory and the basic chipset needed to run as a standalone embedded computer capable of functioning with only a separate power supply and whatever outside input or output devices the application calls for. The embedded PC allows the use of an 802.11b (WI-Fi) and cabled

Ethernet that provides high-speed two way communications link Between the system and PC Database Server.

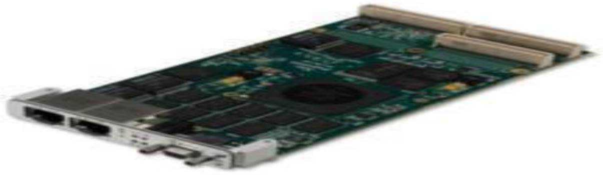

Figure 5: expedite 5502 SBC

CONCLUSION

In this paper, the location attack on the entire network performance under the circumstances of different location, frequency and different number of attack modes are analyzed. Simulation results show, with the increase the location, frequency and the number of attack modes, network performance drops. When the frequency of location attacks in less than a certain value, network performance decreases in inverse proportion to the increasing frequency of attacks. But when the frequency of location attacks is greater than the value, the performance decrease gets smooth. In addition, with the increasing frequency of location attacks, the packet delay firstly increases and then declines to a value of stability in the end.implemented with RTOS based xpediate 5502

REFERENCES

1. S. Corson, J. Macker ‘Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations” RFC 501 January 1999

2. Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang, Resisting Location Attacks in ad hoc Networks, International Conference on Information Technology: Coding and Computing (ITCC2005), IEEEPress, Las Vegas, USA, April 4-6, 2005.

3. S. Desilva and R. V. Boppana, Mitigating malicious control packet floods in ad hoc networks, in Proceedings of 2007 IEEE Wireless Communications and Networking Conference(WCNC2005), March 2007

4. Yinghua Guo, Sylvie Perreau, Trace Location Attack in Mobile Ad Hoc Networks, in Proceedings of 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP 2007), Dec. 2009

5. Yinghua Guo, Gordon, S., Perreau, S., A Flow Based Detection Mechanism against Location Attacks in Mobile Ad Hoc Networks, in Proceedings of 2010 IEEE Wireless Communications and Networking Conference(WCNC2007), March 2010

6. David B. Johnson, David A. Maltz, Yih-Chun Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09.txt, 15 April 2003, http:/ /www. ietf.org/internetdrafts/ draft-ietf-manet-dsr-09.txt

7. xes.2012/ rejaer