An Intrusion Detection System Algorithm for Defending MANET against the DDoS Attacks

Hemant Sonawane
M.Tech. Software Engineering
Computer Sci. & Engg. Dept
P.I.T., Bhopal, M.P., India

Hitesh Gupta
Head of Department
Computer Sci. & Engg. Dept
P.I.T., Bhopal, M.P., India

ABSTRACT

Mobile ad hoc network (MANET) is rapidly deployable, self configuring network able to communicate with each other without the aid of any centralized system. There is no need for existing infrastructure base network. In MANET Wireless medium is radio frequencies and nodes are mobile, topology can be very dynamically. Nodes must be able to relay traffic since communicating nodes might be out of range. A MANET can be a standalone network or it can be connected to external networks like internet. Multihop operation of MANET requires a routing mechanism designed for mobile nodes are internet access mechanisms, self configuring networks requires an address allocation mechanism, mechanism to detect and act on, merging of existing networks and security mechanisms. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self routing capability nature, there are many weaknesses in its security. Therefore Intrusion Detection System (IDS) uses anomaly based detection and signature based detection schemes for detection of Distributed Denial-of-Service (DDoS) attacks found on the wireless ad hoc network.

General Terms

Algorithm, Security, Attacks, Prevention, Simulation, Wireless network.

Keywords

MANET, DDoS, Digital Signature, AODV, SYN Flood, Intrusion Detection System.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. MANET use some routing protocol requirements that is self starting and self organizing, multi-hop, loop-free paths, dynamic topology maintenance, rapid convergence, minimal network traffic overhead, scalable to large networks. MANET is severely affected by Distributed Denial of Service (DDoS) attacks which becomes a problem for users of computer systems connected to the Internet. MANETs are more vulnerable compared to wired networks due the lack of a trusted centralized authority and limited resources. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile.

A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

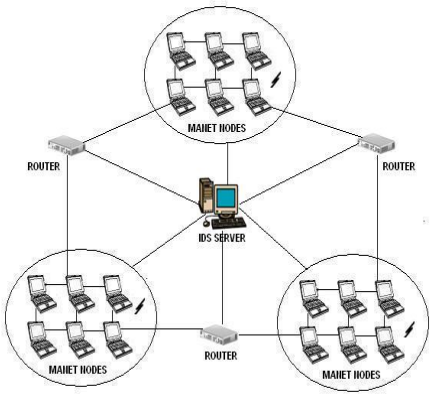

Fig.1 IDS Administration on MANET.

2. RELATED WORK

Prajeet Sharma, Niresh Sharma and Rajdeep Singh [1] analyzed over the throughput, end to end delay, routing load with TCP, UDP and AODV routing protocols for mobile ad hoc network. H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang [2] proposed security in mobile adhoc network challenges and solutions for wireless communication of mobile hosts for prevention of attackers. Pradeep Jawandiya at workshop [3] have presented seminar on routing protocols used in MANET, security in MANET and various attacks on MANET wireless network. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester [4] have presented applications, challenges over wireless mobile ad hoc network and detection over that attacks. S.A.Arunmozhi, Y.Venkataramani [5] proposed DDoS attack and defense scheme in wireless ad hoc networks

for wireless security. Christine Dartigue, Hyun Ik Jang, and Wenjun Zeng [6] proposed a new data mining based approach for network intrusion detection. Jelena Mirkovic, Max Robinson, Peter Reiher, George Oikonomou [7] proposed distributed defense mechanisms against DDoS attacks for network security. An intrusion detection system gives detection [8] mechanisms against attacks on the mobile ad hoc networks. Network Simulator ns-2 [9] simulator gives simulation results with some load distribution among the network. AODV protocol description [10][11]with protocol header formats like request header, reply header formats.

3. PROBLEM STATEMENT

DDoS attack is a natural development from the SYN Flood. The idea behind this attack is focusing Internet connection bandwidth of many machines upon one or a few machines. This way it is possible to use a large array of smaller (or "weaker"), widely distributed computers to create the big flood effect. Usually, the assailant installs his remote attack program on weakly protected computers using Trojan horses and intrusion methods, and then orchestrates the attack from all the different computers at once. This creates a brute force flood of malicious "nonsense" Internet traffic to swamp and consume the target server's or its network connection bandwidth. This malicious packet flood competes with, and overwhelms, the network's valid traffic so that "good packets" have a low likelihood of surviving the flood. The network's servers become cut off from the rest of the Internet, and their service is denied.

To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile.

4. METHODS FOR ATTACK DETECTION

Protocol Used: AODV

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a routing protocol used for dynamic wireless networks where nodes can enter and leave the network at will. To find a route to a particular destination node, the source node broadcasts a RREQ to its immediate neighbors. If one of these neighbors has a route to the destination, then it replies back with a RREP. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination. At that point a chain of RREP messages is sent back and the original source node finally has a route to the destination.

Digital signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

4.1. User Registration

In this module, user registers his/her personal details in database. Each user has unique id, username and password and digital signature. After using these details he can request file from server.

4.2. Upload & Send files to users

In this module, server can upload the files in the database. After verify user digital signature file could be transfer to correct user via mobile ad-hoc network.

4.3. Attack on Ad-Hoc Network

In this module, to see what the attack on ad-hoc is network is Distributed Denial of Services (DDoS). A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

4.4. Simulation Results

In this module, we implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity

4.4.1. Throughput

It is sum of sizes (bits), or number (packets) of generated/sent/forwarded/received packets, calculated at every time interval and divided by its length. Throughput (bits) is shown in bits. Throughput (packets) shows numbers of packets in every time interval. Time interval length is equal to one second by default.

4.4.2. Packet delivery fraction

Packet delivery fraction is average time for delivering the routing packets from source node to destination node.

4.4.3. End to End delay

Average time difference between the time of the packet receipt at the destination node, and the packet sending time at the source node.

4.4.4. Normalized routing load

Sum of numbers of all the intermediate nodes (nodes between source and destination nodes) receiving packets sent by all the source nodes or number of received packets at all the destination nodes.

5. ACTIVITY FLOW

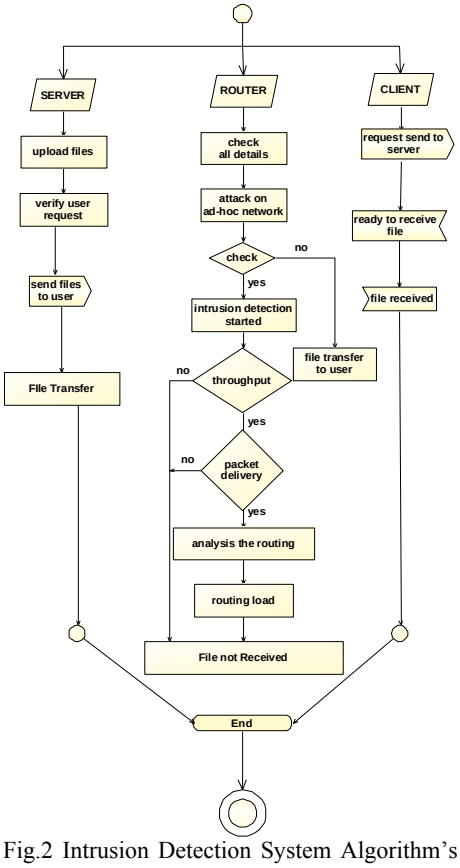

Fig.2 Intrusion Detection System Algorithm's Activity Flow Diagram.

6. ALGORITHM

Intrusion Detection System Algorithm:

1. Start

2. Start IDS server, client module and routing module with AODV and TCP protocol.

3. Login into IDS server (username, password).

4. Upload files on server those wants to send.

5. New client registration with password and digital signature.

6. Login into client (username, password).

6. If RREQ (File ID, IP Address)

//Client request to IDS server.

Then IDS server verify client request with digital signature.

If Request verified

Then RREP (File)

// IDS Server replies by sending file to client.

If DDoS attacks on ad hoc network

Then Go for Intrusion detection algorithm and simulation results as Throughput, End to End Delay, Packet Delivery, and Routing Load.

Else

Then File successfully transmitted to client.

7. Finally client system accept file with digital signature verification.

8. Stop.

7. CONCLUSION

An Intrusion Detection System uses various techniques for detecting attacks like DDoS attack on the wireless mobile ad-hoc network. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion detection on attack is easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. This proposed system algorithm helps programmers, engineers and telecommunications networks to save the efforts for detection of attacks like DDoS for wireless ad hoc networking. The intrusion detection system algorithm is usually implemented and administrated via radio waves where the implementation takes place at physical level with throughput, end to end delay, packet delivery and routing load while communication over network.

MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints. MANET requires a multi fence security solution that provides complete security spanning over the entire protocol stack. The Study of this reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and management, secure architecture, intrusion detection and protection. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities.

8. ACKNOWLEDGMENT

It is my pleasure to express my knowledge on Mobile Ad hoc Network to my respected sir Mr. Hitesh Gupta, Head of Department, Computer Science & Engineering, P.I.T, Bhopal for his valuable guidance, inspiration and continues support. This paper could not be success without algorithmic analysis done which help to understand the necessity for this paper.

9. REFERENCES

[1] Prajeet Sharma, Niresh Sharma and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of Computer Applications March 2012.

[2] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, Security in Mobile Ad hoc Networks: Challenges and Solutions, IEEE Wireless Communications. February 2004.

[3] Adam Burg, "Seminar on Ad Hoc Network Specific Attacks".

[4] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", 2005.

[5] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad-hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[6] Christine Dartigue, Hyun Ik Jang, and Wenjun Zeng, "A New Data-Mining Based Approach for Network Intrusion Detection".

[7] Jelena Mirkovic, Max Robinson, Peter Reiher, George Oikonomou, "Distributed Defense Against DDoS Attacks".

[8] Intrusion Detection System, Information Assurance Tools Report 2009.

[9] Network Simulator- ns-2. http://www.isi.edu/ nsnam /ns/.

[10]www.chicory.stanford.edu/satyaki/research/AodvRouting.html

[11] http://www.moment.cs.ucsb.edu/AODV/aodv.html

[12] Tao Lin, "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications", Ph.D. Dissertation, Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.

[13] Adam Burg, "Seminar on Ad Hoc Network Specific Attacks".

[14] Cryptography and Network Security by William Stallings – 4th Edition Pearson education.

[15] Cryptography and Network Security by Behrouz Forouzan McGraw-Hill publication.

[16] www.wirelessdefence.org.

[17] http://sectools.org/ - various security tools.

[18] http://www.google.co.in.