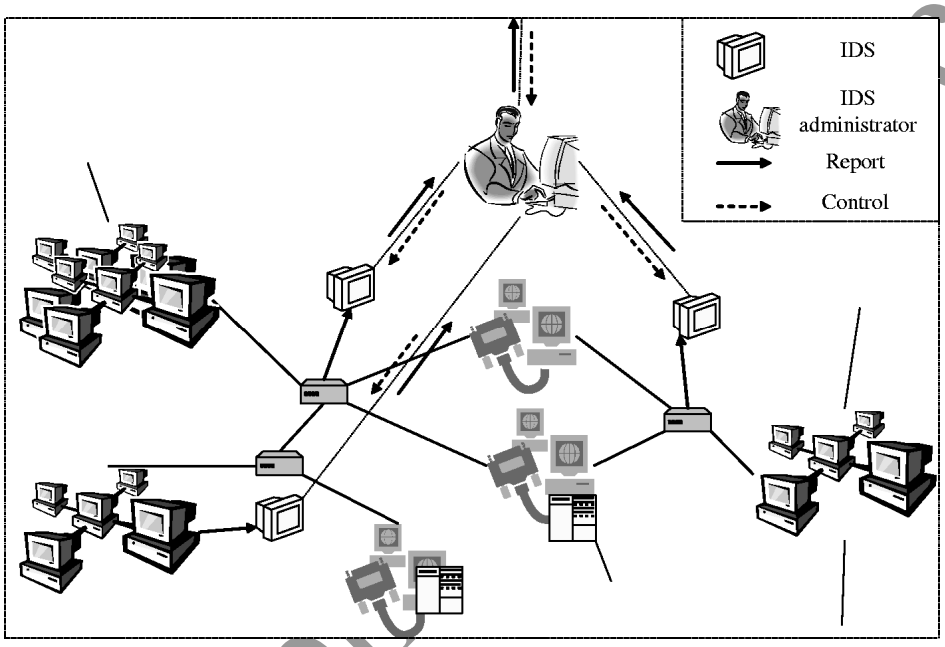
A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network

Abstract

Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

Architecture



Existing System

In existing system, Mobile ad-hoc networks 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.

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. One of the serious attacks to be considered in ad hoc network is DDoS attack.

A 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.

Proposed System

In proposed system, to solve the security issues we need an intrusion detection system. This can be categorized into two models:

1. Signature-based intrusion detection
2. Anomaly-based intrusion detection

The benefits of this IDS technique are that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack.

Modules

1. User Registration
2. Upload & Send files to users
3. Attack on Ad-Hoc Network
4. Criteria for Attack detection
5. Simulation Results

Modules Description

✓ 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.

✓ 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.

✓ 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.

✓ Criteria for Attack detection

In this module, we use multiple nodes and simulate through different criteria are NORMAL, DDoS and IDS (intrusion detection case).

Normal Case

We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behavior comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

✓ 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.

a. Throughput
b. Packet delivery fraction
c. End to End delay
d. Normalized routing load

System Requirements:

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Color.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system : - Windows XP.
- Coding Language : C#.Net