Secure Intrusion Detection System Against DDOS Attack In MANET

RAVIKIRAN PANDURANG PAWAR
M.TECH COMPUTER SCIENCE

ST.MARYS GROUP OF INSTITUTIONS
HYDERABAD, INDIA.

Abstract

Mobile ad-hoc network (MANET) system is a group of mobile devices which need to provide the ability to stream voice, data and video between arbitrary pairs of devices utilizing the others as relays to avoid the need for infrastructure. There are many techniques which are employed in order to provide robust MANET capability, Self-Forming / Self-Healing is a crucial characteristic of MANET systems. In a true mesh network, radios can join or leave the network at any time, and the network will continuously adapt its topology as nodes move in relation to one another. This implies a decentralized architecture in that there are no central "master" hub radios required to administer control of the network, and communications will continue to persist even when one or more nodes are lost. Multicast Traffic presents a set of unique challenges for MANET systems. There are many security attacks in MANET and Distributed denial of service (DDoS) is one of them.

Keywords

Defensive mechanisms, security goal, security attacks, MANET, DDoS attack.

1. Introduction

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router [5].The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet [6].Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. Link Adaptation is the ability for each radio to optimally configure its transmission parameters to maximize the data rate and robustness of the links to each of the other radios it is communicating with [1]. Adaptive Routing is a mechanism for determining which potential relay paths are used when a stream of data needs to be sent

between a given pair of radios. It needs to support self-forming self-healing functionality by adapting dynamically to use all radios present as potential relays and be resilient to the loss of relaying radios. Transparent IP Networking means that any number of standard computer, IP video camera or other devices may be connected to each of the mobile radios and communicates through the mesh network just as if all of the devices were in a single office with wired Ethernet. There are different ways this can be accomplished within the MANET. To enable the most flexibility and ease of use, the best choice is to have the entire MANET network appear as if it is a single Layer 2 networking switch. This means that without any reconfiguration of IP addresses or other settings, a group of IP based devices that work together on a simple Ethernet switch can be connected to MANET radios and resume operations with the new freedom of wireless mobility [8].

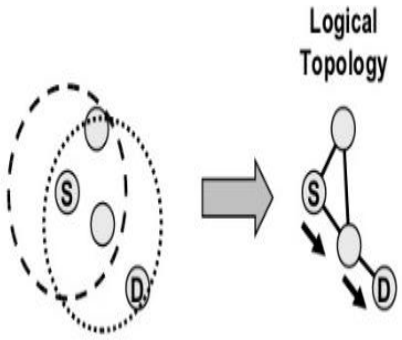

Figure 1: Mobile network: IP routing and MANET Routing

2. Purpose of the project

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. 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.

The benefit of this IDS technique is 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. 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.

3. Study of the System

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 this 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.

4. Attack on Ad-hoc network

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks are described as below

1) Malicious code

Malicious code is code causing damage to a computer or system. It is code not easily or solely controlled through the use of anti-virus tools. Malicious code can either activate itself or be like a virus requiring a user to perform an action, such as clicking on something or opening an email attachment. Malicious code does not just affect one computer. It can also get into networks and spread. It can also send messages through email and steal information or cause even more damage by deleting files. It can be in the form of scripting languages, ActiveX controls, browser plug-ins, Java applets and more. This is why it is often recommended to deactivate these options in Web browsers. Malicious code can come in various other forms. A common type of malicious code is the virus, which is a little program attaching to other programs or files and will copy itself in a computer and even spread to other networked computers. Viruses can range from being relatively harmless to causing significant damage to a system. Worms are pieces of malicious code making copies of itself. Conditions have to be right for a worm to proliferate. They are created mainly using scripting languages. Trojan horses are forms of malicious code appearing as safe software. But that is how they get into a computer. They may be hiding inside another program and be installed with an otherwise safe program. Sometimes they give someone in a remote location control of the victim's computer.

2) Repudiation

A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the

authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.

3) Session hijacking

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. It is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. A popular method is using source-routed IP packets. This allows a hacker at point A on the network to participate in a conversation between B and C by encouraging the IP packets to pass through its machine. If source-routing is turned off, the hacker can use "blind" hijacking, whereby it guesses the responses of the two machines. Thus, the hacker can send a command, but can never see the response. However, a common command would be to set a password allowing access from somewhere else on the net.

4) Flooding

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests [7]. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

5) DDoS attack

Distributed Denial of Service, is a type of DOS attack where multiple compromised systems, which are usually infected with a Trojans are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack[9].In a DDoS attack, the incoming traffic flooding the victim originates from many different sources potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

6) Wormhole Attack

Wireless ad hoc networks have gained popularity in recent years for the ease of deployment due to their infrastructure-less nature. One obvious use of such networks is in hostile environments for communications, monitoring, sensing etc. But being a broadcast medium, wireless medium offers an innate advantage to any adversary who intends to spy in or disrupt the network. Wormhole attacks are one of most easy to deploy for such an adversary and can cause great damage to the network. In this attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be

established by a variety of means, e.g., by using a Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

5. Criteria for attack detection

1. Normal Case

Analyze the network or system and infer what is normal .Apply statistical or heuristic measures to subsequent events and determine if they match the model/statistic of "normal". If events are outside of a probability window of "normal" then generate an alert.

2. Signature-based intrusion detection

In this method, it searches for a known identity - or signature - for each specific intrusion event. It works similar like anti-virus; depend on receiving regular signature updates, to keep in touch with variations in hacker technique. Signature-based IDS is only as good as its database of stored signatures.

3. Anomaly-based intrusion detection

In this method, system detects computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created.

In order to determine what attack traffic is, the system must be taught to recognize normal system activity. This can be accomplished by using technique like neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack.

6. Architecture

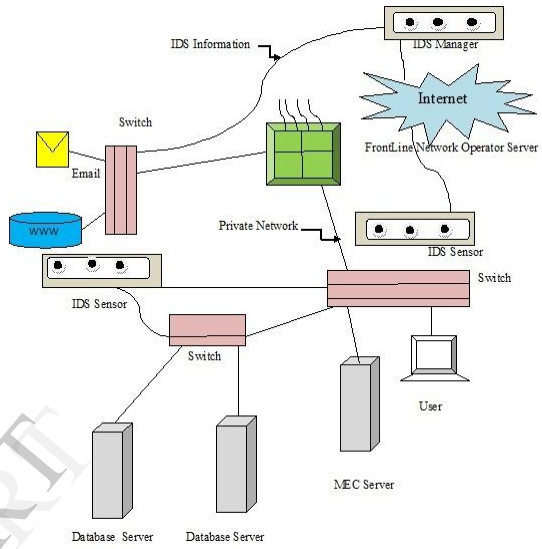

Figure2: Architeural diagram

7. Algorithm

```
Create node =ids;
Set routing = AODV;
If ((node in radio range) && (next hop! =Null)
{
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
{pkt_type; // AODV, TCP, CBR, UDP
Time;
Tsend, trecv, tdrop, rrep, rreq
}
Threshold_parameter ()
If ((load<=max_limit) &&
(new_profile<=max_threshold) &&
(new_profile>=min_threshold))
{
```

```
No any attack;
}
Else {
Attack in network;
Find_attack_info ();
}
Else {
"Node out of range or destination unreachable"
}
Find_attack_info ()
{
Compare normal_profile into each trace value
If (normal_profile! = new trace_value)
{
Check pkt_type;
Count unknown pkt_type;
Arrival time;
Sender_node;
Receiver_node;
Block_Sender_node (); //sender node as attacker
```

8. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Interaction Model

1. Client-driven interventions

Client-driven interventions are the means to protect customers from unreliable services. For example, services that miss deadlines or do not respond at all for a longer time are replaced by other more reliable services in future discovery operations.

2. Provider-driven interventions

Provider-driven interventions are desired and initiated by the service owners to shield themselves from malicious clients. For instance, requests of clients performing a denial of service attack by sending multiple requests in relatively short intervals are blocked (instead of processed) by the service.

9. Modules

Modules Description

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.

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.

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 [1]. 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.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

10. Conclusion

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

References

[1] "*A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network*", International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.

[2] F. Anjum, D. Subhadrabandhu and S. Sarkar. "*Signature based intrusion detection for wireless Ad-hoc networks*," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[3] D. E. Denning, "*An Intrusion Detection Model"*,IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[4] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: "*Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks"*, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[5] ShabanaMehfuz, Doja,M.N.: "*Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs*", Journal of Artificial Evolution and Applications (2008)

[6] Giriraj Chauhan,Sukumar Nandi: "*QoS Aware Stable path Routing (QASR) Protocol for MANETs"*, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[7] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: "*Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals"*, EURASIP Journal on Advances in Signal Processing (2009)

[8] Xiaoxin Wu, David,K.Y.Yau, "*Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach"*, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)

[9] 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, DOI: 10.5121/ijnsa.2011.3312.

[10] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim "*DDoS flooding attack detection through a step-by-step investigation*" 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011

[11] Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu " CBF: "*A Packet Filtering Method for DDoS Attack Defence in Cloud Environment*", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4.2011

[12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "*Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003

[13] K. Balakrishnan, J. Deng, and P.K. Varshney, "*TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks*" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.