IPHV2I20004X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

ENHANCED IDS TECHNIQUES AGAINST DDOS ATTACK IN WIRELESS MOBILE AD-HOC NETWORK

K.Manasa[1], M.KISHORE KUMAR [2]

1. [M.Tech (CS)] , Dept. of Computer Science & Engineering, VITS(N9), Karimnagar.

2. Assistant Professor, Dept. of Computer Science & Engineering, VITS(N9), Karimnagar.

ABSTRACT:

A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment. Ad hoc network 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 likeDistributed 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. We mainly focuses on security against the DDOS attack.

Keywords: *Security, algorithms, distributed denial of attack, intrusion detection system, Wireless mobile ad-hoc network, security goal, security attacks.*

INTRODUCTION

Sensor networks are large sets of small, inexpensive devices with hardware for sensing and a radio for communication with the other sensors. Sensor networks are being enabled by the convergence of several technologies at once. The advent of cheap, low-power microprocessors, sensor technology, and low-power RF design has made it possible to conceive of large networks which can together do what might be impossible (or too costly) to do with fewer, more expensive nodes. Wireless sensor networks are "ad hoc" networks, which means that the topology of the network is not planned, but must be decided by the network nodes themselves. Many fundamental questions about wireless ad hoc networks remain unanswered. Among the questions considered in this dissertation are: To what extent is "layered networking" satisfactory for sensor networks? Is scheduling or contention a better way to control medium access in sensor networks? With what power should nodes in the network transmit? Will nodes determine their neighbors, and if so, how? Ad hoc sensor networks are likely to be designed to fit one application very well. **[12][6]**

This is because sensors will in many cases face a short lifetime as a result of the limitations of battery technology, and energy can be conserved by removing extraneous functions**[3]**. The result of applying this principle is that sensor architectures will be optimized for two things: lasting a long time,

IPHV2I20004X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

and doing well the one thing for which they were designed.

If a given wireless sensor network is to have only one or two objectives, there islittle reason to maintain the generality of the OSI model ("layered networking" [1])within the network stack of the sensor. We should optimize lifetime or performance by making connections across layers of the network stack. In a general purpose computer, which must handle a large set of applications and conform to many networking standards, layering is a reasonable response to the great complexity of software. In a sensor which has a single application and no requirement to conform to a standard (at this time), layering serves as an obstacle to performance, lifetime, or both. For example, some routing algorithms decide which link to forward a packet onto by choosing the path with smallest end-to-end expected delay. A better fit for an energy-constrained node **[5]** might be to choose the path consuming least total energy. However, energy is a physical layer parameter, which would not be available in the routing calculation if we maintained a strict boundary between the routing, link and physical layers. It is quite unclear how the optimal communication system should work, absent layering..

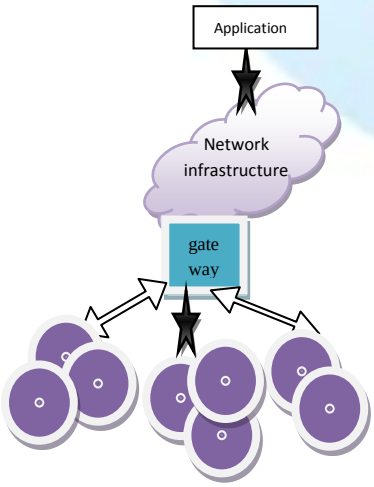
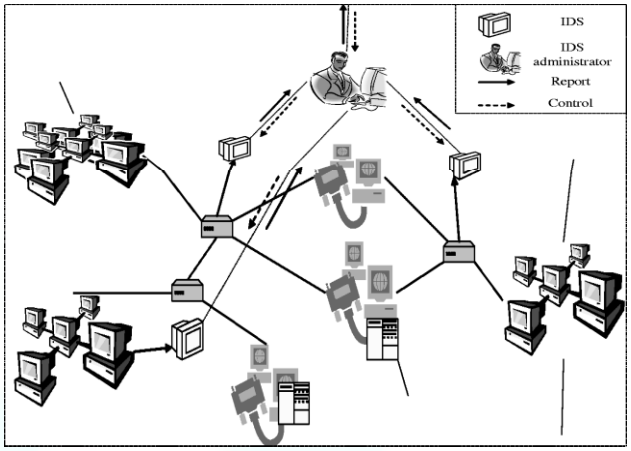


Fig.1. Sensor Networks

ARCHITECTURE:



In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.

4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource
  starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
- Crash the operating system itself.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. DoS they say is a tool for registering dissent. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'.[1] The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

A permanent denial-of-service (PDoS), also known loosely as phlashing,[11] is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.[12] Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image—a process which when done legitimately is known as *flashing*. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

The PDoS is a pure hardware targeted attack which can be much faster and requires fewer

resources than using a botnet in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacker communities.

Performing DoS-attacks

A wide array of programs are used to launch DoS-attacks. Most of these programs are completely focused on performing DoS-attacks, while others are also true Packet injectors, thus able to perform other tasks as well. Such tools are intended for benign use, but they can also be utilized in launching attacks on victim networks.

Handling

Defensive responses to Denial of Service attacks typically involves the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate.[25] A list of prevention and response tools is provided below

Firewalls

Firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses. In the case of a simple attack coming from a small number of unusual IP addresses for instance, one could put up a simple rule to drop all incoming traffic from those attackers.

More complex attacks will however be hard to block with simple rules: for example, if there is an ongoing attack on port 80 (web service), it is not possible to drop all incoming traffic on this port because doing so will prevent the server from serving legitimate traffic.[26] Additionally, firewalls may be too deep in the network hierarchy. Routers may be affected before the traffic gets to the firewall. Nonetheless, firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.

Some stateful firewalls, like pen

BSD's pf(4) packet filter, can act as a proxy for connections: the handshake is validated (with the client) instead of simply forwarding the packet to the destination. It is available for other BSDs as well. In that context, it is called "synproxy".

Switches

Most switches have some rate-limiting and ACL capability. Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection and Bogon filtering (bogus IP filtering) to detect and remediate denial of service attacks through automatic rate filtering and WAN Link failover and balancing.

These schemes will work as long as the DoS attacks are something that can be prevented by using them. For example SYN flood can be prevented using delayed binding or TCP splicing. Similarly content based DoS may be prevented using deep packet inspection. Attacks originating from dark addresses or going to dark addresses can be prevented using Bogon filtering. Automatic rate filtering can work as long as you have set rate-thresholds correctly and granularly. Wan-link failover will work as long as both links have DoS/DDoS prevention mechanism.[*citation needed*]

Routers

Similar to switches, routers have some rate-limiting and ACL capability. They, too, are manually set. Most routers can be easily overwhelmed under a DoS attack. Cisco IOS has features that prevent flooding, i.e. example settings.[27]

Application front end hardware

Application front end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front end hardware analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous. There are more than 25 bandwidth management vendors.

IPS based prevention

Intrusion-prevention systems (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.

An ASIC based IPS may detect and block denial of service attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way

A rate-based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is traffic anomaly. It must let the legitimate traffic flow while blocking the DoS attack traffic. [28]

DDS based defense

More focused on the problem than IPS, a DoS Defense System (DDS) is able to block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as Teardrop and Ping of death) and rate-based attacks (such as ICMP floods and SYN floods).

Blackholing and sinkholing

With blackholing, all the traffic to the attacked DNS or IP address is sent to a "black hole" (null interface or a non-existent server). To be more efficient and avoid affecting network connectivity, it can be managed by the ISP.

Sinkholing routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

Clean pipe

All traffic is passed through a "cleaning center" or a "scrubbing center" via various methods such as proxies, tunnels or even direct circuits, which separates "bad" traffic (DDoS and also other common internet attacks) and only sends good traffic beyond to the server. The provider needs central connectivity to the Internet to manage this kind of service unless they happen to be located within the same facility as the "cleanin

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.

IPHV2I20004X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

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. View 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 users 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.

VIEW 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

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

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

[3] 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)

[4] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and

[5] 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).

[6] 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)

[7] 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)

[8] 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.

[9] 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

[10] 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

[11] 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

[12] "Permanent Denial-of-Service Attack Sabotages Hardware". Dark Reading. December 9, 2008. Archived from the original on December 8, 2008.