www.ijiarec.com

ISSN:2348-2079 Volume 4 Issue 6

International Journal of Intellectual Advancements and Research in Engineering Computations

DETECTION OF DDoS ATTACKS BY SIGNATURE GENERATION WITH PATH AND PATTERN METRICS

Manojkumar.K[1], A.Viswanathan[2]

Abstract

Wireless networks, the dominant and successful networks of today, defined a flexible approach of providing service to the nodes anywhere and anytime. Either autonomous or client machines are distributed spatially to perform its prescribed functions by the base station. The data collected from the environment, considered to be of sensitive importance, have to be ensured to reach the right end. When deciding a framework of the wireless networks, a number of concerns have to be concentrated. Traffic of the data packets, congestion control, and prevention from attacks of any kind, detection and tracing back of attackers will be the prioritized actions. Denial of Service attacks, an attempt to degrade the network's resources such as bandwidth and memory, target a single machine to prevent it from getting or sending the data to the base station. The paper introduces a novel approach to monitor, communicate and determine if there is any attack within the networks. The proposed protocol will be ensuring the confidentiality by enabling a three times check for the originality of data packets. When the system doubts a data packet, signatures are checked in three registers, one from the sender, intermediate and the destined node. Any packet without these signatures will be regarded as an attack packet. The advantage of this method is to counter a low profile DoS attacks, which has evolved into a new type of attack for minimal evidence of an attack.

Introduction

Ability of a person to obtain services from anywhere for enhanced productivity, mobility concerns and faster access are higher priority reasons for employing wireless sensor networks nowadays. Corporate and Enterprises prefer a simpler and wider technology for their applicability. Deploying a wireless network will be comparatively cost effectively on investment and manpower for sure. Yet these merits could never differentiate between the right user and the attacker. The same liberties are promised to the attacker enabling him to block the services to the other users with some extra knowledge over the protocols and traffic managements. Traditional approaches comprise of cables to establish

Author for Correspondence:
[1]Research Scholar, Annamalai University, Chidambaram, Tamilnadu, India. .Email: manojkumar.k@hotmail.com
[2]Professor, Annamalai University, Chidambaram, Tamilnadu, India. Email Idyoursvichu@gmail.com

connection between nodes, and packets transfer to and fro between end to end attached systems. With an open air medium, attackers pose a serious threat to the confidentiality of the packets. Traversing packets could be disrupted, captured and prevented from reaching the right user with the right software and devices of the misbehaving nodes in the region. Gaining unauthorized access to a highly confidential network will reflect on the security of a nation. Thus preventing an illegal entry would be the primary concern of an enterprise or the developer himself.

A packet traversing in the wireless network uses the unbound air medium holding the address of destined nodes in a frame. A wireless Access point would initiate the process of launching the packet into the medium. A device named to sniffer, checks for the packets those are supposed to be searching for a node within, and collects the frames. The frame holds the details of the destination node, the base station and the MAC address of the wireless Access Point. Similarly a NIC (Network Interface Card) employed within node is ordered not to sniff or retrieve the frames of packets those are not intended for the particular network. But still a wireless network will be under attack by a number of packets with a count enough to saturate the bandwidth limitation. There are a number of well defined defensive and preventive mechanisms to control the attacks and innovative approaches are derived for a countermeasure by an attacker. Today, a Denial of Service attack has evolved to evade and overcome the preventive, detection strategies installed in the networks only delivering a very low profile of the attacker to the detection scheme.

The Misbehaving node may obtain access to the wireless network with an open switch, in turn, getting the same usability rights to the contents of the organisation. Mankind has ever been trying to prevent these intrusions facilitating a safe and secure environment for a person to communicate with his/her desired destination. A survey in 1999 denoted that 32% of entire internet users have experienced DoS attacks. And until major web servers like Yahoo, google faced the same attacks, the attacks came to light. Yet, some standards are always proven to be simple to be broken by an intruder. Attacks over the dedicated networks have range of possible methodologies which are discussed in the following section.

According to Christos Papadopoulos et al (2003) Denial of Service attacks can be segregated into two main categories namely flooding attacks and logic attacks. A specific node requires a bandwidth to communicate with the neighbouring nodes. Denial of service attacks when originated in 1990s targeted the bandwidth assigned for each system to block the services. As the space is already filled with meaningless packets from the attacker, the right packets could never find ways to reach the destination. With limited resources surplus bandwidth or alternative paths were limited. Without answering the legitimate requests, a server would result in receiving meaningless packets and finally shut down. Similarly a logic attack involves changes made in the original operative instruction set of the program and the whole system working in a improper manner.

As a network, requires a connection to be established between communicating nodes for starting their packets to traverse, a node sends a SYN packet to the server with a request packet.Yoohwan Kim et al (2003) uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. Depending on the availability of the destined node, server initiates the connection between these nodes. For all these requests, an acknowledgement will be sent between the participating nodes. An attacker takes advantage of the scheme to initiate source or request packets with unmentioned destination addresses. Based on the number of packets without a meaning, a server tries to withstand and finally shut down.

The SYN flood attack QiuXiaofengHao and Jihong Chen Ming (2004) sends TCP connection requests faster than a machine which can process them. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends. Instead of allocating a record, send a SYN-ACK with a carefully constructed Sequence number (seqno) generated as a hash of the clients IP address, port number, and other information. When the client responds with a normal ACK, that special seqno will be included, which the server then verifies. Thus, the server first allocates memory on the third packet of the handshake, not the first. However, the cryptographic hashing used in SYN cookies is fairly expensive, so servers that expect lots of incoming connections may choose not to use it.

An attacker with adequate knowledge on information of a network configuration can change his/her computer into a soft Access Point, making that node a gateway for the same. On the other hand, when a legal user intends to enter the network, the route passes through the newly created Access Point. Availing the login information from the users, attacker gains access to the private and confidential information of the participants. An Ad-hoc network has even simpler security measures to protect the contents of the network. The ability to connect to a network very easily is fascinating since a minimal set of rules have to be satisfied for connection establishment. Yet this simplifies the efforts of the attacker to enter illegally.

The most difficult part of detecting an attacker happens when a user will spoof the original IP and MAC address before forwarding the attack packets. Every packet holds the information of the sender, receiver, sequence number (which represents the path it travelled) updates the routers a packet crossed. With enough skills, an attacker will be able to masquerade the identity. When the server tries to trace the attacker, may end in accusing the wrong user or just end in vain. Tracing back an attacker is the next scheme in DoS attacks. Prevention and Detection schemes have evolved to

tracing back the attacker in order to limit the packets from the same path.

An attacker at the same time could act as an intermediate middle-man trying to accomplish the functions on behalf. When a SYN request reaches the attacker, it will direct towards a wrong destination or increase the traffic by routing a number of users to the same victim.

Spoofing is another serious threat to the security of a network. A packet in the open medium will hold an unencrypted IP address of the respective source, which enables an attacker to sniff the same for misbehaviour. An attacker will always wait for a good chance to enter stealthy into a network. With an unencrypted IP address, attacvker gets a invitation. The IP address could be replaced with the original IP of the attacker, fooling the server to believe that a legitimate user is entering into the network. Even a network provides a MAC filtering scheme for enabling protection, this scheme is decided by the range of access. A smaller network can efficiently implement the MAC filtering whereas a bigger network could not.

All the foreseen attacks have been concentrating on the intensive and selfish behaviour of an attacker to misuse the resources of a secure network. At the same time, attacker will access the personal information such as passwords, login information and other critical/sensitive information for a profit. The next category involve of bogus requests, imposters of successful connection requests/ messages or any other control messages sent to the server to block the intended services for other users.

A Denial of Service is the primary attack to be considered in this paper. The soluion proposed in this concept is to mark the packets with an unique signature including the IP address and the machine time of the source when the message is initiated.

An attacker sends forged Internet Control Message Protocol (ICMP) echo packets with the source address faked to appear at the address of the victim or as the broadcast addresses of vulnerable networks. All the systems on these networks reply to the victim with Internet Control Message Protocol (ICMP) echo replies. This rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users from the server. Similarly, User Datagram Protocol is a sessionless and connectionless networking protocol among systems requiring no framework for a connection for traversing data packets. Flooding can be achieved in UDP for achieving Denial of Service attacks.

A remote host will be receiving numerous UDP packets from a flood of nodes through a number of ports. The host will check for the application listening on that port and reply with an ICMP destination unreachable packet. Thus, for a large number of UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive

ICMP return packets do not reach him, and ensuring the anonymity of the attacker's network location(s).

This attack can be managed by deploying firewalls at key points in a network to filter out unwanted network traffic. The potential victim never receives and never responds to the malicious UDP packets because the firewall stops them. An Internet Control Message Protocol attack can come in many forms. There are 2 basic kinds, Floods and Nukes. An Internet Control Message Protocol flood is usually accomplished by broadcasting either a bunch of pings or UDP packets. The idea is, to send so much data to a system, that it results in significant performance degradation.

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from Uniplexed Information Interchange (UNIX) like hosts. It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

Nukes exploit bugs in certain Operating Systems, Like Windows 95, and Windows New Technology (Windows NT). The idea is to send a packet of information that the Operating System can't handle. Usually, they cause the system or its resources to lock up.

A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD). A Distributed Reflected Denial of Service Attack (DRDoS) involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target.

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) sends Echo Requests to the broadcast addresses of misconfigured networks, thereby enticing many hosts to send Echo Reply packets to the victim. Some early Distributed Denial of Service programs implemented a distributed form of this attack.

Many services can be exploited to act as reflectors, some harder to block than others. Domain Name Server (DNS) amplification attacks involves a new mechanism that increased the amplification effect, using a much larger list of DNS servers than seen earlier.

This describes a situation where a website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a

news story. The result is that a significant proportion of the primary site's regular users — potentially hundreds of thousands of people — click that link in the space of a few hours, having the same effect on the target website as a Distributed Denial of Service attack.

An example when Michael Jackson died in 2009, websites such as Google and Twitter slowed down or even crashed and their servers thought the requests were from a virus or spyware trying to cause a Denial of Service attack. Millions of people ―Googling‖ the star's name were greeted with an error page rather than a list of results – warning users that ―your query looks similar to automated requests from a computer virus or spyware application‖. Twitter.com crashed at least once and ran very slowly for some time. News sites and link sites — sites whose primary function is to provide links to interesting content elsewhere on the Internet — are most likely to cause this phenomenon.

Ping of death is caused by an attacker deliberately sending a ping packet. Many computer systems cannot handle an IP packet larger than the maximum IP packet size of 65,535, and often causes computer system crash. It is illegal to send a ping packet of size greater than 65,535, but a packet of such size can be sent if it is fragmented. When an attacker sends such packets, the receiving computer tries to reassemble the packet. This results in a buffer overflow, which often causes the operating system to crash or reboot. This exploit has affected a wide variety of systems including Unix, Linux, Mac, Windows and routers. An attacker may also send an Internet Control Message Protocol with Extraordinary Computer Handicapping Output (ECHO) request packet that is much larger than the maximum IP packet size to the victim. Since the received ICMP echo request packet is bigger than the normal IP packet size, the victim cannot reassemble the packets. The Operating System may be crashed or rebooted as a result.

This type of denial of service attack exploits the way that the Internet Protocol requires a packet that is too large for the next router to handle to divide it into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. When a large IP data packet is transmitted through a network, it is often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. At the receiver end the fragmented packets are reassembled based on the offset field to retrieve the original data packet.

The Teardrop program creates a series of IP fragments with overlapping offset fields. The attacker sends these mangled IP fragments with overlapping payloads to the target machine. These packets cannot be reassembled properly by manipulating the offset value of the packet. Attempts to re-assemble these packets with overlapping data can cause the operating system of the computer to crash or reboot if the software is not prepared to handle erroneous packet header

information. Many other variants such as targa, SYNdrop, Boink, Nestea Bonk, TearDrop2 and NewTear are available.

Proposed Solution:

SIGNATURE OR CERTIFICATE GENERATION USING SCAN PATTERNS

The need for people's privacy has paved way to secure data due to the growth of network communication and increase in security breaches. Cryptography enables us to store and transmit sensitive information across insecure networks, so that it won't be disclosed to anyone except the intended recipient. The proposed technique employs the processes of permutating the IP address using Scan patterns. Generating scan pattern should follow the upcoming constrains. They are:

- Pattern should exactly visit all the blocks in a matrix.
- Revisiting of the position should be avoided.
- Pattern should be difficult to trace back.

Pattern act as a symmetric key between two users. Symmetric means, both sender and receiver will use identical scan pattern to permutate and re-permutate the IP address and time. With the percentage of difficulty being introduced the much lesser chances to guess the randomly generated key.

In the first step the matrix is created of size 4X4. Then the sender IP address and time are given as input to the matrix. The same was arranged on the matrix in row wise. Then the scan pattern is applied on the matrix to permutate the IP address value along with the time. Generated key named to be IPTkey will be stored in IP header.

Receiver will arrange that IPTkey in 4X4 matrix in row wise. Scan pattern will be shared between the sender and the receiver. So receiver will also apply the same scan pattern on the matrix to get the original IP address and time. If this IP address is same as sender IP address then that packet is accepted. Otherwise the packet will be considered as unauthorized user data and it will be discarded. Time and resource consumption are considerably moderate with our experimental analysis. The randomness of the input increase based on the scan pattern. So it will be difficult for the attacker to spoof the IP address.

ALGORITHM:
Step 1: Get the input from user.
Eg: IP address – 192.168.255.240 & Time - 22 :46.
Step 2: Arrange the input in N x N matrix.

1	9	2	1
6	8	2	5
5	2	4	0
2	2	4	6

Step 3: Apply the Scan pattern on the matrix to permutate the matrix values.
Eg: Applying 'd' Scan Pattern on the input matrix.

1	**9**	**2**	**1**
6	**8**	**2**	**5**
5	**2**	**4**	**0**
2	**2**	**4**	**6**

Step 4:

Encrypt(IP; T; N)

Inputs: IP address IP , Time T, Matrix size N × N (N = 4).
Output: Hexa Decimal values H.
{
//get IP and T in an array named as input[]
for(condition){
for(condition){
inputmatrix[][]=input[];//convert 1-D array into 2D array
}}
for(condition){
for(condition){
//permutate input matrix using Scan path until all the positions are visited exactly once. }}

//read 2 digits from a permutated matrix and convert it into hexa decimal format. Repeat the process until all the values are read from the matrix
}

Every packet is authenticated with a signature. The signature is registered in three nodes. It is a register of packets passing to/fro.

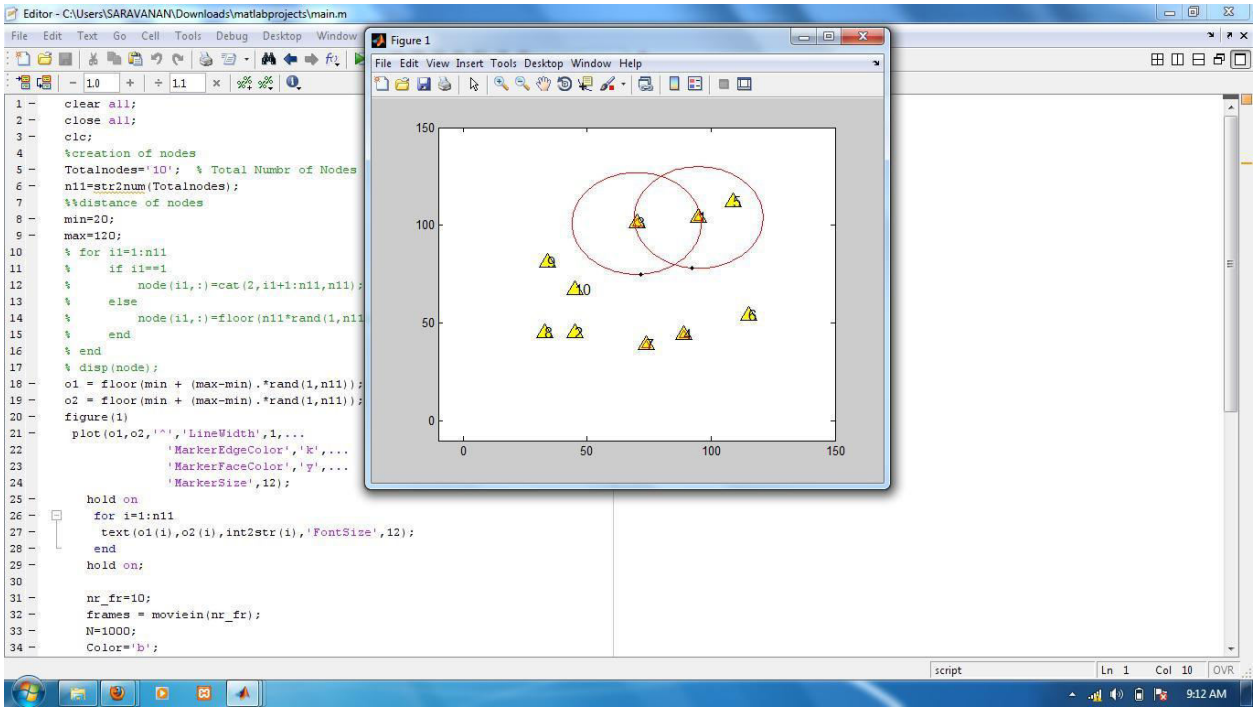
The first node(sender) sends the message with a signature to the destination. Every intermediate node will check the signature which identifies the original set of packets and no attack can be made in between.

Every packet with the signature is considered to be a legitimate packet. Every node confirms with the previous and succeeding node about the presence of the signature in each packet.

Without the signature, the packets are discarded for security reasons. It involves changes in the TWO PHASE COMMIT protocol.

Number of verifications may seem to impose a stress over network performance yet, it can be developed only after simulated results are obtained.

Nodes Communication within an internal organisation



Conclusion:

In order to facilitate Distributed Denial of Service, the attackers need to have several hundred to several thousand compromised hosts. The process of compromising a host and installing the tool is automated and involves the following steps: A client finds one or more systems on the Internet that can be compromised and exploited. This is generally accomplished using a stolen account on a system with a large number of users and / or inattentive administrators, preferably with a high-bandwidth connection to the Internet. The compromised system is loaded with any number of hacking and cracking tools such as scanners, exploit tools, operating system detects, root kits, and Denial of Service / Distributed Denial of Service programs. This system becomes the DDoS handler.

REFERENCES

[1] Qinghua Li, Guohong Cao, ―Mitigating Routing Misbehavior in Disruption Tolerant Networks‖, IEEE Transactions On Information Forensics And Security, , Vol. 7, No. 2, April 2012.

[2] D. Johnson, D. A. Maltz, and Broch. ― The Dynamic Source Routing Protocol for Mobile Ad Hoe Networks ‖, Mobile Ad-hoc Network (MANET) Working Group, IETF, , October 1999.

[3] F. Li, A. Srinivasan, and J. Wu, ―Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets‖, in Proc. IEEE IN-FOCOM , pp. 24282436.2009

[4] H. Yang, J. Shu, X. Meng, and S. Lu, ―Scan: Self-organized network-layer security in mobile ad hoc networks‖, IEEE J. Sel. Areas Commun.,vol. 24, no. 2, pp. 261273, 2006.

[5]J. Burgess, B. Gallagher, D. Jensen, and B. Levine, ―Maxprop: Routing for vehicle-based disruption-tolerant networks,‖ in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.

[6] J. Burgess, G. D. Bissias, M. Corner, and B. N. Levine, ― Surviving attacks on disruption- tolerant networks without authentication‖, in Proc. ACM MobiHoc,, 2007, pp. 6170.

[7]J. P. Hubaux, T. Gross, J.-Y.LeBoudec, and M. Vetterli, ―Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project,‖ IEEE Comm. Magazine, Jan. 2001.

[8] K. Fall, ―A delay-tolerant network architecture for challenged internets‖, in Proc. SIGCOMM, 2003, pp. 2734.

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ― An acknowledgment-based approach for the detection of routing misbehavior in MANETs ‖, IEEE Trans. Mobile Comput. , vol. 6, no. 5, pp. 536550, May 2007.

[10]L. Buttyan and J.-P.Hubaux, ―Enforcing Service Availability in Mobile Ad-Hoc WANs,‖ Proc. MobiHoc, Aug. 2000.

[11]M. Jakobsson, J.-P.Hubaux, and L. Buttyan, ―A Micropayment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks,‖ Proc. Financial Cryptography Conf., Jan. 2003.

[12] Q. Li, W. Gao, S. Zhu, and G. Cao, ― A routing protocol for socially selfish delay tolerant networks‖, in Ad Hoc Networks, ,Aug. 2011, DOI: 10.1016/j.adhoc.2011.07.007.

[13]S. Buchegger and J.-Y. Le Boudec, ―Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,‖ Proc. MobiHoc, June 2002.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ― Mitigating routing misbehavior in mobile ad hoc networks‖, in Proc. ACM MobiCom,2000, pp. 255265