Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection of Denial of Service attacks on Mobile Internet Protocol Nodes

P.Sanjeevi[1]
Student M.S Software Engg,
VIT University,
vellore-632014.
TamilNadu, India.

M.K.Nallakaruppan[2] **&U.SenthilKumaran**[3]
Asst professor,
VIT University,
Vellore-632014.
TamilNadu, India.

M.Ram Murali[4]
Asst professor,
R.V.S.College of Engg.&Tech.
Dindigul-624005.
TamilNadu, India.

Abstract— DDoS (Distributed denial of service) attacks are the most common network attacks that had caused a serious economic loss so it is has to been stopped as early as possible to protect network damage. Earlier solutions for this problem are based on port-hopping between pairs of processors which are synchronous or exchange acknowledgments .Our main aim is to detect the malicious connection from the normal ones by using decision tree analysis and protect the server from attackers .In this paper we understand the packet flow ratio from normal connections and then from abnormal situation if the ratio of the packet flow differs from the normal ratio we distinguish normal and malicious connections.

Key words: Internet, Security, IP traceback, DoS, DDoS, IP spoofing.

1.Introduction

The main aim is to detect the malicious connections from the normal ones and there is no need to modify particular protocols.We have to design a system that should fit in any network topology and the traceback procedure should be efficient.Major categories of attacks during 2006 were viruses insider abuse of access unauthorised access of DDoS attacks. However, attackers can also take of a service from using that service by flooding messages to the corresponding server, which forms a Denial of Service these advantages to prevent legitimate users (DoS) attack.

A. DDoS

There are several types of such attacks. An attacker can possibly launch a DDoS attack by studying the flaws of network protocols or applications and then sending malformed packets which might cause the corresponding features of the Internet, openness and protocols or applications getting into a faulty state. DDoS attacks are classified into flodding and logic attacks.
In flooding attack the victim is overloaded with a large amount of traffic thus consuming resourses. Examples of flooding attacs is the TCP/SYN flooding. Logic attacks are however based on exploiting the vulnerabilities in the target system and can be carried out even with a single well packet.

B. IP Traceback

In DoS/DDoS attack, attacker uses fake source IP addresses to make tracing and stopping of DoS difficult. This technique is called IP spoofing. This technique involves the manipulation of the source IP address in the IP header of a transmitted packet. This gives the attacker a form of anonymity. It is difficult to solve problem of IP Spoofing because of lack of security features in TCP/IP specifications. Use of cryptographic authentication , IP trace back are some of the approaches used to handle forged IP source addresses . The purpose of IP traceback is to identify the true IP address of a host originating attack packets. IP trace back is vital for quickly restoring normal network functionality and preventing reoccurrences.

C. Existing IP Traceback Technique

There is no intrinsic support to identify the real sources of IP packets in the Internet architecture, so different techniques have been proposed to provide traceback capability. Existing trace back schemes can be roughly categorized into three distinct

categories they are traditional, marking and logging. In traditional scheme, victim develops an attack signature, consisting of some data common and unique to the attack traffic. A query including the attack signature is then sent hop-by-hop to each router along the path.

II. RELATED WORK

There are many network-based solutions against DDoS attacks. These solutions usually use routers or overlay networks to filter malicious traffic. In this paper, we focus on application-based mitigation. The propose an ack-based protocol focusing on the communication only between two parties, modeled as sender and receiver. The receiver sends back an acknowledgment for every message received from the sender, and the sender uses these acknowledgments as signals to change the destination numbers of its messages. Since this protocol is ack-based, time synchronization is not necessary.

A. System Model Definition

We focus on the problem that an adversary wants to subvert the communication of client-server application by attacking their communication. We assume that there exists a preceding authentication procedure which enables the server to distinguish the messages from the legitimate clients. We also assume that every client is honest which means any execution of the client is based on the protocol and clients will not reveal the random function to the adversary.

III.Proposed System Architecture

In this section, we will present the proposed detection and traceback system. It includes an artificial intelligence based (AI-based) classifier for DDoS detection and a traffic-flow pattern matcher for comparing traffic signatures and for tracing back DDoS attacks.We propose an ack-based port-hopping protocol focusing on the communication only between two parties, modeled as sender and receiver.The aim of all the traceback approaches is to identify the sources of attacking traffic but path reconstruction algorithms actually reveal the identity of first router on the path. A better approach would be to find an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path. The receiver sends back an acknowledgment for every message received from the sender, and the sender uses these acknowledgments as signals to change the destination port numbers of its messages. Since the attacker can forge any field in the IP header, he can't falsify the Time to live (TTL) field. The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Each router decrements the TTL value by 1, after forwarding the datagram. The problem of determining the first router on the path can be solved by using this field. Thus, even though the attacker can launch the directed attack due to the lost of acknowledgment packets, the sender and receiver can continue the communication by reinitializing the protocol.

IV.Blacklist Extraction And Updation

The flooding DoS attack uses IP spoofing. The problem of this Source address spoofing can be solved by a technique called Ingress Filtering, in which the router discards the packets with illegitimate source addresses. The extraction of source address can be checked from the network id part of the IP address. A serious limitation of this technique arises when the attacker forgets the address to the one that belongs to the same network as the attacker's host and updates the attackers host.

V. Algorithm

Step 1:The algorithm used here is path reconstruction algorithm for the purpose of faster convergence and capability of tracing any type of DoS attack

Step 2:Path reconstruction algorithms actually reveal the identity of first router on the path. A better approach would be finding an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path.

Step 3:Since the attacker can forge any field in the IP header, he can't falsify the Time to live (TTL) field. The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Each router decrements the TTL value by 1, after forwarding the datagram. The problem of determining the first router on the path can be solved by using this field.

VI. Performance Evaluation

Network Simulator (ns-2.31) at network layer to measure the delay for the marked traffic as compared to the normal (unmarked) traffic. The simulator was running on an Intel based machine having 1.7 GHz processor and 512 MB of main memory. The internal files of ns-2.31 were modified to incorporate packet marking in it. The simulated topology is shown in

figure 1. The size of the topology doesn't matter because all the delay incur at the first router only. Traffic originated from node 0 and was destined for node 30.

3. For this traffic, node 0 acts as the first router on the path. Traffic consisted of TCP packets of 1040 bytes carrying FTP data. The additional time taken by marked traffic is just 0.8 milliseconds. Similar delay is also observed.

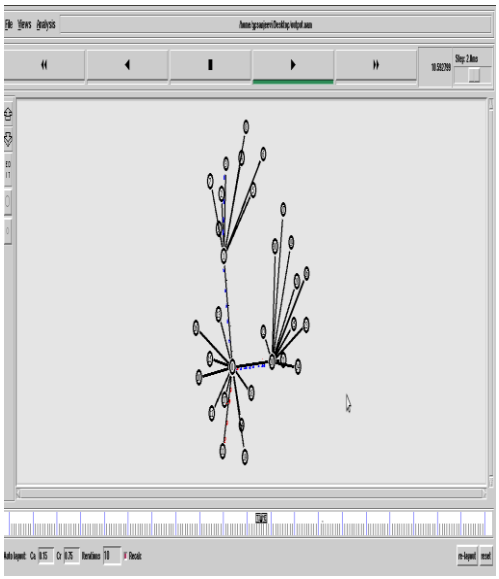

Figure 1 Nam Simulation for DDoS Detection Scenario**D. Packet Distribution With Blacklist Identification**

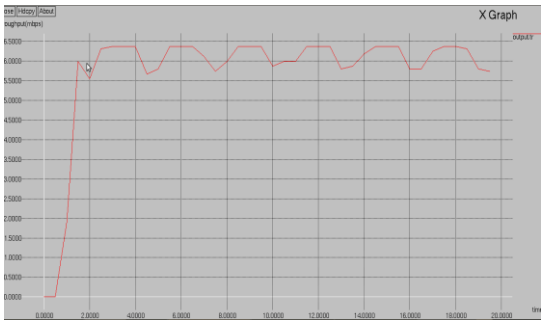

Figure 2 Performance chart for packet throughput with DDoS Detection

VII.TRACEBACK RATIO

The traceback mechanism is calculated using now [expr $bw0/$time*8/261000] and is shown in Table 1

Table 1 shows the traceback file.

1	1.915095785440613
1.5	5.9929501915708814
2	5.5466666666666669
2.5	6.3117241379310345
3	6.3754789272030647
3.5	6.3754789272030647
4	6.3754789272030647
4.5	5.6741762452107283
5	5.3754789272030647
5.5	6.3754789272030647

VIII. Conclusion

The development of IP traceback techniques is motivated by different DDoS attacks in recent years. With the development of traceback technique, more complex DoS attacks can be launched. However, IP traceback is the first step in identifying the attacker behind the attacks. The effectiveness of any traceback technique depends primarily on its overhead, convergence and the ability to trace any type of DoS attack. The DDoS traceback technique presented here is capable
of tracing any type of DoS attack because we can trace even a single packet. Today there is a need of practical implementation of an effective technique so that IP traceback could be carried out in real time across the internet.

Reference

[1] M. Papatriantafilou, and P. Tsigas, "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts," Proc. IEEE Int'l Symp. Reliable Distributed Systems (SRDS), Oct. 2008.

[2] CERT Advisory CA-1997-28 IP Denial of Service Attacks.

[3] K. Argyraki and D.R. Cheriton, "Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks," Proc. Ann. Conf. USENIX Ann. Technical Conf. (ATEC '05), p. 10, 2005.

[4] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling High Bandwidth Aggregates in the Network," ACM SIGCOMM Computer Comm. Rev., vol. 32, no. 3, pp. 62-73, 2002.

[5] D. Dean, M. Franklin, and A. Stubblefield, "An Algebraic Approach to IPTraceback," ACM Trans. Information and System Security, vol. 5, no. 2, pp. 119-137, 2002.

[6] D.X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," Proc. IEEE INFOCOM, vol. 2, pp. 878- 886, 2001. 412 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 3, MAY/JUNE 2012

[7] S. Savage, D. Wetherall, and T. Anderson, "Practical Network Support for IP Traceback," ACM SIGCOMM Computer Comm. Rev., vol. 30, no. 4, pp. 295-306, 2000.

[8] X. Liu, Yang, and Y. Lu, "To Filter or to Authorize: Network- Layer DoS Defense against Multimillion node Botnets," Proc. SIGCOMM, pp. 195-206, 2008.

[9] A.D. Keromytisand D. Rubenstein, "SOS: Secure Over Services," ACM SIGCOMM Computer Comm. Rev., vol. 32, no. 4, pp. 61-72, 2002.

[10] D.G. Anderson, "Mayday: Distributed Filtering for Internet Services," Proc. Fourth Conf. USENIX Symp. Internet Technologies and Systems (USITS '03), p. 3, 2003.

[11] X. Fu and J. Crowcroft, "GONE: An Infrastructure Overlay for Resilient DDoS-Limiting Networking," Proc. Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2006.

[12] A. Stavrou and A.D. Keromytis, "Countering Dos Attacks with Stateless Multipath Overlays," Proc. 12th ACM Conf. Computer and Comm. Security , pp. 249-259, 2005 .

[13] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial of Service with Capabilities," Proc. Workshop Hot Topics in Networks (HotNets-II), Nov. 2003.

[14] A. Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks," Proc. IEEE Symp. Security and Privacy, pp. 130-143, 2004.

[15] X. Yang, D. Wetherall, and T. Anderson, "A DoS-Limiting Network Architecture," Proc. ACM SIGCOMM, Aug. 2005.

