1. Introduction

随着网络的应用越来越广泛，随之而来的网络安全问题成为了互联网发展的主要障碍。拒绝服务攻击（简称DoS）是一种利用网络协议的缺陷和系统存在的漏洞，对网络设备进行攻击进而导致网络或系统瘫痪而停止提供正常网络服务，即“拒绝服务”。分布式拒绝服务攻击（DDOS）是分散在网络各处的机器共同完成对一台主机的攻击操作，更具有危害性。目前，DDoS攻击已经成为一种遍布全球的系统漏洞攻击方法，很多商业站点和政府部门被DoS攻击所困扰，造成巨额经济损失。因此，如何有效的预防以及阻止DoS攻击对网络用户特别是网络管理人员有着十分重要的意义。文献[1]指出，基于TCP协议的DoS攻击占所有DoS攻击的90%-94%。本文就SYN泛洪进行了研究并提出了一种可行的防御方法。

With the increasing application of network, accompanying network security issues have become a major obstacle to the development of internet. Denial of service (DoS) is an attack on network devices exploiting defects of network protocol and vulnerabilities of system which renders network or system unavailable, namely, a denial of service. A distributed denial of service (DDoS) is an attack on a host orchestrated by multiple computers scattered in a network, which is more harmful. Currently, DDoS has become a worldwide attack method exploiting vulnerabilities of system. Many business sites and government departments have been targeted by DoS and thus suffered huge economic losses. Therefore, it makes good sense to effectively prevent and stop DoS on network users, especially network managers. As indicated by literature[1], TCP-based DoS accounts for 90%-94% of all DoS. This paper conducted a research on SYN Flood and proposed a feasible defense method.

2. SYN Flood攻击是最常见也是最有效的DoS攻击手段，要了解这种攻击的原理，需要从建立TCP连接的三次握手过程开始说起。第一次握手：主机发送一个包含SYN（Synchronize）标志的TCP报文给服务器告知其使用的端口以及TCP连接的初始序号。第二次握手：当服务器收到主机的SYN请求包之后，给其返回一个SYN+ACK（Acknowledge）包。第三次握手：主机收到SYN+ACK包后，向服务器发送一个ACK包。至此三次握手过程顺利完成，连接被建立。

SYN Flood is the most common and the most effective DoS form. This paper begins with TCP three-way handshake for connection establishment to understand the principle of SYN Flood. The first-step handshake process: a host sends a TCP message including a SYN (Synchronize) to a server, informing it of port and initial sequence number for TCP connection. The second-step handshake process: In response, the server replies with a SYN+ACK (Acknowledge). The third-step handshake process: after receiving the SYN+ACK, the host sends an ACK to the server. At this point, connection is established.

假如一个主机向服务器发送了SYN报文之后突然死机或者掉线，那么服务器在发出SYN+ACK的应答报文之后是不能够收到ACK确认报文的。发生这种情况时，服务器通常会重新发送报文并等待一段时间后丢弃这个未完成的连接，称为半连接握手状态。

If the host suddenly crashes or goes offline after sending a SYN message to the server, the server cannot receive an ACK acknowledgment message after sending a SYN+ACK message. In this circumstance, the server will usually resend a message and abandon unfinished connection after waiting a period of time, which refers to half-open connection.

攻击者通过伪造IP地址发送TCP连接请求，如果伪造的IP地址确实有人使用，那么在收到服务器发送的SYN+ACK报文后会发送一个RST报文来告知服务器不需要等待一个无效的连接。可如果伪造的IP地址无人使用，服务器将会不断重试直到SYN Timeout时间后才丢弃该连接(TCP协议的漏洞就在于此)。在攻击中(In an attack)攻击者会向服务器发送大量SYN请求(SYN requests)，并且对于ACK确认报文不予回应，导致出现了大量处于半握手状态的连接。这会使得服务器忙于处理伪造的TCP连接请求而无暇顾及正常用户的请求，更严重将会造成堆栈溢出，服务器崩溃。

An attacker sends a TCP connection request using a forged IP address. If the forged IP address is occupied, after a SYN+ACK message sent by the server is received, a RST message will be sent to inform the server that there is no need to wait for an invalid connection. If the forged IP address is not occupied, the server will continuously retry within SYN Timeout value before abandoning the connection (a vulnerability of TCP protocol). In an attack, an attacker sends multiple SYN requests to the server but does not respond to ACK acknowledgment message, which results in many half-open connections. The server is busy with processing falsified TCP connection requests and has no spare time for requests of legitimate users. In severe cases, stack overflow and server crash will be caused.

目前针对SYN泛洪有几种简单有效的应对策略。第一种是缩短SYN Timeout时间。服务器可以保持的最大半连接数量为

最大半连接数量=SYN攻击频率\*SYN Timeout

通过缩短SYN Timeout数量，使得主机尽快释放半连接的资源占用，成倍地降低服务器负荷。这种方法的缺点是当SYN Timeout被缩短以后，客户的正常访问也可能会受到影响。

At present, there are a couple of simple and effective countermeasures to SYN Flood. The first is to reduce SYN Timeout value. Max. quantity of half-open connections which can be maintained by a server

Max. quantity of half-open connections = SYN attack frequency \* SYN Timeout

By reducing SYN Timeout value, a host will release resources occupied by half-open connections as soon as possible, so that server load will be reduced

exponentially. The disadvantage of this method is that when SYN Timeout value is reduced, visit of legitimate users may be affected.

第二种方法是采用SYN Cookie技术。服务器加密生成一个序号而不去记忆序号（sequence number）。当第三次握手时，客户端返回的ACK报文的序号是该加密初始序号加1。此时服务器运行相同的加密算法重新生成正确序号，若与ACK报文序号匹配则建立连接[3]。这种方法的缺陷在于服务器为了验证客户端ACK报文的有效性要进行很多次杂凑运算，而该算法复杂度较高，被攻击时会占用大量的RAM和CPU资源。由此缺陷，黑客们可以针对性地发起ACK Flood攻击。[2]

The second is to adopt SYN Cookie technique. A server will generate an encrypted sequence number instead of memorizing a sequence number. In the third-step handshake process, the sequence number of ACK message returned by the client is the encrypted initial sequence number plus 1. At this point, the server will run the same encryption algorithm to regenerate correct sequence number. Connection will be established if the regenerated sequence number is matching to the sequence number of ACK message[3]. The disadvantage of this method is that the server has to perform hash operations for many times in order to validate the effectiveness of ACK message returned by the client. Hash algorithm has high complexity and will occupy a considerable amount of RAM and CUP resources when attacked. A hacker can wage a targeted ACK Flood attack exploiting this defect. [2]

接下来将介绍一种基于服务器的防御方法，针对性地解决了上述两种常用方法的缺陷。通过对SYN报文两次接收，对连接请求进行筛选，从而防御了DoS攻击。

One of server-based defense methods is introduced as below, which has been designed to address the shortcomings of the aforesaid two commonly used methods. By receiving two same source SYN messages and screening connection requests, DoS will be blocked.

3. Application

同源SYN报文是指源地址和源端口都和另外一个SYN报文相同并且请求同一个服务器的相同服务的SYN请求报文，记做SYN1和SYN2。这个方法的原理是客户端在发送SYN之后一段时间内没有收到ACK确认回应，就会超时重传一个新的SYN连接，所以一定时间内服务器就会收到两个相同源地址和端口号的SYN报文。当服务器第一次接收到SYN报文时，不回复ACK，继续在规定时间内等待第二次重传的SYN报文，通过时间差判断是否为合理的正常请求。

Two same source SYN messages refer to two SYN messages have the same source address and source port, which request the same service from the same server. The two SYN messages are respectively marked as SYN1 and SYN2. The principle behind this method is that if the client doesn’t receive ACK acknowledgement within a certain period of time after the client sends SYN, the client will retransmit a new SYN connection after timeout. As a result, the server will receive two SYN messages with the same source address and port number within a certain period of time. When the server receives the first SYN message, it will not respond with ACK, waiting for the second SYN message, and judge whether the request is legitimate based on time difference.

如何设置合理的时间段就成为了关键所在。首先定义重传时间差

x=第二次接受SYN2包的时间-第一次接受SYN1包的时间。

合理时间段为X={x|Tmin<x<Tmax}。其中Tmin是重传时间差的最小值，定义为服务器端系统超时重传的时间（一般为几秒钟）。Tmax是重传时间的最大值，定义为服务器端系统超时重传时间的两倍。

Therefore, it’s crucial to set up reasonable time period. Firstly, retransmission time difference is defined

X = the time when SYN2 packet is received for the second time - the time when SYN1 packet is received for the first time

Reasonable time period X = {x|Tmin<x<Tmax}, in which Tmin refers to min. value of retransmission time difference, which is defined as the time of timeout retransmission of the server (generally several seconds). Tmax refers to max. value of retransmission time, which is defined as double of the time of timeout retransmission of the server.

因此可以得到：

As a conclusion:

合理的连接请求需要满足以下条件：

A reasonable connection request needs to satisfy the below conditions:

同时满足以上三个条件的SYN报文才能进入三次握手，其余的SYN请求一律丢弃，只将源地址和接收时间保存到重传时间Tmax后清理。不同于普通DoS的一个地址发送大量的SYN连接请求，DDoS攻击会使用不同的IP和端口来发送SYN报文,而同源SYN报文两次接收法可以有效断定是否是DDoS恶意攻击。

Only SYN message which satisfies the above-mentioned three conditions can enter the third-step handshake process, while other SYN requests will be abandoned with only source address and reception time saved to retransmission time Tmax. In DDoS, different from DoS in which superfluous SYN connection requests are sent using an address, SYN messages are sent using different IP and ports. The method of receiving two same source SYN messages can effectively judge whether there is a DDoS malicious attack.

接下来将详细介绍如何实现接收并记录两次SYN报文。首先建立一个开散列HASH表，用这个表来记录客户端第一次发送的SYN报文。然后把32位源IP地址的16位端口号作为关键码来确定一个合适的HASH函数。因为攻击方通常使用随机函数来伪造自己的IP源地址，所以使用

As shown below, this paper introduces in details how to receive and record two same source SYN messages. Firstly, a HASH table is created to record SYN message sent from the client for the first time. Secondly, a HASH function is determined with 16-bit port number of 32-bit source IP address as a key. In consideration that an attacker usually uses an random function to forge its IP source address,

其中s代表输入是48位的源IP地址和源端口号码。每个HASH表节点存储源IP以及端口和时间等内容。

In which, “s” refers to 48-bit source IP address and source port number. Each HASH table node stores contents such as source IP, port and time.

通过HASH表占用内存总量的使用比率η，得出以下公式：

The below formula can be concluded usingη(usage ratio of total memory) of the HASH table:

根据服务器端的专家给出的最佳使用比率η，我们得到了HASH表更新时间T。以T秒为周期，对HASH表进行遍历，释放超时的节点空间，来防止HASH表的溢出。

Based on the optimumηgiven by experts from the server side, update time T of HASH table can be achieved. With a cycle of T seconds, traverse the HASH table to release space of timeout nodes so as to prevent the overflow of HASH table.

如果服务器没有过载，那么说明并未收到攻击，正常进行三次握手就可以了。如果服务器过载，那就启用该方法，将每次收到的SYN报文查看是否已经存入在HASH表内。那么会遇到以下三种情况：

1. HASH表内无该SYN记录，那么就建立新记录，并丢弃这个SYN报文

2. HASH表内有该SYN记录，时间差不在合理范围内，丢弃该SYN请求，同时将HASH表内记录的时间更新。

3. HASH表内有该SYN记录，时间差在合理范围内，判断为正常的连接请求，开始执行三次握手协议，然后将HASH表内的接点空间释放。

If the server is not overloaded, it means an attack has not been received. Go through TCP three-way handshake process as normal. If the server is overloaded, use this method to check if each SYN message received has been stored in the HASH table. The below three circumstances exist:

1. If there is no record of the SYN in the HASH table, establish a new record and abandon the SYN message

2. If there is a record of the SYN in the HASH table, but time difference falls out of a reasonable scope, abandon the SYN request and update the time recorded in the HASH table.

3. If there is a record of the SYN in the HASH table, and time difference falls within a reasonable scope, a legitimate connection request is determined. In such case, go through TCP three-way handshake process and release node space in the HASH table.

4. 方法总结

Method Summary

若无遭到SYN Flood攻击，服务器正常工作。若遭到攻击，在遇到各种情况下该方法都表现良好：

If a SYN Flood attack has not been received, a server functions normally. If such an attack is received, this method works in various circumstances:

1. 攻击方用相同的伪装IP地址连续发送SYN包再重新伪装IP地址。这种连续SYN发送时间差显然小于合理时间段X。每次收到SYN后服务器将丢弃该包并更新HASH表中的时间，不进入半连接状态，方法成功。

An attacker continuously sends SYN packets using a forged IP address and then forges an IP address again. Time difference of sending continuous SYN is obviously less than reasonable time period X. The method works because a server abandons a SYN packet after receiving it each time and updates the time in a HASH table. In other words, no half-open state of connection exists.

2. 攻击方不连续发送SYN报文直接更换IP地址。服务器丢弃SYN包，HASH表超时更新。如果伪装IP经长时间后循环使用，显然时间差大于正常间隔，方法成功。

An attacker discontinuously sends SYN messages and directly changes IP addresses. A server abandons SYN packets and a HASH table is updated after timeout. The method works because if an forged IP is reused for a long time, time difference is obviously larger than normal interval.

该方法有效抵御了SYN Flood攻击并弥补了之前提到的方法的不足。策略简单，不需要复杂的计算，消耗系统资源较少。

This method effectively blocks a SYN Flood attack and addresses the shortcomings of the aforesaid methods. Its advantages lie in simple strategy and calculation as well as low consumption of system resources.

5. 结论

Conclusion

本文首先介绍了DoS攻击并详细分析了SYNFlood的一般攻击流程与方式，同时引入了当前两种被广泛使用的防范SYN Flood的方法。接下来详细解释SYN报文两次接收法，先设置正常时间间隔范围，再使用HASH表记录接收SYN报文的时间，与正常时间间隔比较，以决定是否抛弃该SYN报文，有效的防止了DDoS攻击。最后将该方法和两种常见DDoS防御方法进行优缺点比较。

This paper first introduces DoS and analyzes in detail general attack process and form of SYN Flood. Besides, two methods, which are widely used nowadays to prevent SYN Flood, are introduced. This paper then explains in detail the method of receiving two same source SYN messages. In this method, normal time interval is first set up, a HASH table is then adopted for recording reception time of SYN messages and whether SYN messages should be abandoned is determined after comparing reception time with normal time interval, which effectively prevents and blocks DDoS. In the end, the paper compares this method with other two commonly used methods in terms of advantages and shortcomings.

提高计算机用户的安全意识，是抵御DDoS攻击的简单有效的方法。及时弥补操作系统的漏洞，更新网络安全设备和软件。以此来隔离恶意软件进攻，从而减小DDoS攻击发生的规模。

A simple and effective method to prevent and block DDoS is to increase safety awareness of computer users. Vulnerabilities of operating system should be timely patched and network security devices and software should be updated so that malicious software attacks can be blocked and DDoS scale can be reduced.