第34卷 第19期 计 算 机 工 程 2008年10月
Vol.34 No.19 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)19—0141—03 文献标识码：A 中图分类号：TP309

基于数据包标记的伪造 IP DDoS 攻击防御

冯庆云，曲海鹏，周 英，郭忠文
(中国海洋大学计算机系，青岛 266100)

摘 要：提出一种基于数据包标记的伪造 IP DDoS 攻击防御方案，该方案在 IP 数据包中嵌入一个路径相关的 16 位标识，通过检测标识计数器临界值判断是否发生了 DDoS 攻击，对伪造地址的 IP 数据包进行过滤，达到对 DDoS 攻击进行有效防御的目的。仿真实验表明，该方案对于伪造的 IP 数据包具有较高的识别率。

关键词：分布式拒绝服务攻击；数据包标记；伪造 IP

Packet Marking Scheme to Defend Against Spoofed IP DDoS Attack

FENG Qing-yun, QU Hai-peng, ZHOU Ying, GUO Zhong-wen
(Department of Computer, Ocean University of China, Qingdao 266100)

【Abstract】 A new packet marking scheme is proposed, in which a path identification that represents the route an IP packet has traversed is embedded in each IP packet. And a counter is set for each identification. It represents the number of different IP addresses that have the same identification. The onset of a spoofed DDoS attack can be detected by comparing the sum of the counters with a marginal value that has been set. Spoofed packet can be filtered so as to sustain the quality of protected Internet services. Experimental results show that the proposed scheme is efficient on identifying the spoofed DDoS attack packets.

【Key words】 Distributed Denial of Service(DDoS) attack; packet marking; spoofed IP

1 概述

随着网络技术与应用的发展以及网络对社会、经济和人们日常生活影响的逐步深入，大量网络安全事件的发生引起了广大网络用户对网络安全的广泛关注，网络安全问题也变得越来越重要。拒绝服务攻击是一类常见的攻击，近年来已成为最为严重的网络威胁之一，其中尤以分布式拒绝服务(Distributed Denial of Service, DDoS)攻击危害最大。它的主要目的是降低目标网络的服务质量或者通过不断加重系统资源(如带宽、路由器处理能力或 CPU/存储器)的负载，中断与服务器的连接。

对 DDoS 攻击数据包的识别是攻击防御中难以解决的问题之一。由于因特网路由协议本身的弱点，目前尚没有任何方法保证源地址的正确性。因此，IP 地址伪造技术给拒绝服务攻击的防御提出了严重挑战，它使得在现有的网络条件下，识别和阻止伪造的 IP 数据包变得更为困难。再者，攻击者可以轻易地模拟具有请求目标主机服务特征的数据包，使得受害者无法根据数据包的内容区分合法数据包和恶意数据包。

2 相关工作

近年来，研究者们已经提出了很多的防御措施[1-4]。文献[1]继承了路由器标记数据包的思想，当有数据包经过该路由器时，将代表该数据包的标记填充到IP首部的16位标识域中，然后在目标主机进行存储。对于每个到达的IP数据包，在目标主机中提取标记和源IP地址，以该IP地址检索表，若存在该IP地址，将两者的标记进行比较，如果两者不相同，则判断该数据包为攻击包，但是它存在几个缺点：(1)到达主机的新数据包采取的探测路径标识的措施本身会导致DDoS攻击；(2)因为伪造的IP都是随机的，当攻击发生时，会有大量新的数据包达到目的主机，而此时主机的服务已经受到严重影响，再采取路径探测方法判断数据包的合法性是不可能的；(3)16位IP标识域中，5位用来存储数据包经过的路由跳数，11位用于路径标识，对于5位的距离域，攻击者可以利用traceroute得到源主机和目的主机之间的距离，那么只剩下11位的空间存储路径标识，这就比用16位存储增加了碰撞率。文献[2]提出的过滤机制可以减轻攻击的力度，但需要大大增强路由设施，而且路由器上的过滤相当复杂，同时还要有ISP之间的协作。IP追踪方案[3-4]集中识别伪造DDoS的攻击源，但并不能使受害者立即对攻击作出响应。文献[3]中利用IP追踪技术可以构造出攻击路径，但路径的重构需要大量的数据包，并且计算复杂度高，运算量大。针对随机伪造的IP DDoS攻击，文献[4]提出了基于路由跳数的方案，它的前提是假设大部分伪造IP数据包的跳数都是不一样的，通过提取TTL域的值，就可以判断出伪造的IP包，然而，这一前提假设没有考虑到攻击者可以利用traceroute技术得到源主机和受害主机的跳数值。

本文提出一种基于数据包标记的 DDoS 攻击防御方案，该方案利用 IP 首部中的 16 位标识字段存储路径标识，并采用链表的形式存储标记和源 IP 地址。在目标主机处，为每个路径标识设置计数器，计算相同标识的不同源 IP 的数目。在攻击发生时，当到达主机的数据包标记与计数器最大值对应

基金项目：国家“863”计划基金资助项目(2006AA09Z113)
作者简介：冯庆云(1981－)，女，硕士研究生，主研方向：信息安全，网络安全；曲海鹏，讲师、博士；周 英，硕士研究生；郭忠文，教授、博士
收稿日期：2007-11-15 **E-mail：**quhaipeng@ouc.edu.cn

的标记相同时，判断此包为恶意包，并将其丢弃，从而保证主机服务的可用性。

3 基于数据包标记的伪造 DDoS 攻击的防御方案

3.1 数据包标记算法

为了能对数据包地址进行鉴别，实施防御方案的路由器网络接口都分配有一个 n 位的随机秘密串。在实施防御的主机上建立一个表(M-Table)，用于存储到达数据包的标记与 IP 地址的对应关系。

当 IP 数据包经过路由器时，由路由器对其进行标记。标记包括 2 部分：1 位标志位 flag 和 16 位路径标识 PathID，flag 和 PathID 分别存储在 IP 包头的保留位和 Identification 域中。

当路由器收到IP数据包时，首先检查flag域，如果该位为0，说明此路由器是IP数据包所经过的第 1 个路由器，置flag为 1 并将 16 位的PathID置为该路由器网络接口的n位随机数；若flag域为 1，路由器用H(ID,N_j)更新 16 位的PathID域，ID为当前IP数据包的 16PathID域的值，N_j表示该路由器网络接口的随机数，H为哈希函数，路径标识的过程见算法 1，其中，p表示经过路由器的IP包；p.flag 和p.id 表示该IP包的flag和PathID；N_j表示路由器分配的随机秘密串。

算法 1 路径标识算法

```
if p.flag==0 then
p.flag=1
p.id=Nj
else
p.id=H(p.id,Nj)
endif
```

图 1 给出了IP数据包经过网络中路由器时的标记过程，IP数据包从源主机S出发路经R1-Ri路由器到达目的主机D，途中路经的第 1 个路由器R1，将flag域和 16 位路径标识域分别置 1 和N_1，此后，数据包经过R2, R3, …, Ri时，只是利用哈希函数来更新 16 位标识域。

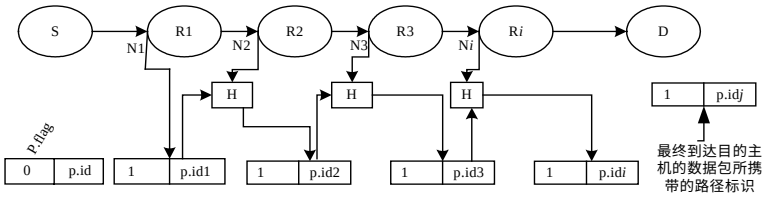

图 1 数据包标记过程

文献[1]利用 IP 首部 16 位标识字段中 5 位存储路由跳数，11 位存储路径标识(path identification)，攻击者可以利用 Traceroute 来确定源主机和目的主机之间的 TTL 值，在哈希函数最理想的情况下，11 位的空间存储路径标识(path identification)碰撞率见式(1)：

$$\frac{2^{11n}-2^{11}\times(2^{11}-1)\times(2^{11}-2)\cdots\times(2^{11}-n+1)}{2^{11n}} \tag{1}$$

16 位空间存储路径标识的碰撞率见式(2)：

$$\frac{2^{16n}-2^{16}\times(2^{16}-1)\times(2^{16}-2)\cdots\times(2^{16}-n+1)}{2^{16n}} \tag{2}$$

由式(1)、式(2)可以得出，该算法与文献[1]中的算法相比，降低了碰撞率。

3.2 M-Table 表的建立与更新

为数据包的路径标识和源 IP 地址建立 M-Table 表，当 IP 数据包到达受害主机时，从中提取数据包标记和源 IP 地址(SourIP)，并为该 IP 数据包标记设置计数器 T，它所记录的值为对应于相同标记不同 IP 地址的个数，Status 为该标记的状态，M-Table 的建立见算法 2。

算法 2 M-Table 表的建立

```
Extract p.flag ,p.id and the SourIP from p
Search M-Table and compare p.flag , p.id with the p.flag ,p.id in the M-Table
if result of the comparison is equal then
Compare SourIP with SourIP in the M-Table
 if result is equal then
return
 else
Ti= Ti +1; //Ti是对应该路径标识的不同IP地址的数目, i=1,2,…
  M-Table<-SourIP
//M-Table 的大小应大于主机每秒处理的数据包个数的 N(N>1)
//倍，N 取值的不同会影响到防御机制的效率
  endif
 endif
 else
 Insert FootPrint and SourIP into M-Table
 Tj=1        j=1,2,3,…, j ≠ i
 endif
```

M-Table的存储结构如图 2 所示，其中，p.SIP 表示数据包的源IP地址[1]。

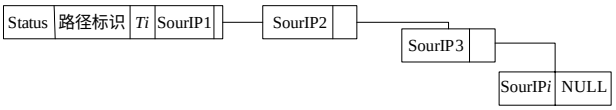

图 2 M-Table表存储结构

为了减少M-Table的存储空间和提高查找的速度，根据平时受害主机处理数据包的能力确定M-Tabel的大小[1]。在下列 2 种情况下，需要对M-Table进行更新：

(1)当有 IP 数据包到达主机时，从中提取的标记与表中存在的任何一个标记都不相同，此时需要插入一项。

(2)网络的拓扑结构发生变化时，也会有新的一项插入到 M-Table。

因为 M-Table 不能将所有的 IP 标记，所以它的更新可以采取 LFU, LRU 和 MFU 中的一种方法，本文不对 3 种替换策略的优劣进行讨论。

3.3 攻击数据包的过滤

该机制具有 2 种工作模式：监视模式和过滤模式，默认状态下处于监视模式。为 2 种工作模式的切换设置临界值 $T1$, $T2$($T1$>$T2$)，将 M-Table 中计数器 T 的总和 TOT 与 $T1$ 比较，若 $TOT \geq T1$，从监视模式切换至过滤模式，$TOT \leq T2$，从过滤模式切换至监视模式。

当$TOT \geq T_1$时，切换至过滤工作状态，检索M-Table表，查找计数器T值最大的一项记作I_s，M-Table中与I_s项对应的除了FootPrint域，其他域的值均清零，并将I_s标记为Spoofed，此后凡是到达主机的数据包中的，其FootPrint与该项相同，均会被过滤掉，如此循环继续，直至$TOT \leq T_2$，接着转到监听状态，见算法 3。

算法 3 伪造数据包的检测

```
while(TOT>=T1)
```

```
Search the M-Table
Find Is
TOT=TOT-T
T <-0
SourIP<-0
Status=Spoofed
end while
if(TOT<=T2) then
exit
```

4 实验

实验验证了从监视模式切换至过滤模式，将攻击包过滤后，又转为监视模式的这段时间内，PI-ANTIS 的工作情况，分别给出了 5 000 p/s, 10 000 p/s, 15 000 p/s(其中，p/s 为每秒攻击包的个数)3 种攻击速率下的实验仿真图。

如图 3 每秒的攻击包数分别为 5 000, 10 000 和 15 000，可以看出，攻击速率越高，攻击包达到相同百分率所需要的时间越短。

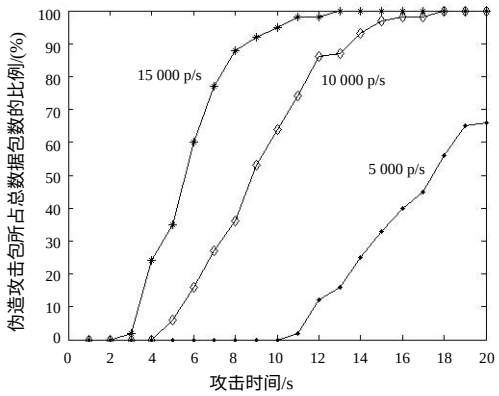

图 3　伪造 DDoS 攻击

图 4 是在 3 种不同的攻击速率下，$T1$ 的值均为 5 000 时，该防御机制过滤攻击包的情况。

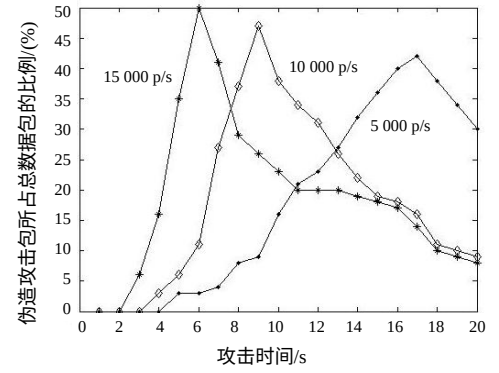

图 4　伪造 DDoS 攻击的防御($T1$ 值相同)

图 5 是在攻击速率为 5 000 p/s,1 0000 p/s,15 000 p/s，$T1$ 的取值分别为 2 500, 5 000, 7 500 这 3 种情况下，该机制过滤伪造的 IP 数据包的情形。

通过图 5 可以看出，根据攻击速率的不同，$T1$ 需取不同的数值才能达到更好的防御效果，应该根据实际情况，对$T1$, T_2进行取值。

在实验中，默认情况下，该机制工作于监视模式下，当检测到计数器 TOT 的值超过预设的值 $T1$ 时，认为遭遇了伪造 IP DDoS 攻击，切换至过滤模式，过滤模式下，按照算法中给出的原则，过滤掉伪造 IP 数据包，同时减小 TOT 的值，直至 $TOT \leq T2$，再次切换至监视模式。

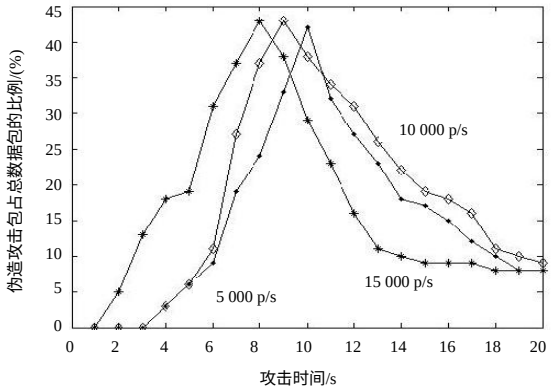

图 5　伪造 DDoS 攻击的防御($T1$ 值不同)

文献[1]中受害主机记录数据包的源 IP 地址以及该数据包的路径标识，当检测到攻击发生时，若主机的记录中不存在到达的数据包的源 IP 地址及路径标识，其以一定的概率发送 ICMP 或 TCP RST 包给源主机，如果返回的包中路径标识与刚才到达的数据包不同，就认为此数据包是伪造的，但由于 DDoS 攻击力度极大，攻击发生时，主机已经不能够提供正常的网络服务，因此探测路径的方法无法有效防御伪造 DDoS 攻击，并且其路径探测的方法本身也会导致 DDoS 攻击，随着攻击的不断加强，会有越来越多的伪造攻击包到达受害主机，克服了文献[1]方案中的缺点。

5 结束语

本文分析了多种拒绝服务攻击(DoS)防御方案，并提出了一种基于数据包标记的伪造 DDoS 攻击防御机制，通过向 IP 数据包中嵌入一个标志路径信息的 16 位标识，检测标识计数器临界值来判断 DDoS 攻击的发生。通过对伪造地址的 IP 数据包进行过滤，保证网络的服务质量。从实验结果可以看出，本文提出的算法能够达到很好的防御效果。

参考文献

[1] Lee Fuyuan, Shieh S. Defending Against Spoofed DDoS Attacks with Path-fingerprint[J]. Computer & Security, 2005, 24(7): 571-586.

[2] Keromytis A D, Misra V, Rubenstein D. SOS: An Architecture for Mitigating DDoS Attacks[J]. IEEE Journal on Selected Areas in Communications, 2004, 2(1): 176-188.

[3] Sung Minho, Xu Jun. IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending Against Internet DDoS Attacks[J]. IEEE Transactions on Parallel and Distributed Systems, 2003, 14(9): 861-872.

[4] Jin Cheng, Wang Haining, Shin K G. Hop-count Ailtering: An Effective Defense Against Spoofed DDoS Traffic[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, D. C., USA: [s. n.], 2003-10.