ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.11, November 2007, pp.2830−2840
DOI: 10.1360/jos182830

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种基于路由器矢量边采样的IP追踪技术*

魏 军+, 连一峰, 戴英侠, 李 闻, 鲍旭华

(中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

An IP Traceback Technique Based on Router's Vector-Edge-Sampling

WEI Jun+, LIAN Yi-Feng, DAI Ying-Xia, LI Wen, BAO Xu-Hua

(State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-62661722, Fax: +86-10-62661700, E-mail: weijun987@yahoo.com.cn, http://home.is.ac.cn

Wei J, Lian YF, Dai YX, Li W, Bao XH. An IP traceback technique based on router's vector-edge-sampling. *Journal of Software*, 2007,18(11):2830−2840. http://www.jos.org.cn/1000-9825/18/2830.htm

Abstract: A new edge sampling approach called the 'Router's Vector-Edge-Sampling (RVES)' is presented, which is simple for PPM (probability packet marking) to be implemented and deployed. In the graph model, vertexes are denoted by network interfaces instead of routers, while edges by vector edges instead of traditional ones. With better simplicity of implementation and flexibility of policy deployment, RVES features effectiveness for Distributed Denial-of-Service (DDoS) attack reconstruction. PPM technologies based on traditional edge sampling are still applicable. Prototypes have been deployed in the Internet and experiments prove the effectiveness and feasibility of RVES.

Key words: IP traceback; PPM (probability packet marking); DoS (denial-of-service); DDoS (distributed denial-of-service); network security

摘 要: 提出了一种新型的边采样方法"路由器矢量边采样"(RVES),使得概率包标记(probability packet marking,简称PPM)设备容易实现和部署.在图论模型上,RVES以网络接口替代路由器作为顶点,以路由器"矢量边"替代传统采样边.该方法实施简单,标记概率的策略配置灵活,可以有效解决分布式拒绝服务(router's vector-edge-sampling,简称DDoS)攻击的重构问题.基于传统边采样的PPM相关技术依然适用于RVES方法.原理样机已经研制出并部署在Internet上.实验结果验证了该方法的有效性和可行性.

关键词: IP 追踪;PPM(probability packet marking);DoS(denial-of-service);DDoS(distributed denial-of-service);网络安全

中图法分类号: TP393 **文献标识码**: A

随着互联网的发展,出现了各种针对协议或操作系统设计缺陷的网络攻击.DoS/DDoS(denial-of-service/distributed denial-of-service)攻击(拒绝服务攻击/分布式拒绝服务攻击)的原理是在一定时间段内直接或者通过跳板向目标网络发送大量的特定数据包(如服务请求包、TCP SYN包等),极大地消耗网络带宽或系统资源,引起

* Supported by the National Natural Science Foundation of China under Grant No.60403006 (国家自然科学基金); the National Basic Research Program of China under Grant No.G1999035801 (国家重点基础研究发展计划(973))

Received 2005-11-30; Accepted 2006-08-22

目标网络的阻塞甚至瘫痪[1].这些攻击包的源IP地址通常是经过伪造的.被攻击网络如何根据收到的数据包,最大可能地追踪和定位攻击者位置,封堵DoS攻击来源,称为IP Traceback技术(IP追踪技术)[2].

虽然IP包头源地址是虚假的,但每个IP包都必须经过从攻击者到目标机之间的路由器转发.借助路由器对数据包进行标记或记录,从而根据收到的数据包重构出攻击路径,是IP追踪研究的基本思路.

1 当前研究进展与问题

早期针对DoS攻击的IP追踪技术有入口过滤、链路测试、注入调试,日志记录等等[3].

近年来,IP追踪研究工作基本上分为“单独生成追踪信息专用数据包”和“IP数据包标记”两大类.前者会增加网络带宽负荷,不易升级,反而充当了一种DoS攻击行为.后者经历了从“节点附加”和“节点采样”到“边采样”标记的发展过程.自从2000年Savage等人提出“边采样”标记方法之后,主流的IP追踪技术进入了“基于日志记录的追踪技术”和“基于边采样的概率包标记(probability packet marking,简称PPM)技术”两大阵营的时代[4,5].

1.1 节点附加和节点采样标记

在节点附加方法中,每个路由器将自己的IP地址附加在标记数据包后面.其缺点是,标记包长度不可控,容易引起标记包的再分片,攻击者可以添加虚假信息路径信息[3].在节点采样标记方法中,路由器按照某种概率将32位IP地址记录到IP头某个位置.其缺点是,未能很好地考虑IP头中有无足够的空间来存储32位IP地址[6].

1.2 基于日志记录的追踪技术

基于日志记录的IP追踪技术要求路由器通过对每个转发包进行Hash运算,记录数据包摘要信息.路径重构时,通过获取的攻击包进行递归得到相邻路由器地址,从而恢复出整个攻击路径.在高速链路情况下,由于数据包到达的速度和记录速度必须相匹配,因此该方法适合的范围受到限制[4,5,7].

1.3 基于边采样的概率包标记技术

基于传统边采样的概率包标记技术[2,3,8,9]适合DoS攻击追踪[10].路由器以一定概率对数据包进行标记,标记内容包括攻击路径上任意两个相邻路由器的地址,即攻击路径图上的“边”以及“边”到攻击目标的距离.被攻击者根据收到的标记信息恢复攻击路径.一般认为,IP头域中适合标记的空间有17位:16bit的包标识域和1bit的分片标志flag的最高位[6,11].受此空间限制,标记信息往往需要先分片再进行标记.为了重构时将标记片段正确地组合在一起,有些算法基于范德蒙行列式[6,8]生成标记信息分片;有些算法将IP地址的Hash结果作为标记信息中的认证码[2]或者将Hash结果和IP地址隔位插入作为标记信息[3].

PPM已成为IP地址追踪研究的一个主要方向.许多研究人员在PPM标记概率、标记信息分片、防止伪造包的加密和认证技术等领域开展了研究工作[2,3,6,8,9,12,13].

图1是目前PPM所依赖的传统“边采样”示意图.*Attacker*表示攻击发起者,*Victim*表示攻击目标,R表示路由器.由左侧网络拓扑示意图可以看出,在传统边采样中,路由器是图的顶点,相邻顶点构成了图的边.右侧图中黑实线表示两个攻击者发起的攻击路径($R_{5,2},R_{4,2},R_{3,1},R_{2,1},R_{1,1}$)和($R_{3,3},R_{2,1},R_{1,1}$),每条攻击路径由若干个相邻接路由器组成的“边”连接而成.

PPM方法基于这些传统边采样技术,存在3个问题:

(1) 传统“边”由相邻路由器构成,下游路由器打标记时必须知道相邻上游标记路由器地址,否则无法生成“边”信息.当两个非相邻标记路由器之间有其他非标记路由器时问题更为突出,因为标记路由器必须知道跨越这几个非标记路由器之前的那个“相邻”标记路由器的地址才能完成这条边的标记.在图1中,路由器$R_{2,1}$必须知道自己的上游相邻路由器$R_{3,1},R_{3,2},R_{3,3}$的地址,并且将其地址分别与自己的地址进行运算,作为对应的标记信息.如果$R_{3,1}$不具备标记功能,则$R_{2,1}$必须知道$R_{3,1}$不是标记路由器,不能与其进行运算,而且还要知道该方向上最相近的标记路由器$R_{4,1}$和$R_{4,2}$的地址并与其进行运算,显然,这是非常困难的.

(2) 在重构时要将收集到的标记片断信息和特定运算结果对照数据库中的片断信息进行对比,以此确定攻击路径上参与标记的路由器.因此在攻击路径重构之前,必须有一个重构对照数据库来保存各路由器IP地址或

者这些地址的 Hash 结果或者相邻路由器地址异或结果.

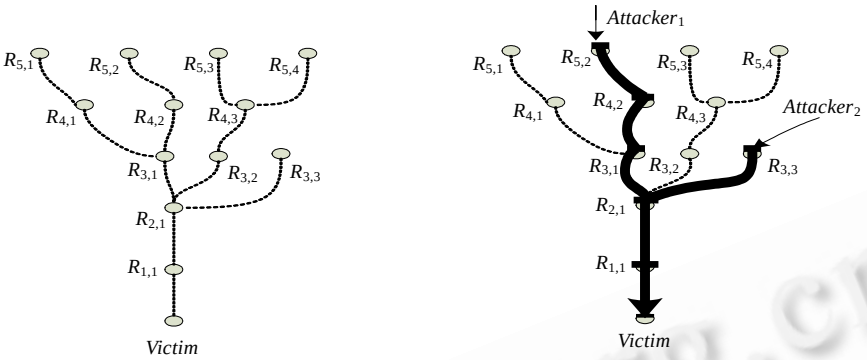


Fig.1 Traditional edge sampling for IP traceback technology

图 1 IP地址追踪技术中的传统边采样

(3) 传统方法将一台路由器定义为图上的一个顶点,两个顶点构成一条边.因此只能用一个 IP 地址代表该路由器作为顶点的信息.路由器的 IP 地址与其自身各个网络接口是对应的,无论用哪个网络接口上的 IP 地址来代表该路由器,都容易引起攻击重构时假边的产生,将重构引入歧途.

2 标记方案

2.1 研究前提假定

本文的研究工作基于以下前提假定条件:

(1) 攻击者可以产生任何攻击包;

(2) 攻击者可能联手或者利用傀儡机器;

(3) 数据包可能被丢弃或重组;

(4) 攻击者和受害者间的路由在一段时间内相对稳定;

(5) 路由器的 CPU 和存储器是有限的;

(6) 大多路由器不会受到攻击破坏;

(7) 标记路由器的部署是循序渐进的,即攻击路径上的路由器并非都具有标记功能;

(8) 若非人工参与,标记路由器很难知道上游最近的标记路由器地址;

(9) 重构时,尽管获得一个路由器拓扑图是容易的,但很难维护一个仅将所有标记路由器按照邻接关系进行 IP 地址运算作为重构对照的数据库.

上述假定条件中的(1)~(6)来自文献[3,8].本文提出假定条件(7)和(8),是基于互联网或者大型局域网上部署的现实性考虑的,既是假定条件也是客观条件限制.标记路由器(也代指具有标记功能的网关设备)的部署只能分步实施,导致标记路由器之间可能夹杂非标记路由器.若非借助于 ISP(Internet service provider,网络服务商)或者其他人工告知方式,则下游路由器很难自动获知上游最近的标记路由器地址.尤其是每条“边”的信息必须分片标记,下游路由器无法从上游来的数据包中发现上游标记路由器完整的 IP 地址信息,从而无法将其与本机 IP 地址进行运算生成标记信息.

互联网协作的无组织特点很难让所有的ISP或某个组织来登记和管理标记路由器IP地址库.尽管获取网络拓扑图是容易的[2],然而很难维护一个仅将所有标记路由器按照邻接关系进行地址运算的重构参照数据库.

考虑到假定条件(7)~(9),目前绝大多数基于“传统采样边”的PPM方案[2,3,8,9]都有标记和重构两方面的实施上的问题.

2.2 定 义

本文定义新的图论模型,将“边”的位置定义在标记路由器内部,顶点恰好是同一台路由器的一对网络接口.

我们提出以“路由器矢量边采样(router’s vector-edge-sampling,简称 RVES)”的方法替代传统边采样方法.数据包流经路由器上的一对网络接口构成路由器内部的一条“矢量边”.基于“传统边采样”方法的 PPM 研究成果可以移植到 RVES 方法上,因为 PPM 技术基于边采样,而与“边”的位置选择无关.

定义 1. 标记路由器$R=(IF_{local},E_R,IF_{wan})$,每台标记路由器都可以从路由器网络接口的角度将路由器定义为三元组.其中:

$IF_{local}=\{L_0,L_1,L_2,\ldots,L_m\}$,表示该路由器本地网络接口集.

$IF_{wan}=\{S_0,S_1,S_2,\ldots,S_n\}$,表示该路由器广域网络接口集.

$E_R=\{(S_{in}S_{out})|S_{in},S_{out}\in R.IF_{wan},S_{in}\neq S_{out}\}$,是路由器的“矢量边”集合.数据包经过路由器是有入/出方向的,S_{in}和S_{out}分别表示某个数据包流经标记路由器时经过的入口和出口.这两个网络接口相连便在路由器体内形成一条矢量边,指向该包流经的方向.E_R是路由器R内部所有可能的矢量边的集合,一个数据包只能经过其中的 1 条.入口和出口仅仅是相对于 1 个包而言的.在路由器任意一个网络接口上,针对入/出数据包的处理策略不同(见算法部分).图 2 中的右图是不同的数据包流经某标记路由器而产生的两条矢量边$(S_0S_1),(S_jS_k)$的示意图.

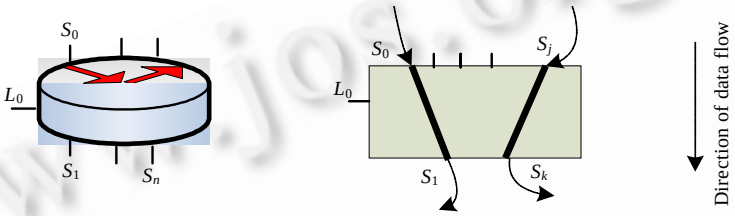


Fig.2 Marking router and vector edges

图 2 标记路由器及其“矢量边”

按照一定的标记算法,路由器将矢量边信息写入数据包,根据对这些包的统计分析,即可恢复出攻击路径.

定义 2. 攻击路径$P=(A,E_{PATH},Victim)$,$A\in\{Attacker_1,Attacker_2,\ldots,Attacker_n\}$表示攻击发起者,$Victim$表示攻击目标,$E_{PATH}=(edge_1,edge_2,\ldots,edge_d)$表示从距离$d$处发起的攻击所经过的标记路由器“体内采样边”连接而成的一条路径,其中,$edge_i=R_i.(S_{in}S_{out})$.

定义 3. 攻击路径图$G=(E_G,V_G)$.$V_G=\{R_i.IF_{wan}|i=1,2,\ldots\}$,表示图$G$的“顶点”集合是所有路由器的广域网络接口集.$E_G=\{edge_i|i=1,2,\ldots\}$,表示图$G$的“边”集合是所有路由器体内网络接口连接而成的“矢量边”集合.

图 3 中的左图是“矢量边”标记路由器部署后的网络拓扑示意图.圆框表示非标记路由器,矩形框表示标记路由器.图 3 中的右图演示了从$R_{7,1}$和$R_{7,4}$处发起攻击后,攻击包所经过的路径上标记路由器“矢量边”连接而成的攻击路径.尽管来自$Attacker_1$的攻击路径$(R_{7,1},R_{6,1},R_{5,1},R_{4,1},R_{3,1},R_{2,1},R_{1,1})$中夹杂了非标记路由器$R_{6,1},R_{4,1}$和$R_{2,1}$,但是,参照网络拓扑图能够实现该路径的重构恢复.

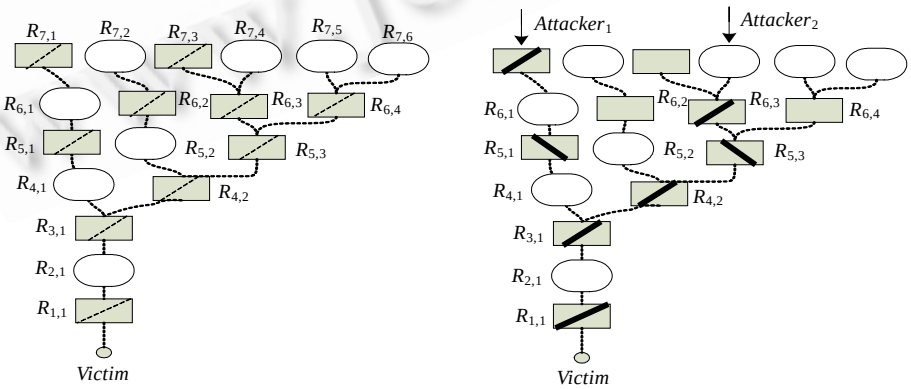


Fig.3 Router’s vector-edge sampling for IP traceback technology

图 3 IP 追踪技术中的路由器矢量边采样

2.3 标记域的选择

数据包标记技术将标记信息存储于 IP 头内.本文只对 IPv4 格式的包头中可能被利用的字段进行分析.

实际网络中只有不到 0.25%的数据包可能被分片[3],因此,研究人员大多将注意力放在标识数据包的ID域和Flags字段上.结合实验,我们采用文献[6,11]的观点,认为IP头域中 17 位空间存储标记信息是比较可靠的,即用于标识数据包的ID域(16bit)和用于分片的Flags字段的最高位(1bit)(图 4 中ID字段和Offset字段之间的 3 位是Flags字段).

文献[8,14,15]认为TOS(type of service)域可用.我们在互联网上进行的计算机改包实验结果表明:TOS域、Flags字段后 2 位、Offset字段都是不能随便修改的,否则数据包无法通过其他路由器进行转发.数据包标记技术的目的是重构攻击路径,而不能因此妨碍正常的网络通信.虽然IP报头中一些字段看似可用,但我们通过实验发现,修改后会影响正常的TCP/UDP数据包转发.当然,如果能在IP头中找到更多存储空间来存储边信息,则基于边采样的PPM功能将更为强大[16].本文使用IP头中的 17 位空间存储标记信息(见图 4 中的阴影部分).

4 bit	4 bit	8 bit	3 bit	15 bit
Ver	HLen	TOS	TotalLen	
ID				Offset
TTL		Protocol	Checksum	
Source IP				
Destination IP				
Destination IP				
IP options				

Fig.4 IP version 4 header format

图 4 IPv4 包头格式

2.4 标记信息

受标记空间的限制,基于边采样的PPM技术一般将一条 64bit的“边”划分为若干标记片段[15].本文采用常用的 8 片段方式,每个标记信息片段格式如图 5 所示.

3 bit	5 bit	8 bit	1 bit
c	*Distance*	$edge_i[c]$	*flag*

Fig.5 17bits marking information format

图 5 17 位标记信息格式

c:数值 0~7,表示是该边的第几个片段.

Distance:数值 1~31,表示标记路由器到目标机距离.

flag:数值 0 或 1.当 *flag* 取 1 时,表示此数据包为已标记包.

$edge_i[c]$:路由器R_i矢量边$edge_i$的第c个 1/8 片段信息,长度为 8bit.

“矢量边”$edge_i$是数据包流经路由器R_i时经过的两个网络接口S_{in}和S_{out}构成的.要标记的内容是它们的 64 位IP地址对,记为(IP_{in},IP_{out}),即“矢量边”$edge_i=(S_{in},S_{out})=(IP_{in},IP_{out})$.本文研究基于“矢量边”采样的PPM技术,因此,标记路由器知道位于本机的$edge_i$数值,可以直接打入标记包,而不需要像传统“边采样”那样去获取相邻路由器地址来进行各种计算作为标记信息.

每条边是一个 64bit的地址对(IP_{in},IP_{out}),因此,每个 1/8 片段信息为

$$edge_i[c]\in\{{}_{R_i}IP_{in}[0],{}_{R_i}IP_{in}[1],{}_{R_i}IP_{in}[2],{}_{R_i}IP_{in}[3],{}_{R_i}IP_{out}[0],{}_{R_i}IP_{out}[1],{}_{R_i}IP_{out}[2],{}_{R_i}IP_{out}[3]\}.$$

2.5 算 法

IP 追踪算法分为标记算法和重构算法两个部分.

本文研究的 RVES 方法中“边”的位置与传统边采样中“边”的位置不同:传统方法“边”的顶点是相邻的两台路由器;RVES 方法“边”定义在路由器内部,顶点恰好是数据包经过标记路由器时的两个网络接口(地址).标记路

由器只需要关注数据包在本体所流经的入口和出口,并将对应的地址作为路径片段标记在数据包上.而传统边采样关注上游标记路由器的地址,将两台相邻路由器的地址作为一条“边”记录下来.两者的标记算法不同,重构算法思路几乎是相同的,但本文的重构算法要简单得多.

标记过程算法如下:

Marking procedure in router R, on one of R's network interfaces S_j, set $q_j \in [0,1]$

for each packet P into R, generate a random number $\mu \in [0,1]$

if $\mu \le q_j$ then

set ($P.distance$,$P.flag$,$P.edge$)←(0,1,j)

for each packet P outfrom R

if $P.flag$==1 then

{if $P.distance$==0

$P.distance$←1

i←$P.edge$

get $edge[c_{i,j}]$ from already known 8 segments of (IP_i,IP_j)

$P.edge$←$edge[c_{i,j}]$

$P.c$←$c_{i,j}$++(mod8)

else $P.distance$++

}

重构过程如下:

重构机位于被攻击目标所在网络内,将听到的包按距离和同一条边的1/8分片号存入库中(如图6所示).

Distance	*Edge*[0]	*Edge*[1]	*Edge*[2]	*Edge*[3]	*Edge*[4]	*Edge*[5]	*Edge*[6]	*Edge*[7]
1	$R_1.IP_{in}[0]$	$R_1.IP_{in}[1]$	$R_1.IP_{in}[2]$	$R_1.IP_{in}[3]$	$R_1.IP_{out}[0]$	$R_1.IP_{out}[1]$	$R_1.IP_{out}[2]$	$R_1.IP_{out}[3]$
…								
d	$R_d.IP_{in}[0]$	$R_d.IP_{in}[1]$	$R_d.IP_{in}[2]$	$R_d.IP_{in}[3]$	$R_d.IP_{out}[0]$	$R_d.IP_{out}[1]$	$R_d.IP_{out}[2]$	$R_d.IP_{out}[3]$

Fig.6 Marked packets storage format at the victim

图6 攻击目标处的标记包存储格式

标记方法中按顺序产生1/8分片,明文标记各片的IP地址.在DDoS攻击时,对于相同距离和分片序号的不同地址分片,参照路由拓扑可以实现定位.重构处理中部分算法如下:

for each packet P, according to the Topology Graph G^T

now there are α marking routers taking part in the marking process at the same distance d

i←$P.c$, d←$P.distance$,

{if i==0 then

{if all $savedEdge[d,\beta].ip[0]$!=$P.edge$ $\beta \in [0,\alpha-1]$, then

create $newEdge[d,\alpha]$

$newEdge[d,\alpha].ip[0].addr$←$P.edge$

$newEdge[d,\alpha].ip[0].count$←1

α++

else if $savedEdge[d,\beta].ip[0].addr$==$P.edge$, then

$savedEdge[d,\beta].ip[0].count$++

}

else {if $savedEdge[d,\beta].ip[i].addr$==$P.edge$

then $savedEdge[d,\beta].ip[i].count$++

if all $savedEdge[d,\beta].ip[i]!=P.edge$
and $(savedEdge[d,\gamma].ip[0].addr,savedEdge[d,\gamma].ip[1].addr,\ldots,savedEdge[d,\gamma].ip[i-1].addr,P.edge)\in G^T$
and $(savedEdge[d,\gamma].ip[i].count==0),\gamma\in[0,\alpha-1]$
then
$savedEdge[d,\gamma].ip[i].addr\leftarrow P.edge$
$savedEdge[d,\gamma].ip[i].count++$
if all $savedEdge[d,\beta].ip[i]!=P.edge$
and $(savedEdge[d,\gamma].ip[0].addr,savedEdge[d,\gamma].ip[1].addr,\ldots,savedEdge[d,\gamma].ip[i-1].addr,P.edge)\in G^T$
and $(savedEdge[d,\gamma].ip[i].count!=0),\gamma\in[0,\alpha-1]$
then create $newEdge[d,\alpha]$
$newEdge[d,\alpha].ip[0\sim i-1]\leftarrow savedEdge[d,\gamma].ip[0\sim i-1]$
…
$newEdge[d,\alpha].ip[i].addr\leftarrow P.edge$
$newEdge[d,\alpha].ip[i].count\leftarrow 1$
}}
accept those saved edges according to their counts and G^T, then present attacking paths

基于 RVES 方法,无须路由拓扑图就可以直接实现 DoS 攻击路径重构,而借助路由拓扑图可以实现 DDoS 攻击路径重构.

3 方案分析

3.1 标记算法对比

传统边采样标记路由器需要从收到的数据包中获取上游标记路由器地址片段信息,推断出其完整 IP 地址,再与本机地址进行 Hash 或插值等运算,生成两路由器连成的边信息再分片打入标记.生成标记信息过程复杂,路径上夹杂非标记路由器时获取上游地址困难.

RVES 标记路由器拥有自身所有的网络接口地址,能够严格控制 1/8 分片标记顺序,标记概率可以随端口策略而定,算法简单,独立于其他路由器,易于实现.

3.2 数据包期望

在基于传统边采样的PPM方法中,往往要求所有路由器参与标记,恢复一条长度距离为d的攻击路径所需要的数据包期望值计算公式如下[3]:

$$E(X)<\frac{k\cdot\ln(kd)}{p(1-p)^{d-1}}.$$

其中,k表示每条边的分片数,这里为 8.p为标记概率,一般选择 4%~5%[3,10].可见,$E(X)$与d成正比.在传统方法中,由于路径上的路由器必须都参加标记,因此距离$d_{传统}$等于攻击者距离攻击目标的全部路由器跳数.

RVES 方法仍然是一种边采样技术.因此,基于 RVES 的 PPM 重构数据包期望值计算公式与上式相同.RVER 容许攻击路径上非标记路由器的存在,距离 d 表示攻击者到攻击目标经历了多少标记路由器.

增加标记概率p虽然可以减弱攻击者隐藏来源的能力,但却影响链路的吞吐性能[10].在本文的标记方法中,可以针对同一个路由器上的不同网络接口S_i采取不同的标记速率q_i.这为一台路由器上制定各种路径服务策略、决定其中哪些“边”参与标记、各端口设置合适的标记速率提供了可能.

3.3 对假标记包的抵御分析

3.3.1 标记路由器邻接时产生的假边分析

传统边采样方法将一台路由器定义为攻击路径图G上的一个顶点,然后通过工具获得路由器上网络接口的

IP地址,在拓扑图中表示出该路由器.由于路由器只能选择 1 个出口或者入口地址代表这个顶点,因此对于多出口/入口的路由器进行标记就会出现问题.比如,选择出口IP代表路由器,当路由器连接如图 7 中的左图所示时,$R_{i+1,1}$有两个不同出口,若以左出口IP代表$R_{i+1,1}$位置,则在路径重构时,重构对照拓扑图中边$(R_{i+1,1},R_{i,2})$的信息与标记包中$(R_{i+1,1},R_{i,2})$的信息是对应不上的.同理,选择入口IP代表该路由器,当路由器级连如图 7 中的右图所示时,也会产生对应不上的问题.

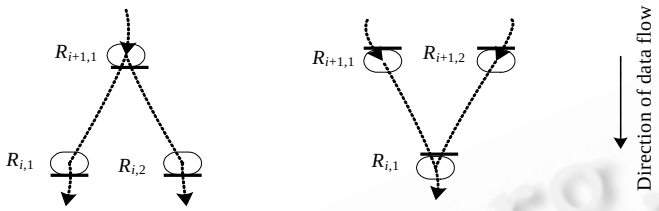


Fig.7 Two kinds of vertex positions in traditional edge sampling to reconstruct false edges

图 7 传统边采样中的 2 种顶点位置会重构出假边

RVES 方法在图 G 的定义中,顶点定义在路由器网络接口上,故而不会产生边的二义性.

3.3.2 标记路由器夹杂非标记路由器时产生的假边分析

传统边采样中的“边”由两台邻接路由器节点构成.若攻击路径上夹杂非标记路由器,则会误将标记路由器和相邻非标记路由器的地址构造为一条假边.RVES 中的“边”在标记路由器体内,因此不会出现这种情况.

3.3.3 注入假包分析

攻击者除了修改攻击包中的源地址来隐藏自己以外,还会采用注入伪造标记包的方法混淆分析人员的视线.标记算法中往往根据 *P.flag* 来判断是否为标记包.伪造的假标记包也会将此数值置1,在标记信息域填入假的边信息,使得重构分析误入歧途.

RVES标记路由器对*P.flag*为 1 的包进行距离加 1 操作:(1) 当假标记包到达目标机时,会因其距离大于正常的标记数据包而被去掉;(2) 在大规模部署时,可以通过对比TTL减少值和距离增加值是否吻合来判断假标记包[17].

3.4 重构DoS和DDoS攻击分析

基于“传统边采样”的PPM技术对DoS攻击重构有效,但对于DDoS攻击则没有很好的办法[3,10,16].一个非常重要的原因是,在传统边采样技术中,“边”跨越两个路由器,要维护一个所有标记路由器按邻接关系进行地址运算的对照数据库,以便重构时正确定位相同距离层面上的多攻击路径标记片段,这是很困难的.下面列举比较有代表性的传统PPM算法.Savage[3]在算法中引入校验码,但对于 10 条攻击路径的分片定位将高达 10^9种组合[3],不适于DDoS攻击追踪.Song[2]在标记中采用Hash算法避免重构时的指数级组合问题,却严重依赖前面提到的网络Hash对照库,而这在分步部署情况下难以做到.

其实,Savage,Song以及很多研究人员[2,3,13]都希望借助于Hash函数或者某种校验算法产生特定标记信息,以减少重构误报率.这要求标记路由器和重构计算机共享相同的Hash算法或校验算法,否则无法在重构时进行标记信息碎片定位.在实际因特网上进行分步实施以及将来算法升级时要慎重考虑这类因素的影响.

针对 DoS 攻击,基于 RVES 的 PPM 能够按照攻击距离的顺序和分片号直接获得标记路由器的地址,从而快速恢复攻击路径.

针对 DDoS 攻击,例如,当攻击者在距离 m 层有 n 条攻击路径时,从第 2.5 节的算法中可以看出,本文对该层的任一分片定位不需要收集全该层全部分片后再进行对比定位,从而避免了组合指数问题.

4 实验设计及结果

PPM 的研究工作都是基于传统边采样的.RVES 方法仍然是一种边采样方法,PPM 的研究工作同样适用.我

们设计了一个基于 RVES 的 PPM 实验环境.

实验环境如图 8 所示.基于RVES技术的标记路由器原理样机R_{i+1},R_{j+1},R_{j+2}部署在实际的互联网上.PC_1,PC_2和PC_3为发包测试机.R_i,R_j和R_k是 3 台处于正常运行的商用路由器,不具备标记功能.标记概率取 4%[3,10].

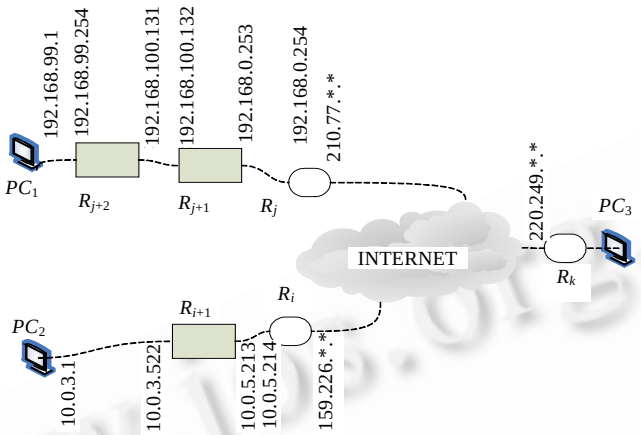


Fig.8 Network topology of PPM/RVES testing experiments

图 8 基于 RVES 的 PPM 测试实验网络拓扑

实验 1. *Victim*={PC3},*Attacker*={PC1}.

由 *Attacker* 向 *Victim* 分别发送 TCP 和 UDP 包.

在 *Victim* 处抓取 IP 包头中已标记数据包,将标记信息按照图 5 的格式换算排列如下:

Distance	*Edge*[0]	*Edge*[1]	*Edge*[2]	*Edge*[3]	*Edge*[4]	*Edge*[5]	*Edge*[6]	*Edge*[7]
1	192	168	100	132	192	168	0	253
2	192	168	99	254	192	168	100	131

从表中可以看出,数据流路径为(192.168.99.254,192.168.100.131)→(192.168.100.132,192.168.0.253)→*Victim*.

实验 2. *Victim*={PC2},*Attacker*={PC1}.

由 *Attacker* 向 *Victim* 分别发送 TCP 和 UDP 包.

在 *Victim* 处抓取 IP 包头中已标记数据包,将标记信息按照图 5 的格式换算排列如下:

Distance	*Edge*[0]	*Edge*[1]	*Edge*[2]	*Edge*[3]	*Edge*[4]	*Edge*[5]	*Edge*[6]	*Edge*[7]
1	10	0	5	213	10	0	3	252
2	192	168	100	132	192	168	0	253
3	192	168	99	254	192	168	100	131

从表中可以看出,数据流路径为

(192.168.99.254,192.168.100.131)→(192.168.100.132,192.168.0.253)→→(10.0.5.213,10.0.3.252)→*Victim*.

实验 3. *Victim*={PC3},*Attacker*={PC1,PC2}.

由 *Attacker* 向 *Victim* 分别发送 TCP 和 UDP 包.

在 *Victim* 处抓取已标记数据包,由于出现同距离的分片,采用第 2.5 节中的重构算法,参照路由拓扑图 8,将路径信息按照图 5 的格式换算排列如下:

Distance	*Edge*[0]	*Edge*[1]	*Edge*[2]	*Edge*[3]	*Edge*[4]	*Edge*[5]	*Edge*[6]	*Edge*[7]
1	192	168	100	132	192	168	0	253
1	10	0	3	252	10	0	5	213
2	192	168	99	254	192	168	100	131

对照路由拓扑图,可以发现攻击来自两条路径,分别是

(192.168. 99.254, 192.168.100.131)→(192.168.100.132,192.168.0.253)→*Victim*,

(10.0.3.252,10.0.5.213)→*Victim*.

受标记路由器原理样机个数的限制,本实验仅演示了距离为 3,最多 2 条攻击路径.从实验中可以看出:

(1) 在RVES方法中,标记路由器距离d是实际跨越的标记路由器距离,虽然攻击路径上夹杂了R_i,R_j和R_k等非标记商用路由器以及跨越因特网上若干商用路由器,但依然可以忠实地记录数据包经历的网段历程,设备可实现、可分步部署.

(2) RVES 标记过程不影响网络中其他正常业务流量.

(3) 采用 17bit 标记空间是可行的.同时我们发现,TOS 域、*Flags* 低两位以及 *Offset* 域修改后的数据包无法跨越实际网络中的商用路由器.

5 总 结

PPM 技术是近年来 IP 追踪技术的一个主流研究分支方向.许多研究人员在 PPM 的编码、加密、认证或者标记概率策略等领域开展工作,对重构期望进行仿真计算,而没有进行实际网络中的标记和重构实验.一些研究人员为了获取更多的标记空间,不合理地占用 IP 头某些域以承载标记算法.这些标记包并不能通过实际网络进行转发.传统边采样方法不能有效应对 DDoS 攻击路径重构.

本文考虑在实际网络不可避免地存在非标记商用路由器的现实条件下,标记路由器能够部署以及快速重构攻击路径,更有效地应对分布式攻击重构.文中分析传统采样方法存在的问题,提出将图论模型中边的位置移到路由器内部,即基于路由器“矢量边”的图论模型,称为 RVES(矢量边采样)方法.研究工作侧重于 RVES 模型定义、标记与重构、实际网络环境中的原理样机实现.当然,RVES 仍然是一种边采样技术,其他文献对于 PPM 的研究工作,如标记概率、重构数据包期望数目、标记信息的加密与验证等等,依然适用.

本文的原理样机可以进行分步部署,归因于 RVES 只关心设备本身的地址,而不依赖上、下相邻标记设备.

RVES 比传统方法更具有可部署性以及标记概率策略配置灵活性.重构过程不依赖于复杂运算标记信息对照库.我们给出本文的标记和重构算法:(1) 无须路由拓扑图直接实现 DoS 攻击重构;(2) 借助路由器拓扑图实现 DDoS 攻击重构.实验表明,标记和重构算法简单、快速有效、结果正确,对于中间跨越商用路由器的实际网络业务不产生影响.即使不更换现有商用路由器,按照本文思路依然可以研制和部署基于 RVES 的 PPM 标记网关设备.

致谢 在此,谨向为本文工作提供支持的信息安全国家重点实验室的朱鹏飞、冯萍慧等同学表示感谢.

References:

[1] Garber L. Denail-of-Service attacks rip the Internet. IEEE Computer, 2000,33(4):12−17.

[2] Song DX, Perrig A. Advanced and authenticated marking schemes for IP traceback. In: Proc. of the IEEE INFOCOM 2001. 2001. 878−886.

[3] Savage S, Wetherall D, Karlin A, Anderson T. Practical network support for IP traceback. In: Proc. of the 2000 ACM SIGCOMM Conf. 2000. 295−306.

[4] Gong C, Sarac K. IP traceback based on packet marking and logging. In: Proc. of the IEEE Int’l Conf. on Communications 2005. 2005. 1043−1047.

[5] Jun L, Sung M, Xu J, Li L. Large-Scale IP traceback in high-speed Internet: Practical techniques and theoretical foundation. In: Proc. of the IEEE Symp. on Security and Privacy 2004. 2004. 115−129.

[6] Chen Z, Lee M. An IP traceback technique against denial-of-service attacks. In: Proc. of the 19th Annual Computer Security Applications Conf. (ACSAC 2003). 2003. 96−104.

[7] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer WT. Hash-Based IP traceback. In: Proc. of the 2001 ACM SIGCOMM Conf. 2001. 3−14.

[8] Dean D, Franklin M, Stubblefield A. An algebraic approach to IP traceback. ACM Trans. on Information and System Security (TISSEC), 2002,5(2):119−137.

[9] Lee T, Wu W, Huang TW. Scalable packet digesting schemes for IP traceback. In: Proc. of the IEEE Int'l Conf. on Communications 2004. 2004. 1008−1013.

[10] Park K, Lee H. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In: Proc. of the IEEE INFOCOM 2001. 2001. 338−347.

[11] Sung M, Xu J. IP traceback-based intelligent packet filtering: A novel technique for defending against Internet DDoS attacks. IEEE Trans. on Parallel and Distributed Systems, 2003,14(9):861−872.

[12] Xiong GH, Wang YG. Research and improve of probabilistic packet marking for IP traceback. Journal of Donghua University, 2004,30(2):5−8 (in Chinese with English abstract).

[13] Qu HP, Li DQ, Su PR, Feng DG. An IP traceback scheme with packet marking in blocks. Journal of Computer Research and Development, 2005,42(12):2084−2092 (in Chinese with English abstract).

[14] Muthuprasanna M, Manimaran G. Space-Time encoding scheme for DDoS attack traceback. In: Proc. of the IEEE Global Telecommunications Conf. (GLOBECOM 2005). 2005. 1842−1846.

[15] Goodrich MT. Efficient packet marking for large-scale IP traceback. In: Proc. of the 9th ACM Conf. on Computer and Communications Security (CCS 2002). 2002. 117−126.

[16] Aljifri H, Smets M, Pons A. IP traceback using header compression. Computers & Security, 2003,22(2):136−151.

[17] Jin C, Wang H, Shin KG. Hop-Count filtering: An effective defense against spoofed DDoS traffic. In: Proc. of the ACM Conf. on Computer and Communications Security. 2003. 30−41.

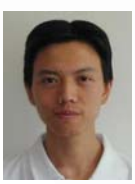
附中文参考文献:

[12] 熊国华,王以刚.基于数据包抽样标记的 IP 追踪技术的研究及改进.东华大学学报(自然科学版),2004,30(2):5−8.

[13] 曲海鹏,李德全,苏璞睿,冯登国.一种分块包标记的 IP 追踪方案.计算机研究与发展,2005,42(12):2084−2092.

魏军(1971－),男,山东日照人,博士生,高级工程师,主要研究领域为网络安全,嵌入式操作系统.

李闻(1980－),男,博士生,主要研究领域为系统安全.



连一峰(1974－),男,博士,副研究员,主要研究领域为网络安全.

鲍旭华(1977－),男,博士生,主要研究领域为入侵检测.

戴英侠(1942－),女,教授,博士生导师,主要研究领域为信息安全.