第37卷 第17期
Vol.37 No.17

计 算 机 工 程
Computer Engineering

2011年9月
September 2011

• 专栏 •

文章编号：1000—3428(2011)17—0011—04 文献标识码：A 中图分类号：TP393.08

重叠哈希分片的概率包标记方法

闫 巧[a]，宁土文[b]

(深圳大学 a. 计算机与软件学院；b. 信息工程学院，广东 深圳 518060)

摘 要：针对压缩边分片采样算法复杂度和重构路径误报率过高的问题，提出一种改进的压缩边分片采样概率包标记方法，即重叠哈希分片(OHF)的概率包标记方法。该方法在不增加包标记位的前提下，通过构造相邻的IP哈希分片之间的4位哈希关系，降低重构算法复杂度，同时改善边采样误报率。在NS2环境下的仿真实验表明了OHF方法的有效性。

关键词：IP追踪；概率包标记；动态概率包标记；压缩边分片采样；分布式拒绝服务

Probabilistic Packet Marking Method of Overlapping Hash Fragment

YAN Qiao[a], NING Tu-wen[b]

(a. College of Computer Science and Software Engineering; b. College of Information Engineering, Shenzhen University, Shenzhen 518060, China)

【Abstract】Aiming at the shortcoming of the compressed edge fragment sampling algorithm, a new method is proposed, called Overlapping Hash Fragment(OHF) Probabilistic Packet Marking(PPM) method. The new method reduces the computational complexity during reconstruction by constructing 4 bits hash relationship between the adjacent IP fragments without increasing the marking amounts. And the new method improves the false alarm rate. Simulation experiment in the NS2 show the validity of the method.

【Key words】IP traceback; Probabilistic Packet Marking(PPM); Dynamic Probabilistic Packet Marking(DPPM); compressed edge fragment sampling; Distributed Denial of Service(DDoS)

DOI: 10.3969/j.issn.1000-3428.2011.17.003

1 概述

概率包标记(Probabilistic Packet Marking, PPM)算法[1]是一种针对拒绝服务(Denial of Service, DoS)攻击或分布式拒绝服务攻击(Distributed Denial of Service, DDoS)的有效源IP追踪(IP traceback)技术，它易于实现，只使用IP包本身的信息，不会产生额外的流量，也不会被防火墙或安全策略堵塞，并且不需要来自ISP的相互合作，因此，吸引了业界的广泛兴趣[2]。但PPM也面临着一些不足，具体包括：

(1)PPM的最弱链、难收敛性

动态概率包标记[3]通过采用自适应概率对数据包进行标记，使受害终端接收到的攻击路径上的各个路由的标记包概率相等，从而解决了该问题。

(2)重构算法复杂度和重构路径误报率过高

假设在多攻击路径下，攻击路径数为m，那么PPM重构出每个边采样的算法复杂度为$O(m^8)$，当攻击路径不断增加时，算法复杂度以指数级别增长，重构路径的时间将会变得很长。而且对于h位哈希的冲突率为$1/2^h$，因此，对于PPM来说h=32，则正确率为$(1-\frac{1}{2^{32}})^{m^8}$，其中，$m^8$为需要进行的哈希次数，因此可知，要进行的哈希次数越多，正确率越低，而误报率$P_E(PPM)=1-(1-\frac{1}{2^{32}})^{m^8}$则越高。ATA算法[4]可以将其重构算法复杂度降为$O(m^3)$，不过其很大部分来自于标记位的增加，从而使分片数降低，其分片数为4片。Network Coding算法[5-6]则是牺牲了算法复杂度去换取用更少的数据包去重构路径。其他的一些算法都以降低分片或者增加包标记位来降低其重构复杂度和误报率[7]。本文提出一种改进的压缩边分片采样概率包标记方法，即重叠哈希概率包标记方法(Overlapping Hash Fragment, OHF)。OHF方法采用自适应概率对数据包进行标记，从而减少重构路径所需要的数据包数。

2 重叠哈希分片概率包标记方法

从攻击路径(图1)可以看出，整条攻击路径上有d个路由，由于IP包头中可标记的位数是有限的，不可能把d个路由的地址全部标记进一个数据包中，因此采用边采样，也即采用相邻路由之间的边采样信息标记进IP包头中，然后收集到所有的边采样信息后再重构出整条攻击路径。

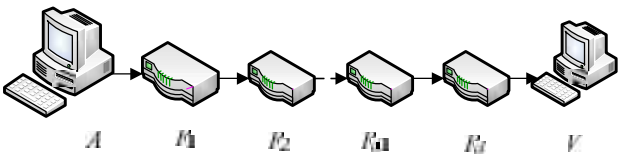


图1 攻击路径示意图

由PPM的标记和重构算法可知，在进行相邻2个路由之间的边采样(也即异或)的同时，将路由地址和路由地址的哈希一共64位分成8片，每片8位。对于是边采样的第几块IP分片，由offset来标记，那么offset需要的标记位为lb8=3位，IP片用8位的addr表示，同时用5位的distance表示边采样距离受害终端有多远。分片时路由IP和哈希奇偶错位，再按每片8位分开。如果得到第1块IP哈希分片，想推出第2块

基金项目：国家自然科学基金资助项目“Non-coherent 网络中的纠错码及其应用”(60972011)

作者简介：闫 巧(1972－)，女，教授、博士、CCF会员，主研方向：概率包标记方法，网络安全；宁土文，硕士研究生

收稿日期：2011-04-07 **E-mail：**yanq@szu.edu.cn

IP 哈希分片，在 PPM 中是做不到的。如果是在单攻击路径下，在同一个采样距离的采样边上得到的第 i 块 IP 哈希分片(其中 $i\in\{1,2,\cdots,8\}$)只有一片，那么重构时就会很简单，而且不会有误报率。但是，在多攻击路径下，假设攻击路径数为 m，在同一个采样距离的采样边上得到的第 i 块 IP 哈希分片(其中 $i\in\{1,2,\cdots,8\}$)就会有 m 片(即 m 个不同的值)。在这里，PPM 采用了穷举法去组合这些分成 8 组，每组有 m 个不同值的 IP 哈希分片，所以，就得到 PPM[1]的重构算法复杂度为 $O(m^8)$。

在 OHF 方法中的多攻击路径下，假设攻击路径数为 m，在同一个采样距离的采样边上得到的第 i 块 IP 哈希分片(其中 $i\in\{1,2,\cdots,8\}$)就会有 m 片(即 m 个不同的值)。在这里 OHF 采用一种改进的分片哈希组合方法，使得从第 i 块 IP 哈希分片(其中 $i\in\{1,2,\cdots,8\}$)是可以推出第 i+1 块 IP 哈希分片(其中 $i\in\{0,1,\cdots,7\}$)，那么在重构时，就不需要用穷举法去组合这些分片，而是对第 i 块 IP 哈希分片(其中 $i\in\{1,2,\cdots,8\}$)的每一个值，推出的第 i+1 块 IP 哈希分片的值，然后从第 i+1 块 IP 哈希分片中的 m 个值中去找到推出来的那个值，即可确定它们来自于同一个路由的 IP 哈希分片。

下面介绍改进的分片哈希组合方法。如图 2 所示，首先将路由器的 32 位 IP 地址分成 8 片，每 4 位一片。编号为：Ipf0, Ipf1,…, Ipf7。其次对于每一片，用一个 4 位的哈希函数去操作，得到 8 片，每 4 位一片的哈希片，编号为：Ipfh0, Ipfh1,…, Ipfh7。然后将前一片的哈希分片与后一片的 IP 片连在一起组成一个新的 IP 哈希片。最后一片的哈希片与第 1 片的 IP 分片连在一起。

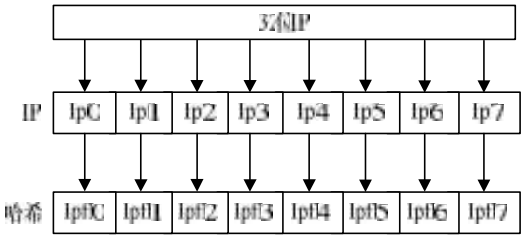


图 2 分片与哈希组合方法

如图 3 所示，依此类推构成 8 片的重叠哈希分片，每片为 8 位，编号分别为：OHF0, OHF1, …, OHF7，其中，当 $i=0$ 时，$\mathrm{OHF0}=\mathrm{Ipfh7}\times 2^4+\mathrm{Ipf0}$。当 $i\neq 0$ 时，$\mathrm{OHF}i=\mathrm{Ipfh}(i-1)\times 2^4+\mathrm{Ipf}i$。假如得到第 1 块 IP 哈希分片，即 OHF0，可以将 OHF0 的低 4 位，即 Ipf0 分离出来，用 4 位的哈希函数去操作，就得到了 Ipfh0。而由 $\mathrm{OHF1}=\mathrm{Ipfh0}\times 2^4+\mathrm{Ipf1}$ 可知 Ipfh0 就是第 2 块 IP 哈希片的高 4 位。同理可知，第 i 块 IP 哈希分片的低 4 位，与第 i+1 块 IP 哈希分片的高 4 位之间是哈希关系。

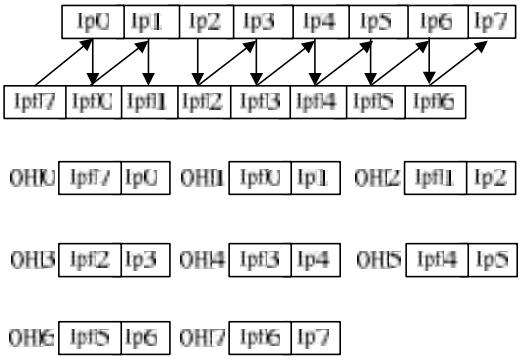


图 3 重叠哈希分片方法

在多攻击路径下假设攻击路径数为 m，在同一个采样距离的采样边上得到的第 i 块 IP 哈希分片就会有 m 片(即 m 个不同的值)，同理第 i+1 块 IP 哈希分片也会有 m 片(即 m 个不同的值)。所以，对于第 i 块 IP 哈希分片的 m 个不同值的每个值，先取出其低 4 位进行一次 4 位的哈希，再与第 i+1 块 IP 哈希分片的 m 个不同值的高 4 位进行比较，如果相等，说明它们来自于同一个节点。如果 8 组 IP 哈希分片之间可以通过 4 位的哈希连接起来，取出连接的 IP 哈希分片的低 4 位，组合成为 IP 地址，最后得到相应路由的地址，与前面进行异或的节点组成原来的采样边。由此可知，重构采样边需要的运算为 $8\times m$ 次 4 位的哈希与 $8\times m^2$ 次 4 位的比较，所以，算法复杂度为 $O(m^2)$。

采用自适应概率对采样边进行标记，可以降低重构路径所需要的数据包数。

如图 1 所示，假如攻击路径上有 d 个路由，每个边采样的标记概率为 $p(i)(i\in\{1,2,\cdots,d\})$，由 PPM 算法可知，在受害终端检测到的相邻路由采样边标记信息的概率为 $p_L(i)(i\in\{1,2,\cdots,d\})$，那么 $p_L(i)$ 如下所示：

$$\begin{cases}p_L(d)=p(d)\\ p_L(d-1)=p(d-1)(1-p(d))\\ \quad\vdots\\ p_L(2)=p(2)\cdots(1-p(d-1))(1-p(d))\\ p_L(1)=p(1)\cdots(1-p(d-1))(1-p(d))\end{cases}$$

如果是 PPM 算法，那么相邻路由边采样的标记概率是一样的，即 $p(i)=p,(i\in\{1,2\cdots,d\})$，那么在终端检测到的各采样边的概率分别为如下方程组：

$$\begin{cases}p_L(d)=p\\ p_L(d-1)=p(1-p)\\ \quad\vdots\\ p_L(2)=p(1-p)^{d-2}\\ p_L(1)=p(1-p)^{d-1}\end{cases}$$

由上面的 $p_L(i)(i\in\{1,2\cdots,d\})$ 可知，$p_L(1)$ 的概率最小，也即最弱链，然而要避免出现最弱链，那么就要使 $p_L(1)=p_L(2)=\cdots=p_L(d)=\dfrac{1}{d}$，由上面方程组解出来的 $p(i)(i\in\{1,2,\cdots,d\})$ 为 $p(i)=\dfrac{1}{i},(i\in\{1,2,\cdots,d\})$，也即第 1 个路由的标记概率为 1，第 2 个路由的标记概率为 1/2，第 d 个路由的标记概率为 1/d。由于 IP 包中的 *ttl* 值是每经过一个路由就减 1 的，因此，假如初始化的 *ttl* 值为 32，那么就可以用 $\dfrac{1}{32-ttl}$ 来代表每一个路由器上的标记概率。在上述思想的基础上提出重叠哈希分片的概率包标记方案(OHF scheme)。

2.1 重叠哈希分片的标记

由上述的重叠哈希分片的概率包标记思想可知，OHF 的分片与标记位与 PPM[1]的是一样的，如图 4 所示。

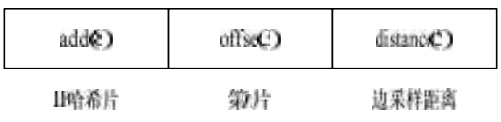


图 4 位预算与标记位

然而 8 位的 *addr* 标记是如图 2 所示中的 {OHF0, OHF1, …,OHF7} 中的任意一片，3 位的 offset 标记的是取到的第几块 IP 哈希片，5 位的 distance 表示的是边采样距离受

害终端有多远。一共需要 16 位，因此，只需要 IP 包头中的 16 位 IP 标识域[1]来进行标记即可。采用自适应概率对数据包进行标记，由于初始化的 *ttl* 值可能为 32、64 和 128，而且大多数包转发不会超过 32 个路由器，因此可以根据 *ttl* 的当前值就可以判断初始化的 *ttl* 值，所以，当 *ttl*<32 时，当前路由对数据包的标记概率为 $P=\frac{1}{32-ttl}$。同理，当 32<*ttl*<64 时，标记概率为 $P=\frac{1}{64-ttl}$，当 64<*ttl*<128 时，标记概率为 $P=\frac{1}{128-ttl}$。

```
Marking procedure at router R:
For each k in [0,1,2,3,4,5,6,7]
Ipf[k]=(R>>(k×4))%(16);
  Ipfh[k]=hash4(ipf[k]);
End
OHF[0]=comb(ipfh[7],ipf[0]);
For i:=0 to 6
  OHF[i+1]=comb(ipfh[i],ipf[i+1]);
End
For each packet w
    If w.ttl<32 then P=1/(32-w.ttl); End
    If 32<w.ttl<64 then P=1/(64-w.ttl);End
    If 64<w.ttl<128 thenP=1/(128-w.ttl);End
Let x be a random number from[0,1]
  If x<P then
  Let b be a random interger from[0,7]
        Write OHF[b] into w.addr8
        Write 0 into w.distance
        Write b into w.offset
  Else
        If w.distance==0 then
Write OHF[w.offset] ⊕ w.addr8 into w.addr8
        End
      Increment w.distance
  End
End
```

标记算法在每一个路由器中都是一样的，标记算法流程为先将路由的地址分成 8 块，对应每一块求出它的哈希块。然后根据图 3，求出 8 块的重叠哈希分片，保存在 OHF[*i*]($i\in\{0,1,\cdots,7\}$) 中。再对每一个通过的数据包 *w* 进行处理，首先判断 *w.ttl* 的数值范围，确定标记概率 *P*。然后从[0 1]中取一个随机数 *x*，如果 $x<P$，就对数据包进行标记，首先从[0 7]中取出一个随机整数赋值给 *b*，将 OHF[*b*]标记进 w.addr8 中，将 w.distance 置为 0，将 w.offset 置为 *b*。否则，即 $x\geqslant P$，先判断 w.distance 是否为 0，如果是，将 w.addr8 置为 OHF[w.offset]⊕w.addr8，这就是分片边采样，相邻 2 个路由节点的异或。然后将 w.distance 增 1。

2.2 重叠哈希分片的重构

由上面的重叠哈希概率包标记思想可知，在多路径攻击下，假设攻击路径数为 *m*，在同一个采样距离的采样边上得到的第 *i* 块 IP 哈希片(其中 $i\in\{1,2,\cdots,8\}$)就会有 *m* 个不同的值。由于采用一种改进的分片与哈希组合方法(如图 3 所示)，因此在重构的时候，就可以从第 *i* 块 IP 哈希片(其中 $i\in\{1,2,\cdots,8\}$)推出在同一个路由器中的第 *i*+1 块 IP 哈希片(其中 $i\in\{0,1,\cdots,7\}$)。从而不需要用穷举法去组合这些 IP 哈希片。因为边采样是相邻节点对应位的异或，所以在对前面节点的 IP 哈希片进行异或以后，再进行分片哈希的组合。对第 *i* 块 IP 哈希片的 *m* 个不同的值的每一个值，先取出它的低 4 位，进行一次 4 位的哈希，再与第 *i*+1 块 IP 哈希片的 *m* 个不同的值的高 4 位比较，如果相等，说明它们来自于同一个节点。如果 8 组 IP 哈希分片之间可以通过 4 位的哈希函数连接起来，取出连接 IP 哈希片的低 4 位组合成为 IP 地址，与前面进行异或的节点组成原来的采样边。得到所有的采样边后，即可重构出所有的攻击路径。

```
Path reconstruction procedure at victim v:
Let Mat be a table of tuples mat(distance, offset, count)
Let G be a tree with root v
Let edges in G be tuples (distance, start , end)
Let maxd:=0
Let last:=v
For each packet w from attacker
  Mat.Insert mat(w.distance,w.offset,
count[w.distance,w.offset])=w.addr8
  Increment count[w.distance,w.offset]
If w.distance>maxd then
Maxd:=w.distance
End
End
For each distance d in mat
    If(d!=0)
 Mat(d,w.offset,count[d,w.offset]) xor the addrs A in distance-1
    End
    For offset=0:7
     We use the 4bits hash relations to connect the segmentations
and chance them into addrs B
If    d==0
        Insert   edge(0, v, B)    into G
Else
       Insert   edge(d, A, B)   into   G
End
End
End
Extract path(R_i⋯R_j)by enumerating acyclic paths in G
```

3 重叠哈希分片概率包标记的性能分析

3.1 重构路径所需的数据包数

重构路径所需要的数据包数目是评价概率包标记算法的一个重要的性能指标，反映了概率包标记算法的效率。

如图 1 所示，由传统 PPM[1]可知，受害者重构一条长度为 *d* 的攻击路径所需要的数据包数量 *N* 的期望值为 $E(N)<\frac{d\ln(d)+O(d)}{dp(1-p)^{d-1}}=\frac{\ln d}{p(1-p)^{d-1}}$，而且每个路由器 IP 地址分成 *k* 个分片，如果攻击路径中有 *d* 个路由器，则共有 *kd* 个分片。假设每一个分片都可能以 $p(1-p)^{d-1}$ 的概率标记，重构路径所需要的数据包数量的期望值为 $E(N)<\frac{k\times\ln(kd)}{p(1-p)^{d-1}}$。传统 PPM 边分片数为 8，所以其重构路径所需要的数据包数约为 $\frac{8\times\ln(8\times d)}{p(1-p)^{d-1}}$。

OHF 方案采用自适应概率标记数据包。路由器标记数据

包的概率为 $1/d_A$(d_A 是路由器距离攻击者的跳数)，确保每个路由器标记过的数据包到达受害者的概率都为 $1/d$，其中，d 为攻击路径长。如 DPPM[3]、DPPM 重构路径需要的数据包为 $E(N)=\frac{k\times\ln(kd)}{1/d}=kd\times\ln(kd)$，其中，$k$ 为分片数；d 为攻击路径长度。而 OHF 分片数为 8，所以，$E(N)=kd\times\ln(kd)=8d\times\ln(8d)$，如图 5 所示为在 NS2 环境下 PPM 和 OHF 的仿真实验的统计结果，表明了 OHF 比 PPM 需要更少的数据包即可重构出攻击路径。

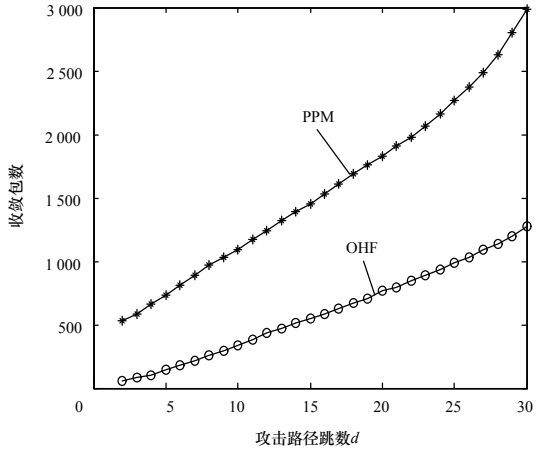


图 5 PPM 与 OHF 重构路径需要的数据包数

3.2 重构路径的算法复杂度

假设攻击路径上有 d 个路由，有 m 条独立的攻击路径，由 PPM[1]和 DPPM[3]的重构算法可知，其需要进行 $8\times md$ 次异或和 $m^8\times d$ 次哈希运算，即 $O(8\times md+m^8\times d)$。由 PPM[1]可知，攻击路径上的路由个数至多为 32，即 $d\leqslant 32$，所以，PPM 和 DPPM 的重构路径算法复杂度都为 $O(m^8)$。

而在 OHF 方案，由其思想可知，重构每个采样边需要的运算为 $8\times m$ 次 4 位的哈希与 $8\times m^2$ 次 4 位的比较。那么当攻击路径上有 d 个路由时，就会有 d 个不同距离的采样边，总的运算为 $8\times md$ 次 4 位的哈希与 $8\times m^2d$ 次 4 位的比较，且 $d\leqslant 32$，所以，OHF 方案的重构路径算法复杂度为 $O(m^2)$，比 PPM、DPPM 的重构算法复杂度都要低很多。

3.3 重构路径的误报率

由传统的 PPM[1]算法可知，PPM 重构是逐边往回追踪，其每一个边采样的误报率为 $P_E(PPM)=1-(1-\frac{1}{2^{32}})^{m^8}$，$m$ 为攻击路径数。而 OHF 方案，也是逐边往回追踪，其主要通过构造相邻 IP 哈希分片之间的 4 位哈希关系来重构采样边的。而相邻 2 个 IP 哈希分片的哈希位加起来就为 8 位，当攻击路径数为 m 时，其连接相邻 2 个 IP 哈希分片的误报率为 $\frac{m}{2^8}$，那么连接 8 块 IP 哈希分片的误报率为 $P=1-(1-\frac{m}{2^8})^8$，即 OHF 每个采样边的误报率为 $P_E(\mathrm{OHF})=1-(1-\frac{m}{2^8})^8$。如图 6 所示，PPM[1]和 DPPM[3]在攻击路径数 $m<15$ 时，误报率比 OHF 的要低，两者都保持了较低的误报率。当 $m\geqslant 15$ 时，OHF 误报率比 PPM 和 DPPM 都要低，且其误报率增长缓慢。当 $m=20$ 时，$P_E(\mathrm{PPM})\approx 1$，而 $P_E(\mathrm{OHF})\approx 0.478\ 35$，由此可见，当在大规模分布式拒绝服务攻击下，OHF 比 PPM、DPPM 更有优势，保持了更低的误报率。

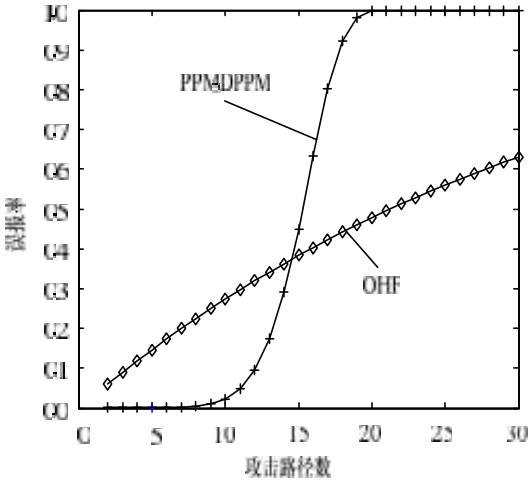


图 6 PPM(DPPM)和 OHF 的边采样误报率

4 结束语

本文提出一种重叠哈希概率包标记方法，理论分析和在 NS2 环境下的实验结果表明，重叠哈希分片方法在不增加包标记位的前提下，降低了重构算法复杂度，同时改善了边采样误报率。下一步的工作是把重叠哈希分片方法应用到 IPv6 追踪。

参考文献

[1] Savage S, Wetherall D, Karlin A, et al. Network Support for IP Traceback[J]. IEEE/ACM Transactions on Networking, 2001, 9(3): 226-237.

[2] 闫 巧, 夏树涛, 吴建平. 改进的压缩边分段采样算法[J]. 西安电子科技大学学报: 自然科学版, 2006, 33(5): 824-828.

[3] Liu Jenshiuh, Lee Zhi-Jian, Chung Yeh-Ching. Dynamic Probabilistic Packet Marking for Efficient IP Traceback[J]. International Journal of Computer and Telecommunications Networking, 2007, 51(3): 866-882.

[4] Dean D, Franklin M, Stubblefield A. An Algebraic Approach to IP Traceback[J]. ACM Trans. on Information and System Security, 2000, 2(5): 119-137.

[5] Wang Xiaojing, Wei Shengjun. IP Traceback Based Probabilistic Packet Marking and Randomized Network Coding[C]//Proc. of the 2nd International Workshop on Computer Science and Engineering. Qingdao, China: [s. n.], 2009: 151-154.

[6] Sattari P, Gjoka M, Markopoulou A. A Network Coding Approach to IP Traceback[C]//Proc. of 2010 IEEE International Symposium on Network Coding. Toronto, Canada: [s. n.], 2010: 1-6.

[7] 宋冬辉, 李丽娟. 改进的概率包标记 IP 追踪方法[J]. 计算机工程, 2011, 37(4): 147-149.

编辑 索书志