# 基于顶点信息采样的随机包标记 IP 追踪算法 NSPPM*)

金 舒 刘凤玉
(南京理工大学计算机科学与技术系 南京 210094)

**摘 要** 本文通过提出一种顶点采样算法及与之相对应的攻击路径重建算法,给出了一种新型的基于随机包标记技术的入侵追踪方案 NSPPM。该方案保持了对现有网络基础设施的兼容并且可以增量地逐渐布置到整个 Internet 中。相比较于一些前期的相关工作,NSPPM 方案可以在仅带来较小开销的情况下为受攻击方提供对多重 DDoS 攻击路径(活跃的或非活跃的)的识别且不需要上游 ISP 的协作。同时,较之传统的基于边采样的攻击路径重建策略,基于顶点采样算法的攻击路径重建策略具有更低的计算复杂度。

**关键词** IP 追踪,随机包标记,NSPPM

## A Node Sampling Approach to Probabilistic Packet Marking-based IP Traceback

JIN Shu LIU Feng-Yu
(Nanjing University of Science and Technology, Nanjing 210094)

**Abstract** In the defending of the distributed denial-of-service attack, which is the most intractable problem in Internet security nowadays, tracing anonymous flooding packets to their sources of origin (IP traceback) is of great importance and in literature there has been considerable interest in this topic. By employing a novel algorithm of node sampling and the subsequent algorithm of attack paths reconstruction, we present in this paper a new solution, namely NSPPM, to address the problem of IP traceback, which can be deployed incrementally while providing backwards compatibility with the existing network infrastructure. As compared with previous work, our approach allows a victim to identify the paths of multiple attack traffics both "on-going" and "post-mortem" without requiring the operational support of Internet Service Providers (ISPs) only at the cost of some computations added to each router with a trivial overhead. Moreover, the approach offers an efficient attack path reconstruction algorithm, which successfully circumvents the combinatorial explosion problem incurred by other techniques.

**Keywords** IP traceback, Probabilistic packet sampling, NSPPM

## 1 前言

随着诸如电子邮件、网络购物、即时通讯等服务在人们日常生活中的使用,Internet 正在社会和经济领域产生着越来越大的影响。在任何时间、任何地点向任何人提供网络连接的同时,Internet 的应用也随之带来了很多安全问题。其中分布式拒绝服务攻击(DDoS)被认为是一类最难解决的问题。近年来发生的一些重大网络安全事件,如 2000 年 Yahoo、Amazon、EBay 等电子商务网站遭遇 DDoS 攻击而瘫痪;2001 年称为"Red Code"的蠕虫攻击白宫网站迫使其将内容转移至备用服务器等。据媒体报道,2000 年全年网络安全入侵使全球范围内的企业共损失了约 14 亿美元,这其中 60%的损失源于病毒及 DDoS 攻击。而考虑到某些企业为了形象而隐瞒了网络安全事件,上述数据可能仅是冰山的一角。结合近来各种网络攻击软件越来越容易操作且被不断大量地传播,DDoS 攻击数量在将来的一段时期内仍将处于一个不断上升的状态。

考虑到 Internet 设计上的局限[1~3],在不对其路由基础设施做出重大改进的情况下,并不可能找到一种彻底杜绝分布式拒绝服务攻击的方法。出于这些原因,特别是 IP 伪装技术的存在,我们为研究设定了一个更实际的目标即尽可能地[4~6]追踪至 DDoS 攻击的源头:攻击发起者的计算机(攻击数据包没有进行 IP 伪装)或攻击发起者所处的局域网(攻击数据包进行了 IP 伪装)。在我们给出的 IP 追踪方案中,经过功能增强(加入用于采样数据包传递路径中的顶点信息的随机包标记技术)后的路由器以一定的概率随机地对过往的数据包进行采样并将自身的识别信息通过带外数据流一同发送至被采样数据包的目的地址。这样,当受害主机通过某种机制(如入侵检测)确认其正在遭受分布式拒绝服务攻击时,该主机可以通过收集由攻击路径上各路由器发送来的带外数据重建整个攻击路径,从而追踪到该次攻击的发起方(即使此时攻击已结束)。

## 2 相关工作

为了对分布式拒绝服务攻击的发起者进行追踪,从而通过对其施加威慑来减少该类攻击事件的发生,人们提出了很多解决方案。这些方案主要分为两大类:即需要上游 ISP 协作的 IP 追踪方案(文[7~9])和通过为网络中的路由器增加相应的功能以实现自动 IP 追踪过程(文[4, 10~12])。按照执行 IP 追踪操作人手的不同角度,本节将这些方案分成 4 类

*)本文受到国家自然科学基金资助项目(60273035)—"软件抗衰和自愈"、南京理式在学科研发燕尾服基金 2005-"网络性能诊断与安全"资助。
金 舒 博士研究生;刘凤玉 教授,博士生导师,研究方向:信息安全技术、软件抗衰技术。

并分别对其做出具体介绍。

### 2.1 源地址过滤

攻击发起者对 IP 伪装技术的应用是 IP 追踪的一大障碍。若没有经过 IP 伪装，任何 DDoS 攻击流中的数据包都可以被用来进行协议分析，提取其源 IP 地址，从而轻易地追踪到该次攻击的发源地。为了彻底防止 IP 伪装的发生，P. Ferguson 与 D. Senie 提出了“Ingress Filtering”[8] 的概念，即在网络服务提供者的接入服务器上加入简单的认证机制，对于发自用户方并准备送入 Internet 的数据包，接入路由器会逐一检查其源地址。如果其源地址在用户所处的子网范围之内(或更进一步，来自该用户)，接入路由器将对其进行正常转发；若其源地址在用户所处的子网之外(包括无效 IP 地址)，接入路由器将丢弃该数据包。虽然该技术一经采用将能有效地防止 IP 伪装的发生，但由于对该技术的应用并不会为各 ISP 带来大于其投入成本的经济利益，这项技术一直没有得到大规模的采用。具有同样命运的“Egress Filtering”[9] 技术也基于类似的原理，其源地址过滤机制位于局域网连接 Internet 的出口路由器上，且仅允许以局域网内有效 IP 地址作为源 IP 地址的数据包通过。

### 2.2 链路测试

一种符合直觉的 IP 追踪方案(“Input Debugging”)是：当发现自身正受到分布式拒绝服务攻击时(短时间内有大量数据涌入)，受害者将向直接与其相邻的路由器(位于其“上游”的 ISP 接入路由器)询问其来源。在确定该组攻击数据流入接口后，该路由器将进一步向位于其上游的(与该接口相连)路由器发送相应的查询。该过程将被持续地执行，直至追踪到攻击的发起者。上面描述的入侵追踪过程由于极大地依赖于攻击路径上各级安全相关工作人员的相互协作和干预，因而实用性大大地受到限制。为解决该问题而提出的“CenterTrack”[7] 方案，可以自动地执行上述的逐级状态查询操作，从而使链路测试技术能够真正得到实际应用。

Burch 与 Cheswick 提出了一种类似的 IP 追踪方案——受控洪泛(“Controlled Flooding”)[5]。在该方案中，受攻击的网络主机将以自身为出发点构建其周围 Internet 的连接拓扑图[13,14]，在此基础上，该主机将向与其直接连接的路由器逐个发送大量噪声数据，并观察 DDoS 攻击数据流是否有减少。如果有减少，则表明攻击数据来自该路由器。再以该路由器为出发点进行同样的受控洪泛操作，持续执行该过程，直至最终追踪到攻击的发起者。由于 Internet 拓扑结构的动态性，为其建立连接拓扑图将十分困难。作为链路测试(“Input Debugging”)技术的两种实现，受控洪泛与 CenterTrack 一样都只能追踪正在进行中的 DDoS 攻击。一旦攻击停止(或依照一定的时间间隔发起)，这两种方案都将无能为力。

### 2.3 路由端日志

日志机制作为一种与系统性能实现相关的权衡因素总会引发一些争论。不考虑随之带来的有关隐私的问题，在路由器上加入数据日志功能，以记录下所有来往数据包的信息，可以为事后追查入侵者提供证据支持。考虑到 Internet 上一个典型的路由器每秒将转发约 2000 万个数据包[15]，若每个数据包平均长 120 字节，为了将这些数据包记入日志，每秒钟需要约 2.4G 的存储空间。即使仅记录协议相关信息(设为 28 个字节：20 字节的 IP 数据包头部加上负载的上层应用协议的前 8 个字节)，每秒也需要占用超过 500M 的存储空间。巨大的数据开销使得在路由器端记录所有的数据包信息几乎不可能。在对安全性要求较高的场合，有选择地将部分数据包中的信息记入日志中就成为一种较现实的选择。

### 2.4 概率方法

作为近年来提出的一种新的 IP 追踪策略，基于概率的数据包标记方法(Probabilistic Packet Marking, PPM)[4, 16~19] 显示出了很好的实用性。这些 IP 追踪方案都在保持与现存设备兼容性的基础上通过增强现有路由器的功能，使其能够以一定的概率(设置得很小，以防止占用过大的带宽，从而影响数据包转发的性能)对过往的数据包进行采样，并将与自身识别相关的信息(如 IP 地址)与该数据包一起发送至目的地。这样，当某台主机发现正受到 DDoS 攻击时，虽然包标记所依据的概率很小，但由于 DDoS 攻击巨大的数据量，受攻击方仍能收集到足够数量的标记数据包，并可以根据其中提供的信息通过执行攻击路径重建算法来重建 DDoS 攻击路径，从而对发起者进行追踪。基于相似的设计，“ICMP Traceback”[20] 方案中的路由器以 1/20000 的概率采样过往数据包，并将自己的 IP 地址通过 ICMP 带外数据一并发送至采样数据包的目的地址，以便目的主机在万一受到 DDoS 攻击时可以对其进行追踪。

即使是当 DDoS 攻击已结束的情况下，因为之前攻击中大量数据的涌入，使受攻击机器收到足够多的标记数据包，仍可能在这些信息的帮助下重建攻击路径，并找到攻击的发起者。因而，可以认为概率包标记方法不仅能够像其他方法那样追踪正在进行中的 DDoS 攻击，还可以为已结束的 DDoS 攻击提供事后追踪的线索。在具有概率包标记方法所有这些优点的基础上，我们提出的基于顶点信息采样的随机包标记算法(NSPPM)可以以相对较小的开销提供对多重攻击路径重建的支持。

## 3 问题与假设

IP 追踪作为一种确定 DDoS 攻击发起者的技术，既可以通过在分布式拒绝服务攻击发生的当时及时追踪到发起者，以便对其警告或更进一步对其诉诸法律行动，也可以对潜在的攻击者构成极大的心理威慑。在具体介绍基于顶点信息采样的随机包标记 IP 追踪策略及其相应的多重攻击路径重建算法之前，本节给出对 IP 追踪问题的形式化描述及为了简化 IP 追踪问题在整个算法设计中所遵循的一组假设。

### 3.1 问题的定义

将运行有可被 Internet 上其他主机访问的服务的计算机称作服务器。若由于在短时间内收到来自不同非法用户(Attacker)的大量服务请求而导致网络带宽、运算资源或存储资源严重消耗，从而造成对合法用户提供服务能力的急剧下降，则可认为受到分布式拒绝服务攻击，此时为受攻击者(Victim)。

**定义 1** 用 $A$ 表示攻击者的计算机(IP 地址)，$V$ 表示受到攻击的计算机(IP 地址)，$R_1, R_2, \cdots, R_n$ 表示攻击数据流从 $A$ 到 $V$ 所经过的一组路由器(IP 地址)，定义序列 $A, R_1, R_2, \cdots, R_n, V$ 为从攻击者 $A$ 至被攻击者 $V$ 的一条攻击路径(Attack Path, $AP$)：

$AP=\mathrm{Seq}\{A, R_1, R_2, \cdots, R_n, V\}$。

**定义 2** 分布式拒绝服务攻击定义为一组攻击路径的集合，即 $\bigcup_{i=0}^{n} AP_i$，$(n>>2)$。

**定义 3** 给定一组标记数据包 $Pkts=\bigcup_{i=0}^{n} Pkt_i$ $(n>>2)$，对任意的算法执行过程 $TB$，如果成立 $A=TB(Packets)$，

则 $TB$ 过程称为 IP 追踪。

**定义 4** 连接用户计算机($H_i$)或局域网($N_i$)与 Internet 的路由器称作边界路由器(Edge Router，$ER$)。其上与用户计算机相连的接口当接收发送自用户计算机的数据包转发入 Internet 时，称为网络进入点(Ingress Point)；当将 Internet 中传来的数据包发送给该相连的用户计算机时称其为网络逸出点(Egress Point)。

**定义 5** 仅与 Internet 中的路由器连接而不与用户计算机相连接的路由器称为中介路由器(Relay Router，RR)。

**定义 6** 以网络中的路由器、攻击者的计算机和被攻击者的计算机为结点，以其相互间的连接关系为边并指出攻击路径的示意图，称作 DDoS 攻击示意图。

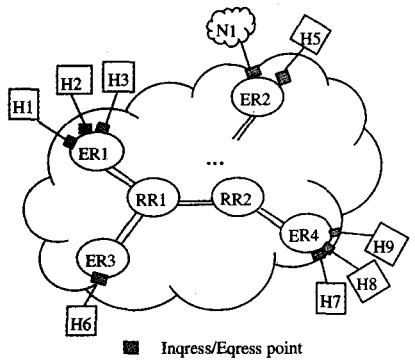


图 1 Internet 拓扑结构及路由器分类

在图 1 所示的 Internet 结构示意中，边界路由器 $ER1$，$ER2$，$ER3$，$ER4$ 分别将用户主机 H1～H9 及局域网 N1 接入 Internet。作为中介路由器的 $RR1$ 与 $RR2$ 与网络中的千万台路由器一样成为整个 Internet 基础设施的一部分。图 2 从被攻击者的角度给出了一个 DDoS 攻击示意图的实例。图中的路由器 $R6$，$R4$，$R7$，$R8$ 为中介路由器；$R1$，$R2$，$R3$，$R5$，$R9$，$R10$ 为边界路由器，用户主机 H1，H2，V，A1，A2，A3(被攻击者计算机与攻击者计算机也是通过边界路由器接入互连网络中的普通用户计算机)通过它们接入 Internet。从攻击者计算机 $A1$，$A2$，$A3$ 分别发出、目标为被攻击者 $V$ 的 3 条攻击路径 $AP1$，$AP2$，$AP3$ 也在图中分别标示出来。

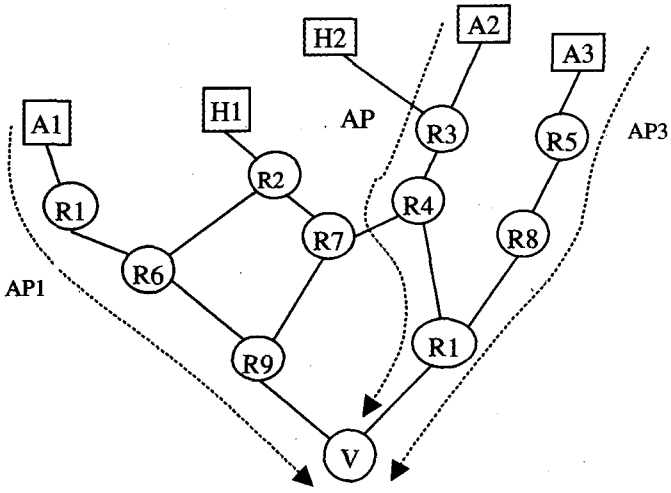


图 2 从被攻击者角度看到的 DDoS 攻击示意图

### 3.2 一组假设

随着地区性子网的不断加入，Internet 正变得越来越庞大，完整地获取其拓扑结构已成为不可能。网络中的各路由器的路由表也随着网络拓扑结构的变化在不断地变化，加之此起彼伏的宕机重启、断线维护、安全入侵等等事件的发生，Internet 的局部状态正变得越来越难以预测。考虑到 Internet 环境的复杂性及前面分析得出的在使用现存的数据转发基础设施的情况下很难从根本上避免很多种类攻击的发生，我们通过提出一组假设来简化 IP 追踪问题，该组假设的提出部分参考了 Savage 等人在文[4]中所做的工作。

- 任何形式的有效数据包都能被送入 Internet；
- 任何数据包都可能被丢弃(概率较低)；
- 单个攻击者之间可以互相协调，以共同发动规模较大的攻击；
- 攻击者向被攻击的目标计算机发送大量数据包；
- 攻击者有可能发现正被追踪；
- 攻击路径上的路由器没有遭到大规模的破坏；
- 攻击路径上的路由器路由表稳定(数据包的转发路径也随之固定)；
- 路由器上可用于数据包转发工作以外的执行能力、存储能力和带宽十分有限；
- 用户计算机上留给入侵追踪功能的计算能力和存储能力十分有限。

## 4 NSPPM 算法

采用 NSPPM 算法的 IP 追踪方案依据其在转发数据包过程中扮演的角色的不同，为边界路由器和中介路由器分别设计了相应的包标记算法。其中边界路由器负责在不影响正常数据转发的情况下为每个通过其网络进入点送入 Internet 的数据包标记上路径特定信息 PSI (Path Specific Identification，用于识别数据包所处的传输路径，其编码方案将在下节给出)。由于该标记将在数据包的整个传输过程中保持不变，其可用于识别相应数据包在网络中传输的路径的始端(进入点)。同时，由于具有相同 PSI 的一组数据包位于同一条攻击路径上，进而 PSI 也可以作为对该数据包的整个传输路径的一种标识。中介路由器类似地以一定的概率将自身位置信息(顶点信息)标记入经其转发的数据包中。被攻击的计算机在发现遭受到分布式拒绝服务攻击后，可以通过对其收集到的标记数据包执行多重路径重建算法来追踪攻击的发起者。

边界路由器中所执行的包标记算法如算法 1 所描述：表示路径特定信息的 PSI 被计算出来，并赋予每一个从网络进入点送入的数据包，以作为对其进入 Internet 位置的标识；对于从网络进入点送入的每个数据包，边界路由器依据概率 $p$ ($p<<1$)决定是否对其进行标记，即将结点信息(该边界路由器的位置 IPER)标记入该数据包，并设其距离为 1，表示该顶点为数据包转发路径上的第一个结点。

**算法 1** 边界路由器包标记算法

```
calculate PSI from ER
for each packet w coming from the ingress points
  w. psi←PSI
  w. distance←0.
  generate a random number －x from[0. . 1)
  if x<p
  then
    w. node←IP_ER.
  w. distance←1
```

与边界路由器类似，中介路由器以概率 $p$ 对通过转发的所有数据包进行标记，以将其传输路径上的该顶点信息（路由器的 IP 地址）记入数据包中，并设置其距离字段为 1。对于落在概率 $p$ 之外（极大的概率）的其他数据包，中介路由器将检查其是否在传输中已被标记上路径中某结点的信息（w. distance≠0）。如果发现已被标记，则将该字段加 1，以表示该数据包在网络中又传经过一台路由器（一跳）。经过边界路由器与中介路由器的标记，在足够多的到达目的地的数据包中将会包含传输路径上所经过的所有结点的信息，即各路由器的地址及其与该目标计算机之间的跳数距离（由 distance 字段给出）。

**算法 2** 中介路由器包标记算法

```
for each packet w to be forwarded
    generate a random number—x from[0..1)
    if x<p
    then
      w. node←IP_RR
      w. distance←1.
    else
      if w. distance≠0
      then
        w. distance←w. distance+1.
```

由于受到 DDoS 攻击时将收到大量的发送自攻击者的数据包，当其数目达到一定值时（在理想情况下仅与 $p$ 相关），被攻击的计算机可以获得用于重建攻击路径所需要的完整的信息，并通过执行算法 3 最终追踪到攻击数据的注入点（有 IP 伪装的情况下）。算法 3 给出了受到 DDoS 攻击时，在被攻击计算机上执行的攻击路径重建算法。AP 为算法中记录一条路径信息的数据结构，其中字段 distcounter 用于记录被攻击计算机上所收到的来自不同距离的结点的标记数据包的条数。该字段虽然并不直接应用于攻击路径的重建，但其包含的统计信息可以用于对重建的攻击路径的正确性进行判断。AP 结构中的另一个字段 nodes 用来记录该路径上距离被攻击计算机不同跳数的结点的位置信息（路由器 IP 地址），而 max_hops 字段表示路径的长度。运行攻击路径重建算法的计算机，从收到的每个数据包中提取其路径特定信息 PSI，并在 MAP 数据结构 APS（PSI，AP）中为该路径建立相应的映射表项。随后，所有标记数据包（其 distance≠0）中记入的相应顶点信息将被填入与其路径相连的 AP 数据结构中。APS Map 中的每个 AP 对象表示一条攻击路径，在获取了完整的数据后（各 AP 对象的相应字段均已赋值），仅将其 nodes 字段按顺序列出，就可得到相应的一条攻击路径。

**算法 3** 击路径重建算法

```
let AP(Attack Path) structure contains:
    int distcounter [maxd].
    Node nodes [maxd].
    int max_hops.
let APS (Attack Path Set) be the map of (PSI, AP)
for each attack packet w in a DDoS attack
    if w. psi is not contained in APS
    then
      insert a new item (w. psi, new AP) into APS
      if w. distance≠0
      then
        APS [w. psi]. distcounter [w. distance] ← APS
        [w. psi]. distcounter [w. distance]+1.
        APS [w. psi]. nodes. [w. distance]←w. node.
        APS [w. psi]. max_hops←w. distance.
          for each psi contained in APS
              extract an attackpath: APS [psi]. nodes [1]
              ··· APS [psi]. nodes [max_hops]*
```

与传统的基于边信息采样的随机包标记方案[4,5]中应用的相对较复杂的攻击路径重建算法相比较（从边信息中构建图），基于对顶点信息采样的随机包标记算法 NSPPM 中的攻击路径重建仅包含一些赋值与查表操作，从而可以近似认为其具有 $O(n)$ 的时间复杂度（$n$ 为执行该算法的计算机收到的数据包数）。考虑到一台连网主机正常情况下与外界连接的数目相当有限，NSPPM 方案中的攻击路径重建算法的空间占用仅与 DDoS 攻击的路径数目 $m$ 线性相关，即算法具有 $O(m)$ 的空间复杂度。作为具有线性复杂度的算法，相对于传统的基于采样的边信息进行的攻击路径重建算法，NSPPM 攻击路径重建算法极大地减少了被攻击计算机端对攻击路径进行重建所需要的开销。特别是在经受到 DDoS 攻击而被攻击计算机执行能力极度缺乏的情况下，NSPPM 攻击路径重建算法的低开销特性就显得更加重要。

## 5 编码

图 3 给出了 IP 数据包包头的结构，图中用阴影标记的字段相对于其他字段而言，对报文的传输并不起决定性的作用。为了在给 IP 数据包进行标记后不影响其在 Internet 中的继续转发，NSPPM 算法在标记顶点采样信息（路由器 IP 地址及其与目标计算机之间的距离）时仅用到 IP 包头中的这些用阴影所标识的字段作为标记信息的载体。其中，路由器 IP 地址及其与目标计算机之间的距离用“TOS”和“identification”两个字段作为载体，而路径特定信息 PSI 则以紧邻 IP 数据包头部的 4 个 IP Option 为载体。如果此位置已存在 IP Option，则将用来标识 PSI 的 4 个 IP Option 链接在其后，即 IP 数据包中的最后 4 个 IP Option 被用来保存 PSI 信息。

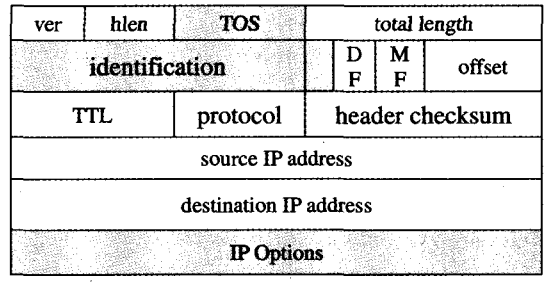


图 3 IP 数据包头部结构

### 5.1 路径特定信息（PSI）的编码

边界路由器（ER）在所有通过它送入 Internet 的用户数据包上标记自身的识别信息，即其 IP 地址 $IP_{ER}$。由于该标记在数据包的整个传输过程中保持不变，因此可用于受攻击计算机在通过收集到的众多标记数据包重建攻击路径时确定各个数据包所处的路径。由于边界路由器的 IP 地址 $IP_{ER}$ 具有

32位，而IP数据包包头中并没有足够的空间，NSPPM算法并不直接将其作为PSI，而是通过对其执行散列函数（如MD5）后再取结果的前20位作为PSI的取值，即

PSI=get_left_n_bits (hash ($IP_{ER}$), 20)

计算出PSI之后（路由器启动时即可完成执行），将每个从网络进入点收到的IP数据包转发至Internet之前，边界路由器将会在其包头信息的最后加上4个IP Option，其中每个IP Option含有PSI 20位信息中的5位。为了不影响该数据包此后的转发，新增的4个IP Option中表示其类型的class字段均被设为保留值3。图4给出了完整的路径特定信息PSI编码方案。考虑到在Internet中传递的数据包的均长度约为420个字节，用于标记PSI的4个IP Option字节的增加仅将网络流量提高了不到1%，并不会对整个Internet数据传输带来多大的影响。

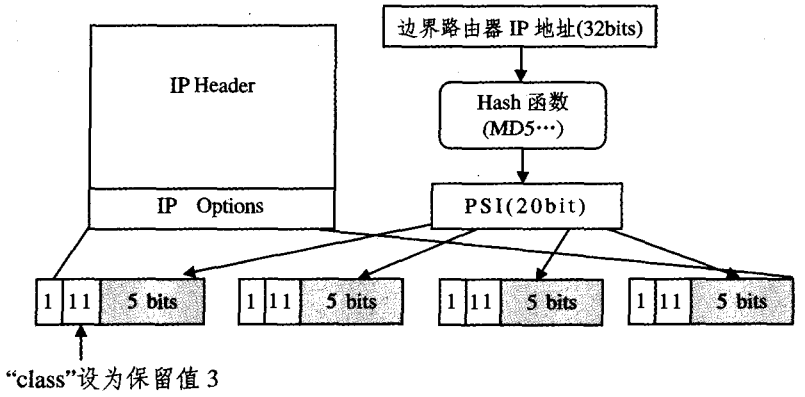


图4 路径特定信息PSI编码方案

### 5.2 顶点信息编码

边界路由器和中介路由器都会以概率 $p$ 将自身的识别信息标记在经其转发的IP数据包中，该识别信息中包括路由器的IP地址及其与目标计算机间的距离（即"跳数"，初值为1，每经过一次转发，由相应的路由器加1）。上述的由路由器标记的识别信息即为攻击路径上的顶点信息，将在对攻击路径进行重建时使用。本节给出对顶点信息进行编码的两种方案。

#### 5.2.1 保守方案

在应用该方案对包转发路径上的顶点信息进行编码时，路由器将其自身具有的32位IP地址分成4个字节，并在标记经转发的数据包时将其中的一个字节写入该数据包identification字段的前8位中。接着写入的是该字节在路由器IP地址中的偏移（即该字节在整个IP地址中所处的位置0～3），此偏移值（part num）占用identification字段中随后两位。路由器将在执行的过程中维护一个两位（2 bits）的循环记数器，并根据其值在标记过往数据包时写入其IP地址的相应部分。由于该计数器在每次执行标记后增加1，且在达到4时回滚至0，路由器IP地址的4个字节因而可以被均匀（等概率）地标记于过往的数据包中。被攻击的计算机可以通过收集到4个由相同路由器标记的数据包（PSI相同，distance相同，part num分别为0,1,2,3）来获取该顶点的位置信息。由于Internet数据通讯中很少有数据包会经过30跳以上的转发[4]，distance标记占据identification字段中剩下的6位（其可表示 $2^6=64$ 跳的距离），足够用来表示路由器到目标地址的距离。该顶点信息编码方案的示意图见图5。

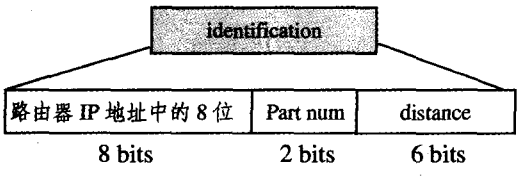


图5 顶点信息编码的保守方案

#### 5.2.2 积极方案

不同于上面给出的保守方案，如图6所示在积极的顶点信息编码方案中，完整的32位路由器IP地址将被直接标记入数据包的identification（16位）和4个新增的IP Option（各提供4位空间）中，这4个IP Option将链接在标记PSI的4个IP Option之前；而distance标记将占据TOS的5位（3个被忽略的优先级为一个保留位及4个TOS位中的任意一位，这里采用的是"最小通信成本"位，最大可表示 $2^5=32$ 跳的距离）。这样，被攻击的计算机只要接收到一个由某路由器标记的数据包，即可确定其位置及与其之间的距离，从而得出该结点在攻击路径上的位置。该积极顶点信息编码方案可以使得重建攻击路径所需要接收的数据包的数量较之保守方案极大地减小，付出的代价是增加了额外的约1%的网络流量。

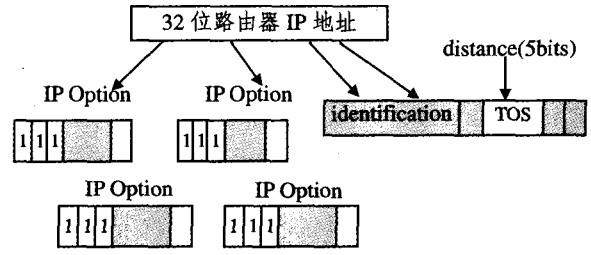


图6 顶点信息编码的积极方案

## 6 讨论

给定各路由器上执行包标记的概率 $p$ 与攻击路径的长度 $d$（攻击者与被攻击者之间的路由转发跳数），在理论上被攻击者仅需收集 $1/p(1-p)^{d-1}$ 个数据包就可以得到重建整条攻击路径所要需的信息。在实际的网络环境中，由于丢包、超时等种种不可预见的因素，为在被攻击端重建一条攻击路径需要接收更多的数据包，以保证其中包含整条路径的信息。Savage等人在文[4]描述的工作中提出：被攻击者需要至少接收到 $N$ 个数据包才能保证以 $(c-1)/c$ 的概率重建整条攻击路径。计算 $N$ 的公式在下面给出，其中 $k$ 表示发送攻击路

径中一条边(对于顶点仍然适用)的完整位置信息需要的标记包的数目:

$$N=\frac{k\ln(kdc)}{p(1-p)^{d-1}}$$

在不考虑其他因素的理想情况下,将 $d$ 看作常量参数,当 $N=1/p(1-p)^{d-1}$ 取最大值时,有 $p=1/d$。而在发生具体的分布式拒绝服务攻击时,由于多条路径间的不对称性(各路径的 $d$ 值可能有较大的差异)等因素的影响,简单地依此选择参数 $p$ 的取值并不合适,其值的选取需要结合对 DDoS 攻击中的流量、范围、攻击时间等信息的统计分析。

在相关的研究中,对于随机包标记技术中概率 $p$ 的选择多采用经验值。常用的两个概率 $p$ 的取值是 Savage 等人在文[4]中给出的 1/25 及 Bellovin 等人在文[20]中给出的 1/20000。分别以这两个参数代入 $N$ 的计算公式,得到如图 8 和图 9 显示的结果。从该两组结果中可以看出,虽然在保守的顶点信息编码方案中含有标记信息的数据包长度较小(载荷比较高从而对带宽占用较小),但由于需要收到要成倍数目的数据包才能保证获得重建整个攻击路径的信息,该方案的综合效率较低。与之相比较,积极的顶点信息编码方案因具有与理想值近似的数量级而显示出很高的效率。

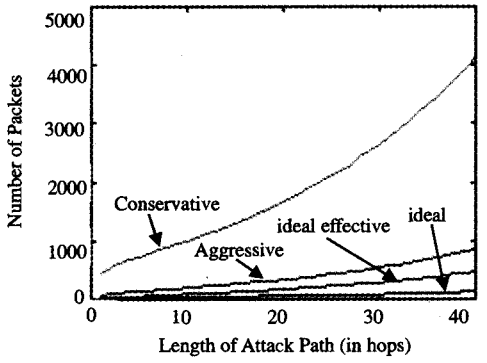


图 8 重建攻击路径需要的数据包数目($p=1/25$)

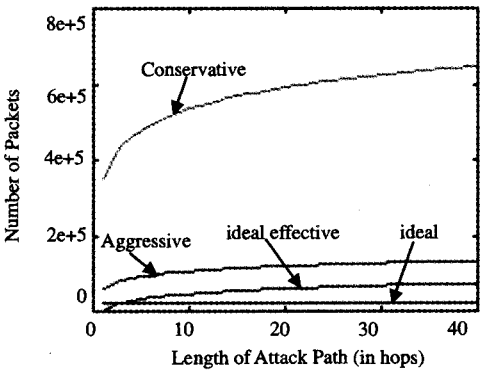


图 9 重建攻击路径需要的数据包数目($p=1/20000$)

一旦大规模地布置到 Internet 中,NSPPM 入侵追踪方案将可能遇到以下这些挑战:(1)中介路由器被攻击者操纵并给转发的数据包赋予无效的 distance 信息。给定一个用于表示一条攻击路径的数据结构 AP,通过其 distcounter 字段中含有的关于收到来自各个不同距离上的顶点所发送的标记包的数目统计信息,可以识别出这些无效距离信息。(2)边界路由器被攻击者操纵并为发出的数据包赋予随机的(或多个)PSI 值,此时仍可识别多条源头指向该路由器的攻击路径仍可被识别,不过巨大数量的 PSI 将可能耗尽试图重建攻击路径的计算机的资源,从而从另一个角度形成拒绝服务攻击,因此需要对边界路由器加强安全防护。(3)边界路由器还可能被攻击者操纵并为发出的数据包赋予随机的(或多个)distance 值,由于各中介路由器仅对已含结点标记的数据包的 distance 字段进行递增,此时只需简单地把算法 3 中由'*'标示处从:

extract an attack path: APS [psi]. nodes [1] … APS [psi]. nodes [max_hops]

改为

find the first i that APS[psi]. nodes [1]! =nil
if i>max_hops
then
max_hops←$2^{\text{bit of the distance field}}$-(i-max_hops).
i←0.
loop: extract an attack node: APS [psi]. nodes [i].
if i<max_hops
then
i←i+1.
goto loop.

即可解决该问题(已考虑 max_hops 取值大于最大容许值 $2^{\text{bit of the distance field}}$ 时的回绕)。NSPPM 算法并不支持对长度超出最大容许值(如两种顶点信息标记方案中所分别给出的 $2^6=64$ 和 $2^5=32$)的攻击路径的重建。

**结论及未来工作** 基于对顶点信息进行采样并依据其重建 DDoS 攻击路径的 NSPPM 算法,在仅带来较小开销的情况下(在每个 IP 数据包中加入 4 字节的 PSI 信息,将把 Internet 中的数据流量增加约 1%;而标记数据包较之标记前长度增加约 2%长度。考虑到路由器仅以很小的概率 $p$ 对过往的数据包进行标记,该开销 $p*2\%$ 在很大程度上可以忽略不计)为受攻击方提供了对多重 DDoS 攻击路径(活跃的或非活跃的)自动重建的支持。且较之传统的从边采样信息中重建攻击路径的算法,在顶点信息采样基础上执行的攻击路径重建算法时空复杂度更低,从而在真正面对 DDoS 攻击时能够更加有效地工作。

对参数 $p$ 的选取还需要通过对不同类型分布式拒绝服务攻击的攻击时间、数据包的特点(如长度、分段、服务类型)、协作的规模获取相应的统计数据并进行相应的分析和研究。下一步拟通过软件模拟深入研究 NSPPM 算法的实际运行性能,并探索相应的将现存路由器增强为边界路由器和中介路由器的实现方法。

## 参 考 文 献


1 Comer D E. Internetworking with TCP/IP volume II, Design, Implementation, And Internals. New Jersey: Prentice Hall, 1994
2 Huitema C. IPv6 - The New Internet Protocol. Second Edition. New Jersey: Prentice Hall, 1998
3 Yurcik W, Doss D, Kruse H. Challenges to the End-to-End Internet Model [A]. In: Proceedings of the Americas Conference on Information Systems (AMCIS)[C]. 2000,8
4 Savage S, Wetherall D, Karlin A, et al. Practical Network Support for IP Traceback [A]. In: Proceedings of the ACM SIGCOMM Conference [C], 2000, 8. 295~306
5 Burch H, Cheswick B. Tracing Anonymous Packets to Their Approximate Source [A]. In: Proceedings of the 14th Systems Administration Conference(LISA)[C], 2000. 319~327


(下转第 49 页)

53 Lipmaa H, Asokan N, Niemi V. Secure Vickrey auctions without threshold trust. In: M. Blaze, ed. Proc. of 6th FC Conference, volume 2357 of LNCS. Springer, 2002
54 Shneidman J, Parkes D C. Specification Faithfulness in Networks with Rational Nodes. In: Twenty-Third Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2004), July 2004
55 Shneidman J, Parkes D C, Massoulie L. Faithfulness in Internet algorithms. In: Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems Sep. 2004
56 Phelps S, McBurney P, Parsons S, Sklar E. Applying genetic programming to economic mechanism design: evolving a pricing rule for a continuous double auction. In: Proceedings of the second international joint conference on Autonomous agents and multi agent systems. Jul. 2003
57 Conitzer V, Sandholm T. Automated mechanism design for a self-interested designer. In: Proceedings of the 4th ACM Conference on Electronic Commerce. Jun. 2003
58 Conitzer V, Sandholm T. Applications of automated mechanism design. In: Proceedings of the UAI Bayesian Modeling Applications Workshop, Acapulco, Mexico, 2003
59 Nisan N, Segal I. The communication requirements of efficient allocations and supporting prices. Journal of Economic Theory, 2006. Forthcoming. http:// www. stanford. edu/~ isegal/prices. pdf
60 Larson K, Sandholm T. Mechanism design and deliberative agents. In: Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems Jul. 2005

(上接第 19 页)

再根据引理 1～3，我们有

$$NC_{s_i^1,s_i^a}(0)$$
$$=q+\sum_{i\notin P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)+\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$+\sum_{\substack{i+a\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$=q+\left(\frac{-1+a}{q}\right)-\sum_{i+1\in Q_0}\left(\frac{i}{p}\right)+\left(\frac{-a+1}{q}\right)\sum_{i+a\in Q_0}\left(\frac{i}{p}\right)$$
$$-p-\sum_{i\in P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)$$
$$=q-p+1。$$

所以，当素数 $p$ 和 $q$ 恒定时，序列$\{s_i^1\}$和其它任意一个NMJS具有同样的无转移互相关值，这个值在 $p$ 和 $q$ 为孪生素数时取得最小。

对于任意非零的 $\omega$，如果 $A_s(\omega)=C_{a,b}(\omega)=\frac{-1}{n}$，则称$\{s(i)\}$具有理想的相关值分布。实际上，满足这样的条件是非常困难的。对于密钥流序列，只要它们的相关值的分布相对比较平坦就可以了。为满足密钥流序列大周期的需要，本文中的 $p$ 和 $q$ 的取值都比较大(大于 48 比特)。由定理 1 和 2 可知，这时的相关值分布是非常平坦的。具有平坦的低相关值分布的序列也具有平坦的二元段(run)分布，其对应的密码函数也具有平坦的差分分布和高的非线性度[1]。从而，这种序列若作为密钥流，则具有很强的抗差分攻击的能力[1]。

**结束语** 笔者新设计了大量的二元序列，并给出了其中一类序列的自相关值以及它与其它类的序列在无转移情况下的互相关值。结果表明，这类序列在一定条件具有非常平坦的低相关值分布，并且这种分布是可控的。这类序列的实现方法和修改的 Jacobi 序列[2]非常类似。如果考虑这些序列在流密码中的应用，线性复杂度及游程分布等性质有待进一步研究。

## 参 考 文 献

1 Green D H, Green P R, Modified Jacobi sequences [J]. In: IEE Proc. Comput Dig Tech, July 2000, 147 (4): 241～251
2 Cusick T, Ding Cunsheng, Renvall A. Stream Ciphers and Number Theory [M]. North-Holland Mathematical Library 66. Elsevier Science Pub Co, April 1, 1998
3 Damgard I B. On the Randomness of Legendre and Jacobi Sequences [A]. In: Advances in Cryptograpy-CRYPTO' 88, LNCS403 [C]. Berlin: Springer-Verlag, 1990. 163～172
4 Brandstatter N, Winterhof A. Some Notes on the Two-prime Generator of Order 2 [J]. IEEE Trans Inf Theory, October 2005, 151(10): 3654～3657

(上接第 43 页)

6 Lee S C, Shields C. Tracing the Source of Network Attack: A Technical, Legal and Societal Problem[A]. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security [C], 2001. 239～246
7 Stone R. CenterTrack: An IP Overlay Network for Tracking DoS Floods[A]. In: Proceedings of USENIX Security Symposium[C], 2000
8 Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing (RFC 2827). The Internet Society, 2000
9 Global Incident Analysis Center. Special Notice - Egress filtering. http://www. sans. org/y2k/egress. htm.
10 Dean D, Franklin M, Stubblefield A. An Algebraic Approach to IP Traceback[A]. In: Proceedings of the Network and Distributed System Security Symposium(NDSS)[C], 2001, 2: 119～137
11 Song Xiaodong, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback[A]. In: Proceedings of IEEE INFOCOMM[C], 2001. 878～886
12 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
13 Cheswick B, Burch H, Branigan S. Mapping and Visualizing the Internet[A]. In: Proceedings of USENIX Annual Technical Conference[C], 2000
14 Floyd S, Paxson V. Difficulties in Simulating the Internet. IEEE/ACM Transactions on Networking, 2001, 9(4): 392～403
15 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
16 Hastings J R. Incremental Bayesian Segmentation for Intrusion Detection: [Maseter's Thesis]. Massachusetts Institue of Technology, 2003
17 Park K, Lee Heejo. On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack[A]. In: Proceedings of IEEE INFOCOM[C], 2001. 338～347
18 徐永红. Internet 拥塞控制/信息可用性技术研究: [学位论文]. 南京理工大学, 2002
19 Sanchez L A, Milliken W C, Snoeren A C, et al. Hardware Support for a Hash-based IP Traceback[A]. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEXII)[C], 2001. 146～152
20 Bellovin S. The ICMP Traceback Message. Internet Draft, IETF, March 2000