自治系统的攻击入口追溯技术研究

金 光 赵杰煜 赵一鸣 王肖虹

(宁波大学信息科学与工程学院 宁波 315211)

摘 要： 针对因特网上的 DDoS 攻击，提出一种新的以自治系统为单位的攻击入口追溯模型，通过在入口链路端进行地址标记，受害主机能以较低的运算复杂度还原出攻击入口。详细描述了算法的物理模型和数学依据，给出了还原虚报率和关联函数的理论公式。对自治系统结构与出入口链路的关系作了阐述，并讨论了该模型的部署应用。具体的示例和试验表明，该算法效果理想，具有理论和实用价值。

关键词： 分布式拒绝服务攻击，追溯，自治系统，入口地址标记，虚报率

中图分类号： TN393 **文献表示码：** A **文章编号：** 1009-5896(2005)03-0346-05

A Study on IP Traceback of DDoS Attack Ingress within an Autonomous System

Jin Guang Zhao Jie-yu Zhao Yi-ming Wang Xiao-hong

(*Faculty of Info. Science and Tech., Ningbo University, Ningbo* 315211,*China*)

Abstract To defend against DDoS attacks on Internet, a new scheme called Ingress Address Marking (IAM) within an Autonomous System (AS) is proposed, with which the IP addresses of the ingress can be embedded into the forwarding packets. A victim can traceback the addresses of the attack ingress in a low complexity by analyzing the marking information. Besides the physical model, the mathematical formulation of false positive ratio and correlation function are provided. The relationship of the ingress link and the structure of AS is reviewed. The construction and deployment of IAM are discussed. Simulation results have shown that this scheme has a good performance and is valuable on both theory and application.

Key words DDoS, IP traceback, Autonomous system, Ingress address marking, False positive ratio

1 引言

因特网上频繁发生的网络攻击，引起了广泛关注。其中分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是最具威胁的主要攻击类型之一。攻击者操纵大量傀儡机从多条途径汇聚大量数据包来消耗目标机 V 的资源，堵塞其链路，从而造成合法访问无法进行的“拒绝服务”局面。由于攻击便于实施和难以追踪，更得益于多种工具程序可用，近年来呈日益蔓延之势[1,2]。对此，网络安全机构和研究人员也作了很多努力，尤其针对攻击源追溯(IP Traceback)技术[3,4]，提出了多种设想和措施，试图找到匿名攻击的真实攻击源和路径，但效果并不理想。

针对 DDoS 攻击，本文提出一种新颖的攻击入口地址追溯模型，核心是基于自治系统(Autonomous System，AS)的入口地址标记(Ingress Address Marking，IAM)算法：由攻击入的路由器 R_{in} 在转发的 IP 数据包首部标记入口地址的编码信息；V 收到后可提取和分析这些标记，并还原出入口，进而通知因特网服务提供商(ISP)和 R_{in}，采取拦截、过滤等有效对策。

2 AS 中的攻击入口标记和还原模型

2.1 AS 的入口路由器

众所周知，因特网分成许多 AS 分别进行经营和管理，AS 具有相对独立性，有各自统一的行政归属，即 ISP 的管辖区[5]。显然，在安全防范上，AS 也是整个网络安全体系中相对独立的基本单位，我们的讨论也以 AS 作为主要对象。

见图 1，可把 AS 中承担路由选择的路由器分为 3 类：一类连接外部网络，称为边界路由器 R_b；二是接入内部局域网主机，称为接入路由器 R_i；三是系统内承担链路转接的，称为转接路由器 R_t。攻击入口也可分为 2 类，外来的是 R_b，内部的是 R_i，它们就是本 AS 中潜在的攻击转发者，本文统称为入口路由器 R_{in}。

2003-08-04 收到，2004-03-01 改回
浙江省科技厅重点项目(2003C21009)，宁波市软件产业发展基金(R200336)和宁波大学校内科研基金资助课题

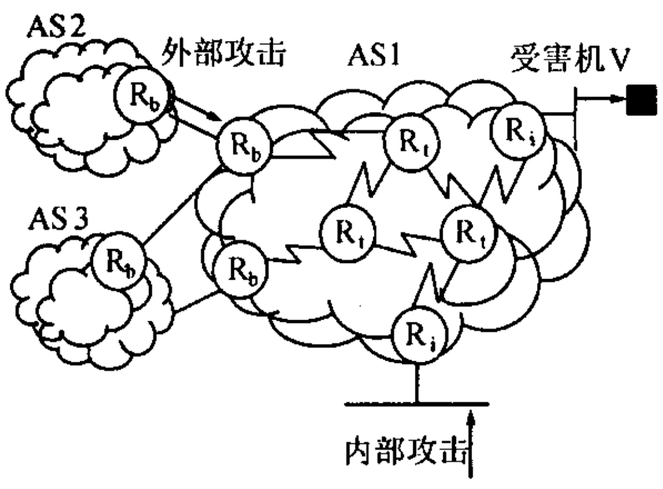


图 1　AS 中的路由器分类

2.2　入口地址的标记与还原

各 R_{in} 在转发自外向内的数据包时，用相应的入口链路 IP 地址对包作标记。但需要指出：参与标记作业的 R_{in} 要区别对待。如各边界的 R_b 必须全部参与标记；而内部接入的 R_i，可视具体情况而定。至于标记概率，为保证较高敏感性，可选 1/5~1/20 为好。

需标记的入口 IP 地址长度为 32bit。Savage 等[6]和 Dean 等[7]都建议占用 IP 包首部的 ID 域，见图 2。由于 ID 域实际很少使用，我们赞同并采纳这一建议。与 ID 域相邻的 Flags 域中尚有 1bit 空置，所以实际最多可用 16 或 17bit。尽管如此，仍放不下 32bit 地址。所以还需对地址进行分解处理，即按序分解成长为 l 的 n 片。

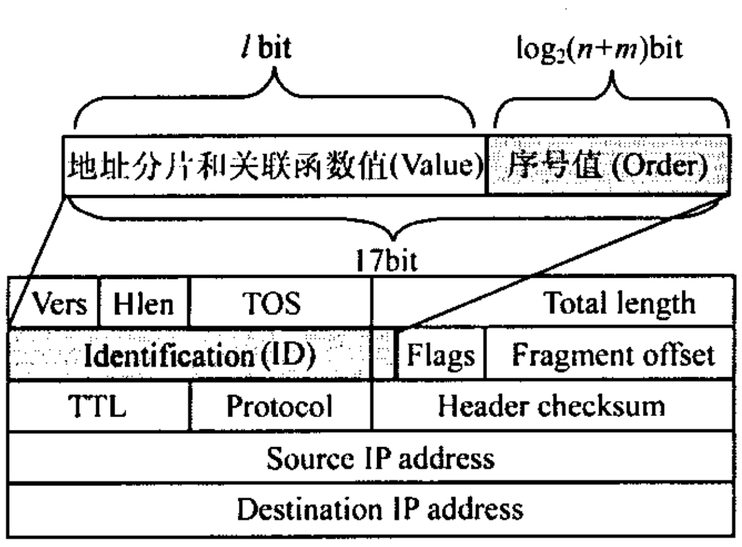


图 2　IAM 模型中的 IP 包首部标记域

V 收到含标记的数据包，可读出地址分片标记，然后进行拼接还原。所需的数学运算和验证，将在后面阐述。为了提高还原准确率，采用了两项重要的辅助措施：一是让属于同一地址的各分片首尾适量重叠(冗余分解)，以提高彼此关联度；二是引用多个关联函数 f_r，r=1,2,⋯,m，让它们对地址分片作运算，生成 m 个长度为 l 的函数值。这些函数值与 n 个地址分片一起，由 R_{in} 逐个选取其一存入数据包 ID 域。为了识别，还须对它们添加序号，所需位数为 $\log_2(n+m)$bit。所以实际需要位数总长应满足条件：$l+\log_2(n+m)=17$ 或 16。

还原时，先从足够的包中取得地址标记信息，分成$(n+m)$组：n 组地址分片 $B_1, B_2, \cdots, B_n$ 和 m 组关联函数值 $B_{n+1}, B_{n+2}, \cdots, B_{n+m}$。将 n 组地址分片合成 n 阶笛卡儿积：$B=B_1\times B_2\times \cdots \times B_n$，各 R_{in} 的真实 32bit 地址信息均应包含于 B 中。m 组函数值则应包含对各地址分别进行关联函数运算得出的函数值。还原实际上是一个比对运算：若能从 B 中找出一个元素，即有序 n 元组$<b_1,b_2,\cdots,b_n>$，既满足各分片首尾重叠的冗余分解条件，同时对该元组进行 m 个函数运算得出的值均包含于 m 组函数值之中，该有序 n 元组就应是真实的 R_{in} 地址之一。

3　IAM 算法的数学表述

3.1　地址的分解运算

将 R_{in} 的入口链路 IP 地址 a 分解为有序 n 元组 $a=<\alpha_1,\alpha_2,\cdots,\alpha_n>$，各元素 $a_i=<\alpha_{i1},\alpha_{i2},\cdots,\alpha_{il}>$, i=1,2,⋯,n (α_{ij}，j=1,2,⋯,l 是地址域中的二进制位)是 IP 地址的一个分片，则 $a_i\in W$，$W=\{x\mid x\in N\wedge 0\le x<2^l\}$，$N$ 是自然数集合。

设有 m 个函数 f_r，r=1,2,⋯,m，对 n 元组$<a_1,a_2,\cdots,a_n>$运算得出的函数值可表示为 $f_r(x)\in W$。f_r 是 W 上的 n 元运算，$<W, f_1, f_2, \cdots, f_m>$可组成一个代数结构。我们称 $f_1, f_2, \cdots, f_m$ 为关联函数。

实际标记时，取定 m 个函数 f_r，分别对 IP 地址 a 的 n 元组$<a_1,a_2,\cdots,a_n>$作运算，形成 m 个长度均为 l 的函数值 $f_r(x)$，r=1,2,⋯,m，然后让这 m 个函数值与 n 元组的元素一起参与标记。

3.2　地址的还原运算

对所有 n 元组，$f_r(x)$, r=1,2,⋯,m 函数值的取值范围，亦即所形成的子集空间记为$|W_r|$，但$|W_r|\le|W|$。若有 k 个入口站点，f_r 对各元组运算的函数值将可构成 m 个子集 $F_r^k=\{f_{r1}, f_{r2}, \cdots\}$, r=1,2,⋯,m，式中 k 仅是上标。F_r^k 的元素数 $|F_r^k|$ 换成相应的均值期望，可记为 $E(F_r^k)$。实际上，如果 $f_r(x)$函数值无重复，则 $E(F_r^k)=k$；但无论 k 多大，$E(F_r^k)\le|W_r|$。

还原计算中将不会遗漏任何真实入口地址，但也会“虚增”一些地址。可定义虚报率 $\eta=(k'-k)/k$，即“虚增”入口与真实入口数之比。其中 k' 为笛卡儿积 B 中所有 n 元组经 m 个函数运算，其结果分别属于 F_r^k, r=1,2,⋯,m 子集，而且又能满足冗余分解条件要求的 n 元组数量。各分片的重叠位数为 x_i, i=1,2,⋯,$n-1$，经相应的数学推导（证明略），最后可得：

$$\eta=\left(\prod_{r=1}^{m}\frac{E(F_r^k)}{|W_r|}\right)\cdot\left(\frac{k^{n-1}}{2^{\sum_{i=1}^{n-1}x_i}}-1\right) \tag{1}$$

可看出，虚报率 η 主要决定于参数 k, n, m。随着 k 和 n 减少，m 增大，η 趋近于 0。n=1 时 η=0，此时为全地址用作单一标记元素的一对一状况。k=1 时 η=0，即单一攻击源的情况，所形成的笛卡儿积 B 中仅含一个元素，简单列出即可。3 个参数中，k 主要取决于攻击方，上限为本 AS 入口总数。受到 ID 域空间的限制，n 和 m 的选择余地均不大。例如 $n\ge 2$，而 m 太大会增加计算工作量。冗余分解对降低 η

值有良好作用。但要指出，这是基于平均概率的公式，仅适合 $k>>1$ 的情况。例如仅 1 个入口站点时，公式就失去了成立的条件。

关于关联函数的选取，由于我们的推导是基于平均概率，应使函数值在其取值范围内尽可能均匀分布。事实证明关联函数对整个模型具有举足轻重的作用，经反复试验比较，建议采用均布性较好的 Hash 函数，式(2)和式(3)即为其代表：

$$f_1(a_1,a_2,\cdots,a_n)=a_1\oplus a_2\oplus\cdots\oplus a_n \tag{2}$$

$$f_2(a_1,a_2,\cdots,a_n)=(a_1\cdot a_2\cdot\cdots\cdot a_n)\bmod(2^t-1) \tag{3}$$

还需对还原计算时间复杂度作出估算。计算工作包括对笛卡儿积中的每个 n 元组计算各 $f_r(x)$值，并与 m 个函数值子集作比对，时间开销主要集中于比对过程。设基本运算单元取为一次比对，则当 $k>>n,m$ 时，复杂度为 $O(k^{n+1})$。

4 计算程序和试验结果分析

4.1 IAM 算法实例程序和仿真试验

图 3 列出了依据优化取值的一种算法实例程序，标记长度为 17bit，3 个分片长均为 14bit，关联函数为 5 个，累计冗余位为 10bit，标记概率为 0.2。

```
a0=0~13bit of IP
a1=9~22bit of IP
a2=18~31bit of IP
ai+2=fi(a0,a1,a2), i=1,2,…,5.
for each income-packet P
  let r be a random number from [0,1]
  if r<0.2 then
    if(j<7)&&(j>0) then j++
    else j=0;
    P.Value=aj;
    P.Order=j;
```

(a) 入口路由器地址标记

```
Let Bi be subsets, i=0,1;…,7;
for each received-packet P
  if P.ID is marked then
    i=P.Order;
    Bi←P.Value;/*by ascending order*/
for all Tuples a=(a0,a1,a2)∈B0×B1×B2
  if(9~13bit of a0==0~4bit of a1)&&
  (9~13)bit of a1==0~4bit of a2) then
  for (i=0;i<5;i++)
    zi=lookup fi(a0,a1,a2) in Bi+2;
    if all zi!=NIL then Recover a;
```

(b) 受害机还原入口地址

图 3 17bit IAM 模型算法程序实例

我们在较大规模的校园网络环境中进行了仿真试验，主要目的是测试地址分片、ID 域标记、地址解读和还原算法的可行性，仿真试验过程示例简要介绍如下：

对一台普通的服务器 V(PIV，1.5GHz)进行的攻击测试中，泛滥类攻击工具发出的攻击包从 100 个入口进入，每个入口的攻击包从 100-400 不等。在约 10min 的持续时间内，V 收到了大约 20000 个攻击包。当 V 配备的入侵检测系统(IDS)检测到攻击发生后，入口标记归纳进程开始：形成 8 个子集，将收到攻击包的 8 种标记信息按递增插入排序分别放入各对应子集。V 收集到足够的攻击包后，即可开始还原计算。在不到 0.5s 的时间内计算完毕，100 个攻击入口全部还原成功，虚报率 η 为 0。这里要求各子集按升序排列，是为了消除比对中的重复计算，从而优化还原过程。

4.2 试验结果分析

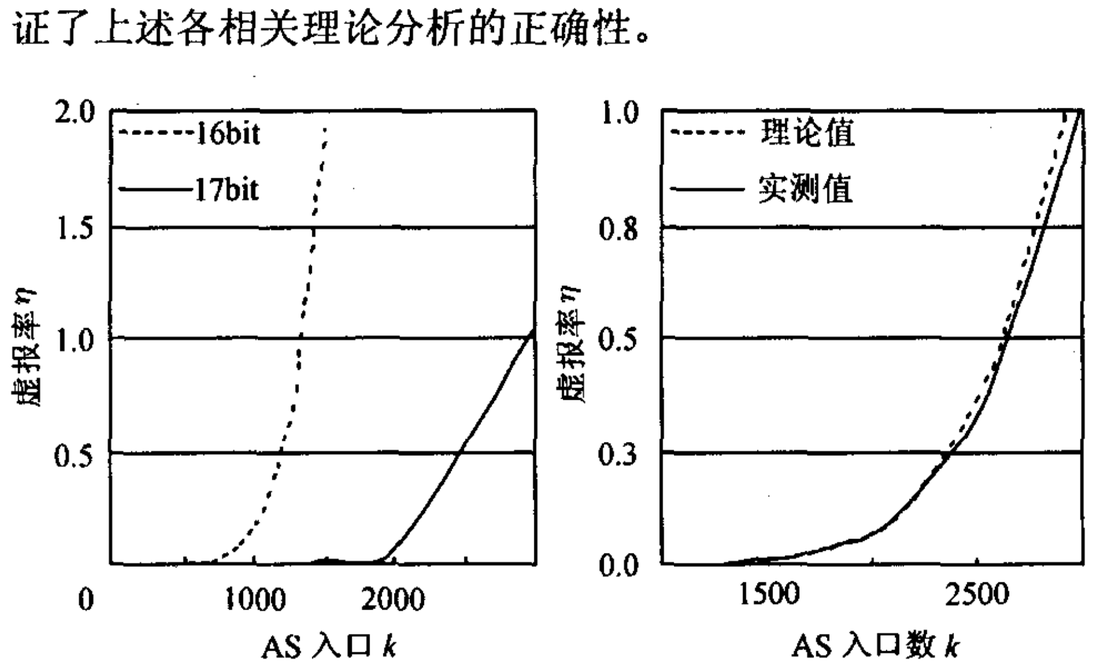
在图 3 所示的模型程序中，标记过程依照 0.2 的概率进行。还原过程中，V 平均收到来自同一入口路由器转发的 40 个攻击包，就可还原出该攻击入口地址。此外对还原时间的实际测试表明，500 个入口地址还原时间约为 3s，1000 个则需要约 33s。可看出该时间均处于实际操作可容许的合理范围。

有一个问题需要讨论，即启动还原计算的时间。简单考虑就是 IDS 一旦检测到攻击开始即开始还原，但显然过早开始还原会因标记信息收集不足而无法还原出有效地址；而如果不停地重复还原，则会持续消耗 V 的系统资源，也不可取；无休止的等待也不可能。为此，可引入单位延迟时间 Δt：从 IDS 检测到攻击开始到检测到的攻击包 S_p 累计数满足式(4)的时间间隔，即可启动还原计算：

$$S_p>\left(\mathrm{Max}(|B_{i+j}|)\cdot(n+m)\right)/r \tag{4}$$

$|B_{i+j}|$表示已归纳形成的子集 B_{i+j}，$i+j=1,2,\cdots,n,\ n+1,\cdots,n+m$ 的大小(无重复元素)，r 为标记概率(0.2)。如果攻击包继续增长，可在本次还原结束并作出相应处置后间隔一定时间后重新计算。如各子集大小不再增加，说明后续攻击仍从已还原的入口进入，则无须重新计算。

对于选用不同长度标记位，图 4(a)比较了 16bit 和 17bit 实例的追溯还原效果，前者同时面对 800 个攻击入口，约 0.05 的虚报率足以应付一般规模 AS 的防御要求。而后者更提升了性能，即使多达 1800 个入口，仍能保持 $\eta\approx 0$ 的效果。还可看出，即使面对多达 3000 个入口同时转发的 DDoS 攻击（能包含几万或更多攻击源），仍然具有良好的还原效果，这足够应对目前所能见到的最恶劣情况。图 4(b)则作了 17bit 实例理论估算和实测结果的比较，吻合得较为理想，从而验证了上述各相关理论分析的正确性。



(a) 16bit 与 17bit IAM 实例的虚报率比较

(b) 17bit IAM 实例虚报率理论和实测值比较

图 4

5　AS 结构与入口地址标记

5.1　AS 的功能和结构

要理解 R_{in} 的出入口链路的作用，需了解因特网 AS 的层次结构。为此，我们用图 5 的简化模型作说明。据统计，因特网上 AS 的总数到 2002 年 4 月约为 1.1 万个[8]。因特网的主干主要是北美的少数几个大网络，如 Sprintlink、AT&T、GBLX 等互联形成。表 1 给出了排名最前的几个 AS 的出入链路情况，可看出即使最大的 AS 其边界入口链路也较为有限，普通 AS 则更少。核心层的 ISP 控制着整个因特网的通信中枢。后来接入的网络，可视为它们的外围层次，业务上形成一种客户关系。当然它们也会向外发展，为更外层的客户提供转接服务。在这种多层次的结构中，每个 ISP 都有自己所经营管理的网络系统，技术上称为自治系统 AS。虽然 AS 大小与所处层次有不同，但基本上是一个 ISP 管辖一个 AS，少数大的 ISP 管辖多个 AS。不同 AS 之间还可建立一些更紧密的关系，作为示例，图 5 中列出了其中较常见的几种[9]：对等关系：同一层次的 AS 之间实现某种互惠互利关系；亲属关系：相邻 AS 共享客户、内部路由、外部连接等资源；以及备用关系等。

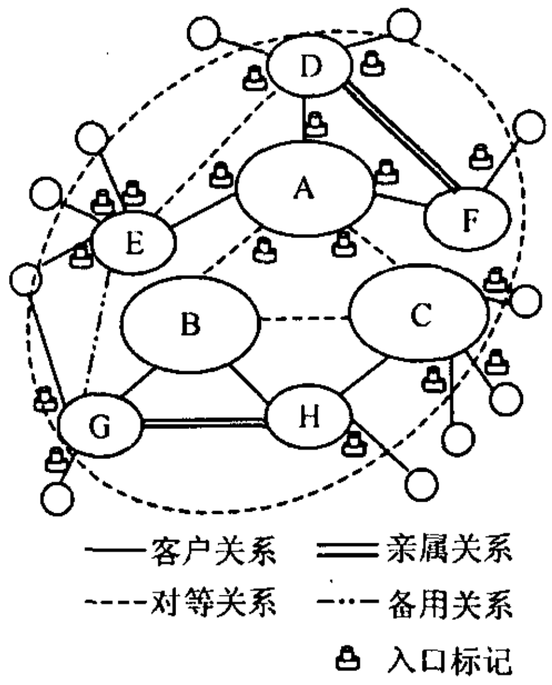


图 5　因特网 AS 结构和入口链路标记示意

表 1　Internet 规模最大的 AS 入度和出度

AS 编号	名称	入度	出度
701	ALTERNET	470	2749
6461	ABOVENET	468	908
1239	SPRINTLINK	279	1655
3549	GBLX	255	809
1	BBNPLANET	255	696

5.2　入口地址标记的实施

技术上，不同 AS 就是通过边界路由器的出入口链路相连接，依赖边界网关协议（BGP）实现外部路由选择。此外，AS 还可以与许多受其管辖的局域网及终端主机连接，即通过图 1 中的接入路由器 R_j。每个 AS 与外界的通路是有限的，这些出入口对 AS 辖区的管理至关重要，这也是本文重点关注 AS 的攻击入口的依据。图 5 的示例中，自治系统 A 可以在其入口链路处实施入口标记。如若能与周围 AS 实现联防，还可形成图中虚线所示更大范围的防御边界。实施 IAM 防御机制后，即使发生了大规模 DDoS 攻击，入口多达 1000 个或更多（攻击源可能多达上万个），也有能力将它们逐一还原出来。

采用灵活的部署策略不仅是降低虚报率的又一项重要措施，而且使管理更为高效和方便。尽管 AS 入度最多不到 500，但内部接入的入口可能较多，为有效扩大 IAM 算法模型的应用面，充分降低虚报率，我们可采用优化的入口标记部署策略。建议采用类似路由器中配置访问控制列表的策略：既考虑到充分接近攻击源，又要减少协调和管理工作量。图 6 分别表示了 3 种典型的不同内部接入入口的标记策略：(a)路由器外部接口远多于内部接口，则在内部接口处进行标记；(b)路由器外部接口远少于内部接口，则在外部接口处进行标记；(c)路由器外部接口和内部接口相等或较接近，则可自行选择，一般在外部接口处标记更为合适(更接近攻击源)。

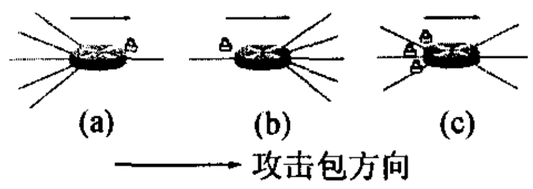


图 6　AS 内部入口 IAM 部署策略

6　讨论和结论

本文提出的 IAM 模型，核心也是数据包标记[10]，所以也具有该类方法的各项优点：如除要求路由器进行标记外，对网络系统及 ISP 别无要求；将网上追溯转化为受害机的网下分析计算，很大程度上减轻了网络系统和 ISP 的负担。此外还具明显的自身特点：如仅要求入口路由器参与作业，并不苛求追溯整条路径，工作量和难度明显减轻；计算简单，在线或事后分析均适用；不要求必须有大流量的数据包，因为标记与还原基本上一一对应，所以很适合于目前最难对付的多源点、小流量的 DDoS 类攻击。

本方法的局限性主要在于还原计算本身工作具有概率特性，正是这种概率特性导致还原可能会出现虚报。对此，可采取两项措施作进一步辨认：采用式(1)核算其虚报率 η，以此来估算和控制可能的虚报；由于仅限于 AS 范围，其入口地址悉数为 ISP 所掌握，可完全通过比对来排除虚报地址。

此外，虚报率会随入口路由器的数量上升，超过一定阈值而迅速增大，太大的 η 值会失去意义，故 IAM 模型对攻

击入口路由器有数量限制。但正如前面所分析，AS 中入口链路数最多不过几千个，而同时参与转发攻击包的入口路由器数量就更为有限，所以至少到目前为止，本文提供的结果已足够应付。

针对追溯 DDoS 攻击源这一难点，我们将攻击路径以 AS 为界分为两段，IAM 模型可直接获取 AS 内这一段路径的攻击源或入口。而对于 AS 之间，即从外部真实攻击源到攻击入口这一段攻击路径的追溯，这显然需要相关各方的充分协作。我们将继续深入研究，以获得一个较为理想的全网协同防御方案。

参 考 文 献

[1] Dittrich D. Distributed denial of service (DDoS) attack/toolspage. http://staff.washington.edu/dittrich/misc/ddos/.

[2] 金光, 朱锡雄. 因特网防御 DoS 攻击技术评述. 宁波大学学报(理工版), 2004, 17(4): 460 – 465.

[3] Belenky A, Ansari N. On IP traceback. *IEEE Communications Magazine*, 2003, 41(7): 142 – 153.

[4] Lipson H. Tracking and tracing cyber-attacks: technical challenges and global policy issues. http://www.cert.org/archieve/pdf/ 02sr009. pdf, 2002, December.

[5] Gao L. On inferring autonomous system relationships in the Internet. *IEEE Trans. on Networking*, 2001, 9(6): 733 – 745.

[6] Savage S, Wetherall D, Karlin A, *et al*.. Practical network upport for IP traceback. Proc. of ACM SIGCOMM'2000, Stockholm, Sweden, 2000: 295 – 306.

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

[8] CAIDA, AS Internet Grapgh, http://www.caida.com, 2002, April.

[9] Huston G. Interconnection, peering and settlements Part I; II. *Internet Protocol Journal*, 1999, 2(1): 2 – 17; 2(2): 2 – 24.

[10] Park K, Lee H. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attacks. Proc. of IEEE INFOCOM'2001, Anchorage, Alaska, 2001: 338 – 347.

金 光： 男，1972 年生，讲师，硕士，研究方向：计算机网络和信息安全.

赵杰煜： 男，1965 年生，教授，博士，研究方向：人工智能和信息安全.

赵一鸣： 男，1958 年生，副教授，硕士，研究方向：计算智能和信息安全.

王肖虹： 女，1972 年生，讲师，硕士，研究方向：Java 和因特网相关技术.