DOI：10.7652/xjtuxb201310003

面向拒绝服务攻击的多标签 IP 返回追踪新方法

陈秀真[1,2]，李生红[3]，凌屹东[2]，李建华[3]
（1. 西安交通大学制造系统工程国家重点实验室，710049，西安；2. 上海交通大学信息安全工程学院，200240，上海；3. 上海交通大学电子信息与电气工程学院，200240，上海）

摘要：针对网络安全中拒绝服务攻击难以防御的特点，提出面向拒绝服务攻击的多标签 IP 返回追踪方法(iTrace-DPPM)，用以识别基于互联网控制报文协议(ICMP)的直接和反射式拒绝服务攻击的真实源地址。该方法首先结合 ICMP 数据段大小及最大传输单元阈值，计算单一 ICMP 数据报文可携带的路由标记数，再根据数据包的幸存时间推断路由器与攻击源头的距离，将路由器的标记概率设定为距离的倒数，并针对每个标记域独立地执行概率标记算法，最后受害目标根据接收的标记信息，实现转发路径的重构及源头识别。与已有的动态概率包标记方法相比，iTrace-DPPM 方法具有路径重构所需数据包少、支持部分部署及无额外负载的优点。NS2 环境下的模拟实验结果证实，路径重构所需的攻击包数降为 DPPM 方法的路由标记数的倒数。

关键词：网络安全；IP 返回追踪；拒绝服务攻击；动态概率标记；多标签
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2013)10-0013-05

A New Approach of IP Traceback with Multiple Marking Tags for DoS Attacks

CHEN Xiuzhen[1,2], LI Shenghong[3], LING Yidong[2], LI Jianhua[3]
(1. State Key Laboratory for Manufacturing Systems Engineering, Xi'an Jiaotong University, Xi'an 710049, China; 2. School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240, China; 3. School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: A novel traceback method of dynamic probabilistic packet marking with multi-tag, called iTrace-DPPM, is proposed to solve the problem that DoS attacks are difficult to defend in the field of network security. True source addresses of direct and reflective DoS attacks based on internet control message protocol (ICMP) are identified with the proposed method. The method firstly calculates the number of routing tags stored in an ICMP packet with considering the size of data segment and the threshold value of maximum transmission unit. When a router is prepared to mark a packet, the distance from the generating node of the packet is deduced according to the time to live, the marking probability is set as the reciprocal of distance, and the probabilistic packet marking algorithm is further performed for one time at each tag field of one packet independently. Finally, the victim host reconstructs the complete forwarding paths from the received routing mark information and determines the true source host who launches DoS attacks. A comparison with existing dynamic probabilistic packet marking approach shows that the

收稿日期：2013-04-17。 作者简介：陈秀真(1977—)，女，博士，副教授；李生红(通信作者)，男，教授。 基金项目：国家科技支撑计划资助项目(2012BAH38B04)；国家自然科学基金资助项目(61271316)；机械制造系统工程国家重点实验室开放基金资助项目(sklms 2012005)。
网络出版时间：2013-07-19 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20130719.0910.003.html

proposed iTrace-DPPM has the following three advantages: less attacking packets needed in reconstructing attack paths, support of partial deployment, and no extra network load. A series of simulations under NS2 show that the number of attacking packets needed by the iTrace-DPPM is reduced to the reciprocal of the number of routing tags of the traditional DPPM.

Keywords: network security; IP traceback; denial of service attacks; dynamic probabilistic marking; multiple tags

黑客利用网络协议缺陷发起的拒绝服务(Denial of Service,DoS)攻击是最常见的一种网络攻击,旨在使目标系统无法提供正常的服务或资源访问。DoS攻击每年造成高达上千万美元的商业损失,是造成互联网财产损失第二多的网络攻击类型,而且攻击者可利用网络上已被攻陷的大量主机组建僵尸网络(Botnet),控制其向某一特定目标发动密集式的拒绝服务攻击,即分布式拒绝服务攻击(Distributed DoS,DDoS)[1]。DoS攻击由于其实现简单、追踪困难、后果严重等特点,严重威胁着Internet及其基础设施的安全。

在抵制DoS网络攻击的各种方法中,IP返回追踪(IP Traceback)技术是一种非常有威慑力的防御方法[2]。但是,由于IP协议设计之初,没有考虑验证网络数据包源IP地址的真实性,致使攻击者常常采取伪造自身IP地址的方法来隐藏自身、逃避罪责,这给及时定位、应对DoS攻击及攻击发生后的司法取证都带来一定的困难。为了有效识别DoS攻击的源头,国内外学者提出包记录、包标记及结合以上两者的混合追踪算法[3-4]。其中,由于包标记方法不会带来额外的网络负载,具有一定的抗伪造能力和可扩展性,已成为返回追踪的主流方法[5]。典型的包标记算法有:静态概率标记(PPM)[6-7]、动态概率标记(DPPM)[8]和基于互联网控制报文协议(ICMP)的标记(iTrace)[9-10]。其中,PPM方法中路由器以固定概率将IP地址写入数据包头部中不用或保留的字段,受害者端根据接收到的标记信息重构流转发路径。该方法存在的问题是标记空间受限,可能出现标记信息完全损失而无法重构攻击路径的情况,如何选择标记概率是一个难点。DPPM有效实现了标记概率随路由跳数的动态变化,达到了路由器最终标记概率的均匀分布,但是仍然受标记空间的限制。iTrace的基本思想是路由器以一定的概率取样被转发分组,并把分组及邻接路由器的信息复制到一个特定的ICMP分组中,然后发送该ICMP分组到相同的目的地址,受害者分析相关ICMP包即可重构路径。该方法可用于追踪各种协议类型的数据包,但这是一种带外消息传递(out-of-band signaling)的方法,给网络传输造成额外负担。

为了确保互联网的安全可靠运行,需要寻求一种快速定位攻击源的有效方法,达到及时切断攻击源头、阻止恶意攻击进一步扩散的目的。本文研究了面向取证的IP追踪技术,针对基于ICMP协议的DoS攻击手段ICMP洪水和Smurf攻击,利用ICMP协议数据段的可扩展特性,设计了一种多标签、动态概率追踪方法(iTrace-DPPM),通过逐步确定攻击数据流的转发路径,进而确定攻击的源头。本文方法可有效支持反射式拒绝服务攻击的追踪,大大降低数据包转发路径重构所需的攻击包数量。

1 基于ICMP协议数据段的多标签追踪方法

大多数ICMP洪水攻击都是基于ICMP回显(echo)请求/回复消息,而且把ICMP的数据域填充到最大长度,以产生大尺寸的数据包耗尽受害目标的带宽资源。在ICMP协议行为实验中发现,其请求和回复数据包的数据域保持不变。当主机收到一个ICMP请求数据包时,其回复数据包的数据域仍然采用请求包中的数据内容。因此,请求或回复数据包中数据域的任意修改,都能传递到目的主机。基于这一发现,本文提出基于ICMP数据段的动态标记追踪方法iTrace-DPPM,即利用ICMP数据域来携带跟踪信息,包括转发路由器的地址、与攻击发起主机的距离等,为追踪直接式和反射式DoS攻击到源头提供足够信息。

下面详细给出iTrace-DPPM方法的具体设计内容。

1.1 数据结构设计

iTrace-DPPM方法中路由器利用可扩展的ICMP数据域,将完整的32位IP地址标记在一个数据包中,而且一个数据包携带多条标签,即存储多个路由器的标记地址,将{路由器IP地址,请求标志,幸存时间}作为标记元组,设计以下字段。

标记数(N)：数据包中已写入的路由器标记个数，路由器写入一次标记信息，N 的取值加 1。同时，该字段用于计算标记信息的存放地址。

路由器 IP 地址(R)：转发路径上路由节点的 32 位地址。

请求标志(F_{echo})：区分 ICMP echo 请求和回复数据包，设置此标志位的目的是用于构造反射式攻击的路径。F_{echo}取值为 1，表示数据包为 echo 请求，反之为 echo 回复数据包。

幸存时间(T_{TTL})：数据包的存活时间标识(TTL)，用于确定路由器在数据流转发路径上的位置。

标记元组数(m)：单个 ICMP 包的数据域所能存储的标记元组数，即一个数据包携带的标签条数。m 的取值与协议的最大传输单元(MTU)相关，由于 MTU 很大，理论上 m 的取值也很大。然而，在实际的网络环境中，出于安全原因、防止 ping 之死攻击等，防火墙会对 ICMP 包的大小有所限制。为此，本文方法中的 m 可参照常用操作系统 Windows 和 Linux 下 ICMP ping 包数据段的默认值来计算。

综上，本文提出的基于 ICMP 数据域的标记方法 iTrace-DPPM 的数据结构如图 1 所示。

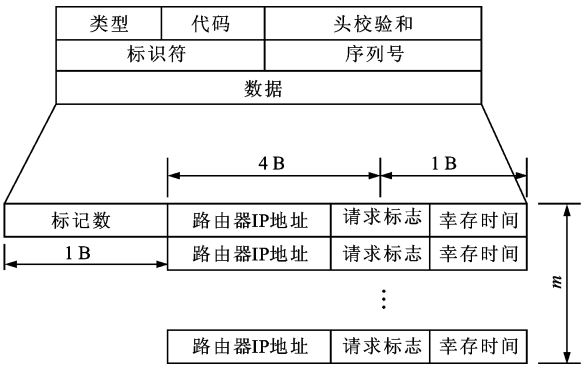

图 1　iTrace-DPPM 方法的数据结构

1.2　自适应标记概率

本文引入基于 TTL 的概率自适应调整方案，实现动态的概率包标记，保证所有路由器的标记信息以等同概率到达目标主机。具体步骤如下。

(1)数据包头部 TTL 初始值推断。数据包的源节点设置 TTL 的默认初始值，这与操作系统、通讯协议相关，操作系统在不同的协议上采用不同的 TTL 初始值，且常见的 TTL 初始值落在幸存时间集合 $S=\{32, 64, 128, 255\}$中。考虑到互联网中大多数据包经过的路由器数目不多于 25 个，初始 TTL 值 t_0 拟取集合 S 中大于或等于当前 TTL 值的最小元素。由数据包头部的当前 TTL 值 T_{TTL}推断初始值 t_0 的公式如下

$$t_0 = \min\{x \mid x \geqslant T_{\text{TTL}}, x \in S\} \tag{1}$$

(2)标记路由器与攻击流源头的距离推断。当数据包在网络中传播时，所经过的每个路由器将其 TTL 值减 1，故取 TTL 的初始值与当前值的差作为数据包与攻击发起点的距离 d，即

$$d = t_0 - T_{\text{TTL}} \tag{2}$$

(3)动态标记概率计算。为了实现攻击路径上所有路由器具有等同的最终标记概率，即受害端有等同概率获得路径上每一个路由器的信息，数据包越远离攻击发起方，其标记概率应该越小。本文依据标记路由器与攻击源头的距离 d，动态调整标记概率。对于数据流路径上与攻击源头的距离为 d_i 的第 i 个路由器，其在每条标签域的标记概率为

$$p_i = 1/d_i \tag{3}$$

1.3　iTrace-DPPM 方法中的概率标记算法

每个路由器标记转发的数据包时，独立进行 m 次概率标记算法。路径上第 i 个路由器转发一个 ICMP echo 数据包 P 时，采用的标记算法如下：

(1)路由器 i 将标记数 N 清 0；

(2)产生 m 个随机数 r_j($j=1, 2, \cdots, m$)；

(3)For $j=1$ *to* m

　　If 随机数 $r_j <$ 标记概率 p_i，then

　　根据 echo 的类型，设置请求标志位 F_{echo}；

　　拷贝路由器 IP 地址、T_{TTL}、F_{echo}于(1 $+N\times5$)字节之后；

　　标记数目 N 加 1；

　　Else

　　不标记数据报 P；

　　End

(4)End

上述标记算法可保证每个路由器标记经过的数据包时，可将自己的 IP 地址以 p_i 的概率分别写入 m 条标记空间中。最坏情况下，iTrace-DPPM 方法对经过路由器 R_i 的一个数据包标记 0 条 R_i 的 IP 地址；最好情况下，iTrace-DPPM 方法对经过路由器 R_i 的一个数据包标记 m 条 R_i 的 IP 地址。同时，路由器 R_i 的 m 个标记概率相互独立，互不影响。

1.4　概率标记算法性能分析

(1)路由器标记数据包的概率。在 iTrace-DPPM方法中，一个数据包中有 m 条标签域，每条标签域的标记概率为 p_i，每个路由器有 m 次机会将

自己的信息写入数据包中。因此，路由器 r_i 能将自己的信息写入数据包的概率为

$$p'_i = m/d_i \tag{4}$$

(2)最终标记概率。最终标记概率是指路由器能将自己的标记信息留在数据包中，并携带到受害者处的概率。根据 iTrace-DPPM 方法的工作原理，每个路由器以相互独立、互不影响的 m 个标记概率向一个数据包中写入标记信息，且标记概率取路由器与攻击源头的距离 d 的倒数。对于数据包中的一个标签位置，从受害者角度来看，接收到每条标签域信息的概率与 DPPM 方法一致。所以，iTrace-DPPM 方法的最终标记概率是 DPPM 方法的 m 倍，其最终标记概率为

$$\alpha_i = m/D \tag{5}$$

式中：D 为数据流转发路径上路由器的个数。由式(5)可以看出，iTrace-DPPM 方法达到了路由器的最终标记概率均匀分布。

(3)重构所需最小攻击包数。iTrace-DPPM 方法的实质是针对一个数据包中的每条标签域，让每个路由器都做一次标记选择。数据包有 m 条标签域，则路由器共需做 m 次标记选择。理论上来讲，包含 m 条标记域的数据包 m_tag_packet 携带路由信息的能力将是包含 1 条标记域 1_tag_packet 的 m 倍，其在受害者处完成 IP 追踪过程的能力也是 1_tag_packet 的 m 倍。对于 iTrace-DPPM 方法，最好情况下 D 个路由器的信息不重复的被记录下来。由于一个数据包中标记空间为 m，即可存储 m 条路由器 IP 地址信息，因此最小重构攻击包数为

$$\min(N_{\text{iTrace-DPPM}}) = \lceil D/m \rceil \approx D/m \tag{6}$$

(4)重构所需的平均包数。文献[10]已经证明求解 DPPM 方法所需的平均包数问题等同于礼券收集问题，其所需的平均包数近似为 $D\ln D$。从受害者重构路径的角度来看，iTrace-DPPM 方法中一个数据包携带的路由信息相当于 DPPM 方法数据包携带信息的 m 倍，因此其重构所需的平均包数为

$$E(N_{\text{iTrace-DPPM}}) = \left\lceil \frac{1}{m} D\ln D \right\rceil \approx \frac{1}{m} D\ln D \tag{7}$$

2 iTrace-DPPM 方法测试与分析

由于 NS2 是一个用于网络模拟的软件平台，支持流行的大多数网络协议和路由算法，可模拟多种局域网和广域网，因此本文选择在 NS2 模拟环境下实现基于 ICMP 协议的 DoS 攻击与源头追踪，以测试 iTrace-DPPM 方法的性能与效果。本文建立的用于 DoS 攻击模拟的网络拓扑结构如图 2 所示。

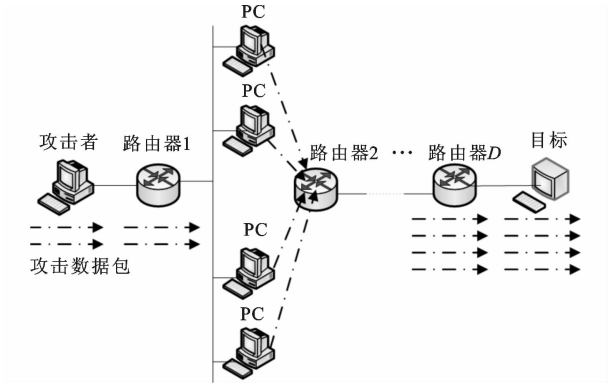

图 2 DoS 攻击模拟与追踪拓扑结构

由于 Windows 和 Linux 下 ICMP ping 包的数据段默认长度分别为 32 B 和 56 B，为了不影响使用 ICMP echo 请求或应答包的 ping 测试应用，本文设定包标记算法使用的数据段长度有 16 B、26 B、36 B，即数据包可携带的路由标记数分别为 3、5、7。参照文献资料的统计结果[11]，设定网络数据包经过的平均路由器个数为 15，由于经过路由个数超过 25 的情况很少出现，因此本文设定场景中的路由个数分别从 1 到 25。针对不同的路由器数及不同的数据段长度，均做 1 000 次实验并取其平均值，作为路径重构所需的数据包数。图 3 给出了 iTrace-DPPM 和 DPPM 这 2 种标记方法的测试结果。

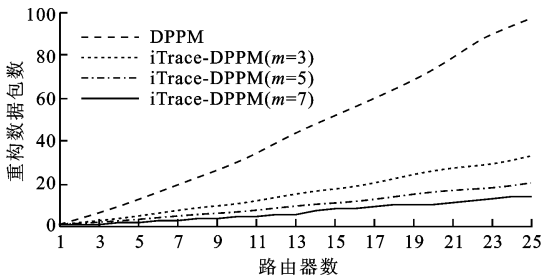

图 3 2 种标记方法的测试结果

实验结果表明：①iTrace-DPPM 方法重构 D 个路由器所需的数据包数与理论推导一致，当路由器总数为 15、标记域总数为 5 时，1 000 次实验结果的路径重构所需数据包平均值为 10，根据式(7)可得理论结果为 $(15\times\ln 15)/5=9.96$；②在不考虑链路带宽限制的约束条件下，iTrace-DPPM 的重构包数基本上降低到 DPPM 重构包数的 $1/m$。比如 $m=7$、$D=20$ 的情形，实验测得 iTrace-DPPM 方法路径重构所需的数据包平均数为 10，DPPM 方法所需的数据包数为 72，DPPM 所需的重构包数为 iTrace-DPPM 方法的 7.2 倍；③iTrace-DPPM 方法重构数

据转发路径需要的数据包数大大减少，而且随着标签域 m 的增加，所需的数据包数随之减少。攻击路径重构所需的数据包数的减少，主要是由于本文方法采用了以下 3 个核心措施：①基于 ICMP 数据域的多标签机制；②标记概率的动态调整方法；③路由器针对一个数据包中的 m 条标签域独立做 m 次标记选择，保证了最终标记概率的均匀分布。

另外，本文 iTrace-DPPM 方法是采用概率标记原理，仍然具有包标记追踪机制的特点：①即使网络系统中只有部分路由器具有源追踪功能，受害目标仍然可以根据接收到的标记信息重构转发路径，这很好地克服了不能同时在所有路由器上部署追踪系统的问题；②可扩展到整个 Internet，能够实现单个自治系统、多个自治系统与运营商之间的 IP 追踪；③使用数据包已有的域存储标记信息，没有带来额外的网络负载，很好地满足了追踪系统不能加剧带宽饱和的原则；④一定程度上可以避免欺骗标记对重构过程的干扰，数据包携带的虚假标记有可能被随后合法路由器的标记信息覆盖。

3　结　论

本文提出的多标签动态概率标记追踪方法 iTrace-DPPM 结合了 ICMP 协议特性及动态概率标记算法的优势，有效实现了一个数据包携带多条路由标记信息，而且路由器的标记概率随路由特性而动态改变。本文方法针对 ICMP 数据包的 m 个标签域独立做 m 次标记选择，达到路由器的最终标记概率均匀分布，可追踪基于 ICMP 协议的直接式和反射式 DoS 攻击源头，大大降低了路径重构所需的数据包数量。我们下一步工作将集中在：①标记算法自身安全性能的提高，在标记数据段中加入一些安全控制措施，如 hash 值验证、校验码验证等，防止攻击者破坏路由器的 IP 标记机制；②增强对 iTrace-DPPM 标记算法性能的测试，在传输路径上增加正常用户业务数据流，设置不同的网络传输速率及网络带宽限制，分析各种场景下的算法性能。

参考文献：

[1] ALOMARI E, MANICKAM S, GUPTA B B, et al. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art [J]. International Journal of Computer Applications, 2012, 49 (7): 24-32.

[2] PENG Tao, LECKIE C, RAMAMOHANARAO K. Survey of network-based defense mechanisms countering the DoS and DDoS problem [J]. ACM Computing Surveys, 2007, 39(1): 1-42.

[3] VINCENT S, RAJA J I J. A survey of IP traceback mechanisms to overcome denial-of-service attacks [C] // Proceedings of the 12th International Conference on Networking, VLSI and Signal Processing. Stevens Point, WI, USA: World Scientific and Engineering Academy and Society, 2010: 93-98.

[4] MALLIGA S, TAMILARASI A. A hybrid scheme using packet marking and logging for IP traceback [J]. International Journal of Internet Protocol Technology, 2010, 5(1): 81-91.

[5] BELENKY A, ANSARI N. On IP traceback [J]. IEEE Communication Magazine, 2003, 41(7): 142-153.

[6] SANTHANAM L, KUMAR A, AGRAWAL D P. Taxonomy of IP traceback [J]. Journal of Information Assurance and Security, 2006, 1(2): 79-94.

[7] 蒋华，李明珍，王鑫. 一种基于概率包标记的 PPM 算法改进方案 [J]. 山东大学学报：理学版，2011，46(9)：85-88.
JIANG Hua, LI Mingzhen, WANG Xin. A PPM probabilistic packet marking improving scheme [J]. Journal of Shandong University: Natural Science, 2011, 46(9): 85-88.

[8] LIU J, LEE Z J, CHUNG Y C. Dynamic probabilistic packet marking for efficient IP traceback [J]. Computer Networks, 2007, 51(3): 866-882.

[9] BELLOVIN S M. ICMP traceback messages [EB/OL]. (2003-02-05) [2013-03-10]. http://tools.ietf.org/html/draft-ietf-itrace-04.

[10] GUERID H, SERHROUCHNI A, ACHEMLAL M, et al. A novel traceback approach for direct and reflected ICMP attacks [C] // Proceedings of 2011 Conference on Network and Information Systems Security (SAR-SSI). Piscataway, NJ, USA: IEEE, 2011: 1-5.

[11] ETHAN K B. Practical reverse traceroute [EB/OL]. (2009-01-09) [2013-01-10]. http://www.nanog.org/meetings/nanog45/presentations/Tuesday/Katz_reversetraceroute_N45.pdf.

（编辑　刘杨　赵大良）