IP 追踪中的自适应包标记

李德全[1],徐一丁[2],苏璞睿[1],冯登国[1]
(1. 中科院软件所,信息安全国家重点实验室,北京 100080;2. 中国 UNIX 用户协会,北京市学院路 31 号,北京 100083)

摘 要: 拒绝服务(DoS)攻击是目前最难处理的网络难题之一. 最近,研究人员针对 DoS 攻击提出了多种方案,这些方案都各有优缺点. 其中,由 Savage 等人提出的概率包标记方案受到了广泛的重视,也有不少的变种出现. 在这一类的标记方案中,路由器以固定的概率选择是否标记一个数据包,这导致受害需要较多的数据包进行攻击路径的重构. 本文提出一种自适应的标记策略,经实验验证受害者用较少的数据包即可重构攻击路径,这不仅为受害者及早地响应攻击争取了更多的时间,还限制了攻击者的伪造能力.

关键词: 追踪; DoS; DDoS; 拒绝服务
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2004) 08-1334-04

Adaptive Packet Marking for IP Traceback

LI De-quan[1], XU Yi-ding[2], SU Pu-rui[1], FENG Deng-guo[1]
(1. *State Key Laboratory of Information Security, Institute of Software, CAS, P. O. box 8718, Bejing 100080, China;*
2. *UNIX User's Association of China, No. 31 Xueyuanlu, Bejing 100083, China*)

Abstract: Denial of service attack is among the hardest network problems. Several countermeasures are proposed for it in the literature, among which, Probabilistic Packet Marking (PPM) first developed by Savage et al is promising and has many variants. In these marking schemes, router marks packets with a probability which is fixed and uniform. Using fixed probability causes that many packets are needed for a victim to reconstruct the attack path(s). In this paper, an adaptive marking scheme is given, which reduces the number of packets needed for attack path reconstruction, thus also saves time for the victim and reduces the ability for attackers to spoof.

Key words: traceback; DoS; DDoS; denial of service

1 引言

最近,拒绝服务攻击事件持续上升,每年递增达 50 %以上[1]. 为什么会有这么多的 DoS 攻击呢? 研究表明,一方面 DoS 攻击极易实施,网络上也有很多现存的攻击工具,攻击者只需下载这些工具,就可以随意地对受害者发动攻击;另一方面,与特权提升攻击不同,DoS 攻击一般不需要攻击者与受害者进行交互,这样,攻击者就可以伪造攻击性数据包中的源 IP 地址,而对于有些 DoS 攻击(如 SYN 风暴等),伪造 IP 地址会使攻击更有效,这就使得受害者不知攻击来自于何方,从而既难采取有效的措施防范攻击或缓解攻击所造成的影响,又难以找到攻击者,追究其责任. 此外,分布式拒绝服务(DDoS)攻击使得多个拥有较少资源(如带宽、运算能力等)的攻击者通过协同工作可以有效地攻击资源较丰富的受害者. 病毒、蠕虫也加剧了 DoS 攻击中业已不平衡的攻击者和受害者的关系,使受害者益发处于不利地位.

在受害者看来,DoS 攻击特别是风暴型 DoS 攻击的数据包与普通的数据包是难以区分的,因此,DoS 攻击的防范是非常困难的. 然而,人们发现,攻击者也常会担心被发现从而受到惩罚. 因此,如果我们能够有效地追踪到攻击者,则拒绝服务攻击就会因此而大为减少. 在 DoS 攻击中,攻击者也常利用其控制下的傀儡机实施攻击,这样,如果傀儡机被发现,攻击者仍希望保持其匿名性. 虽然如此,找出用于攻击的傀儡机也是有意义的,受害者可以对傀儡机发来的数据流采取过滤、限流等措施从而减少受害的程度,受害者也可以通知傀儡机的管理员,从而堵塞傀儡机的漏洞、加强傀儡机的安全(这对攻击者而言也是个损失,因其可能因此而失去对傀儡机的控制,从而失去利用傀儡机资源的能力),甚至从傀儡机进一步追踪到真正的攻击者. 最早由 Savage[2] 等人进行了深入研究的概率包标记方案就是为了追踪攻击者或傀儡机而提出的. 本文主要研究概率包标记的概率选择策略,以期减少在攻击路径重构过程中所需的数据包数,从而使受害者能及早地追踪到攻击者(傀儡机)并及时对 DoS 攻击予以响应.

2 概率包标记

概率包标记[2~4]的主要思想是让路由器以一定的概率向过往的数据包中填塞部分的路径信息. 当收到足够的来自于攻击者或傀儡机的数据包以后,受害者就能从这些数据包中提取出相应的路径信息,然后重构出攻击数据包经过的完整的路径. 这在风暴型 DoS 攻击的情况下是很容易满足的,因为

收稿日期:2003-04-01;修回日期:2004-01-15
基金项目:国家杰出青年基金(No. 60025205);国家重点基础研究发展规划 973 项目(No. G1999035802)

这种攻击的力度靠的就是包的数量.本文中我们称文献[2]中最好的那个算法为基本包标记,因为此后不少的作者都在这一算法的基础上作工作.

由于数据包在途中经分段(fragment)处理的情况是很少出现的(不超过 0.25 %[5]),因此 *IP* 头中的识别号域(Identification field)也很少使用.于是,Savage 等人建议将路径信息嵌入到 16 bit 的识别号域中.在文献[2]中,路由器的 IP 地址及另外的 32bit 校验码共 64bit 被分成 8 块,每块 8bit,以 0 到 7 对其编号(称为偏移).为了顺利进行路径的重构,还需要一个距离域表示路由器到受害者之间的距离,由于路径极少有超过 25 跳(hop)的,因此 5bit 的空间就够.当一个路由器标记一个数据包时,其随机地从其 8 个分块中选取一块(8bit),连同对应的偏移(3bit),以及距离(5bit,在标记时置 0)填入该数据包的标记域(即识别号域)中.当一个路由器选择不标记一个数据包时,它先检查距离域的值是否为 0,如是,则其把自己的与标记域中偏移量对应的分块与包中已有的分块异或再填入原有位置,然后把距离增 1;如果距离不是 0,则它只需把距离增 1.这样一来,数据包中的标记信息实际上是两个相邻路由器之间的边(或连接)的信息.在这个方案中,至少需要 8 个数据包才能传送一个路由器(或边)的完整信息.

文献[3]中的高级包标记和带认证的包标记与此类似,主要的不同在于其 8 个分块不再是 IP 地址和校验码,而是 IP 地址的 8 个不同的 hash 值(共有 8 个不同的 hash 函数).另外,这两种方法在重构攻击路径时,还需要网络的拓扑信息.有兴趣的读者请参考文献[3].

在现有的标记方案如基本包标记、高级包标记以及带认证的包标记中,所有的路由器在决定是否标记一个数据包所采用的概率 p 是固定的、统一的,一般选 0.04.当一个路由器标记一个数据包以后,该数据包可能被后续的路由器重新标记,使原有的标记信息被覆盖.设路由器 R 离受害者的距离为 k,一个数据包在 R 处被标记以后不再被后续路由器标记的概率为 $(1-p)^{k-1}$.因此,对于到达受害者的数据包而言,它被 R 标记而不被随后的其它路由器标记的概率为 $p(1-p)^{k-1}$.距离 k 越大,这个概率越小.对于离攻击者最近的边或节点,由于数据包在到达受害者时,其中的标记信息包含该边或节点信息的概率最小(文献[4]称该边为"最弱的连接"),这使得受害者必须收到较多的数据包才能获得该边或节点的信息,从而总体而言,受害者需较多的数据包重构攻击路径,类似的讨论见文献[4].此外,如果攻击者到受害者的距离为 d,则来自于攻击者的数据包不被途中的任何一个路由器标记的概率为 $(1-p)^{d-1}$,这就为攻击者伪造路由信息提供了很大的可能.对基本包标记、高级包标记、带认证的包标记的详细分析以及对基本包标记的一些改进请参考文献[6].

3　自适应包标记

这里,我们将给出一个自适应的标记策略以期减少路径重构时所需包的数量并使所有的包在其途中都得以标记.这是很有意义的:(1)所需数据包越少,受害者就能越快地得到攻击路径,从而可尽早地实施响应如过滤、限流等,减少攻击带来的危害;(2)减少攻击者伪造的余地;(3)如果攻击者想要逃避追踪,其必须从每个攻击点发送更少的包,这就降低了攻击的力度;或者,如果攻击者既要逃避追踪,又要维持攻击的力度,则其需要更多的攻击发出点(傀儡机),从而增加攻击者的难度.

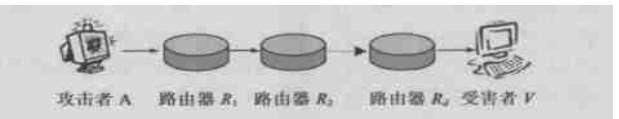


图 1　攻击路径

假设从攻击者到受害者的距离为 $d+1$,即从攻击者处出发,数据包需经过 d 个路由器后到达受害者.设中间的路由器按顺序为 R_1、R_2、…、R_d,其中 R_1 离攻击者最近,R_d 离受害者最近,如图 1 所示.如果从攻击者到受害者的所有数据包都被中间的某个路由器标记,则攻击者就没什么余地可以伪造的了(当然,攻击者仍可以伪造 IP 地址、IP 包的其他内容等等,这里指的是攻击者不能增加追踪的难度或通过插入其他信息干扰追踪.)如果每个数据包最终被哪个路由器标记(即被该路由器标记后没有再被后续的路由器重新标记)的概率都是相等的,即都为 $1/d$,则由 coupon collector 问题[7]知所需包数为最少.由于路由器 R_d 离受害者最近,当其标记一个数据包以后,不会再有其他的路由器标记之.因此,R_d 应以概率 $1/d$ 标记来自于该攻击者的数据包.记 R_i 标记数据包的概率为 p_i,$i=1$、2、…、d.对于 R_{d-1},当一个数据包被其标记以后,该数据包又经 R_d 再一次标记的概率为 p_d,因此,一个数据包最后一次被标记这一事件发生在 R_{d-1} 处的概率为 $p_{d-1}(1-p_d)$.同理,我们有:

$$1/d = p_d$$
$$1/d = p_{d-1}(1-p_d)$$
$$1/d = p_{d-2}(1-p_{d-1})(1-p_d)$$
$$\cdots$$

因此,得到

$$p_d = 1/d$$
$$p_{d-1} = 1/(d-1)$$
$$\cdots$$
$$p_2 = 1/2$$
$$p_1 = 1$$

即,每个路由器标记一个数据包的概率刚好是该数据包由攻击者开始到达此路由器为止已经经过的路径长度的倒数.这样,重构攻击路径所需的数据包数达到最少,平均为 $d(1+1/2+\cdots+1/d)$[7].然而,通常情况下路由器并不知道一个数据包经过了多长的路径以后才到达该路由器的(虽然在包头中有个 TTL 域或许可用作此用途,但不同的应用程序或不同的系统会设置不同的 TTL 初始值,另外,TTL 是由终端系统设置的,而终端系统通常是不可靠的,因此一般而言 TTL 也是不可信的).Peng[8]等人提出在 IP 的选项域增加一个额外的域用来存放数据包经过的路由器数.为了对付伪造,他们还提出采用与带认证的包标记[3]中类似的,在一段时间延迟后才公布的密钥进行加密.然而,我们发现,这个方法其实是不可行的,原因是:(a)首先,在数据包的传送过程中往选项域写数据是

很费时的操作[2]. (b) 由于这个距离域需要被途中的每一个路由器读取、修改("加 1"操作),因此这种认证只能发生在相邻的两个路由器之间,这也使得每个路由器都要对每个数据包做一次加密和解密操作,而加解密是计算量很大的工作. (c) 最后一点,也是最为重要的一点是,为了对付假冒,用于认证的密钥必须在一段时间延迟后才能公布,而一个路由器如果决定不标记一个数据包,它就必须要将距离增加 1,而距离域却是由其上一级路由器加密了的,因此每个路由器必须要预先或者立即得到上一级路由器对该数据包所用的密钥,这是个无法解决的矛盾. 因此,采用一段时间延迟后公布的密钥进行认证的方法是行不通的. 由于找不到合适空间存放数据包经过的路径长度,也没有合适的方法来对该路径长度的数值实施认证,我们只好寻求别的解决途径.

在现有的所有类似的包标记方案中,都有一个距离域用以存放从上一次标记到当前路由器的距离. 我们也许可以利用此距离域,并使路由器根据此域的值选取标记的概率. 设,当距离域为 0、1 …时路由器对数据包进行标记的概率分别为 q_0、q_1 …;如果数据包尚没有被标记过,路由器对其标记的概率为 q_{-1}. 为了保证所有的数据包都得到标记,边界路由器必须标记所有的包. 因此只有在边界路由器处才会出现数据包未被标记的情况(如图 1 中 R_1 处,因为数据包没有经历过其他任何路由器,因此未被任何路由器标记),因此 R_1 以概率 q_{-1} 标记所有数据包,于是 $q_{-1} = p_1$. 当数据包到达路由器 R_2 处,由于距离由 R_1 设置为 0,还没有改变过,因此 R_2 标记数据包的概率为 q_0,于是有 $q_0 = p_2$. 在 R_3 处,数据包中的距离域分别可能有 0 和 1 两个值,前者是经 R_2 标记了的,有 p_2;后者是经 R_1 标记了且未经 R_2 标记的,因被 R_1 标记的共有 p_1,其中又有 $p_1 q_0$ 被 R_2 再一次标记,因此被 R_1 标记而未被 R_2 标记的有 $p_1(1 - q_0)$. 因此 $p_3 = p_2 q_0 + p_1(1 - q_0) q_1$. 在 R_4 处,数据包中的距离分别可能有 0、1、2 共三种情况. 被 R_3 标记过的数据包中距离为 0,有 p_3. 如果数据包被 R_2 标记而不被 R_3 标记,则距离为 1,有 $p_2(1 - q_0)$;如果数据包被 R_1 标记而不被 R_2、R_3 标记的,则距离为 2,有 $p_1(1 - q_0)(1 - q_1)$. 因此 $p_4 = p_3 q_0 + p_2(1 - q_0) q_1 + p_1(1 - q_0)(1 - q_1) q_2$,如此等等. 于是,我们得到 $p_1 = q_{-1}$

$$
\begin{aligned}
p_2 &= q_0\\
p_3 &= p_2 q_0 + p_1(1 - q_0) q_1\\
p_4 &= p_3 q_0 + p_2(1 - q_0) q_1 + p_1(1 - q_0)(1 - q_1) q_2\\
p_5 &= p_4 q_0 + p_3(1 - q_0) q_1 + p_2(1 - q_0)(1 - q_1) q_2\\
&\quad + p_1(1 - q_0)(1 - q_1)(1 - q_2) q_3\\
&\cdots
\end{aligned}
$$

将所有的 $p_i = 1/i$ 代入上面各式,可得,

$$
\begin{aligned}
q_{-1} &= 1\\
q_0 &= 1/2 = 0.5\\
q_1 &= 1/6\\
q_2 &= 1/10\\
q_3 &= 19/540 \approx 0.0352\\
&\cdots
\end{aligned}
$$

如果所有的路由器都遵守规则,按规定标记数据包,则选择以上的标记概率 q_i 是比较好的. 但是,路由器也可能被攻击者攻破了,或者攻击者就是某些路由器的网络管理员,这时路由器可能会根据攻击者的意愿而不按规定对数据包进行标记. 在本文中,我们把由攻击者控制的所有网络设备(包括路由器、傀儡机等)与攻击者等同对待从而不加区分,因为这些设备会按攻击者的意愿行事. 当 i 较大时,q_i 很小,如果攻击者伪造距离域并将距离置为一个较大的数值 i_0,并确保 $i_0 + d_0 \leq 32$,这里 d_0 为攻击者到受害者的实际距离,则后续路由器会以较小的概率标记该数据包. 这对攻击者而言是非常有用的:一方面,较少的包会经中间路由器标记,受害者从一定量的数据包得到的标记信息就较少,从而总的而言,受害者需得到更多来自于攻击者的数据包才能恢复出攻击路径;另一方面,更多的伪造信息会送达受害者,使得攻击者有更多的机会陷害他人(如使得重构的路径中较多的指向其他地方)或增大追踪的不确定性. 解决这一问题的途径有两种. 最直接的、也最容易想到的就是采用认证方式确保这个距离不能伪造. 如同前面讨论过的认证数据包所通过的距离一样,在这里采用认证也会带来同样的困难. 另一种途径是采取一种折衷方法,即在概率 q_i 变得很小之前将其固定为某个适当的值 q. 文献[2]说明采用固定概率时取概率为 0.04 是一个较好的选择. 因此,当 i 较大时,我们将概率固定为 0.04. 由于在前面的计算中有 $q_3 < 0.04$,因此对于所有的 $i \geq 3$,我们令 $q_i = 0.04$. 因此路由器根据距离域以概率 q_i 标记数据包,q_i 如下:

$$q_{-1} = 1,\ q_0 = 1/2,\ q_1 = 1/6,\ q_2 = 1/10,\ q_3 = q_4 = \cdots = 0.04$$

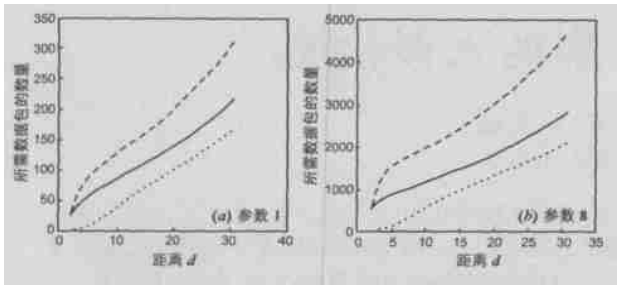
在这种情况下,如果攻击者控制的某个路由器 R_a 伪造距离,其能做到的最多是设置距离为大于 2 的某个值(当然要保证其与攻击者到受害者之间实际距离之和不超过 32).

4 实验分析

本节我们通过模拟实验比较固定概率策略和自适应策略的效果. 对自适应策略需分两种情况讨论,一种是路由器都诚实的情形,另一种是有些路由器也参与伪造的情形. 由于我们只需要数据包的数量,因此不一定非得在实际的网络中把标记算法和路径重构算法完全实现,只需模拟其相应的概率实现过程就可以了*.

图 2 是两种方法下重构攻击路径平均(重复同一过程 10000 次取均值)所需的包数的比较,其中图 2(b) 是假设需 8 个数据包才能传送一个路由器的完整信息的情况,如文献[2,3]中的方法,图 2(a) 是假设只需 1 个数据包就能传送一个路由器的完整信息的情况. 事实上,究竟需要多少数据包才能传送一个路由器的完整信息,这点随着方法的不同而有所区别. 例如,文献[9]中把一个路由器的信息分成 4 块,因此只需 4 个数据包就可传送一个路由器的完整信息. 从图 2(a) 和(b) 我们可以看出,在有路由器参与伪造的情况下,自适应策略的

* 对此感兴趣的读者可以直接与作者联系,作者愿意提供源代码供参考使用.



——固定概率　$p = 0.04$　　……自适应策略,路由器诚实

- - - - 自适应策略,路由器不诚实

图 2　重构攻击路径所需包数的比较

效果不如固定概率策略的好(参数 1 时,所需包数增加 45 %,参数 8 时则增加 65 %);而在没有路由器参与伪造的情况下,自适应策略比采用固定概率时有更好的表现,这使得重构攻击路径所需数据包的量平均减少 44 %(参数 1)和 43 %(参数 8).为什么在路由器参与伪造的情况下,自适应策略的效果反而会更差呢?原因是离攻击者(这里是指参与伪造距离的路由器,设为 R_a)最近的路由器会发现数据包中的距离较大,其就以较小的概率(0.04)标记这些数据包,而在这个路由器标记某数据包以后,与采用固定概率的情形相比,按照我们的自适应策略,该数据包会以更大的概率被后续路由器重新标记,这就存在我们在前面提到的最弱连接(如果在图 1 中的攻击者为 R_a,则最弱连接就是 R_1 - R_2)且其概率比固定概率时最弱连接的概率更小,在这种情况下,我们的自适应方法使得概率的分布更加不均,导致需要更多的数据包以重构攻击路径.虽然在路由器参与伪造的情况下自适应方法会有比固定概率方法更差的结果,我们认为总的来说,自适应策略还是比采用固定概率好,理由如下:

(1)一般来说,相比终端系统而言,路由器被攻破的案例要少很多,这是因为:

(a)和绝大多数终端应用系统相比,路由器的功能较单一,其漏洞就会相对少一些;(b)路由器作为网络的关键基础设施,其安全性会受到更多的重视;(c)路由器通常由网络管理员管理着,他们与普通的终端用户相比,会更专业,对安全的理解会更深;而多数的终端用户中,新手较多,据文献[10],网民数每年按约 50 %的增幅递增,即有约 1/3 网民的网龄不足一年,他们可能没有时间、精力或者没有能力去保障其系统的安全性,或者他们对安全的要求较低,没有必要维持其系统很高的安全性.

(2)即使一些路由器被攻击者攻破,对于攻击者来说,这些路由器是"来之不易"的,因此攻击者一般会将其用于更重要(对攻击者而言)、更隐蔽的其他目的,而不会轻易地将它们用于风暴型拒绝服务攻击,因为相比而言,风暴型攻击比较容易追踪到,从而容易暴露这些路由器.

(3)即使攻击者不惜代价,将手中的路由器用于风暴型拒绝服务攻击,与其控制并利用的终端系统的相比,这种情形会少很多.因此,整体而言,与固定概率策略相比,在系统采用自适应标记的情况下,受害者需更少的数据包重构攻击路径.因此,在包标记中,以采用自适应的标记策略为佳.

5　结论

本文给出了用于 IP 追踪的包标记的一个自适应策略.通过实验证实,与通常的固定概率策略相比,采用自适应策略可以使得受害者通过更少的数据包(相当于固定概率时的 56 %)就能重构攻击路径,从而为受害者及早地对 DoS 攻击作出响应、减少攻击带来的危害创造了条件.此自适应策略既可用于增强已有的标记方案,也可用于新的标记方案的组件.此外,我们还指出了文献[8]中采用认证的方法确保距离真实性的方法是不可行的,从而推翻了该文的主要结论.

参考文献:

[1] CERT/CC Statistics 1988 - 2002[OL]. http://www.cert.org/stats/cert_stats.html.

[2] Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson. Practical network support for IP traceback[A]. Proceedings of the 2000 ACM SIGCOMM Conference[C]. Stockholm, Sweden, August 2000. 295 - 306.

[3] Dawn X Song, Adrian Perrig. Advanced and authenticated marking schemes for IP traceback[A]. Proceedings of IEEE INFOCOM '01[C]. Anchorage, Alaska, April, 2001. 878 - 886.

[4] K Park, H Lee. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack[A]. Proceedings of IEEE INFOCOM '01[C]. Anchorage, Alaska, April, 2001. 338 - 347.

[5] I Stoica, H Zhang. Providing guaranteed services without per flow management[A]. Proceedings of the 1999 ACM SIGCOMM Conference[C]. Boston, MA, Aug. 1999. 81 - 94.

[6] Dequan Li, Purui Su, Dengguo Feng, Notes on packet marking for IP traceback[J]. Journal of Software 2004, 15(2): 250 - 258. [OL] http://www.jos.org.cn/1000 - 9825/15/250.htm.

[7] Arnon Boneh, Micha Hofri. The coupon-collector problem revisited[J]. Commun Statist Stochastic Models, 1997, 13(1): 39 - 66.

[8] T Peng, C Leckie, R Kotagiri. Adjusted probabilistic packet marking for IP traceback[A]. Proceedings of the Second IFIP Networking Conference (Networking 2002)[C]. Pisa, Italy, May 2002. 697 - 708.

[9] Dequan Li, Purui Su, Dengguo Feng. Router numbering based packet marking[A]. Proceedings of the Ninth International Conference on Distributed Multimedia Systems[C]. Miami, Florida, USA September, 2003. 698 - 703.

[10] CNNIC. 中国互联网络发展状况统计报告[R]. 北京:中国互联网络信息中心, 2002. 7.

作者简介:

李德全　男,1969 年 2 月出生于四川乐山市,博士,主要研究领域为信息安全、网络安全.
Email: dequanli@ieee.org.