文章编号:1001 - 9081(2006)07 - 1646 - 03

基于移动代理的分布式拒绝服务攻击防御模型

叶 茜,张基温
(江南大学 信息工程学院,江苏 无锡 214122)
(kapok6652@sina.com)

摘 要:使用报文标记和移动代理技术,构建基于移动代理的分布式拒绝服务(DDoS)攻击防御模型,在很大程度上降低了来自 ISP 域外的分布式拒绝服务攻击对域内主机的影响。并利用移动代理的容错性,使模型中重要元件具有很好的抵抗分布式拒绝服务攻击的性能,提高了防御模型自身的抗攻击性。最后讨论了模型的具体实现。

关键词:分布式拒绝服务;移动代理;报文标记;数据包过滤;攻击签名
中图分类号: TP393.08 **文献标识码**:A

A model for defending against DDoS attacks based on mobile-agent

YE Qian, ZHANG Ji-wen
(*School of Information Engineering, Southern Yangze University, Wuxi Jiangsu* 214122, *China*)

Abstract: A model for defending against DDoS(Distributed Denial of Service) attacks based on mobile agent was proposed, using the technique of packet marking and mobile agent. This model can minimize the damage of the DDoS attacks in the ISP domain. The model has a good anti-attack character by mobile agent's tolerant ability and the components can resist the DDoS attack. Finally, the implementation of the model was discussed.

Key words: Distributed Denial of Service(DDoS); mobile agent; packet marking; packet filtering; attack signature

0 引言

DDoS 攻击是 Internet 目前面临的最严峻的威胁之一,攻击技术近年来也不断发展,造成的破坏也越来越大。根据 CNCERT/CC(国家计算机网络应急技术处理协调中心)2005 年上半年网络安全工作报告[1],分布式拒绝服务攻击在技术实现上开始通过成群的受控主机进行分布式的高强度攻击;同时产生非常随机的源 IP 地址,能够更好地保护攻击源不被追踪到;攻击数据包结构形式随机变化,很难用统一的方法检测;利用网络协议缺陷与系统漏洞缺陷,加强攻击强度;更高的发包速率,攻击特征更不明显等。

研究人员提出了多种防御 DDoS 攻击的方法。Ferguson 等人使用的边界过滤法是在边界路由器上对来自网络内部的报文进行检查,如果报文的源 IP 地址不在本网络的范围内,则可以断定它是伪造报文,对其进行过滤[2],但由于启动报文源地址检查功能会给路由器的性能带来较大影响,并且攻击者仍然可以伪造同一网域内其他主机的 IP 地址。文献[3~5]使用不同的方法进行 DDoS 攻击源追踪,文献[3]提出一种随机采样的方法,路由器随机地采样转发的网络数据包,填写部分网络路径信息,被攻击子网在接收大量网络数据包后,就可以恢复出完整的路径信息,从而确定攻击源;Belovin 在文献[4]中提出了类似的方法,利用 ICMP 报文进行攻击源追踪。Burch 和 Cheswick 提出的方法使用已知的映射技术描绘出从受害者到每个网络的路由图[5]。这些方法的主要不足在于即使追踪到攻击源和受害者之间的路由,也无法及时采取有效的防御措施,而且,攻击源和受害者之间的路由器也许已受到破坏。基于集中拥塞控制(Automatic Congestion Control, ACC)[6]给核心路由器增加了新的功能,以检测由 DDoS 攻击引起的拥塞,并把从速率上限制高带宽的集中作为响应的手段,但由于 ACC 不能很好区分合法流量和恶意流量,所以在丢弃恶意流量的同时也丢弃了合法流量。U. K. Tupakula[7]等提出一个控制器 - 代理的自动化模型以此来降低 ISP 域内 DDoS 攻击发生的可能性,但该模型中控制器一旦受到 DDoS 攻击,则整个防御系统就无法正常运转。

本文通过研究移动代理的优点,对 Tupakula 的自动化模型进行改进,构造出基于移动代理的 DDoS 防御模型。该防御模型能较容易地确定来自不同攻击系统的攻击签名;可以在接近攻击源的位置阻止攻击流;并降低了建立健壮的分布式防御系统难度。

1 移动代理

移动代理[8]是一段独立运行的计算机程序,它能自主地在网络中按照一定的规则从一个节点迁移至另一个节点,利用合适的计算资源,代表用户完成特定的任务;它可以在执行的任一点挂起,等迁移到另一个节点后再继续执行。一般来说,移动代理可以是一些驻留在主机上的小程序或代码片段,对它的建立、撤消、迁移和维护相对而言是比较容易的。所以,移动代理具有降低网络流量,支持移动用户,支持服务定制,容错性好等优点。

本文利用 Agent 的移动特性,将报文标记和过滤等功能封装在 Agent 实体中,并分派到边界路由器、网关、服务器等关键网络节点上。在这些节点上分析、过滤可疑数据和异常行为,可以避免单点失效;同时位于不同节点上的 Agent 可以交换信息,使得能够进行协同检测和防御分布式拒绝服务攻

收稿日期:2006 - 01 - 23;**修订日期**:2006 - 03 - 15

作者简介:叶茜(1980 -),女,安徽淮南人,硕士研究生,主要研究方向:网络安全; 张基温(1943 -),男,山西临汾人,教授,主要研究方向:网络安全.

击;将 Agent 分派到边界路由器,使得处理更接近攻击源,可以保证在攻击发生的第一时刻采取有效防御措施,并减少了网络延迟;另外,Agent 具有智能特性,能够适应不断变化的网络环境,实现自身的知识进化,使得防御体系更加有效。

2　基于移动代理的 DDoS 攻击防御模型

本文把包含 ISP 和客户的体系结构作为研究对象[7],将路由器分为内部路由器和外部路由器。内部路由器属于 ISP 域,外部路由器属于客户或其他 ISP 域;边界路由器指与外部路由器相邻的内部路由器,其他内部路由器被看作中转路由器。虽然存在攻击流量来自内部路由器的可能,但通常情况下 DDoS 攻击都是跨域进行,即攻击流量来自 ISP 域外,通过边界路由器,最后到达 ISP 域内的受害者。因此本文中防御模型主要针对来自域外的攻击流量。虽然 DDoS 攻击具有假冒源地址、使用广泛的攻击签名等特性,通过在边界路由器上进行设置,可在离攻击源最近的点阻止攻击,从而提高响应效率。

基于移动代理的分布式拒绝服务攻击防御模型由执行代理(ExcuteAgent,EA)和控制代理(ControlAgent,CA)两个主要部分组成,如图 1 所示。将具有报文标记和过滤行为的执行代理派往 ISP 域的所有边界路由器上,其功能是标记流往受害者报文的分片域,并对攻击流进行过滤。控制代理可在 ISP 域内任何主机或具有 ACC 控制的中转路由器上运行,并按预先规定的路线和策略在控制节点间迁移,对执行代理进行控制操作和收集数据。ISP 域内所有节点上都存在移动代理执行环境,可以接受移动代理并且提供对本地资源的访问。

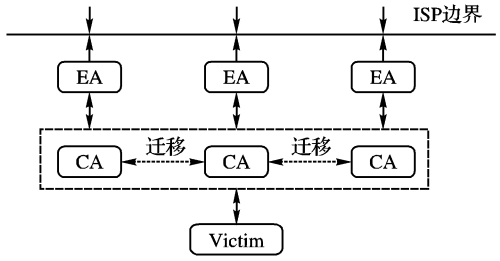

图 1　基于移动代理的 DDoS 攻击防御模型结构

2.1　节点结构模型

节点的结构模型如图 2 所示。

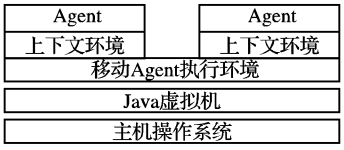

图 2　节点结构模型

2.1.1　泊位

泊位(Place)是移动 Agent 执行环境上的一个虚拟的位置,它管理移动 Agent 的到来和离开并为其提供可以访问的资源,同时还为 Agent 之间的信息交换提供支持。一个移动 Agent 要么驻留在某个泊位上,要么在两个泊位之间迁移。在移动 Agent 执行环境的安全策略下,由泊位赋予迁移到其上的移动 Agent 一定的权限,从而对移动 Agent 的行为进行约束。每个泊位有自己惟一的名字,一个执行环境可以有多个泊位。

2.1.2　移动 Agent 执行环境

移动 Agent 执行环境是支持 Agent 系统的关键部分。移动 Agent 的交互行为以及对本地资源的访问均由它来控制和支持,它主要包括以下几部分:

认证服务　每当一个移动 Agent 迁移到某个泊位上时,就要对它的身份域以及对资源的请求进行验证,以决定是接受这个移动 Agent 还是拒绝它的访问。

资源管理　为这个执行环境中活动的 Agent 分配资源,同时对这些资源进行管理。

通信模块　实现各 Agent 之间、Agent 与系统之间的通信和数据交换。

2.2　运算组成元件

本文参照 Cubaleska 等人[8]定义的代理元件加以修改,制定满足模型需要的两个移动代理运算组成元件。

2.2.1　执行代理运算组成元件

在边界路由器 $Erouter_i$ 上执行报文标记和过滤行为后的状态,包含代理的资料数据。

执行代理:$Eagent^j = (bc, r, md^i, rid^i)$

1) bc: Agent 执行的二进制代码。

2) r: 描述 Eagent 的迁移路径,包括和边界路由器直接相邻的中转路由器。

3) md^i: Agent 在 $ERouter_i$ 上执行任务后累积的所有资料($Md^{i-1} \subset Md^i$),如果该边界路由器不幸被攻陷,则和它相邻的中转路由器可以利用 md^i 进行信息恢复。

4) rid^i:边界路由器 $Erouter_i$ 在攻击经过重新恢复功能后,送给相邻中转路由器的恢复确认码,通知中转路由器 $Erouter_i$ 已经恢复,使得 $Erouter_i$ 重启报文标记和过滤功能。

2.2.2　控制代理运算组成元件

在域内主机 $Host_j$ 上对执行代理进行控制操作和收集数据后的状态,包含代理的资料数据。

控制代理:$CAgent^j = (bc, r, md^j, uid^j, voc)$

1) bc: Agnet 执行的二进制代码。

2) r: 描述 Agent 迁移路径,包括 ISP 域内所有可以访问的主机。

$r = (Host_1, \cdots, Host_j, \cdots, Host_n)$

3) md^j: Agent 在 $Host_j$ 上执行任务后累积的所有资料($Md^{j-1} \subset Md^j$),如果该主机作为控制器在执行任务期间不幸被攻陷,则其他正常主机可以利用它进行信息恢复。

4) uid^j:每个 $Host_j$ 产生的独特回复确认码,当 $CAgent^j$ 移动到下个 $Host_{j+1}$ 时回复 uid^j 给 $Host_j$,确认是否正确到达。

5) voc:可以为移动 Agent 的迁移路径指定独立或非独立两种计算[8],在独立计算中不需要其他主机资料来加以计算;在非独立计算中则需要其他主机资料输入才可以计算。若使用非独立计算则可限制 ISP 域内作为控制器的主机。

首先使得每一主机储存前一主机的 uid 值,当 $Host_j$ 上控制代理 $CAgent^j$ 移动到 $Host_{j+1}$,正常情况下 $Host_{j+1}$ 会给 $Host_j$ 回复正确的 uid^{j+1},然后 $Host_j$ 将此值对比自己存储的 uid^{j+1} 看是否相符。不相符,则可知作为控制器的 $Host_j$ 已被攻陷,这时控制代理就会根据 voc 中设定的路径移动到另一安全主机,并同时转移 md^j 到新主机,同时设定该新主机作为新的控制器。

一旦 DDoS 攻击发生,此时移动到某主机或路由器上的控制代理就被激活,该主机或路由器则成为控制器。

3　模型具体实现

3.1　控制代理

当 DDoS 攻击发生时,受害者向当前控制器发出攻击产生报文,控制代理被相应激活。控制代理做如下准备:

1) 随机产生一个控制 ID 号;

2) 为每个执行代理分配唯一标识符(执行代理 ID 号);

3) 维护 ISP 域内边界路由器 32 位 IP 地址和分配在其上

的与执行代理 ID 号相关联的数据库。

控制代理为每个执行代理赋予唯一标识符(执行代理 ID 号),假设某 ISP 域内有 250 个边界路由器,只需 16 位数据报文分片域中的 8 位($2^8 - 1 = 255$)就可存放所有执行代理 ID 号。根据转发数据报文分片域中被标记的执行代理 ID 号,通过关联数据库映射,就可重构出边界路由器的 IP 地址。因此,由一个被标记过的攻击报文,就可大致识别出攻击源所在的 ISP 域。若控制代理迁移一次,控制器位置改变,以上步骤就重新进行一次。

准备工作完成后,控制代理立即向受害者发送含有控制 ID 和所有执行代理 ID 的加密报文。随后,控制代理对执行代理产生两个重要命令。

第一个是:当控制代理收到来自受害者的攻击产生报文时,它向所有执行代理发送包含控制 ID、执行代理 ID、受害者 IP 地址的命令 1 报文,格式为:Command1 (Cagent_ID;Eagent_ID;Victim_IPaddress)。

第二个是:当受害者识别出基于执行代理 ID 的攻击签名,并要求控制代理对被识别出的执行代理发送攻击阻止请求,控制代理则向所有执行代理发送包含控制 ID、执行代理 ID、受害者 IP 地址、攻击签名的命令 2 报文,格式为:Command2 (Cagent_ID;Eagent_ID;Victim_IP address;Attack_signature)。

3.2 执行代理

在通常情况下执行代理像普通路由器一样运作,只有在 DDoS 攻击发生期间执行代理的特殊功能才被激活。当执行代理收到来自控制代理的特殊命令时,对流向受害者的网络流量进行标记,并只对流向受害者且符合攻击签名的攻击流进行过滤。

3.2.1 报文标记

当执行代理收到 Command1 报文,报文标记功能被激活。执行代理首先检查通过该路由器上的报文目的 IP 地址是否与命令 1 中受害者 IP 地址相同:若不同,则不予标记;若相同继续进行处理。其次检查该报文片头域是否被标记:若没被标记,则将 Command1 中控制 ID 和自身执行代理 ID 填入该报文分片域;若已标记则检查该报文分片域中是否具有合法控制 ID,若不合法,则判定为攻击者伪造直接丢弃。这样处理,执行代理不需了解其他执行代理的合法 ID,就可过滤掉一部分伪造攻击报文,不仅使受害者受攻击程度得到缓解,而且使搜索更有效。

随后受害者收到所有经过标记的报文,由于受害者知道合法的执行代理 ID,则通过检查该报文分片域中执行代理 ID 是否合法,可过滤掉分片域中是伪造执行代理 ID 的数据报文。由于受害者知道合法的控制 ID 和执行代理 ID,所以受害者在识别来自不同攻击源的攻击签名时能更快捷和有效。

```
Pi = Input packet
Markpacket(Pi)
{ if Markpacket(Pi) = = true                    //报文已被标记
  { if Cagent_ID = = false                      //控制代理 ID 不合法
    Drop(Pi);                                   //丢弃该报文
    Log(Pi)                                     //生成日志和攻击签名
  }
  Else                                          //报文没被标记
  { Pi_fragment field_1 = Cagent_ID;
    Pi_fragment field_2 = Eagent_ID;
    Markpacket(Pi) = true
  }
}
```

3.2.2 报文过滤

当受害者识别出来自不同攻击源的攻击签名后,它向控制代理更新攻击签名信息,控制代理则根据相应的执行代理 ID 要求它们对攻击流量进行过滤。由于是通过执行代理 ID 来确定攻击签名,因此仅有攻击流量流过的执行代理才会接收到 Command2 报文。

当执行代理收到 Command2 报文时,则激活报文过滤功能。首先检查通过自己的报文是否与 Command2 中的攻击签名相匹配,若匹配,则丢弃该报文;若不匹配则重新对该报文进行标记。其中对不符合攻击签名的合法报文进行重新标记的目的是:可以使得受害者及时获知网络流量的变化特征,易于受害者跟踪攻击流量模式的变化。执行代理在收到控制代理的复位命令前会持续地对攻击流量进行阻止。

```
Pi = Input packet
Filterpacket(Pi)
{ if Pi = = Attack signature
  { Drop(Pi);
    Log(Pi)
  }
  Else
    Markpacket(Pi)
}
```

4 结语

本文提出的基于移动代理的 DDoS 防御模型具有良好的可扩展性,可以自动适应网络拓扑的变化。防御体系的大小不依赖于攻击者的数量,而是取决于移动代理数目,即 ISP 域的规模。当攻击没有发生时,代理可以像普通路由器一样运行。根据合法执行代理 ID 号,受害者能容易地确定来自不同攻击系统的攻击签名;在接近攻击源的位置对攻击流量进行阻止,响应迅速;每个执行代理只需检查和阻止流经它的攻击签名,延迟相对较小。控制代理可以在 ISP 域内的不同主机或路由器之间迁移,攻击者很难通过瘫痪控制代理而破坏整个防御体系。但该模型并没有考虑代理之间和代理与受害者之间以及代理进行迁移时所涉及的通信安全问题,这将是下一阶段工作的重点。

参考文献:

[1] CNCERT/CC 2005 年上半年网络安全工作报告[EB/OL]. http://www.cert.org.cn/upload/2005CNCERTCCAnnualReport.pdf, 2005.

[2] FERGUSON P, SENIE D. RFC2827, Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing[S]. IETF, 2000.

[3] SAVAGE S, WETHERALL D, KARLIN A, *et al*. Practical Network Support for IP Traceback[A]. Proceedings of the 2000 ACM SIGCOMM Conference[C], 2000.295 - 306.

[4] BELLOVIN SM. ICMP Traceback Messages[Z]. IETF, 2000.

[5] BURCH H, CHESWICK B. Tracing anonymous packets to their approximate source[A]. Proceedings of 2000 USENIX LISA Conference[C], 2000.319 - 327.

[6] MAHAJAN R, BELLOVIN SM, FLOYD S, *et al*. Controlling High Bandwidth Aggregates in the Network[J]. Computer Communications Review, 2002, 32(3):62 - 73.

[7] TUPAKULA UK, VARADHARAJAN V. A practical Method to counteract denial of service attacks[A]. Proceedings of the twenty-fifth Australasian computer science conference in research and practice in information technology[C], 2003.204 - 275.

[8] CUBALESKA B, SCHNEIDER M. Detecting DoS attacks in mobile agent systems and using trust policies for their prevention[A]. Proceedings of the 6th world multiconference on Systemics Informatics and Cybernetics[C]. Orlando, USA, 2002.