分布式拒绝服务攻击研究进展

文伟平 卿斯汉 王业君

中国科学院 信息安全技术工程研究中心，北京 100080
中国科学院 软件研究所，北京 100080

摘 要 分布式拒绝服务攻击是目前一种常见而有效的网络攻击手段。本文首先介绍了分布式拒绝服务攻击的实现原理，并讨论了当前DDoS攻击防范的难点及防范的关键技术；然后讨论了DDoS攻击的热点问题——攻击源追踪问题；最后对DDoS攻击的研究方向进行了归纳和展望。

关键词 分布式拒绝服务 攻击 防范 追踪

1 引 言

拒绝服务攻击[1][2]（Denial-of-Service Attack，DoS Attack）通过消耗目标主机或者网络资源，干扰或者完全阻止为合法用户提供正常服务。分布式拒绝服务攻击(Distributed Denial-of-Service Attack, DDoS Attack)[3]则是增强型DoS攻击，采用了分布式对单个或者多个目标进行大规模的协同攻击。这种攻击非常容易发起，却难以被阻止或者追踪。2000年4月，Yahoo、CBay、AMazon和CNN等几大著名网站都遭受到DDoS攻击，造成了严重的经济损失。据CERT统计，拒绝服务攻击以每年50%的速度增加，而预防和追踪DDoS的技术却未能以相同的速度发展。2001年，加州大学研究机构发布的一份报告中指出全世界范围内每周至少发生40次拒绝服务攻击。同年中美黑客大战中，DDoS攻击也被广泛使用。至此，DDoS攻击已成为网络安全不容忽视的问题。

DDoS攻击的防范根据其实现手段分为：基于网络的DDoS防范和基于主机的DDoS防范。在防范技术上主要有以下三种方式：①入侵检测。主要采用传统的基于模式匹配[4]的检测思想，对网络连接，数据源、数据内容、数据包等网络元素进行检测，这种检测准确度不高，只能对几种特定类型的DDoS入侵进行有限的防御，在网络攻击手段发展变化后就无能为力了；②基于数据流量的异常检测。这种检测主要是为源地址或源地址段设定一个流量范围，超出范围就认为出现异常，但是此方法过于单一，准确率也较低，有时会对正常服务造成影响；③手动分析。由系统管理员手动分析入侵特征，然后依靠经验在保证最小的漏判率和最大限度的保证系统性能的基础上建立检测规则和策略。手动分析的方法易于操作但工作量大、速度慢、规则更新不全面，并需要大量的实践经验，很难达到满意的检测效果，误判率往往较高。因此，对DDoS攻击防范的研究依然是一个长期研究的课题。

本文的组织如下：第2节介绍DDoS攻击的原理；第3节分析DDoS攻击防范的难点；第4节阐述了DDoS攻击防范的关键技术；第5节讨论了DDoS攻击的源追踪技术；第6节对DDoS攻击的发展趋势和研究方向进行了展望；最后是简短小结。

2 DDoS攻击的原理

DDoS攻击系指采用分布式的攻击方式，联合或控制网络上能够发动DoS攻击的节点主机同时发动攻击，制造数以百万计的数据分组流入欲攻击的目标网络，致使流向目标网络的服务请求极度拥塞，而

造成目标网络系统瘫痪的攻击手段。DDoS 采用一种三层客户服务器结构，如图 1 所示：

攻击者在攻击控制台操纵整个攻击过程。每个攻击服务器是一台已被入侵并运行了特定程序的系统主机，能够控制多个攻击代理（Attack Agent）。每个攻击代理也是一台已被入侵并运行特定程序的系统主机。攻击代理接收受控服务器下发的命令向被攻击目标网络发送拒绝服务攻击数据包。迄今为止，攻击者最常使用的 DDoS 攻击工具包括以下几种：Trinoo[5], TFN2K[6]、Stacheldraht[7] 、 Mstream[8] 和 Shaft[9]。

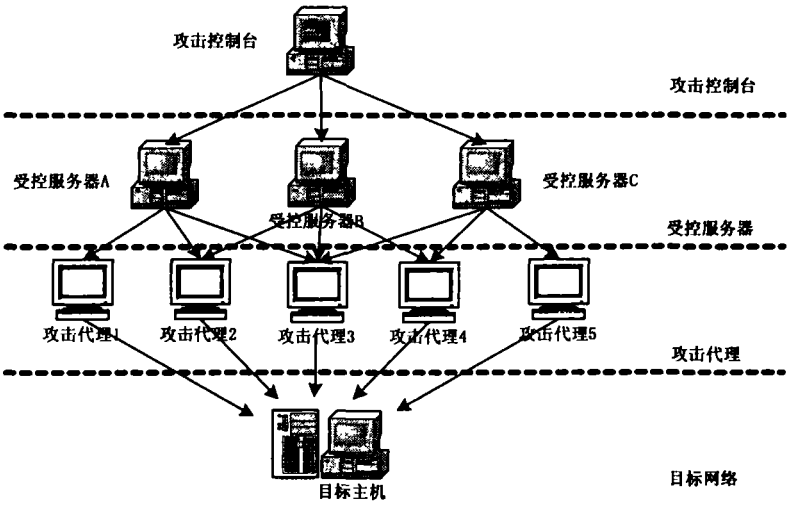

图1 分布式拒绝服务攻击入侵示意图

为了提高 DDoS 攻击的成功率，攻击者需要控制成百上千的被入侵主机。这个过程可分为以下几个步骤：①探测扫描大量主机以寻找可入侵主机目标；②入侵有安全漏洞的主机并获取控制权；③在每台入侵主机中安装攻击程序；④利用已入侵主机继续进行扫描和入侵。

由于整个过程是自动化的，攻击者能够在几秒钟内入侵一台主机并安装攻击工具，在短短的数小时内可以入侵并控制数千台主机。

3 当前 DDoS 攻击防范的难点

3.1 攻击数据包的随机性

目前对DDoS攻击的检测大都采用传统的入侵检测思想，攻击者将攻击数据包内容的随机化，能够使部分DDoS攻击逃避对抗工具的检测和过滤。随机数据包的构造方法有以下几种：①源IP地址的随机化。产生无规律的随机源IP地址是进行DDoS攻击的基本要求，分布式的攻击再加上伪造的随机IP地址，使得攻击源更加难以追踪；②系统标识的随机化。计算包结构的时候会生成一种系统标识（SYS Indent），这种标识决定常见操作系统构造包的特征，攻击者根据这些特征再使用随机量，形成和正常系统基本近似的数据包；③数据包结构和其他内容的随机化。数据包结构和内容的随机化可以逃避模式匹配算法的检测。例如早期的TFN构造包中使用了一些固定数据，而成为被检测的对象，现在的TFN3K数据包中的包结构基本上都是随机形成的了。一些其他的随机包构造方法如图2所示。

```
ipheader.id = SYSIdent.id + random()
ipheader.ttl = SYSIdent. ttl + random(10)
tcpheader.th_win = SYSIdent.window;
tcpheader.seq = random();     //随机量符合系统Seq的要求
tcpheader.sport = randdom(65535); //随机量要同系统常用的接近
```

图2 随机攻击包的构造方法

3.2 多种协议及多种形式混合的攻击

混合攻击综合了多种协议和多种形式的攻击，能够更大地扩大攻击的效果，这也从侧面反映了当前DDoS攻击防御技术的单一性。例如SYN Cookie是当前防御SYN Flood[10]攻击最有效的方法，SYN Cookie不仅能够扩大 TCB 的最大数量限制，而且也能更小地存储 SYN 请求。对于 SYN Cookie，其 CPU 资源主要消耗在对 SYN 包的 Cookie 计算，在接收到 SYN 包的时候，SYN Cookie 将这个包加密生成 Cookie，

SYN 攻击发起的时候，保存 Cookie 的表就可能增大。当 SYN Cookie 接收到 ACK 包的时候，会检查包中的 ACKnowledgement Number，查看是否正确。对于 RST 包，会对应地删除 Cookie 队列，会进行相应查询。因此 SYN Flood 综合 RST Flood 和 ACK Flood 则可以加强 SYN 攻击对主机资源的消耗。

3.3 大规模分布式高强度攻击

这是一种通过提高 DDoS 攻击强度来提高攻击效果的攻击手段。很多 DDoS 攻击者掌握着大量的攻击代理，很多攻击代理有高速的带宽和高档的系统配置，这些优势势能够让攻击者发起高强度的分布式攻击，不仅会对目标服务器造成伤害，也能对网络的路由器等核心设备造成威胁。而对网络设备的攻击将造成大范围的网络拥塞或网络中断。这也是对抗 DDoS 攻击的一大挑战。

3.4 分布式反射拒绝服务攻击

分布式反射拒绝服务攻击（Distributed Reflection Denial-of-Service Attack，DRDoS Attack）[11][12]是 DDoS 攻击的变形，与 DDoS 的不同之处就是它不需要在实际攻击之前控制大量攻击代理。攻击时，攻击者利用特殊发包工具把伪造了源地址（被攻击者地址）的 SYN 连接请求包发送给那些大量的被欺骗的服务器，根据 TCP 三次握手规则，这些服务器群会向源 IP（也就是被攻击者）发出大量的SYN+ACK或RST包来响应此请求。结果原来用于攻击的洪水数据流被大量服务器所分散，并最终在被攻击者处汇集为洪水，使被攻击者难以隔离攻击洪水流，并且更难找到洪水流的来源。分布式反射拒绝服务攻击的结构如图 3 所示。

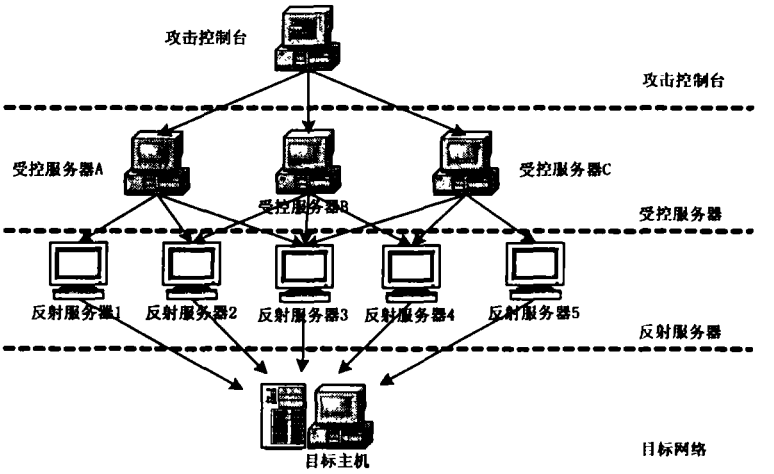

图3 分布式反射拒绝服务攻击示意图

这里反射服务器是指当收到一个请求数据报后就会产生一个回应数据报的主机，如 WEB 服务器。不象以往 DDoS 攻击，利用反射技术，攻击者不需要把服务器做为网络流量的放大器，甚至可以使洪水流量变弱，最终才在目标主机处合为大容量的洪水。这样的机制让攻击者可以利用不同网络结构的服务器作为反射服务器以发起攻击。现在有三种特别有威胁的反射服务器：DNS 服务器、Gnutella 服务器、和基于 TCP/IP 的服务器（特别是 WEB 服务器）。

4 DDoS 攻击的防御技术

目前在 DDoS 攻击的防御方面，大多数工作都还是尽量去缓解攻击。实际上带宽消耗式的攻击从单一的被攻击者来说，基本上是没有办法消除的。DDoS 攻击的防御技术有：入口过滤、随机丢包、SYN Cookie 和 SYN Cache 技术、消极忽略、主动发送 RST 和 PUSHBack 与 CENTERBack 技术等。

4.1 入口过滤（Ingress Filtering）[13]

防火墙、路由器等边界设备的数据包过滤是现在对抗拒绝服务攻击的主要办法。通过对一些攻击特征的分析，将攻击数据流在外围过滤掉，可以大大缓解被攻击主机的负担。例如防御 ICMP Flood，可以在边界上直接关闭 ICMP 包。对于其它的攻击方式，可以通过过滤部分源 IP 地址来缓解攻击，国内大部分站点就是通过过滤非国内 IP 地址的访问来实现防范目的的。

入口过滤防御 DDoS 攻击也存在一些问题，主要有以下几点：①需要进行特征分析，而大部分攻击很难获得有效的特征；②在攻击发生时要及时进行攻击分析，这并不是每个安全管理员具备的能力，而且要求管理员必须自己能够控制边界设备；③边界设备被攻击的情况是没有办法过滤的，现在很多攻击就是朝着路由器去的，这本身就是一个很难解决的问题。

4.2 随机丢包（Random Drop）

部分网络设备为了防御 DDoS 攻击采取了随机丢包的方法，这种方法利用了网络设备本身的特性，网络设备常常在流量较大的时候采取丢包的方式来维持其功能的正常。随机丢包是在难于获取有效特征或无其它有效防御措施的情况下所采取的一种方法，要维持网络正常，只好随机地将数据包丢弃，尽量保证能提供服务，当然丢弃的包并不一定就是攻击的数据包，而放行的也并不一定就是正常的包。

4.3 SYN Cookie 和 SYN Cache

防范 SYN Flood 攻击必须要减少为维持很大数量状态而分配的系统资源，或者通过完成 TCP 连接释放更多的可分配资源。SYN Cache 和 SYN Cookie 就是要来达到这个目的的，SYN Cache 主要用于行为监控，分配很少的状态结构来纪录最初的连接请求，而 SYN Cookie 的功能就是编码那些能够完成 TCP 三次握手过程的正常的连接。

初始的 SYN 请求包含一些连接选项，通常包含 MSS,时间戳等，SYN Cache 在主机上为这些连接选项分配一些资源，它能够应对状态资源分配溢出的情况，并且选择丢弃合适的状态保证下一步存储的顺利进行。

SYN Cookie 技术实现了对 SYN Flood 攻击的防范。在收到客户端的 SYN 包后，防火墙代替服务器向客户端发送 SYN+ACK 包，如果客户端在一段时间内没有应答或中间的网络设备发回了 ICMP 错误消息，防火墙则丢弃此状态信息；如果客户端的 ACK 到达，防火墙代替客户端向服务器发送 SYN 包，并完成后续的握手最终建立客户端到服务器的连接。通过这种技术，保证了每个 SYN 包的真实有效性，确保服务器不被虚假请求浪费资源，从而彻底防范对服务器的 SYN Flood 攻击。

这种方法的主要问题有：①SYN Cookie 是通过返回的 ACK 来完成整个连接的建立，不依赖于流程化的 SYN，SYN+ACK 传送，可能造成 ACK Flood 攻击；②提供一种基于 ACK 绕过防火墙的机制。因为防火墙依赖 SYN 来过滤外部连接，而现在建立连接根本不依赖 SYN 包。

4.4 消极忽略

根据 TCP/IP 协议，在客户端发起 SYN 连接请求后，如果服务器没有 SYN+ACK 的回应，系统通常会在一段时间后再次发出连接请求。在高强度 DDoS 攻击的情况下，可以采用消极忽略方法，忽略所有的第一次 SYN 请求，等待第二次 SYN 请求的到来，如果第二次请求数据包出现，则可认为是有效包。因为多数的 SYN Flood 攻击发送数据包是一次性的，这种办法在高强度的 DDoS 攻击下能够起到一定的缓解作用。

这种方法的不足主要有：①第一次连接都将被忽略，正常连接就需要花费更多时间；②只能针对那些仅仅发一次包的攻击，局限性大。

4.5 主动发送RST

这也是一种防御 SYN 攻击的办法，SYN 攻击造成危害的原因主要是很多不正常的 SYN 请求占据了 TCB 表，从而让新的请求无法得到回应。当服务器接受到 RST 包的时候，就会将 TCB 中的相应纪录释放。主动发送 RST 的方法就是利用了这种特点，通过第三方主动发送 RST 包，让服务器的缓冲区尽快释放。但是，这种办法并未将攻击请求包和正常请求包区别对待。

4.6 PUSHBack[14]与CENTERBack[15]

PUSHBack 和 CENTERBack 是两种对抗 DDoS 攻击的防范技术。DDoS 攻击造成网络拥塞控制问题，但是因为这种拥塞是由于 DDoS 攻击造成，而不是传统的终端对终端的拥塞，所以，这个问题只能由路由器来解决。对每个路由器加入检测攻击和优先丢包功能。为了将路由器的资源都被用于合理的数据流，上游路由器也需要被通知丢弃这一类的包。而这类包需要路由器能够准确地进行特征描述。

PUSHBack 与 CENTERBack 都是基于路由器的主动防御措施，目前处于研究阶段，因为这些方法的实施，需要网络大范围的路由器功能支持，如果某段路由的功能不支持，容易导致防御失败。关于 PUSHBack 与 CENTERBack 的详细请参阅文献[14]和[15]。

5 DDoS 攻击源的追踪技术

DDoS 攻击源追踪算法[16][17][18]的基本原理：由于网络上进行 DDoS 攻击的数据包具有“伪装”的 IP 源地址或者随机化构造的特征，使得我们无法获取真正的源信息。但从另一个角度来说，尽管 IP 包头中的源地址是虚假的，但每个 IP 包都必须经过从攻击方到被攻击者之间的路由器转发，如果能够记录下这些路由器，就可以恢复出攻击所经过的路径。追踪算法就是从最接近被攻击主机的路由器开始，然后开始检查上游数据链，直到找到攻击流量发起源。目前比较常用几种追踪算法有：链路测试、ICMP 追踪、数据包记录和随机数据包标记追踪等。

5.1 链级测试

5.1.1 入口过滤

很多路由器都提供输入调试特性，这能让管理员在一些出口端过滤特定的数据包，而且能决定可以达到那些入口，这种特性可以被用来追踪。被攻击主机在确定被攻击后，从所有的数据包中描述出攻击包特征。通过这些特征，管理员在上游的出口端配置合适的入口监控策略。这个过滤会体现出相关的输入端口，过滤过程可以一直朝上游进行，直到能够到达最初的源头。当然这种工作大部分依赖于手工，一些国外的 ISP 联合开发的工具能够在它们的网络中进行自动的追踪。

这种方法最大的问题就是输入调试的管理量大，需要同多个 ISP 协作。

5.1.2 控制淹没[19]

这种方法主要通过制造控制淹没，观察路由器的状态来判断攻击路径。分析者首先拥有一张上游的路径图，当受到攻击的时候，可以从被攻击主机的上级路由器开始依照路径图对上游的路由器进行控制淹没，由于这些数据包同攻击者发起的数据包同时共享了路由器，因此增加了路由器丢包的可能性。通过这种方式沿路径图不断向上搜索，就能够接近攻击发起的源头。

该方法存在以下几个问题：①本身就是一种拒绝服务攻击，会对一些信任路径也进行拒绝服务攻击；②控制淹没要求有一个几乎覆盖整个网络的拓扑图。③只能对正在进行攻击的情况有效。

5.2 ICMP追踪[20]

这种算法利用了加载跟踪机制的路由器，称为 ITrace 路由器，一个 ITrace 路由器以概率 p 发送对数据包的一个特殊形式的拷贝，该拷贝是一种经过特殊定义的 ICMP 数据包，其中包含发送它的路由器的 IP 地址、上游和下游路由器的 IP 地址及诱发数据包的信息。路由器向源或目的地址都转发该 ICMP 数据包。这种算法可以发现分布式反射拒绝服务攻击的攻击源，因为 ITrace 数据包以一定的概率同时也发往源 IP 地址。ITrace 算法不需要上游路由器地图，因为路由器地址被编码在了 ITrace 数据包中。由于主机一般都可以发送 ICMP 包，这种算法在 LAN 中使用时可以指定一些主机代替路由器来完成。

这种算法存在以下不足：①由于产生 ITrace 数据包的概率不高，所以该算法需要的攻击数据包很多；

②攻击者可伪造 ICMP 包，反向追踪包可能丢失。

5.3 数据包记录

数据包记录[21]通过边界路由器以一定的规则记录所有与它们邻接的链路上的数据包，这些规则可以包括源地址、目的地址、以及近似的数据包数量等信息。这些数据保留在路由器中，可以在攻击发生的同时，或攻击发生之后，由被攻击者根据提取出的攻击数据包的共有特征，与这些保存在各级路由器中的信息进行比较，从而一级一级的恢复出攻击路径。虽然这种办法可以用于对攻击后的数据进行追踪，它也有很明显的不足，它会占用边界路由器大量的系统资源，并且存在大量数据的挖掘问题。

5.4 随机数据包标记追踪[22]

Burch 和 Cheswick 提及了通过标志数据包来追踪 DDoS 攻击的可能性，通过在路由器处标记数据包来重构攻击路径。这种办法很多潜在的优点：①不需要 ISP 的支持，因此没有输入调试那么大的管理量；②相对于控制淹没而言，不需要额外大的网络流量，并且可以用来追踪多攻击源；③跟数据包记录一样，具有在攻击事件后进行路由发现的能力；④数据包标志机制不需要路由器太多的消耗。

所有的标记算法都可以分成以下两部分：①标记过程。由网络上的路由器完成，主要是对数据包进行信息附加；②路径重构过程。由被攻击者完成，实现对候选攻击路由的重构，路由器以数据包经过的路径信息来标记一个或多个数据包。被攻击者使用被标记的数据包中的这些信息来重构攻击路由。常见的标记算法有：节点附加、节点采样和边缘采样。

5.4.1 节点附加

该算法的原理就是针对每一个经过路由器的数据包，该节点在其末尾附加上它自己的地址。这种算法的优点健壮性好，攻击者无法阻止被攻击者发现攻击路径，重构攻击路径只需单独一个数据包。其不足之处在于要向每个数据包中添加数据，使得路由器的负载过高，并可能导致包分片，与 MTU 发现技术不兼容等。

算法描述：

(1)在路由器 R(设其 IP 为 R_{IP})上的标记过程:对每一个攻击数据包 W，附加 R_{IP} 给 W；

(2)在被攻击者 V 处的路径重构过程:对每个来自攻击者的包 W，从 W 的后缀重构攻击路径 $(R_1,\ldots,R_i,\ldots,R_j)$。

5.4.2 节点采样

该算法需要在数据包首部保留一个节点域(Node)以存放 IP 地址。当节点接收到一个数据包时，它以概率 p 在该域写入自己的 IP 地址，一个这样被标记的数据包称为该节点的一个样本。如果攻击数据包足够多，就可以保证被攻击者对攻击路径上的每一个节点都可以接收到至少一个样本。被攻击者根据样本的数量将节点排序，在有了足够数量的样本后就可以重构正确的攻击路径。这种算法主要有两个问题：①会改变样本的地址域并导致校验和的重新计算；②需要在包首部占用一个域，且该算法接收上游远程节点样本的时间很长。

算法流程：

(1)路由器 R(设其 IP 为 R_{IP})上的标记过程：对每一个攻击数据包 W.设 x 为[0,1)区间的任意随机数，如果 $x<p$（p 为写入地址的概率），则将 R_{IP} 写入 W 的节点域。

(2)被攻击者 V 处的路径重构过程:①设 NodeTable 为一个结构数组，存放结构（Node, Count)，其中 Node 存放节点 IP，Count 存放计数值。②对于每一个攻击数据包 W，查看其 Node 域，如果在 NodeTable 中存在该 Node 域的值，就将其对应的 Count 域增一，否则在 NodeTable 中增加一项:(W.Node, 1)。③根据 Count 值对 NodeTable 中的元素进行排序，重构出攻击路径$(R_1,\ldots,R_i,\ldots,R_j)$。

算法类 C 语言描述：

(1)标记过程：

```
For each packet W from attacker do
{
x = Random（0,1）;
if x<p then
    Write R_IP into W;
 }
```

(2)路径重构过程:

```
Define NodeTable,Z tuples(Node, Count);
 For each packet W from attacker do
 {
 Z = Search(W.Node, NodeTable);
if  Z != NULL
      {Z.Count++;}
else
     {Insert(W.Node,1) into NodeTable;}
      }
Sort(NodeTable) by Count;
Extract path(R_1,...,R_i,..., R_j);
```

5.4.3 边缘采样

该算法需在数据包首部设置两个域:“开始”域(Start)和“结束”域(End)，以对树型路由图的边信息进行采样，并用一个距离域(Distance)记录从边到被攻击者的距离值，当数据包到达一个路由器时，路由器将其地址写入“开始”域并以概率 p 将距离域置零。如果距离域为零，该节点会将自己的地址放入结束域并增加距离域，这样一个采样数据包记录了一条边信息，即使路由器不在“开始”域中写入自己的地址，它也要对距离域做增加操作。被攻击者可以从接收的数据包的边信息中重构攻击路径，而且重构出的攻击路径以树形结构图的形式获得。该算法的不足之处为需要在包首部增加空间。

算法流程：

(1)路由器 R(设其 IP 为 R_{IP})上的标记过程：对每一个攻击数据包 W.设 x 为[0,1)区间的任意随机数，如果 x<p，则将 R_{IP} 写入 W.Start，在 W.Distance 中写入 0；否则，如果 W.Distance 等于 0，则将 R_{IP} 写入 W.End,并使 W.Distances 加一。

(2)被攻击者 V 处的路径重构过程：①假设 G 是一个以 V 为根的树，设 G 上的每一条边都是一个结构:(Start, End, Distance)，其中 Start 存放数据包 W 中的 Start 域值，End 存放数据包 W 中的 End 域值，Distance 中存放距离值；②对于每一个攻击数据包，如果 W.Distance 的值为 0，则把边(W.Start,V,0)插入到 G 中，否则，将边(W.Start ,W.End, W.Distance)插入到 G 中；③步骤②完成之后，考察 G 中的所有边(x, y, d)，如果 d 不等于 G 中 x 到 V 的距离，则将该边从 G 中删除。④获得的 G 就是重构的攻击路径。

算法类 C 语言描述：

(1)标志过程：

```
For each packet W from attacker do
{
x = Random（0,1）;
if x<p then
    {Write R_IP into W.Start and 0 into W.Distance;}
else
     if W.Distance = 0 then
         {Write R_IP into W.End;}
          Increment W.Distance;
 }
```

(2)路径重建过程：

```
Define G a tree with root V
Define edges in G tuples(Start,End,Distance)
For each packet W from attacker do
{
if W.Distance=0 then
```

```
    {Insert edge(W.Start,V,0) into G;}
else
    {Insert edge(W.Start,W.End,W.Distance) into G;}
 }
for x to V in G
{
   if d!=Distance then
        Remove edge(x,y,d);
 }
Extract path(R1,...,Ri,..., Rj) by enumerating acyclic paths in G;
```

6 DDoS攻击研究的方向

目前全球对DDoS攻击进行预警、检测和阻断的研究工作还没有突破性的进展。普遍认为，DDoS攻击已经成为Internet基本架构所带来的难以避免的缺陷之一。本文作者认为未来的DDoS研究主要有以下几个方向：①高速网络下DDoS攻击和防范的研究成为研究重点。现有系统大多能运行在多种主流的100M网络平台和操作系统平台上，但随着网络速度的提高，高速网络上研究DDoS攻击和防范成为重点；②分布式的防范策略将是防范DDoS攻击的研究热点。目前没有能准确预测DDoS攻击发生的有效方法，根据系统检测的方式可分为集中式检测和分布式检测，分布式的防范策略将是防范DDoS攻击的研究热点，其实现难点在于处理负载均衡问题；③基于网络的防范手段成为主流。目前基于DDoS攻击的防范基本上采用传统模式匹配方法，本文作者认为，采用分布式体系结构，充分利用网络环境中各节点提供的海量信息和数据，采用数据挖掘和异常检测的方法，通过对各节点之间的数据作关联分析，实现大规模网络环境下的有效预警是DDoS对抗技术研究的一个新方向；④DDoS工具的智能化和自动化。目前实行DDoS攻击还有很多步骤需要手工完成，未来的DDoS工具将入侵攻击一体化，更易操作，功能更完善，破坏性更大；⑤路由器和网关成为DDoS攻击的重点。目前专门针对路由器的DDoS攻击还没有成熟的产品出现，但DDoS攻击将会更多的针对路由器和网关的弱点进行，如何绕过防火墙和入侵检测系统等防御体系，如何反检测跟踪，都是未来DDoS攻击的研究方向。

7 结 束 语

DDoS攻击的检测与防御是一个长期的过程，这主要因为：①DDoS攻击的工具种类繁多，攻击者往往不需要掌握复杂技术，利用这些工具进行攻击就能够达到很好的效果；②DDoS攻击通常是分布式对单个或者多个目标进行大规模的协同攻击，这种攻击可以非常容易地发起，却难以被阻止或者追踪；③不能准确地预见新产生的拒绝服务攻击类型。所以，我们既要掌握当前DDoS攻击的实现机理，还要加强对未来DDoS攻击发展趋势的研究，真正作到防患于未然。

参 考 文 献

[1] D. Moore, G. Voelker, and S. Savage. *Inferring internet denial-of-service activity. In Usenix Security Symposium*, 2001.
[2] http://www.cert.org/tech_tips/denial_of_service.html.
[3] http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html.
[4] U. Grenander. *General Pattern Theory: a Mathematical Study of Regular Structures*. Clarendon Press, Oxford .1993.
[5] http://staff.washington.edu/dittrich/misc/trinoo.analysis.
[6] http://staff.washington.edu/dittrich/misc/tfn.analysis.
[7] http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.
[8] http://www.cert.org/incident_notes/IN-2000-05.html.

[9] S. Dietrich, N. Long, and D. Dittrich. *Analyzing Distributed Denial of Service Tools: The Shaft Case. In Proceedings of USENIX LISA XIV*, December 2000.
[10] CERT Advisory CA-1996-21. *TCP SYN flooding and IP spoofing attacks.* http://www.cert.org/advisories/CA-1996-21.html.
[11] *Distributed Reflection Denial of Service,*http://grc.com/dos/drdos.htm.
[12] V. Paxson. *An analysis of using reflectors for distributed denial-of-service attacks, ACM SIGCOMM Computer Communication Review*, v.31 n.3, July 2001.
[13] P. Ferguson, D. Senie, RFC 2267. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,* Cisco Systems Inc., BlazeNet Inc., January 1998.
[14] J. Ioannidis and S. M.Bellovin. *Implementing Pushback: Router-Based Defense Against DDoS Attacks. In Proceedings of the Network and Distributed System Security Symposium (NDSS),* February 2002.
[15] R. Stone. CenterTrack: *An IP Overlay Network for Tracking DoS Floods. In 9th Usenix Security Symposium,* August 2000.
[16] D. Song and A. Perrig. *Advanced and authenticated marking schemes for IP traceback. In IEEE Infocomm,* 2001.
[17] C. Snoeren. *Hash-based IP traceback, Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications,* p.3–14, August 2001, San Diego, California, United States.
[18] M. Adler. *Tradeoffs in probabilistic packet marking for IP traceback, Proceedings of the thiry-fourth annual ACM symposium on Theory of computing,* May 19–21, 2002, Montreal, Quebec, Canada.
[19] H. Burch and B. Cheswick. *Tracing anonymous packets to their approximate source. In Usenix LISA (New Orleans) Conference*, 313–322, 2000.
[20] S. M. Bellovin. *ICMP traceback messages.* In Work in Progress, Internet Draft draft-bellovin-itrace-00.txt, March 2000.
[21] G. Sager. *Security Fun with OCxmon and. cflowd,* a presentation. PICS, at the Internet2 Working Group meeting, November 1998.
[22] S. Savage , D. Wetherall , A. Karlin and T. Anderson. *Practical network support for IP traceback. Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication.* p.295–306. August 28-September 01, 2000. Stockholm, Sweden.

Research and Development of Distributed Denial of Service Attacks

Wen Weiping Qing Sihan Wang Yejun

Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China

Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China

Abstract Distributed Denial-of-Service (DDoS) attacks have become one of common and effective attacks method against network security today. In this paper we explore the mechanism of DDoS attacks and present the difficulty and key technology of DDoS defenses, then discuss hotpot issue of DDoS attacks, i.e. trackback of attack origin. The remaining problems and emerging trends in this area are also addressed in the end.

Keywords Distributed Denial-of-Service; attack; defense; trackback