孙知信 著

网络异常流量识别与监控技术研究

清华大学出版社

网络异常流量识别与监控技术研究

孙知信 著

清华大学出版社
北京

内 容 简 介

本书系统地阐述了路由器端异常流量的检测与防范技术。首先介绍了 DoS 和 DDoS 的原理，综述了目前 DDoS 异常流量的检测技术现状和最新的研究成果；在此基础上介绍了作者创新性地设计并实现的 5 种 DDoS 检测算法以及对算法进行的局部仿真测试。在理论研究的基础上，作者结合一个具体的研究项目将上述算法应用到具体的开发中，阐述了开发的系统的总体设计、详细设计及安装测试。

本书是作者多年从事科研项目研究的成果结晶，书中内容都来自具体的项目，有很好的工程基础，特色是学术与具体的工程应用相结合。本书可作为计算机网络与信息安全相关专业研究生及高年级本科生的教材，也可作为科研人员的参考书，同时可作为研究生、博士生及老师论文写作的参考书。

图书在版编目(CIP)数据

网络异常流量识别与监控技术研究/孙知信著. —北京：清华大学出版社，2010. 9
ISBN 978-7-302-22357-3

Ⅰ. ①网…　Ⅱ. ①孙…　Ⅲ. ①计算机网络－流量－监测－研究 ②计算机网络－流量－控制－研究　Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2010)第 059547 号

责任编辑：丁　岭　王冰飞
责任校对：时翠兰
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：14　**字　数**：337 千字
版　　次：2010 年 9 月第 1 版　　**印　　次**：2010 年 9 月第1 次印刷
印　　数：1～2000
定　　价：35.00 元

产品编号：031042-01

前　言

传统的网络安全技术侧重于企业用户网络的系统入侵检测、防病毒软件或防火墙，这类安全措施通常并不能减少运营商网络中的非正常流量。为了降低网络中的异常流量，减少或消除用户所遭受的分布式拒绝服务攻击(Distribution Denial of Service Attacks，DDoS)，运营商的网络与路由交换设备需要具备异常流量监控与拒绝服务能力。路由器中的异常流量监控与拒绝服务方法研究对于运营商向用户提供安全服务具有重要意义。运营商网络中的路由器应该能够对攻击用户的异常流量进行监控并做出反应，根据报文源地址、源端口信息和报文长度等信息的统计特征采用一定的干预规则，比如禁止某些端口的流量或者禁止来自某一端口地址的带宽，对这些非法流量进行抑制或者拒绝服务。

路由器面临的威胁有：(1)将路由器作为攻击平台，入侵者利用不安全的路由器作为生成对其他站点的扫描或侦察的平台，并作为发动 DoS 攻击的一块跳板。(2)尽管路由器在设计上可以传送大量的传输流，但是它常常不能处理传送给它的同样数量的传输流，入侵者利用这种特性攻击连接到网络上的路由器，而不是直接攻击网络上的系统。相比较而言，前者的难度要大一些。因而 DoS（拒绝服务）成为了对路由器发起攻击的主要手段，在大范围内带来服务器的可用性问题，从而对整个因特网造成严重影响。目前应用于路由器安全的主要技术有防火墙技术、VPN 技术、入侵检测和认证技术，这几种当前的主流安全技术在路由器中都得到了应用。此外，路由器特有的网络地址转换(NAT) 技术也能进一步提高因特网的安全性。但是，多种安全技术也有相互制约的方面。防火墙根据 IP 报头中信宿地址、信源地址以及其他一些信息决定是否让该数据包通过，而 NAT 改变了信源或信宿地址。现阶段，端到端的 IPSEC 无法在 NAT 转换路由器中实现。

鉴于目前的这种状况，本书系统地阐述了路由器端异常流量的检测与防范技术。本书首先介绍了 DoS 和 DDoS 的原理，综述了目前 DDoS 异常流量的检测技术现状和最新的研究成果。在此基础上介绍了作者创新性地设计并实现的 5 种 DDoS 检测算法以及对算法进行的局部仿真测试。在理论研究的基础上，作者结合一个具体的研究项目将上述算法应用到具体的开发中，阐述了开发的系统总体设计和详细设计及安装测试。最后，作者对全文进行了总结。全书共分 10 章，主要内容介绍如下。

第 1 章　阐述了 DDoS 攻击的概念及原理，总结了 DDoS 的基本特征，以及 DDoS 分析方法。

第 2 章　阐述了对 DDoS 检测与防御的相关技术，并分析国内外现有的研究成果以及 DDoS 攻击发展的新趋势。

第 3 章　提出了一种改进的 CUSUM(cumulative sum)算法，并在此基础上对核心路由器流量进行实时监控，检测网络流量异常。

第 4 章　提出了一种基于攻击流量特征聚类的特征提取算法 AFCAA(Anomaly Traffic Character Aggregation Algorithm)，给出一种过滤攻击流量的反应策，并用实验测试结果加以表明。

第5章 设计了一种基于聚集和协议分析的防御分布式拒绝服务攻击的模型APA-ANTI-DDoS(aggregate-based protocol analysis anti-DDoS)。

第6章 提出了一种基于源目的IP地址数据库的防范DDoS攻击策,并利用这一策略设计了源目的IP地址检测系统SDIM(Source and Destination IP Monitoring)进行仿真验证。

第7章 提出了一种异常流量检测方法——防抖动的M-MULTOPS(modified-multi-level tree for online packetstatistics)结构。

第8章 给出了路由器的面向聚集的多层次异常流量控制机制AMAT(Aggregates-Oriented Multi-Levels Anomaly Traffic Control Mechanism in Router)系统总体设计。

第9章 阐述了AMAT系统的详细设计。

第10章 阐述了AMAT系统的安装及测试。

本书可供从事计算机网络与安全应用和研究人员及大专院校的教师、研究生和高年级本科生使用,也可供有关工程技术人员参考。

本书是作者在南京邮电大学从事多年相关研究的基础上撰写的,并得到国家自然基金(项目号:60973140)、江苏省自然基金(项目号:BK2009425)、江苏省高校自然基金(项目号:08KJB520005)资助。由于路由器端DDoS攻击检测和防范技术是一个热门的研究领域,有许多问题尚待进一步研究,因此书中难免存在错误和不足之处,欢迎读者批评指正。作者的E-mail:sunzx@njupt.edu.cn。

最后,在本书出版之际,我要诚挚感谢张伟博士、宫婧硕士、唐益慰硕士、姜举良硕士、李清东硕士、陈松乐硕士、陈亚当硕士和高同硕士等,他们为本书的出版提供了很多有益的帮助。感谢我的学生唐益慰、姜举良、李清东,他们为本书中的算法和系统作出了重要的贡献。感谢我的爱人张娟和儿子孙翌博,他们给予了我无私的支持和帮助。另外,我也要感谢清华大学出版社的领导和编辑,没有他们的辛勤劳动,就没有本书的出版。

孙知信

2010年1月于南京邮电大学

目　录

第1章　DDoS攻击原理及特征

随着计算机和通信技术的发展，计算机网络技术得到广泛的应用，人们无论是在生活还是工作上都越来越离不开计算机网络。特别是20世纪90年代以后，因特网得到了长足的发展，电子商务、电子政务如火如荼地发展起来。计算机网络已经渗透到人们的生活、工作当中，同时也渗透到社会的各方面。网络在为人们提供便利、带来效益的同时，也使人们面临着信息安全方面的巨大挑战。网络安全事件对计算机网络造成了很大的破坏，同时也带来不可弥补的经济损失。网络安全越来越成为人们关注的焦点。

计算机网络具有扩展性、开放性等特点，这些特点也使得它容易受到攻击。网络安全的主要威胁有：

(1) 安全漏洞。安全漏洞包括操作系统漏洞、网络协议漏洞、数据库系统漏洞和硬件漏洞等。漏洞可能造成计算机资料的丢失或计算机不能正常使用，而且当这些漏洞被利用进行攻击时，往往造成信息的泄露。

(2) 操作人员的疏忽。例如操作人员的安全意识不强，配置不当，失误、误操作等。

(3) 黑客攻击。黑客攻击是计算机网络所面临的最大威胁。

根据网络攻击手段的类型，可以将网络攻击分为主动攻击和被动攻击。

(1) 主动攻击。主动攻击是指使用各种方法、手段对信息的有效性、安全性等进行破坏，包含攻击者访问他所需信息的故意行为。主动攻击包括拒绝服务攻击、信息篡改、资源使用和欺骗等攻击方法。

(2) 被动攻击。被动攻击是指不影响正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。它的目的主要是进行信息收集而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。

根据近年来已公布的网络攻击事件的分析，在这些攻击手段中，以分布式拒绝服务(DDoS)攻击的危害最大，最难防御。分布式拒绝服务攻击是人们恶意地对网络进行干扰，使服务受到一定的影响，严重的可以造成巨大的经济损失。2004年，DDoS攻击使DoubleClick Inc公司的广告服务系统陷入瘫痪。Yahoo、eBay、Amazon. com、E Trade、ZDnet、Buy. com、FBI和其他一些网站都遭受过DDoS攻击。这些年来，DDoS攻击的频率和方式都呈上升的趋势，并且出现了攻击强度更大的高分布式拒绝服务(HDDoS)攻击和反射式拒绝服务(DRDoS)攻击。Gibson研究团体认为，目前DDoS攻击将大幅度增加(据Gibson估计为每星期4000次)。从理论上讲，这将使因特网因为成百上千的DDoS攻击而减慢速度。

DDoS之所以这么流行，主要是它有几个特点：

(1) 破坏力强，一般的服务器都不能幸免于难或造成网络带宽的巨大浪费。

(2) 有很多现成的攻击工具可以使用，它使得攻击者并不需要很高深的黑客知识就可以轻而易举地发起一次DDoS攻击，而且攻击者还不容易被抓到。

DDoS攻击已经对因特网造成越来越大的干扰，但它却不易于防范，因为DDoS在网络层和传输层消耗服务器资源和带宽资源，而在这两个层面上很难去确认哪些流量是合法的，

哪些流量是恶意的，并且大多数的 DDoS 攻击都伪造源 IP 地址。

为了保证网络稳定和信息安全，全世界的网络安全人员都投入到了这场斗争中，也相继提出了许多不同的算法和技术，取得了一定的成果。但是，传统的网络安全技术侧重于企业用户网络的系统入侵检测、防病毒软件或防火墙，这类安全措施通常并不能减少网络中的非正常流量。为了降低网络中的异常流量，减少或消除用户所遭受的拒绝服务攻击，路由交换设备需要具备异常流量监控与拒绝服务能力。路由器中的异常流量监控与拒绝服务方法的研究对于向用户提供安全服务具有重要意义。

1.1 DDoS 的原理及其发展

1.1.1 DoS/DDoS 的概念

从网络攻击的各种方法和所产生的破坏情况来看，DoS(Denial of Service，拒绝服务)是一种很简单但又很有效的进攻方式[1]。主要是对网络服务有效性的一种破坏，使受害主机或网络不能及时接收并处理外界请求，或无法及时回应外界请求，从而不能提供给合法用户正常的服务，形成拒绝服务。DoS 攻击方式有很多种，最基本的 DoS 攻击就是使网络服务器在短时间内充斥大量要求回复的信息，迅速消耗网络带宽和系统资源，导致网络或系统不胜负荷而瘫痪或停止提供正常的网络服务。DoS 攻击是采用一对一的攻击方式，如图 1-1(a)所示，当攻击目标的 CPU 性能、内存容量、网络带宽等各项性能指标不高时，DoS 攻击的效果是明显的。

随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了，因为目标对恶意攻击包的“消化能力”加强了不少，例如攻击软件每秒钟可以发送 3000 个攻击包，但被攻击主机与网络带宽每秒钟可以处理 10 000 个攻击包，这样一来攻击就不会产生什么效果。这时 DDoS(Distributed Denial of Service，分布式拒绝服务)就应运而生了，它是基于 DoS 特殊形式的拒绝服务攻击，采用分布、协作的大规模攻击方式，利用很多傀儡机来发起进攻，以比从前更大的规模进攻受害者[1]，如图 1-1(b)所示。由于是多对一的不对称关系，因此很容易导致被攻击主机拒绝服务。

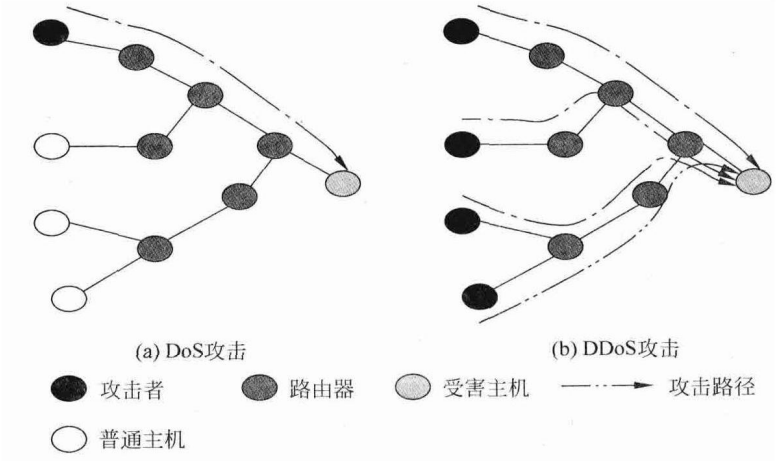

图 1-1 DoS 和 DDoS 攻击

DoS 攻击需要攻击者手工操作，而 DDoS 又把 DoS 向前发展了一大步。早期的 DDoS 攻击程序多半属于手动攻击，黑客手动寻找可入侵的计算机入侵并植入攻击程序，再下指令攻击目标；半自动的攻击程序则多半使用 handler 控制 agent 程序发起攻击，黑客首先在网络散布自动化入侵工具，并在入侵的主机植入 agent 程序，然后使用 handler 控制所有 agent 程序对目标发动 DDoS 攻击；自动攻击更进一步自动化整个攻击程序，将攻击的目标、时间和方式都事先写在攻击程序里，黑客散布攻击程序以后就会自动扫描可入侵的主机植入 agent 并在预定的时间对指定目标发起攻击，例如 W32/Blaster 网虫即属于此类。

1.1.2　DDoS 攻击原理

当前 DDoS 攻击越来越复杂，且攻击者能有效地隐藏自己。DDoS 攻击过程可分为以下几个步骤：

(1) 攻击者探测扫描大量主机以寻找可入侵的目标主机。

(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。

(5) 利用已入侵主机发动攻击。

如图 1-2 所示[2]，DDoS 攻击主要由 4 部分组成——攻击者、控制傀儡机、攻击傀儡机和受害主机。攻击者一般首先在 Internet 上探测扫描大量主机，侵占一些在标准网络服务程序和通用操作系统上存在安全漏洞的计算机，这些被侵占的计算机就成为了主控傀儡机和攻击傀儡机。主控傀儡机和攻击傀儡机的区别在于实际攻击包是从攻击傀儡机上发出的，主控傀儡机只发布命令而不参与实际的攻击。攻击者将 DDoS 程序传到这些平台上，这些程序与正常的程序一样运行并等待来自攻击者的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，一旦攻击者想要发动攻击，只需先登录到作为控制台的傀儡机，然后向所有的攻击傀儡机发出命令，这时候埋伏在攻击傀儡机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机以高速度发送大量的数据包，导致受害主机死机或是无法响应正常的请求。

攻击者有效地达到了隐藏自己实施攻击的目的，即使攻击傀儡机和控制傀儡机的 IP 地址被追查出来，它们也只是被攻击者控制的用户的 IP 地址，而它们本身也是受害者。

拒绝服务的攻击方式有很多种[3]，一般的 DDoS 攻击有两种基本类型——带宽攻击和应用攻击。带宽攻击是指在网络中发送大流量的数据包，消耗极大的网络资源，使得目标路由器、服务器和防火墙等设备疲于处理这些无效的数据，造成其性能的降低，甚至可能会最终崩溃。常见的带宽攻击形式是洪水攻击，这种攻击模式是将大量的 IP 包(TCP、UDP、ICMP 等)发往指定的目的地，直接将受害者淹没。应用攻击一般是利用系统的漏洞、协议的漏洞和服务的漏洞对计算机发动攻击，使计算机无法正常对外服务。

现将常见的拒绝服务攻击的方法归纳为以下几种：

(1) 利用传输协议上的缺陷发送出畸形的数据包，导致目标主机无法处理而拒绝服务；

(2) 利用主机上服务程序的漏洞发送特殊格式的数据，导致服务处理错误而拒绝服务；

(3) 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信；

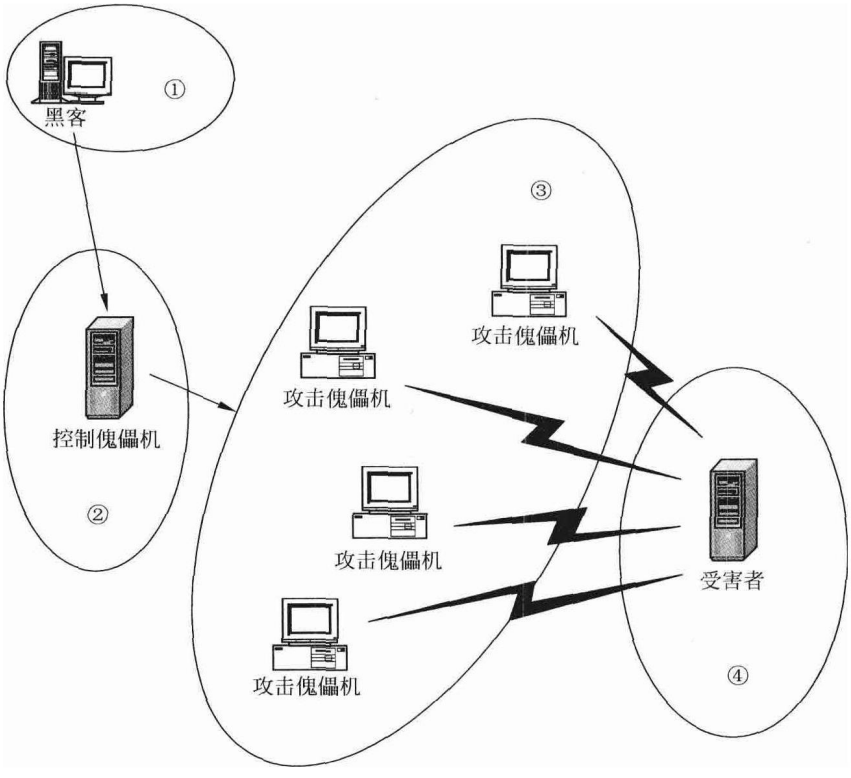

图 1-2 DDoS 攻击原理图

(4) 利用受害主机上服务的缺陷，提交大量的请求将主机的资源耗尽，使受害主机无法接受新的请求。

下面介绍几种常见的 DDoS 攻击实现原理。

1. SYN Flooding 攻击

SYN Flooding 攻击是最典型的利用协议漏洞的攻击，它是利用 TCP/IP 协议的漏洞完成攻击。基于 TCP 协议的主机在进行一次 TCP 连接之前需要进行三次“握手”的连接过程。在正常情况下[4]，请求通信的客户端要与服务器建立一个 TCP/IP 连接时，客户端需要先发一个 SYN 数据包向服务器提出连接请求。当服务器收到后，就回复一个 ACK/SYN 数据包确认/请求给客户端，然后客户端再次回应一个 ACK 数据包确认连接请求。一个完整的 TCP/IP 连接前必须经过这个三次“握手”的过程，如图 1-3 所示。

SYN Flooding 攻击就是利用三次握手的这个特性来发动攻击[4]。它的攻击原理就是攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，因此服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。使用随机伪造 IP 地址的 SYN Flooding 攻击原理如图 1-4 所示。

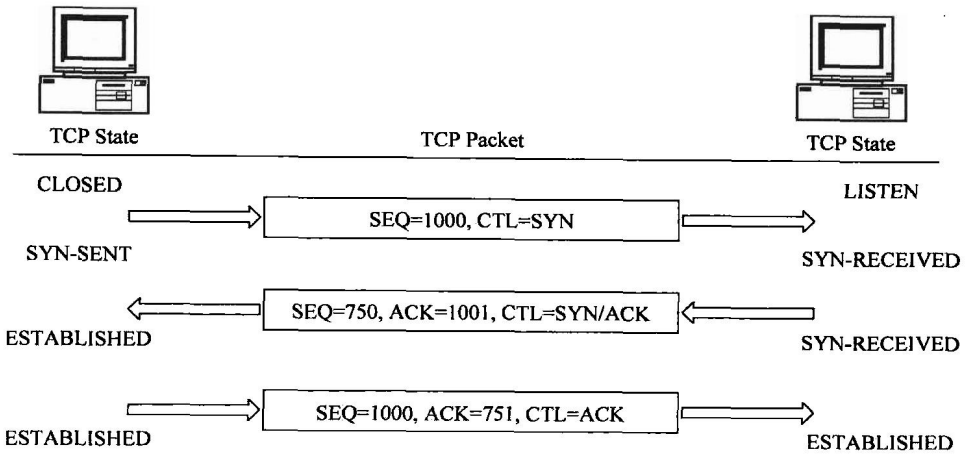

图 1-3　TCP/IP 连接三次“握手”过程

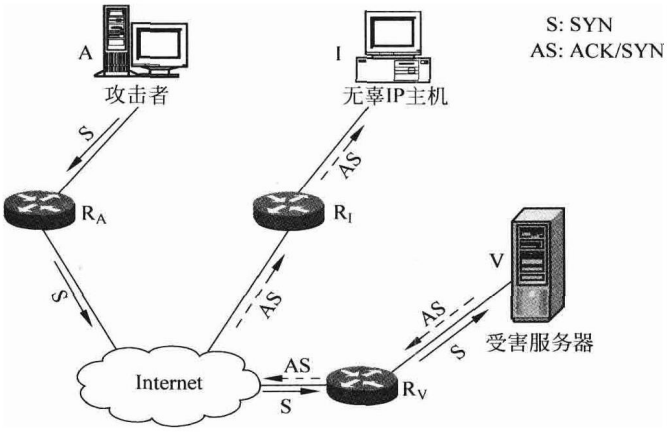

图 1-4　使用随机伪造 IP 的 TCP 三次“握手”过程

2. UDP Flooding 攻击

UDP Flooding 主要是利用主机能自动进行回复的服务(例如使用 UDP 协议的 chargen 服务和 echo 服务)进行攻击[5]。当向 echo 服务的端口发送一个数据时,echo 服务会将同样的数据返回给发送方。向 echo 服务发送一个字符 A,echo 也会返回给一个字符 A,而 chargen 则会随机返回字符。由于这两个服务的特性,当两个或两个以上系统存在这样的服务时,入侵者伪造其中一台主机向另一台主机的 echo 或 chargen 服务端口发送数据,echo 和 chargen 服务会对发送到服务端口的数据自动进行回复,这样开启 echo 和 chargen 服务的主机就会相互回复数据。由于这种做法使一方的输出成为另一方的输入,因此两台主机间会形成大量的 UDP 数据包。当多个系统之间互相产生 UDP 数据包时,最终将导致整个网络瘫痪。

3. Smurf 攻击

Smurf 攻击是以最初实现这种攻击方式的程序名 Smurf 来命名的[6]。利用 IP 欺骗和

ICMP 回复以引起目标主机网络阻塞而实现拒绝服务攻击。以太网中的网络接口都能接受的目的地址是本地硬件地址和广播地址的数据包，也就是说，发往广播地址的数据包会被网络中所有的主机接收并处理。Smurf 攻击就是利用这一点进行攻击的，发动攻击的主机向网络的广播地址发送 ICMP ECHO 包，并且把包的源地址设为目标主机的地址，这个包的目的是要求收到数据包的主机回复发送数据包的主机。由于发往广播地址的数据包会被网络上所有的主机收到并进行处理，因此所有收到这个包的主机就会向包中的源地址回复一个 ICMP 响应。如图 1-5 所示，入侵者的主机发送了一个数据包，而目标主机就收到了三个回复数据包。如果目标网络是一个很大的以太网，有 200 台主机，那么在这种情况下，入侵者每发送一个 ICMP 数据包，目标主机就会收到 200 个数据包，因此目标主机很快就会被大量的回复信息吞没，无法处理其他的任何网络传输。这种攻击不仅影响目标主机，还可能影响目标主机的整个网络系统。

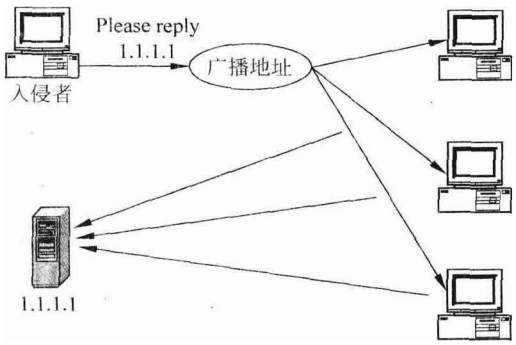

图 1-5 Smurf 攻击

1.2 DDoS 攻击的基本特征

DDoS 攻击包括 UDP Flooding、TCP Flooding、ICMP Flooding 和这些攻击的任意组合。文献[7]详细分析了 DDoS 攻击的特性，把 DDoS 攻击分为直接攻击(Direct Attack)和反射攻击(Reflector Attack)，如表 1-1 和表 1-2 所示。

表 1-1 直接攻击

协议	类型	特 性 1	特 性 2
TCP	SYN	大量 SYN 包流向被攻击机服务端口	被攻击机返回大量 SYN/ACK 包
	RST	大量 SYN 包流向被攻击机随机端口	被攻击机返回大量 RST 包
UDP	UDP	大量 UDP 包流向被攻击机随机端口	被攻击机返回大量 ICMP(DESTUR)包
ICMP	ECHO	大量 ECHORQ 包流向被攻击机	被攻击机返回大量 ECHORP 包
	MASK	大量 MASKRQ 包流向被攻击机	被攻击机返回大量 MASKRP 包
	TIME	大量 TIMERQ 包流向被攻击机	被攻击机返回大量 TIMERP 包
	INFO	大量 INFORQ 包流向被攻击机	被攻击机返回大量 INFORP 包

表 1-2　反射攻击

协议	类型	特　性　1	特　性　2
TCP	SYN	大量 SYN 包流向 Reflector 服务端口，源地址是被攻击机	大量 SYN/ACK 包流向被攻击机
	RST	大量 SYN 包流向 Reflector 随机端口，源地址是被攻击机	大量 RST 包流向被攻击机
	DNS	大量 DNS query 包流向被 DNS 服务器，源地址是被攻击机	大量 DNS reply 包流向被攻击机
UDP	UDP	大量 UDP 包流向 Reflector 随机端口，源地址是被攻击机	被攻击机返回大量 ICMP(DESTUR)包
	DNS	大量 DNS query 包流向被 DNS 服务器，源地址是被攻击机	大量 DNS reply 包流向被攻击机
ICMP	ECHO	大量 ECHORQ 包流向 Reflector，源地址是被攻击机	大量 ECHORP 包流向被攻击机
	MASK	大量 MASKRQ 包流向 Reflector，源地址是被攻击机	大量 MASKRP 包流向被攻击机
	TIME	大量 TIMERQ 包流向 Reflector，源地址是被攻击机	大量 TIMERP 包流向被攻击机
	INFO	大量 INFORQ 包流向 Reflector，源地址是被攻击机	大量 INFORP 包流向被攻击机
	Broad-cast	大量 ECHORQ 包流向 Reflector，源地址是被攻击机所在子网广播地址	大量 ECHORP 包流向被攻击机所在子网

比如，直接攻击 Trinoo 的攻击方法是向被攻击目标主机的随机端口发出全 0 的 4 字节 UDP 包，在处理这些超出其处理能力的垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，甚至崩溃。而 ICMP ECHO Flooding 攻击则是典型的反射攻击，攻击者伪造大量的 ICMP Request 数据包，使这些数据包的源地址为受害主机的地址，从而导致短时间内大量 ICMP ECHO 包回流向受害主机，堵塞受害主机的网络通信。

对 DDoS 直接攻击和间接攻击进行分析，可以得到下面 DDoS 攻击的基本特征：

(1) 攻击流量目的地址过于集中，且无拥塞控制特性。正常 TCP/IP 流量应该遵循拥塞控制规则，正常的网络应用程序应该是考虑到网络拥塞的，当发现网络通信质量很差时，正常的应用程序应该减少相互通信速率。这种拥塞控制规则可能由传输层实现，如 TCP 拥塞控制策略；也可能由应用层负责实现而传输层没有实现，比如 UDP 协议没有拥塞控制策略。DDoS 攻击流量不会考虑网络拥塞，致使攻击流量持续不断，出现网络拥塞后仍然大量发包。

(2) 流向目标机的 TCP/UDP 流量目的端口散度太大(端口太多)或者聚度太大(端口过于集中)。用随机端口攻击目标机，出现同时向目标机数千端口发送数据包；用固定端口攻击目标机，出现同时向目标机单一端口发送大量数据包。

(3) TCP Flooding/ICMP Flooding 时，流向目标机的某个标志位(TCP 是 SYN、RST、…，ICMP 是 ECHO、MASK、TIME、TIMEX、…)，包请求流量急速增长，堵塞目标机网络带宽。

(4) 被攻击机反馈大量特征流量。UDP Flooding 随机端口攻击时，被攻击机产生大量 ICMP 目的端口不可达包；ICMP ECHO REQUEST Flooding 攻击时，被攻击机产生大量 ICMP ECHO REPLY 包；TCP SYN Flooding 攻击时，被攻击机产生大量的 TCP SYN-