1. 引言

进入2000年以来，网络遭受攻击事件频频发生，全球许多著名网站如yahoo、cnn、buy.com、ebay、fbi等等，包括中国的新浪网也相继遭到不名身份的黑客攻击，值得注意的是，在这些攻击行为中，黑客摒弃了以往常常采用的更改主页这一对网站实际破坏性有限的做法，取而代之的是，在一定时间内，彻底使受攻击的网站丧失正常服务功能，这种攻击手法为 DDoS，即分布式拒绝服务攻击(Distributed denial of service)。

简单的讲，拒绝服务就是用超出被攻击目标处理能力的海量数据包消耗可用系统，带宽资源，致使网络服务瘫痪的一种攻击手段。在早期，拒绝服务攻击主要是针对处理能力比较弱的单机，如个人pc机，或是窄带宽连接的网站，对拥有高带宽连接，高性能设备的网站影响不大，但在99年底，伴随着DDoS的出现，这种高端网站高枕无忧的局面不复存在，与早期的DoS攻击由单台攻击主机发起，单兵作战相较，DDoS实现是借助数百，甚至数千台被植入攻击守护进程的攻击主机同时发起的团战行为，在这种几百，几千对一的较量中，网络服务提供商所面对的破坏力是空前巨大的。

分布式拒绝服务(DDoS)攻击是目前严重威胁网络安全和影响网站服务质量的一种攻击手段DDos攻击就是利用多个分布式攻击源向攻击对象发送超出攻击目标处理能力的海量数据包，来消耗可用系统和带宽资源，从而导致网络服务瘫痪的一种攻击

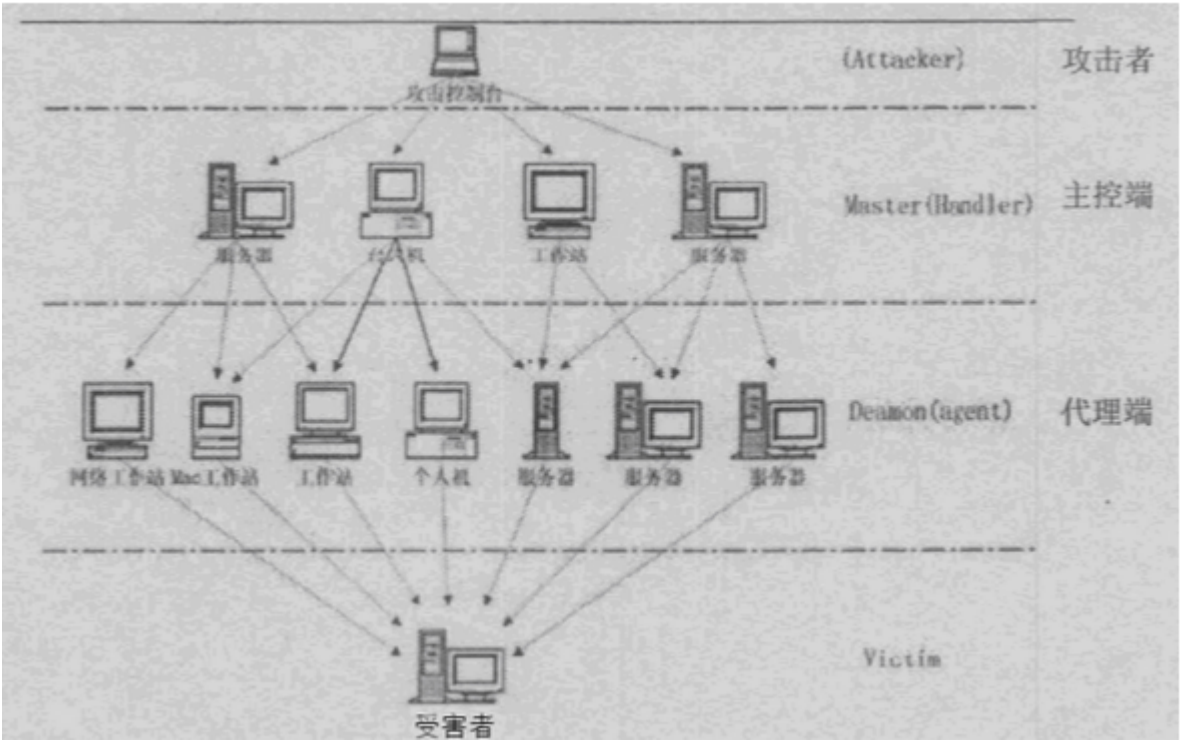
[1]目前有很多方法检测和防御DDoS攻击，传统的检测和防范措施是基于特征匹配的检测往往要求有一定的先验知识难以区分突发正常流量与DDoS 攻击

[2]至今没有一种有效的办法区分DDoS攻击流和正常的突发流，因此，检测和防御DDoS攻击仍旧是一个艰巨的课题。而区分DDoS攻击流和正常的突发流就成了问题的关键。

以上例子只是DDoS攻击的一个缩影，诸如此类的事件在网络或者电视、报纸上层出不穷。从DDoS攻击事件可以看出，即使是具有雄厚技术支持的高性能网站也逃不过DDoS攻击的厄运。由此可见，DDoS攻击已经对当今的因特网造成了巨大的威胁，如何及早检测出DDoS攻击，采用有效的防御成为网络安全研究领域的重点和热点。

2. DDoS攻击原理

DDoS攻击是一种基于DoS攻击的分布式、协作的大规模攻击方式，它直接或间接通过互联网上其他受控主机攻击目标系统或者网络资源的可用性。一般而言，DDoS攻击架构为三层:攻击者(Client)、主控端(Master)、代理端(Daemon)和被攻击者(Victim)，它利用受控主机向攻击目标发起攻击，具有威力更大、更难防御、更难追随的特征。DDoS攻击原理图如图2-1所示。



各层分工不同，具体如下：

攻击者：可以是网络上的任何一台主机，甚至是一台便携机。在整个攻击过程中，它是攻击主控台，负责向主控端发送攻击命令，控制整个过程。攻击者与主控端的通信一般不包括在DDoS工具中，可以通过多种连接方法完成，最常用的有“telnet”TCP终端会话，此外还有绑定到TCP端口的远程shell，基于UDP的客户/服务器远程shell等。

主控端：是攻击者非法侵入并控制的一些主机，它们分成了两个层次，分别运行非法植入的不同的攻击程序。每个主控端控制着大量的代理端，有其控制的代理端的地址列表，它通过监听端口，接收攻击者的命令，然后将命令转发给代理端。主控端与代理端的通信根据DDoS工具的不同而有所不同。比如：Trinoo使用UDP协议，TFN使ICMP协议通过ICMP_ECHOREPLY数据包完成通信,Stacheldraht使用TCP和ICMP协议进行通讯等。

代理端：在其上运行攻击程序，监听端口接收和运行主控端发来的命令，是真正进行攻击的机器。

被攻击者：可以是路由器、交换机、主机等网络设备。遭受攻击时，它们的资源或带宽被耗尽。防火墙、路由器的阻塞还可能导致恶性循环，加重网络阻塞情况。

3. DDoS攻击检测模型与防御的研究现状及常用方法

3.1 研究现状

一般而言，DDoS攻击实施过程可以分为三个阶段

(1) 收集目标主机信息。

通常，攻击者的攻击并非盲目进行的，他需要了解目标主机许多的信息，如被攻击目标主机数目、配置、性能、操作系统、地址情况以及目标网络带宽等。因此，在攻击发生前，攻击者需要先对目标进行侦查，如利用扫描攻击对攻击目标进行扫描。

(2) 占领主控机和代理主

攻击者首先利用扫描器或其它工具选择网上一台或多台代理主机用于执行攻击行动。为了避免目标网络对攻击的有效响应和攻击被跟踪检测，代理主机通常应位于攻击目标网络和发动攻击网络域以外。代理主机必须具有一定脆弱性以方便攻击者能够占领和控制，且需具备足够资源用于发动强大攻击数据流。代理主机一般应具备以下条件：

① 链路状态较好和网络性能好；② 系统性能好；③ 安全管理水平差。

攻击者侵入代理主机后，选择一台或多台作为主控主机，并在其中植入特定程序，用于接受和传达来自攻击者的攻击指令。其余代理主机被攻击者植入攻击程序．用于发动攻击。攻击者通过重命名和隐藏等多项技术保护主控机和代理主机上的程序的安全和隐秘。被占领的代理主机通过主控主机向攻击者汇报有关信息。

(3) 攻击的实施

攻击者通过攻击主机发布攻击命令，主控主机接收到命令后立即向代理主机传达，隐蔽在代理主机上的攻击程序响应攻击命令，产生大量UDP、TCP SYN和 ICMP响应请求等垃圾数据包，瞬间涌向目标主机并将其淹没。最终导致出现目标主机崩溃或无法响应请求等状况。在攻击过程中，攻击者通常根据主控主机及其与代理主机的通信情况改变攻击目标、持续时间等,分组、分头、通信信道等都有可能在攻击过程中被改变。

通过上述讲解后，我们已经了解了DDoS攻击的基本原理，那么DDoS攻击的特性可以概述如下

第一： DDoS的攻击者的分布式特性：DDoS攻击处于不同区域的多个攻击者同时向一个或数个目标发送攻击，或者一个或多个攻击者控制了位于不同区域的多台傀儡机并利用这些傀儡机对目标主机同时实施攻击。由于DDoS攻击采用分布式协作方式，使其难于防御和跟踪，同时，资源、目标和中间域之间缺乏协作也不能对攻击做出快速、有效和分布式的响应。

第二： DDoS攻击流的不易识别特性：DDoS攻击流和网络中通讯的正常数据流十分相似，都符合网络协议并且能够通过Internet网络中的路由选择，两者难以区分。此外，数据包、数据包头、通信信道等都有可能在攻击过程中改变，导致DDoS攻击流不存在能用于检测和过滤的共同特性。因此，在受害者端对DDoS攻击防范是极为困难的。这使得攻击者和受害者之间的力量极为悬殊，而攻击者总是处在极有利的地位。

第三： DDoS攻击是洪泛攻击：即使Victim可以从众多接收数据包中识别出DDoS攻击数据包，它也无力抵御大规模的洪泛攻击，巨大的攻击数据流使得Victim无法为合法用户提供服务，攻击者从而达到了使Victim服务质量降低甚至崩溃的目的。

DDoS攻击具有很强的隐蔽性：攻击者为了隐藏自己的身份、躲避追踪，通常都会伪造