大规模DDos攻击趋势的调查和基于云的缓解

作者：FuiFui Wong Cheng Xiang Tan

同济大学，中国上海，计算机科学与技术专业

摘要

分布式拒绝服务攻击如今已经被宽带互联网介入扩大为千兆位数量；同时，实施在小或大规模网络和服务中的更有力的僵尸网络、常见的DDos缓解策略和解决办法都不再有效。我们的调查提供了一个运用超过300Gbps如今最大规模的DNS响应攻击Spamhaus.org的深度研究。我们回顾并研究了当前最广泛的由黑客发起的DDos攻击类型。最后，我们两人一起提出了有效的基于云的DDos缓解和保护技术，并讨论了大型商业云端DDoS服务提供商。

关键字

Dos，DDDos，DNS响应或放大攻击，SYN泛洪，UDP泛洪，ICMP泛洪，HTTP泛洪攻击

1. 介绍

在2013年4月，Seamhaus.org遭遇了记录以来最大规模的分布式拒绝服务攻击，大概的规模超过了300Gbps。CloudFlare采用基于云的DDoS保护解决方案致力于缓解这种攻击。根据Prolexic的《Q1 2013 Global DDoS Attack》报告，如今多于10%的大型DDos攻击超过了60Gbps，多余75%的攻击是针对基础设施的（第三四层），限制带宽容量和路由基础设施，剩下的攻击是针对应用层的。

在一次DDos攻击中，攻击者试图暂时的中止或延迟一个网页的服务，使之对用户不可用。Akamai的2012年第四季度互联网状况报告中陈述了2012年总数768次DDos攻击。超过三分之一（269或35%）的攻击针对商业领域的公司，164（22%）次的攻击针对媒体或者娱乐公司，155次（20%）的攻击针对包含金融服务的企业公司，110次（14%）的攻击针对高科技公司，70次（9%）的攻击针对公共部门机构。这些攻击对这些目标公司在资金，客户满意度和声誉等方面造成了不同程度的损失。

这篇论文目的是提供一个对当前最广泛应用的大量DDos攻击类型完整的更新并讨论多种有效的基于云的DDos缓解策略和保护技术。在论文的第二个部分，我们首先详细研究Spamhaus当前最大规模的DDoS攻击。然后我们在第三部分讨论当前最广泛应用的针对基础设施（第三四层）和应用层的攻击类型。第四部分讨论了多种有效的基于云的DDos缓解策略和保护技术，最后，我们在第五部分提出了自己的结论。

1. 对Spamhaus历史的DDos攻击

在2013年3月18，Spamhaus的一个在线提供反垃圾邮件过滤服务的网站Seamhaus.org，被超过100Gbps的大量DDos攻击了，这次攻击非常巨大，互联网连接饱和，用户无法进入该网站。这次攻击被分类为第三层攻击，并且很难用软件来解决，因为接入的请求远远大于路由器能处理的通信数量，导致路由器饱和。那时，攻击者的身份也是未知的。

这些第三层攻击来源非常广并且是分布式的，信息来源发送流量以淹没目标互联网位置。一群一起工作的个人，一个盗用PC形成的僵尸网络，一个盗用客户端形成的僵尸网络，配置错误的DNS解析器，甚至是一个弱口令的家用网络路由器都可能成为攻击阻塞通信的来源。

像IP过滤这样的DDoS防御机制将不再有效，因为针对第三层攻击是通过发送包含欺骗信息和来源IP的随机数据包启动的，接受到的回应都会被忽略。CloudFlare是一家提供基于云的DDoS保护解决方案的公司，由Spamhaus聘请来减轻攻击，该网站在几小时内就完成了工作。

* 1. 针对Spamhaus网站75Gbps的DDoS攻击的生成

自从2012年开始，DNS反射攻击已成为第3层DDoS攻击的主要来源，Spamhaus最大的攻击流量就来自于DNS反射。

Spamhaus的攻击者首先从开放的解析器请求指向ripe.net的DNS区域文件，分配给Spamhaus的CloudFlare IPs在其DNS请求中被攻击者欺骗。DNS区域文件通过打开解析器来响应，由于36字节的响应被放大到3000字节，导致这些解析器生成了大约75 Gbps的攻击流量。

3000个不同的DNS解析器都参与到了Spamhaus的攻击之中。每一个开放的DNS解析器发送2.5Mbps的DNS区域文件，大部分解析器都允许这样的操作。然后，攻击者仅使用DNS放大并控制僵尸网络或服务器群集来生成750

Mbps DNS区域文件。

* 1. 针对Spamhaus网站75Gbps的DDoS攻击的减轻

CloudFlare使用Anycast来减轻对Spamhaus的75Gbps攻击。Anycast将对Spamhaus的攻击分散到CloudFlare的23个全球数据中心。每个数据中心都使用与Spamhaus相同的IP地址，这导致流量无法定位到某一个地点。这种方法 把多对一的攻击转换为多对多的攻击，这样就不能在网络中的某一个单独节点造成瓶颈。在攻击被分散后，在抵达Spamhaus服务器之前，针对第三层的攻击就被每一个CloudFlare的数据中心停止了。

1. 当前大规模DDoS攻击类型的上升趋势

开放系统互连（OSI）模型将通信系统划分为七个逻辑层。每一层都有独特的安全挑战，容易受到拒绝服务攻击（Dos）与分布式拒绝服务攻击（DDos）。近两年分布式拒绝服务攻击呈上升趋势，主要分为两种主要攻击：基础设施攻击（第3,4层）和应用攻击（第7层）。第一类基础设施攻击，它试图通过发送大量虚假请求信息来压倒带宽容量和路由基础设施。第二类应用攻击利用特定应用程序的限制来导致性能下降或最终导致远程服务器崩溃。

3.1基础设施攻击（第3,4层）

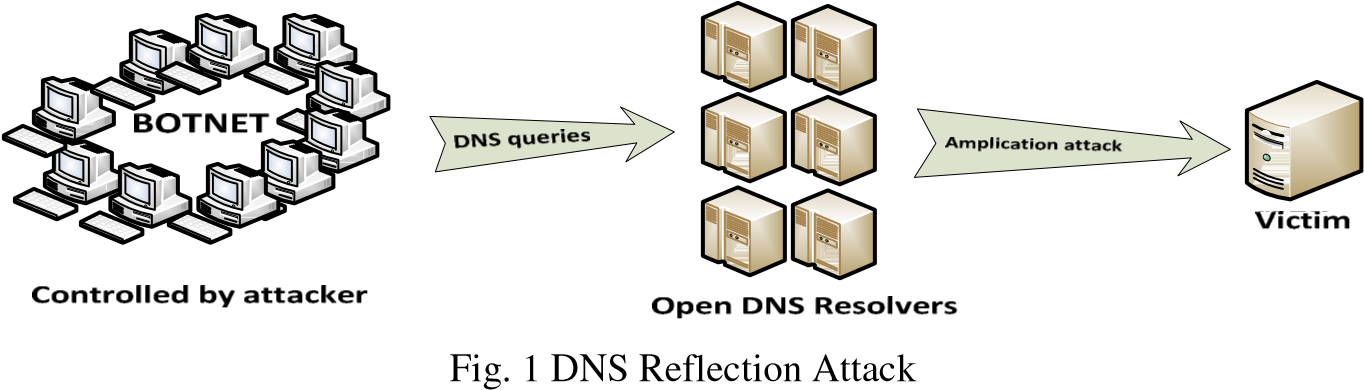
本节描述OSI模型中第三层网络层和第四层传输层上当前最流行的DDos攻击类型，如下：

* DNS反射攻击
* TCP、SYN泛洪
* UDP泛洪
* ICMP泛洪

基于由成熟领先工业在安全报告上发布的统计记录，这些攻击类型是恶意行为者的主要关注点，将在全球威胁格局中占据首位。

* + 1. 域名服务器（DNS）的反射或放大攻击

DNS反射或放大攻击是一种分布式拒绝攻击，攻击者将DNS名称查找请求发送给一个开放的DNS解析器，源地址被欺骗为受害者地址。当DNS服务器发送DNS记录响应时，它被发送到受害者（被欺骗时使用的源地址）。由于响应的大小通常要比请求大得多，因此攻击者可以放大针对受害者的流量。通过利用僵尸网络来执行额外的DNS欺骗查询，攻击者只需要很少的努力就可以产生大量的流量，如图一所示，因为响应是来自有效服务器的合法数据，所以阻止这些类型的攻击非常困难。

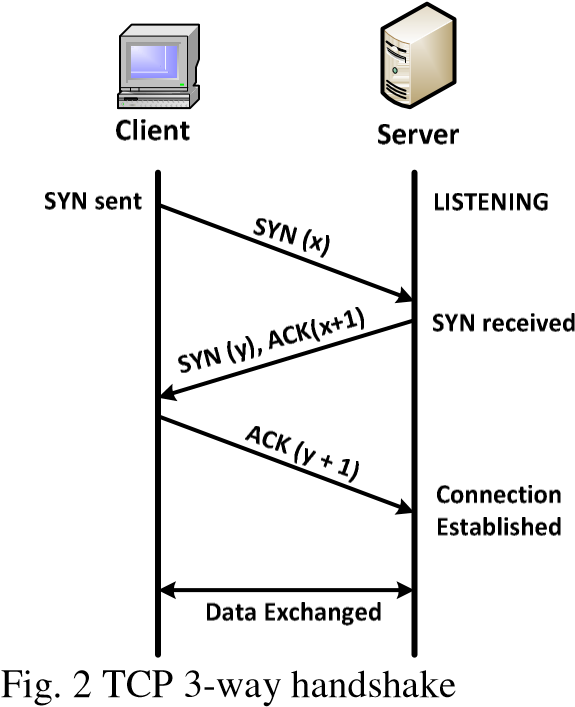


DNS反射攻击可以通过以下方法实现：

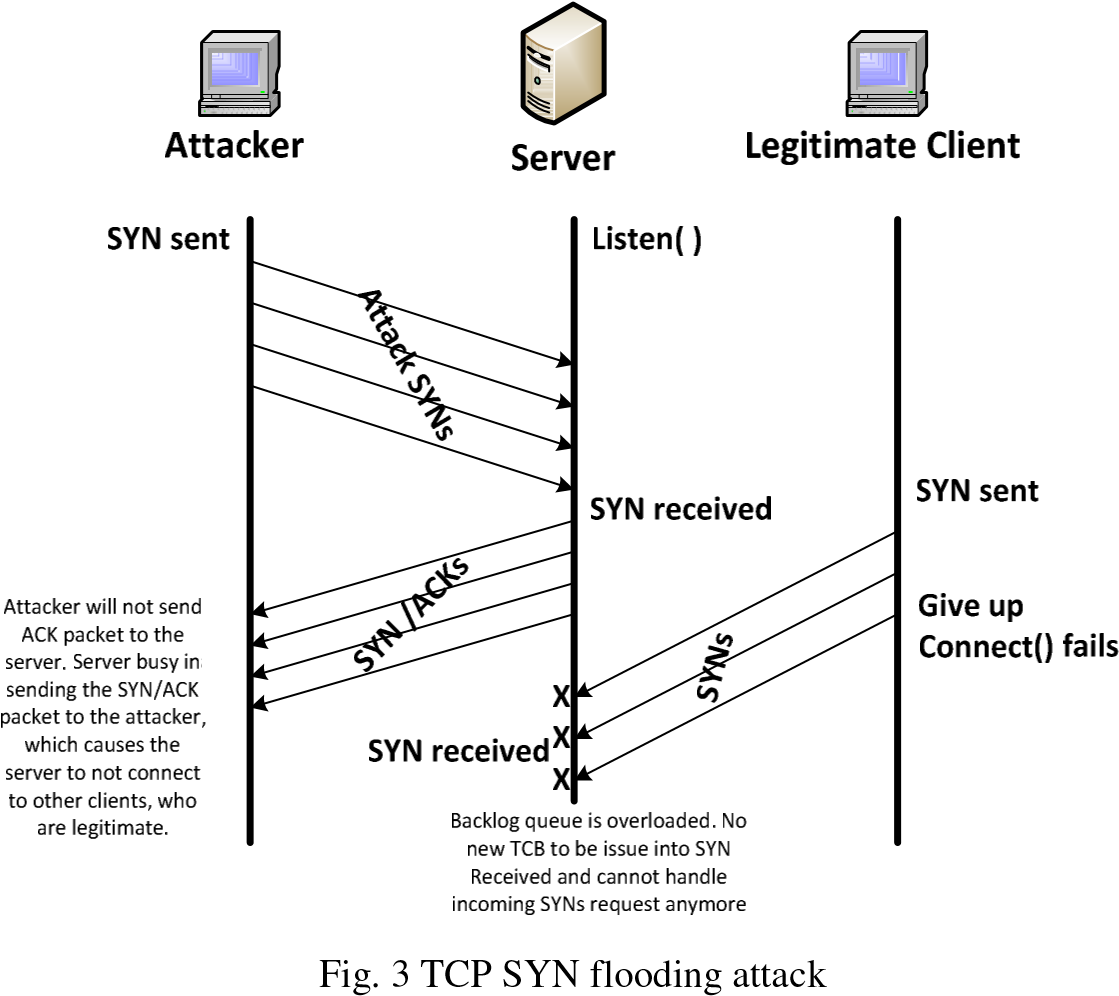
开放的递归。

* + 1. TCP、SYN泛洪

SYN泛洪攻击的工作原理是设计一个三向握手开始TCP连接。在此握手中， 如图2所示，客户机系统首先向服务器发送一条SYN消息。 然后，服务器通过向客户机发送同步ack消息来确认SYN消息。然后客户端通过响应ACK消 息来完成连接的建立。然后打开客户机和服务器之间的连接，可以在客户机和服务器之间交换特定于服务的数据。当服务器系统向客户机发送了一个确认(synack),但尚未收到ACK消息时，就可能出现滥用。

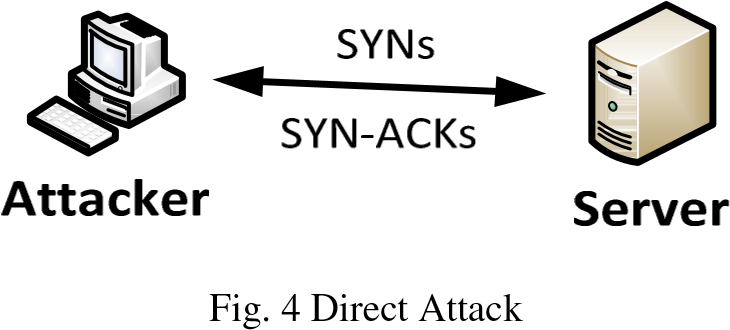


传输控制块(TCB)是一种传输协议数据结构， 用于保存连接上的所有信息。在从客户机接收ACK消息之前，服务器接收了SYN包之后，该连接仅处于半开状态。这种情况会导致服务器的内核内存被传入的syn耗尽，这会创建太多TCB分配。然而操作系统通常会使用一个与一个监听套接字”积压参数,以避免该内存耗尽但消耗积压TCPSYN洪水攻击的目标，它试图发送SYN片段足以填满整个积压因此导致服务被拒绝到新连接请求。下面的图3对TCP SYN泛洪攻击中涉及的事件序列进行了简化。

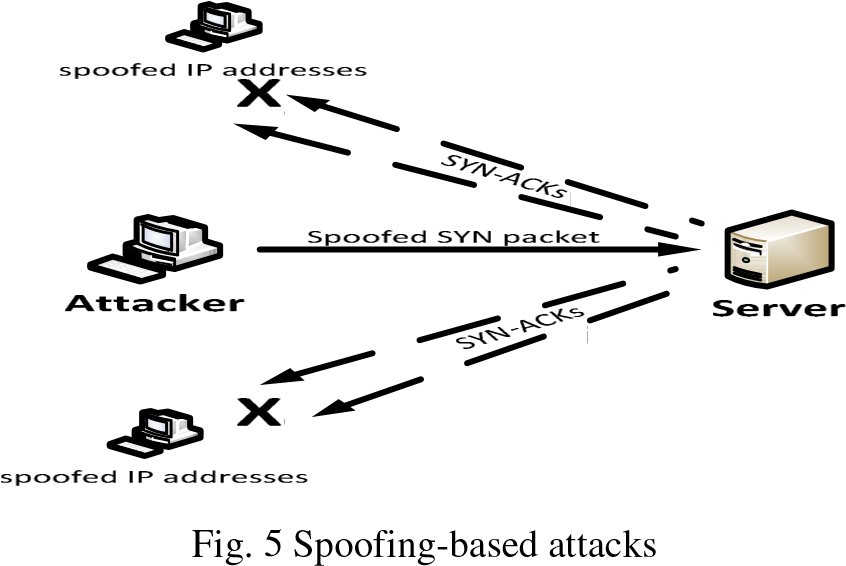


目前，在互联网上发现的TCP SYN泛洪攻击有3种变体:

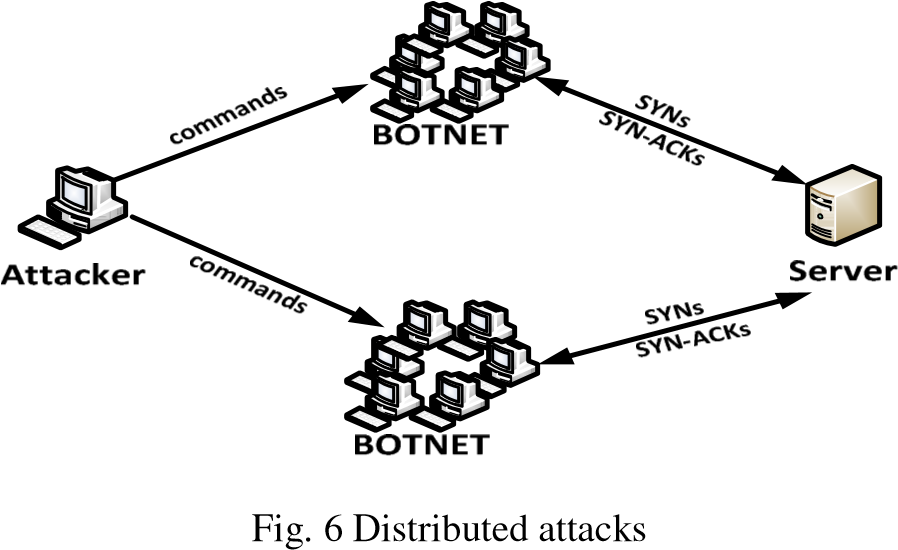
1.直接攻击。直接攻击是攻击者在不欺骗IP源地址的情况下发送许多SYN段，并且阻止操作系统对同步做出响应。这个场景可以通过防火墙规则来实现，防火墙规则可以将传出的包过滤到侦听器(只允许SYNS out)， 也可以过滤传入的包，以便在到达本地TCP处理代码之前丢弃任何语法，如图4所示。



2.Spoofing Based攻击。SYN洪水 攻击[12]使用P地址欺骗欺骗客户端系统源地址在哪里不应对SYN-ACKS发送给他们，因为不存在客户端系统的地址目前还是因为假设一些比例的伪造地址不会响应 如图5所示。



3.分布式的攻击。分布ITSYN泛洪攻击是指攻击者利用Internet 上的许多无人机机器或僵尸网络，每个可变无人机使用一个欺骗攻击和多 个欺骗地址，使得攻击更难被阻止或停止，如图6所示。

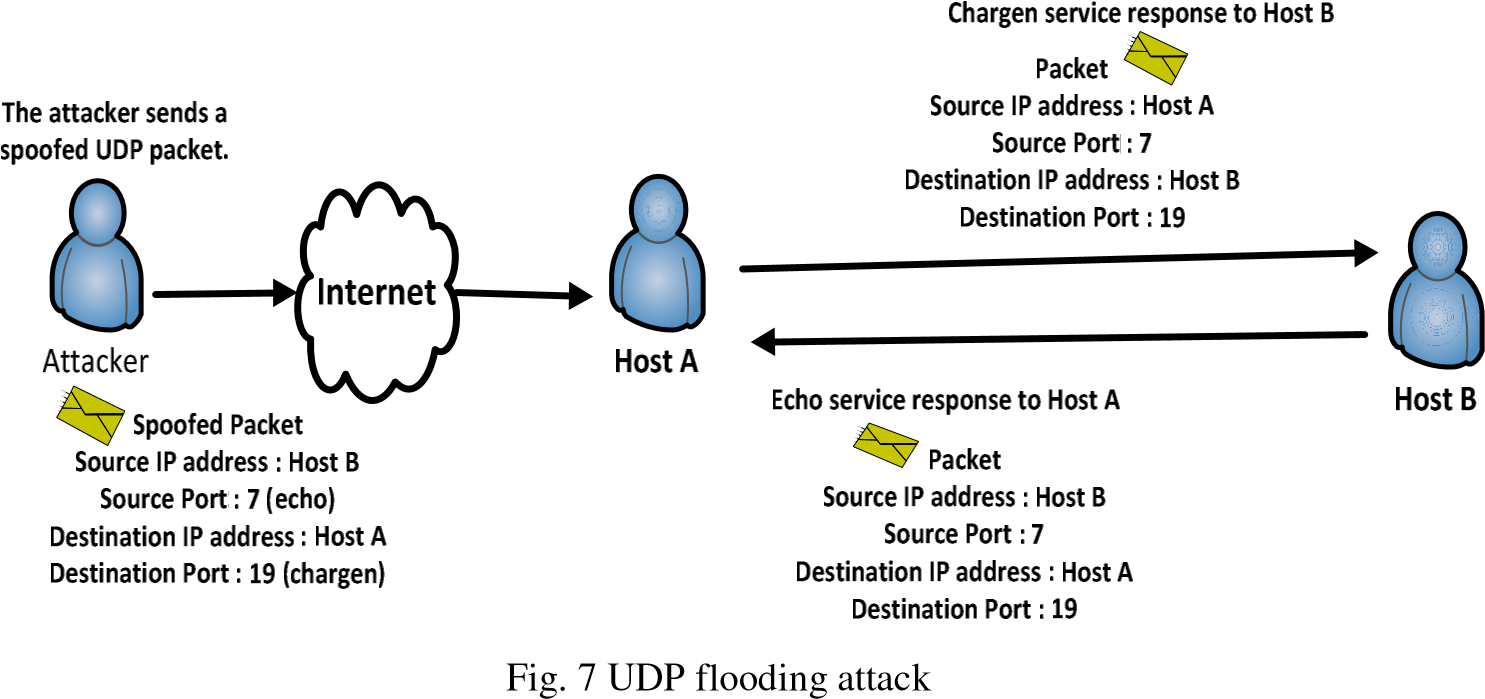


* + 1. UDP泛洪

UDP泛洪是一种使用用户数据报协议(UDP)的带宽攻击类型。UDP是一 种无状态的传输协议，它不需要客户端和服务器具有已建立的会话，并且在传输信息时强调最小化延迟而不是可靠性。UDP洪水攻击可以通过向受害 者系统上的随机端口生成大量UDP数据包来启动。受害系统将确定哪个应用程字正在目标端口上等待对传入UDP包的响应。当实现这些服务的受害 者系统响应时，如果没有应用程序在端口上等待，它将用IMCP不可到达的消息响应每个UDP包。在这种情况下，恶意的UDP发送方将IP源地址伪造为受害者的地址，从而使受害者的系统受到多个UDP流量响应程序的重载。这种类型的攻击最 常利用的弱点"chargen”和“回声服务如图7所示，有用的DoS攻击(例如,一个源端口的UDP数据包是由回波的目标主机B和目的地港口目标主机的chargen) [13]。 chargen服务将继续生成一 些随机字符并将它们发送回明显的源，而echo服务将继续响应包， 将随机字符返回到chargen。攻击者可以通过管道将chargen的输出发送到echo,从而导致网络活动的无限终止流。这个场景 在两个UDP服务之间创建了一个无限循环， 其中主机B将向主机a回送一个包。 主机a然后响应主机B的回送端口，直到耗尽一些共享资源(例如缓冲区、链接、容量)[14]。

因为UDP是一个不可靠的协议， 不规范它的发送通信量，这个场景很容易让恶意UDP发送者伪造IP源地址成为受害者。

由于很容易从许多不同的脚本和编译语言15]生成UPD包，大多数UDP洪水常常用于带宽大于1gbps的DDOS攻击。

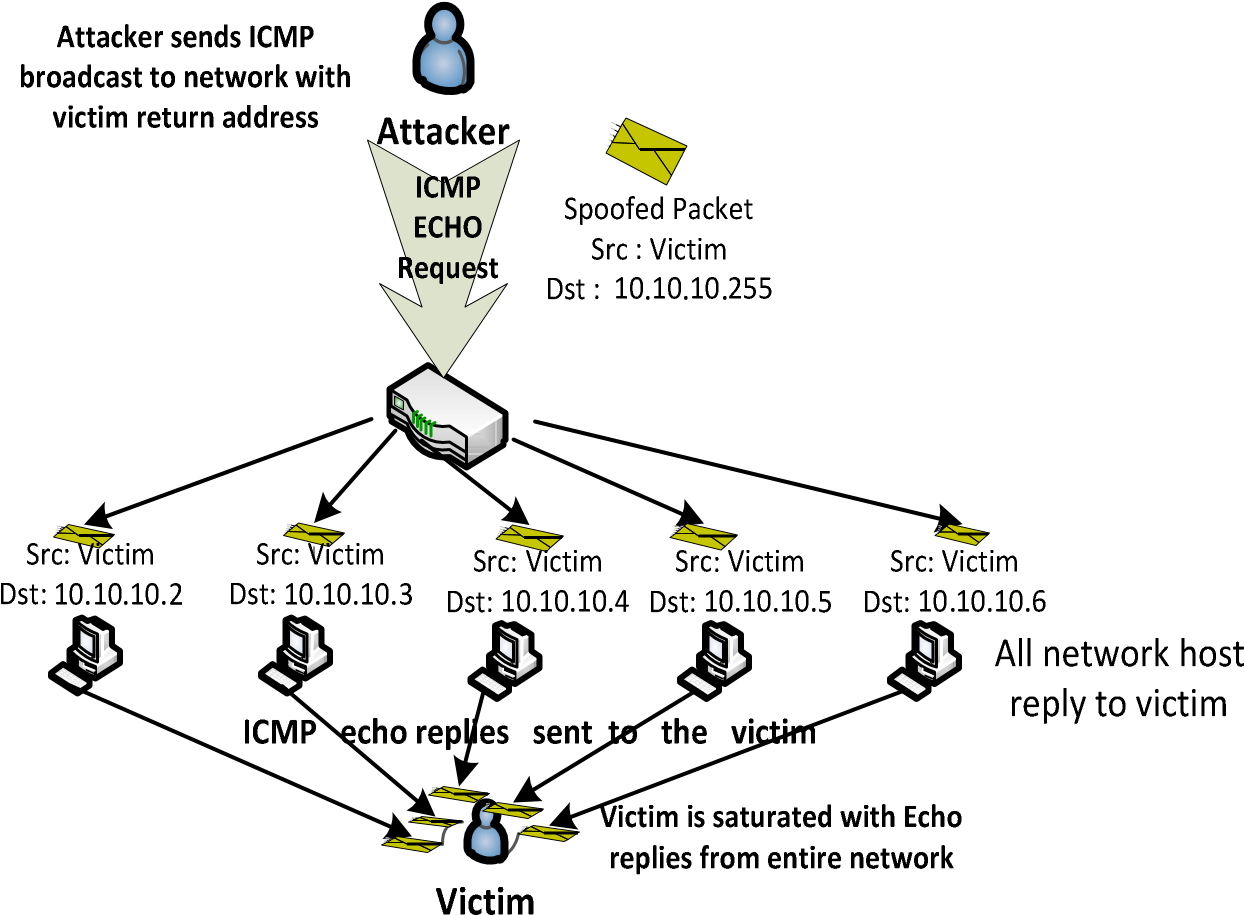


* + 1. ICMP泛洪

ICMP flood有时被称为"Smurf"攻击或"Ping"攻击，是一种基于Ping的DOS攻击，它将大量ICMP包发送到服务器，并试图崩溃服务器上的TCP/IP堆栈，使其停止响应传入的TCP/IP请求。

然后，使用安装在受损计算机上的hping或自定义per脚本启动ICMP泛洪。基本SYN洪水偶尔与ICMP洪水[2]-起发起。

SMURF攻击发生在攻击者将ICMP请求连同受害者的欺骗IP发送到路由器的网络广播地址时，该路由器被配置为将ICMP转发到路由器后面的所有设备。当所有这些设备都对ping作出响应时，攻击就会被放大，此时ICMP不包含握手，源IP也不会被验证。下面的图8给出了一个蓝精灵攻击[16]。有关蓝精灵攻击的详细描述，请参考[17]和[18]。



3.2 应用程序(第7层)攻击

应用层DDOS攻击在复杂性和普及性方面继续增长。研究公司高德纳(Gartner)在题为《武装金融和电子商务服务,抵御2013年最严重的网络威胁》(“ 武装金融和电子商务服务，抵御2013年最严重的网络威胁”)的报告中预测，2013年DDoS攻击中， 有25%将基于应用程序。应用层中的DDoS攻击试图 用web泛滥攻击特定的服务，例如，HTTP洪水攻击向服务器发送高速率的合法应用层请求，试图淹没服务器资源。这些攻击通常消耗更少的带宽，而且更难以识别，因为攻击者通过大量台法请求[20]攻击受害服务器。

3.2.1 常见应用层DDoS攻击类型

应用层攻击可以细分为四类[21[22]：

i) 当大量合法应用层请求(如HTTP get、DNS查询和SIP邀请 发送到服务器以压倒其会话资源时，就会发生请求泛滥攻击。

ii) 非对称攻击是指将消耗大量 服务器资源如CPU、内存或磁盘空间的正常请求发送到web服务器，其目的是严重削弱其服务或使服务器完全宕机。

iii) 当跨多个TCP会话的高工作负载请求发送到服务器时，会发生重复的一次性攻击，目的是降低或降低服务器的服务。这些攻击类似于执行请求泛洪攻击和非对称应用层攻击

iv) 应用程序漏洞攻击应用程序中的目标漏洞， 通过在服务器操作系统或应用程序中引起故障，允许攻击者控制应用程序系统或网络。脚本漏洞、 缓冲区溢出、cookie中毒、隐藏字段操作、 跨站点脚本和结构化查询语言(SQL)注入就是这些攻击[23]的例子。

3.2.2 HTTP泛洪攻击

根据Prolexic 2013年Q1 Global DDoS攻击报告，23. 46%的DDoS攻击来自application (layer 7)攻击，19 33%的DDOS攻击来自HTTP 请求泛洪，这是绝大多数的应用攻击。Http 发送泛洪是第二流行的应用程序攻击，它使攻击者能够向应用程序发布大量数据，占DDoS攻击总数的1 .43%。

有3种类型的HTTP泛洪可以启动，如下[21]：

i) 当无效的HTTP数据包发送到web服务器以耗尽服务器资源时，就会发HTTP格式错误攻击。这种攻击的一个例子是Zafi.B蠕虫,它使用了格式不正确的HTTP GET请求。

ii) 当不同类型的合法HTTP请求(即，HTTP get和post)被发送到web服务器，试图通过使用服务器资源[24]来淹没它们。

iii) HTTP空闲攻击发生在HTTP连接打开并处于空闲状态，而没有通过攻击实际发送完整的HTTP请求的情况下。这种攻击的一个例子是'slowloris"[25],它无限期地为每个包分配少童字节，以防止连接超时，但永远无法完成请求。

1. 当前和云一起使用的DDos缓解和保护技术

目前，在小型和大型组织的网络和服务器上实现的常见DDoS缓解和保护技术发现很难或不再可能减轻压倒性的千兆攻击。云计算具有地理分布的高带宽和高处理能力，是这些DDoS缓解和保护技术发挥作用的必要条件。

各大商业云服务提供商如Prolexic、CloudFlare、 Cisco、 Akamai、 Arbor等都在研究和使用各种有效的大规模DD0S缓解和保护技术，以缓解上述章节提到的攻击类型,具体讨论如下:

* 1. DNS反射或放大攻击

4.1.1 输入过滤。

输入过滤检查属于您的网络的所有输出数据包的IP地址的有效性,并在最佳通用实践文档(BCP-38)中完整地记录下来。DNS服务器反映了依赖于欺骗IP地址的流量，这些IP地址通过使用这种过滤被删除，而且很容易在路由器中实现，因为所有主要路由器供应商都有内置的方法来实现BCP-38[26]。

4.1.2 限制DNS递归

限制DNS递归[5]可以通过：

i) 配置您的服务器，以允许递归的授权DNS服务器列表

ii) 配置防火墙,以阻止不是来自您指定的内部递归DNS服务器的DNS查询。

iii) 将您的服务器配置为使用ISP的递归DNS服务器，然后只允许与这些服务器相关的DNS查询。

iv) 分割您的权威递归DNS服务器，使递归DNS只能从LAN内部访问，如下面的图9所示。

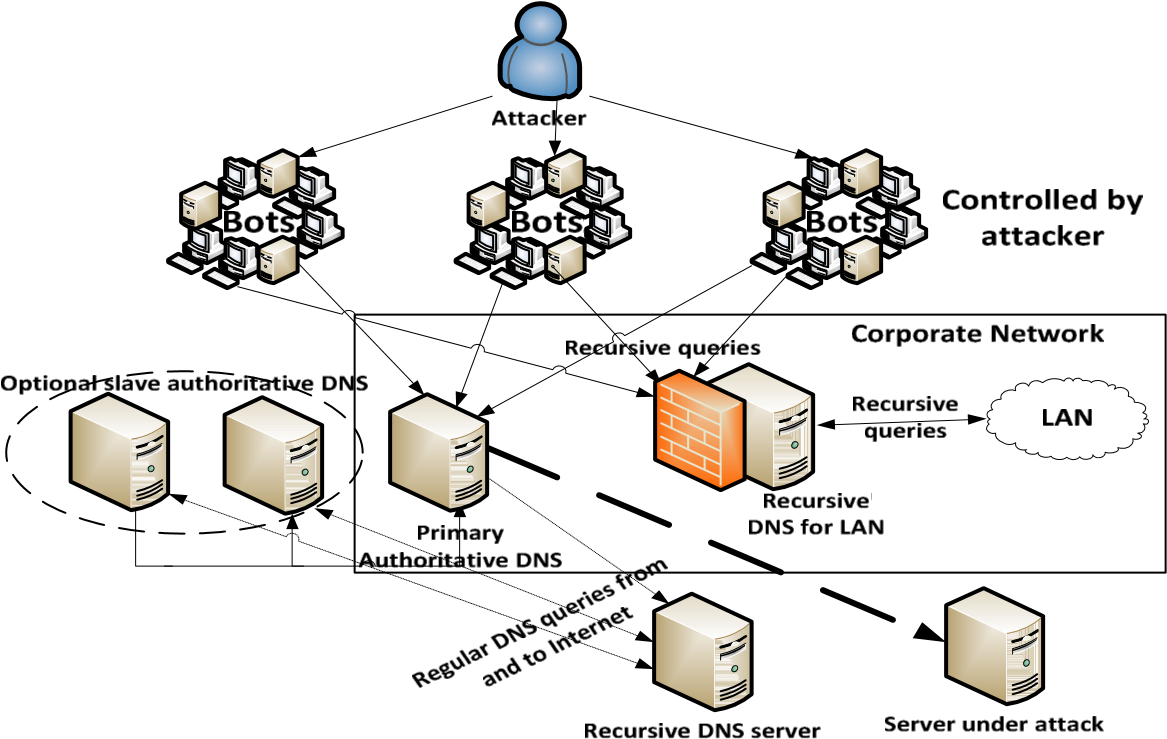
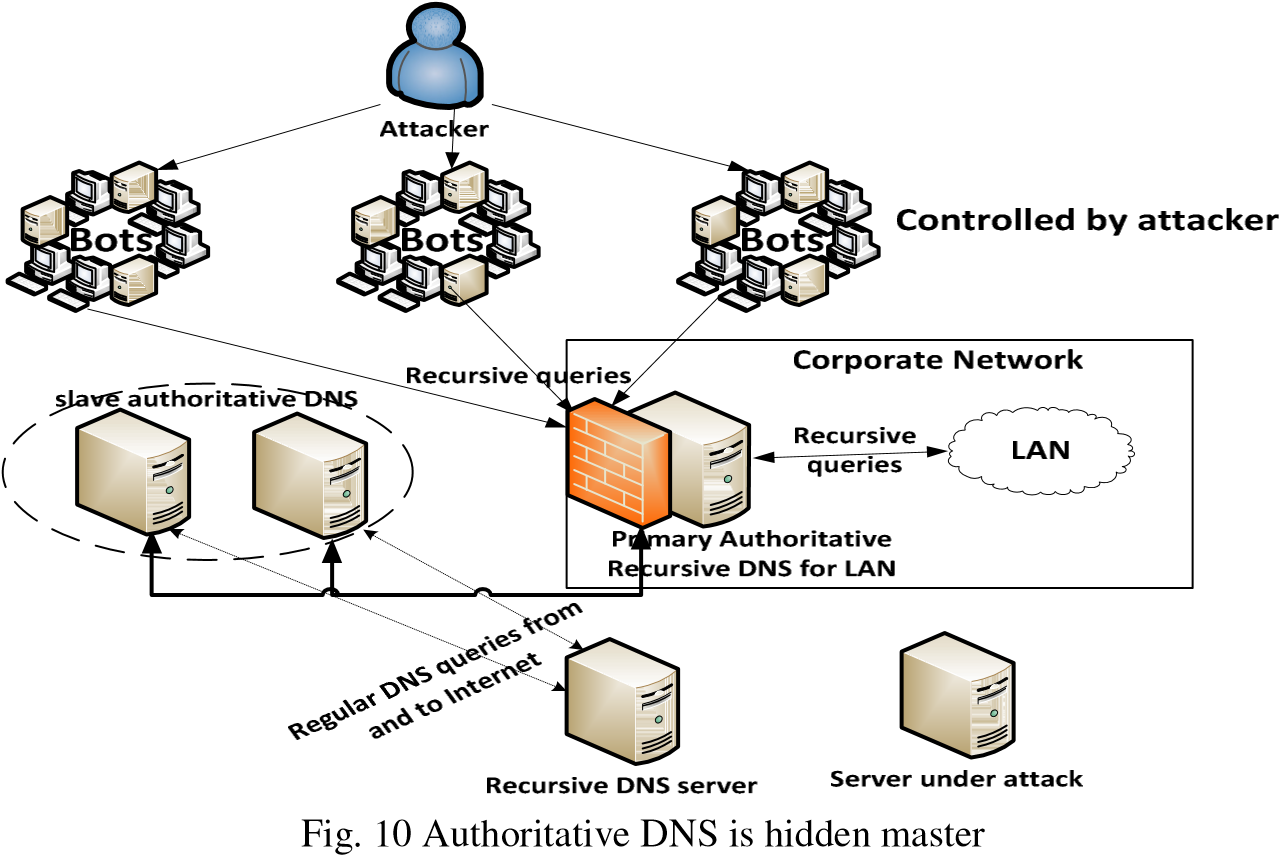


图9权威DNS服务器和递归DNS服务器的划分

v)使用隐藏的主服务器,以便只有你的从属的权威DNS服务器可以在Internet上公开可用，如下面的图10所示。



4.1.3 DNS响应速率限制

DNS-RRL。DNS响应速率限制是一种实验机制， 用于限制DNS服务器每秒返回的响应数量。DNS扩 增攻击的有效性可以通过删除超过配置速率限制的响应来降低。有三种方法可以对DNS服务器应用响应速率限制通过源IP地址、目标IP地址和DNS查询类型[27]。

4.1.4 Anycast任播

Anycast允许多个相同的全球部署DNS服务器发布相同的IP地址。使用Anycast, 每个DNS服务器IP对应于全球范围内从不同地理位置宣布的数百个系统。DNS服务器反映具有欺骗IP地址的流量，然后在离查询客户机最近的DNS服务器上删除这些流量。

Anycast的大部分实现都在网络层，但作者loannis Avramopoulos和Martin Suchara的研究已经证明Anycast可以在一个应用层实现， 结果表明，Anycast的安全性能与网络层实现[28]基本相同。

* 1. TCP SYN泛洪

SYN泛洪缓解已经发展为两类，分别是端机和网络。终端主机缓解包括加强终端主机TCP实现，这包括更改用于连接查找和建立的算法和数据结构。基于网络的缓解包括加强网络，这可以降低攻击前提条件的可能性，也可以插入中间盒，将网络上的服务器与非法SYNs[11]隔离开来。

最终宿主缓解技术包括:

i) 增加TCP Backlog

ii) 减少SYN接收计时器

iii) SYN缓存和SYN cookie通过减少初始分配给接收到的SYN生成的TCB的状态(SYN缓存)生成零状态(SYN cookie)来操作，并推迟实例化完整状态。

iv) 将上述两种或两种以上技术结合起来的混合方法

基于网络的缓解技术包括：

i) 输入过滤依赖于欺骗IP数据包，是非常有效的防止SYN泛滥攻击

ii) 使用防火墙和代理通过欺骗同步到发起者或欺骗到侦听器来缓冲来自SYN泛洪攻击的端主机

iii) 使用一种成本较低且易于部署的活动监控设备来观察并向整个网络的侦听器注入流量，而不需要每个侦听器的操作系统实现终端主机缓解

终端主机和基于网络的缓解经常波使用，并且在组合使用时通常不会干扰。终端主机上的缓解优先于基于网络的，因为SYN泛洪是针对终端主机的，而不是试图耗尽网络容量。

SYN缓存技术是目前最有效、最常用的终端主机缓冲技术，它可以在不受SYN cookie负面影响的情况下抵御严重攻击，并且在许多混合方法中使用阈值设置时不需要启发。

对于基于网络的缓解，防火墙/代理的同步ack欺骗和ack欺骗产生了相同的效果，由于其低成本和易于管理，主动监控器比防火墙/代理更受欢迎，而入口和出口过滤通常被用作一种良好的Internet安全实践。

* 1. UDP泛洪

UDP泛洪攻击之所以引人注目，是因为最近一群名为Anonymous(匿名)的互联网活动人士发起了高调攻击[29,30]。一种被称为LOIC(低轨道离子加农炮)的DoS攻击工具，使用UDP数据包执行洪水攻击，在web上广泛可用。为了减轻UDP泛洪攻击的影响，提出了几种抑制这类攻击的方法，如禁UDP服务、限制UDP流量的速率、保护代理服务器以及配置路由器来停止IP定向广播传输。例如， Komatsu et al[31]进行了-一个模拟，使用扼流与ACC(复杂带宽控制)作为拥塞控制方法，以证明限速方法在减轻UDP洪水攻击方面的有效性。