分布式拒绝服务攻击研究新进展综述

孙长华,刘 斌
(清华大学计算机科学与技术系,北京 100084)

摘 要: 分布式拒绝服务攻击一直是网络安全领域的研究难点.本文在进一步分析分布式拒绝服务攻击的危害及其原因的基础上,重点综述了 2005 年以后对该问题的研究和解决方案,主要包括:基于网络服务提供商的网络过滤、基于校验工作、基于重叠网络和基于网络功能.通过分析它们的优缺点,总结出可部署的解决方案的特点,并对今后的研究进行了展望.

关键词: 分布式拒绝服务; 综述; 网络功能; 反向图灵测试
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2009) 07-1562-09

Survey on New Solutions Against Distributed Denial of Service Attacks

SUN Chang-hua, LIU Bin
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract: Distributed denial of service (DDoS) attacks remain a serious threat on the Internet and again it is very difficult to devise a perfect DDoS defense mechanism. In this paper, we investigate the damage caused by the DDoS attacks and analyze the root reasons why DDoS attacks take place. After that, we make a survey on the new solutions against DDoS attacks especially after year 2005, which mainly includes 1) Network filters based on ISP; 2) Proof-of-work; 3) Overlay network; and 4) Network capabilities. We analyze the advantages and disadvantages of these solutions, and conclude the features of the deployed solutions. Finally, we discuss possible future defense strategies against the DDoS attacks.

Key words: DDoS (distributed denial of service); survey; network capabilities; reverse turing test

1 引言

分布式拒绝服务(Distributed denial of service, DDoS)攻击依然是目前 Internet 很大的威胁,2007 年 9 月 Arbor 公司调查报告[1]显示,网络服务提供商(ISP)头号运营威胁是僵尸网络(Botnet),其次是 DDoS 攻击,且僵尸网络往往被用来进行 DDoS 攻击.因此,DDoS 攻击被认为是 ISP 目前最大的运营危害.DDoS 攻击相对容易发生,因为目前 Internet 缺乏有效的认证机制,其开放结构使得任意数据包都可以到达目的地,加上网络上已有现成的工具[2]可被利用,为发起 DDoS 攻击创造了便利.精心构造的攻击甚至能够达到 24 Gbps 的攻击流量[1],足以充斥任一服务器的接入带宽.因此,DDoS 攻击的解决方案一直是网络安全研究领域的难点问题,顶级会议如 SIGCOMM 从 2001 年开始,几乎每一年都会有一篇跟 DDoS 研究相关的论文,但 DDoS 攻击问题依然没有得到彻底的解决.

自 2001 年,国外学术界出现了不少关于 DDoS 攻击及其检测防御方面的综述如[3~7],其中文献[3]主要综述了 DDoS 攻击工具和方法,文献[4]根据是否为反射攻击(reflection attack)来对已有的 DDoS 攻击进行分类,文献[5]详细综述了 DDoS 攻击手段,简要介绍了防御办法,文献[6]综述了识别 DoS 洪泛攻击的方法,文献[7]对 2005 年前的 DDoS 防御方法进行了详实的综述,而之后新出现的 DDoS 攻击解决方案目前还没有完整的综述见诸报道.国内也有一些综述[8,9],但仅对当时的解决方案进行综述[8],或仅对部分领域解决方案进行综述[9].本文主要对 2005 年后出现的解决方案进行综述,分析它们的优缺点,总结出可部署的解决方案,并对未来可能的解决方案进行展望.

2 DDoS 攻击背景分析和攻击分类

2.1 DDoS 攻击现状和危害

拒绝服务攻击(DoS),目的是通过各种手段阻止系统服务于正常用户,可分为两种形式[4],一是利用目标系统或软件漏洞,发送一个或多个精心构造的数据包给目标系统,让被攻击系统崩溃、运行异常或重启等,导致无法为正常用户提供服务,如"ping-of-death"攻击发送很大的 ICMP ping 包给被攻击系统,这些 ping 包会被分片重组,某些操作系统设计不完善可能会因为缓冲区溢

收稿日期:2008-06-05;修回日期:2009-01-12
基金项目:国家自然科学基金(No. 60573121, No. 60625201, No. 60873250);教育部培育基金(No. 705003)和博士点基金(No. 20060003058);国家 863 高技术研究发展计划(No. 2007AA01Z216, No. 2007AA01Z468)

出而重启、崩溃;另一种称为洪泛攻击,它让无用的信息占去系统的带宽或其他资源,使得系统不能服务于合法用户.第一种攻击可以通过给系统打补丁、找出系统漏洞的方法进行防御,第二种攻击比较难解决.这两种形式的攻击也可结合,本文偏向于第二种形式的攻击.DDoS 攻击是 DoS 攻击中数据包来自不同的攻击源端,即利用网络中不同的主机同时发起 DoS 攻击,使得被攻击对象不能服务于正常用户.DDoS 攻击因为使用了不同的攻击源,攻击效果被大为放大.

自 2000 年 2 月,针对 Yahoo 网站的 DDoS 攻击使其瘫痪 3 个小时后,DDoS 攻击目前依然在发生:2006 年 3 月,ICANN 安全和稳定咨询委员会报道了利用 DNS 服务器进行放大的 DDoS 攻击,攻击的聚合流量达到 2.4Gbps;DDoS 攻击也被广泛用于网络敲诈、商业竞争、甚至政治斗争,如 2007 年爱沙尼亚的政府网站遭受 DDoS 攻击而被迫封禁国外 IP 的访问.[2]赛门铁克公司所做的 Internet 安全威胁报告[10]显示,政府部门和关键的基础设施遭受的网络攻击中,DDoS 攻击以 46 %的比例位居第一;其报告中 DDoS 攻击的判断仅统计 SYN 洪泛攻击,实际情况应更为严重.

2.2　DDoS 攻击分类和存在原因

典型的 DDoS 攻击包含四方面要素:1) 实际攻击者;2) 用来隐藏攻击者身份的机器,可能会被隐藏好几级,该机器一般用于控制僵尸网络(实际发起攻击的机器)并发送攻击命令;3) 实际进行 DDoS 攻击的机器群,一般属于僵尸网络;4) 被攻击目标即受害者.在 DDoS 反射攻击中,还利用 IP 源地址伪造,迫使合法的反射/放大方(如 DNS 服务器)向受害者发起攻击.

就攻击包的内容而言,DDoS 可分为两类:基于网络传输协议的攻击和应用层的攻击.前者比较流行的有 SYN 洪泛(包括 SYN/ ACK、Rerest 洪泛),ICMP 洪泛,UDP 洪泛和 IP 包分片洪泛.后者主要是在应用层上进行洪泛和资源占用攻击,常见的有 HTTP 洪泛,如 MyDoom 蠕虫,SIP 洪泛和 DNS 请求洪泛,资源占用攻击包括数据库资源消耗如利用脚本查询数据库,及利用 SMTP、SSL、VPN 等进行攻击.这些攻击的详细介绍可参见文献[5].就攻击效果而言,基于网络传输层协议的攻击主要以消耗攻击者带宽为目的,大部分应用层攻击以消耗 CPU、内存、数据库等资源为目的.如表 1 所示,Arbor 公司的调查报告[1]显示,无论是攻击流量(比特每秒)还是攻击的包速度(包每秒),UDP 洪泛,SYN 洪泛和应用层攻击为最常用的 DDoS 攻击形式,占据了绝大部分的比例.

目前,还出现一种新的 DDoS 攻击,即对等网络中的 DDoS 攻击[11],它利用目前广泛使用的 P2P 文件共享系统,使大量正常的用户访问被攻击对象,导致目标遭受过多的网络连接,并且带宽被消耗.

表 1　DDoS 攻击形式以及所占比例[1]

序号	每秒攻击的流量比特数		每秒攻击的包数	
	攻击类型	比例	攻击类型	比例
1	UDP 洪泛	43 %	UDP 洪泛	41 %
2	应用层	19 %	TCP SYN	26 %
3	TCP SYN	18 %	应用层	17 %
4	反射/放大	7 %	ICMP 洪泛	6 %
5	ICMP 洪泛	5 %	反射/放大	4 %
6	IP 分片	4 %	其他	4 %
7	其他	4 %	IP 分片	2 %

以下分析 DDoS 攻击存在的原因.需要指出,这些原因恰好是 Internet 获得成功和快速发展的设计理念.首先,Internet 是一个开放的资源共享系统,理论上任何 Internet 上的用户都可以将数据包发往任一网络可达的目的端,任一目的端可以自行决定是否响应收到的数据包,但其自身却不能控制外界向本目的端发送 IP 包;其次,Internet 设计的基本原则是核心简单和边缘复杂,核心网络最基本的功能甚至仅仅是路由转发数据包,故任一目的端无法控制网络数据数据包的到达.Internet 的设计理念使它得以快速发展,并且承载不断涌现的新业务,然而,就网络服务质量和网络安全问题,因没有核心网络的有效参与,一直很难解决.另外,网络缺乏有效的认证措施,即很难验证数据包是否为包中源 IP 地址所发出,导致很容易伪造源 IP 地址而进行网络攻击;而且,大多数接入端的带宽都要远小于核心端的带宽,如目前核心主干已经达到 OC-192 (10Gbps) 速率,而接入带宽大多数均小于 1Gbps,来自核心主干链路上的聚合流量很容易阻塞接入链路.DDoS 攻击正是利用了这个特性,从不同的地方向攻击目标发送无用的数据,并且这些数据聚集后很容易超过攻击目标的接入带宽.

3　DDoS 攻击解决方案分类

DDoS 攻击的解决方案已有很多,可归纳为解决两方面的问题:1) 区分正常和攻击流量.可根据正常流量和攻击流量的不同行为、统计特征等进行区别,也可通过认证的方式让所有用户付出一定的代价,如计算、人工参与输入认证码等来区别;2) 控制流量到达受害者,即解决带宽占用问题,通常情况,仅靠被攻击者是很难解决带宽占用攻击的,因为目前的 Internet 设计无法让接收端本身控制 IP 包的到达,只能使其选择是否处理或者响应到达的 IP 包.解决带宽占用有三种思路:1) 不改变现有网络核心的前提下,尽量少的对边缘路由器进行改动,利用 ISP 及其联合来过滤攻击流量.2) 从整个 Internet 设计的角度考虑 DDoS 攻击,即重新设计 In-

ternet,如在核心路由器中增加认证丢包等机制.3)采用CDN或者重叠网络来吸收流量.本文将DDoS解决方案分成如图1所示的几类:1)从源头上预防和消除,指解决IP源地址伪造和僵尸网络的问题;2)追踪攻击源,指源IP追踪,尽量找到实际的攻击者;3)DDoS攻击检测:包括利用各种行为特征进行DDoS攻击检测;4)基于校验工作(Proof-of-work)区分攻击流量;5)网络过滤(Network filters):包括传统的基于路由器拥塞控制及基于ISP的过滤;6)基于网络功能(Network capabilities)的解决方式;7)基于重叠网络(Overlay network)和CDN的解决方式;8)其他解决方案.

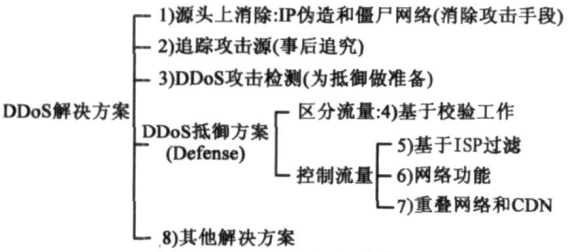

图1 DDoS解决方案分类

前三类本身并不能解决DDoS攻击.然而,DDoS攻击跟IP地址伪造、僵尸网络有着密切的联系,如果能够消除IP源地址伪造,尽量减少可被作为攻击工具的僵尸网络主机的数量,将极大缓解DDoS攻击强度;如果能够追踪到攻击者,可以诉诸法律,对发起DDoS攻击者具有很强的威慑作用;DDoS攻击检测需要跟某种抵御方案合作才能消除DDoS攻击.抵御方案中,基于网络功能和让核心路由器参与网络过滤的方法属于从重新设计Internet的角度考虑DDoS攻击.一般情况下,DDoS攻击的解决方案均是针对开放的服务器,但也有解决方案如重叠网络针对能区分合法用户(如经过用户身份认证)的通讯系统,其研究目标主要是如何控制流量到达受害者.

IP源地址伪造、IP追踪问题、传统的DDoS攻击的检测和基于行为特征的包过滤以及部份重叠网络的研究都是以前研究的热点,详细介绍可以参阅文献[7],本文仅对它们做简要介绍,以便对DDoS解决方案的整体了解.本文综述的重点是2005年后新出现的DDoS攻击解决方案,主要包括:基于自治系统AS的IP源地址认证、基于ISP的网络过滤、基于校验工作、基于重叠网络和基于网络功能的解决方式.因篇幅限制,对以前的研究本文不直接给出参考文献,相关文献可从文献[7]中找到.

3.1 源头上预防

从源头上预防和消除基于切断DDoS攻击依赖的攻击源,包括消除源IP地址伪造、消除僵尸网络的危害以及从攻击端进行检测和防御.

消除源IP地址伪造,以前的研究包括:入出口过滤、uRPF、SAVE协议、HCF和基于路由器标记的方法如PI等.简要介绍前三种.入出口过滤过滤(BCP 38/RFC 2827)部署在ISP的边缘路由器上,主要思想是:对于到本AS的数据包,检测数据包的源IP是否来自本AS或者其他不合法的IP;对于从本AS发出去的数据包,检测数据包的源IP是否合法.uRPF(RFC3704)即单播反向路径转发检测,当路由器的某个端口收到一个IP包后,查看以此源IP地址作为目的地址的IP包,是否可以通过接收端口转发出去,从而判断该IP包是否伪造.不对称和动态路由的存在,对uRPF实施有一定的局限性.SAVE主要解决了uRPC的缺陷,需要路由器更新某个端口运行出现的源IP地址或者范围.

文献[12]提出了让AS之间认证的SPM方法,基于AS之间认证的还有PassPort[13],文献[14]提出了基于BGP的BASE协议,重点强调有激励能够增量式部署,基于BGP的防止IP地址伪造的还有IDPF[15].文献[16]提出了可用于IPv4和IPv6的SAVA架构,也用于增量式部署,并解决了BCP 38中一些问题.目前该项工作在IETF中成为SAVI WG,正在进行标准化工作[17].

消除IP源地址的研究,大多都侧重于如何提高方法的激励,能够增量式部署,并且解决多路由、ISP之间的问题.但是,这些方法均很难解决同一个子网或AS内的IP伪造.另外,消除IP源地址伪造并不能直接消除DDoS攻击,目前DDoS攻击大多数由僵尸网络发起的,僵尸网络往往直接使用真实的源IP进行攻击,应用层的DDoS攻击无法伪造源IP地址.僵尸网络的综述可参见文献[18],消除或减少僵尸网络需要尽可能保证每台接入Internet主机的安全,相当艰巨.

3.2 攻击者追踪

从威慑攻击者角度而言,如何找到攻击源是非常重要的问题.定位攻击者有如下限制:1)IP源地址容易伪造;2)路由器的路由是无状态的,只知道下一跳地址,不记录经过该路由器的IP包;3)由于真正的攻击者往往隐藏很深,采用僵尸网络进行直接攻击,即使找到了某些直接攻击源即僵尸网络,也很难找到真正的攻击者.

针对如何找到攻击源,尤其是IP源地址伪造的问题,以前的研究主要集中在IP追踪上,提出了很多方法,如基于概率的包标记PPM、FIT和基于hash的IP包追踪.文献[19]提出了一种分布式分而治之的方式来解决追踪攻击源的问题,该方法将三个问题分开来进行研究:攻击树的构建、攻击路径频率的检测和包与攻击路径的关联检测,能够以较小的开销和很高的效率对单个包进行追踪,但该方法是否能有效部署依然存在问题.

3.3 DDoS攻击的检测

DDoS攻击的检测是传统的DDoS攻击解决方案之

一,并得到了广泛的研究,它分为两类,第一类是基于某种具体的 DDoS 攻击的检测,第二类是借用入侵检测系统进行异常检测. 第一类检测中,有代表性的有: MULTOPS 监控入和出链路的流量,当流量比异常时,认为可能有 DoS 攻击发生; SYN 和 FIN 包比例最早用于 SYN 洪泛攻击检测,文献[20]对此进行了改进,引入 Bloom filter[21] 记录一段时间内的 SYN 包数,根据此 Bloom filter 对 FIN/ RST 包数进行统计,消除了无用 FIN/ RST 包的影响,提高了检测的有效性;另外,还有一些基于时间序列、光谱分析、小波分析和统计特性等[22]来检测 DDoS 攻击的,详细的介绍可参阅综述[6,7],后面所述的这些检测方法往往需要有一个或者多个假设,如光谱分析假设攻击流量没有周期性的特征并仅对 TCP 流有效、时间序列分析仅对部分已知的攻击有效,这些假设有时候可能不成立,并且,DDoS 攻击完全可以采用与正常流量一样的流量,这使得以上检测方法的适用性变弱.

基于特征行为模型的包过滤与检测 DDoS 攻击的某些方法相类似,如基于统计特性和机器学习等来区分正常流量和攻击流量,既可以检测 DDoS 攻击,也可以用于作为特征进行攻击包过滤.

针对应用层 DDoS 攻击,因为需要在传输层之上,没有 IP 源地址伪造的问题. 文献[23]利用隐藏的半马尔可夫模型来描述用户浏览网页的行为,然后根据此检测 HTTP 请求洪泛攻击,然而,该数学模型的有效性依然需要进一步研究和论证. 文献[24]采用组测试理论来检查应用层的 DDoS 攻击者,假设攻击者的请求速率大于正常用户. 组测试理论是用最少的检测次数找到与其他成员不一样的成员,核心思想是如何判定某个攻击者的请求速率大于正常速率,因为不知道正常速率是多少,目的是利用用较少的资源来完成. 该方法认为僵尸网络规模比以前预计的要小,主机数量级在几百,其方法的开销与攻击者的规模成比例,然而,僵尸网络的规模本身是有争议的问题,文献[25]认为僵尸网络主机数在百万级别. 故该方法仅检测方面还存在一定局限性.

3.4　基于校验工作的认证方式

基于检验工作的认证方式有两类研究,1) 用户如果想要获得服务,必须付出某种"货币"(currency),如 CPU(解难题如大数分解问题等)、内存,甚至带宽资源[26];2) 基于认证如反向图灵测试(CAPTCHA)来区分攻击者和正常用户.

用户需要付出某种代价才能获得服务,最早的研究是付出计算资源,即解难题,难题需要满足的基本条件有:服务器端较容易的生成和验证难题,能够控制难题难度的级别;难题大多数情况下能被一般的客户端所解,不能让客户端能预解难题;整个过程对于服务器端是无状态的. 典型的解难题工作如下:服务器端随机选取一序列 N_s 以及难题难度级别 k 发给客户端,客户端再随机选取一序列 N_c 并需要寻找 X,需要满足将 N_s, N_c, X 结合起来哈希后结果的低 k 比特为 0,即: $h(N_s \| N_c \| X) \bmod 2^k = 0$,一般哈希函数选择 MD5 或者 SHA,服务器端可以通过增加难度级别使得客户端需要更多的计算才能找到答案. 因为服务器端验证难题需要哈希计算获得,验证过程也可能被用于 DDoS 攻击,即消耗服务器端的验证资源,因此也有设计难题不通过哈希计算验证,而通过查找验证. 然而,解难题的出发点是客户端需要付出计算资源才能获得服务,一定程度上能够限制客户端访问频率,但是如果攻击者使用僵尸网络进行攻击,僵尸网络的主机也可以付出计算资源,因此解难题并不能从本质上区分攻击者和正常用户,而且,它还会让正常用户建立网络连接的时间加长.

另一种需要用户付出资源的典型是利用带宽作为"货币",如 speak-up[26]. speak-up 假定网络带宽足够,尤其是被攻击目标接入带宽丰富,并假定被用来攻击的机器都占用完了它们的带宽用做攻击. 当发生 DDoS 攻击时,被攻击目标让所有的客户端(包含正常用户和攻击机器)都增大带宽,因为实施攻击的机器已经用完了它们的带宽,只有合法的客户端才能增大带宽,从而让合法的客户端获取更多的服务. 该方法有一些局限性,仅针对应用层非带宽占用的攻击,且在发生 DDoS 攻击时,让所有的客户端都增大带宽,有可能使情况越来越糟,并对网络其余部分造成负面影响. 另外,假设实施攻击的机器已经用完了它们的带宽不一定成立,这些机器为了不引起注意,往往只用少量的带宽实施攻击,完全可以和正常用户一样增大带宽. 文献[27]基于之前以带宽作为"货币"的方式可能需要保存很多认证状态,而提出了自适应选择验证 ASV 的方法. ASV 可以让客户端自适应的发送额外的请求(以带宽作为代价),服务器端可以选择性的验证然后给予某些客户端更多的服务. 文章的主要贡献在于通过理论分析比较了 ASV 与之前理想协议(攻击的参数为服务器和所有客户端所知晓)的性能,发现 ASV 与之相当,并且,采用 ASV 的方式使服务器端变成无状态,有很强的可扩展性. 然而,这种采用带宽作为"货币"的方式,都无法精确的区分正常用户和攻击者,并且不能用于带宽消耗的洪泛攻击.

基于校验工作的另一种方法是反向图灵测试. 图灵测试原本用于人工智能中人来区分计算机和人脑,现在希望通过计算机(被攻击的服务器)通过测试来区

分是计算机自动访问还是正常人访问,因此,称之为反向图灵测试或者 CAPTCHA(Completely Automatic Public Turing tests to tell Computers and Humans Apart)技术. CAPTCHA 的基本形式是利用机器难以自动识别的图片(图片上有人可以容易识别的字母,而机器很难辨认)来区分是否为自动访问,或者恶意访问. 反向图灵测试能够以较低的成本来区分攻击者和正常用户,但不能每次都使用,否则正常用户每次都需要被打扰. 另外,CAPTCHA 图片也有被自动识别的可能性.

Kill-bots[28]解决了 CAPTCHA 需要每次都要被验证的问题,因为可能正常用户有时候不愿意被打扰去做反向图灵测试. Kill-bots 主要用于保护网页服务器,其工作流程如图 2 所示,它有两个工作阶段,并利用 Bloom filter 记录攻击者 IP 地址. 当新的 TCP 连接建立时,Kill-bots 首先检测该客户端是否为攻击 IP,如果不是,将根据目前系统的负载按照一定概率接受连接(接纳控制). 在第一阶段时,接纳的连接还要进行 CAPTCHA 测试,如果客户端能够正确输入图片上的文字,则会被短暂给予一个 HTTP Cookie,用于接下来的连接,而不需要再经过根据负载的接纳控制和输入图片上的文字. 在第二阶段时,接纳的连接直接给予 HTTP Cookie,因为在第一阶段时已经检测到攻击者的 IP 地址列表,且这个列表已经稳定. 在第一阶段时,Kill-bots 根据不能回答 CAPTCHA 测试的次数来判断是否为攻击者,利用 Bloom filter 进行记录,只有测试失败的次数超过一定阈值的才会被归为攻击者,这样,正常用户可在一定程度上不被 CAPTCHA 测试打扰. 另外,为了解决反向图灵测试使用图片造成带宽消耗过多,也有设计基于文字的 CAPTCHA.

基于校验工作的方法均是针对应用层的 DDoS 攻击,即占用被攻击对象的资源,它不能单独用于解决基于洪泛的 DDoS 攻击,但是,基于付出资源如 CPU 和带宽的方法提供了有效的服务器端资源分配的方法,而反向图灵测试提供了简单的识别攻击者和正常用户的方法,容易部署. 这类方法可与其他方法结合起来用于 DDoS 防御.

3.5 基于网络过滤的防御

网络过滤的想法很直观,如果能区分攻击流量和正常流量,则尽量早的将攻击流量过滤掉,有助于缓解甚至消除 DDoS 攻击. 最理想的方式是在攻击源的附近部署过滤装置,在被攻击目标处或者附近部署检测 DDoS 攻击的装置,过滤和检测装置构成一个分布式系统,联合起来对 DDoS 攻击进行防御. 之前的研究中,在攻击源端进行 DDoS 攻击防御有一定优势,但部署激励很小;进行分布式系统联合防御一样也存在激励很小的问题,且整个系统协同工作也会很困难. 但网络过滤依然得到重视,研究者转向基于路由器或基于 ISP 及 ISP 联合的思想,前者利用网络中的核心路由器来控制流量,后者依据 ISP 的带宽容量远大于被攻击者的接入带宽,且在被攻击者所在的 ISP 上部署有很强的激励作用,当本地 ISP 无法有效防御 DDoS 带宽攻击时,可以求助于上一级或者对等 ISP.

之前的研究主要有 Pushback,它利用路由器的拥塞程度,当某个路由器拥塞到一定程度时,开始丢包,丢弃那些去往同一个目的地的数据包,并发送一个 Pushback 消息给相连的路由器,让它们也限制去此目的地的包,最终目的希望能够在攻击包进入网络时即被丢弃,以最大程度的减轻攻击危害;Pushback 方法的假阳性(即不是 DDoS 攻击包,也可能被丢弃)很大,因为它不能区分攻击包和正常包.

文献[29]提出在 ISP 和 ISP 间利用路由和隧道来抵抗 DDoS 攻击,主要思想是在网络中部署一些控制点,由这些控制点来安装过滤器以过滤掉被攻击者不希望接收的网络流量,所有到接收端的流量需要经过控制点才能到达,实现技术采用隧道方式. CAT[30]在被保护的受害者的可信任的区域,部署很多 Cookie box,这些 box 利用 SYN cookies 技术与客户端建立 TCP 连接,防止源 IP 伪造;然后 Cookie box 在 TCP 时间戳选项中加入 flow cookie,此 cookie 不断 refresh,客户端需要将此 cookie 返回才能与服务器端通信,同时由受害的服务器区分正常和攻击的流量,并通知 Cookie box 来过滤掉不正常的流量. 文献[31]认为目前网络上在接近攻击源的路由器上有充足的资源来过滤攻击流量,提出了主动网络过滤 AITF. AITF 通过 IP 包中的路由记录选项来寻找尽可能接近攻击源的路由器,然后被攻击者与接近攻击源的路由器协商交互过滤规则. 文献[32]认为当接入链路被 DDoS 占满时,只有 ISP 才有可能进行 DDoS 防御,因此,认为由 ISP 实现网络中的 DDoS 检测和缓解是非常有前景的,并提出在 ISP 进行多阶段检测 DDoS 攻击的方法:LADS,第一阶段利用比较低开销 SNMP Data 进行检测,判断的依据有包的速率之类,当发现异常时,触发第二阶段,利用 NetFlow 收集流级别的数据进行检测. Reval[33]是一种实时帮助评估 DDoS 攻击的影响并确

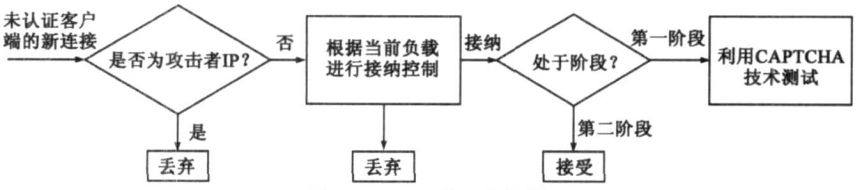

图2 Kill-bots的工作流程

定可行的缓解攻击的策略的工具. dFence[34]与文献[29,30]类似,采用称为 middle-box 的中间层进行流量代理和网络过滤,过滤策略采用全状态. 文献[35]提出了基于自治域 AS 之间的责任性进行 DDoS 防御,即要求所有流量的源地址都是正确、可识别的,接收方可有效的过滤来自任意源的流量. PATRICIA[36]利用 AS 的代理和认证 DDoS 防御,服务器端在遭受攻击时,由本地 AS 来代理流量,所有与服务器端通信的客户端都需要经过服务器端所在的 AS 和客户端所在的 AS 的同意. StopIt[37]与 AITF 类似,但 AS 之间使用 StopIt 服务器交换过滤规则,由被过滤攻击机器所在的 AS 的接入路由器实施过滤,并考虑了过滤规则的膨胀、增量式部署等设计目标.

基于 ISP 的防御方法大多数都是利用 ISP 的带宽优势来吸收 DDoS 洪泛攻击,一般在 ISP 或 ISP 间部署中间代理层,由中间层隐藏被保护的服务器,攻击者和正常用户的流量都由中间层代理处理. 这种方式如果精心设计,在抵御 DDoS 带宽攻击上会起到比较好的作用.

3.6　基于网络功能的认证方式

基于网络功能(Network Capabilities)的防御假设整个 Internet 的路由器是可以改变的,即利用核心路由器来防御 DDoS 攻击. 网络功能指 IP 包中携带的信息,该信息可以被路由器检验并确认该包是否为目的地所需要. 基于网络功能的方法主要有: SIFF、TVA[38]和 Portcullis[39]. 其中 SIFF 和 TVA 的主要思想是:发送方 X 和接收方 Y,如果 X 想与 Y 进行通信,X 必须首先获得 Y 的同意,即向 Y 申请 Capabilities,如果 Y 不同意与 X 通信,可以忽略请求,否则,Y 返回网络功能给 X,以后 X 发送给 Y 的 IP 包内都需要附上网络功能. 网络功能由 X 与 Y 之间的路由器负责校验,不正常时路由器可以丢包. 图 3 示意了 TVA 的工作流程,当客户端与服务器端建立连接时,路由器会在请求包中增加基于本地的网络功能,这些网络功能和请求包一起到达服务器端,如果服务器端同意与客户端通信,将请求包中的网络功能附在回应包上,沿途的路由器修改认证信息,使这个客户端携带合适的网络功能的包可以通过. 路由器中,可以对带有通过认证的网络功能的包给予优先处理. 网络功能需要解决的问题有:如何保证获取网络功能的路径不被 DDoS 攻击,如何保证网络功能不被假冒,且路由器以较低的代价验证. 文献[40]总结分析了网络功能的优缺点,重点指出 Denial-of-capabilities(获取网络功能时没有被保护,可能会有 DDoS 攻击,导致正常用户无法获取)和路由器中需要保存 Per-capability 的状态.

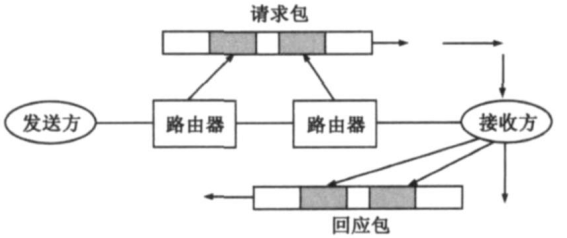

图3　网络功能的示意工作流程

Portcullis[39]主要解决 Denial-of-capabilities 的问题,认为文献[40]的分析考虑不周,文献[40]认为用来保护获取网络功能的通信通道的方法也可以用来保护所有的通信数据,实际上建立网络功能的过程允许有较高的丢包率和不确定性,因为只要有一个包成功到达目的地,网络功能即可建立,故 Portcullis 利用解难题的思想,即基于计算来区分正常和攻击用户,来解决网络功能建立过程中可能出现的 Denial-of-capabilities 攻击. 具体而言,客户端端自己生成难题和答案,载有难题难度信息,由沿途的路由器进行验证;如果简单的难题没有被允许,则客户端端加大难题的难度.

基于网络功能的认证机制,虽然会给正常流量的处理带来额外开销,且需要在大量核心路由器中部署,但它的思想能解决接收端可控制是否接收任意发送方发送的数据. 然而,它在部署上缺存在较大问题,因激励很小,很难说服营运商去修改核心路由器. 并且,网络功能的认证机制也颠覆了目前 TCP/IP 的工作模式,需要所有客户端和服务器端都做出相应的改变.

3.7　基于 CDN 和重叠网络的解决方式

以前的研究中,利用重叠网来抵御 DDoS 攻击,如 SOS、Mayday 和 WebSOS. 其目标是用重叠网络隐藏被攻击服务器,仅适用于非开放性的服务. OverDoSe[41]将客户端与被攻击的服务器在 IP 层隔离,只有重叠网络的节点才能访问服务器端,客户端不能直接访问服务器端,它只需要在服务器端所属的 ISP 进行部署,ISP 可以部署 MPLS、VPN 等隧道的方式让重叠网络与服务器互相访问,在一定程度上能减轻 DDoS 攻击. OverDoSe 需要服务器端通过应用层验证的方式区分攻击者,然后通知重叠网络的节点过滤掉这些攻击流量.

CDN 即内容分发网,用于加快网络访问速率和质量,一般会在不同 ISP 内部署节点,形成很大的分布式网络,将用户请求自动指向到健康可用且距离用户最近 CDN 节点上. 由于具有很大的带宽,CDN 如 Akamai、ChinaCache 具有防御 DDoS 带宽消耗攻击的能力,尤其对静态和动态可缓存的页面非常适合,但对于动态不可缓存的页面,CDN 节点也需要从原始的服务器实时访问获取信息,然后提供给用户,如果攻击者大量的请求此类页面,也可能造成 DDoS 攻击. 与重叠网络相比,CDN 除了提供网络可访问性,还提供应用层服务.

Phalanx[25]试图解决动态不可缓存页面的保护问题,它将 CDN 的节点称为 Mailbox,用来进行流量代理. Mailbox 的功能跟实际生活中的信箱类似,信件只送往信箱,需要用户自己到信箱中取才能看到信件,Phalanx 中流量不能直接通过 Mailbox 传递到被保护的服务器,需要在服务器的主动请求下,才能发送给服务器,这样,服务器能够有效控制到达它的流量. 在 Mailbox 和服务器之间,由服务器所在的 ISP 以及更上一级的 ISP 部署称为过滤环的过滤装置,过滤掉恶意以及服务器没有请求的数据包. 初始建立连接时,客户端与 Mailbox 之间采用基于解难题的(与 Portcullis 类似)认证机制,即需要客户端付出一定计算资源,并且难题的难易程度可以控制,客户端才能获得服务,同时,对于一些预先认证的客户端,采用认证令牌桶机制,给予这些客户端认证的 Cookie,不必再进行解难题. 为了保护某一个 Mailbox 被攻击时通信还能继续,客户端与服务器之间的通信通过一系列 Mailbox 转发进行,这个 Mailbox 集合由客户端和服务器协商的信息计算获得. Phalanx 的工作机制能够很好的控制流量到达目的端,但也会对连接造成一些延时,并且,基于解难题的认证并不能有效的区分攻击者和正常用户,另外,不断变换 Mailbox 进行转发也可能会影响 TCP 连接的性能,并可能需要修改上层应用.

3.8 其他解决方案

DDoS Shield[42]利用调度的方式来保护应用层的资源,该方法在被攻击目标处采用基于计数器的方式,对每个客户端给予连续的计数器值而不是二进制形式,然后根据这些计数器的值进行有效的调度. 还有一类低速的 DDoS 攻击,攻击的速率比较小,但可能会影响 TCP 的性能,文献[43]认为基于路由器和基于终端节点的方式均只能减轻这种攻击,而如何有效的检测这种低速攻击依然是开放性研究问题. PSP[44]采用优先级的丢包来隔离不同流的带宽占用,需要在核心路由器上部署,通过对包到达速率的测量对包的优先级进行标记. 该方法需要核心路由器协作,部署上并不容易.

4 DDoS 攻击解决方法展望

DDoS 攻击实际上涉及两个层面的问题,一是如何控制带宽攻击;二是如何区分攻击者和正常用户. 基于网络功能的解决方案能够带宽控制问题,但部署上存在较大问题. 综合已有对 DDoS 攻击解决方案的需求,本文总结在目前 Internet 上解决 DDoS 攻击的方案应具有如下的特点:

(1) 可部署性:控制带宽攻击的方法需有明显的可部署性,且这种部署具有明显的激励性,换言之,需要单个 ISP 即可以部署并且能有不错的效果,或者大型 CDN 可以进行部署;

(2) 减少对正常通信的影响:目前 Internet 的简单和开放性极大的促进了其发展,DDoS 攻击虽然具有很强的危害性,但相比正常网络通信,它发生的概率还是会小很多,因此,提出的 DDoS 攻击解决方案需要尽可能减少对正常通信的影响,尽可能不要做出让整个网络的客户端都进行修改的情形;

(3) 保护已经建立的网络连接:任何 DDoS 防御措施都应该尽量不影响已经建立的网络连接,如果有影响,也应该将其影响控制在一定程度内;

(4) 接收端可控性:即接收端能够控制包的到达,它能够控制允许或者拒绝和某个用户通信,在接收端拒绝通信后,用户的数据包应尽可能少的发向接收端;

(5) 有效性:在部署 DDoS 防御方法后,发生 DDoS 攻击时,整个通信性能应该尽可能接近没有 DDoS 攻击的情况,否则,就等效于攻击者已经成功的达到 DDoS 攻击目的了;

(6) 健壮性:即 DDoS 防御方法尽量简单,保证自身不受或者能够承受 DDoS 攻击,并且,整个方法需要有较好的健壮性.

这些特点强调解决方案应易于部署,即尽可能小的对整个网络产生影响,并需要满足"谁部署、谁受益"的激励方案. 基于此,我们对已综述的 DDoS 解决方案(除去从源头上解决和攻击源追踪)进行了比较,结果见表 2.

表 2 DDoS 解决方案的简单比较

解决方案	部署地点	部署难易	区分流量	区分对待	控制流量	对 Internet 开放设计原则的影响
攻击检测	受害者	易	具体方法	否	否	无
传统包过滤	受害者	易	是	是	否	无
解难题	受害者	易	否	是	否	轻微
带宽货币	受害者	易	否	是	否	无
CAPTCHA	受害者	易	是	是	否	无
Capabilities	Internet	难	是	是	是	影响
基于 ISP 过滤	ISP	适中	具体方法	是	是 一定程度	无
CDN	Internet	易	未知	是	是	无
封闭 Overlay	Internet	难	是	是	是 一定程度	影响
OverDoSe	ISP	易	否	是	是 一定程度	无

综合已有的研究,在不改变目前 Internet 整体构架下,即接收端无法控制 IP 包是否到达的情况下,DDoS 攻击彻底解决是比较困难的. 而改变 Internet 的框架,如基于网络功能的解决方案,部署上有存在很大的问题. 极端情况下,攻击者可以采用与正常用户一样的攻击流量,这使 DDoS 攻击的防御变成了如何构建吸收大量

流量的网络分布式系统的问题.

本文认为,今后解决 DDoS 攻击依然需要解决本节开头的两个基本问题:控制流量和区分流量.解决带宽攻击可部署的途径是基于 CDN 和 ISP 过滤的方式.基于 CDN 的方式,对于可以缓存的内容能够提供很好的保护,但是对于如何保护动态不可缓存页面,除了 Phalanx 方法外,还有研究的空间.而基于 ISP 的网络过滤解决方案,已有的研究重点在于设计 ISP 之间如何联合(这方面的部署激励性还存在一定问题),而以尽量小的代价在 ISP 边缘路由器上实施网络过滤依然是重要有意义的研究课题.在区分流量方面,基于校验工作的认证方式,尤其是反向图灵测试,已取得一定的成绩,对其存在的问题还有一定的研究空间.

除了以 CDN 和 ISP 过滤的方式解决 DDoS 攻击外,以较小的代价较精确的检测出 DDoS 攻击,进而采取抵御措施如[45],也是非常有益的补充.DDoS 检测方法研究较多,但已有的一些方法有些假设性较强,有些误判率较高,还存在一定的改进空间.

总结而言,可部署的 DDoS 解决方案如基于 CDN、基于 ISP 及其联合过滤只能在一定程度上抵御 DDoS 攻击,在这两种已有的框架下,还存在一些问题需要进一步研究和解决.

5　结论

本文分析了 DDoS 攻击形成的原因及其危害,重点对 2005 年以后出现的解决方案进行了综述,分为:1) 基于检验工作的验证;2) 基于网络功能的认证方式;3) 基于 ISP 的网络过滤和 4) 基于重叠网络以及 CDN 的解决方式,总结出可部署的解决方案的特征,并对未来可能的解决方案进行了展望.

参考文献:

[1] Worldwide Infrastructure Security Report, Volume Ⅲ[OL]. Arbor Networks, http://www.arbornetworks.com/report, September 2007.

[2] Dittrich D. Distributed Denial of Service (DDoS) Attacks/tools [OL]. http://staff.washington.edu/dittrich/misc/ddos/.

[3] Kargl F, Maier J, Weber M. Protecting web servers from distributed denial of service attacks [A]. In Proc. International Conference on World Wide Web[C]. 2001.

[4] Hussain A, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks [A]. In Proc. ACM SIGCOMM[C]. 2003.

[5] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communications Review. 2004, 34(2): 39 - 53.

[6] Carl G, Kesidis G, Brooks R R, et al. Denial-of-service attack-detection techniques [J]. IEEE Internet Computing. 2006, 10 (1): 82 - 89.

[7] Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems [J]. ACM Computing Surveys. 2007, 39(1).

[8] 徐恪,徐明伟,吴建平. 分布式拒绝服务攻击研究综述[J]. 小型微型计算机系统. 2004, 25(3): 337 - 346.
Xu Ke, Xu Ming-wei, Wu Jian-ping. Research on distributed denial-of-service attacks: a survey [J]. Mini-micro Systems. 2004, 25(3): 337 - 346. (in Chinese)

[9] 孙知信,李清东. 路由器端防范 DDos 攻击机制综述[J]. 南京邮电大学学报. 2007, 27(1): 89 - 96.
Sun Zhi-xin, Li Qing-dong. A survey on defending DDos attack in router [J]. Journal of Nanjing University of Posts and Telecommunications. 2007, 27(1): 89 - 96. (in Chinese)

[10] Symantec Internet Security Threat Report[OL]. http://www.symantec.com/business/theme.jsp?themeid=threatreport, April 8 2008.

[11] Naoumov N, Ross K. Exploiting P2P systems for DDoS attacks[A]. In Proc. International Conference on Scalable Information Systems[C]. 2006.

[12] Bremler-Barr A, Levy H. Spoofing prevention method[A]. In Proc. IEEE INFOCOM[C], 2005.

[13] Liu X, Li A, Yang X, et al. Passport: Secure and adoptable source authentication[A]. In Proc. USENIX NSDI[C]. 2008.

[14] Lee H, Kwon M, Hasker G, et al. BASE: an incrementally deployable mechanism for viable IP spoofing prevention[A]. In Proc. ACM symposium on Information, computer and communications security[C]. 2007. 20 - 31.

[15] Duan Z, Yuan X, Chandrashekar J. Constructing inter-domain packet filters to control IP spoofing based on BGP updates [A]. In Proc. IEEE INFOCOM[C]. 2006.

[16] Wu J, Ren G, Li X. Source Address validation: architecture and protocol design[A]. In Proc. IEEE ICNP[C]. 2007. 276 - 283.

[17] SAVI WG[OL]. http://tools.ietf.org/wg/savi/.

[18] 诸葛建伟,韩心慧,周勇林,等. 僵尸网络研究[J]. 软件学报. 2008, 19(3): 702 - 715.
Zhuge Jian-Wei, et al. Research and development of botnets [J]. Journal of Software. 2008, 19(3): 702 - 715. (in Chinese)

[19] Muthuprasanna M, Manimaran G. Distributed divide-and-conquer techniques for effective DDoS attack defenses [A]. In Proc. IEEE ICDCS[C]. 2008.

[20] Sun C, Fan J, Liu B. A robust scheme to detect SYN flooding attacks[A]. In Proc. International Conference on Communications and Networking in China (ChinaCom) [C]. Shanghai, China, 2007.

[21] Broder A, Mitzenmacher M. Network applications of bloom filters: a survey[J]. Internet Mathematics. 2004, 1(4): 485 -

509.

[22] 李金明,王汝传. 基于 VTP 方法的 DDoS 攻击实时检测技术研究[J]. 电子学报. 2007,35(4):791 - 796.
Li Jin-ming, Wang Ru-chuan. Real-time detection of DDoS attack based on VTP[J]. Acta Electronica Sinica. 2007, 35(4):791 - 796. (in Chinese)

[23] Xie Y, Yu S-Z. A novel model for detecting application layer DDoS attacks[A]. In Proc. First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS '06)[C]. 2006. 56 - 63.

[24] Khattab S, Gobriel S, Melhem R, et al. Live baiting for service-level DoS attackers[A]. In Proc. IEEE INFOCOM[C]. 2008.

[25] Dixon C, Anderson T, Krishnamurthy A. Phalanx: withstanding multimillion-node botnets[A]. In Proc. USENIX NSDI[C]. 2008.

[26] Walfish M, Vutukuru M, Balakrishnan H, et al. DDoS defense by offense[A]. In Proc. ACM SIGCOMM[C]. 2006.

[27] Khanna S, Venkatesh S S, Fatemieh O, et al. Adaptive selective verification[A]. In Proc. IEEE INFOCOM[C]. 2008.

[28] Kandula S, Katabi D, Jacob M, et al. Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds[A]. In Proc. USENIX NSDI[C]. 2005.

[29] Greenhalgh A, Handley M, Huici F. Using routing and tunneling to combat DoS attacks[A]. In Proc. USENIX workshop on Steps to Reducing Unwanted Traffic on the Internet[C]. 2005.

[30] Casado M, Akella A, Cao P, et al. Cookies along trust-boundaries (CAT): accurate and deployable flood protection[A]. In Proc. USENIX workshop on Steps to Reducing Unwanted Traffic on the Internet[C]. 2006.

[31] Argyraki K, Cheriton D R. Active internet traffic filtering: Real-time response to denial-of-service attacks[A]. In Proc. USENIX Annual Technical Conference[C]. 2005.

[32] Sekar V, Duffield N, Spatscheck O, et al. LADS: Large-scale automated DDoS detection system[A]. In Proc. USENIX Technical Conference[C]. 2006.

[33] Vasudevan R, Mao Z M, Spatscheck O, et al. Reval: A tool for real-time evaluation of DDoS mitigation strategies[A]. In Proc. USENIX Technical Conference[C]. 2006.

[34] Mahimkar A, Dange J, Shmatikov V, et al. dFence: Transparent network-based denial of service mitigation[A]. In Proc. USENIX NSDI[C]. 2007.

[35] Simon D R, Agarwal S, Maltz D A. AS-based accountability as a cost-effective DDoS defense[A]. In Proc. First Workshop on Hot Topics in Understanding Botnets (HotBots '07)[C]. 2007.

[36] Wang L, Wu Q, Luong D D. Engaging edge networks in preventing and mitigating undesirable network traffic[A]. In Proc. Workshop on Secure Network Protocols (NPSec) in conjunction with IEEE ICNP[C]. 2007.

[37] Liu X, Yang X, Lu Y. To filter or to authorize: network-layer DoS defense against multimillion-node botnets[A]. In Proc. ACM SIGCOMM[C]. 2008.

[38] Yang X, Wetherall D, Anderson T. A DoS-limiting network architecture[A]. In Proc. ACM SIGCOMM[C]. 2005.

[39] Parno B, Wendlandt D, Shi E, et al. Portcullis: protecting connection setup from denial-of-capability attacks[A]. In Proc. ACM SIGCOMM[C]. 2007.

[40] Argyraki K, Cheriton D. Network capabilities: The good, the bad and the ugly[A]. In Proc. ACM Workshop on Hot Topics in Networks (HotNets-IV)[C]. 2005.

[41] Shi E, Stoica I, Andersen D, et al. OverDoSe: A Generic DDoS Protection Service Using an Overlay Network[OL]. Technical report, Carnegie Mellon University, http://reports-archive.adm.cs.cmu.edu/anon/anon/2006/CMU-CS-06-114.pdf, 2006.

[42] Ranjan S, Swaminathan R, Uysal M, et al. DDoS-resilient scheduling to counter application layer attacks under imperfect detection[A]. In Proc. IEEE INFOCOM[C]. 2006.

[43] Kuzmanovic A, Knightly E W. Low-rate TCP-targeted denial of service attacks and counter strategies[J]. IEEE/ACM Transactions on Networking. 2006, 14(4):683 - 696.

[44] Chou J, Lin B, Sen S, et al. Proactive surge protection: a defense mechanism for bandwidth-based attacks[A]. In Proc. USENIX Security Symposium[C]. 2008.

[45] Sun C, Liu B, Shi L. Efficient and low-cost hardware defense against DNS amplification attacks[A]. In Proc. IEEE GLOBECOM[C]. New Orleans, LA, USA, 2008.

作者简介:

孙长华 男,1982 年 8 月出生于湖北公安. 2004 年获西安交通大学工学学士学位,现于清华大学计算机系攻读博士学位,从事高速网络安全相关研究.
E-mail: sch04@mails.tsinghua.edu.cn

刘 斌 男,教授、博士生导师. 1964 年 7 月出生于山东潍坊. 1985 年、1988 年和 1993 年于西北工业大学获工学学士、硕士、博士学位. 1995 年至今任教于清华大学. 主要从事高速路由和交换技术、网络处理器、业务管理与测量以及高速网路安全等方面的研究工作.
E-mail: liub@tsinghua.edu.cn