

DDoS 攻击防御技术发展综述

陈飞^{1,2}, 毕小红^{1,2}, 王晶晶^{1,2}, 刘渊^{1,2}

(1. 江南大学数字媒体学院, 江苏 无锡 214122;
2. 江苏省媒体设计与软件技术重点实验室(江南大学), 江苏 无锡 214122)

摘要: 分布式拒绝服务攻击(DDoS)是当前互联网面临的主要威胁之一, 如何对 DDoS 攻击进行快速准确的检测以及有效的防御一直是网络信息安全领域的研究热点。从早期的集中式防御技术, 到以云计算、SDN 为基础的综合型防御体系, 针对 DDoS 攻击各个时期的相关防御技术进行了总结。结合 DDoS 攻击的特性, 系统地分析了各类防御机制在不同应用场景中的优点和潜在问题, 为下一代网络安全体系构建提供新的思路 and 参考。

关键词: DDoS 攻击防御; 云计算; SDN; 分布式网络

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00202

Survey of DDoS defense: challenges and directions

CHEN Fei^{1,2}, BI Xiao-hong^{1,2}, WANG Jing-jing^{1,2}, LIU Yuan^{1,2}

(1. School of Digital Media, Jiangnan University, Wuxi 214122, China;
Jiangsu Key Laboratory of Media Design and Software Technology, Wuxi 214122, China)

Abstract: The distributed denial of server (DDoS) attack is a major threat to the Internet. Numerous works have been proposed to deal with this problem through attack detection and defense mechanism design. A survey was presented to introduce the DDoS defense technologies, from the traditional strategies, through Cloud-based systems, toward SDN-based mechanisms. According to the characteristics of DDoS attack, the features and drawbacks of these systems were discussed, which could provide new insights for the development of the new generation of network security framework in the future.

Key words: DDoS defense, cloud computing, software-defined network, distributed networks

1 引言

Internet 的迅猛发展极大地推动了全球信息化进程, 然而其背后的网络安全形势也日益严峻。在各类安全威胁中, 以分布式拒绝服务(DDoS, distributed denial-of-service)攻击的危害尤为显著^[1]。

攻击者通过控制网络中不同位置的多台主机同时向受害者实施攻击, 利用资源的不对称, 产生庞大的攻击流量造成服务瘫痪, 从而阻止合法用户正常访问目标服务。

近年来, DDoS 攻击愈演愈烈, 无论受控主机还是攻击对象, 都日益呈现出大规模化和多样

收稿日期: 2017-04-05; 修回日期: 2017-08-18。通信作者: 陈飞, chenf@jiangnan.edu.cn

基金项目: 国家自然科学基金资助项目(No.61602214); 江苏省自然科学基金资助项目(No.BK20160191); 国家科技支撑计划基金资助项目(No.2015BAH54F01); 江苏省普通高校专业学位论文实践创新计划基金资助项目(No.SJZZ16_0218)

Foundation Items: The National Natural Science Foundation of China(No.61602214), The Natural Science Foundation of Jiangsu Province(No.BK20160191), The National Science and Technology Support Program of China(No.2015BAH54F01), Research Innovation Program for College Graduate of Jiangsu Province(No.SJZZ16_0218)

化的态势^[2,3]。在 DDoS 攻击中,被控制的主机称为傀儡机,而由傀儡机组成的网络称为僵尸网络。利用僵尸网络和攻击对象之间的资源不对称性,DDoS 攻击可以产生庞大的攻击流量,造成严重的破坏效果。一方面,僵尸网络中受控主机数量和规模越来越大。据调查,全世界接入 Internet 的主机中大约有 40%是傀儡机,每天约有 75 000 台活跃的傀儡机被检测到,而中国拥有的傀儡机数量约占全世界总数量的 13%,是最大的僵尸网络受害国。另一方面,随着信息化技术,尤其是物联网的普及,僵尸网络的主机种类越来越多。美国电信商 Verizon 在 2017 年的安全报告中揭露了一所美国大学遭到 DDoS 攻击的案例,起初该校校园网络速度明显变慢,后来发现学校的域名服务器(DNS)有大量异常的域名查询,最终追查发现这些查询来自校内约 5 000 台的物联网装置,包括路灯、自动贩卖机等设备组成的僵尸网络。与此同时,DDoS 攻击对象的种类也日益广泛,大到骨干网链路、DNS 服务器,小到普通的主机,都可能成为攻击对象。Arbor Networks 公司 2009 年的网络安全报告指出,DDoS 攻击的能力正在逐年增长,其中 2009 年出现的最大 DDoS 攻击流速达 49 Gbit/s,超过了当时同步光纤网的最大信道带宽 40 Gbit/s;2010 年我国发生的一起针对“456 游戏”网站的攻击事件中,攻击流速峰值高达 100 Gbit/s;2014 年阿里云遭受了全球互联网历史上最大规模的一次 DDoS 攻击,攻击峰值流量达 453 Gbit/s;2016 年 10 月 21 日美国东部时间 7:00,美国最主要的 DNS 服务商 Dyn 遭大规模 DDoS 攻击,导致 Twitter、Spotify、Netflix、AirBnb、CNN、华尔街日报等数百家网站无法访问。媒体将此次攻击称作是“史上严重 DDoS 攻击”,攻击行为来自超过 1 000 万 IP 来源,并创下了 1 Tbit/s 的 DDoS 世界记录。

作为当前 Internet 面临的最重要安全威胁之一,频繁出现的 DDoS 攻击事件给全社会造成了重大经济损失。面向 DDoS 攻击的防护技术逐渐得到学术界和工业界的广泛关注,成为网络安全领域的研究热点。目前,已有的 DDoS 攻击防御方法主要包括攻击检测和攻击响应 2 方面。本文从分析 DDoS 攻击的特性入手,总结各个阶段的 DDoS 攻击防御的

关键技术和存在问题。

2 DDoS 攻击

在多种网络安全威胁中,拒绝服务(DoS, denial of service)攻击的危害一直被广泛关注。本节首先对 DDoS 攻击实施的原理进行介绍,然后根据不同的攻击方式进行分类阐述。

2.1 攻击技术简介

DoS 攻击源于 20 世纪 80 年代,是一种阻止合法用户正常访问目标网络的攻击,其实质是攻击者对受害者的资源压制^[3]。随着硬件技术的发展,网络设备的存储与处理能力得到了显著提升,传统的点对点的 DoS 攻击很难再对攻击对象的网络服务产生明显影响。为了达到攻击目的,攻击者往往通过控制网络中大量分布式的傀儡主机同时向受害者发起攻击,因此又被称为分布式拒绝服务攻击。本质上来看,DDoS 是一种大规模的 DoS 攻击,它直接或间接地通过互联网上被控制的设备攻击目标系统^[4]。与 DoS 攻击一次只能采用一种攻击方法攻击一个目标的方式有所不同,DDoS 攻击可以采用多种 DoS 攻击方法,也可以同时攻击多个目标。攻击发生时,攻击者利用成百上千个受控节点向目标系统发动 DoS 攻击,通过消耗目标系统的网络带宽、CPU 和内存等主机资源使其性能急剧下降甚至发生崩溃,从而无法对用户提供服务。与 DoS 攻击相比,DDoS 攻击的破坏性更强,涉及的范围更广,防御的难度也更大。

DDoS 攻击流程如图 1 所示,完整的 DDoS 攻击包含攻击者、攻击控制机、攻击傀儡机以及攻击目标 4 类参与主体。其中攻击者主机由真实攻击者操作,是攻击指令源。在整个攻击过程中,攻击者主机与目标主机没有直接交互,而是利用攻击控制机和攻击傀儡机发起 DDoS 攻击。攻击控制机是攻击者控制攻击傀儡机发起 DDoS 攻击的跳板,有助于隐藏攻击者的真实身份,从而实现攻击者主机与傀儡机之间的命令与控制通信,如发布攻击指令、更新傀儡机的攻击工具、更改僵尸网络通信机制等。攻击傀儡机是真正发送大量攻击流量的攻击源,由传统的主机逐渐发展为包含智能手机在内的多种无线设备。

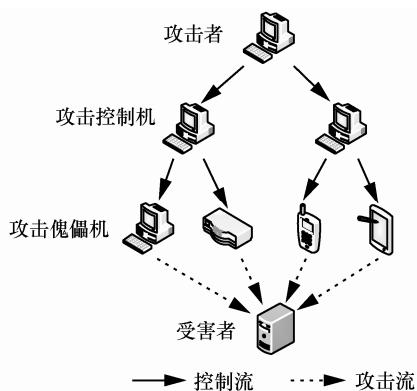


图1 DDoS 攻击组成

2.2 攻击方式分类

多年来,研究者对DDoS攻击提出了不同的分类方法^[5,6]。其中,最普遍的是根据攻击对象的协议层进行划分,大致可以将DDoS攻击分为2种类型。1) 网络/传输层的DDoS攻击,又称为网络带宽耗尽型攻击。攻击者操纵攻击源向目标网络发送大量的垃圾流量,致使其可用带宽急剧降低,从而导致目标主机无法与外界进行正常通信,常见的手段有TCP SYN洪流、UDP洪流,以及ICMP洪流等。2) 应用层的DDoS攻击,又称为基于主机资源耗尽型攻击,利用目标主机提供的网络服务以及网络协议的某些特性,发送超出目标主机处理能力的伪服务请求,大量占用目标主机的系统资源(包括CPU、Sockets、内存、数据库等),导致其丧失响应正常服务请求的能力。该类型攻击通常利用HTTP、DNS,以及SIP等方式,其中以通过HTTP发起的DDoS攻击最为常见,具体又包含访问请求洪流攻击、非对称攻击,以及重复单次攻击等手段,如表1所示。由于攻击者模仿正常用户的访问请求,攻击的Sessions很难与正常用户区分,此外,很多DDoS攻击者采用慢速请求的方式,在延长系统等待时间的同时逃避防御系统的检测。从发展现状来看,DDoS攻击一方面将更多地采用合法的协议或服务构造攻击,

表1 常见的通过HTTP发起的DDoS攻击

DDoS攻击类型	描述
访问请求洪流攻击	攻击者在应用层的Session里加入大量的访问请求
非对称攻击	攻击者发送高任务量的请求,加重服务器计算或数据库查询的负载
重复单次攻击	将请求任务分发到多个Session,并提高Session发送量

从而使攻击更加隐蔽,也更具破坏性;另一方面攻击者会不断地采用更加复杂的欺骗技术,以躲避各类防御系统的检测。

3 DDoS 防御技术概述与分类

DDoS防御一直是网络安全领域的研究热点,但至今仍然缺乏一种方法可以有效地杜绝DDoS攻击的泛滥和危害。除了DDoS攻击隐蔽性的特点,目前整个因特网环境自身结构复杂、管理松散、子网间缺乏有效的合作,从而限制了各种防御机制的实施。从防御的过程来看,大致分为攻击检测和攻击响应2个步骤:首先,攻击检测是防范DDoS攻击的第一步,其主要任务是发现网络中的DDoS攻击,产生报警;其次,攻击响应将采取措施尽快恢复受害者正常工作能力,并进一步追踪溯源DDoS攻击的发起者。

3.1 攻击检测技术

DDoS攻击流检测通过收集和分析被保护网络系统的信息,实时发现网络中存在的DDoS攻击行为。目前,大多数攻击检测机制都将攻击特征、拥塞模式、协议和源地址作为检测攻击的重要依据,从检测模型上大致可以分为误用检测和异常检测两类。攻击误用检测是将采集并提取到的用户行为与已知的DDoS攻击进行特征匹配;而DDoS攻击异常检测是通过建立目标系统及用户的正常行为模型,监测系统 and 用户的活动是否偏离该模型,从而判断是否存在攻击。误用检测和异常检测各具优缺点。前者能够准确识别已知攻击,但无法有效应对未知攻击,并且需要不断更新攻击特征库;后者通用性强,能够识别多类攻击,但容易产生误判。

一般而言,根据部署位置的不同,DDoS检测策略可以分为源端检测、末端检测、中间网络检测以及混合型分布式检测,如表2所示。源端检测策略一般部署在用户本地网络的接入路由器,能够在源端及早地阻止攻击行为,从而避免造成过多的资源浪费^[7,8]。另外,由于DDoS攻击可能在不同区域发起,单一区域的攻击流量没有形成规模时往往难以被检测到,而且在大范围部署时成本会大大提高。相对而言,末端检测机制运行在服务端,在提高检测精度

表 2

DDoS 攻击检测

检测机制	准确度	时效性	通信开销	部署成本	代表方案
源端检测	低	高	较低	较高	MULTOPS ^[7] 、D-WARD ^[8]
末端检测	高	低	低	低	IP Traceback ^[9] 、主动检测 ^[10]
中间网络检测	较高	较高	高	高	路由报文过滤 ^[11,12]
分布式型检测	高	高	较高	较高	ACC ^[13] 、StopIt ^[14]

的同时降低了部署开销,但其滞后性导致无法对攻击流量及时有效地处理^[9,10]。结合前两者的特点,研究者开始考虑基于中间网络的防御机制作为折中方案,通过部署在传输路径中的路由器,建立多点的流量检测分析模型实现攻击检测以及快速的响应^[11,12]。与此同时,如何降低多路由器协作所导致的计算存储负载和传输开销也逐渐成为未来方案设计的重点问题,尤其在高额攻击流量情况下防御机制本身的通信能力也成为需要考虑的因素。

近年来,随着网络分布式计算的发展,DDoS 攻击检测方面的研究思路逐渐从集中式单点检测向分布式检测方案转变,后者更符合 DDoS 攻击的分布式特点,逐渐成为应对 DDoS 攻击的最有效方案之一^[13,14]。例如,文献[15]提出了基于全局网络的 DDoS 检测方法,通过由多个分布式的处理单元采集以其所在位置为目的端的 OD (origin-destination) 矩阵,从而检测以该节点为攻击目标的 DDoS 攻击。文献[16]提出了基于流量控制技术的分布式 DDoS 攻击检测框架,从受害者网络、受害者上层网络和受害者 ISP 这 3 个层次着手,利用管理中心、入侵检测模块和分组分析模块实现 DDoS 攻击的分布式检测和攻击流量过滤。文献[17]利用移动 Agent 技术提出一个全面、主动、具备攻击缓解功能的 DDoS 防御模型。总体而言,相对于集中式的单点检测,分布式的混合型机制能够利用位于网络中不同位置的节点进行全面的攻击检测和响应,从而尽早确认攻击流量并在源端进行防御。同时,在构建分布式的混合型防御体系过程中,节点间的信任机制、通信负载和计算复杂度,以及系统自身的健壮性等问题仍有待进一步探讨。

3.2 攻击响应技术

攻击响应是 DDoS 攻击发起之后,对网络流

量进行适当的过滤或限制等措施,尽量降低到达攻击目标主机的攻击流量,缓解拒绝服务攻击的影响。攻击响应的最基本技术包括报文过滤、速率限制、攻击容忍和攻击溯源 4 个方面。

1) 报文过滤技术针对地址欺骗的 DDoS 攻击,通过检测报文源 IP 地址真实性并过滤源地址欺骗报文进行防御^[18,19]。位于末端网络的分组过滤主要利用路由器中的访问控制列表功能过滤地址伪装特征明显的分组。

2) 速率限制通过抑制可疑攻击流的发送速率,避免大量报文拥塞链路或淹没攻击受害者^[13,20]。对于速率限制而言,在最大限度地抑制攻击流的同时,将对正常用户的影响降低到最小。此外,还要避免因实施速率限制而带来的过多处理开销。

3) 攻击容忍的目的是缓解 DDoS 攻击对目标系统的影响,尽可能地维持系统服务的继续进行,但本身并不能阻止 DDoS 攻击^[21,10]。目前常用的攻击容忍手段主要有随机丢弃、“蜜罐”系统和负载均衡等。

4) 攻击溯源的作用是追踪发起 DDoS 攻击的真正攻击者,为攻击响应机制提供真实的攻击源位置及攻击路径信息^[22,23]。常见的 IP 追踪技术包括链路测试、基于覆盖网溯源、基于 ICMP 的攻击溯源、基于 IPsec 的追踪,以及基于分组标记和日志记录的报文追踪方法。一般而言,不同的响应策略可以与攻击检测策略搭配实施,并在实际部署应用中具有不同的作用,具体如表 3 所示。

4 云环境下的 DDoS 防御

借助于云计算技术所提供的灵活便捷的全球化服务,越来越多的企业和组织选择将其应用迁移到云环境中执行。然而,云数据中心所支撑的在线业务的高速增长促使了以恶意竞争为目的的

表 3

DDoS 攻击响应策略

攻击响应技术	优点	缺点	代表方案
报文过滤	过滤通过地址欺骗的 DDoS 攻击, 保护正常用户流量	①无法防御利用真实主机和 IP 地址的攻击; ②对检测的精确度依赖较高; ③大规模攻击时负载较高	分布式报文过滤 ^[18] 路径标识 ^[19]
速率限制	能够避免大量报文拥塞链路, 保障攻击情况下的系统正常运行	①需要大规模部署; ②可能对正常用户造成影响	Pushback ^[13] 最大最小公平限流 ^[20]
攻击容忍	尽可能维持系统的正常运行和用户的使用, 为反攻措施争取时间	①本身不能阻止 DDoS 攻击; ②需要大量的系统资源开销以维持服务正常运行	Honeynet ^[21] 负载均衡 ^[10]
攻击溯源	追踪攻击的发起者进行主动防御, 从根源上抑制攻击产生	①需要大规模部署; ②需要利用空间有限的报文头信息进行标记; ③利用大量路由存储数据分组信息	Packet marking ^[22] Logging ^[23]

DDoS 攻击, 云环境下的 DDoS 攻击频率、规模和种类以前所未有的速度快速增加, 云环境下 DDoS 攻击的安全防御也日益受到广泛关注。

一方面, 云计算的普及为 DDoS 安全防御带来了新的解决方案。与传统网络相比, 云平台通过资源池弹性提供云服务, 从资源博弈的角度, 其近乎无限的资源提供能力保证了云服务提供商通常可以投入大量的资源防御 DDoS 攻击。在企业界, 各大主流云平台逐渐推出了其安全产品, 如 Amazon CloudWatch、阿里云盾等。目前普遍采用的最基本的方式是将传统网络中的 DDoS 攻击防御手段经过适当改进, 应用在云计算环境中^[24,25]。然而, 云环境中的动态资源分配、大规模流量、虚拟化等特性使传统方法通常面临效能方面的种种问题。对此, 为满足云环境下的应用需求, 研究人员提出了一系列云特定的 DDoS 防御方法^[26]。具体而言, 在攻击检测方面, 文献[27]提出了公有云面对 DDoS TCP 洪流攻击的防御策略, 通过历史记录对来访数据分组进行分类划分, 并通过分类结果对恶意 IP 源地址进行隔离。文献[28]利用 Netflow 协议对数据流量进行采集, 并通过自我学习的方式进行 DDoS 攻击检测。针对攻击者利用云平台发起 DDoS 攻击的问题, 文献[29]结合云计算灵活部署和多租户的特性, 提出了资源限定条件下的基于虚拟机的 DDoS 系统检测机制。在攻击响应方面, 文献[30]提出了使用 fast-flux 群智网络解决云环境下的 DDoS 攻击, 在遭受 DDoS 攻击时, 该网络会自动调整结构, 从而保证提供高质量的服务。文献[31]则提出按需安全体系结构, 根据云环境下用户的个性化 DDoS 防御需求提供不同的防御服务。

另一方面, 云计算的飞速发展也给 DDoS 攻击防御带来了新的安全隐患^[32]。具体体现在:

1) 现有云平台的按需自助服务使攻击者可以在短时期内构建大规模僵尸网络发动 DDoS 攻击; 2) 云计算的泛在接入保证用户可以通过各种移动设备访问云服务, 然而绝大多数的移动设备缺乏基本安全防御手段, 容易成为黑客控制发起大规模 DDoS 攻击的潜在利用工具; 3) 云服务提供商通过虚拟化技术和多用户模型动态提供资源, 针对某一虚拟机的 DDoS 攻击会影响其相关设施的虚拟机; 4) 云计算使用“即用即付”计费模型, 从而导致攻击者将其对云数据中心的 DDoS 攻击转移至针对使用云服务用户的 EDOS (economic denial of sustainability attack) 攻击。

5 基于 SDN 的 DDoS 防御

随着软件定义网络 (software-defined network) 技术的兴起, 近年来, 研究者开始考虑利用其对数据流细粒化的控制来抵抗 DDoS 攻击^[33]。SDN 将控制层从数据转发设备中解耦合, 从而在控制层形成虚拟的网络操作系统且具有全局视图。由于所有流量均需经过控制器指定其处理规则, 因此, 便于在控制器中集成各种防御策略。

1) 基于 SDN 攻击检测机制

在大多数 SDN 防御机制中, 控制器用来检测异常流量, 过滤恶意包, 以及验证源 IP 地址的有效性。利用 SDN 对网络层的可编程性, 文献[34]设计了一种面向办公室或家庭的可编程路由器用来检测各种安全问题。通过 OpenFlow 交换机和 NOX 控制器, 实现了 4 种主流的流量异常检测以及不同的限速策略。针对来自移动端的恶意 DDoS 攻击, 文献[35]通过在入口节点使用 OpenFlow 交换机来限制流入的 IP 地址, 从而实现在线流量分析。文献[36]利用 OpenFlow 协议设

计了 VAVE 机制, 从全局角度验证源地址的有效性。文献[37]提出了一种基于分布式协作的数据流监测系统, 通过引入 SDN 在数据交换面实现自定义的动态检测。文献[38]提出了一种在 SDN 环境下基于 KNN 算法的模块化 DDoS 攻击检测方法, 通过选取 SDN 网络的 5 个关键流量特征, 采用优化的 KNN 算法对选取的流量特征进行流量异常检测。

2) 基于 SDN 攻击响应机制

基于 SDN 对数据流细粒化的控制, 在 DDoS 攻击中可以利用控制器方便地进行报文过滤、速率限制和攻击溯源。例如, 文献[39]提出了 AgNOS 架构, 包含了位于不同域的分布式 SDN 控制器, 在应对 DDoS 攻击时相互协作进行报文过滤。文献[40]讨论了在 SDN 架构中通过速率限制、事件过滤、分组丢失以及超时设置应对 DDoS 攻击。文献[41]利用 OpenFlow 控制器对数据层的转发进行记录和协调, 从而实现在 DDoS 攻击流中的溯源。文献[42]进一步提出了一种能够对抗 DDoS 攻击的软件定义安全网络机制 SDSNM, 包含由 IPv4 路由器和通信链路等组成的核心网以及由众多 SDN 子网组成的边缘网 2 部分, 利用云计算与 Chord 技术设计了原型系统, 并实现了接入管理、DDoS 审计查询、溯源操作等多种功能。文献[43]设计了控制器之间的安全协议, 使不同自治系统中的 SDN 控制器可以分享攻击的信息, 从而在源

端对攻击者进行隔离。

尽管软件定义网络给云数据中心的网络层 DDoS 攻击防御带来了诸多便利, 其本身也引入了各种 DDoS 攻击漏洞^[44]。与传统网络技术的云数据中心相比, 采用 SDN 架构的应用层、控制层、数据层三层分离, 每一层均有可能受到攻击, 潜在的受攻击平面变大, 如图 2 所示。1) 在应用层, SDN 开放的北向接口使 SDN 应用的功能日益丰富, 同时也为各种病毒、蠕虫等恶意代码提供了机会, 攻击者可以通过在应用层中植入恶意程序达到窃取网络信息, 以及占用网络资源的目的; 2) 在控制层, 攻击者可以通过高速率向软件定义网络发送新的流, 使逻辑集中的控制器的带宽资源耗尽无法与外界通信, 或者因流处理时间过长而造成控制器节点失效; 3) 在数据层, 类似于传统的 DDoS 攻击方式, 发送大量攻击流量堵塞数据传输链路或者利用协议的漏洞造成系统拒绝服务。

目前, SDN 中相关防御工作主要围绕控制层 DDoS 展开。与传统网络路由器中的规则相比, OpenFlow 协议所规定的规则更复杂。因此, 软件定义网络流表的存储能力通常很有限, 在受到数据层泛洪攻击时很容易成为性能上的瓶颈。对此, 有的研究者尝试根据 DDoS 攻击强度对网络流表处理进行任务调度, 尽可能保证系统在受到攻击情况下仍正常工作^[45]。

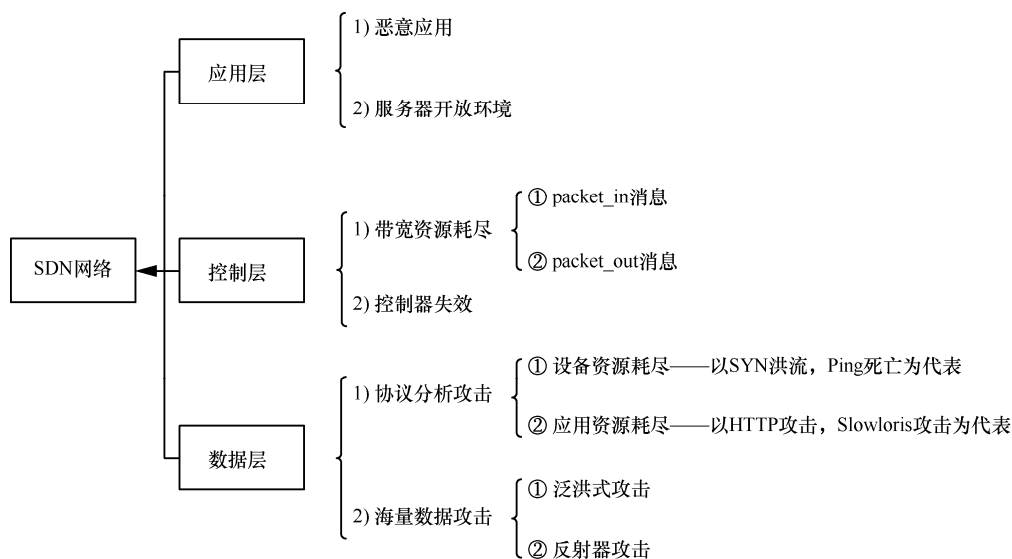


图 2 针对 SDN 网络的 DDoS 攻击

6 DDoS 防御技术分析与展望

本文对 DDoS 攻击防御中的关键技术进行了系统的分类和总结,如表 4 所示,将 DDoS 防御技术发展大致分为 3 个阶段。早期的 DDoS 防御技术主要通过部署在不同位置的网络节点,从源端、中间网络到末端节点,采用单点或组内协作的方式,因此又称为集中式防御。相对而言,基于云计算的防御策略借助于云平台的庞大资源和管理体系,从系统的角度为用户提供防范 DDoS 攻击的屏障,而且云平台可以方便地接入各种流量监控工具以及复杂的数据分析算法进行流量清洗。此外,基于 SDN 的 DDoS 防御技术体现出日益明显的优势,通过获得全局的网络拓扑和链路流量状态发现和识别网络中的恶意攻击行为并进行攻击溯源,使其能够在较小的资源消耗下更加精准地采取防御措施。然而,虽然不同的防御策略在攻击检测和响应方面各具特点,在一定程度上对某些特定场景的 DDoS 攻击起到了较好的防御效果,但在种类日益繁多的攻击手段面前,单一的防御技术仍然有局限性,而且防御机制本身可能成为被攻击对象而无法正常工作。

由于 DDoS 攻击本质上是对资源的占用,随着对系统和网络资源的管理控制手段不断完善,构建全方位多尺度的综合型防御体系已经成为未来 DDoS 攻击防御的发展趋势,这种趋势具体体现在两方面。一是部署位置的分布性上,防御机制不仅限于源端、末端或者中间网络的单点集中部署,而是更多地强调跨区域的协同性。二是不同技术的融合性上,很多传统的防御机制采用新的技术手段取得了较好的效果。例如,文献[44]研究通过 SDN 技术实现攻击溯源;文献[46]研究 DDoS 攻击下基于 SDN 的负载均衡。此外,不同技术之间配合与互补也提供了应对 DDoS 攻击新的途径。文献[47]研究了 SDN 技术和云计算相

互协作进行 DDoS 防御的策略,一方面利用 SDN 灵活的可编程性进行攻击检测和快速响应,另一方面通过云计算的资源动态部署对 SDN 提供支持。文献[48]讨论了在云环境中部署 SDN 进行 DDoS 攻击检测,以及利用云计算保障 SDN 自身的可靠性。由此可以预见,未来多尺度综合型的体系结构将成为有效防御 DDoS 攻击的重要手段。

7 结束语

长远来看,DDoS 攻击和防御仍然会处于无止尽的博弈,如何建立主动、高效、全面的防御体系,注定面临诸多困难和挑战。同时,以虚拟化、数据中心网络、SDN、大数据技术为代表的新兴技术为 DDoS 防御体系的构建带来了新的机遇和思考。未来针对 DDoS 攻击问题的解决方案有待进一步探讨,具体包含以下两方面。

1) 近年来,随着 DDoS 攻击技术的发展和攻击规模的提升,建立分布式综合型防御体系的必要性日益显著。由于传统单点部署的 DDoS 检测方法仅根据本地采集的信息检测流量异常,受限于 DDoS 攻击的隐蔽性和分散性,检测准确率不高;同时在攻击流量聚合到一定程度、距离攻击受害者较近的位置进行报文过滤,导致末端网络的网关负载过高、压力过大。新一代 DDoS 防御措施将由早期的集中式防御逐渐演化为分布式协作的网络防御体系。此外,借助于 SDN,云计算以及大数据技术形成合理有效的系统分工,对实现 DDoS 早期、高精确度的防御具有重要的研究意义。

2) 面对 DDoS 攻击,云计算平台和 SDN 应用的普及是把双刃剑:一方面,它们提供了更多的检测防御措施;但另一方面,DDoS 攻击的手段也在不断发展,越来越多的攻击开始围绕云计算平台和 SDN 展开,从而产生新的安全问题。例

表 4

DDoS 防御技术对比

防御技术	文献	攻击检测	攻击响应	协作机制
集中式防御	[5~24]	分析报文为主	报文过滤、限速等	单点/组内协作
云计算	[25~32]	分析网络流量为主	网络结构调整、隔离等	云接入点/Hypervisor
SDN 网络	[33~44]	分析流表为主	数据流过滤、溯源等	SDN 控制器/交换机

如, 云计算平台本身可能被攻击者利用成为组建僵尸网络的工具; SDN 中的应用层、控制层和数据层都有可能成为潜在的被攻击目标。因此, 综合型安全体系中各个环节之间的信任以及安全性保障又成为新的亟待解决的研究问题。

参考文献:

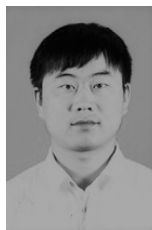
- [1] 诸葛建伟, 韩心慧, 周勇林, 等. 僵尸网络研究与进展[J]. 软件学报, 2008, 19(3): 702-715.
ZHU-GE J W, HAN X H, ZHOU Y L, et al. Research and development of Botnets[J]. Journal of Software, 2008, 19(3): 702-715.
- [2] SMITH J, SIMS J. Securing cloud, SDN and large data network environments from emerging DDoS attacks[C]//The International Conference on Cloud Computing, Data Science & Engineering. 2017.
- [3] AHMED M E, KIM H. DDoS attack mitigation in internet of things using software defined networking[J]. Proceedings of Big Data Computing Service and Applications, 2017.
- [4] HOQUE N, BHATTACHARYA D K, KALITA J K. Botnet in DDoS Attacks: Trends and Challenges[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2242-2270.
- [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] ZARGAR S T, JOSHI J, TIPPER D. A survey of defense mechanism against distributed denial of service flooding attacks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069.
- [7] GIL T M, POLETO M. MULTOPS: a data-structure for bandwidth attack detection[C]//The 10th Conference on USENIX Security Symposium. 2001.
- [8] MIRKOVIC J, REIHER P. D-WARD: a source-end defense against flooding denial-of-service attacks[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(3): 216-232.
- [9] YAO G, BI J, VASILAKOS A V. Passive IP traceback: disclosing the locations of ip spoofers from path backscatter[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 471-484.
- [10] KANSAL V, DAVE M. Proactive DDoS attack detection and isolation[C]//The International Conference on Computer, Communications and Electronics. 2017.
- [11] LU N, SU S, JING M, et al. A router based packet filtering scheme for defending against DoS attacks[J]. IEEE China Communications, 2014, 11(10): 136-146.
- [12] MIZRAK A T, SAVAGE S, MARZULLO K. Detecting compromised routers via packet forwarding behavior[J]. IEEE Network, 2008, 22(2): 34-39.
- [13] MAHAJAN R, BELLOVIN S M. Controlling high bandwidth aggregates in the network[J]. ACM Sigcomm Computer Communication Review, 2002, 32(3): 62-73.
- [14] LIU X, YANG X, LU Y. To filter or to authorize: network-layer DoS defense against multimillion-node botnets[C]//ACM Sigcomm Conference on Data Communication. 2008: 195-206.
- [15] 柳伟, 付枫, 孙鑫. 基于全局网络PCA的DDoS攻击检测方法[J]. 计算机应用研究, 2012, 29(6): 2205-2207.
- LIU Y, FU F, SUN X. DDoS detection method based on network-wide PCA[J]. Application Research of Computers, 2012, 29(6): 2205-2207.
- [16] 黄靖, 杨树堂, 陆松年. 一种基于流量控制技术的分布式 DDoS 攻击检测框架研究[J]. 计算机应用与软件, 2008, 25(6): 6-7.
HUANG J, YANG S T, LU S N. On framework of distributed DDOS attack detection based on flow control technique[J]. Application Research of Computers, 2008, 25(6): 6-7.
- [17] 田晓朋, 邬家伟, 陈孝全. 基于 DDoS 攻击的检测防御模型的研究[J]. 计算机工程与科学, 2009, 31(1): 14-16.
TIAN X P, WU J W, CHEN X Q. Research on the model of detection and defense based on DDoS attacks[J]. Computer engineering and science, 2009, 31(1): 14-16.
- [18] PARK K, LEE H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets[J]. ACM Sigcomm Computer Communication Review, 2001, 31(4): 15-26.
- [19] YAAR A, PERRIG A, SONG D. StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853-1863.
- [20] YAU D K Y, LUI J C S, LIANG F. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles[C]//The 10th IEEE International Workshop on Quality of Service. 2002: 35-44.
- [21] KIM J, SHIN S. Software-defined HoneyNet: towards mitigating link flooding attacks[C]//IEEE/IFIP International Conference on Dependable Systems and Networks. 2017.
- [22] YANG M H, YANG M C. RIHT: a novel hybrid IP traceback scheme[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 789-797.
- [23] KARASAWA T, SOSHI M, MIYAJI A. A novel hybrid IP traceback scheme with packet counters[C]//The 5th International Conference on Internet and Distributed Computing Systems. 2012.
- [24] WANG B, ZHENG Y, LOU W, et al. DDoS attack protection in the era of cloud computing and software-defined networking[J]. Elsevier Computer Networks, 2015, 81(C): 308-319.
- [25] WANG H, JIN C, SHIN K G. Defense against spoofed IP traffic using hop-count filtering[J]. IEEE/ACM Transactions on Networking, 2007, 15(1): 40-53.
- [26] PATIL S P, PATIL Y S. A survey on DDoS attacks and its defending methods in cloud[J]. International Journal of Innovative Research in Computer and Communication Engineering, 2015, 3(11): 119878-11976.
- [27] SAHI A, LAI D, LI Y, et al. An efficient DDoS TCP flood attack detection and prevention system in a cloud environment[J]. IEEE Access, 2017, 5: 6036-6048.
- [28] RUKAVITSYN A, BORISENKO K, SHOROV A. Self-learning method for DDoS detection model in cloud computing[C]//IEEE Young Researchers in Electrical and Electronic Engineering. 2017: 544-547.
- [29] WAHAB O A, BENTAHAR J, OTROK H, et al. Optimal load distribution for the detection of VM-based DDoS attacks in the cloud[J]. IEEE Transactions on Services Computing, 1939, (99): 1.
- [30] LUA R, YOW K C. Mitigating DDoS attacks with transparent and

- intelligent fast-flux swarm network[J]. IEEE Network, 2011, 25(4): 28-33.
- [31] CHEN J, WANG Y, WANG X. On-demand security architecture for cloud computing[J]. Computer, 2012, 45(7): 73-78.
- [32] SOMANI G, GAUR M S, SANGHI D, et al. Combating DDoS attacks in the cloud: requirements, trends, and future directions[J]. IEEE Cloud Computing, 2017, 4(1):22-32.
- [33] DAYAL N, SRIVASTAVA S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN[C]//The International Conference on Communication Systems and Networks. 2017: 274-281.
- [34] MEHDI S A, KHALID J, KHAYAM S A. Revisiting traffic anomaly detection using software defined networking[C]//The International Conference on Recent Advances in Intrusion Detection. 2011: 161-180.
- [35] JIN R, WANG B. Malware detection for mobile devices using software-defined networking[C]//IEEE Research and Educational Experiment Workshop. 2013: 81-88.
- [36] YAO G, BI J, XIAO P. Source address validation solution with OpenFlow/NOX architecture[C]//IEEE International Conference on Network Protocols, IEEE Computer Society. 2011: 7-12.
- [37] YU Y, CHEN Q, LI X. Distributed collaborative monitoring in software defined networks[J]. Computer Science, 2014.
- [38] 肖甫, 马俊青, 黄洵松, 等. SDN 环境下基于 KNN 的 DDoS 攻击检测方法[J]. 南京邮电大学学报, 2015, 35(1):84-88.
- XIAO F, MA J Q, HUANG X S, et al. DDoS attack detection based on KNN in software defined networks[J]. Journal of Nanjing University of Posts and Telecommunications, 2015, 35(1): 84-88.
- [39] PASSITO A, MOTA E, BENNESBY R, et al. AgNOS: a framework for autonomous control of software-defined networks[C]//IEEE International Conference on Advanced Information Networking and Applications. 2014: 405-412.
- [40] KLOTI R, KOTRONIS V, SMITH P. OpenFlow: a security analysis[C]//IEEE International Conference on Network Protocols. 2014:1-6.
- [41] WUNDSAM A, DAN L, SEETHARAMAN S, et al. OFRewind: enabling record and replay troubleshooting for networks[C]//Usenix Conference on Usenix Technical. 2011:29-29.
- [42] 王秀磊, 陈鸣, 邢长友, 等. 一种防御 DDoS 攻击的软件定义安全网络体制[J]. 软件学报, 2016, 27(12): 3104-3119.
- WANG X L, CHEN M, XING C Y, et al. Software defined security networking mechanism against DDoS attacks[J]. Journal of Software, 2016, 27(12): 3104-3119.
- [43] HAMEED S, KHAN H A. Leveraging SDN for collaborative DDoS mitigation[C]//The International Conference on Networked Systems. 2017.
- [44] FRANCOIS J, FESTOR O. Anomaly traceback using software defined networking[J]. International Workshop on Information Forensics & Security, 2014.
- [45] YAN Q, GONG Q, YU F R. Effective software-defined networking controller scheduling method to mitigate DDoS attacks[J]. Electronics Letters, 2017, 53(7):469-471.
- [46] BELYAEV M, GAIVORONSKI S. Towards load balancing in SDN-networks during DDoS-attacks[C]//IEEE Science and Technology Conference. 2015:1-6.
- [47] JESUS W P D, SILVA D A D, JUNIOR R T D S, et al. Analysis of SDN contributions for cloud computing security[C]// IEEE/ACM International Conference on Utility and Cloud Computing. 2015: 922-927.
- [48] YAN Q, YU F R. Distributed denial of service attacks in software-defined networking with cloud computing[J]. IEEE Communications Magazine, 2015, 53(4):52-59.

作者简介:



陈飞 (1984-), 男, 山东泰安人, 博士, 江南大学讲师, 主要研究方向为云计算、计算机网络。



毕小红 (1989-), 男, 山西长治人, 江南大学硕士生, 主要研究方向为网络虚拟化技术。



王晶晶 (1996-), 女, 江苏扬州人, 江南大学本科生, 主要研究方向为 SDN 网络。



刘渊 (1967-), 男, 江苏无锡人, 江南大学教授, 主要研究方向为网络流量分析和数字媒体软件。