第 43 卷 第 12 期
2020 年 12 月

计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS

Vol. 43 No. 12
Dec. 2020

云计算中 DDoS 攻防技术研究综述

岳 猛 王怀远 吴志军 刘 亮

（中国民航大学电子信息与自动化学院 天津 300300）

摘 要 云计算是一种服务模式的革新，它将物理资源（例如，计算资源、存储资源、数据资源）集中化，并通过网络以按需的方式提供给用户. 云计算面临诸多安全挑战（例如，数据隐私、资源管理），其中分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是主要的安全威胁之一. DDoS 攻击严重影响了云计算的连续性和可用性. 尽管 DDoS 攻击早已在传统网络中盛行，但云计算的应用给 DDoS 攻防带来了全新的挑战和机遇. 一方面，云计算赋能攻击. 云计算的大规模和集中化将传统攻击进一步放大. 此外，云计算本身的漏洞被用于组织新型的攻击. 在上述情况下，传统的防御技术难以应对云计算中大规模、多样化、复杂化的 DDoS 攻击. 另一方面，云计算赋能防御. 云计算丰富的资源结合新技术（例如，软件定义网络、自动伸缩）可保证自身的安全以及向用户提供云安全服务. 充分利用云计算的新技术抗 DDoS 攻击是目前的发展趋势. 云计算中的 DDoS 攻击引起了广泛的关注. 许多研究工作致力于揭示新的漏洞或设计有效的抗 DDoS 方案. 为了使相关研究人员能够全面了解最新的研究进展并激发他们开发新的方案应对各种 DDoS 攻击，本文对现有研究进行了广泛调研形成综述. 首先，我们总结了云计算在技术和服务上存在的漏洞，并进一步揭示了攻击者如何利用这些漏洞发起 DDoS 攻击. 接下来，我们描述了云计算中 DDoS 攻击的组织方式. 此外，我们还分析了云计算中各种 DDoS 攻击的原理，并根据攻击速率将其分类. 然后，我们给出一个 DDoS 防御的总体架构. 基于此，我们从攻击预防、攻击检测和攻击缓解三个方面对现有的抗 DDoS 攻击技术进行了详细的分析和评估. 重要的是，我们比较了这些技术的优缺点. 除技术外，我们还简要讨论了为应对 DDoS 攻击在服务和管理上需要关注的问题. 最后，我们讨论了当前开放性的问题以及面临的挑战，并展望未来的研究方向. 希望本文能使读者更好地了解云计算中的 DDoS 攻击问题、当前已有解决方案以及未来的研究范畴，以便更有效地应对 DDoS 攻击.

关键词 云计算；分布式拒绝服务攻击；攻击防范；攻击检测；攻击缓解

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2020.02315

A Survey of DDoS Attack and Defense Technologies in Cloud Computing

YUE Meng WANG Huai-Yuan WU Zhi-Jun LIU Liang

(*School of Electronic Information and Automation, Civil Aviation University of China, Tianjin* 300300)

Abstract Cloud computing is an innovation of the service model. It centralizes physical resources (e.g., computing resources, storage resources, and data resources) and provides them to users on demand through the network. Cloud computing faces many security challenges (e.g., data privacy, resource management). Distributed Denial of Service (DDoS) attack is one of the major security threats to cloud computing. The DDoS attack seriously affects the continuity and availability of cloud computing. Although the DDoS attack has been prevalent in traditional networks, the application of cloud computing brings new challenges and opportunities to attack and defense. On the one hand, cloud computing empowers attacks. The large scale and centralization of cloud computing amplifies traditional attacks. In addition, the vulnerabilities of cloud computing itself can be exploited to organize new types of DDoS attacks. In this case, it is difficult for traditional

收稿日期：2019-09-03；在线发布日期：2020-02-16. 本课题得到国家自然科学基金（U1933108）、天津市教委科研计划项目（2019KJ117）、中央高校基本科研业务费项目（3122020076）资助. **岳 猛**，博士，副教授，主要研究方向为云计算、网络安全. E-mail：myue_23@163.com. **王怀远**，硕士研究生，主要研究方向为云计算、网络安全. **吴志军**，博士，教授，主要研究领域为网络信息安全、云计算安全. **刘 亮**，硕士，主要研究方向为网络信息安全.

defense technologies to deal with large-scale, diverse, and complex DDoS attacks in cloud computing. On the other hand, cloud computing empowers defense. The cloud computing provides large amounts of resources combined with new technologies such as Software Defined Network (SDN), auto-scaling to guarantee its own security and provide cloud security services to users. The current development trend is to take full advantage of new technologies of cloud computing to defense DDoS attacks. The DDoS attack in cloud computing has attracted extensive attentions. Currently, many researches have been devoted to exposing new vulnerabilities and designing effective anti-DDoS strategies. In order to enable researchers to comprehensively grasp the current research progress and excite them to develop new solutions against various DDoS attacks, this paper extensively reviews existing studies for a survey. First, we summarize the vulnerabilities of cloud computing in technology and service, and further reveal how to exploit these vulnerabilities to launch DDoS attacks. Next, we describe the organization approaches of DDoS attacks in cloud computing. In addition, we analyze the principles of various DDoS attacks in cloud computing and categorize them according to attack rate. Then, we present an overview of DDoS defense architecture in cloud computing. After that, we analyze and evaluate existing anti-DDoS technologies in detail from three aspects: attack prevention, attack detection and attack mitigation. The important thing is we compare advantages and disadvantages of these technologies. Beyond technology, we briefly extend our discussion on some important issues in service and management for anti-DDoS attack. Finally, we discuss current open issues and challenges, and prospect future research directions. We hope this paper can provide better understanding of the DDoS attack in cloud computing environment, current solution space, and future research scope to deal with such attacks more efficiently.

Keywords cloud computing; distributed denial of service attack; attack prevention; attack detection; attack mitigation

1 引 言

云计算安全一直受到广泛的关注. 虽然云计算下的安全问题与传统网络环境下的安全问题有相似之处,但是其特有的实现技术和运营模式,导致其面临新的安全威胁. 2016 年,云安全联盟(Cloud Security Alliance,CSA)发布了云计算面临的 12 种安全威胁[1]:数据泄露;身份、凭证和访问管理不足;不安全的应用程序编程接口;系统漏洞;账户劫持;恶意内部员工;高可持续性威胁;数据丢失;责任条款调查欠缺;滥用和恶意使用云服务;拒绝服务攻击;共享的技术漏洞.

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击一直被视为互联网面临的主要安全威胁之一[2-6]. 近年来,DDoS 攻击频发,最具代表性的攻击事件有两次,一次是 2016 年美国 Dyn 域名服务器供应商遭受大规模 DDoS 攻击,这次攻击的影响几乎波及半个美国,Twitter、GitHub、Amazon 等大型网站无一幸免. 这次事件体现出受害规模之大. 第二次是 2018 年一家名为“US-based service provider”的游戏服务商遭遇了峰值流量达 1.7 Tbps 的 DDoS 攻击. 这次事件体现出攻击速率之高. DDoS 攻击频发的原因在于,首先它作为一种破坏型的攻击,具有实施简单的特点,只需暴力式地消耗资源. 而其攻击效果又十分显著,受害者很难做出及时有效的响应,而攻击溯源也较为困难. 此外,低廉的成本是其频发的另一个原因. 从博弈的角度,攻击者只需要较小的攻击成本,就可以发动一次大规模的 DDoS 攻击. 例如,仅需 2.4 万美金便可购买 10 万台僵尸主机[7],而如此规模的僵尸网络造成的经济损失可达 44.4 万美金[8]. 云计算促使互联网业务高速增长,这些业务产生了巨大的经济效益. 随着大量用户数据和应用向云计算平台的迁移,针对云计算数据中心的攻击与日俱增,而 DDoS 正是恶意竞争者非法获利的惯用手段.

世界知名信息安全服务商 Arbor Networks 指出，几乎没有云计算平台能免遭 DDoS 攻击. 主流的云服务商(例如，Akamai、AWS、阿里云等)针对实际遭遇的 DDoS 攻击会专门发布安全报告[9-11]. 综合这些报告可以归纳出，目前攻击者仍然以实施高速率、大规模的 DDoS 攻击为主. 攻击者通常以僵尸网络和反射的方式汇聚大规模流量. 例如，阿里云声称 2019 年上半年 DDoS 攻击流量大于 50 Gbps 的事件有 5500 余次，其中 300 Gbps 以上的占 20%，同时已经连续 2 个月出现近 Tb 级的攻击. Akamai 声称 2018 年抵御了一波 1.3 Tbps 的 DDoS 攻击. 此外，云服务商也普遍指出当前 DDoS 攻击者通常利用的协议仍然是 TCP 和 UDP，而不可忽视的是应用层 DDoS 攻击呈增长趋势. 这些报告还指出 IoT 设备的增加为组织大规模 DDoS 攻击提供了便利. 例如，Mirai、Spike 等感染 IoT 僵尸网络的恶意程序已经被云服务商广泛关注.

随着越来越多的用户开始使用虚拟化数据中心和云服务，云平台的新技术和新模式带来了新的漏洞，例如防护边界降低问题[12]、虚拟化安全问题[13]等. 这些漏洞给 DDoS 攻击提供了更广阔的空间. 攻击者可以采取暴力式的淹没型攻击，这种攻击难以缓解. 攻击者也可以实施技术式的攻击，这种攻击以精准打击云计算的某种漏洞为目标，往往具有难以察觉以及对传统防御方法免疫的特点. 当前，云计算中的 DDoS 攻击防御面临着严峻的挑战.

针对愈演愈烈的 DDoS 攻击，云服务商为防御攻击提供了良好的实践范例，其应对措施可概括为以下三点：一是利用云计算本身的弹性机制，通过动态的资源伸缩来缓解 DDoS 攻击. 例如，Amazon Elastic Compute Cloud (EC2) 和 Amazon Elastic Load Balancing (ELB) 都是利用这一方法；二是采用分布式的多点防护技术，尽量将 DDoS 攻击防御推向攻击源. 例如，Akamai Prolexic Routed 将流量重定向到遍布全球的清洗中心，而 Amazon CloudFront 和 Akamai Web Application Protector 则通过内容分发网络(Content Delivery Network，CDN)，实现攻击流边缘过滤；三是运用大数据、机器学习等新技术对流量建模，快速识别恶意流量.

如何应对 DDoS 攻击一直也是学术界关心的问题，目前很多致力于云计算中 DDoS 攻击的研究已经取得一定成果. 本文主要从技术层面梳理现有的研究成果，综述云计算中的 DDoS 攻防问题，希望能为相关领域的研究者提供一定的借鉴. 本文主要贡献在于以下三点：(1) 分析了云计算下攻击者能够利用的主要漏洞，对面向云计算的 DDoS 攻击进行分类梳理；(2) 对 DDoS 攻击防范、攻击检测和攻击缓解三类技术分别进行对比分析；(3) 探讨了目前 DDoS 攻击防御中存在的问题，提出可行性建议.

本文第 2 节讨论云计算的新特征，揭示其安全隐患；第 3 节对云计算下的 DDoS 攻击进行分类评述；第 4 节对现有的 DDoS 攻击解决方案进行归纳比较；第 5 节总结当前研究中存在的问题，并展望未来研究发展的趋势；第 6 节总结全文.

2　云计算中 DDoS 攻击隐患分析

云计算的飞速发展，给互联网用户带来了诸多便利，但是云计算的新特点也暴露出一定的安全隐患，这使 DDoS 攻击有了更佳的用武之地.

2.1　新技术

(1) 数据中心网络(data center network)

数据中心网络是云计算的基础设施，而数据中心网络技术则是指数据中心的通信体系结构，通常以网络拓扑结构、路由器/交换机设备和所使用的协议来描述. 目前，云计算数据中心网络的拓扑结构种类很多[14-16](例如，树形结构、胖树形结构、VL2、雪花结构、Dcell、BCube、Helios 等)，这些拓扑结构普遍面临着带宽不足和拥塞控制的问题. 一方面，云计算数据中心通常具有百微秒级的网络时延. 按照带宽时延积规则，网络交换设备的缓存相对较小，通常只缓存几十至数百个包. 在这种情况下，带宽资源对单条流而言并不是问题. 但是，数据中心网络中同步、聚合高速率流却比较容易实现，几乎不需要任何额外的同步机制. 过高的汇聚流使得网络出现带宽不足的问题，导致临时的瓶颈，而这些瓶颈链路正是 DDoS 攻击者潜在的攻击目标. 另一方面，由于数据中心网络负载难以预测，网络实体的独立、非协作路由决策等因素，导致拥塞控制非常复杂. 攻击者可通过拥塞瓶颈链路，诱发端系统不断地进行拥塞控制. 而一旦启动拥塞控制，那么必然会影响系统服务的稳定性.

(2) 虚拟化(virtualization)

虚拟化技术将云计算平台的基础设施和各类物理资源(如 CPU、内存、网络等)动态地汇聚起来，形成多租户共享的资源池，这些资源以网络服务的方式按需提供给用户. 这种资源池化是导致 DDoS 攻

击的一个因素.当多个用户通过虚拟机共享同一主机的资源时,如果某一个虚拟机被 DDoS 攻击,那么将会导致主机上的其它虚拟机产生资源饥饿、服务不响应的问题.有研究表明,在遭受 DDoS 攻击时,在虚拟机中托管的 Web 服务性能会下降 23%,而在相同硬件情况下,托管在非虚拟化主机时,其性能只下降 8%[17].在物理服务器等底层基础设施上,系统可以通过虚拟化技术来控制分配给当前用户的虚拟操作系统及其存储和应用程序,甚至自定义虚拟网络.这种开放性使得安全性变差.例如,攻击者可以利用虚拟机分配或迁移算法来控制某一台虚拟机成为傀儡机.此外,管理程序(hypervisor)平台存在被 DDoS 攻击的可能,目前已有很多公开的 CVE(Common Vulnerabilities&Exposures)漏洞(例如,CVE-2012-2625、CVE-2010-4255、CVE-2010-4247、CVE-2010-3699),造成 hypervisor 拒绝服务.

(3)软件定义网络(software define network)

SDN 将控制平面和数据平面解耦,可以满足云计算对网络的需求,例如可编程按需定制、集中式统一管理、动态流量监管、自动化部署等.但是,SDN 本身却可能成为 DDoS 攻击的对象.SDN 架构从上到下可分为三层,应用层、控制层和基础设施层,每一层都面临 DDoS 攻击的威胁[18].首先,对于应用层的 DDoS 攻击可以以应用程序或北向 API 为攻击对象.由于应用程序或资源的隔离没有得到很好的解决,因此对一个应用程序的攻击可能会影响到其它应用程序.其次,SDN 的控制器在物理上分布式存在,而在逻辑上集中.控制层容易出现单点失效的问题,因此控制器会成为 DDoS 攻击的重点目标.此外攻击者还可以对各向 API、流表、带宽发起攻击.最后,对于基础设施层的 DDoS 攻击主要攻击对象是交换机或南向 API.例如,攻击者可以通过伪造未知流的方式,产生许多虚假流规则,进而耗尽数据层交换机的存储资源.

2.2 新服务模式

(1)弹性伸缩(auto-scaling)

弹性伸缩体现了云计算按需分配资源的特点.它是按照一定的策略自适应地调整计算资源(例如,带宽资源、存储资源、CPU 资源等),从而满足不同业务负载的需求,保证服务的正常运行.弹性伸缩以硬件虚拟化为基础,包括物理主机内的垂直伸缩和物理主机间的水平伸缩[19].如果攻击者伪造大量虚假请求注入目标机,则会导致系统的过载.之后,弹性伸缩机制被触发.系统会首先在本地资源池中寻找空闲资源来保障业务需求,即垂直伸缩.如果仍无法满足业务需求,系统会继续寻找其它具备资源的物理主机,并以新建虚拟机实例的方式,将服务迁移至新的服务器上,这即是水平伸缩.虽然弹性伸缩机制在一定程度上保证了资源数量,但其中所涉及的虚拟机过载判定,资源分配策略探测利用率、分配和激活新资源,以及在水平伸缩下,新虚拟机实例启动及虚拟机迁移等一系列复杂的处理将消耗较长的时间.因此,过于频繁的伸缩将导致服务质量的降低甚至拒绝服务.此外,从理论上来说可扩充的资源并不是无限多的,这意味着 DDoS 攻击者只要不断增大攻击流量,就可以消耗掉所有资源,仍然能达到拒绝服务的效果.而目前攻击成本廉价,组织大流量的攻击并不困难.

(2)即用即付(pay-as-you-go)

即用即付是指云计算以租赁的方式向用户提供各种资源,并按照所用资源数量的多少来计费.这种模式虽然节省了用户购买及维护物理设备的成本,但却导致了用户遭受 EDoS(Economic Denial of Sustainability)攻击的风险[20].EDoS 攻击可通过“显式”或“隐式”的形式实现.“显式”攻击是指攻击者伪装成某个正常用户向云计算数据中心服务器发送大量请求,从而造成该正常用户使用资源虚高的假象.如果系统以资源使用量计费,EDoS 攻击将导致正常用户费用增高.“隐式”攻击是利用小的请求包触发大的响应包,也可称之为放大式 EDoS 攻击.以 Web 服务为例,一个 GET 请求通常为 1024 Byte,而一个网页通常在 1 MB 以上.假设攻击者发送 GET 请求的速率为每秒一次,则每天触发的服务响应将达到 84 GB[21].如果系统以流量计费,这种攻击方式可以慢慢诱发额外流量.可想而知,这种“隐式”的 EDoS 攻击表面上看速率很低,而实际上在日积月累后同样造成巨大的经济损失.综上,EDoS 攻击主要造成了云服务提供者(cloud service provider)和云消费者(cloud customer)的经济损失.一是云服务提供者为保障自身的服务质量,不得不向云基础设施提供者(cloud infrastructure provider)支付高额的费用.二是云计算消费者面临虚假消费的问题,不得不向云服务提供者付费.

(3)多租户(multi-tenancy)

IaaS(Infrastructure as a Service)是云计算的一种服务模式.云基础设施提供者通过虚拟化技术,将不同云服务提供者的业务驻留在同一物理主机上.这种共享 IaaS 资源的模式虽然提高了硬件利用

率，但也面临存储、带宽等资源竞争的问题[22-23]. 假如有来自云计算数据中心外部的恶意用户攻击内部虚拟机，使其占用高额的资源，那么与其共享物理资源的其它租户必然受到影响. 攻击发生时，为保证服务质量，系统往往会进行虚拟机迁移，而这会导致正常租户承担高额的管理费用. 此外，如果数据中心内部某个虚拟机本身是恶意租户，或被攻击者控制，则可能导致针对数据中心外部、内部租户之间、以及虚拟机对基础设施的攻击. 而更为严重的情况是，云基础设施提供者成为 DDoS 攻击的策划者. 在利益的驱动下，它们可直接或间接（与攻击者合谋）地攻击基础设施租户. 由于物理设施、资源管理策略、资源利用率、计费模式等关键信息都掌握在云基础设施提供者手中，因此这种攻击既容易实施又难以识别和举证.

对上述安全隐患进行归纳总结，如表 1 所示. 攻击者可以利用这些安全隐患，采用不同的技术实施多样的 DDoS 攻击.

表 1　云计算的安全隐患

隐患名称		总结描述
新技术	数据中心网络	容易出现带宽不足和拥塞控制的问题，攻击者可轻易拥塞瓶颈链路
	虚拟化	虚拟机共享物理资源的竞争问题，加剧了攻击影响；虚拟化技术本身的漏洞
	软件定义网络	应用程序缺乏隔离；控制层容易单点失效；消耗基础设施资源；开放的 API 隐患
新服务模式	弹性伸缩	攻击者恶意触发弹性机制，消耗资源
	即用即付	EDoS 导致虚假付费
	多租户	受害租户消耗资源；恶意租户对数据中心内外部的攻击

3　云计算中 DDoS 攻击技术

云计算平台下组织和实施 DDoS 攻击越来越简单和多样. 虚拟机、物联网、移动端都成为僵尸程序寄宿的新宠，攻击目标可以选择应用程序、底层服务、基础设施等.

3.1　云计算中 DDoS 攻击的组织

云平台的可用资源丰富，为了快速聚集攻击流量消耗资源，攻击者通常利用分布在不同地域的僵尸网络，甚至组织与僵尸网络具有同一量级资源的攻击云[23]，从而形成超大规模的 DDoS 攻击. 典型的攻击场景如图 1 所示.

随着互联网的发展，攻击者可控制的僵尸机不再局限于 PC，任何接入网络的设备都有可能被攻击者利用来组织 DDoS 攻击.

第一，移动端引入的安全隐患日益增加. 移动互联网的快速发展，带来了设备性能的升级和各种资源的激增. 但是，大多移动设备目前的安全防护措施还有所欠缺，用户的安全意识也较为薄弱. 因此，移动端成为助力 DDoS 攻击的利器. 例如，有研究指出 Android 平台下的恶意软件可实施 DDoS 攻击[24].

第二，云平台下用户可以通过各种各样的终端访问数据中心资源，这种泛化的接入方式有利于组织大规模 DDoS 攻击. 随着智能终端、物联网的发展，攻击者选择僵尸机的范围扩大. 例如，通过僵尸摄像头发动 DDoS 攻击. 在未来，攻击者有可能利用电视机、打印机等设备组织 DDoS 攻击.

第三，僵尸云（BotCloud）的出现，极大地节省了攻击者感染傀儡机的时间和成本. 按需服务是云计算的典型特征，而发动攻击正是黑客的一种需求. 因此，出现了诸如恶意软件即服务 MaaS（Maleware as

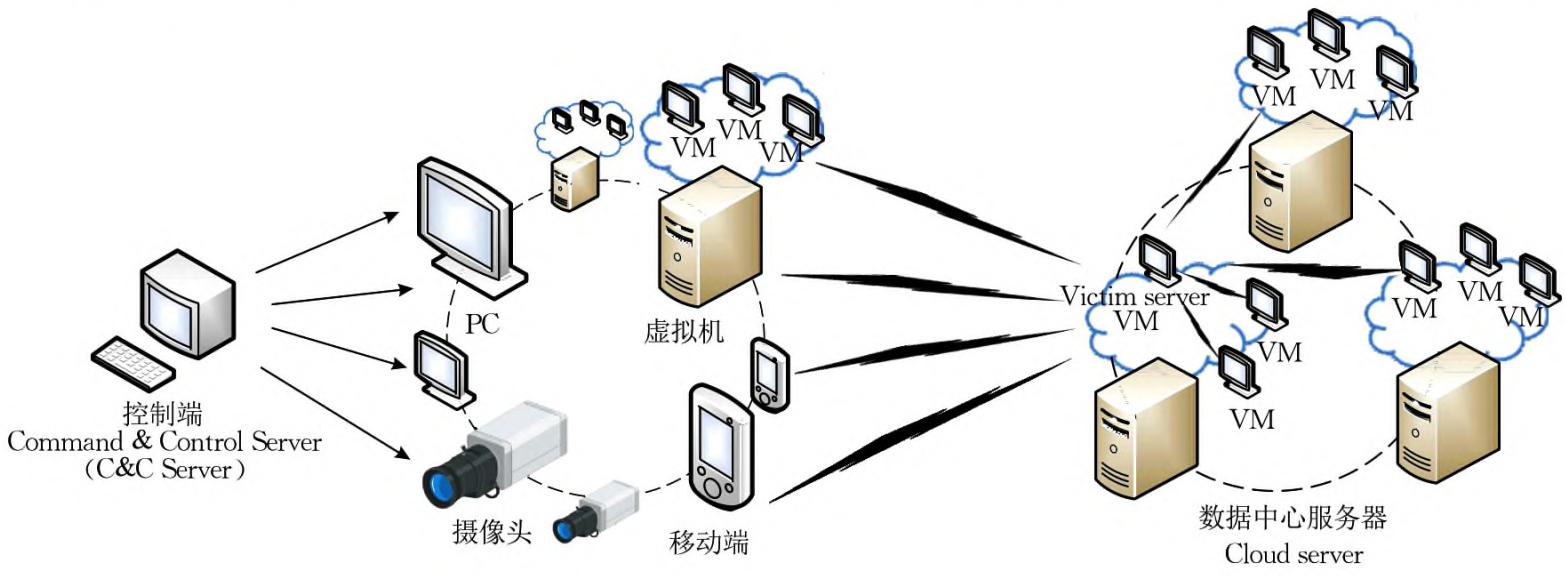

图 1　云计算下 DDoS 攻击场景

a Service)、攻击即服务 AaaS(Attacks as a Service)等黑色服务.借助于云平台感染虚拟机,出租和部署僵尸网络的黑色产业链日趋成熟[25-26].

3.2 云计算中 DDoS 攻击的分类

目前,云计算中的 DDoS 攻击主要向两个方向发展,一是将传统的攻击方式平移到云计算平台,主要采取"暴力"的方式不断增大攻击流量,消耗系统资源;二是以精准打击云计算的新漏洞为目标,在云平台上释放更"智能"的新型 DDoS 攻击.

(1)云计算中的传统 DDoS 攻击

传统网络中的 DDoS 攻击几乎可以平移到云计算平台下,攻击者可以直接利用 UDP flood、ICMP flood、Fragmentation、DNS flood、VoIP flood 等,也可以组织 Smurf 和 Fraggle 等反射或放大方式的攻击.此外,由于云计算下基于 Web 的应用较为普遍,因此 HTTP、TCP 也成为黑客重点攻击的对象.典型的有利用强制解析机制的 XML-DoS,利用 HTTP 请求机制的 HTTP get/post flood 等,以及利用 TCP 漏洞的各种 TCP flood 攻击(TCP SYN flood、TCP SYN-ACK flood、ACK & PUSH ACK flood、RST/FIN flood 等).研究上述攻击的成果较多[27-28],在此不再赘述.

(2)云计算中的新型 DDoS 攻击

DDoS 攻击分类的角度很多,传统的是从协议层的角度来分类[5,18,27].本文从攻击速率的角度进行分类,选择这个角度原因有两点:①原生 DDoS 攻击的特点是大规模流量,而目前涌现出很多低速率的 DDoS 攻击(例如,EDoS),已经成为云环境下 DDoS 攻击的一个重要分支;②在对抗 DDoS 攻击的实践中,云服务商或安全商首要关注的是攻击速率.应对高速和低速的攻击所采取的方法有所不同.以下对云计算平台特有的 DDoS 攻击进行具体分析.

第一,在云计算数据中心内部,不同虚拟机之间的泛洪式 DDoS 攻击.典型的有云滴冻结(Cloud Droplet Freezing,CDF)攻击、流表泛洪攻击、存储资源消耗攻击和 Power 攻击.

①CDF 攻击

CDF 攻击[29]会先在目标服务器集群中感染虚拟机.如图 2 所示,攻击者利用这些被感染的虚拟机之间互相泛洪发送消息(可以是同一物理主机上的虚拟机泛洪,也可以是不同物理主机上的虚拟机泛洪),来消耗集群内部通信链路的带宽资源与物理服务器的计算资源.CDF 攻击发送格式正常、源目地址真实的数据包,发送方和接收方是多对多的连接关系.CDF 攻击导致物理服务器与核心交换机的通信时延大大增加,从而导致物理服务器处理合法用户请求的能力降低,甚至被"冻结".而为了达到上述目的,攻击者还可以采取加密网络消息的方式来增加系统的负担.

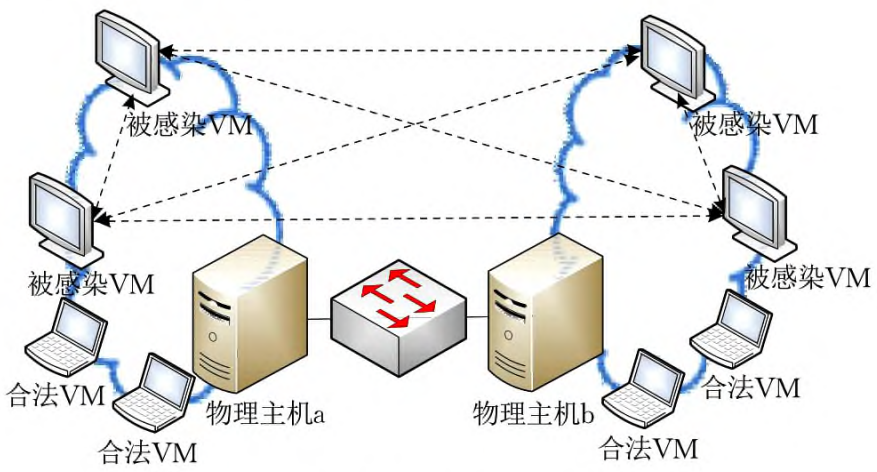

图 2 CDF 攻击

②流表泛洪攻击

流表泛洪攻击是针对 SDN 架构的一种 DDoS 攻击[30].在 SDN 应用于云计算数据中心的场景下,SDN 的控制层和数据层都有可能成为被攻击的对象,攻击模型如图 3 所示.一方面,控制器通过 OpenFlow 协议为所有流量指定流表规则.攻击者可向数据中心交换机注入大量非法的新请求,交换机会向控制器发送 Packet_In 数据包请求流规则,而处理这些数据包会大量消耗控制层资源(包括控制器本身资源以及控制器和交换机之间带宽资源).之后,如果再有合法的用户请求到来,那么控制器将无法下发对应的流规则.另一方面,交换机在流表中缓存转发规则,而流表的大小通常比较有限.因此,如果攻击目标是交换机,那么可以通过注入新的请求,使控制器向交换机发送新的流规则(通常以 Flow_Mod 数据包发送),当流规则足够多时就会占满流表.之后,合法用户的流规则无法进入流表.

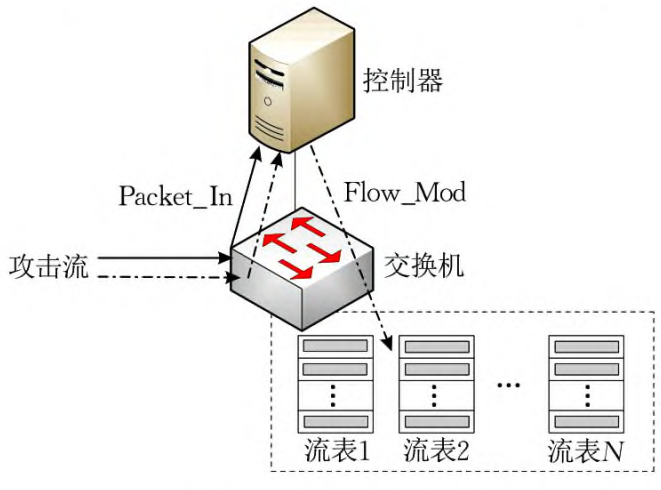

图 3 流表泛洪攻击

③存储资源消耗攻击

存储资源消耗攻击[22]专门攻击提供 IaaS 服务的云平台. IaaS 模式下，多个租户通常会驻留在一台物理主机上，共享物理资源，这些资源包括 LLC (Last Level Cache)、Bus、IMC(Integrated Memory Controller) 和 DRAM (Dynamic Random Access Memory). 在这种情况下，多租户对存储资源的竞争暴露出一定的漏洞. 如果某个恶意租户过度占用存储资源，那么与其共享物理资源的其它租户势必因资源不足而降低服务质量. 攻击模型如图 4 所示[22]. 攻击者可以采用基于存储的攻击策略，通过 LLC 清理的手段将受害者的数据从高级缓存中清除. 攻击者还可以采用基于调度的攻击策略，通过 Bus 锁定的手段，降低受害者请求被调度器处理的概率. 甚至，攻击者将基于存储的策略和基于调度的策略相结合，通过提高攻击者自身优先级或发送大量非法请求的手段占用 IMC 和 DRAM 资源.

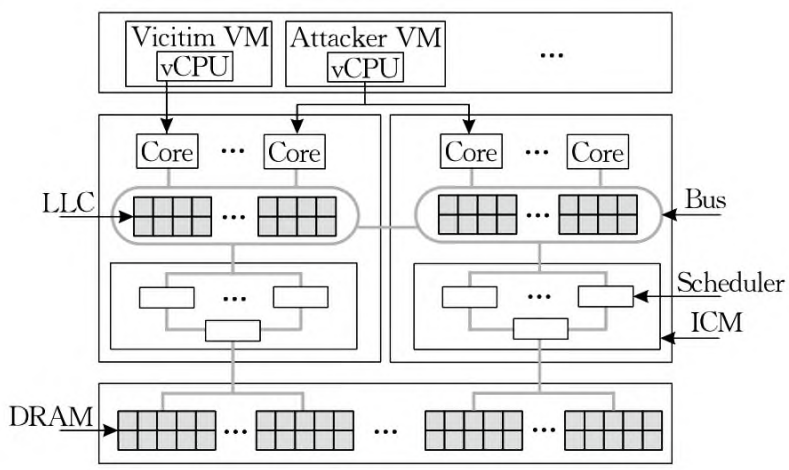

图 4　存储资源消耗攻击[22]

④ Power 攻击

Power 攻击严重威胁云计算数据中心的可用性和可靠性，电力超额认购是导致这种攻击的主要原因[31-32]. 攻击者向数据中心注入大量的恶意工作负载，迫使多台服务器同时达到功率峰值. 当功率过载时，必然会触发跳闸断电. 最终导致被害服务器因停电而终止服务. 这种攻击的实施方式很多，例如，IaaS 下虚拟机迁移、PaaS 下高性能计算、SaaS 下缓存缺失的 Web 请求都是触发高负载的典型手段.

第二，除以上泛洪式 DDoS 攻击之外，各种低速率 DDoS 攻击在云计算平台下日益流行. 主要有欺骗性资源消耗(Fraudulent Resource Consumption, FRC)攻击、Yo-Yo 攻击、流表超时攻击、带宽拥塞攻击. 对于受害者而言，遭受这类攻击的系统往往会大幅度降低服务质量. 而对于攻击者而言，使用这类攻击往往能够获得最佳的性价比，攻击者只需花费很小的代价就可以获得极其理想的攻击效果. 此外，由于这类攻击速率低，因此容易逃避检测.

① FRC 攻击

FRC 攻击是专门针对云计算数据中心的一种低速率 DDoS 攻击，主要利用云计算即用即付的计费模式实现 EDoS 的攻击效果[33-34]. 攻击模型如图 5 所示，攻击者先伪造与合法用户行为完全相同的攻击流，然后以“小而慢”的速率持续发送到数据中心. 此时，数据中心服务器会正常响应这些流量请求. 这样一来，攻击者消耗了数据中心的资源，而更重要的是这种攻击造成了合法用户使用资源的假象，从而骗取合法用户的费用.

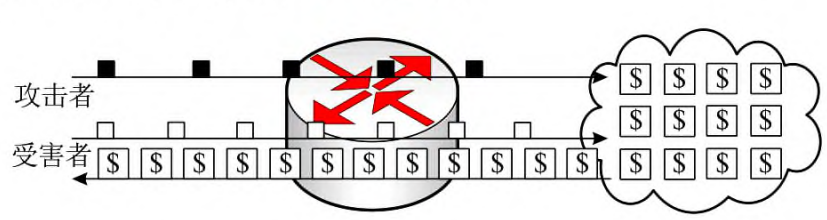

图 5　FRC 攻击

② Yo-Yo 攻击

Yo-Yo 攻击利用云计算的自动伸缩机制[35]. 攻击者周期性地发送 on-off 攻击流，使系统在 scale-up 与 scale-down 之间交替震荡. 攻击模型如图 6 所示，当 scale-up 完成时，攻击流停止(off). 当 scale-down 完成时，攻击者再次开始攻击(on)，依此类推. 这种攻击会造成受害者占用额外资源的假象，从而导致受害者不得不向云基础设施提供者付费. Yo-Yo 攻击与 FRC 攻击都属于 EDoS 范畴，但与 FRC 攻击不同的是，Yo-Yo 攻击是间歇性的攻击流，而 FRC 是以同一速率持续发送攻击流.

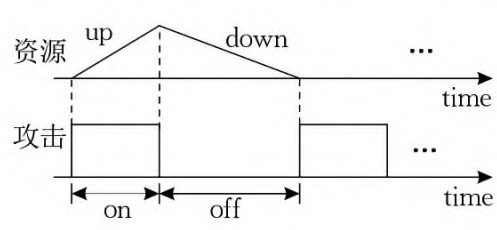

图 6　Yo-Yo 攻击

③流表超时攻击

流表超时攻击利用了 OpenFlow 协议的流表空闲超时机制[36]，攻击模型如图 7 所示. OpenFlow 协议通过设置一个空闲超时定时器来管理流表规则. 如果有数据包匹配流表规则那么定时器重置，否则如果在定时器溢出前一直无数据包匹配某个流表规则，那么该流表规则将被删除. 利用这一机制，攻击者只需按照与定时器匹配的周期注入攻击流，每当空闲超时定时器溢出前重新激活该流表规则，即可达到长期占据流表资源的目的.

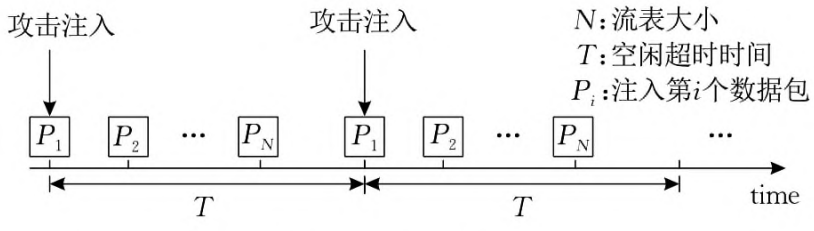

图 7 流表超时攻击

④带宽拥塞攻击

云计算下的带宽拥塞攻击是利用云计算数据中心网络架构存在的漏洞,最终导致端系统降低服务质量[37].云数据中心多租户往往共享一条网络链路,当各租户的聚合流量高于链路带宽时,就导致链路瓶颈出现.如图 8 所示,R1 路由域内各主机的汇聚带宽远高于瓶颈链路带宽,攻击者只要控制 R1 路由域下的一台主机向 R2 路由域的一台主机发送较小的攻击流,就可以拥塞瓶颈链路.此时,与攻击者处于同一路由域的其它主机成为受害者,其对外的服务质量降低.攻击流的选择,一方面可以采用传统的 UDP 流(非响应流)来拥塞链路.另一方面,利用 TCP Incast 问题,攻击者也可以发起 TCP 攻击流(响应流).

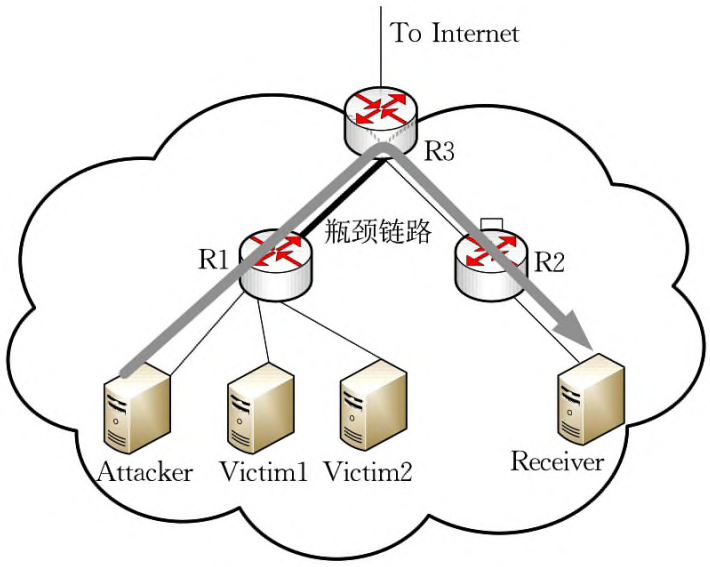

图 8 带宽拥塞攻击

以上对传统的和云平台下新型的 DDoS 攻击进行了分析.可以看出,传统网络中的各种 DDoS 攻击在云计算平台下依然有效,而专门针对云计算的 DDoS 攻击则主要是利用了云计算下的新技术、新服务模式.随着云计算中越来越多的漏洞被曝出,可以预见新型的 DDoS 攻击会层出不穷,防御 DDoS 攻击面临严峻的挑战.

表 2 对目前云计算中几种典型的新型攻击进行归纳比较.可以看出,云计算中除了持续关注高速率攻击外,低速率攻击也不可忽视.这些攻击直接威胁的目标包括云基础设施提供者、云服务提供者和云消费者,而不论哪一者被攻击都会间接影响其它两者.此外,攻击所造成的危害可能是资源消耗、经济损失或者电力过载,这体现出云计算下 DDoS 攻击效果多样化的特点.

表 2 云计算中新型 DDoS 攻击比较

名称	攻击速率		威胁目标			攻击效果		
	高速	低速	云基础设施提供者	云服务提供者	云消费者	资源消耗	经济损失	电力过载
CDF	√		√			√		
Flow table flood	√			√	√	√		
Memory flood	√		√			√		
Power attack	√		√					√
FRC		√			√		√	
Yo-Yo attack		√		√			√	
Flow table timeout	√		√		√	√		
Bandwidth congestion	√		√			√		

4 云计算中 DDoS 攻击防御技术

云计算下的 DDoS 攻击呈现出规模大和手段多的趋势,因此对防御技术提出了新的要求.目前的应对措施主要在于两个方面:一是将传统的防御方法应用于云平台;二是针对新型的 DDoS 攻击,提出专门的解决方案.

4.1 总体防御体系

云计算中 DDoS 攻击总体防御体系如图 9 所示.云计算平台包括 Internet 外部网络和数据中心内部网络.而云计算下的 DDoS 攻击一种是来自于数据中心外部,指向数据中心的攻击流.这种攻击目标较为多样,例如应用程序、底层服务、基础设施等.另一种则是爆发于数据中心内部的攻击,其攻击目标往往是内部租户.

因此,在图 9 中除了传统的在主机前或网络边界部署防御策略(例如 IDS、IPS)之外,在 hypervisor 与虚拟网络之间配置虚拟防火墙(virtual FireWall, vFW)也尤为必要.据统计来自于云计算数据中心内部不同服务器之间的流量(东西流量)占 75% 以上[38],这意味着租户之间极有可能互相泛洪形成攻

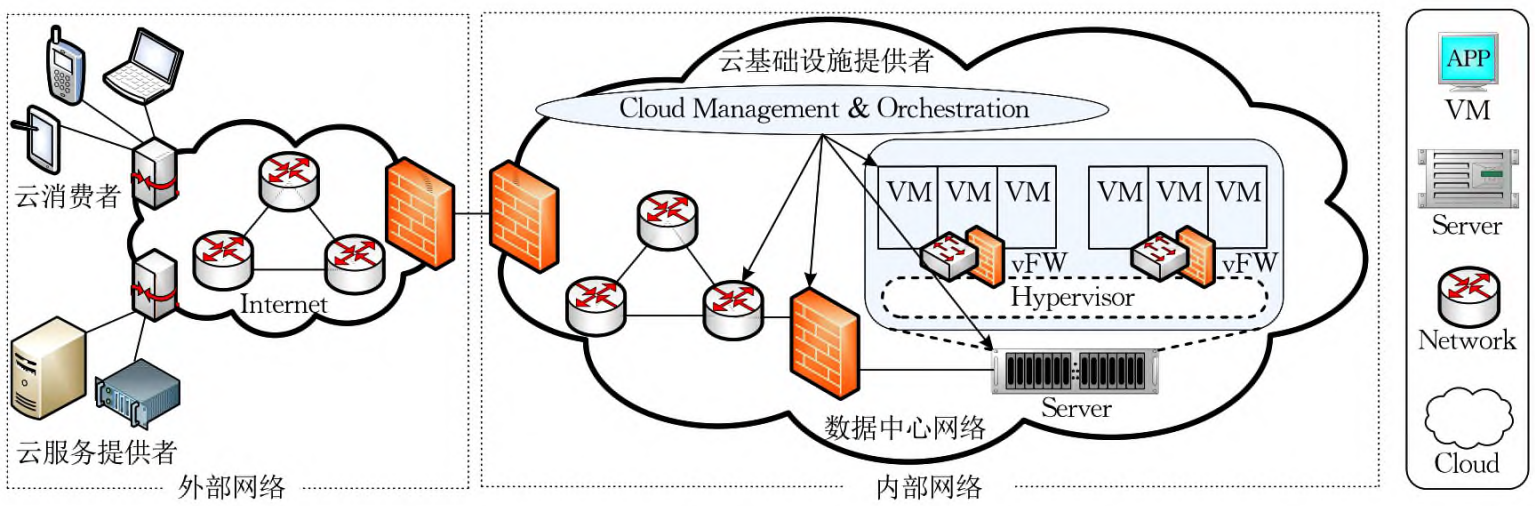

图 9　云计算中的 DDoS 攻击总体防御体系

击流，vFW 的部署可以防止数据中心内部爆发大规模 DDoS 攻击[39]. 无论 DDoS 攻击源来自何处，其应对措施一般包含三个层次，分别是防范(prevention)、检测(detection)和缓解(mitigation). 首先，攻击防范的目的是尽早发现恶意用户请求，并将其阻止在攻击源端，防止大规模攻击流的形成. 其次，攻击检测的功能是当攻击流或攻击效果已经形成后，通过特征提取判断攻击发生. 最后，攻击缓解的目的是检测到攻击后，采取一定措施最大限度地降低攻击损失，或者增加攻击者的消耗，提高攻击实施的复杂性.

此外，图 9 在逻辑层面上，将云计算中的 DDoS 攻击防范、检测和缓解技术分为 VM 级、Server 级、Network 级和 Cloud 级. VM 级解决方案包含两个方面，一方面是 VM 以受害者的角色应对来自数据中心外部的攻击. 云租户(即云服务提供者，例如一个企业租户)的应用驻留在 VM 上，可对外部服务使用者(云消费者)进行身份识别和行为检测来阻止恶意请求进入数据中心. 另一方面，VM 以攻击者的角色发起的内部攻击，可通过监视和过滤 VM 之间、VM 与 hypervisor 之间、以及虚拟网络中的异常来防御攻击. Server 级解决方案是指云数据中心的每个物理服务器可以根据主机性能指标判断是否发生 DDoS 攻击，并且可以采用资源限制和垂直伸缩的技术来缓解攻击. Network 级解决方案是指在数据中心外部网络(ISP 网络)和内部网络中可以对网络流量进行统计分析，据此进行攻击检测以及在网络边界过滤攻击流. Cloud 级解决方案由云基础设施提供者，对基础设施进行顶层管理，可获取攻击的全局视图. 云基础设施提供者可以对所有的接入用户(云服务提供者和云消费者)进行入口级过滤. 此外，水平伸缩、虚拟机迁移、资源克隆的决策也是在云级别进行. 实际应用中，上述四个级别可共享监控数据，达到协同防御的目的.

4.2　云计算中 DDoS 攻击的防范

DDoS 攻击防范的目标是尽量将攻击流遏制于源端. 目前，基于挑战/应答协议的认证技术和限制接入技术是 DDoS 攻击防范技术的两大分支，如图 10 所示.

图 10　云计算中的 DDoS 攻击防范技术

(1) 挑战/应答技术

基于挑战/应答协议的认证技术用于辨别机器行为和人类行为，目前最广泛使用的挑战/应答测试是全自动区分计算机和人类的图灵测试(Completely Automated Public Turing Test to tell computers and Humans Apart，CAPTHA)[40]. 挑战/应答的防范模型如图 11 所示，该方法根据黑白名单过滤或丢弃可疑的请求，而只允许合法请求接入数据中心. 目前，已有很多研究成果将图形测试、文本测试、密码测试、工作量证明等方法用于防范云计算下的 DDoS 攻击. 实际中，可以在接入网的边界、云数据中心的边界或由某个 VM(承载具体应用)发起挑战.

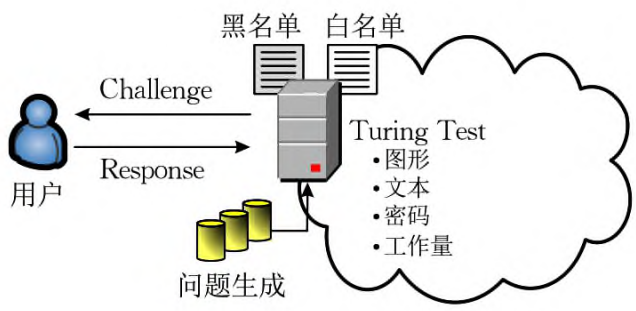

图 11　挑战/应答模型

文献[41]提出了一种阻止 EDoS 僵尸网攻击数据中心的方法，称之为 EDoS Shield. 该方法本质就是基于图形测试技术，将用户请求分为黑白名单，只有通过测试的请求才可以接入并加入白名单，未通

过的请求将被加入黑名单，以此不断更新虚拟防火墙的黑白名单列表. 图形测试的优点是辨识度较高，但缺点在于生成图形会消耗较多的资源，而存储图形需要较大的空间. 文献[42]提出了一种文本测试的方法. 该方法构造一个文本问题库对用户进行随机测试，仅允许通过测试的用户接入云平台. 此外，文章还设计了基于词汇功能语法(Lexical Functional Grammar，LFG)的问题生成模块，通过从单词池中随机选取单词再利用功能结构的语法形式组成人类容易理解而僵尸机难以理解的问题，这样一来提高了对合法用户的识别率. 文本测试的优点在于需要的资源较少，但缺点是存在字典式破解的隐患，所以必须预备大量非重复的文本问题. 文献[43]提出了一种基于密码测试的系统 sPoW(self-verifying Proof of Work)，用于防御云计算中网络层和应用层的分布式 EDoS 攻击. sPoW 通过客户端自我验证密码难题所需资源来确定用户请求优先级，从而区分 EDoS 流量和合法流量. 文献[44]采用基于密文策略属性的加密来防范 EDoS 攻击. 数据拥有者首先生成一些随机挑战明文和相应的密文. 当有用户要访问数据时，云服务器要求其解密随机选择的密文. 只有解密正确，才可授权访问. 密码测试一般会占用较多的服务器资源，这是因为服务器要对预先准备的问题进行求解. 文献[45-46]提出基于工作量证明的测试方法来识别云计算中的合法用户. 系统由防火墙、入侵防御系统和反向代理服务器组成. 防火墙对信息包的来源进行黑白名单处理，入侵防御系统以流的形式检查数据包的内容，反向代理服务器可以隐藏受保护服务器的位置. 用户只有通过测试，其请求才会被牵引至隐藏的代理服务器中. 工作量证明的方法本质上也属于密码测试的范畴，它的优点是客户端负责问题的计算，这样减轻了服务器的负担.

(2) 限制接入技术

限制接入技术用于处理用户请求，包括对用户请求的延迟、选择以及对端口的速率限制等. 如图 12 所示，实施接入限制的策略可以基于门限、基于优先级或基于模式匹配等. 而确定这些指标，通常要依据历史数据，并采用统计学习的方法进行分析建模.

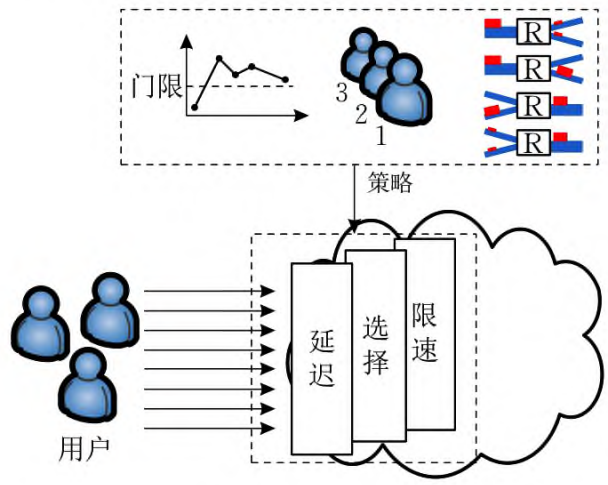

图 12 限制接入模型

文献[47-48]利用延迟接入技术来处理可疑的访问请求，当用户的访问速率高于某一门限时对其进行延时接入，门限值通常根据统计分析历史行为进行设定. 延迟的方法虽能够较为有效地防范非法接入，但门限值的选取是一个难题，如果设置不合理将导致大量合法用户的请求被一并限制. 文献[49]提出基于优先级的选择接入方法，系统首先以一定的控制算法计算允许接入的用户数量，然后按照用户信誉确定优先级，再根据优先级分配资源，信誉高的用户优先接入. 一般，用户优先级可通过浏览频率、消费记录、会话时间等历史数据确定. 选择接入的方法可能导致一定的不公平性，而且对于伪冒成正常用户的攻击者而言效果并不理想. 文献[50]提出了对端口流的速率限制方法，该方法不仅考虑端口流量的增长，还考虑端口流量增长的模式. 对路由器出口和入口的流量进行监视，如果出口流量超过门限值则认为是可疑流，对可疑流进一步结合入口匹配流量增长模式，不同的模式有不同的优先级. 优先级越高表示是 DDoS 攻击流的可能性越大，系统对该入口流优先限速. 速率限制方法同样面临公平性的问题，此外，当可测量节点较少时会出现局部匹配混淆的问题. 表 3 对上述 DDoS 攻击防范技术进行了比较.

表 3 DDoS 攻击防范技术的比较

名称	优点	缺点	基本原理	适用范围
挑战/应答[41-46]	有效的区分人类行为和机器行为，具有较高辨识度	占用资源多 难以应对字典式攻击、光学字符识别(Optical Character Recognition，OCR)攻击	接入者是否能完成测试	攻击源端 VM 级/Network 级/Cloud 级 低/高速率攻击
限制接入[47-50]	易于网络部署 可动态设置阈值 漏警时可发挥作用	无法完全阻止攻击流 可能一并降低正常用户的服务质量 对于大规模 DDoS 呈现不可扩展性	限制可疑流接入	攻击源端 VM 级/Network 级/Cloud 级 高速率攻击

4.3　云计算中 DDoS 攻击的检测

云计算中的 DDoS 攻击流多数都指向数据中心. 对于攻击检测，可以提取新的特征指标，也可以沿用传统检测方法中的一些特征指标，而检测方法部署的位置在云平台中更加多样化. 可以在数据中心外部 Internet，或内部网络节点、主机或数据中心的管理平面上部署. 通常，希望在靠近攻击端的位置尽早发现攻击，但由于尚未汇聚成较大规模的攻击流，因此特征可能并不明显. 而在靠近受害端的位置往往可以获得较好的检测效果，但缺点是发现攻击的时间较晚. 在实际应用中，为了兼顾实时性和准确性，可分布式部署入侵检测系统[51]. 目前，针对特征已知的 DDoS 攻击，往往采用特征检测法. 而对云计算中不断涌现的新型 DDoS 攻击，异常检测法较为有效，尤其适用于特征未知的攻击. 而在提取特征和构建检测模型时，往往使用网络测量、信号处理、信息度量、神经网络等技术. 图 13 将目前云计算中主流的 DDoS 攻击检测技术分为三类，检测指标包括流量、主机性能和用户行为.

图 13　云计算中 DDoS 攻击检测技术

(1) 流量检测

云计算按需服务的特点使攻击者可以快速组织起僵尸网络，向目标发送各种速率的攻击流量. 网络层流量特征的统计分析，是检测 DDoS 攻击的常用手段[52-53]，诸如端口实时速率、受害端吞吐量、路由器缓存包个数等都是反应流量特征的指标. 流量检测法的一个主要问题是如何分辨合法的闪拥(flash crowd)流与 DDoS 攻击流. 云平台下高并发的场景并不罕见，使上述问题变得尤为突出. 为此，研究者通常在流量统计的基础上，结合数据包分析(例如，源目地址/端口、TTL、TCP 标识等)来提高检测精度. 流量检测的一般流程如图 14 所示，首先是对网络流量进行采样，样本经一定的算法(例如，信号处理算法、信息度量算法等)处理后提取出特征指标，然后将特征输入到分类器模型(例如，神经网络模型、马尔科夫模型等)输出分类结果.

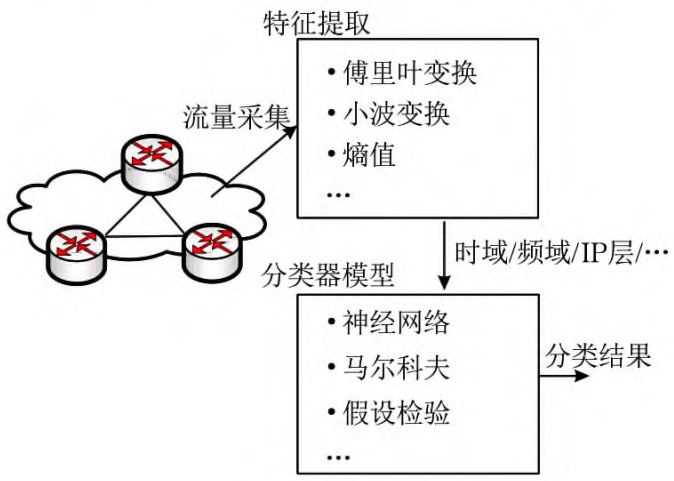

图 14　流量检测流程

文献[54]解决了传统网络中的低速率 DDoS 攻击检测问题，验证了在攻击场景中网络流量的多重分型特性，然后采用基于小波分析的 Holder 指数估计方法来反应网络流量的突发程度，当 Holder 指数高于门限值时认为发生攻击. 上述低速率 DDoS 几乎可以平移到云环境中[37,55]. 文献[55]认为攻击者可通过数据中心外部网络或感染数据中心内部虚拟机来实施低速率 DDoS 攻击. 研究者提出基于频域特征的攻击检测方法，首先在云网络的入口处捕获网络流量，然后利用快速傅里叶变换计算采样流量的功率谱，以此来检测该攻击. 文献[56]对进入受害端、流出受害端以及双向的流量进行分析，利用小波变换提取不同时间尺度上的攻击特征，并用组合神经网络来建立低速率 DDoS 攻击检测模型. 文献[57]针对云计算中 IP 地址欺骗式的 DDoS 攻击提出基于 TCP/IP 头分析的检测方法，该方法置于云数据中心的前端. 对于进入数据中心的包，通过主动和被动两种探测方式分别提取 TTL、Window size、total length 和 DF 字段，如果主被动探测的结果不匹配则判定为 IP 欺骗的主机. 文献[58]将 TTL 信息结合到 IP 黑白名单中，以此来解决 IP 地址欺骗问题. 该方法的核心思想是在一段时间内源目端 TTL 值的变化范围有限，如果超过一定阈值，则可判定为攻击端. 上述方法用于检测云计算中的 EDoS 攻击，类似地也可以通过统计跳数信息来实现[59]. 文献[60]研究了 SDN 下的 DDoS 攻击检测方法，在控制器层面统计流表信息，包括包大小、包个数、流规则、IP 地址、流速和端口. 对这些数据进行处理形成多特征，利用自组织映射(Self Organizing Maps，SOM)神经网络对输入的特征分类，以此区分合法流与 DDoS 攻击流. 对于流量检测，时域检测法对高速率的 DDoS 攻击较为有效，但对低速率 DDoS 攻击效果不好. 而频域检测法虽然适用于低速率 DDoS 攻击，但算法复杂度较高. 云计算中数据流规模较为庞大，因此需要消耗较多的资源对其进行分析. 此外，在云计算复杂的场景下，流量采集点较多(例如数据中心入口、VM、Hypervisor 等)，采集点的择优问题需要考虑. 一般而言，在受害端采集虽然特征较为明显，但存在一定的滞后性，即攻击已经成型. 在攻击源端采集，虽然能及时做出响应，但是攻

击流可能尚未汇聚,容易导致误判.而分布式的采集又会导致数据量庞大的问题.

(2)主机性能检测

受害端主机性能指标能为检测 DDoS 攻击提供一定的依据.如图 15 所示,云计算中通常需要部署监视代理器来完成对 CPU、缓存、队列、线程池、哈希表等资源的监视.检测系统会根据监视对象的响应时间、利用率、吞吐率等指标做出响应,一旦发现系统性能超出预设的阈值则判断为发生攻击.

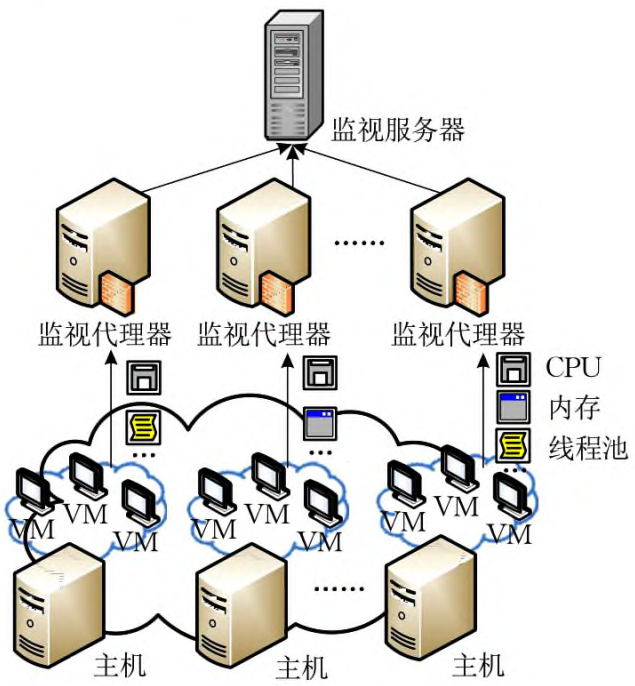

图 15 主机性能监视场景

文献[61]认为云计算数据中心应用程序对计算资源的访问(参考样本)遵循一定的概率分布,云基础设施提供商可以监视缓存(LLC 存取时间)、网络(TCP 连接建立时间)和磁盘(Disk 存取时间)的访问特征(收集样本).如果收集样本的概率分布与参考样本的概率分布相差很大,则可以怀疑某一个 VM 正在实施 DDoS 攻击.在实现上,可通过离线学习建立参考模型,通过 K-S 检验确定样本的比对结果是否落入置信区间.文献[62]提出了一种针对云计算的 SIPDAS(Slowly-Increasing-Polymorphic DDoS Attack Strategy)的攻击,并提出了基于主机 CPU 负荷的阈值检测法,该方法持续监视多个虚拟机的 CPU 负荷,当总的负荷大于门限值并且这种情况持续超过一定时间(服务商可容忍的异常状态最大时间)后判定为 DDoS 攻击.主机性能检测的一个难题在于如何选择监视对象,以及如何设置合理的阈值.首先,实时地、频繁地监视所有指标不太现实,因为这会消耗较多资源.一般而言,监视对象和阈值的选择取决于应用程序的性质、工作负载及其潜在的漏洞[62].在云计算这种高动态的环境中,如果不能自适应调节监视对象和阈值,那么将导致漏警率或虚警率上升.另外一个问题是,受害者必须在目标机上部署监视代理,而这些代理工作时又需要可扩展的资源,这在一定程度上增加了成本.

(3)用户行为检测

统计分析用户行为是较为常用的一种 DDoS 攻击检测方法,检测模型如图 16 所示.通常可从 Web 日志和用户会话来提取一定的行为特征.该方法首先依据提取的历史数据训练出一个正常行为的模型,然后将该模型用于判断当前用户行为.若当前用户行为未能与正常模型相匹配,则可判定异常.该技术比较适用于检测流量和主机特征不显著的新型 DDoS 攻击.例如,流量检测法或主机性能检测法对 FRC 攻击难以奏效,这是因为 FRC 攻击流量小,对系统资源的消耗在较小的时间尺度上也并不明显.文献[33-34]提出通过 Web 用户对云计算数据中心的访问请求是否服从“Zipf”分布可以检测 FRC 攻击.

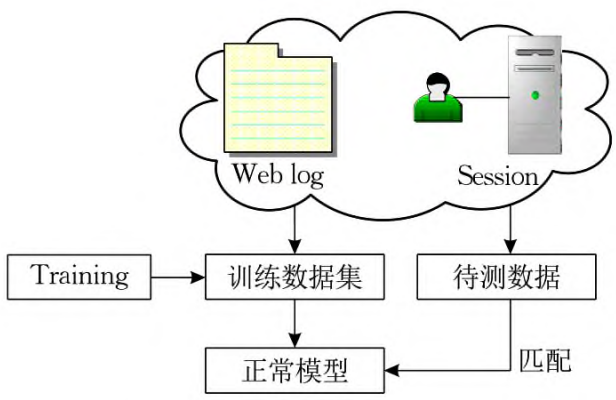

图 16 用户行为检测模型

文献[63]从 Web 日志中提取了 5 个用户行为特征(在检测窗口内用户发送的请求数、用户在此请求上持续的时间、用户请求响应成功率、用户平均请求负载、用户请求相似度),并与 5 个流量特征(检测窗口内源 IP 数量、总流量、平均流量、请求总数量、平均请求数量)相结合来提高 DDoS 攻击检测率.上述特征作为 BP 神经网络的输入,最后得到分类结果.文献[64]指出云计算中正常用户和 EDoS 攻击者在会话访问时间(Time Spent on a Page,TSP)上表现出不同的行为.如果某个用户对 Web 页面的 TSP 趋近于零,或者为一个固定值,又或者其访问行为具有周期性,则认为是僵尸主机.用户行为检测法的关键取决于建立正常行为的模型.而模型的鲁棒性受训练方法、历史数据样本等因素的影响,如果处理不好则无法保证检测效果.表 4 中比较了各种 DDoS 攻击检测技术.

表 4　DDoS 攻击检测技术的比较

名称	优点	缺点	基本原理	适用范围
流量检测[52-60]	攻击特征明显 现有算法较多，检测模型成熟 与数据包分析结合检测率高	算法复杂，待处理数据多 流量采集点选取困难	流量特征超过阈值	网络端/受害端 VM 级/Network 级 低/高速率攻击
主机性能检测[61-62]	系统破坏前能及时响应 受害端特征明显，检测率高	高动态场景，难以确定对何种资源度量何种指标 阈值选取困难 资源消耗及成本问题 难以应对低速攻击	资源使用率超过阈值	受害端 Server 级 高速率攻击
用户行为检测[33-34,63-64]	能有效检测 FRC 低速攻击 对应用层 DDoS 攻击效果明显	建模困难 难以应对应用层以下的攻击	有悖于正常用户行为模型	受害端 VM 级 低/高速率攻击

4.4　云计算中 DDoS 攻击的缓解

完全阻止 DDoS 攻击流非常困难，目前主要关注的是在检测到攻击后如何缓解攻击，最大限度地保障云计算服务质量. 用于缓解攻击的主要技术如图 17 所示. 对于来自数据中心外部网络的 DDoS 攻击，主要采用流量过滤和路径隐藏技术，在攻击流进入数据中心前进行缓解. 而在数据中心内部网络，资源重配置和 SDN 技术可以有效地应对来自内外部的 DDoS 攻击.

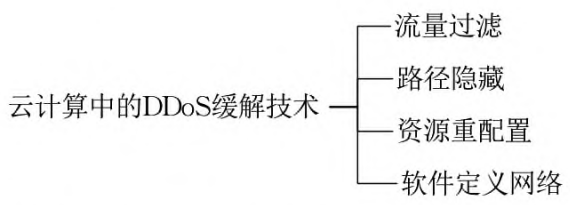

图 17　云计算中的 DDoS 攻击缓解技术

(1) 流量过滤

流量过滤技术的目的是尽量清洗掉攻击包，同时最大限度地允许合法包通过. 如图 18 所示，该方法主要基于地址、特征和异常三种策略实现过滤.

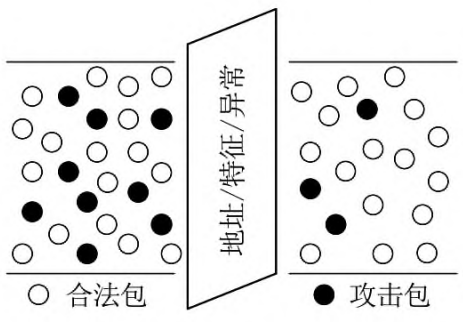

图 18　流量过滤原理

地址过滤可依据数据包的 MAC 地址、IP 地址，并结合端口号、协议号来实现. 文献[65]提出了一种分布式的源地址过滤方案，网络中的路由器相互协作，每个路由器只检查源地址中的部分比特位而不是所有位，以此提高效率. 此外，为解决存储资源成为地址过滤的瓶颈问题，该方案采取了在每个路由器分布存储黑名单的机制. 地址过滤在实施上简单、快速，可以有效地过滤攻击流. 但是，当攻击流与正常流来自同一地址时，地址过滤不得不将正常流一并过滤. 特征过滤针对与攻击特征匹配的流进行过滤，文献[66]将特征分析从时域转换到频域，发现低速率 DoS 攻击流的幅度谱集中分布在低频段. 据此，文章设计了一种梳状滤波器，在频域上过滤攻击流. 实验结果表明，该方法可以有效缓解攻击，而对合法 TCP 流量的影响很小. 特征过滤的有效性依赖于攻击特征库，对已知特征的攻击较为有效，而对于特征未入库的新型 DDoS 攻击效果欠佳. 异常过滤将有悖于正常模型的所有流量全部过滤，该方法对于已知或未知攻击特征的 DDoS 攻击均有一定效果. 文献[67]通过在 Web 服务器端统计分析用户的请求序列，来估计用户点击网页的行为. 利用隐半马尔科夫模型对请求序列进行建模(从采样的请求序列中提取网页元素标识符和标识符请求间隔作为观测向量，以不同网页的跳转表示隐藏状态转移). 最后，根据隐半马尔科夫模型中的参数，用 M 算法计算用户请求的熵值来判断用户异常行为，并进行过滤. 异常过滤的实时性通常依赖于检测时间，而正常行为和异常行为的区分往往需要经过一个较为复杂的建模过程. 此外，云计算复杂背景下，建立一个准确的正常行为模型较为困难[68-69].

(2) 路径隐藏

流量过滤是一种被动式的缓解措施，往往在攻击流出现后才能响应，且依赖于检测的精度与速度. 而路径隐藏属于一种主动式的 DDoS 攻击防御技术，通过全网节点协同工作实现分布式防御. 安全覆盖网服务 SOS(Security Overlay Services)就属于路径隐藏的一种方法[70-71]，其结构如图 19 所示. 它通过隐藏路由节点信息，增强了路由平台自身的健壮性. 合法用户通过安全节点到达服务器，由于节点角色并不公开，因此攻击者难以对安全路径上的节点发动有效的攻击.

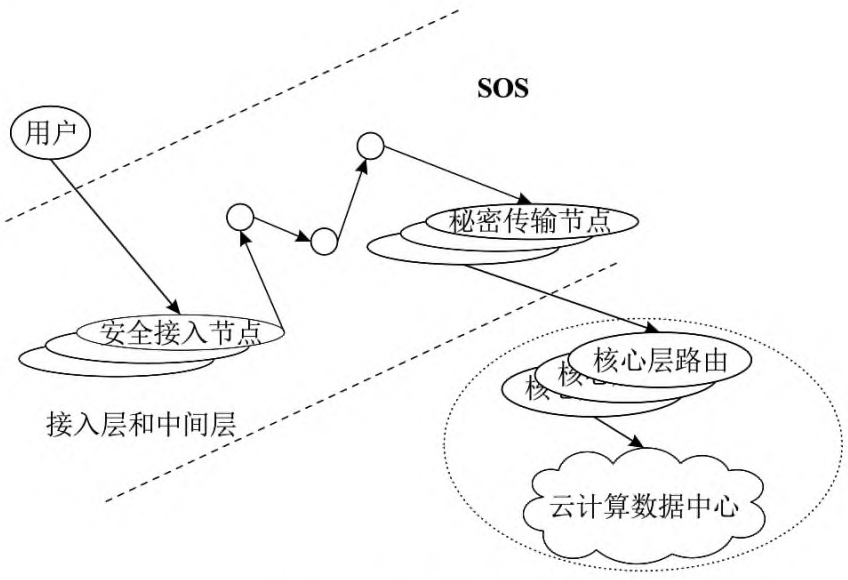

图 19 安全覆盖网结构

文献[72]提出了一种虚拟散列安全访问方法，用于构建云计算平台的 SOS，并结合云计算本身的弹性机制无缝切换安全节点，从而有效地缓解了来自云计算外部的 DDoS 攻击. 文献[73]基于云计算泛联路由架构，设计出一种安全访问路径算法 SAPA(Security Access Path Algorithm). SAPA 对传统的 SOS 进行了三点改进：第一，简化角色节点；第二，周期性更新角色节点；第三，缓存安全访问路径. 上述改进使得 SAPA 更适用于云平台下防御 DDoS 攻击. 尽管 SOS 及其变种能较好地保护云计算数据中心，但是 SOS 方法也有一定的局限性. SOS 无法应对来自覆盖网内部的攻击，难以解决安全节点的损耗问题. 路径标识 PIDs(Path IDentifiers)隐藏是一种新的 DDoS 攻击缓解方法，文献[74]指出在信息中心网络，不公开 PIDs 可以增大攻击难度，以及有效消除大量的攻击流. 但是，上述方法是建立在 PIDs 不可伪造的基础上，目前尚无方法验证 PIDs 的真实性.

(3) 资源重配置

资源重配置是在整个云数据中心层面应对 DDoS 攻击的有效手段. 云计算下的自动伸缩技术、虚拟机迁移技术、资源克隆技术、资源限制技术已非常成熟. 云基础设施提供者可采用以上技术动态地改变资源配置，来满足业务需求. 资源配置过程需要一定策略保证公平性和有效性. 总体模型如图 20 所示.

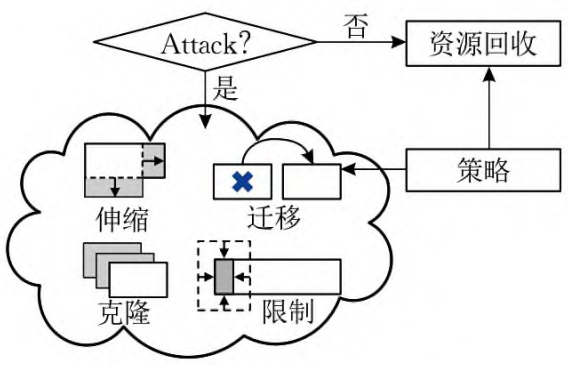

图 20 资源重配置方案

自动伸缩技术首先以垂直伸缩的方式从同一物理主机上扩展硬件资源，以缓解被害端资源不足的问题. 如果单一物理主机资源仍然难以满足服务质量，则以水平伸缩的方式跨物理主机扩展资源. 但是，该技术并不能根本解决 DDoS 攻击问题[75]. 这是因为资源扩展要考虑成本的问题，无限制地扩展资源来应对不断增强的攻击流是不现实的. 此外，自动伸缩机制存在被 EDoS 攻击的隐患. 虚拟机迁移技术首先隔离受害目标，然后将受害端承载的服务迁移到安全的虚拟机上. 这种方法可达到服务器与 DDoS 攻击隔离的效果，或者至少增加了实施攻击的难度. 这是因为攻击者不得不花费更多的代价去寻找新迁移的虚拟机. 文献[37]就利用虚拟机迁移技术来防御数据中心内部的 DDoS 攻击，首先通过可用带宽测量检测攻击，然后将受害虚拟机的业务迁移到正常虚拟机上. 虽然这种技术能够在一定程度上缓解 DDoS 攻击，但是也存在一定的问题. 例如，迁移策略寻优，业务迁移开销等[61]. 资源克隆主要是通过服务资源克隆(例如，虚拟机克隆)或防御资源克隆(例如，IPSec 克隆、IPS 克隆)来增强系统的抗 DDoS 攻击能力. 文献[76]提出了利用云计算空闲资源克隆入侵防御系统来对抗大规模 DDoS 攻击，通过排队论建立最优化资源的数学模型. 该方法可以快速过滤 DDoS 攻击包，保证合法用户的服务质量. 资源克隆技术可以比较有效地缓解 DDoS 攻击，但如何付出最少的代价保护最多的资源是一个博弈的问题[77-78]. 文献[79]提出了一种 CoFence 防御框架，其利用网络功能虚拟化(Network Function Visualization，NFV)技术和多角色 Stackelberg 博弈机制来对 DDoS 攻击进行防御. CoFence 是一种协同防御机制，它将网络中的入侵防御系统统一管理. 当某个节点遭遇高强度 DDoS 攻击时，CoFence 将攻击流重定向到邻居节点，由邻居节点的入侵防御系统协助抵御攻击. 此外，为了保证资源分配的公平有效，文章还利用 Stackelberg 博弈模型设计了一种动态分配网络资源的方案. 采用资源限制技术应对 DDoS 攻击，主要方法是在云中放置固定的资源服务器或者在每个服务器中设置资源上限. 一些供应商已经开始提供实时监控服务，对虚拟机设置资源购买和维持的最大值来进行资源限制. 文献[75]在资源扩展的基础上，提出了一种称作“Scale Inside-out”的方法来缓解 DDoS 攻击. 该方法的核心在于，攻击发生时，系统不再给受害虚拟机分配资源，而是将资源分配给其它正常用户或将资源用于攻击缓

解.这样一来可以避免资源竞争,提高攻击缓解的速度.文献[80]提出了一种资源分配策略 DARAC (DDoS Aware Resource Allocation)来缓解 DDoS 攻击.该方法可以精确快速地区分合法请求和攻击请求,通过计算合法客户的份额,来决策资源限制策略.资源限制能够降低资源动态缩放在成本上的损失,但同时也会影响云计算的按需分配功能.此外,如何判断是合法突发流量还是 DDoS 攻击流量引起的资源激增是一项比较困难的工作.

(4) SDN

SDN 应用于云计算平台,为 DDoS 攻击的检测与防御提供了极大的便利[81-84].SDN 防御 DDoS 攻击的核心架构如图 21 所示,可部署在攻击源端、网络端或云计算数据中心[18].SDN 将控制平面与数据平面解耦合,Controller 通过 OpenFlow 协议对网络进行集中地监控与管理,能够收集网络的全局信息(例如,网络拓扑、流量统计等),而不同的控制器、交换机还可协同工作[85].上述特点有利于大规模地、动态地部署安全策略.此外,Controller 提供丰富的北向接口,可以方便地开发 IDS、IPS 等应用.

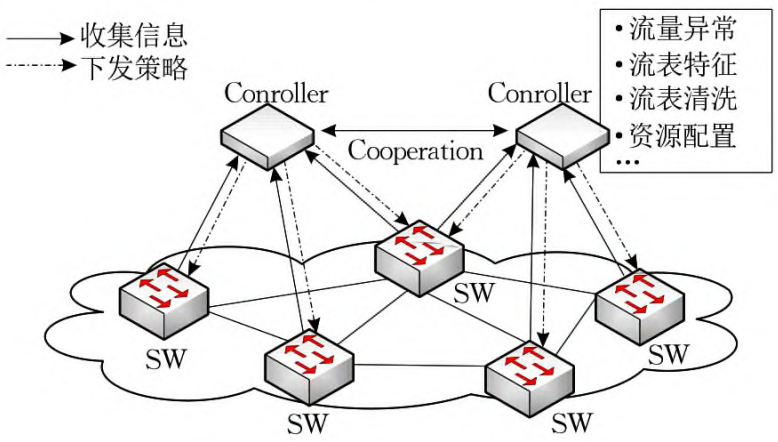

图 21　SDN 防御 DDoS 架构

文献[86]提出了一种在 SDN 网络中基于流特征值的 DDoS 攻击检测方法.作者利用 SDN 控制器的集中控制特点,提取了流表中与 DDoS 攻击相关的六元组特征值信息,以此作为判定 DDoS 攻击的依据.文献[87]在基于 SDN 的云平台下,从控制器中提取原始数据,采用一种基于支持向量机和自组织映射算法的混合机器学习模型对攻击流量进行识别,并提出一种基于历史 IP 的过滤方案来提高检测速率.文献[88]提出了一种基于调度的 DDoS 攻击防御结构,该结构可使 SDN 控制器有效地限制攻击强度,从而减轻对整个网络的影响.传统网络中,网络拓扑的动态变化影响了防御策略的部署,而 SDN 下网络虚拟与集中控制解决了上述问题,并扩大了 DDoS 攻击防御半径[89].此外,云计算的弹性机制常与 SDN 协同工作,弹性机制扩展了 SDN 控制面通信与计算的瓶颈[18].文献[89]提出了一种抗 DDoS 攻击的软件定义安全网络机制(Software Defined Security Networking Mechanism,SDSNM).该机制将 DDoS 攻击防御扩展到边缘 SDN 网络,同时继承了核心 IP 网络体系架构,因此具有增量部署特性.作者在云计算平台下,结合 Chord 技术设计实现了原型系统,实验结果表明,SDSNM 具有很好的扩展性和可用性.虽然 SDN 有助于抵御 DDoS 攻击,但 SDN 技术也存在网络单点失效的风险,其自身容易成为攻击目标[90].对上述 DDoS 攻击缓解技术进行比较,如表 5 所示.

表 5　DDoS 攻击缓解技术的比较

名称	优点	缺点	基本原理	适用范围
流量过滤[65-68]	易于网络部署 地址过滤灵活地添加或删除地址 对已知攻击特征的流过滤效果好	可能一并过滤正常流 特征过滤无法应对未知特征的攻击 异常过滤实时性欠佳	牵引清洗攻击流	攻击源端/网络端/受害端 VM 级/Network 级 高速率攻击
路径隐藏[70-74]	主动防御 能保证通信率和访问延迟	安全覆盖网内部攻击 存在安全节点消耗问题 PIDs 伪造验证问题	赋予网络节点不同角色,不公开安全路径	网络端 Network 级 低/高速率攻击
资源重配置[37,61,75-80]	运用云计算新技术有效缓解攻击 充分利用资源 易于实施	资源重配置过程开销较大 对大规模 DDoS 攻击扩展性差 难以平衡“性价比” 限制按需分配功能	动态配置资源保证服务质量	受害端 Server 级/Cloud 级 低/高速率攻击
软件定义网络[83-90]	可提供全局视图,便于集中管控 可延伸防御半径 不受网络拓扑动态变化的影响	控制器易成为新的攻击目标 本身很容易造成网络的单点失效	控制器收集全局信息,大规模部署防御策略	攻击源端/网络端/受害端 Network 级 低/高速率攻击

4.5 延伸讨论

云计算中的 DDoS 攻击防御技术目前得到了较为广泛的研究，然而仅仅依赖技术是不够的，技术结合服务及管理才能更好地防范 DDoS 攻击.

在服务层面，针对所面临的 DDoS 攻击威胁，云平台需要具备应对 DDoS 攻击的安全服务能力，重点关注以下 3 个方面：(1) 服务部署. DDoS 攻击的目标是降低服务的可用性，云上的服务需要跨可用区域部署，在 DDoS 攻击局部爆发时仍能保证服务的高可用性；(2) 服务分级. 划分服务等级(例如，相较于为企业或机构提供的其它云服务而言，云 DNS 服务的等级就相对较高，这是因为一旦 DNS 服务被攻击则全线服务不可用)，遭受 DDoS 攻击时，按服务的安全级别弹性分配资源；(3) 有损服务. 在应用服务设计时，尽量避免“单点瓶颈”导致整个系统的瘫痪，既一个系统被 DDoS 攻击下线但不影响其它系统在线服务.

在管理层面，根据 DDoS 攻击流在网络中爆发的方式，重点关注以下 4 个方面：(1) 外部用户管理. 由于外部用户泛化的接入方式，因此需要对外部用户进行严格的身份管理和接入管理，避免其成为僵尸网络，将 DDoS 攻击流引入数据中心；(2) 内部租户管理. 对数据中心内部租户而言，要严管租户身份，监控异常行为. 及时对恶意租户进行隔离，避免其对其它租户或云基础设施的攻击；(3) 虚拟化管理. 弥补虚拟化的安全漏洞，避免攻击者租用云平台虚拟机实例组建僵尸网络；(4) 第三方认证. 以行业标准为依据，开展第三方认证，提升租户和服务商的信任关系，对信任双方进行约束. 从而避免云基础设施提供商对租户进行消费欺诈式的 DDoS 攻击.

5 问题与展望

目前，对抗云计算中的 DDoS 攻击仍存在诸多问题，对于研究者既是挑战又是机会. 从技术的角度，本节首先分析当前面临的问题及可能的应对措施. 然后，展望未来的研究趋势.

5.1 问题与挑战

云计算是把双刃剑，既赋能防御，又赋能攻击. 云计算下大规模的 DDoS 攻击不停刷新速率，新型的攻击手段又不断涌现. 随着信息技术的快速发展，没有任何一个解决方案能够应对未来所有的 DDoS 攻击问题. 云计算中的 DDoS 攻击与防御将是一个无休止的博弈过程，如何快速、高效、主动地防御 DDoS 攻击，仍然面临许多挑战，有以下几个问题需要特别关注.

(1) DDoS 攻击的特征

需要关注云计算中 DDoS 攻击的以下几个重要特征：① 隐蔽性. 攻击者采用较低的攻击速率达到隐蔽的目的. 这种攻击方式往往可以逃避检测，从而长期在网络中“暗流通动”造成经济损失；② 分布式. 分布式的攻击流增大了在攻击源端检测和防范攻击的难度. 而在目标端，攻击流汇聚成极高的流量，即使能及时发现，但缓解这种攻击方式有一定的难度，对实时性也提出了挑战；③ 多样化. 云计算暴露出诸多的漏洞使 DDoS 攻击方式呈现出多样化的特点，揭示新漏洞弥补老漏洞是要解决的重点问题. 尤其关注云计算数据中心内部的 DDoS 攻击.

(2) 数据收集与分析

云计算具有大规模特性，这使得传统的数据处理方法在云计算环境下应对大规模 DDoS 攻击有一定困难. 例如，很多 DDoS 攻击防御方法以网络异常特征分析为基础，以较低开销收集与分析大规模的异构数据是面临的一项挑战. 基于大数据分析的 DDoS 攻击防御研究是当前的一个发展方向，它能够全面有效地分析大量不同的复杂数据，如事件、行为、风险等. 从而能够挖掘数据背后隐藏的模型、特征及其它信息.

(3) 算法选择与部署

云计算环境下的 DDoS 攻击复杂度更高，应用于检测和防御的算法也多种多样. 例如，小波变换、机器学习、信息度量等技术经常用于提取攻击特征，建立检测和防御模型. 但遗憾的是没有一种算法能够适用于所有种类的 DDoS 攻击. 另外，每种算法往往也受限于具体的网络环境，当网络参数改变时，算法性能可能会有所降低. 另一方面，在云计算环境下，集中式的防御将面临单点失效的问题，通常需要跨越多个虚拟机来部署检测和防御策略. 此外，在算法选择与部署时还要考虑效率与成本方面的问题，从博弈论的角度评估“性价比”.

(4) 云计算数据中心性能分析与建模

选择合理的性能指标和建立科学的数学模型来分析评估 DDoS 攻击性能和 DDoS 攻击防御性能是一个根本问题. 一方面是如何定量分析 DDoS 攻击对云平台各项指标的影响. 另一方面是如何验证防御系统的各类性能指标，这是衡量防御系统是否切实有效的重要评判依据. 在云计算中，除关注传统的

响应时间、吞吐量、CPU 利用率等指标外，诸如虚拟机迁移频度、流表匹配率等新指标也需重点关注. 而在评价指标性能的时候，常将排队论、马尔科夫链等方法用于建立评估模型.

(5) 实验验证问题

当前的诸多研究成果往往是基于简单的模拟仿真环境，来验证 DDoS 攻击检测和防御方法的性能. 这种没有充分考虑复杂网络的各种实际情况而得到的实验结果有时欠缺说服力，所提出的解决方案也会因此而较为理想化. 此外，目前尚没有一个较为典型的实验平台或实验数据集，这导致不同方法的优缺点难以具体地量化比较. 如何构建真实的、较大规模的实验场景，验证及优化算法是一个重要的问题.

5.2　未来研究展望

除云计算之外，目前还有很多新兴的网络平台或技术，它们的出现虽可以为防御 DDoS 攻击提供有益的帮助，同时也有可能成为 DDoS 攻击的目标. 未来可从以下几个方面拓展研究范围.

(1) 针对 SDN 的 DDoS 攻击研究

SDN 为缓解 DDoS 攻击提供了有效的途径，由于 SDN 的用途极为广泛，因此其自身遭受 DDoS 攻击的问题也是未来需要重点关注的领域. SDN 的应用层、控制层和基础设施层均有可能遭受 DDoS 攻击. 如果 SDN 控制器被攻击，那么攻击者将很容易地打破 SDN 架构. 目前 SDN 中 DDoS 的攻防研究大多从流表中提取一些直观的特征进行检测，然后通过简单的丢包方式防御攻击. 从流表缓存建模、超时机制、拥塞控制等方面应对 DDoS 攻击是未来值得深入研究的方向.

(2) 针对 NFV 的 DDoS 攻击研究

NFV 为数据中心中的每个“租户”提供自己的网络拓扑结构，并能控制自身流量[91]. NFV 提供了灵活性，促进了多样性，并承诺安全性和增强的可管理性[92]. 在虚拟化网络中，DDoS 攻击可以由一个虚拟网络启动，以攻击其它虚拟网络或网络虚拟化基片(Network Visualization Substrate, NVS)[93]. 针对 NFV 的 DDoS 攻击研究是一项有意义工作.

(3) 大数据中的 DDoS 攻击研究

随着大数据的兴起，依托用户访问数据结合信誉机制可建立完整的 DDoS 防御系统. 但是，大数据平台也面临遭受 DDoS 攻击的风险. 例如，目前有研究揭示了大数据分析 Hadoop 平台不同配置模式下的 DDoS 攻击[94]. 然而，目前的研究主要停留在理论分析的层面上，缺乏深入系统的建模、测试等工作. 因此，大数据中 DDoS 攻击的相关探索及其应对措施有一定的研究前景.

(4) 信息中心网络中的 DDoS 攻击研究

信息中心网络(Information Centric Network, ICN)是未来网络发展的一个方向，将网络连接变成以信息(或内容)为中心的模式，使得内容与终端位置剥离. ICN 中的 DDoS 攻击是目前研究的一个热点. 例如，待定请求表(Pending Interest Table, PIT)溢出攻击[95]、内容/缓存中毒攻击[96-97]、命名解析攻击[98]等. 如何应对 ICN 场景下的 DDoS 攻击是未来研究的一个趋势.

6　结束语

云平台建立在新的计算技术、网络技术以及业务应用的基础上. 云计算不仅是技术革新，更是服务革新. 随着虚拟化数据中心和云服务的广泛使用，云计算受到 DDoS 攻击的威胁. 攻击者可以采用传统的泛洪式暴力攻击，也可以针对专门的协议漏洞、服务模式、管理规则、基础设施发动技术性攻击. 表面上看 DDoS 攻击的目的是吞噬网络和主机资源，最终迫使业务访问异常，但其背后往往涉及到敲诈勒索、利益冲突、表达政治立场等真正的意图.

云计算的新技术和新服务模式暴露出新的漏洞，本文首先归纳了云计算弹性伸缩、即用即付和多租户的安全隐患，揭示了攻击者基于这些隐患实施 DDoS 攻击的手段. 接着，本文分析了云计算中 DDoS 攻击的组织方式，当前移动网络、物联网甚至是僵尸云都有可能成为实施大规模 DDoS 攻击的途径. 除了传统大流量的 DDoS 攻击之外，面向云计算的 DDoS 攻击也呈现出多样化的特点，出现了很多新型的攻击方式. 因此本文对 DDoS 攻击进行了分类比较. 然后，本文从攻击防范、攻击检测和攻击缓解三个层面进行综述，针对每一层面中的典型技术进行评价与比较. 然而，在抗 DDoS 攻击的实践中，仅有技术是不够的，技术结合服务及管理才能更好地防范 DDoS 攻击. 因此，本文对服务和管理层面的相关问题进行了延伸讨论. 最后，本文讨论了目前研究中存在的典型问题，并展望了未来研究的发展趋势. 希望本文所做的工作能够为相关领域的研究者提供一些有益的启示，扩展研究思路.

参 考 文 献

[1] Nikolai J, Wang Y. A system for detecting malicious insider data theft in IaaS cloud environments//Proceedings of the 59th IEEE Global Communications Conference. Washington, USA, 2016: 1-6

[2] Feng Deng-Guo, Zhang Min, Zhang Yan, et al. Study on cloud computing security. Journal of Software, 2011, 22(1): 71-83(in Chinese)
(冯登国, 张敏, 张妍等. 云计算安全研究. 软件学报, 2011, 22(1): 71-83)

[3] Chen Xing-Shu, Ge Long. Cloud Security Principle and Practice. Beijing: Mechanical Industry Press, 2017(in Chinese)
(陈兴蜀, 葛龙. 云安全原理与实践. 北京: 机械工业出版社, 2017)

[4] Somani G, Gaur M S, Sanghi D, et al. Combating DDoS attacks in the cloud: Requirements, trends, and future directions. IEEE Cloud Computing, 2017, 4(1): 22-32

[5] Hoque N, Bhattacharyya D K, Kalita J K. Botnet in DDoS attacks: Trends and challenges. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2242-2270

[6] Zhang Yu-Qing, Wang Xiao-Fei, Liu Xue-Feng, et al. Survey on cloud computing security. Journal of Software, 2016, 27(6): 1328-1348(in Chinese)
(张玉清, 王晓菲, 刘雪峰等. 云计算环境安全综述. 软件学报, 2016, 27(6): 1328-1348)

[7] Li Ke, Fang Bin-Xing, Cui Xiang, et al. Study of botnets trends. Journal of Computer Research and Development, 2016, 53(10): 2189-2206(in Chinese)
(李可, 方滨兴, 崔翔等. 僵尸网络发展研究. 计算机研究与发展, 2016, 53(10): 2189-2206)

[8] Zand A, Modelo-Howard G, Tongaonkar A, et al. Demystifying DDoS as a service. IEEE Communications Magazine, 2017, 55(7): 14-21

[9] Akamai Research and Development Team. DDoS and application attacks. Cambridge, Massachusetts, USA: Akamai, Security DDoS and Application Attacks Report: Volume 5, Issue 1, 2019

[10] Amazon Web Services. AWS Best Practices for DDoS Resiliency. Seattle, Washington, USA: Amazon. com Inc, 2016

[11] Alibaba Cloud Security Team. First half of 2019 DDoS attack situation report. Hangzhou: Alibaba Network Technology Co., 2019(in Chinese)
(阿里云安全团队. 2019 年上半年 DDoS 攻击态势报告. 杭州: 阿里巴巴网络技术有限公司, 2019)

[12] Khalil I, Khreishah A, Azeem M. Cloud computing security: A survey. Computers, 2014, 3(1): 1-35

[13] Lin Chuang, Su Wen-Bo, Meng Kun, et al. Cloud computing security: Architecture, mechanism and modeling. Chinese Journal of Computers, 2013, 36(9): 1765-1784(in Chinese)
(林闯, 苏文博, 孟坤等. 云计算安全: 架构、机制与模型评价. 计算机学报, 2013, 36(9): 1765-1784)

[14] Quwaider M, Jararweh Y, Al-Alyyoub M, et al. Experimental framework for mobile cloud computing system. Procedia Computer Science, 2015, 52(1): 1147-1152

[15] Li C, Guo D, Wu J, et al. DCube: A family of network structures for containerized data centers using dual-port servers. Computer Communications, 2014, 53: 13-25

[16] Hu Z, Qiao Y, Luo J. ATME: Accurate traffic matrix estimation in both public and private data center networks. IEEE Transactions on Cloud Computing, 2018, 6(1): 60-73

[17] Shea R, Liu J. Performance of virtual machines under networked denial of service attacks: Experiments and analysis. IEEE Systems Journal, 2013, 7(2): 335-345

[18] Yan Q, Yu F R, Gong Q X, et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622

[19] Bremler-Barr A, Brosh E, Sides M. DDoS attack on cloud auto-scaling mechanisms//Proceedings of the 2017 IEEE Conference on Computer Communications. Atlanta, United States, 2017: 39

[20] Shawahna A, Abu-Amara M, Mahmoud A, et al. EDoS-ADS: An enhanced mitigation technique against economic denial of sustainability (EDoS) attacks. IEEE Transactions on Cloud Computing, 2018, (99): 1-1

[21] Somani G, Sanghi D, Sanghi D. DDoS/EDoS attack in cloud: Affecting everyone out there!//Proceedings of the International Conference on Security of Information and Networks. Sochi, Russian Federation, 2015: 169-176

[22] Zhang T W, Zhang Y, Lee R B. Memory DoS attacks in multi-tenant clouds: Severity and mitigation. arXiv: arXiv1603.03404v2, 2016

[23] Memarian M R, Conti M. EyeCloud: A BotCloud detection system//Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015). Helsinki, Finland, 2015: 1067-1072

[24] Karim A, Salleh R B, Shiraz M, et al. Review: Botnet detection techniques: Review, future trends, and issue. Frontiers of Information Technology & Electronic Engineering, 2014, (11): 943-983

[25] Li Z, Kihl M, Lu Q, et al. Performance overhead comparison between hypervisor and container based virtualization//Proceedings of the 31st IEEE International Conference on Advanced Information Networking and Applications (AINA 2017). Taipei, China, 2017: 955-962

[26] Di S, Cappello F. GloudSim: Google trace based cloud simulator with virtual machines. Software-Practice and Experience, 2015, 45(11): 1571-1590

[27] Zargar S T, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069

[28] Fernandez E B, Monge R, Hashizume K. Building a security reference architecture for cloud systems. Requirements Engineering, 2016, 21(2): 225-249

[29] Wang Y C, Ma J F, Lu D, et al. From high-availability to collapse: Quantitative analysis of "Cloud-Droplet-Freezing" attack threats to virtual machine migration in cloud computing. Cluster Computing, 2014, 17(4): 1369-1381

[30] Yan Q, Yu F R. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 2015, 53(4): 52-59

[31] Xu Z, Wang H N, Xu Z C, et al. Power attack: An increasing threat to data centers//Proceedings of the 2014 Network and Distributed System Security Symposium. San Diego, USA, 2014: 132-147

[32] Francesco P, Sergio R, Ugo F, et al. Energy-oriented denial of service attacks: An emerging menace for large cloud infrastructures. The Journal of Supercomputing, 2015, 71(5): 1620-1641

[33] Idziorek J, Tannian M, Jacobson D. Detecting fraudulent use of cloud resources//Proceedings of the ACM Cloud Computing Security Workshop. Chicago, USA, 2011: 61-72

[34] Idziorek J, Tannian M, Jacobson D. Attribution of fraudulent resource consumption in the cloud//Proceedings of the IEEE International Conference on Cloud Computing. Beijing, China, 2012: 99-106

[35] Sides M, Bremlerbarr A, Rosensweig E. Yo-Yo attack: Vulnerability in auto-scaling mechanism. ACM SIGCOMM Computer Communication Review, 2015, 45(5): 103-104

[36] Cao J, Xu M W, Li Q, et al. Disrupting SDN via the data plane: A low-rate flow table overflow attack//Proceedings of the International Conference on Security & Privacy in Communication Systems. Springer, Cham, 2017: 356-376

[37] Liu H. A new form of DoS attack in a cloud and its avoidance mechanism//Proceedings of the ACM Cloud Computing Security Workshop. Chicago, USA, 2010: 65-76

[38] Shameli-Sendi A, Pourzandi M, Fekih-Ahmed M, et al. Taxonomy of distributed denial of service mitigation approaches for cloud computing. Journal of Network & Computer Applications, 2015, 58(C): 165-179

[39] Abdel Wahab O, Bentahar J, Otrol H, Mourad A. Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. IEEE Transactions on Services Computing, 2020, 13(1): 114-129

[40] Ahn L V, Blum M, Hopper N J, et al. CAPTCHA: Using hard AI problems for security//Proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003). Warsaw, Poland, 2003: 294-311

[41] Alsowail S, Sqalli M H, Abu-Amara M, et al. An experimental evaluation of the EDoS-shield mitigation technique for securing the cloud. Arabian Journal for Science and Engineering, 2016, 41(12): 5037-5047

[42] Huang S M, Huang R, Ming C. A DDoS mitigation system with multi-stage detection and text-based turing testing in cloud computing//Proceedings of the International Conference on Advanced Information NETWORKING and Applications Workshops. Taipei, China, 2013: 655-662

[43] Khor H, Nakao A. sPoW: On-demand cloud-based eDDoS mitigation mechanism. HotDep (Fifth Workshop on Hot Topics in System Dependability). Estoril, Lisbon, Portugal, 2009: 1-6

[44] Xue K, Chen W K, Li W, Hong J, et al. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2062-2074

[45] Alosaimi W, Al-Begain K. An enhanced economical denial of sustainability mitigation system for the cloud//Proceedings of the 7th International Conference on Next Generation Mobile Apps, Services and Technologies. Barcelona, Spain, 2013: 19-25

[46] Wang H X, Jia Q, Fleck D, et al. A moving target DDoS defense mechanism. Computer Communications, 2014, 46(6): 10-21

[47] Saini B, Somani G. Index page based EDoS attacks in infrastructure cloud//Proceedings of the International Conference on Security in Computer Networks and Distributed Systems. Trivandrum, India, 2014: 382-395

[48] Baig Z A, Sait S M, Binbeshr F. Controlled access to cloud resources for mitigating economic denial of sustainability (EDoS) attacks. Computer Networks, 2016, 97: 31-47

[49] Masood M, Anwar Z, Raza S A, et al. EDoS Armor: A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments //Proceedings of the Multi Topic Conference. Karachi, Pakistan, 2014: 37-42

[50] Wang F, Hu X, Wang X, et al. Unfair rate limiting on traffic aggregates for DDoS attacks mitigation//Proceedings of the IET International Conference on Information Science & Control Engineering. Shenzhen, China, 2012: 1-11

[51] Agrawal N, Tapaswi S. Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey. Information Security Journal: A Global Perspective, 2017, 26(2): 61-73

[52] Wu Z J, Pan Q B, Yue M, et al. Sequence alignment detection of TCP-targeted synchronous low-rate DoS attacks. Computer Networks, 2019, 152: 64-77

[53] Jing X, Yan Z, Member S, et al. Security data collection and data analytics in the Internet: A survey. IEEE Communications Surveys & Tutorials, 2019, 21(1): 586-618

[54] Wu Z J, Zhang L, Yue M. Low-rate DoS attacks detection based on network multifractal. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 559-567

[55] Agrawal N, Tapaswi S. Low rate cloud DDoS attack defense method based on power spectral density analysis. Information Processing Letters, 2018, 138: 44-50

[56] Yue M, Liu L, Wu Z, et al. Identifying LDoS attack traffic based on wavelet energy spectrum and combined neural network. International Journal of Communication Systems, 2018, 31(2): 1-16

[57] Osanaiye O A, Dlodlo M. TCP/IP header classification for detecting spoofed DDoS attack in cloud environment// Proceedings of the 16th IEEE International Conference on Computer as a Tool. Salamanca, Spain, 2015: 1-6

[58] Al-Haidari F, Sqalli M H, Salah K. Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses//Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012). Liverpool, United Kingdom, 2012: 1167-1174

[59] Karnwal T, Sivakumar T, Aghila G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack//Proceedings of the Electrical, Electronics and Computer Science. Hsinchu, China, 2013: 1-5

[60] Wang T, Chen H C. SGuard A lightweight SDN safe-guard architecture for DoS attacks. China Communications, 2017, 14(6): 113-125

[61] Zhang T W, Lee R B. Host-based DoS attacks and defense in the cloud//Proceedings of the 6th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2017). Toronto, Canada, 2017: 1-1

[62] Ficco M, Rak M. Stealthy denial of service strategy in cloud computing. IEEE Transactions on Cloud Computing, 2015, 3(1): 80-94

[63] Jiang J, Yu Q, Yu M, et al. ALDD: A hybrid traffic-user behavior detection method for application//Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering (Trustcom/BigDataSE 2018). New York, United States, 2018: 1565-1569

[64] Koduru A, Neelakantam T, Saira Bhanu S M. Detection of economic denial of sustainability using time spent on a Web page in cloud//Proceedings of the IEEE International Conference on Cloud Computing in Emerging Markets. Santa Clara Marriott, USA, 2013: 1-4

[65] Xu M, Yang S, Wang D, et al. Source address filtering for large scale networks. Computer Communications, 2014, 37: 64-76

[66] Wu Z J, Wang M X, Yan C C, et al. Low-rate DoS attack flows filtering based on frequency spectral analysis. China Communications, 2017, 14(6): 98-112

[67] Xie Y, Yu S Z. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors. IEEE/ACM Transactions on Networking, 2009, 17(1): 54-65

[68] Singh K, Singh P, Kumar K. User behavior analytics-based classification of application layer HTTP-GET flood attacks. Journal of Network & Computer Applications, 2018, 112: 97-114

[69] Miu T, Wang C, Luo X, et al. Modeling user browsing activity for application layer DDoS attack detection//Proceedings of the 12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2016). Guangzhou, China, 2017: 747-750

[70] Keromytis A D, Misra V, Rubenstein D. SOS: An architecture for mitigating DDoS attacks. IEEE Journal on Selected Areas in Communications, 2004, 22(1): 176-188

[71] Keromytis A D, Misra V, Rubenstein D. SOS: Secure overlay services. ACM SIGCOMM Computer Communication Review, 2002, 32(4): 61-72

[72] Wu Zhi-Jun, Cui Yi, Yue Meng. VHSAP-based approach of defending against DDoS attacks for cloud computing routing platforms. Journal on Communications, 2015, 36(1): 30-37 (in Chinese)
(吴志军, 崔奕, 岳猛. 基于虚拟散列安全访问路径 VHSAP 的云计算路由平台防御 DDoS 攻击方法. 通信学报, 2015, 36(1): 30-37)

[73] Yue Meng, Li Kun, Wu Zhi-Jun. SAPA-based approach for defending DoS attacks in cloud computing. Journal on Communications, 2017, 38(4): 129-139(in Chinese)
(岳猛, 李坤, 吴志军. 云计算中基于 SAPA 的 DoS 攻击防御方法. 通信学报, 2017, 38(4): 129-139)

[74] Luo H B, Chen Z, Li J W, Vasilakos T. On the benefits of keeping path identifiers secret in future Internet: A DDoS perspective. IEEE Transactions on Network and Service Management, 2018, 15(2): 650-664

[75] Somani G, Guar M S, Sanghi D, et al. Scale inside-out rapid mitigation of cloud DDoS attacks. IEEE Transactions on Dependable and Secure Computing, 2018, 15(6): 959-973

[76] Yu S, Tian Y H, Guo S, et al. Can we beat DDoS attacks in clouds?. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(9): 2245-2254

[77] Chowdhury F Z, Idris M Y I, Kiah M L M, et al. EDoS eye: A game theoretic approach to mitigate economic denial of sustainability attack in cloud computing//Proceedings of the Control & System Graduate Research Colloquium. Shah Alam, Malaysia, 2017: 164-169

[78] Assis M V O D, Hamamoto A H, Abrão T, et al. A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. IEEE Access, 2017, 5(99): 9485-9496

[79] Rashidi B, Fung C, Bertino E. A collaborative DDoS defence framework using network function virtualization. IEEE Transactions on Information Forensics and Security, 2017, 12(10): 2483-2497

[80] Somani G, Johri A, Taneja M, et al. DARAC: DDoS mitigation using DDoS aware resource allocation in cloud// Proceedings of the 11th International Conference on Information Systems Security (ICISS 2015). Kolkata, India, 2015: 263-282

[81] Li H, Ota K, Dong M X. Virtual network recognition and optimization in SDN-enabled cloud environment. IEEE Transactions on Cloud Computing, 2018, 1-1

[82] Jarraya Y, Madi T, Debbabi M. A survey and a layered taxonomy of software-defined networking. IEEE Communications Surveys & Tutorials, 2014, 16(4): 1955-1980

[83] Li C H, Wu Y, Yuan X Y, et al. Detection and defense of DDoS attack — based on deep learning in OpenFlow-based SDN. International Journal of Communication Systems, 2018, 31(5): 1-15

[84] Sahay R, Blanc G, Zhang Z H, et al. Towards autonomic DDoS mitigation using software defined networking// Proceedings of the 2015 NDSS Workshop on Security of Emerging Networking Technologies. San Diego, USA, 2016: 100-108

[85] Yuan B, Zou D, Yu S, et al. Defending against flow table overloading attack in software-defined networks. IEEE Transactions on Services Computing, 2019, 12(2): 231-246

[86] Zhang Y L, Ye J. Research on DDoS attack detection and judgment based on stream eigenvalues of software defined networks. Journal of Guangxi University (Natural Science Edition), 2017, 42(6): 2208-2213

[87] Phan T, Park M. Efficient distributed denial-of-service attack defense in SDN-based cloud. IEEE Access, 2019, 7: 18701-18714

[88] Lim S, Yang S, Kim Y, et al. Controller scheduling for continued SDN operation under DDoS attacks. Electronics Letters, 2015, 51(16): 1259-1261

[89] Wang Xiu-Lei, Chen Ming, Xing Chang-You, et al. Sofware defined security networking mechanism to defend against DDoS attacks. Journal of Software, 2016, 27(12): 3104-3119(in Chinese)
(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机制. 软件学报，2016，27(12)：3104-3119)

[90] Arivudainambi D, Varun Kumar K A, Sibi C S. LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks. Neural Computing and Applications, 2019, 31(5): 1491-1501

[91] Ye Z, Cao X J, Wang J P, et al. Joint topology design and mapping of service function chains for efficient, scalable and reliable network functions virtualization. IEEE Network, 2016, 30(3): 81-87

[92] Liang C, Yu F R. Wireless virtualization for next generation mobile cellular networks. IEEE Wireless Communications, 2015, 22(1): 61-69

[93] Richart M, Baliosian J, Serrat J, et al. Resource slicing in virtual wireless networks: A survey. IEEE Transactions on Network and Service Management, 2016, 13(3): 1-15

[94] Shakeel A, Amanullah Y, Qaisar S. DDoS attacks analysis in bigdata (Hadoop) environment//Proceedings of the 15th International Bhurban Conference on Applied Sciences & Technology. Islamabad, Pakistan, 2018: 495-501

[95] Zhi T, Luo H, Ying L. A Gini impurity based interest flooding attack defence mechanism in NDN. IEEE Communications Letters, 2018, 22(3): 538-541

[96] Tourani R, Mick T, Misra S, et al. Security, privacy, and access control in information-centric networking: A survey. IEEE Communications Surveys & Tutorials, 2016, 20(1): 556-600

[97] Gouge J, Seetharam A, Roy S. On the scalability and effectiveness of a cache pollution-based DoS attack in information centric networks//Proceedings of the International Conference on Computing, Networking and Communications. Kauai, USA, 2016: 1-5

[98] Ren J, Li L M, Wang S. Analysis of DoS attack on name resolution system in information-centric network. Application Research of Computer, 2016, 33(2): 495-497

YUE Meng, Ph. D., associate professor. His research interests include cloud computing and network security.

WANG Huai-Yuan, M. S. candidate. His research interests include cloud computing and network security.

WU Zhi-Jun, Ph. D., professor. His research interests include network information security and cloud computing security.

LIU Liang, M. S. His research interest is network information security.

Background

Cloud computing has promoted the rapid growth of Internet businesses, which have produced huge economic benefits. With the migration of large amounts of user data and applications to cloud computing platforms, attacks against cloud computing are increasing. The DDoS attack is one of the major security threats to the Internet in the era of

cloud computing. The DDoS attack is favored by attackers as the implementation of DDoS attacks is simple, efficient and economical. From the game theory perspective, hackers can get huge benefits by a small cost. New technologies and models in the cloud platform have brought new vulnerabilities, which provide a wide space for DDoS attackers. DDoS attacks in cloud computing environment present large-scale, diversified, and complicated features, and challenge existing defense technologies.

Currently, a lot of studies focus on the DDoS attack in cloud computing. Researchers have proposed many DDoS attack strategies and defense approaches for cloud computing platform. This paper extensively collects existing research results and presents a survey on DDoS attack and defense technologies. On the attack side, this paper summarizes the vulnerabilities exposed in cloud computing and discusses how to organize large-scale DDoS attacks exploiting new strategies. In addition, this paper classifies various DDoS attacks in cloud computing and analyzes their principles in detail. On the defense side, this paper classifies anti-DDoS attack technologies into three categories, including attack prevention, attack detection, and attack mitigation. Further, this paper compares these technologies. After that, this paper explores the existing issues of current researches and proposes feasible suggestions. Finally, this paper looks forward to future research trends. This paper can provide some useful information for related researchers, so that they can quickly obtain relevant research results and comprehensively grasp the latest research progress.

This paper is supported in part by the National Natural Science Foundation of China (No. U1933108), the Scientific Research Project of Tianjin Municipal Education Commission (No. 2019KJ117) and the Fundamental Research Funds for the Central Universities of CAUC (No. 3122020076). These projects aim to address the network security issues in cloud computing related fields and improve the ability of the network to respond to attacks.

Our team has been devoted many efforts to the research of network security, especially DDoS attack and its defense. In the past 5 years, we have published 3 academic monographs, undertaken 4 National Natural Science Foundations, and published more than 20 papers, in which more than 10 papers were indexed by SCI /EI.