doi:10.11959/j.issn.1000-436x.2017079

云计算中基于 SAPA 的 DoS 攻击防御方法

岳猛，李坤，吴志军
（中国民航大学电子信息与自动化学院，天津 300300）

摘 要：拒绝服务（DoS, denial of service）攻击是云计算平台面临的主要安全威胁之一。安全访问路径算法（SAPA, security access path algorithm）通过节点路由表（NRT, node route table）合成安全路径，简化了传统安全覆盖网服务（SOS, secure overlay services）的角色节点，并采用周期性更新角色节点以及缓存安全访问路径的策略。SAPA 更适用于云计算平台防御 DoS 攻击。基于云计算泛联路由架构，建立 SAPA 的数学模型并对其性能进行理论分析。通过 OMNeT++实验平台测试 SAPA 的性能，并将实验场景扩展到 Test-bed 平台来评估 SAPA 对 DoS 攻击的防御效果。实验结果表明，相较于 SOS 方法，SAPA 能够更有效地降低 DoS 攻击对通信成功率的影响，并保证足够小的访问延时。

关键词：云计算；DoS 攻击；安全访问路径算法；防御
中图分类号：TP393.08 **文献标识码**：A

SAPA-based approach for defending DoS attacks in cloud computing

YUE Meng, LI Kun, WU Zhi-jun
(School of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Denial of service (DoS) attack was one of the major threats to cloud computing. Security access path algorithm (SAPA) used node route table (NRT) to compose security access path. It simplified role nodes of traditional secure overlay services (SOS), and periodically updated role nodes, and cached security access paths. Therefore, SAPA was more appropriate for cloud computing to defend DoS attacks. Based on the turn routing architecture of cloud computing, the mathematical model of SAPA was built and its performance was analyzed in theory. The performance of SAPA was tested in OMNeT++ experimental platform. Also, the Test-bed experiments were performed to evaluate the effectiveness of SAPA for defending DoS attack. Experimental results show that comparing with SOS, SAPA can degrade the impact of communication success rate caused by DoS attack effectively, and guarantees the access delay small enough.

Key words: cloud computing, DoS attack, secure access path algorithm, defense

1 引言

云计算的大规模以及前所未有的开放性与复杂性，使其本身存在许多安全漏洞。由此，相关的安全问题伴随而来，给云计算的发展带来了巨大的挑战。云计算面临的安全问题包括数据安全、隐私保护和攻击防御等，其中，攻击问题非常严重[1]。DoS 攻击[1]一直被认为是互联网的严重威胁之一。云平台的基础架构和应用具有新的特征，这些特征给 DoS 攻击者提供了更广阔的空间。随着越来越多的用户开始使用虚拟化数据中心和云服务，资源高度集中的云平台已成为黑客攻击的重点目标。Arbor 公司 2016 年的调查报告显示，33%的受访者经历过针对云服务的攻击，而 51%的数据中心运营商曾遭

收稿日期：2016-11-02；**修回日期**：2017-02-16
基金项目：国家自然科学基金资助项目（No.61601467, No.U1533107, No.U1433105）；中央高校基本科研业务费基金资助项目（No.3122016D005）
Foundation Items: The National Natural Science Foundation of China (No.61601467, No.U1533107, No.U1433105), Fundamental Research Funds for the Central Universities of CAUC (No.3122016D005)

受到 DoS 攻击。

针对云计算的 DoS 攻击一般来自云计算平台外部，这种攻击具有高速率、大流量的特征，给防御带来了困难。目前，结合云平台自身的新特性或新技术设计 DoS 攻击防御方法是研究热点之一。本文在云计算泛联路由架构下，提出一种新的安全访问路径算法 SAPA，以阻断 DoS 攻击。该方法基于 Chord 协议，改进了传统的安全覆盖网服务，使其更适用于云计算平台。SAPA 不仅保护了云数据中心的端系统，而且还有效降低了 DoS 攻击对云计算核心路由节点的影响，提高了云计算服务的安全性，保证了路由平台的高可用性。

2 相关工作

目前，针对云计算的 DoS 攻击检测和防御方法，研究成果颇多。Chonka 等[2]提出了一种新型的 HX-DoS 攻击，这种攻击利用云计算中广泛使用的 HTTP 和 XML 漏洞，降低云计算的服务质量。针对该攻击，还提出了一套 ENDER 防御系统，其核心是利用分组标记的方法来缓解云平台中的 HX-DoS 攻击。Yu 等[3]针对云计算数据中心的 DDoS 攻击，提出了一种动态资源配置策略。利用闲置的云资源，复制足够的入侵防御服务器，达到快速过滤 DoS 攻击流的目的。Girma 等[4]分析了目前针对不同参数的 DDoS 检测技术及其优缺点，提出了能有效缓解 DDoS 攻击的混合统计模型。Osanaiye 等[5]通过分析 TCP/IP 报文头部特征，检测 DDoS 攻击数据分组的源头。Liu 等[6]利用 BIRTH 算法，以网络流量的频域特性作为聚类特征，对终端用户流数据进行分组，克服 BIRTH 算法的缺陷，将聚类结果重新合并，以区分异常网络流量，该方法检测精度高于 70%。韩志杰等[7]主要研究了云计算平台上对 HTTP 应用进行拒绝服务攻击的问题，通过 CPU、网络吞吐量等特征来检测攻击，通过黑白名单的方法过滤攻击流。韩伟等[8]对基于 Hadoop 云计算平台的工作流进行研究，并结合其自身的心跳监测机制，提出了一种全新的基于 Hadoop 云节点 DoS 检测与自修复防御模型。文献[9]提出了适用于云计算平台的虚拟散列安全访问方法，并利用弹性机制实现节点的无缝切换，从而缓解了云计算中的 DoS 攻击。

从研究现状来看，目前防御 DoS 攻击的主要方法是通过已知攻击的模型匹配或通过统计异常通信量的方式来检测是否发生了 DoS 攻击。但是，通过改变攻击模式和掩盖异常的通信量，上述方法就会失效。此外，通过统计异常通信量的方式来过滤 DoS 攻击还有可能把正常的通信量也过滤掉。基于 IP 追踪的方法也有一定局限性，由于 Internet 是一个跨越若干管理域和管理权限的网络，通过联系最靠近攻击源的网络管理员来阻止攻击，虽然不是完全不可能，但也是非常困难的。实际上，这种攻击行为不能被及时予以防御，经常需要花费几个小时。况且即使一个攻击节点能及时被找到，但是该节点可能并不是攻击的发动者，而仅仅是被远程攻击者入侵和控制的傀儡机，即使阻止了一个攻击节点的攻击，攻击者仍然可以利用其他被控制的傀儡机继续攻击。

SOS 为解决上述问题提供了有意义的借鉴[10,11]。在传统网络中，SOS 能够较好地防御 DoS 攻击，体现出以下 2 个优点：1) SOS 是一种主动防御的策略，而非发现攻击后被动采取措施。这就使攻击流本身难以到达目标主机；2) SOS 通过隐藏路由节点信息，增强了路由平台自身的健壮性，使 DoS 攻击者无法找到有效的目标路由节点作为攻击对象。但是，SOS 也存在一些缺点，导致其不适用于云计算平台。SOS 中角色节点种类较多，导致安全路径较长，这样增加了传输延时，也会导致路径节点被攻击的概率增加。SOS 中每有一个访问请求都要重新查找一次路径，对于云计算这种分布式、高并发的场景来说，角色节点负荷较大。另外，SOS 存在角色节点快速消耗的问题。当角色节点遭受 DoS 攻击后，SOS 只是简单地使受攻击节点退出覆盖网，这样攻击者更容易发起随机变化目标的 DoS 攻击，以此消耗掉大量角色节点。而角色节点的减少必然影响用户的访问质量。

基于以上问题，本文提出一种基于 SAPA 的 DoS 攻击防御方法。

3 基于 SAPA 的 DoS 攻击防御方法

3.1 安全访问路径架构

云计算数据中心是资源高度集中的架构，支持众多异构业务以及海量信息的交互与处理。泛联路由平台作为数据传输平台，通过各层次路由设备的接入与业务处理能力，满足云计算数据中心对终端用户提供的高可用性、易用性和可扩展性。泛联路

由平台具有层次化的特点[12]，一般可分为接入层、中间层和核心层。云服务的终端用户数量大、分布广泛、接入方式多种多样。终端用户的请求从接入层进入，经由中间层以及核心层最终到达数据中心。

SAPA 的核心思想是选取云计算泛联路由平台中的节点构成安全访问路径，只有通过安全访问路径的请求才能到达云计算数据中心。在云计算泛联路由平台中，核心层路由器执行高速数据转发，而接入层泛化的接入方式使在核心层的路由器更容易成为攻击目标。一旦核心层路由被攻击，就会影响受害路由器域内的所有服务器。因此，SAPA 的设计不仅要保护云计算数据中心，同时还要保护核心层路由器。基于 SAPA 的云计算路由平台架构如图 1 所示。

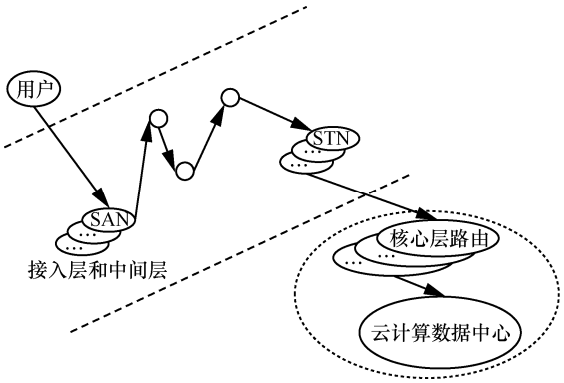


图 1　基于 SAPA 的云计算路由平台架构

在图 1 中，SAPA 在接入层和中间层选取部分路由节点作为安全接入节点（SAN, security access node）和秘密传输节点（STN, secret transmission node）。当用户访问数据中心时，首先会通过互联网将访问请求发送至邻近的 SAN 进行认证（通过 IPSec 等认证协议）。认证通过后，用户获取一条以 SAN 为起点，STN 为终点的安全访问路径，从而建立合法用户与数据中心的通信链路。

SAPA 与 SOS 的不同在于以下 2 点。1) 简化了角色节点的种类。在 SAPA 中只有 SAN 和 STN 这 2 种角色节点，角色节点的减少有利于提高路径生成效率，同时降低角色节点被攻击的可能性。2) 采用周期性更新角色节点以及缓存安全访问路径的策略。周期性更新角色节点在理论上使网络中所有的节点都有可能被选为角色节点，攻击者要想采用消耗角色节点数量的攻击方式，必然要付出更大的代价。而缓存安全访问路径使用户在访问时不需再重新查找路径，节约了用户获取安全访问路径的时间，提高了访问效率。

3.2　安全访问路径生成算法

生成安全访问路径是 SAPA 中用户和数据中心通信的前提。只有成功生成了安全访问路径，用户请求才能通过该路径到达云计算数据中心。

1) 角色节点的动态更新

SAPA 通过随机选取角色节点并进行动态更新的方式，达到隐藏角色节点信息的目的，从而增加了攻击者攻击安全访问路径上 SAN 与 STN 的难度，增强了路由平台的安全性。

假设路由平台上所有节点组成的集合为 Φ。周期性地随机在 Φ 中选取部分节点作为 SAN 和 STN，分别用集合 Φ_{SA} 和 Φ_{ST} 表示。Φ_{SA}、Φ_{ST} 和 Φ 的关系为

$$\begin{aligned} &\Phi_{SA} \subset \Phi \\ &\Phi_{ST} \subset \Phi \\ &\Phi_{SA} \cap \Phi_{ST} = \varnothing \end{aligned} \tag{1}$$

通过动态更新 SAN 和 STN，使用户在不同更新周期内访问数据中心时，获取不同的安全访问路径；而在发送访问请求之前，用户无法确定数据传输所需要的路由节点。

2) 安全访问路径的生成

SAPA 基于 Chord 协议进行数据转发。Chord 协议是一种应用于对等网络系统的分布式查询协议，通过一致性散列算法为节点分配唯一的 m 位编号，能够实现资源的快速、有效定位[13]。

Chord 由麻省理工学院在 2001 年提出[13]，其初衷是提供一种能在 P2P 网络中快速定位资源的算法，Chord 在一致性散列的基础上提供了优化的路由算法，优化后的算法具有负载平衡、分布性、可扩展性、可用性、命名的灵活性等优点。它可用于全球文件系统、命名服务、数据库请求处理、互联网级别的数据结构、通信服务、事件通知和文件共享等应用中。Chord 常用于构建结构化 P2P 的分布式散列表（DHT）系统，除 Chord 算法外，类似的算法还包括加州大学伯克利分校提出的内容寻址网络算法 CAN、英国剑桥的微软研究院和莱斯大学提出的 Pastry、加州大学伯克利分校提出的一种新型 P2P 网络定位和路由算法 Tapestry 等。2002 年，Angelos 等首次提出基于 Chord 的 SOS 可以用于防御 DoS 攻击。

为了减少路由平台的网络冗余，提高路由效率，SAPA 仅采用了 Chord 协议的指针表（FT，finger table）思想实现资源快速、有效定位，而舍弃了其他复杂的、不适用于云计算路由平台的功能（如节点加入、节点退出等）。

SAPA 基于 Chord 协议的指针表为每个节点生成一个节点路由表，用来合成安全路径。根据 Chord 协议的查询策略[13]，NRT 以当前节点的前驱节点（逆时针方向相邻的第一个节点）为查询对象，通过记录查询路径的节点编号而生成。以 m=4 的 Chord[13]为例进行说明，如图 2 所示。

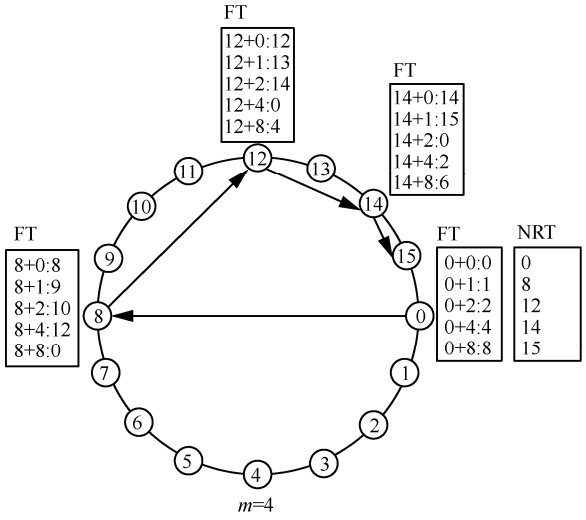


图 2 NRT 的生成

图 2 描述了节点 0 生成 NRT 的过程：节点 0 以其前驱节点 15 为查询目标。根据 Chord 协议，查询请求将依次在节点 0、8、12、14、15 之间跳转。这样，节点 0 记录这些节点编号，就得到了 NRT。其他节点的 NRT 生成与之相同。

假设路由平台中编号为 i 的节点记为 n_i，n_i 的 NRT 第 k 项记录的节点编号记为 $n_i.NRT[k]$，根据设计的前驱节点查找规则，有

$$\begin{cases} n_i.NRT[k]=i, & k=0 \\ n_i.NRT[k]=(i+\sum_{j=1}^{k}2^{m-j}) \bmod 2^m, & 1\leqslant k\leqslant m \end{cases} \tag{2}$$

由式(2)可以看出，NRT 共维护了 m+1 个表项(0,…, m)，每个表项记录一个节点编号，每个 NRT 中的首项（第 0 项）记录当前节点编号。

根据 NRT 的生成过程，不难发现，节点之间对应表项满足

$$n_j.NRT[k]=(n_i.NRT[k]+j-i) \bmod 2^m \tag{3}$$

其中，$0\leqslant i\leqslant 2^m$，$0\leqslant j\leqslant 2^m$，$0\leqslant k\leqslant m$。

利用 NRT，节点之间可以进行路径合成。只要 2 个节点的 NRT 具有公共表项（同时保存了相同的一个或多个节点编号），就能够合成安全路径；反之，则不能合成安全路径。以上过程用伪代码表示如下。

```
1) construct_route(n_i.NRT, n_j.NRT)
2)    for p=0 up to m
3)        for q=0 up to m
4)            if(n_i.NRT[p] == n_j.NRT[q])
5)                return true;
6)            else
7)                return false;
```

在 NRT 的基础上，为了进一步建立 SAPA 数学模型以分析其性能，构造一个二进制数来表示 NRT，称为二进制路由序列（BRS，binary route sequence）。构造规则如下。

给定一个 2^m 位的二进制数 B，初始值为 0。对于节点 n_i，以 NRT 中的节点编号为索引，从左往右将 B 中索引对应位置 1，其余位保持不变，可得节点 n_i 的 BRS，记为 $n_i.BRS$。如图 2 所示，$n_0.BRS$=1000000010001011。

假设对二进制数 B 循环右移 x 位，记为 $RR(B,x)$，循环左移 x 位，记为 $RL(B,x)$，显然 $RR(B,x)=RL(B,-x)$。根据式(3)，对于任意 2 个节点 n_i、n_j，它们的 BRS 具有如下关系

$$\begin{aligned} n_j.BRS &= RR(n_i.BRS,(j-i)) \\ &= RL(n_i.BRS,(i-j)) \end{aligned} \tag{4}$$

式(4)说明任意节点的 BRS，可以由其他节点经过循环移位得到。

借助 BRS，可以很容易判断任意 2 个节点 n_i 和 n_j 是否能够合成路径。

$$\begin{cases} n_i.BRS\&n_j.BRS=0, \text{合成失败} \\ n_i.BRS\&n_j.BRS\neq 0, \text{合成成功} \end{cases} \tag{5}$$

其中，“&”表示按位与运算。

当合成路径的 2 个节点分别是 SAN 与 STN 时，所合成的路径即为安全访问路径。数据由 SAN 进入，经由公共表项节点，最终由 STN 到达数据中心。SAN 与 STN 具有动态随机的特性，因此，安全访问路径也具有动态随机的特性。每当 SAN 和 STN 的更新完成时，SAN 便尝试与各 STN 合成路径。

如果合成路径成功，则缓存所有路径。因为攻击者仅探测到 SAN 上的路径，或仅探测到 STN 上的路径，都是无法达到数据中心的。采用路径合成的方法，可以提高安全性。

3.3　安全访问路径算法性能分析

1) 合成成功率

合成成功率描述了 SAN 能够合成安全访问路径的概率。由式(5)可以看出，并非任意 2 个节点都能够成功地合成路径。对于任意的节点 n_i 和 n_j，假设不能与 n_i 合成路径的节点数目为 F_i，不能与 n_j 合成路径的节点数目为 F_j。根据式(4)的循环移位特征，有 $F_i=F_j$。这说明，对于路由平台上的每个节点，不能与之合成路径的节点数目是相同的，被称为失败基数，用 F 表示。

由于 SAN 与 STN 的动态随机特性，每次更新后，每个 SAN 与所有的 STN 进行路径合成，并缓存安全访问路径。那么对于任意的 2 个 SAN，其合成成功率是相等的。

假设集合 Φ_{SA} 中元素个数为 N_{SA}，集合 Φ_{ST} 中元素个数为 N_{ST}，集合 Φ 中元素个数为 N。通过上述分析可知，Φ_{SA} 中各 SAN 的合成成功率是独立且相等的；Φ_{SA} 中的每个 SAN 与 Φ_{ST} 中的 STN 分别进行路径合成，每个 SAN 至少能够合成一条安全访问路径的概率为

$$R_{\text{success}}(N_{\text{ST}})=1-\frac{\mathrm{C}_N^1\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_N^1\mathrm{C}_{N-1}^{N_{\text{ST}}}}=1-\frac{\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_{N-1}^{N_{\text{ST}}}} \tag{6}$$

式(6)说明合成成功率与 STN 的数目 N_{ST} 有关，STN 越多合成成功率越高。

2) 通信成功率

用户访问云计算数据中心时，会首先接入某个 SAN，如果该 SAN 未缓存任何安全访问路径，或所缓存的安全路径被 DoS 攻击，则会直接导致访问失败。为解决此问题，SAPA 将访问请求在 Φ_{SA} 中进行转发，直至获取安全访问路径，便可以大幅度提高用户获取安全访问路径的成功率。不过当 Φ_{SA} 数目较小时，遍历 Φ_{SA} 无法获取安全访问路径的可能性依旧存在。因此，定义通信成功率 $R(N_{SA}, N_{ST})$来描述用户获取安全访问路径的概率，则有

$$\begin{aligned}R(N_{\text{SA}},N_{\text{ST}})&=\sum_{i=1}^{N_{\text{SA}}}R_{\text{success}}(N_{\text{ST}})(1-R_{\text{success}}(N_{\text{ST}}))^{i-1}\\&=\left(1-\frac{\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_{N-1}^{N_{\text{ST}}}}\right)\sum_{i=1}^{N_{\text{SA}}}\left(\frac{\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_{N-1}^{N_{\text{ST}}}}\right)^{i-1}\end{aligned} \tag{7}$$

令访问请求在 Φ_{SA} 转发的次数为 h，h=0,1,…, $N_{SA}-1$，对应的通信成功率表示为 $R_h(N_{ST})$，则

$$\begin{aligned}R_h(N_{\text{ST}})&=R_{\text{success}}(N_{\text{ST}})(1-R_{\text{success}}(N_{\text{ST}}))^h\\&=\left(1-\frac{\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_{N-1}^{N_{\text{ST}}}}\right)\left(\frac{\mathrm{C}_F^{N_{\text{ST}}}}{\mathrm{C}_{N-1}^{N_{\text{ST}}}}\right)^h\end{aligned} \tag{8}$$

称 $R_h(N_{ST})$为转发 h 次的通信成功率。显然，$R_{\text{success}}(N_{\text{ST}})=R_0(N_{\text{ST}})$，$R(N_{\text{SA}},N_{\text{ST}})=\sum_{h=0}^{N_{\text{SA}}-1}R_h(N_{\text{ST}})$。

3) 平均接入延时

将访问请求在 Φ_{SA} 中转发，能够大幅度提高通信成功率，不过也增加了用户发送访问请求至获取安全访问路径的延时，即接入延时。

假设访问请求经互联网传输至 SAN 的延时为 D_I，假设访问请求在 Φ_{SA} 中一次转发延时为 D_P。根据以上定义，接入延时 D_A 可以表示为

$$D_{\text{A}}=D_{\text{I}}+hD_{\text{P}},\ h=0,1,\cdots,N_{\text{SA}}-1 \tag{9}$$

其中，当 h=0 时，$D_A=D_I$。

式(9)将节点间的转发延时 D_P 看作固定值，这是因为 SAPA 是基于 Chord 协议生成 NRT，而 Chord 是根据一致性散列运算生成的编号进行资源查询，事实上已经忽略了网络节点的物理距离。加之云计算中物理资源高度集中，节点之间的距离相对较近。因此，SAPA 中忽略节点间的物理距离，以常量时间 D_P 表示访问请求在节点间的转发延时是合理的。

进一步，可以得出平均接入延时为

$$\begin{aligned}D_{\text{A-AVERAGE}}&=\frac{D_{\text{I}}R_0(N_{\text{ST}})+\sum_{j=1}^{N_{\text{SA}}-1}D_{\text{P}}R_j(N_{\text{ST}})}{\sum_{j=0}^{N_{\text{SA}}-1}R_j(N_{\text{ST}})}\\&=\frac{D_{\text{I}}R_0(N_{\text{ST}})+D_{\text{P}}\sum_{j=1}^{N_{\text{SA}}-1}R_j(N_{\text{ST}})}{R(N_{\text{SA}},N_{\text{ST}})}\end{aligned} \tag{10}$$

4　实验及结果分析

4.1　实验环境

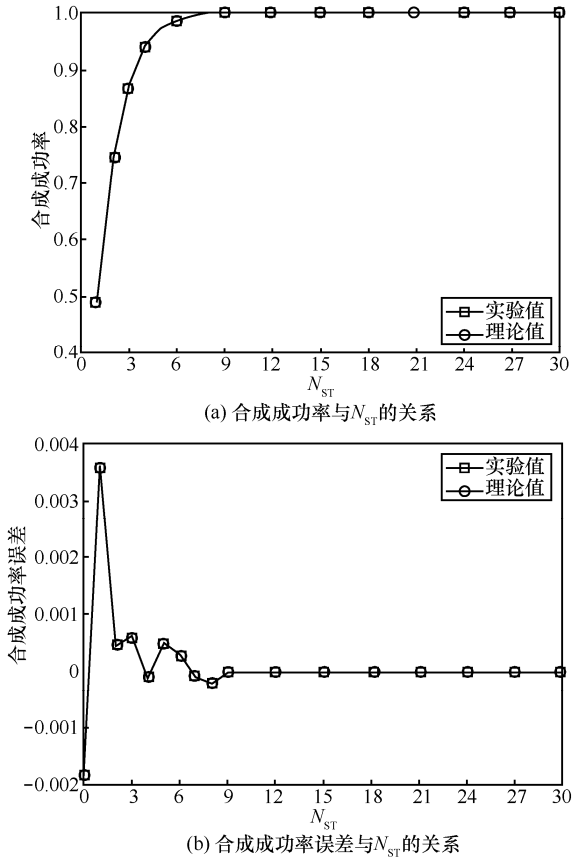
为验证 SAPA 的性能及其防御 DoS 攻击的效果，利用 OMNeT++建立实验测试平台。设置实验平台中路由节点总数为 64，路由节点呈环形排列。实验主要验证：1) SAPA 的性能；2) SAPA 对 DoS 的防御效果。

4.2 SAPA 性能测试及验证

通过改变 N_{SA} 和 N_{ST} 统计实验数据。针对合成成功率、通信成功率以及接入延时进行测试。每个实验数据通过发送 100 000 次访问请求获得。

1) 合成成功率分析

测试每个 SAN 的路径合成成功率，仿真结果如图 3 所示。



(a) 合成成功率与N_{ST}的关系

(b) 合成成功率误差与N_{ST}的关系

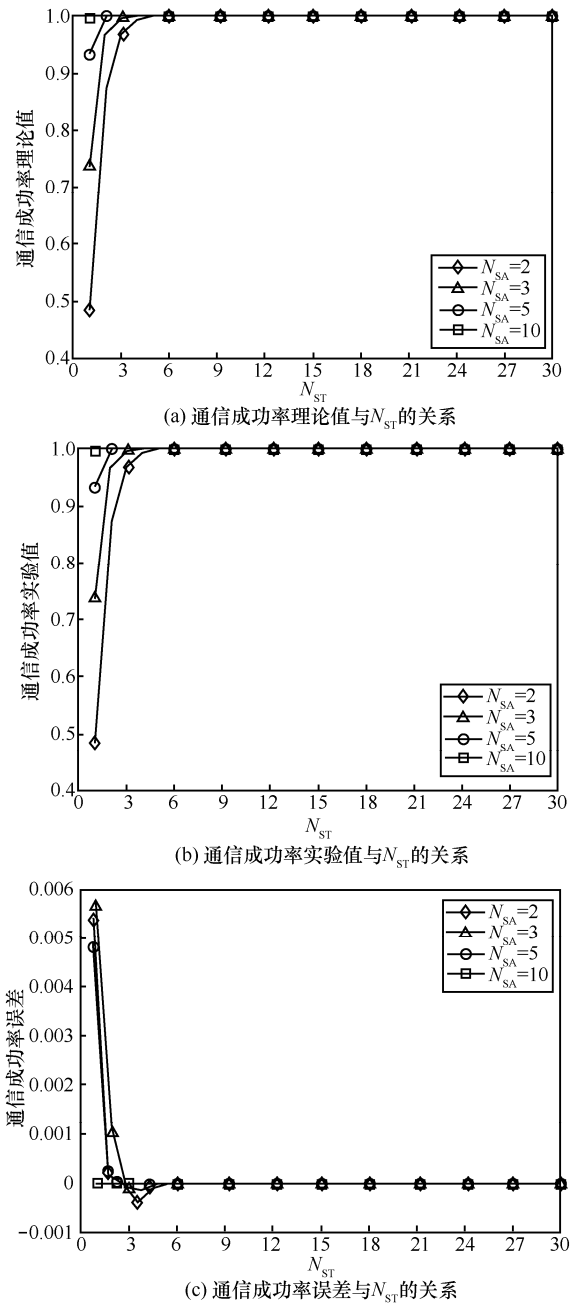
图 3 合成成功率及误差与 N_{ST} 的关系

图 3(a)表示合成成功率的实验值和理论值分别与 N_{ST} 之间的关系；图 3(b)表示合成成功率误差与 N_{ST} 之间的关系。可以看出，理论值和实验值的误差很小，最大只有 0.37%。当满足 N_{ST}>7 时，合成成功率逐渐趋近于 1。

2) 通信成功率

在验证通信成功率的实验中，设定 N_{SA}={2,3,5,10}，仿真结果如图 4 所示。

由图 4 可以看出，通信成功率的理论值与实验值误差很小。通信成功率不仅随着 N_{ST} 的增加而上升，同时也随着 N_{SA} 的增加而上升。但无论 N_{SA} 取何值，当 N_{ST}>5 时，通信成功率几乎为 1，误差几乎为 0。



(a) 通信成功率理论值与N_{ST}的关系

(b) 通信成功率实验值与N_{ST}的关系

(c) 通信成功率误差与N_{ST}的关系

图 4 通信成功率及误差与 N_{ST} 的关系

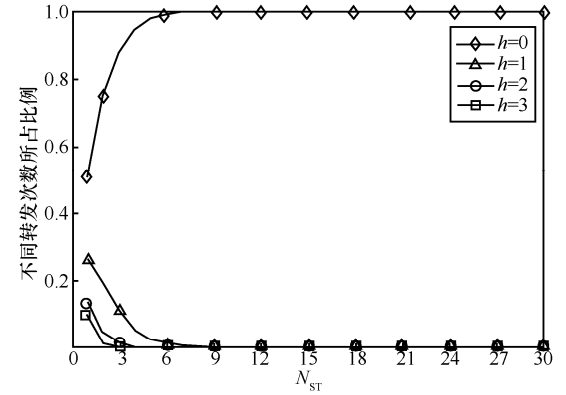
3) 平均接入延时

为测试平均接入延时，需要设定 D_I 和 D_P。首先给出访问请求在互联网中的传输延时 D_I 的设置依据。文献[14]指出网络延时一般在数十毫秒级别。用户通过互联网接入泛联路由平台，因为服务接入点（SAN）距离所属的区域数据中心（region）跳数较少，且泛联路由平台具有高带宽、低延时的特点。所以可忽略 SAN 到所属区域数据中心的传输延时，这样就可将用户请求到区域数据中心的延时等效成用户请求到 SAN 的延时。一般情况下用户

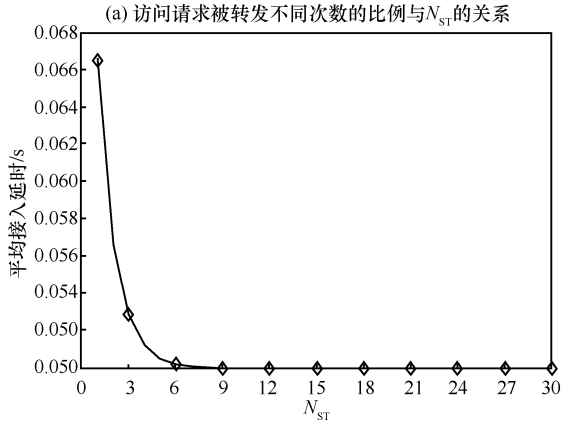
访问请求到不同区域数据中心的传输延时主要和两者的相对位置有关，如国内某用户到 Amazon AWS 云平台不同区域数据中心的延时在几十毫秒到几百毫秒之间。因此，设定 D_{I}=0.05 s 符合实际情况。

接下来，给出 D_{P} 的设置依据。转发延时包括 SAN 节点处理延时和 SAN 节点间的传输延时。由于泛联路由平台内部高带宽、低延时，因此忽略传输延时，仅考虑 SAN 处理延时。在真实网络中，SAN 的处理包括服务的鉴权（判断请求服务的用户是否有资格获得服务）、对用户进行认证（如 IPSec）、对服务的请求内容进行鉴别、对服务的条件进行判断。同时，要判断是否有可用的安全访问路径。对于到达 SAN 的访问请求，全网中 SAN 的处理流程均是透明统一的。因此，在访问请求被转发的时候，每经过一个 SAN 都要带来一定的处理延时。影响该延时的因素较多，如认证方式、用户请求并发数量等[15]。根据 QoS 的要求，处理时间一般应保持在毫秒级别[15~17]，在此将转发延时设置为 D_{P}=0.02 s。

最后设置 N_{SA}=10，保证有充足的 SAN 可供访问请求接入和转发。实验结果如图 5 所示。



(a) 访问请求被转发不同次数的比例与N_{ST}的关系



(b) 平均接入延时与N_{ST}的关系

图 5　不同转发次数占比及平均接入延时与 N_{ST} 的关系

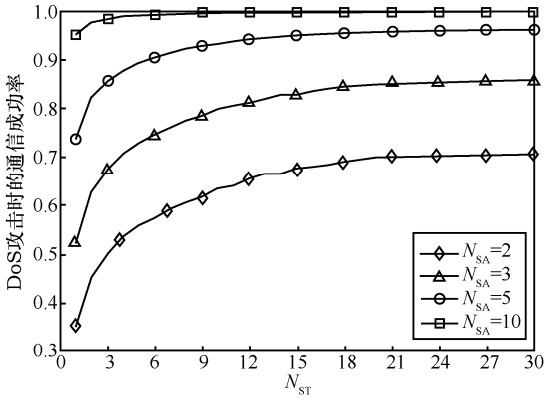
图 5(a)表示访问请求被转发 h(h=0,1,2,3)次的比例与 N_{ST} 之间的关系。图 5(b)表示平均接入延时与 N_{ST} 之间的关系。可以看出，当 N_{ST} 较小时，由于合成成功率较低，因此，访问请求在 Φ_{SA} 中的转发次数较多，不同转发次数的访问请求各占一定比例，从而导致平均接入延时较高。而随着 N_{ST} 的增加，合成成功率迅速趋近于 1，访问请求也可以不经过转发而获取安全访问路径，同时，平均接入延时也逐渐减小，最终 $D_{\text{A-AVERAGE}}$=D_{I}=0.05 s。

4.3　SAPA 防御 DoS 攻击性能分析

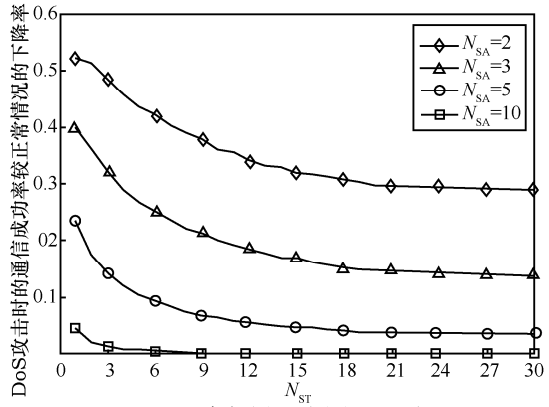
为分析 SAPA 防御 DoS 攻击性能，假设 DoS 攻击者不知道路由节点角色，随机选取部分节点作为攻击目标；攻击者拥有足够的资源，能够保持攻击强度不变，即能够保持同时攻击的节点数目 N_{A} 不变。

1) DoS 攻击对通信成功率的影响

在测试 DoS 攻击对通信成功率影响的实验中，设定 N_{A}=10。测试不同 SAN 数目下，通信成功率与 N_{ST} 的关系如图 6 所示。



(a) 通信成功率与N_{ST}的关系



(b) 通信成功率下降率与N_{ST}的关系

图 6　DoS 攻击对通信成功率的影响与 N_{ST} 的关系

由图 6 可以看出，当受到 DoS 攻击时，随着 N_{ST} 的增加，通信成功率仍然保持上升趋势，但同

正常情况相比，上升趋势有所减缓。N_{SA} 取不同数值时的通信成功率均有所下降。SAN 越多，通信成功率越高，下降率越低。在 N_{SA}=10 时，通信成功率基本不受 DoS 攻击的影响。

2) DoS 攻击对平均接入延时的影响

同样设置 D_I=0.05 s，D_P=0.02 s，N_{SA}=10。实验结果如图 7 所示。

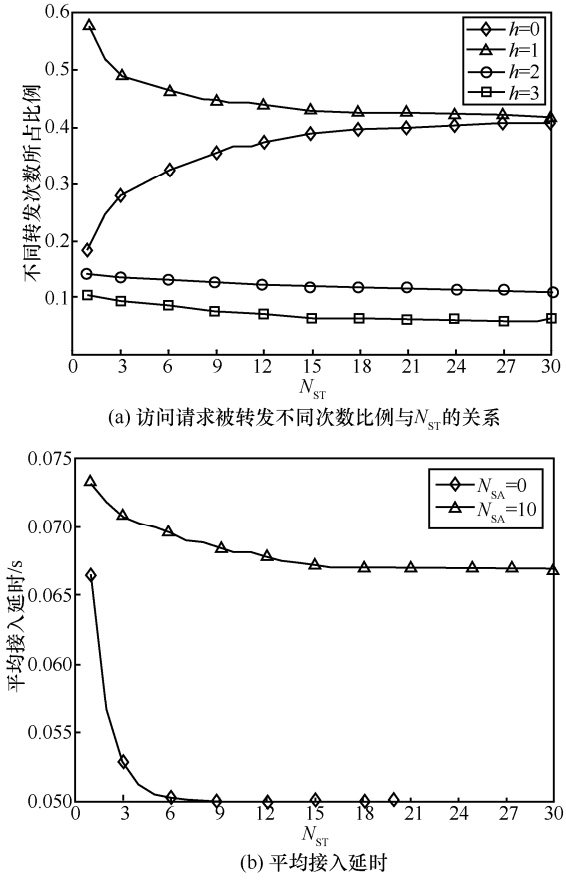


图 7　DoS 攻击下访问请求被转发不同次数占比及平均接入延时与 N_{ST} 的关系

图 7(a)表示 DoS 攻击下访问请求被转发不同次数的比例。图 7(b)比较了在 N_A=0 与 N_A=10 情况下的平均接入延时。可以看出，当受到 DoS 攻击时，访问请求在 Φ_{SA} 中转发 1 次所占比例较正常情况明显增加，最终达到 40%；转发 2 次和转发大于或等于 3 次所占比例也较正常情况明显增加，分别为 13%和 8%。随着 N_{ST} 的增加，SAN 能够合成安全访问路径的概率增加，从而访问请求被转发 0 次的数量增加，被转发 1 次、2 次以及大于或等于 3 次的数量有所下降。在 DoS 攻击下，由于仍然有大部分被转发多次的访问请求存在，因此，平均接入延时明显高于正常情况下的接入延时。

以上实验结果说明基于 SAPA 的 DoS 攻击防御方法有较好的效果。只要设置一定数量的角色节点，SAPA 就可以有效地缓解 DoS 攻击的影响，保证正常的通信成功率和接入延时。在实际应用中，N_{SA} 与 N_{ST} 需要保持相对均衡与稳定，以避免在 SAN 或 STN 处形成瓶颈链路，导致网络拥塞。同时，设置适当的 N_{SA} 与 N_{ST}，将访问请求分散至整个路由平台，无需添加其他的负载均衡策略，减少系统冗余。

4.4　SAPA 与 SOS 防御 DoS 攻击性能的比较

如上所述，传统的 SOS 也具有防御 DoS 攻击的能力。为了能更好地与 SOS 方法进行比较，本文将 4.1 节中 OMNeT++下的实验环境扩展到 Test-bed 中。下面分别给出 OMNeT++和 Test-bed 的实验结果。

文献[10]已经证明当 SOS 中的 3 种角色节点个数分别取 10 的时候可以达到良好的防御效果。同样，本文经过 OMNeT++仿真验证，在 SAPA 中当 SAN 与 STN 分别为 10 时也能达到良好的效果。因此，实验中设置 SAPA 的 SAN 与 STN 分别为 10，更新周期为 5 s。随机选取 10 个节点作为攻击目标，攻击在 15 s 的时候开始，至 40 s 结束。在相同的仿真环境和 Test-bed 平台下测试 SAPA 和 SOS 防御 DoS 攻击的性能。

安全覆盖网在逻辑上是一个环形网络[18]，而在物理上可以通过交换设备进行星型连接。Test-bed 实验拓扑如图 8 所示[10,18,19]，该实验环境符合云计算泛联路由平台架构，具有一定代表性。

User 端运行访问请求发生程序，在实验中模拟用户发起 HTTP 访问请求。PC1~PC64 分别通过交换机连接在 2 台路由器上，用来模拟泛联路由平台中的 64 个节点。PC1~PC64 的配置：Intel(R) Core(TM) i3-4370 CPU 3.80 GHz，4 GB 内存，运行 Linux Redhat 5.5，每台 PC 上加载 SAPA 和 SOS 规则。其中，SOS 的实现采用美国哥伦比亚大学的源代码。Server 采用一台 DELL R710 服务器，模拟云计算数据中心响应用户的请求，并向 64 个节点广播控制消息以周期性改变节点角色，每个周期随机选取 10 个 SAN 和 10 个 STN。攻击者回放 CERNET 上采集到的 DoS 攻击数据集，随机选取 10 个节点发起 DoS 攻击。实验平台中 4 台路由器采用 CISCO 2911，其间均配置 1 Gbit/s 的带宽。

关注通信成功率随时间的变化情况，实验结果如图 9 所示。可以看出，不论是 OMNeT++实验还是 Test-bed 实验，通信成功率的变化趋势一致，都说明 SAPA 的性能更好。

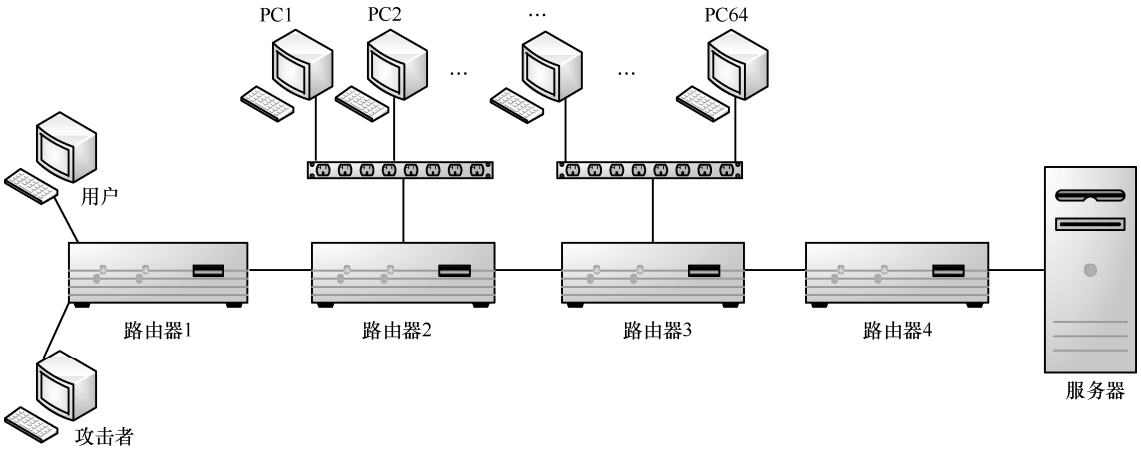


图 8　Test-bed 实验环境

如图 9 所示，当攻击未开始时，SAPA 与 SOS 保持良好的通信成功率。攻击开始后，SAPA 与 SOS 的通信成功率出现下降，且 SOS 下降幅度更大。SAPA 在经过每个周期的节点更新后，通信成功率可维持在较高的水平，而 SOS 在攻击持续期间，通信成功率一直维持在较低水平，直到攻击结束才得以恢复。

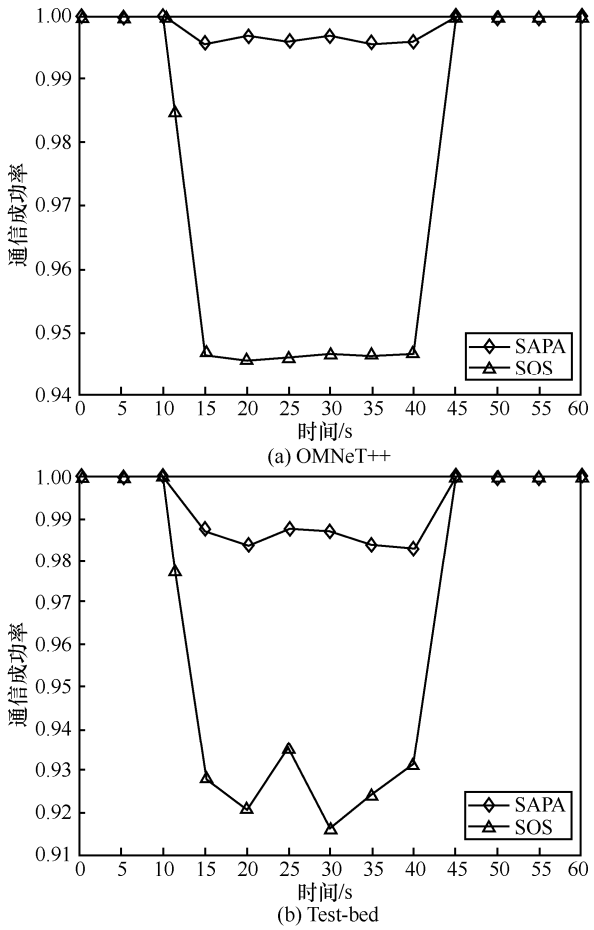


图 9　SAPA 与 SOS 通信成功率比较

以上结果说明 SAPA 相较于 SOS 有更好的安全性，其原因主要在于以下 2 点。1) SOS 的角色节点多，因此被随机选取作为攻击目标的可能性较大，尤其是当 SOS 的指引节点（beacon node）受到攻击时，会导致与其相关联的安全接入节点（SOAP）与秘密节点（secret node）均失效[10]。当角色节点被攻击下线时，通信成功率必然下降更多。2) SAPA 是周期式地更新角色节点，因此有可能在攻击结束前就更新了角色节点，这些更新的角色节点是未被攻击节点的可能性较大，这样一来通信成功率就得以保证。而 SOS 在攻击结束前，都会保持被攻击节点从安全覆盖网下线，这必然导致通信成功率降低。

进一步，在实验中统计比较单位时间内 2 种算法处理访问请求的数量，结果如表 1 所示。

表 1　　单位时间内处理访问请求的数量

方法	无 DoS 攻击/（次·秒$^{-1}$）	有DoS攻击/（次·秒$^{-1}$）
SOS（OMNeT++）	4 667	3 209
SAPA（OMNeT++）	7 299	6 582
SOS（Test-bed）	4 459	3 071
SAPA（Test-bed）	7 024	6 344

由表 1 可以看出，相较于 SOS 方法，SAPA 单位时间内处理的访问请求更多。这主要是因为在接入节点相同的情况下，SAPA 角色节点总数少，同时，采用了缓存安全访问路径的方法，在应对云计算大量高并发的访问请求时，能够缩短访问延时，提高用户访问效率。尤其是在 DoS 攻击下，SAPA 的优势更为明显。

5　讨论

尽管本文针对云计算环境下的 DoS 攻击，提出

了基于 SAPA 的防御方法，并比较证明了其有效性。但仍存在一定局限性，有待于更加深入的研究。

1) 本文的研究是建立在泛联路由 3 层模型的基础上，但是随着云计算的发展，云计算数据中心外部的网络架构可能呈现出多变的趋势，此时安全访问路径算法有可能会受网络架构的限制。尤其在小规模私有云扁平化网络架构下，网络节点较少，角色节点数量比较有限，可能导致 SAPA 的性能欠佳。在未来的研究中，考虑不同云计算路由平台的异构性，从安全覆盖网的拓扑结构和节点协同的角度，设计更为理想的安全访问策略。

2) 对于直接以云计算数据中心为目标的 DoS 攻击而言，SAPA 算法设计的前提是 SAN 能够准确判断一个数据流是正常流还是 DoS 攻击流。然而随着攻击手段的进步或新漏洞的挖掘，攻击者有可能绕过 SAN 的认证。这一问题在 SOS 中同样存在，如何解决该问题是未来的研究工作之一。计划从安全管理和漏洞评估的角度开展进一步研究。

3) 目前的实验是在 OMNet++仿真环境和小规模的 Test-bed 平台下开展的。期望以后能够在更大规模、更复杂的开源云平台下部署本文提出的方案，完成测试工作。

6 结束语

本文以云计算路由平台的分层特性为基础，以保护云计算数据中心以及云计算核心路由为目标，以改进 SOS 为手段，设计了一种新的基于安全访问路径算法 SAPA 的 DoS 攻击防御方法。首先，建立了 SAPA 的数学模型，完成了对安全访问路径算法的理论分析。然后，通过实验验证了 SAPA 的性能并与 SOS 方法进行比较。实验结果证明，SAPA 能够保证良好的通信率和足够小的访问延时。在防御 DoS 攻击方面，SAPA 比 SOS 更适用于云计算平台，防御效果更佳。

云计算中 DoS 攻击与防御是一个无休止的博弈过程，如何主动、高效、快速地防御 DoS 攻击，仍然面临许多挑战。云计算集成了虚拟化、数据中心网络、软件定义网络和大规模数据处理等技术，其开放性、复杂性、分布式和异构性导致能做的工作还比较有限，针对某些问题的解决方案还需要进一步地分析和完善。在未来的研究中，还需特别关注云计算的新漏洞以及各种变种的 DoS 攻击方式。结合云平台自身的新特性，灵活运用云计算的心跳机制、克隆技术、弹性机制等新技术设计 DoS 攻击检测和防御方法。

参考文献：

[1] CHANG R K C. Defending against flooding-based distributed denial-of-service attacks: a tutorial[J]. IEEE Communications Magazine, 2002, 40(10): 42-51.

[2] CHONKA A, XIANG Y, ZHOU W L, et al. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks[J]. Journal of Network and Computer Applications, 2011,34(4): 1097-1107.

[3] YU S, TIAN Y H, GUO S, et al. Can we beat DDoS attacks in clouds?[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(9):2245-2254.

[4] GIRMA A, GARUBA M, LI J, et al. Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect ddos attacks on cloud computing environment[C]//12th International Conference on Information Technology-New Generations. 2015: 212-217.

[5] OSANAIYE O A, DLODLO M. TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment[C]//EUROCON 2015 International Conference on Computer as a Tool. 2015: 1-6.

[6] LIU Z G, YIN X C, LEE H J. A new network flow grouping method for preventing periodic shrew DDoS attacks in cloud computing[C]//2016 18th International Conference on Advanced Communication Technology (ICACT). 2016: 66-69.

[7] 韩志杰，段晓阳. 基于云计算平台的防御拒绝服务攻击方法[J]. 信息化研究, 2011,37(5):67-69.
HAN Z J, DUAN X Y. Defense strategy of denial of service attacks based on cloud computing platform[J]. Informatization Research, 2011, 37(5): 67-69.

[8] 韩伟. 基于 Hadoop 云计算平台下 DDoS 攻击防御研究[D]. 太原: 太原科技大学,2011.
HAN W. DDoS attack defense research based on Hadoop cloud computing platform[D]. Taiyuan: Taiyuan University of Science and Technology, 2011.

[9] 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[J]. 通信学报, 2015, 36(1): 1-8.
WU Z J, CUI Y, YUE M. VHSAP-based approach of defending against DDoS attacks for cloud computing routing platforms[J]. Journal on Communications, 2015, 36(1): 1-8.

[10] KEROMYTIS A D, MISRA V, RUBENSTEIN D. SOS: secure overlay services[C]//The 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. 2002.

[11] KEROMYTIS A D, MISRA V, RUBENSTEIN D. SOS: an architecture for mitigating DDoS attacks[J]. IEEE Journal on Selected Areas in Communications, 2004, 22(1): 176-187.

[12] 卢国强. 云计算环境下的泛联路由平台[J]. 信息安全与技术, 2010(8): 106-108.
LU G Q. Tum routing platform in cloud computing[J]. Information Security and Technology, 2010(8): 106-108.

[13] STOICA I, MORRIS R, LIBEN-NOWELL D, et al. Chord: a scalable peer-to-peer lookup protocol for internet applications[J]. IEEE/ACM Transactions on Networking, 2003, 11(1): 17-32.

[14] 刘孟. 云环境下 DDoS 攻击攻防体系及其关键技术研究[D]. 南京: 南京大学, 2016.
LIU M. Architecture of DDoS attacks defense in cloud environment and its key technology[D]. Nanjing: Nanjing University, 2016.

[15] ZOLTAN F, PETER F, STEFAN L, et al. Performance analysis of IPsec in mobile IPv6 scenarios[C]//The 16th IST Mobile and Wireless Communication Summit. 2007:1-5.

[16] KHALED S, KHALID E, RAOUF B. Performance modeling and analysis of network firewalls[J]. IEEE Transactions on Network and Service Management, 2012, 9(1):12-21.

[17] LIU M, DOU W C, YU S, et al. A decentralized cloud firewall framework with resources provisioning cost optimization[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(3): 621-631.

[18] MOREIN W G, STAVROU A, COOK D L, et al. Using graphic turning tests to counter automated DDoS attacks against Web servers[C]//The 10th ACM Conference on Computer and Communications Security. 2003: 8-19.

[19] ANGELOS S, DEBRA L C, WILLIAM G M, et al. WebSOS: an overlay-based system for protecting Web servers from denial of service attacks[J]. Journal of Computer Networks, 2005, 48(5):781-807.

作者简介：

岳猛（1984-），男，河北沧州人，天津大学博士生，中国民航大学讲师，主要研究方向为网络安全、云计算。

李坤（1989-），男，新疆奎屯人，中国民航大学硕士生，主要研究方向为网络与信息安全。

吴志军（1965-），男，河南固始人，博士，中国民航大学教授、博士生导师，主要研究方向为网络与信息安全。