doi:10.11959/j.issn.1000-436x.2015004

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

吴志军，崔奕，岳猛
（中国民航大学 天津市智能信号处理重点实验室，天津 300300）

摘 要：防御分布式拒绝服务 DDoS（distributed denial of service）攻击是云计算平台安全保护中的一个关键问题。在研究大规模网络防御 DDoS 攻击的安全覆盖服务 SOS（security overlay service）方法的基础上，揭示了 SOS 在节点被攻击时退出机制存在的安全漏洞，根据云计算路由策略改进了一致性散列算法 Chord，提出了适用于云计算路由平台 3 层架构的虚拟散列安全访问路径 VHSAP（virtualization hash security access path），在安全访问路径中引入了心跳机制，利用虚拟机技术实现弹性的虚拟节点，完成在云平台中被攻击节点之间的无缝切换，保证用户对云计算平台的安全访问。针对 VHSAP 防御 DDoS 的性能进行了仿真实验，重点研究了在散列安全访问路径 HSAP 中被攻击节点数和切换时延等参数，并将实验结果与 SOS 方法进行了比较。实验结果表明在 DDoS 攻击下，VHSAP 具有较高的数据通过率，可以提高云计算平台的安全性。
关键词：云计算；路由平台；DDoS；一致性散列；虚拟化；无缝切换
中图分类号：TP393.08 **文献标识码**：A

VHSAP-based approach of defending against DDoS attacks for cloud computing routing platforms

WU Zhi-jun, CUI Yi, YUE Meng
(Tianjin Key Laboratory for Advanced Signal Processing, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Based on the analysis of security overlay service (SOS) approach of defending against DDoS attacks in large scale network, the vulnerability in the exit mechanism of being attacked nodes in SOS approach is explored. The vulnerability is solved by improving the Chord algorithm according to the routing strategy in cloud computing. Hence, the virtualization hash security access path (VHSAP) in three-layer structure is proposed to protect the cloud computing platform. In VHSAP, the heartbeat mechanism is applied to realize virtual nodes by using the virtual technology. Therefore, the virtual nodes have the ability of resilience, which can complete the seamless switching between being attacked nodes in cloud computing platform, and guarantee the legitimate user's authority of accessing to the resource in cloud computing platform. Experiments of VHSAP defending against DDoS attacks are carried out in simulation network environment. The parameters, such as the number of being attacked nodes in hash secure access path (HSAP), and the switching time and the handoff delay between nodes, are focused in experiments. The result shows that VHSAP achieves a higher data pass rate than that of SOS approach, and enhances the security of cloud computing platform.
Key words: cloud computing; routing platforms; DDoS; consistent hashing algorithm; virtualization; seamless switch

收稿日期：2013-06-04；**修回日期**：2014-03-06
基金项目：国家自然科学基金资助项目（61170328，U1333116）；天津市应用基础与前沿技术研究计划基金资助项目（12JCZDJC20900）；2013 年民航科技引导基金资助项目（MHRD20130217）；中国民航大学科研平台建设基金资助项目；中央高校基本科研业务费基金资助项目（3122013P007, 3122013D007, 3122013D003）
Foundation Items: The National Natural Science Foundation of China (61170328, U1333116); The Key Project of Tianjin Natural Science Foundation (12JCZDJC20900); Civil Aviation Science and Technology Innovation Fund (MHRD20130217); Research Laboratory Construction Funds of Civil Aviation University of China; Fundamental Research Funds for the Central Universities (3122013P007, 3122013D007, 3122013D003)

1　引言

分布式拒绝服务攻击 DDoS（distributed denial of service）是云计算面临的安全威胁之一[1]。随着虚拟化数据中心和云服务的快速发展，针对云计算的 DDoS 攻击也由发送大流量攻击数据分组的暴力式攻击转变为针对基础应用程序的技术性攻击。DDoS 攻击可以造成云计算平台瘫痪，导致其无法向云用户提供正常服务，经济损失和社会影响巨大[2]。2012 年 8 月初，著名的维基揭秘遭到 DDoS 攻击而瘫痪。因此，防御 DDoS 攻击是云计算平台面临的首要问题。

从防御角度来看，云计算平台防御 DDoS 攻击的策略可以分为外部和内部 2 个层面。云内部的安全取决于云计算基础架构及其应用和服务的需求和特点。而云外部安全，主要是指从通过互联网访问云计算中心的访问路径上考虑防御 DDoS 攻击，保证云计算中心的可靠性和可用性。根据云用户与云计算中心之间的云计算泛联路由平台的结构特点，提出改进的一致性散列（consistent hash）算法，利用安全覆盖网服务 SOS[3]构建虚拟散列安全访问路径 VHSAP，在访问路径中采用心跳机制，利用虚拟化技术实现弹性节点，能够实现云计算外部防御 DDoS 攻击的功能。

2　相关工作

针对大规模网络基于安全访问路径 SAP 防御 DDoS 攻击的方法，现有研究成果很多，许多学者提出了创新性的方法。IEEE 成员 Angelos D Keromytis 等提出了一种安全覆盖网络服务 SOS，利用强大过滤功能和安全隧道技术，能够有效阻止 DDoS 攻击，并利用一致性散列 Chord 协议针对接入点有可能被攻击者扫描并攻击提出解决方法[3]。之后，Angelos D Keromytis 又假设攻击者可能针对 SOS 方法中的接入节点进行集中攻击，并提出对客户的接入方式进行改进，使用户能够随机通过多个接入节点进入 SOS 结构，进而避免被攻击者追踪到[4]。IEEE 成员 Xun Wang 等针对原覆盖网络的结构提出入侵攻击与拥塞攻击结合的新型攻击方式，并通过改变结构层数、映射度数、节点数等参数来分析安全覆盖网络服务性能[5,6]。以上方法虽然提出了新的攻击方式，但是都没有考虑到 SOS 节点受到攻击后应对方式的问题。Chi Hyung In 等针对原覆盖网络安全措施的漏洞提出突发式攻击与渐变式攻击来提高攻击效率，并提出对网络流量使用聚类方法检测流量异常[7]。但是此方法需要所有 SOS 中的节点进行联动，不仅实施复杂，还需要处理大量的数据流量以建立规则库，这对 SOS 节点本身就是一种负担。Ramanpreet Kaur 等则总结说明了目前为止针对 SOS 结构可能出现的各种攻击方式[8]。通过以上分析，提出了一种在不增加 SOS 结构负担的前提下，能够使 SOS 节点很好应对攻击的云计算路由平台策略。

3　云计算路由平台的散列安全访问路径 HSAP 结构

云计算的数据传输平台也称为泛联路由平台[9]。它承载着云计算中海量的信息数据。它通过各层次路由设备的接入和业务处理能力，满足云计算数据中心对终端用户业务提供的高可用、易用和可扩性。云计算路由平台具有层次化的特点，通常分为 3 层：核心层、中间层和接入层。云用户发送的请求经接入层路由通过中间层路由和核心层路由到达云计算中心。

3.1　散列安全访问路径 HSAP 结构

通过研究层次化云计算路由平台的结构，结合应用于对等 P2P（peer-to-peer）网络的 SOS 的访问策略[3]，提出了基于云计算路由平台的散列安全访问路径 HSAP (hash SAP)，其结构如图 1 所示。

散列安全路径 HSAP 在采用一致性散列算法 Chord[9]的应用层路由方式的同时，结合层次化网络拓扑结构的特点，在保证滤除 DDoS 攻击流的同时，使路由方式尽量适合层次化的物理拓扑。

HSAP 以云计算中心为目标，分别在核心层、中间层、接入层中设置部分节点作为 HSAP 中的秘密节点、指引节点和安全接入节点[3,4]。云用户如果需要访问云计算中心，首先会将请求发送至接入层节点。如果该节点不是安全接入节点，则会将请求转发到相邻的安全接入节点上。安全接入节点对请求进行身份验证后按照一致性散列算法 Chord[10]向上一层指引节点进行路由转发，通过指引节点将数据分组转发至秘密节点。最后，秘密节点再将数据分组转发至目标（云计算中心）。云计算中心周围的过滤器上设定的规则只允许来自于秘密节点的数据分组通过。合法云用户的数据分组传输的过程都是建立在应用层上的路由方式，而攻击者如果要对云计算中心发动攻击，就只能按照网络层的路由协议进行。

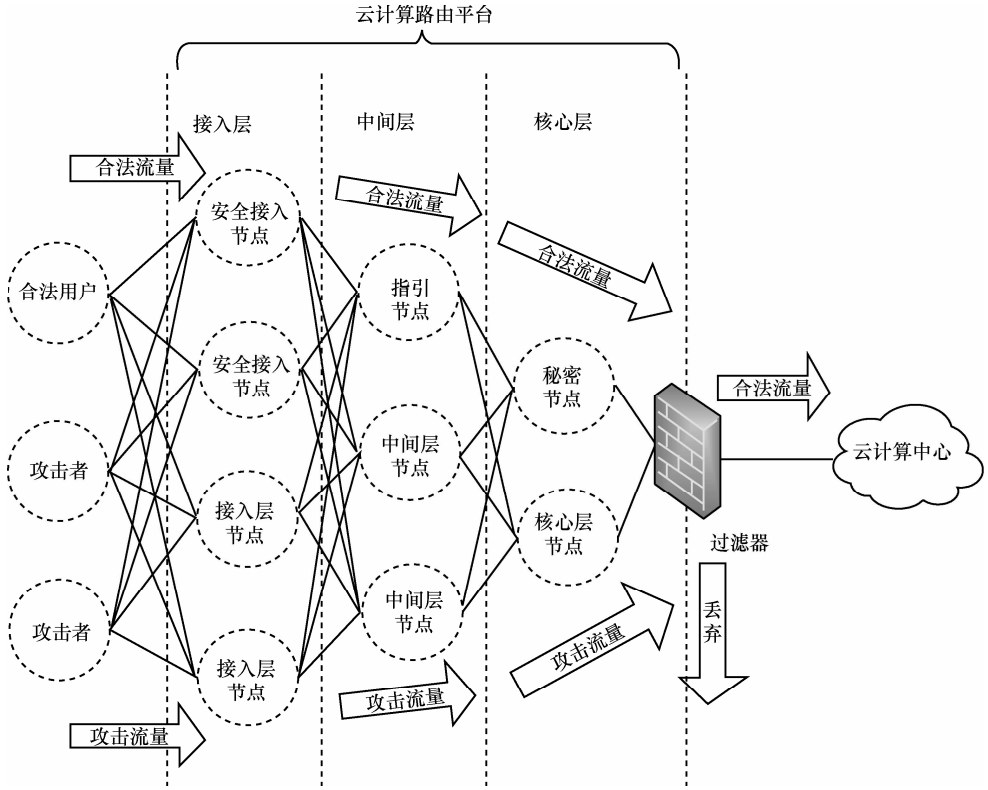

图 1 云计算路由平台散列安全访问路径结构

图 1 所示，HSAP 中的指引节点和秘密节点连接的路由器上均设定规则，丢弃不属于 HSAP 结构中的节点转发而来的数据分组，这样 DDoS 攻击者所发动的攻击流就必须要在 3 层转发中都能够选择通过 HSAP 的节点才有可能到达目标。

3.2 3 层转发的一致性散列算法

在云计算路由平台 3 层结构中所采用的路由算法的原型是应用于 P2P 网络的一致性散列算法 Chord[10]。在 P2P 网络中，Chord 将网络中所有节点的节点信息如 IP 地址进行散列映射，然后将节点标识符从小到大顺时针排列成一个环状，排列中的下一个节点就是环形中沿顺时针方向的下一个节点。为了使一致性散列的链路访问策略能够应用于 3 层的网络结构，将 Chord 的路由算法的查询步骤进行分解，只取前 3 次跳转，使其符合安全路径的结构。

1) 对云计算路由平台的节点的地址和目标服务器的地址进行散列运算，得出标识符，全部映射在 Chord 环上[3,4]。

2) 选取目标标识符的后向节点的顺时针之后的一个区域，这个区域称为安全接入区，区域的大小根据选取节点个数的需要可以在半个环之内任意选取。节点标识符在安全接入区内且位于云计算路由平台接入层的节点可以选取作为安全接入节点。在这安全接入区的顺时针 180°相对应的另外一部分区域称为指引区。节点标识符在指引区内且位于云计算路由平台中间层的节点可以选取作为指引节点。从指引区的最后一个节点到目标标识符的后向节点之间所形成的区域则称为秘密区。节点标识符在秘密区内且位于云计算路由平台核心层的节点可以选取作为秘密节点。秘密节点都存有目标节点的地址信息。当数据分组到达秘密节点时秘密节点不必再按照原 Chord 的路由方式继续往下查找，而是直接将数据分组送往目标地址。未被选取到的节点则不在散列安全路径结构内，排除 Chord 环，不参与 Chord 路由过程[3,4]。

3) 在 Chord 算法[10]中，当安全接入节点查询过程指针表最大表项对应的节点的后向节点在指针区不存在或发生故障时，那么按照原 Chord 算法，指针表中这些安全接入节点的指针表将会超过指引区的范围将秘密区的节点作为查询的对象。因此，对 Chord 的节点指针表进行了改进，在安全接入节点上增加判断，如果其查询目标对应的后向节点的值超过了指针区的标识符的范围，则不能继续顺时针选择下一个节点，而是选择指针区中标识符

最大的节点。这样设计可以保证该策略在受到攻击时，不会出现安全接入节点转发而来的数据分组由于指引节点的下线而直接映射到秘密区的节点上。

当总节点数为 64 时，改进的基于 Chord 环的 3 层划分结构[10]如图 2 所示。在图 2 中，接入层节点 *N*16 要将经过认证后的合法用户的数据分组顺时针传递。通过其指针表即可看出，其下一跳转的节点为 *N*58，超过了指引区的范围。将其修改为指引区中标识符最大者即 46。当数据分组被转发至标识符为 46 的节点上时，此节点再通过指针表找出下一跳的节点为 *N*3。当节点 *N*3 接收到数据分组时则不管自己是否是目标标识符的后向节点，直接将数据分组转发到自身已经保存的目标服务器的地址。通过这种转发流程，就能够完成数据分组在散列安全路径中的 3 层路由转发。

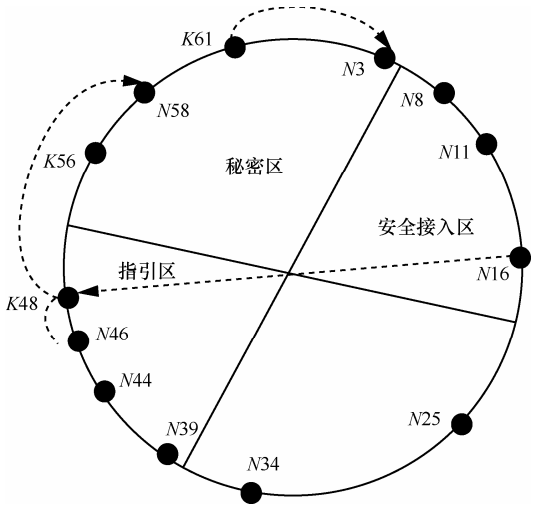

图 2　改进的 64 个节点 Chord 环的 3 层划分示意

图 2 中，假定 *K*61 为目标标识符。节点 *N*16 的指针表改变前后的对比情况如表 1 所示。

表 1　　节点 *N*16 的指针表改变前后的对比

改变前		改变后	
查询标识符项	后向节点	查询标识符项	后向节点
$16+2^0$	25	$16+2^0$	25
$16+2^1$	25	$16+2^1$	25
$16+2^3$	25	$16+2^3$	25
$16+2^3$	25	$16+2^3$	25
$16+2^4$	34	$16+2^4$	34
$16+2^5$	58	$16+2^5$	46

3.3　虚拟化的安全节点

采用 Chord 算法[10]能够有效地减轻恶意数据分组对目标服务器的影响。但是，云计算路由平台自身也可能成为攻击者的目标。假设攻击者能够实时掌握到云计算路由平台节点的信息，即攻击者能够对处于云计算路由平台 3 层结构中的所有节点发动攻击。根据 Keromytis[3]在安全覆盖网络服务 SOS 中的描述，它的特性之一就是其中任何一个节点被攻击，则该节点都会简单地退出覆盖网络[3,7]。因此，SOS 方法容易遭受周期性变换目标的节点攻击。另外，一致性散列链路策略的自我修复特性能够通过周期性的稳定化过程完成故障节点的排除，防止故障节点影响网络正常通信。但上述 2 种机制都会造成网络中节点数的快速消耗。即使能够实时地对整个云计算路由平台进行监测并采用计算机重启的方法也不能够彻底解决这个问题，而且频繁的重启对计算机硬件的损耗也很大。

因此，针对 SOS 方法容易遭受周期性节点攻击的缺陷，提出了一种改进方法。

1) 虚拟化节点。利用虚拟机技术[11]，在不增加原有网络结构开销的情况下，在每一台宿主机上分出多台虚拟机，将网络中的节点转换为大量的虚拟节点。将大部分的虚拟节点作为安全结构中节点的备份节点，通过对安全结构中节点状态的实时监测，及时将备份的虚拟节点替换现有的被攻击节点，加入 Chord 环中进行工作。其中，为了保证安全路径内备用虚拟节点能够接替 Chord 环上原节点的工作，每台宿主机上的虚拟节点标识符应是连续排列在一起的。通过新旧节点的无缝切换，就能够将攻击对节点的影响降低到最小，保证通信顺利进行。

2) 心跳机制。为了能够实时地监测到整个云计算路由平台节点的健康状况，在 VHSAP 中引入心跳机制[12]，如图 3 所示。

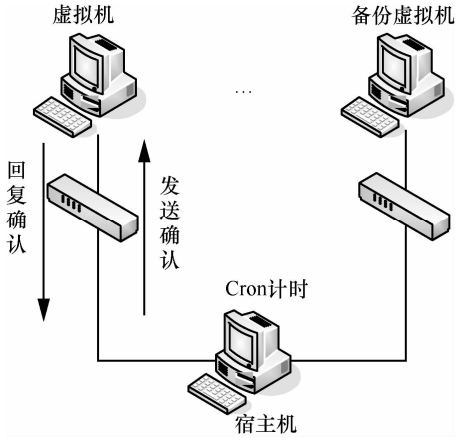

图 3　心跳机制示意

心跳机制定期向目标发送探测分组并等待其回应。如果目标超时后仍无回应，就代表目标已经失效，进行报警。此时，安全路径内的备份虚拟节点按照 Chord 算法开始加入 Chord 环，获取自身的后向节点并改变后向节点的前向节点。而 Chord 环也会在周期性的稳定化过程中在指针表中排除失去响应的节点，并加入新节点，完成一次修复。由于故障节点是虚拟化的，所以重新配置过程比较方便，能够容易地在新节点加入网络的时间内完成。其中，心跳分组的间隔应小于攻击与修复周期。目前，许多心跳测试工具均能够达到 0.1 s 的心跳分组间隔[13]，所以采用 0.1 s 的心跳分组间隔，能够连续地监控 Chord 环中节点的健康状态。而 0.1 s 的心跳分组间隔远小于后续实验中攻击与修复周期，对于实验的影响非常小。因此，在后续实验中就将心跳分组间隔的时间略去不计。

4 实验及结果分析

利用 OMNeT++仿真工具[14]根据 HSAP 的结构，建立了网络分析模型，针对提出的 VHSAP 进行了实验。仿真模型分为 5 层，分别为用户、接入层、中间层、核心层、目标。主要仿真的是用户的合法数据分组通过云计算路由平台到达目标的过程。实验环境的拓扑结构如图 4 所示。

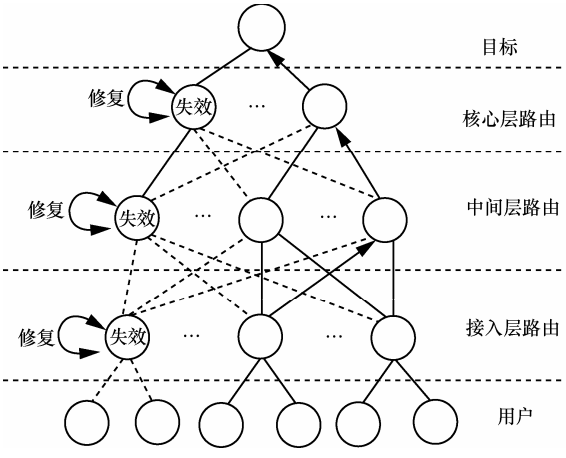

图 4 实验环境拓扑

图 4 中虚线表示失效链路，带箭头的路径为用户数据分组的安全路径示意。失效节点在周期修复后可以正常工作。首先在 3 层云计算路由平台节点上都预先设定每层间节点发送的对应规则，使其符合 Chord 环的规律。接着在路由平台节点中周期性随机抽选部分节点成为被攻击节点，同时也周期性的选择部分攻击节点进行修复。被修复的节点则根据采用的修复方式的不同，可以继续工作或直接退出网络。在目标节点上设定计数，统计所有到达目标的数据分组个数。

4.1 实验

由相关工作的分析可知，目前针对 SOS 网络防御策略的论文工作中，并没有针对 SOS 网络节点在受到攻击后的应对措施方面进行研究。因此在仿真中，主要是仿真验证在不同的参数下受到攻击后节点的应对措施方法的不同对网络通信成功率的影响，并且与 SOS 方法进行了比较分析。

1) 网络总节点数 N 与网络成功通信数据分组比例关系。

在网络总节点数 N 与分组丢失率关系的实验中，设定参数如下：攻击节点数选取 30；攻击周期为 1 s；修复周期为 1 s；各层散列安全路径的节点数分别为 12、6、3。仿真的结果如图 5 所示。

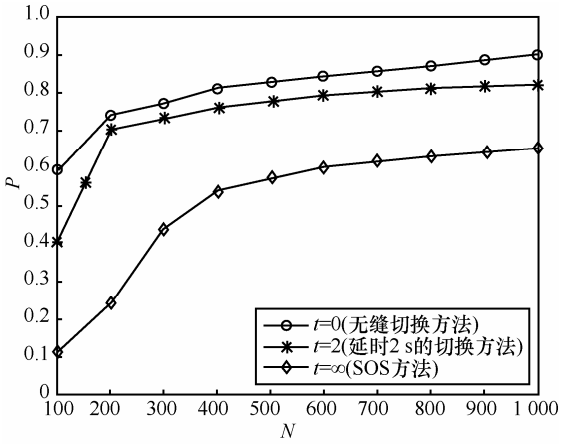

图 5 总节点数与网络成功通信数据分组比例的关系

图 5 中，横轴 N 代表网络中总节点数，纵轴 P 代表网络在一定时间内的数据通过率。其中，修复周期是指散列安全路径中 Chord 环将受到攻击的节点排除，并将准备好进行工作的新节点加入安全路径的时间。

图 5 中的 3 条曲线分别是不同总节点个数与网络数据通过率的关系。曲线的总体趋势都是随着总节点数上升，数据通过率上升。这是由于随着网络总节点数 N 的增加，使攻击者能够攻击到 HSAP 中节点的概率变小，数据分组丢失的概率自然就减小。而采用无缝切换方法的曲线数据通过率是最高的。即使在网络总节点个数较少的情况下，数据通

过率也能达到 60%以上。而当网络总节点数提升时，数据通过率能够达到 90%以上。

2) 网络攻击节点数 *Na* 与网络成功通信数据分组比例关系。

在网络攻击节点数 *Na* 与分组丢失率关系的实验中，设定参数如下：总节点数 *N* 设为 1 000；攻击与修复的速率之比为 1；各层散列安全路径的节点数分别为 120、60、30。仿真得到的结果如图 6 所示。

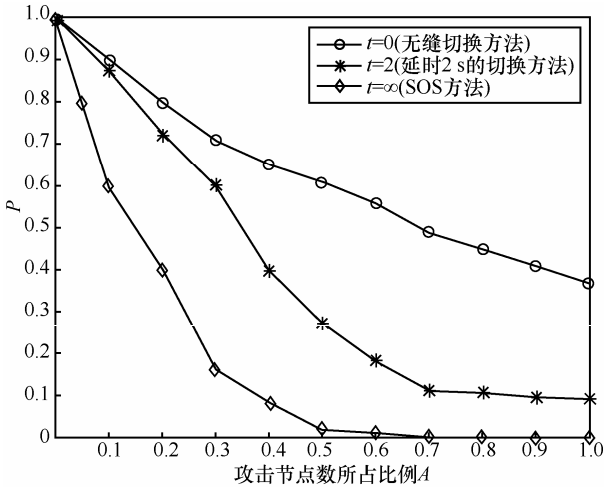

图 6　攻击节点数与网络成功通信数据分组比例的关系

图 6 中的 3 条曲线分别是不同切换时延下攻击节点数与网络数据通过率的关系。在没有攻击的时候，数据通过率是 100%，但是随着攻击节点的数量不断上升，数据通过率明显下滑。而采用了无缝切换的 HSAP 比带有延时的切换以及未采用切换的 HSAP 方法在保证网络正常通信的能力上更好。即使在网络被攻击的节点数较大时，无缝切换由于能够无间隔地替换故障节点，仍然能够保证数据通过率大约在 40%左右。而延时 2 s 的切换方法的数据通过率则在 10%左右，未采用节点切换方法的数据通过率则为 0。

3) 攻击与修复周期比 *w* 与网络成功通信数据分组比例关系。

在攻击与修复周期比 *w* 与数据通过率关系实验中，设定参数如下：总节点数 *N* 设为 1 000；攻击节点数 *Na* 为 300；保持修复间隔 1 s 不变；攻击间隔从 0.1 s 至 10 s 变化；各层散列安全路径的节点数分别为 120、60、30。仿真结果如图 7 所示。

图 7 中的 3 条曲线分别是不同切换时延下攻击与修复周期比与网络数据通过率的关系。

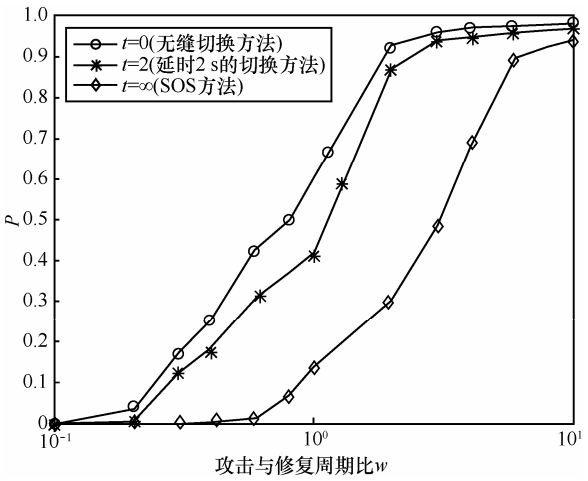

图 7　攻击修复周期比与网络成功通信数据分组比例的关系

从图 7 可以看出，随着攻击与修复周期比逐渐变大，整体网络的通信成功率是明显上升的。在攻击与修复周期比非常小的时候，攻击进行的较为频繁，攻击者经过较短的时间就能够找出散列安全路径上的节点并实施攻击，而网络修复却很慢。此时尽管采用无缝切换的方法，但是由于整体网络的修复过程执行周期相较于攻击周期太长，所以备份节点无法及时加入到安全路径中，因此，网络中数据通过率是很低的，尤其是当攻击周期接近于修复周期的 1/10 时，数据通过率接近于 0。但是当网络中攻击周期逐渐提升，攻击与修复的周期差距逐渐缩小时，网络中的数据通过率就开始迅速上升。当攻击周期是修复周期的一倍时，无缝切换方法的数据通过率已经达到了 90%以上，而此时未采用节点切换的方法数据通过率只有 30%。因此，图 7 结果表明采用无缝切换的方法能够比普通切换和无切换效果都好。

4) 备份节点切换时延 *t* 与网络成功通信数据分组比例关系。

在备份节点切换的时延 *t* 与数据通过率之间关系的实验中，设定参数如下：总节点数 *N* 设为 1 000；攻击节点数 *Na* 为 300；各层散列安全路径的节点数分别为 120、60、30。仿真结果如图 8 所示。

图 8 中的 3 条曲线分别是不同攻击与修复周期比下切换时延与网络数据通过率的关系。*t*=0 表示采用无缝切换方法时切换时延为 0；而实验时间设置在 10 s 以内，切换时延到 10 s 则代表原 SOS 的结构中不含有切换策略。

从图 8 可以看出，3 条曲线的通信成功率随着切换时延从 0 s 到 10 s 的增大均有 30%程度以上的

降低，这是因为切换时延的变大提高了攻击者攻击到散列安全路径节点的概率，从而降低了数据通过率。而当攻击周期比修复周期相比较大时，切换时延变化的影响并不明显。这是因为在攻击周期较大时，执行修复过程之后还可能有充足的时间进行节点的重启配置。而当攻击周期与修复周期接近或攻击周期比修复周期较小时，就能很明显地看出切换时延对数据通过率的影响。

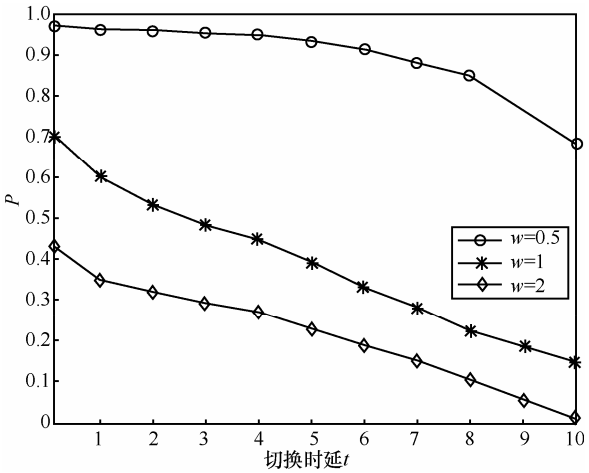

图 8 切换时延与网络成功通信数据分组比例的关系

在不同参数设置情况下，将本文无缝切换 VHSAP 方法与 SOS 的数据通过率进行了比对，如表 2 所示。

表 2 不同参数下 VHSAP 与 SOS 的数据通过率比较

参数配置/方法名称	通过率	
	VHSAP	SOS
N=100，*Na*=30, *w*=1	60%	11%
N=1 000, *Na*=30, *w*=1	91%	65%
N=1 000, *Na*=100, *w*=1	90%	60%
N=1 000, *Na*=500, *w*=1	62%	2%
N=1 000, *Na*=300, *w*=1	60%	14%
N=1 000, *Na*=300, *w*=2	93%	30%

通过表 2 结果分析，以及图 5~图 7 中 VHSAP 与 SOS 的实验曲线比较，可以得出：在变化总节点数、攻击节点数、攻击与修复周期比的情况下，采用无缝切换的访问策略在网络访问数据通过率方面都优于 SOS 策略。而从图 8 节点切换时延与数据通过率的关系可以看出：随着节点切换时延从零开始增长即从无缝切换到无切换的过程中，网络数据通过率呈现逐渐减小趋势。

实验结果分析表明：采用虚拟散列安全访问路径 VHSAP 的方法能够较好地应对 DDoS 攻击。

4.2 比较分析

现有成果中，检测网络异常的算法很多，其中，聚类和小波等方法比较典型。

1) 聚类方法：以探索的方式进行分析网络流量等的内在特点和规律。聚类方法进行网络异常检测首先需要建立数据库。因此，聚类分析就需要庞大的数据流量作为训练，往往较为依赖训练数据的质量。而且网络数据的种类复杂多样，实时的网络环境的变化要比异常检测的方法快很多，异常检测模型往往跟不上网络环境变化的速度。

2) 小波方法：将网络流量作为信号进行处理，用以检测流量中的突变点。小波方法仍然需要在节点上对采集的数据流量进行大量的计算得出结果，这样的方法只适合对于单目标网络进行异常检测。

提出的心跳机制与聚类、小波异常检测方法的分析比较如表 3 所示。

表 3 心跳机制与聚类、小波方法的特性比较

名称/项目	无需大量样本训练	应对更新快	无需进行大量计算	针对平台节点的防御
聚类分析	×	×	×	×
小波分析	√	√	×	×
心跳机制	√	√	√	√

提出的心跳机制采用虚拟散列安全路径的方法，该方法与聚类、小波等异常检测的算法相比其优势在于并不需要进行大量的数据训练样本，也不需要在节点上进行复杂的数学计算。同时，心跳机制配合虚拟散列安全路径并不仅仅是针对单个目标的异常检测，而是针对整个路由平台的节点进行有效的防御。

5 结束语

首先针对 DDoS 攻击对云计算中心的巨大威胁，提出将散列安全访问路径 HSAP 策略应用于保护云计算路由平台，通过对一致性散列 Chord 路由算法的跳转步骤进行分层对应，并根据分层区域的范围在节点指针表上加入判断，使基于云计算路由平台的一致性散列链路访问策略能够在保证滤除攻击流的同时改善原 SOS 结构的时延问题。本文研究与应用于大规模网络的安全覆盖网络服务 SOS 方法的区别在于 1）SOS 结构应用于无层次结构的

P2P 网络[3]，它是一种遵照 Chord 算法[10]，忽略物理拓扑的路由方式。这种路由方式虽然能够很好地滤除攻击流，但是同时也带来了很大的时延问题[3]。而 HSAP 通过云计算路由平台到达云计算中心只需要 3 次物理层次间的跳转，相比 SOS[3]结构中查询过程的多次无视物理拓扑结构的跳转能够节省大量的时间，时延较小；2）安全覆盖网络服务 SOS 具有被攻击节点简单地退出覆盖网络[3~7]的缺陷，容易遭受周期性节点攻击。采用心跳机制实时地监测到整个云计算路由平台节点的健康状况，采用虚拟机实现的弹性节点可以实时无缝的切换，在节省被攻击开销的同时，增强了抵御通过大量消耗云计算路由平台的节点来破坏云平台正常通信的攻击的能力。

在未来的研究中，尚需要解决的问题包括：1）在论述时已经假设攻击者是无法侵入安全接入点的，如果攻击者能够侵入安全接入点，那么其他防御功能就失去了作用；2）限于硬件开销的问题，若在同一时间内，云计算中心访问用户数量过多则有可能会造成链路拥塞，影响服务质量。

参考文献：

[1] 孙长华, 刘斌.分布式拒绝服务攻击研究新进展综述[J].电子学报, 2009, 37(7):1563-1568.
SUN C H, LIU B. Survey on new solutions against distributed denial of service attacks[J]. ACTA Electronica Sinica, 2009, 37(7):1563- 1568.

[2] 冯登国, 张敏, 张妍等.云计算安全研究[J].软件学报, 2012, 22(1):72-81.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2012, 22(1): 72-81.

[3] 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.

[4] STAVROU A, KEROMYTIS A D. Countering DoS attacks with stateless multipath overlays[A]. Proceedings of the 12th ACM Conference on Computer and Communications Security CCS '05[C]. Alexandria, Virginia, USA, 2005. 249-259.

[5] XUAN D, CHELLAPPAN S, WANG X, *et al*. Analyzing the secure overlay services architecture under intelligent DDoS attacks[A]. Proceedings of the 24th International Conference on Distributed Computing Systems[C]. Tokyo Japan, 2004.408-417.

[6] WANG X, CHELLAPPAN S, BOYER P, *et al*. On the effectiveness of secure overlay forwarding systems under intelligent distributed DoS attacks[J]. IEEE Transactions on Parallel and Distributed Systems, 2006, 17(7):619-632.

[7] IN C H, HONG C S, WEI J, *et al*. An enhanced SOS architecture for DDoS attack defense using active network technology[A]. Proceedings of Advanced Industrial Conference on Telecommunications/ Service Assurance with Partial and Intermittent Resources Conference/ ELearning on Telecommunications Workshop[C]. Lisbon, Portugal, 2005. 90-95.

[8] KAUR R, SANGA A L, KUMAR K. Secure overlay services (SOS): a critical analysis[A]. 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing[C]. Ottawa, Canada, 2012. 457-462.

[9] 卢国强.云计算泛联路由平台[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.

[10] DING S L, ZHAO X H. Analysis and improvement on Chord protocol for structured P2P[A]. IEEE 3rd International Conference on Communication Software and Networks[C]. Xi'an, China, 2011. 214-218.

[11] THIRUVATHUKAL G K, HINSEN K, LÄUFER K, *et al*. Virtualization for computational scientists[J]. Computing in Science & Engineering, 2010,12(4):52-60.

[12] 邓谦. 基于 Hadoop 的云计算安全机制研究[D]. 南京：南京邮电大学, 2013.
DENG Q. Research on Security Mechanism of Cloud Computing Based on Hadoop[D]. Nanjing: Nanjing University, 2013.

[13] ZHU H, CHEN H P. Adaptive failure detection VIA heartbeat under hadoop[A]. 2011 IEEE Asia-Pacific Services Computing Conference[C]. Jeju, Korea, 2011. 231-238.

[14] 赵永利, 张杰. OMNeT++与网络仿真[M]. 北京: 人民邮电出版社, 2012.
ZHAO Y L, ZHANG J. OMNeT++and Network Simulation[M]. Beijing: Posts &Telecom Press, 2012.

作者简介：

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。

崔奕（1989-），男，福建龙岩人，中国民航大学硕士生，主要研究方向为网络与信息安全。

岳猛（1984-），男，河北沧州人，中国民航大学博士生、讲师，主要研究方向为网络与信息安全。