多云环境下基于博弈论的用户行为分析模型

聂婷婷 郭玉翠
(北京邮电大学理学院 北京 100876)

摘 要 针对多云环境下用户的分布式拒绝服务攻击缺乏有效处理机制的现状,从云服务提供商收益角度出发,提出多云环境下基于博弈论的用户行为分析模型。模型首先基于博弈论构造收益矩阵,之后利用模糊隶属度函数判定用户的行为,并进一步评估非协作和协作场景下云服务提供商的资源消耗和收益。经仿真验证,协作模型能够在减少资源消耗的基础上,有效地降低云服务提供商遭受分布式拒绝服务攻击的风险,相对于非协作场景,可以将单位资源的收益提高3倍以上,具有很强的现实意义。

关键词 云计算,多云环境,模糊隶属度函数,博弈论,协作
中图法分类号 TP39 **文献标识码** A

User Behavior Analysis Model Based on Game Theory under Multi-clouds Environment

NIE Ting-ting GUO Yu-cui
(School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract Aiming at the situation of lacking research on Distributed Denial of Service (DDoS) attack under multi-clouds environment, a user behavior analysis model based on game theory under multi-clouds environment was proposed from the perspective of cloud service provider. The model firstly constructs a payoff matrix based on game theory, and then it judges user behavior through fuzzy membership function, and evaluates the resource consumption and profit of cloud service provider under non-cooperation and cooperation scenarios. Simulations show that the proposed cooperation model can reduce resource consumption, lower the risk of DDoS attack for cloud service providers, and prompt the profit of each resource unit for more than three times, which takes an effective significance.

Keywords Cloud computing, Multi-clouds, Fuzzy membership function, Game theory, Cooperation

1 引言

随着互联网的蓬勃发展和网络经济的日益繁荣,继并行计算、网格计算、P2P计算之后,云计算作为一种新的计算模式应运而生。云计算是一种随时随地通过网络按需访问可配置资源(例如网络、服务器和存储系统)、应用和服务的模式。在这种模式下,只需要少量的管理工作和云服务提供商的参与,就能够实现快速地提供和释放资源、应用和服务[1]。很多公司和企业都考虑在采用云计算来解决海量信息存储和大规模计算的同时降低运维成本。但是,云计算仍处于发展初期,在使用过程中还存在很多挑战,例如安全性、稳定性、可用性等,其中安全问题尤其重要。

在云环境下,安全问题主要来自两个方面。一方面来自云服务提供商,因为大量的用户敏感信息存储在云服务提供商中,但是云服务提供商可能存在风险,所以确保云服务提供商可信度成为一个重点关注的问题[2]。单云服务可能存在服务可用性的失败风险和潜在的内部恶意因素,因此云终端用户只与单个云服务提供商进行交易会存在一定的风险。近年来,学术界提出了一种基于多云或称云与云之间的合作提供服务的方法,即多云协作(multi-clouds cooperation),并已有一些基于多云协作的相关架构和安全风险的分析研究[3,4]。与单云相比,多个云服务提供商之间可以通过信息交互来获取各自的可信度,从而有效降低云计算用户所面临的安全风险[5],而当前诸多研究仍停留在对单个云系统进行安全分析的阶段,多云环境的安全分析仅仅处于概念阶段。

另一方面的威胁来自用户,目前分布式拒绝服务攻击(Distributed Denial of Service)这种传统的安全攻击方式成为了云服务提供商所面临的新威胁。攻击者采用DDoS攻击的目的主要有两个:1)消耗计算机的资源(CPU、内存等),使得服务对其他合法用户不可用;2)通过假冒合法用户来隐藏其身份,以产生大量的代理来执行攻击[5,6]。云计算的基础设施由成千上万的用户共享,云系统中的海量数据对攻击者很有诱惑力,因此分布式拒绝服务攻击对云系统的影响要大于云计算出现之前所用的单一的租赁式架构[7]。为了避免云系统遭受分布式拒绝服务攻击,必须要确保云终端用户的身份真实性和行为可信性。目前身份认证技术比较成熟,但身份认证并不能阻止身份认证失败或合法身份的恶意端用户对系统的攻击,因此对云终端用户行为进行有效分析控制是当前

到稿日期:2013-04-06 返修日期:2013-10-12 本文受国家自然科学基金项目(60973146)资助。
聂婷婷(1989—),女,硕士,主要研究方向为数学与信息安全,E-mail:nietingting89@126.com;郭玉翠(1962—),女,教授,主要研究方向为数学与信息安全。

云计算应用中的一个研究重点[8]。

目前针对云终端用户行为的分析多是基于单云环境下的。在多云环境下，若恶意终端用户隐藏在正常用户之中，以适当小的频率对多个云服务提供商轮番发送错误请求或进行DDoS攻击，考虑到系统的漏报率和误报率，单个云服务提供商很难辨别出恶意行为。而通过多个云服务提供商之间的共同协作分析可以检测出这种行为。进一步，基于博弈论的云资源共享可以作为参考依据之一[9]。

基于以上分析，本文将博弈论运用到多云环境下的用户动态行为的研究中，利用多云间的协作确定用户的DDoS行为并采用合适的阻止机制，建立一个多云环境下基于博弈论的用户行为分析模型。本文第2节介绍相关工作；第3节构造云服务提供商和用户的博弈分析模型；第4节评估了非协作场景和协作场景下云服务提供商的效益；第5节对提出的模型进行了仿真，验证了其有效性；最后给出了结论和下一步的工作。

2 相关工作

云环境下，用户的DDoS攻击已经成为一个不可忽视的问题，而传统的防御方法并不能直接用于云环境。针对该问题，文献[6,10]在云系统中引入用于过滤和分析攻击数据的模块，建立处理DDoS攻击的IP回溯追踪模型和类似于云代理的过滤树安全服务模型。该模型分析云终端用户的IP地址和请求的合理性，通过网络逆向获取实际攻击源，建立一个能够防止DDoS攻击的虚拟云防御。文献[11]在云系统中引入新的DDoS攻击分析方法，在未遭受攻击时对数据包进行记录并形成分析结果，依据该结果分析攻击时刻内数据的合理性并采取必要的措施对云环境下的用户访问数据包进行实时过滤。文献[8]将博弈论运用到云终端用户动态行为的研究中，提出了一种基于动态博弈的用户行为模型。该模型通过多次观察子博弈中云终端用户的行为，并结合其历史行为动态更新用户的信任等级，对访问过程中的异常行为进行实时监控和防范，从而降低不可信云终端用户发送异常请求的概率。针对云服务的行为，文献[12]基于隶属度理论建立了云服务行为信任评估模型，但是并未分析用户行为所带来的影响。文献[13]提出了多个云服务提供商协作建立资源池，为云环境下的移动应用提供服务，并引入最佳算法来控制访问以达到收益最大化，资源池中的服务提供商利用合作博弈模型分配收益。但是这些模型还存在以下问题：

1. 在云系统中引入额外的模块，增加了云系统架构的复杂性，缺乏理论依据的支撑，并且防御效果不很明显；

2. 在未遭受攻击时对数据包进行记录并形成分析结果，依据该结果分析攻击时刻内数据的合理性，这不需要引入新的模块，但如何区分正常时间和攻击时间有一定困难；

3. 利用博弈论思想解决云安全问题，根据博弈结果划分用户信任等级，并据此采取相应的访问控制措施，富有创新性，但其模型计算复杂，实用性较差，而且没有考虑多云环境下的用户行为；

4. 在云计算中引入多云协作思想，能够节约资源，又能够达到利益最大化的目的，具有一定的参考意义，但是没有考虑多云环境下的安全问题。

本文借鉴上述相关研究成果，将博弈论和多云协作运用到云计算中，从云服务提供商收益角度出发，提出多云环境下基于博弈论的用户行为分析模型。实验证明，该模型能够有效地降低云服务提供商遭受分布式拒绝服务攻击的风险，提高其资源利用率和收益。

3 博弈分析模型

博弈论(Game Theory)又称对策论，研究的是在竞争环境中，参与方如何进行有效决策[14]。近年来，博弈论作为分析和解决冲突与合作的工具，被人们广泛用于经济、社会和管理领域中。与此同时，随着互联网的快速发展，博弈中的决策思想也被用来解决网络中的冲突与合作的问题。本文将云终端用户和云服务提供商之间的攻防关系抽象为博弈。

本节首先给出了本文所使用的相关概念，之后给出了多云环境下的博弈收益矩阵，构造出用户和云服务提供商的收益矩阵，以为下一步分析用户行为做准备。

3.1 相关概念

本文将多云环境分为以下几个部分：参与方、行为集、收益矩阵，以及各参与方的行为概率等。

(1)参与方。参与方包括 N 个云终端用户集合 $U=\{u_1,u_2,\cdots,u_N\}$ 和 M 个不相交云服务提供商的集合 $C=\{c_1,c_2,\cdots,c_M\}$。其中 u_i 的状态可以分为两种 $S=\{s_1,s_2\}=\{$可信，可疑$\}$。可疑用户的状态需要通过多云协作才能鉴别出来。每个 u_i 均可以访问任意一个 c_j。

(2)行为集。每个用户可能产生两种行为：$\boldsymbol{A}=\{a_1,a_2\}=\{$正常请求，异常请求$\}$，云服务提供商的行为集合 $\boldsymbol{B}=\{b_1,b_2\}=\{$接受请求，拒绝请求$\}$。

(3)收益矩阵 $\boldsymbol{H}=\{h_{kl}\}$。收益矩阵定义了针对处于不同状态的用户，云服务提供商 c_i 采用不同的行为来获得收益。该矩阵对每个用户 i 和服务提供商 j 都适用。其中每项 h_{kl} 表示用户采用行为 $k(k=1,2$，分别表示正常，异常请求$)$和提供商采取行为 $l(l=1,2$，分别表示接受请求和拒绝请求$)$时的收益元组。

(4)行为概率。行为概率包括用户的行为概率矩阵 $\boldsymbol{P}^U=\{p^u_{ijk}\}$ 和云服务提供商的概率矩阵 $\boldsymbol{P}=\{p_{ijl}\}$ 两部分。其中 p^u_{ijk} 表示第 i 个用户和第 j 个云连接时采用行为 k 的概率，p_{ijl} 表示云服务提供商 j 对用户 i 采取行为 l 时的概率。

本文的重点包括确定收益矩阵 $\boldsymbol{H}$ 和行为概率矩阵 $\boldsymbol{P}^U$ 和 $\boldsymbol{P}$，下面使用博弈论确定收益矩阵 $\boldsymbol{H}$。

3.2 博弈矩阵

在本文中，我们需要分析用户与服务提供商的博弈收益。为了简化模型，假设请求的开销一致，对博弈过程中的相关参数定义如下：

$\boldsymbol{D}=\{d_1,d_2\}$ 表示用户采用不同行为 a_i 时对应的开销。$\boldsymbol{E}=\{e_1,e_2\}$ 表示用户采用不同行为 a_i 时的收益。

对于云服务提供商，设：

1)用户的正常请求，其收益为 γ；

2)监测出的不可信用户的惩罚为 δ 时，其收益为0；

3)当异常状态被检测出来但是被阻止时，其所获得的收益为 σ。

假设系统的误报率(把正常请求报成异常请求)为 α，漏报率(把异常请求报成正常请求)为 β，则由以上分析可以得到博弈双方的收益矩阵，如表1所列。

表1 博弈收益矩阵

收益矩阵		云服务提供商	
		接受请求	拒绝请求
用户	正常请求	$(1-\alpha)e_1-d_1,(1-\alpha)\gamma$	$-\alpha\delta-d_1,-\alpha\gamma$
	异常请求	$\beta e_2-d_2,-\beta e_2$	$-(1-\beta)\ \delta-d_2,(1-\beta)\sigma$

收益矩阵的每一项可以细分为 $h_{kl}=[o_{kl},q_{kl}]$的子项，分别表示用户和提供商的收益，本文重点考虑云服务提供商的收益。为了确定最后的收益，需要明确 $\boldsymbol{P}^U$ 和 $\boldsymbol{P}$，它们分别通过用户行为模型分析和优化模型来获取。

3.3 用户行为分析

对用户行为进行分析的目的是确定用户身份，针对不同身份的用户，云服务提供商采取不同的行为，从而达到利益最大化的目的。我们分别针对单云场景和多云间协作的场景对用户行为概率进行分析。

3.3.1 非协作场景

对任意时刻 $t\in T$，设用户 i 的行为关系 k 和云服务提供商 j 的连接关系为布尔变量 $f_{ijk}(t)$，在一个周期 T_i 中，用户 i 与单个云服务提供商 j 的正常请求次数设为 v_{ij}，异常请求次数为 ρ_{ij}。假设用户之间的行为相互独立，则存在如式(1)—式(3)所示的3个等式：

$$v_{ij}=\sum_{t\in T}f_{ij1}(t) \tag{1}$$

$$\rho_{ij}=\sum_{t\in T}f_{ij2}(t) \tag{2}$$

$$v_{ij}+\rho_{ij}=\sum_{t\in T}\sum_{k}f_{ijk}(t) \tag{3}$$

进一步有单位时间内的请求次数 V_{ij}，如下所示：

$$V_{ij}=\frac{v_{ij}+\rho_{ij}}{T} \tag{4}$$

下面通过 V_{ij} 确定用户的状态，设单位时间的异常访问次数门限为 ϵ，并进行如下判定：

1)当 $\rho_{ij}>\epsilon$ 时，可以认为用户 i 为不可信用户的概率很高，云服务提供商以较高的 p_{ijl} 拒绝为其提供服务。

2)当 $\rho_{ij}\leqslant\epsilon$ 时，取 V_{ij} 作为依据，建立用户正常请求的隶属度函数。在网络随机过程中，正态分布是常见的模型，因此这里采用正态隶属度来建立概率关系：

$$\mu_{\tilde{A}}(V_{ij})=\int_{V_{ij}}\frac{1}{\sqrt{2\pi}\kappa}\exp\left[-\frac{(V_{ij}-\bar{\omega})^2}{2\kappa^2}\right] \tag{5}$$

式中，κ 和 $\bar{\omega}$ 分别表示单位时间访问次数的期望和方差。在确定了隶属度概率之后，需要进一步确定用户的行为概率，分析如下：

1)当 $\rho_{ij}>\epsilon$ 时，具体有 $p^u_{ij1}=\xi$，$p^u_{ij2}=1-\xi$。ξ 为伪装概率。

2)当 $\rho_{ij}\leqslant\epsilon$ 时，具体有 $p^u_{ij1}=\mu_{\tilde{A}}(V_{ij})$，$p^u_{ij2}=1-\mu_{\tilde{A}}(V_{ij})$。

3.3.2 协作场景

基于以上收益矩阵和概率矩阵，设每经过一个博弈周期 T，多云之间可以互相协作通信，从而获取各个用户的上述信息。为了不失一般性，多云协作为两两之间相互协作。

在协作状态下，从单个用户的角度，其在单位时间上对整个云系统的请求次数为：

$$V_{[i]}=\sum_{j}V_{ij} \tag{6}$$

对应的正常请求次数为：

$$v_{[i]}=\sum_{j}v_{ij} \tag{7}$$

异常请求次数为：

$$\rho_{[i]}=\sum_{j}\rho_{ij} \tag{8}$$

且有如下等式：

$$\rho_{[i]}+v_{[i]}=V_{[i]} \tag{9}$$

该场景下设用户的状态概率为 $p^{u'}_{ijk}$，同3.3.1节的分析，有：

1)当 $\rho_{[i]}>\epsilon$ 时，对任意 j，具体有 $p^{u'}_{ij1}=\xi$，$p^{u'}_{ij2}=1-\xi$。

2)当 $\rho_{[i]}\leqslant\epsilon$ 时，对任意 j，具体有 $p^{u'}_{ij1}=\mu_{\tilde{A}}(V_{[i]})$，$p^{u'}_{ij2}=1-\mu_{\tilde{A}}(V_{[i]})$。

4 云服务提供商效益评估

在确定了用户行为概率之后，本节的重点是分析云服务提供商采取不同行为时的资源消耗和对应的收益。为了获取最终的收益，需要确定两个关键因子：隶属度函数和云服务提供商行为概率矩阵 $\boldsymbol{P}$。据我们所知，当前已有将模糊隶属度函数用于云环境下分析云服务行为信任模型的研究，本文基于该研究，首次将隶属度函数运用于多云环境下用户行为的检测分析，并深入研究了隶属度函数与收益之间的关系。

4.1 非协作场景

由于每个云的容量(包括CPU利用率、内存、带宽等)有限，并且协作时也需要消耗资源，因此本文将信息协作所消耗的资源作为代价和收益所需考虑的因素之一。设单个云 j 的容量为 Ca_j，正常请求的单次资源需求为 φ，异常请求的单次资源需求为 ω(通常有 $\omega>\varphi$)。对单个云服务提供商 j，在时刻 t，其所需的期望资源 $R^R_j(t)$ 为：

$$R^R_j(t)=\varphi\cdot\sum_i\sum_l p^u_{ij1}\cdot p_{ijl}\cdot f_{ij1}(t)+\omega\cdot\sum_i\sum_l p^u_{ij2}\cdot p_{ijl}\cdot f_{ij2}(t) \tag{10}$$

第一项是正常状态用户的请求所需的资源，取正常用户的资源和异常的伪装值两项，第二项是异常用户的请求所需的资源。

在时刻 t，单个云 j 在用户 i 上的收益为：

$$R^T_{ij}(t)=\sum_k\sum_l p^u_{ijk}\cdot q_{kl}\cdot p_{ijl}\cdot f_{ijk}(t) \tag{11}$$

t 时刻云 j 的总收益为：

$$R^T_j(t)=\sum_i R^T_{ij}(t) \tag{12}$$

以上分析确定了单云场景中不交换信息时的收益模型。

由于协作和非协作状态下资源和收益各不相同，本文将收益资源比作为主要的优化目标之一。对于非协作场景，各个云服务提供商的收益资源比为：

$$\psi_j(t)=R^T_j(t)/R^R_j(t) \tag{13}$$

t 时刻的平均收益资源比为：

$$\widetilde{\psi(t)}=\sum_j R^T_j(t)/\sum_j R^R_j(t) \tag{14}$$

4.2 协作场景

同样，在时刻 t 单个云服务提供商 j 在协作场景下所需的资源为：

$$R^{R'}_j(t)=\varphi\cdot\sum_i\sum_l p^{u'}_{ij1}\cdot p_{ijl}\cdot f_{ij1}(t)+\omega\cdot\sum_i\sum_l p^{u'}_{ij2}\cdot p_{ijl}\cdot f_{ij1}(t)+\mu\cdot\sum_i g\left(\sum_k f_{ijk}(t)\right) \tag{15}$$

其中，μ 是交换信息的单位开销，g 是访问次数即交换信息量与资源之间的映射关系函数。$\sum_k f_{ijk}(t)$ 表示在服务提供商 j 下用户 i 的访问次数。

该场景下云系统 j 的收益为：

$$R^{T'}_j(t)=\sum_k\sum_l\sum_i p^{u'}_{ijk}\cdot q_{kl}\cdot p_{ijl}\cdot f_{ijk}(t)+\lambda\cdot\sum_i y\left(\sum_k f_{ijk}(t)\right) \tag{16}$$

式中，λ 是交换信息的单位收益，y 是访问次数即交换信息量与额外收益之间的映射关系函数。

同样可得，对于协作场景，各个云服务提供商的收益资源比为：

$$\psi_j'(t)=R_j^{T'}(t)/R_j^{R'}(t) \tag{17}$$

t 时刻的平均收益资源比为：

$$\widetilde{\psi'(t)}=\sum_j R_j^{T'}(t)/\sum_j R_j^{R'}(t) \tag{18}$$

从直观上来说，依据用户的行为隶属度函数采用对应的接受概率，对云服务提供商有益。本文简化考虑云服务提供商的接受概率。假设 p_{ijl} 取值与 p_{ijk}^{u} 成正比，则对非协作场景取值如下：

$$p_{ij1}=p_{ij1}^{u} \tag{19}$$

$$p_{ij2}=1-p_{ij1}^{u} \tag{20}$$

对于协作场景，取值如下：

$$p_{ij1}=p_{ij1}^{u'} \tag{21}$$

$$p_{ij2}=1-p_{ij1}^{u'} \tag{22}$$

在单云场景的数学模型中，云服务提供商检测访问其的各个用户的行为。如果在检测的时间段内，用户 i 对云服务提供商 j 的累积异常访问次数 ρ_{ij} 小于等于异常门限 ε，则认为用户 i 正常概率较高。但是这段时间内用户 i 可能对其他云服务提供商也进行了异常访问，形成的 DDoS 攻击并不能得到有效的检测。而协作场景通过交换信息，能够获取单个用户在整个时间段内对所有云的累积异常访问次数 $\rho_{[i]}$，且有 $\rho_{[i]}\geqslant\rho_{ij}$，从而提升用户 i 的 DDoS 攻击行为检测的精确度。

5 仿真实验

5.1 仿真环境

仿真场景如图 1 所示，一共有 3 个云、10 个用户。用户 i 对云 j 的访问是随机生成的，在时刻 t，可能存在正常请求、异常请求 2 种状态。设仿真时长为 T，用户行为每 1 分钟变化一次。

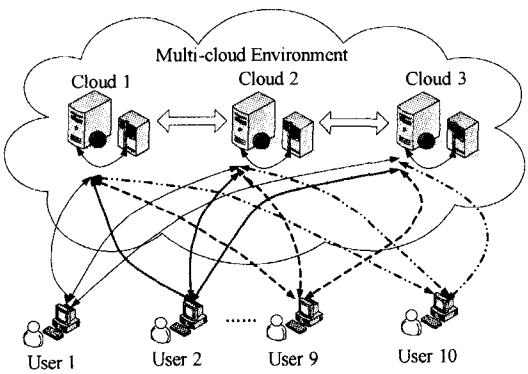

图 1 仿真场景示意图

参考已有研究[8]，在博弈分析中，各变量的取值如表 2 所列。

表 2 博弈矩阵各变量取值

变量	取值	变量	取值
d_1	4	d_2	5
e_1	8	e_2	10
γ	5	δ	3
σ	6	α	0.01
β	0.005	T	50min

参照文献[9]的仿真环境分析，在用户行为模型中，为了减少异常请求所带来的损失，设 $\varepsilon=1$。$\bar{\omega}$ 作为访问次数的均值，也设为 1。仿真中需要进一步研究 κ 与访问次数的关系。伪装概率 ξ 的取值为 0.01，每个云的资源上限为 100。正常请求资源需求为 $\omega=1$，异常请求资源需求为 $\varphi=2$。针对协作状态下的额外资源开销，取 $\mu=0.1$，针对额外的收益，取 $\lambda=0.3$。同时函数 g、函数 y 均取线型函数，即 $g(x)=y(x)=x$。

5.2 结果和分析

在仿真中，我们重点研究 κ 随用户 i 对提供商 j 的最大访问次数 $MV=\max\{V_{ij}\}$ 的比例变化的结果。图 2 显示了隶属度函数的变化情况。

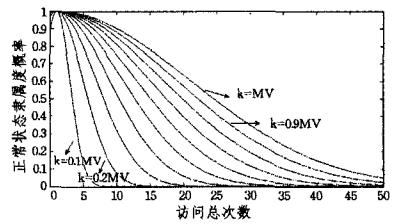

图 2 隶属度概率与访问总次数之间的关系

由图 2 可知，随着系数的增加，用户的正常状态隶属度函数呈非线性提升，且趋势变缓。

我们进一步考察资源需求和收益之间的关系。当 $\kappa=MV$ 时，图 3、图 4 则显示了非协作场景下，各云服务提供商的资源需求和收益变化。

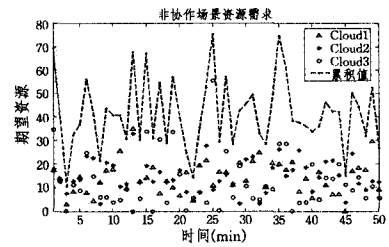

图 3 非协作场景资源需求

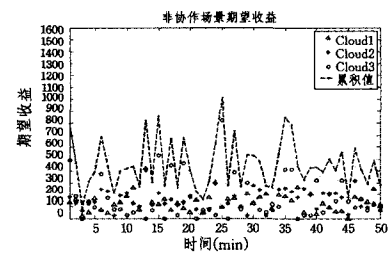

图 4 非协作场景期望收益

图 5、图 6 则显示了在协作场景下，各云服务提供商的资源需求和收益变化。

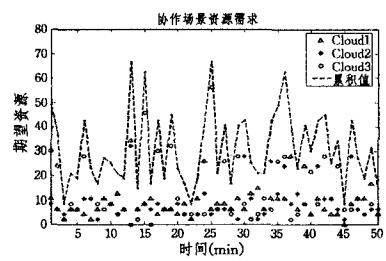

图 5 协作场景资源需求

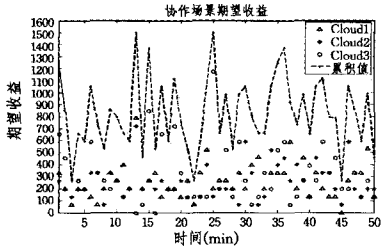

图 6　协作场景期望收益

通过图 3—图 6 的分析，我们可以得出如下结论：

1. 无论是不采用协作还是采用协作，消耗的资源和收益近似成正比，即变化规律类似。说明资源和收益之间存在直接的线型关系。

2. 随着访问序列的变化，资源和收益也随之变化抖动，说明了资源收益在时间上也具有动态性，与现网场景接近。

3. 协作场景下虽然需要额外的交换资源开销，但是同时更好地甄别了异常请求，减少了资源消耗，因此最终的资源消耗低于非协作场景。

4. 协作的期望收益高于非协作场景，资源消耗也相对较小，更好地验证了本文方法的合理性。

针对用户行为，如表 3 给出了用户和云服务提供商之间的异常访问值的分布。

表 3　异常访问值分布

	Cloud 1/ρ_{ij}	Cloud 2/ρ_{ij}	Cloud 3/ρ_{ij}	累积值/$\rho_{[i]}$
User 1	2	3	1	6
User 2	2	1	2	5
User 3	0	1	0	1
User 4	0	1	0	1
User 5	2	0	0	2
User 6	1	1	0	2
User 7	0	1	0	1
User 8	0	1	1	2
User 9	0	1	0	1
User 10	1	4	2	7

由表 3 可发现，针对单云场景，user 1，user 2，user 5，user 10 会被判定为具有 DDoS 攻击的用户，但是只针对 ρ_{ij} 大于 1 的云服务提供商有效。由于不存在云间协作，虽然 cloud 1 和 cloud 2 将 user 1 判定为存在 DDoS 攻击的异常用户，但是 cloud 3 仍然将其看作正常用户，因此存在被攻击的风险。同样，user 2 对 cloud 2，user 5 对 cloud 2 和 cloud 3，user 10 对 cloud 1 都存在同样的攻击可能性。而 user 3，user 4，user 7 和 user 9 由于其累积异常访问次数未超越门限，因此被判定为正常用户。user 6 和 user 8 由于对每个云服务提供商的异常访问均未超越门限，因此也被看作正常用户，但是这些用户由于累积异常访问次数高于门限，因此存在 DDoS 攻击的可能性很高。

在协作场景下，云服务提供商之间通过信息交互，获取每个用户对云服务提供商的累积异常访问次数 $\rho_{[i]}$。经过判决，除了 user 3，user 4，user 7 和 user 9 之外，剩余的用户均判决为具有高 DDoS 攻击可能性的用户，与真实情况较为一致。同样，云之间的协作能够使得所有的云知晓各个用户的行为概率，从而改变接受和拒绝的概率，大幅降低遭受 DDoS 攻击的风险。

进一步，图 7 和图 8 给出了非协作和协作场景下，云服务提供商的收益资源比的变化情况。

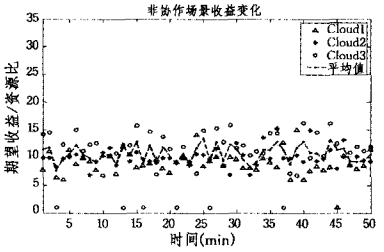

图 7　非协作场景期望收益/资源比

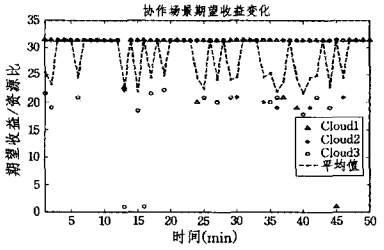

图 8　协作场景期望收益/资源比

由图 7 和图 8 可知，在各个时刻，针对各个云服务提供商，协作机制可以大大提高期望收益/资源比，提高单位资源的效益，具有很强的现实意义。

以上从微观角度分析了资源和收益之间的变化关系。进一步，我们考察当 κ 随 MV 变化时，协作场景下和非协作场景下平均单位资源的效益的比值($\widetilde{\psi'(t)}/\psi'(t)$)变化情况。通过图 9 可以发现，在不同比例下，协作场景的单位资源的效益比值变化总是优于非协作场景。同时，当 κ=0.3MV 时能够获取最大的增益，此时最大瞬时值能够提高 15 倍以上，平均值提升 3 倍以上。

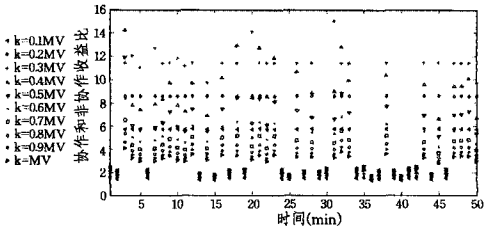

图 9　协作场景与非协作场景平均单位资源效益比

综上所述，采用协作机制后，能够在不增加资源消耗的基础上，有效降低云服务提供商遭受 DDoS 攻击的风险，将单位资源的效益提高 3 倍以上，获取较大的经济效益。

结束语　本文提出的多云协作机制能够减少云服务提供商遭受分布式拒绝服务攻击的风险，并大幅提高单位资源的收益，具有很强的现实意义。下一步工作是兼顾用户的收益，针对不同的用户，以服务提供商的行为概率矩阵 $\boldsymbol{P}$ 为优化目标，获取更加均衡和优化的收益。

参 考 文 献

[1] 陈康，郑纬民. 云计算：系统实例与研究现状[J]. 软件学报，2009，20(5)：1337-1348

[2] Alok T，Abhinav M. Cloud Computing Security Considerations [C]// IEEE ISCPCC. Xian，China，2011：1-5

[3] AlZain M A，Pardede E，Soh B，et al. Cloud Computing Security：From Single to Multi-Clouds[C]// HICSS. Hawaii，USA，2012：5490-5499

[4] AlZain M A, Soh B, Pardede E. MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing[C]//DASC. Sydney, Australia, 2011: 784-791

[5] Trostle J. Protecting Against Distributed Denial of service attacks Using Distributed Filtering[C]//Securecomm and Workshops. Baltimore, USA, 2006: 1-11

[6] Bhaskaran M, Natrarajan A M, Sivanandam S N. Tracebacking the Spoofed IP Packets in Multi ISP Domains with Secured Communication[C]//ICSCN. Chennai, India, 2007: 579-584

[7] Joshi B, Vijayan A S, Joshi B K. Securing Cloud Computing Environment Against DDoS Attacks[C]//ICCCI. Coimbatore, India, 2012: 1-5

[8] 陈亚睿，田立勤，杨扬. 云计算环境下基于动态博弈论的用户行为模型与分析[J]. 电子学报，2011，8：1818-1823

[9] Niyato D, Vasilakos A V. Resource and Revenue Sharing with Coalition Formation of Cloud Providers: Game Theoretic Approach[C]//CCGrid. Newport Beach, CA, USA, 2011: 215-224

[10] Karnwal T, Sivakumar T, Aghila G. A Comber Approach to Protect Cloud Copmputing against XML DDoS and HTTP DDoS attack[C]//SCEECS, Bhopal, India, 2012: 1-5

[11] Chen Qi, Lin Wen-min, Dou Wan-chun, et al. CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment [C]//DASC. Sydney, Australia, 2011: 427-434

[12] 谢立军，朱智强，孙磊，等. 基于隶属度理论的云服务行为信任评估模型研究[J]. 计算机应用研究，2012，30(4)：1051-1054

[13] Niyato D, Wang P, Hossain E, et al. Game Theoretic Modeling of Cooperation among Service Providers in Mobile Cloud Computing Environments[C]//WCNC. Shanghai, China, 2012: 3128-3133

[14] 张维迎. 博弈论与信息经济学[M]. 上海：上海人民出版社，2004

(上接第 110 页)

7 $\Delta\vec{H}_{U_{ij}}$ $(j=1,2,\cdots,m)$、延迟抖动率态势熵差向量 $\Delta\vec{H}_{I_{ij}}$ $(j=1,2,\cdots,m)$、故障度态势熵差向量 $\Delta\vec{H}_{F_{ij}}$ $(j=1,2,\cdots,m)$和漏洞等级态势熵差向量 $\Delta\vec{H}_{G_{ij}}$ $(j=1,2,\cdots,m)$，m 为单位分析时间窗口的数量，再按式(6)计算对应的主机脆弱性指数值变化序列，如图 2 所示。

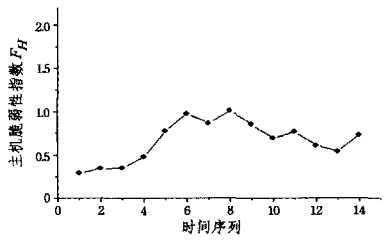

图 2 主机 H_1 脆弱性安全态势

图 2 表明该主机的脆弱性处于较稳定的状态，变化平稳，主机系统受到的攻击或威胁不是很剧烈。根据表 1 提供的描述分级，可以认定该主机在分析时间序列范围内，脆弱性态势处于“一般”状态，这与基于 DS 融合的态势评估值保持一致。

结束语 通过建立网络安全态势指标的识别空间和评估准则，并基于专家意见融合的推理过程，实现了一种基于 DS 证据融合理论的专家网络安全态势评估方法，并通过脆弱性指数实验对其进行了验证，二者可以相互印证。实验表明该方法能克服复杂网络中大量不确定因素的影响，可很好地解决态势评估中存在的正确性和合理性质疑等问题。本文主要以脆弱性评估为例进行描述，对于其他评估角度(如稳定性、威胁性和容灾性等)也有相同的评估效果。而利用态势评估值对态势进行预测，建立有效的网络安全态势预警系统是下一步要进行的工作。

参 考 文 献

[1] Farinelli A, Nardi D, Pigliacampo R, et al. Cooperative situation assessment in a maritime scenario[J]. International Journal of Intelligent Systems, 2012, 27(5): 477-501

[2] 付钰，吴晓平，叶清. 基于改进 FAHP-BN 的信息系统安全态势评估方法[J]. 通信学报，2009，30(9)：135-140

[3] Zhao Jin-hui, Zhou Yu, Shuo Liang-xun. A situation awareness model of system survivability based on variable fuzzy set[J]. Telkomnika, 2012, 10(8): 2239-2246

[4] 姜伟，方滨兴，田志宏，等. 基于攻防博弈的网络安全测评和最优主动防御[J]. 计算机学报，2009，32(4)：817-827

[5] Jakobson G. Mission cyber security situation assessment using impact dependency graphs[C]//Proceedings of the International Conference on Information Fusion (FUSION). Chicago, IL, USA: IEEE, 2011

[6] Kirillov V P. Constructive stochastic temporal reasoning in situation assessment[J]. IEEE Transactions on Systems, Man and Cybernetics, 1994, 24(8): 1099-1113

[7] Miao A X, Zacharias G L, Shih-ping K. Computational situation assessment model for nuclear power plant operations[J]. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 1997, 27(6): 728-742

[8] Xiao Hai-dong, Li Jian-hua. Analysis of security situation of networks based on knowledge base[J]. WSEAS Transactions on Electronics, 2006, 3(1): 34-39

[9] Holsopple J, Sudit M, Nusinov M, et al. Enhancing situation awareness via automated situation assessment[J]. IEEE Communications Magazine, 2010, 48(3): 146-152

[10] Zhao Jin-jing, Wen Yan, Wang Dong-xia. A network security evaluation method framework based on multiple criteria decision making theory[C]//Proceedings of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Seoul, Korea: IEEE Comput. Soc, 2011: 371-375

[11] Feng Xue-wei, Wang Dong-xia, Ma Guo-qing, et al. Security situation assessment based on the DS theory[C]//Proceedings of the 2nd International Workshop on Education Technology and Computer Science. Wuhan, China: IEEE Comput. Soc, 2010: 352-356

[12] 王春雷，方兰，王东霞，等. 基于知识发现的网络安全态势感知系统[J]. 计算机科学，2012，39(7)：11-17，24

[13] 唐成华，王鑫，张瑞霞，等. 基于态势熵的网络安全态势评估指标体系研究[J]. 桂林电子科技大学学报，2011，31(4)：270-274

[14] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006，17(4)：885-897