计算机科学
COMPUTER SCIENCE

基于用户行为的云邮件防御资源分配方法

张万友, 宋礼鹏

引用本文

张万友, 宋礼鹏. 基于用户行为的云邮件防御资源分配方法[J]. 计算机科学, 2026, 53(2): 442-453.

ZHANG Wanyou, SONG Lipeng. Cloud Email Defense Resource Allocation Method Based on User Behavior [J]. Computer Science, 2026, 53(2): 442-453.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250300041

基于用户行为的云邮件防御资源分配方法

张万友　宋礼鹏
山东大学机电与信息工程学院　山东 威海 264200
(zhwanyou@foxmail.com)

摘　要　近年来,随着云邮件应用的普及,用户数量不断增加,钓鱼攻击等邮件安全威胁日益严重。有效的防御资源分配成为保障云邮件系统稳定运行的关键。然而,现有的防御资源分配方法往往未充分考虑用户行为、多个云节点间的关联关系和横向钓鱼攻击问题,难以精准应对复杂的安全威胁,导致资源利用效率低下和防御效果不佳。为解决这一问题,提升云邮件节点的安全性和资源利用率,提出了一种基于用户行为的云邮件防御资源分配方法。首先,构建了云邮件节点风险评估模型,综合评估钓鱼邮件攻击成功率以及单个云邮件节点和多个关联节点的云端风险。随后,设计了单个节点防御资源动态分配算法和多个相互关联节点防御资源协同分配算法,根据用户登录概率、信任关系、行为模式、节点拥有的防御资源量和实时威胁态势动态调整资源分配策略。实验结果表明,与现有防御资源分配方法相比,所提方法能够实现节点之间资源的协同调配,有效提高了资源利用率并取得了最低全天系统总损失值,表现出了优越的效果,为云邮件节点的防御资源分配提供了更优的解决方案。

关键词:云邮件;用户行为;钓鱼邮件;防御策略;资源分配
中图分类号　TP393

Cloud Email Defense Resource Allocation Method Based on User Behavior

ZHANG Wanyou and SONG Lipeng
School of Mechanical, Electrical & Information Engineering, Shandong University, Weihai, Shandong 264200, China

Abstract　In recent years, with the widespread adoption of cloud-based email applications, the number of users has steadily increased, and security threats such as phishing attacks have become more prevalent. Effective defense resource allocation has thus become crucial for ensuring the stable operation of cloud email systems. However, existing resource allocation methods often fail to adequately consider factors such as user behavior, the interrelationships between multiple cloud nodes, and lateral phishing attacks, leading to inefficiencies in resource utilization and suboptimal defense performance. To address these issues and enhance the security and resource utilization of cloud email nodes, this paper proposes a user behavior-based defense resource allocation method. Firstly, a risk assessment model for cloud email nodes is developed, which comprehensively evaluates the success rate of phishing attacks and the cloud risks associated with both individual nodes and multiple interconnected nodes. Next, dynamic defense resource allocation algorithms are designed for both individual nodes and collaborative resource allocation across multiple interlinked nodes. These algorithms adjust resource allocation strategies in real-time based on factors such as user login probabilities, trust relationships, behavior patterns, the available defense resources at each node, and the current threat landscape. Experimental results show that, compared to existing methods, the proposed approach enables collaborative resource allocation, improves utilization, achieves the lowest system loss, and offers a better solution for cloud email node defense resource allocation.

Keywords　Cloud email, User behavior, Phishing emails, Defense strategies, Resource allocation

1　引言

在数字化时代,云邮件凭借其便捷、高效和低成本等优势,已成为现代社会不可或缺的通信工具,被广泛应用于个人通信、企业协作和商业活动等领域。全球范围内,电子邮件用户数量持续增长,大量的信息通过云邮件进行传输和交互。相关统计数据显示,全球超过半数人口都在使用电子邮件[1],并且随着互联网的日益普及,这一数字仍在不断攀升[2-4]。云邮件的广泛应用也带来了日益严峻的安全威胁。钓鱼邮件作为其中最为突出的问题之一,威胁着个人和企业数据的安全[5]。这些攻击所带来的危害不容小觑,不仅会导致用户个人隐私的泄露和财产损失,还可能对企业的声誉和正常运营造成严重的负面影响。

面对大量钓鱼邮件的侵扰,传统防御措施需要消耗大量计算资源进行邮件扫描、过滤和分析,这不仅会增加网络带宽的压力,还可能对云邮件节点的响应速度与稳定性产生不利影响[6]。尤其是发生大规模钓鱼攻击时,云邮件节点需要处理海量的异常邮件,这可能导致节点性能下降,邮件处理延迟,甚至出现节点崩溃的严重情况。当前,尽管已经存在多种防御手段,如基于比对黑名单来筛查钓鱼邮件[7-8],基于邮件

到稿日期:2025-03-10　返修日期:2025-06-07
通信作者:宋礼鹏(slp880@sdu.edu.cn)

内容过滤钓鱼邮件[9-11]，但这些方法都需要大量的计算资源来维持高效运作[12-13]。高频率的计算资源需求不仅会增加云邮件节点的负担，还可能导致资源消耗过高，影响节点的整体性能。

因此，科学合理地分配云邮件节点中的防御资源，对于保障云邮件节点的安全稳定运行至关重要。合理的防御资源分配，能够在有限的资源条件下实现对钓鱼邮件的高效防御，降低节点面临的安全风险，同时优化节点性能，减少资源浪费，提高云邮件节点的整体可靠性和用户体验。深入研究基于用户行为的云邮件防御资源分配方法，能够为云邮件节点的安全防护提供更加智能化、精准化的解决方案，具有重要的理论意义和实际应用价值。

本文的主要贡献总结如下：

1）通过构建云邮件系统风险评估模型，量化了钓鱼邮件攻击成功率、单个云节点局部风险以及多个相互关联节点的云端全局风险，解决了云邮件系统的安全风险评估问题；

2）通过单个云节点防御资源动态分配算法，考虑用户登录概率、信任关系、行为模式和云节点的资源数量、实时威胁态势，实现了单个云节点的防御资源高效分配；

3）通过多个关联节点的云端防御资源协同分配算法，充分考虑云端多个云节点相互关联的情况，实现了节点之间资源的协同调配，能够更好地应对跨节点横向钓鱼攻击，有效提高资源利用率；

4）在真实的高校邮件数据集上进行了实验，结果表明，与现有防御资源分配方法（Victor 方法、Wang 方法、Masaki 方法、Essia 方法及随机分配策略）相比，在防御资源数量一定时，本文方法均取得了最低的全天系统总损失值。

2 相关工作

随着云邮件技术的迅速发展，其在为用户带来便捷性的同时，也使得邮件防御节点对资源高效利用的需求愈发迫切，尤其是在高流量、大规模的应用环境中，如何在云端防御资源有限的条件下实现高效的防御，成为当前研究的重要课题。从云资源分配优化算法的角度来看，目前主要有元启发式优化算法、机器学习优化算法和混合优化算法三大研究方向。

元启发式优化算法通过模仿自然现象或生物行为，进行全局搜索和迭代改进，以提升云计算节点的效率和资源利用率。这类算法通过优化资源分配，实现性能提升、成本降低或多目标平衡。Wei 等[14]基于微分进化算法设计了云资源优化模型，将整体问题拆解为多个子问题，提高了求解效率。但是，该模型未考虑动态资源需求，可能导致资源分配不合理。Wei 等[15]提出的随机资源需求算法解决了动态资源需求问题，但其计算复杂度较高。Wei 等[16]提出了一种显著加速元启发式搜索过程的资源配置算法，其能快速收敛并提高资源分配效率，但面临非线性定价和复杂约束问题。Gill 等[17]通过布谷鸟算法管理云节点资源，降低了能耗并提高了可靠性，但忽略了实际操作中的不确定性。

机器学习优化算法通过分析历史数据和实时需求，动态调整资源分配策略。Ahlawat 等[18]利用 Q-learning 设计了基于聚类的资源分配方法，优化了节点效能，但在大规模节点中存在高计算复杂度问题。Jeong 等[19]使用 BiLSTM 预测资源使用情况以优化分配，但未充分考虑任务迁移和执行时间等因素。Yu 等[20]采用了基于深度强化学习的资源分配算法，从经验中学习多进制卸载模式，从而减少任务迁移和执行所需要的时间。Gan 等[21]提出的双驱动资源分配机制，性能表现优异，但计算资源消耗较大。Nawrockip 等[22]结合神经网络预测资源使用情况，所提方法适用于需求波动较大的场景，但可能面临突发资源紧张的问题。

混合优化算法结合多种优化技术提高资源分配效率。Neema 等[23]提出的模糊逻辑与遗传算法相结合的资源分配方法，优化了负载分配，但在高维度问题中面临计算资源消耗问题。Yang 等[24]提出的分层聚类和联合优化相结合的方法，降低了时延和能耗，并提升了负载均衡水平。Shaik 等[25]结合粒子群优化与模拟退火优化实现资源负载平衡，但该方法存在局部最优解问题。Senthil 等[26]结合猫群优化和蝙蝠优化的方法，提高了全局搜索能力，但计算负担较大。Narwal[27]结合鲸鱼优化和鹿群优化的改进方法，解决了资源负载均衡问题，但可能因任务迁移和资源动态变化产生不完全合理的资源分配。

综合现有大量研究可以看出，云邮件防御资源分配仍有若干关键问题未得到有效解决。首先，尽管元启发式优化算法、机器学习优化算法和混合优化算法在提高资源分配效率方面取得了一定进展，但这些方法主要聚焦于性能和成本优化，忽视了对节点安全性问题的深入探讨。特别是在大规模云邮件节点中，如何根据不断变化的攻击策略和用户行为动态调整防御资源的配置，仍然是一个亟待解决的问题。其次，现有研究局限于单个云节点资源分配，未充分考虑云端的多个节点相互关联情况，会导致资源配置不合理，从而影响节点的整体性能。此外，许多算法在面对高流量、大规模的云环境时，存在计算复杂度过高、收敛速度较慢等问题，使得实时、高效的防御资源分配变得困难。最后，尽管部分研究提出了应对云资源需求波动的优化算法，但大多数算法假设了理想条件，未考虑到实际环境中用户需求的不确定性和用户行为的动态变化，导致它们在实际应用中存在局限性。

为解决上述问题，本文构建云邮件节点风险评估模型，并提出基于用户行为的云邮件防御资源分配方法，旨在优化云邮件节点中的防御资源配置。通过深入分析用户行为和云邮件架构及其所面临的安全威胁，本文方法能够合理地动态调整防御资源分配，提升资源利用效率，使防御效果显著提高。

3 云邮件系统风险评估模型

3.1 云邮件系统架构与通信模式分析

云邮件系统通常是由同一家大型公司下多个不同地方的分公司的云邮件节点服务器相互连接形成的一个庞大的网络（云端）。在这个网络中，各个分公司的邮件服务器（云节点）负责管理和存储本分公司用户的邮件数据，并通过网络与其他分公司的邮件服务器进行通信。以某跨国大型企业的云邮件系统为例，该系统包含了位于亚洲、欧洲、北美洲等地的多个分公司的云邮件节点，这些节点通过高速网络连接在一起。在实际应用中，云节点内部和节点之间会产生大量邮件交互。

用户之间的通信方式主要包括节点内部通信和多个关联节点的云端通信。节点内部通信是指节点内的用户之间通过

邮件进行沟通协作，这种通信方式通常具有频繁的交互和较高的信任度。云端通信则是指不同节点的用户之间进行邮件往来，这种通信方式涉及到不同节点之间的信息共享和协作，需要确保信息的准确性和安全性。

在此基础上，引入分布式分配和集中式分配两个资源分配模型。分布式分配是指各个节点的防御者 $D=D_1,D_2,\cdots,D_{|D|}$ 在其负责保护的单个云节点中进行防御资源分配。集中式分配是指云邮件服务商 D_{cloud} 在其负责保护的多个相互关联节点的云端中进行防御资源分配。分布式分配强调每个防御者独立管理各自的防御资源，专注于提升内部通信安全性。而集中式分配涉及多个防御者协同分配防御资源，提升内部通信安全性的同时强化跨节点通信安全。

攻击者与防御者在云邮件节点中的互动是一个复杂的博弈过程。攻击者通常会通过发送钓鱼邮件或垃圾邮件等方式，试图获取用户的敏感信息或破坏节点的正常运行。攻击者会精心设计钓鱼邮件的内容和形式，使其看起来像是来自可信的银行、政府机构或企业内部的重要节点；他们还会利用社交工程技术，了解用户的行为习惯和兴趣爱好，从而提高钓鱼邮件的成功率。而防御者则通过有效的防御资源配置策略，降低攻击造成的损害，提升节点的安全性。防御者会采用多种技术手段，如邮件过滤、身份验证、加密通信等，来识别和拦截钓鱼邮件和垃圾邮件；他们还会根据用户的行为模式和风险评估结果，动态调整防御资源的分配，以应对不断变化的攻击威胁。

图 1 展示了攻击者与防御者的互动过程。

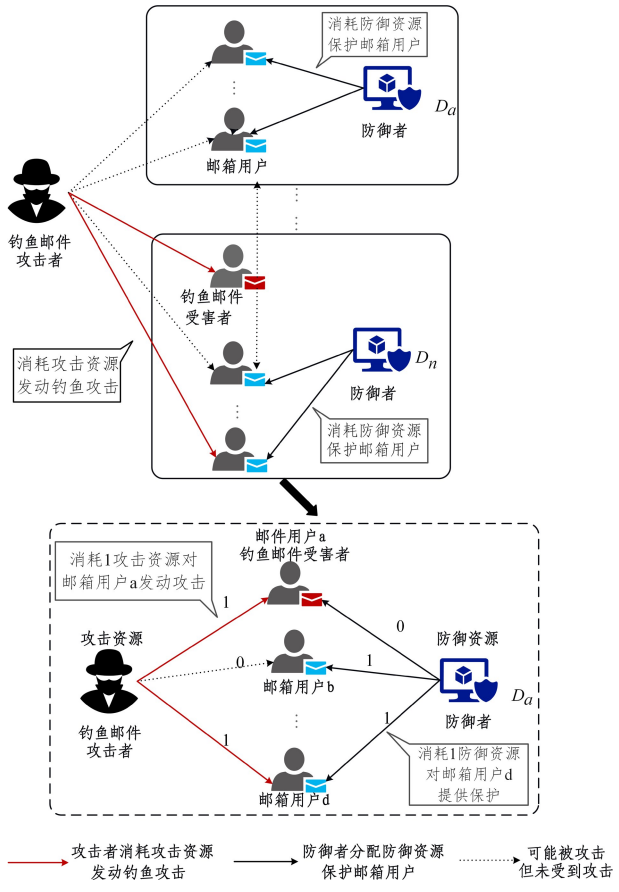


图 1 攻击者和防御者的互动过程

Fig. 1 Process of interaction between the attacker and the defender

防御者 D_a 负责保护单个云节点中的所有邮箱用户集合 $V_a\subseteq V$。攻击者对防御者 D_a 保护的两个邮箱用户 $v_{a|a}$ 和 $v_{a|d}$ 发起钓鱼攻击，$v_{a|a}$ 没有防御资源保护而可能被攻击成功，$v_{a|d}$ 受到防御资源保护而未攻击成功。若 $v_{a|a}$ 身份被盗用，则会对其联系人 $v_{a|b}$ 和防御者 D_n 负责保护的邮箱用户构成潜在威胁。防御者需要在防御资源有限的情况下，规划并执行恰当的防御资源分配策略，从而提升节点的安全性。

3.2 钓鱼邮件攻击成功率

3.2.1 用户信任关系

在云邮件节点中，为了深入理解和分析用户间的通信关系，采用有向图来进行精确表示。具体而言，设 $G=(V,E)$，其中 V 是云邮件节点中所有邮箱用户的集合，E 是云邮件节点中邮件发送方和邮件接收方之间所有通信记录的集合。每条有向边 $(s|i,m|j)\in E$ 代表由防御者 D_s 负责保护的邮箱用户 $v_{s|i}$ 向防御者 D_m 负责保护的邮箱用户 $v_{m|j}$ 发送邮件的行为。边的权重 $w(s|i,m|j)$ 则反映用户 $v_{m|j}$ 对用户 $v_{s|i}$ 的信任程度，其定义如下：

$$w(s|i,m|j)=e^{-\frac{1}{2\times n_{s|i,m|j}+n_{s|i\to m|j}}} \tag{1}$$

其中，$n_{s|i,m|j}$ 表示邮箱用户 $v_{m|j}$ 和邮箱用户 $v_{s|i}$ 互动的次数，发送一次邮件并得到一次回复计为一次互动；$n_{s|i\to m|j}$ 为邮箱用户 $v_{s|i}$ 向邮箱用户 $v_{m|j}$ 单向发送的邮件次数。当两个邮件用户沟通次数少时，信任程度会随着沟通次数增加而快速提升；然而，随着沟通次数的进一步增加，信任程度的提升速度逐渐减缓。这种量化方式能够较为准确地反映用户之间的实际信任关系。

当攻击者使用未知邮箱账号（该邮箱账号与目标用户未曾有过任何交流）对目标邮箱用户发送钓鱼邮件时，只考虑向单向发送一次邮件的情况，则 $n_{s|i,m|j}=0$。这种情况下，目标用户对未知邮箱账号的信任程度较低。攻击者还可能盗用邮箱用户的身份，利用用户之间的信任关系进行横向钓鱼攻击。由于盗用身份的邮箱用户与目标用户存在一定的信任关系，其发送的钓鱼邮件可能更容易被目标用户接受，从而增加了攻击成功的概率。例如，若攻击者盗用用户 A 的身份，向与 A 有频繁邮件往来且信任程度较高的用户 B 发送钓鱼邮件，则用户 B 可能会因为对 A 的信任而放松警惕，点击邮件中的恶意链接或泄露敏感信息，导致攻击成功。

3.2.2 攻击成功率计算模型

在云邮件节点中，用户的登录习惯、用户之间的信任程度和防御资源的分配情况，对钓鱼邮件的攻击成功率有着重要影响。为了准确评估攻击成功率，需要综合考虑这些因素。设 $p_{m|j(t)}$ 表示用户 $v_{m|j}$ 在第 t 个时间段内的登录概率，$x_{m|j(t)}$ 为邮箱用户 $v_{m|j}$ 在该时间段内的防御资源分配情况。假设 $x_{m|j(t)=1}$ 表示该邮箱用户此时被保护，$x_{m|j(t)=0}$ 表示该邮箱用户此时未被保护，$w(s|i,m|j)$ 表示被攻击用户 $v_{m|j}$ 对发起攻击用户 $v_{s|i}$ 身份的信任程度，则攻击者在第 t 个时间段内对邮箱用户 $v_{m|j(t)}$ 实施钓鱼攻击的成功概率模型定义如下：

$$P_{\text{attack}}(m|j,t)=p_{m|j}(t)\cdot w(s|i,m|j)\cdot(1-x_{m|j}(t)) \tag{2}$$

从式(2)可以看出，攻击成功率与用户的登录概率和用户之间的信任程度成正比。当被攻击用户未分配防御资源，且用户登录概率和用户之间信任程度较高时，攻击成功的概率会显著增加。在用户登录频繁的时间段，如果没有足够的防

御资源进行保护，攻击者就有更多机会发送钓鱼邮件并成功实施攻击。相反，若为用户分配了防御资源，即使登录概率较高，攻击成功的可能性也会大大降低。这是因为防御资源可以对邮件进行过滤筛查，及时发现并拦截钓鱼邮件，从而保护用户的安全。

在实际的云邮件节点中，通过分析用户的历史登录数据，可以准确估算用户的登录概率。对一定时间范围内用户登录时间和频率的统计分析，可以揭示用户的登录规律，从而预测其在不同时间段的登录概率。图 2 展示了本文实验中使用的邮件数据集中所有邮箱用户在一天 24 个时间段内的平均登录情况。云邮件节点中的防御资源分配应依据节点的风险评估结果和现有资源状况进行合理调整。在高风险时间段，例如用户登录高峰期（如图 2 中的 9－13 时和 15－22 时）或钓鱼邮件攻击频发时段，应适当增加防御资源的投入，以确保用户的安全。而在低风险时间段，则可以适当减少防御资源的分配，以提高资源的利用效率。

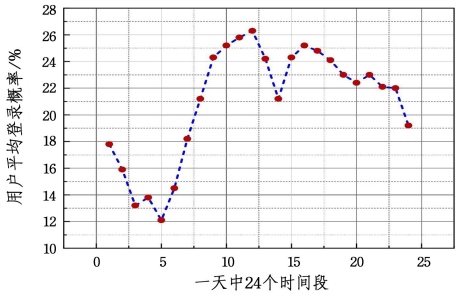


图 2　所有用户一天内的平均登录概率

Fig. 2　Average probability of logging in over the course of a day for all users

3.3　单个云邮件节点的风险

在单个云邮件节点中，评估单个邮箱用户未被保护时对节点带来的风险，需要考虑目标邮箱用户可能遭受来自未知邮箱账号或其常用联系人的攻击。这些常用联系人既可能是同一节点内的用户，也可能是云端其他节点内的邮箱用户。实际情况中，假设某企业员工（防御者 D_m 保护的用户 $v_{m|j}$）的一个常用联系人是其他节点 D_{-m} 中的邮箱用户 $v_{-m|i}$，若 $v_{m|i}$ 的身份被攻击者盗用，其就有可能利用这一信任关系向 $v_{m|j}$ 发送钓鱼邮件。

一个邮箱用户的常用联系人列表具有特定的网络结构特征，不同邮箱用户给云节点带来的风险程度各不相同。若某员工的常用联系人之间联系紧密，形成了一个复杂的网络结构，那么一旦其账号身份被盗用，攻击就有可能通过这个网络迅速传播，对云端邮件节点造成更大的威胁。若某员工的常用联系人较少且相互之间联系松散，其带来的风险相对较小。

邮箱用户的在线活跃度也是一个重要因素。在线活跃度高的用户，由于频繁使用邮件节点，与其他用户的交互也更为频繁，因此更容易成为攻击者的目标。在企业的业务高峰期，员工需要频繁地通过邮件进行沟通协作，此时在线活跃度高的员工收到钓鱼邮件的概率也会相应增加。若防御者能够合理分配防御资源，对高风险用户进行重点保护，那么节点的整体风险就会降低。

考虑上述因素，构建单个云节点中邮箱用户的风险评估模型。首先，定义 $U^t_{m|j}$ 为第 t 时间段内，防御者 D_m 负责保护的所有邮箱用户中，邮箱用户 $v_{m|j}$ 未分配防御资源的常用联系人所构成的集合，则 $|U^t_{m|j}|$ 表示该集合中的用户总数量。对于不能感知到的云端其他节点中的常用联系人，防御者考虑最坏情况，认为其全部未分配到防御资源。从单个云节点的角度来看，第 t 时间段内，单个云节点中邮箱用户被攻击成功的概率（邮箱用户给云节点带来的风险）定义如下：

$$R^t_{m|j}=P_{\text{unknown}}(m|j,t)+P_{\text{contact}}(m|j,t)-P_{\text{unknown}}(m|j,t)\times P_{\text{contact}}(m|j,t) \tag{3}$$

其中，$P_{\text{unknown}}(m|j,t)$ 表示目标邮箱用户 $v_{m|j}$ 被互联网中未知邮箱账号攻击成功的概率；$P_{\text{contact}}(m|j,t)$ 表示邮箱用户 $v_{m|j}$ 被 $U^t_{m|j}$ 中的邮箱用户发送钓鱼邮件攻击成功的概率。由于被互联网中未知邮箱账号攻击成功和攻击者盗用常用联系人身份后攻击成功这两种情况相互独立，因此需减去重复计算概率的部分。$P_{\text{contact}}(m|j,t)$ 的计算具体定义如下：

$$P_{\text{contact}}(m|j,t)=\sum_{s|i\in U_{m|j}} w(s|i,m|j)\cdot p_{m|j}(t)\cdot(1-x_{m|j}(t)) \tag{4}$$

在此基础上，云节点 D_m 中所有邮箱用户在第 t 时间段对云节点造成的风险总和可以表示为：

$$R^t_m=\sum_{m|j\in v_m} R^t_{m|j} \tag{5}$$

通过这个风险评估模型，可以全面、准确地评估单个云节点的风险程度，为后续的防御资源分配提供科学依据。在实际应用中，可以根据这个模型的计算结果，对风险较高的用户和时间段进行重点防御，合理分配防御资源，从而有效降低云节点的安全风险。

3.4　多个相互关联节点的云端风险

与单个云节点不同，云端中的各个节点之间存在着复杂的关联和交互。在评估云端风险时，需要综合考虑多个节点中用户的用户行为、信任关系以及防御资源分配情况。由于云端涉及多个云节点之间的邮件通信，攻击者的攻击范围更广，攻击手段也更加多样化，这增加了风险评估的复杂性。某攻击者可能通过攻击一个节点中的邮箱用户，进而利用该用户与其他节点中的用户联系，来扩大攻击范围，对云端邮件节点造成威胁。

信息不完全在云邮件节点风险评估中也带来了独特的挑战。单个节点的防御者在制定防御策略时，因无法获取其他节点的资源配置信息，往往将其他节点中自身的常用联系人邮箱用户默认判定为缺乏对应防御资源的对象，这会导致部分邮箱用户被攻击的风险被高估，使得防御资源分配次优。而云邮件服务商则具备对整个云端用户之间的邮件通信模式和防御资源分配策略进行全面分析的能力，能够整合来自不同节点的用户数据，给出更为准确的风险评估。这一能力使得云邮件服务商 D_{cloud} 在云端邮件节点风险评估中扮演着重要角色，其能够利用更全面的信息，为防御策略的制定提供更可靠的依据。

为了准确评估云端邮件节点的风险，定义 $U^{t,\text{cloud}}_{m|j}$ 为在第 t

时间段云端所感知到的用户(云端所有节点 V 中的所有邮箱用户)$v_{m|j}$ 的常用联系人中未分配防御资源的邮箱用户构成的集合。第 t 个时间段内,邮箱用户 $v_{m|j}$ 对多个相互关联节点的云端造成的风险如下:

$$R_{m|j}^{t,\text{cloud}} = P_{\text{unknown}}(m|j,t) + P_{\text{contact}}^{\text{cloud}}(m|j,t) - P_{\text{unknown}}(m|j,t) \times P_{\text{contact}}^{\text{cloud}}(m|j,t) \tag{6}$$

其中,$P_{\text{contact}}^{\text{cloud}}(m|j,t)$ 表示目标邮箱用户 $v_{m|j}$ 被 $U_{m|j}^{t,\text{cloud}}$ 中的邮箱用户发动钓鱼邮件攻击成功的概率,具体定义如下:

$$P_{\text{contact}}^{\text{cloud}}(m|j,t) = \sum_{s|i \in U_{m|j}^{t,\text{cloud}}} w(s|i,m|j) \cdot p_{m|j}(t) \cdot (1 - x_{m|j}(t)) \tag{7}$$

从多个相互关联的云端(云邮件服务商)角度来看,用 $R_{m|j}^{t,\text{cloud}}$ 表示邮件用户 $v_{m|j}$ 给防御者(节点)D_m 带来的风险。D_m 中所有邮箱用户在第 t 时间段的总风险可以表示为:

$$R_m^{t,\text{cloud}} = \sum_{m|j \in V_m} R_{m|j}^{t,\text{cloud}} \tag{8}$$

最后,多个相互关联节点的云端风险是云邮件节点中所有用户风险的总和,可以通过式(9)计算云邮件服务商面临的总风险。

$$R_{\text{cloud}} = \sum_{t=1}^{24} \sum_{m \in D} R_m^{t,\text{cloud}} \tag{9}$$

通过准确计算云邮件服务商的风险,可以确定不同云节点、不同用户在不同时间段的风险程度,从而有针对性地分配防御资源。对于风险较高的节点和用户,加大防御资源的投入,提高其防御能力;对于风险较低的节点和用户,可以适当减少防御资源的分配,优化资源利用效率。

4 防御资源分配方案的设计

4.1 分配防御资源,降低节点风险

防御者 D_m 的核心目标是通过制定科学合理的防御资源分配策略,有效降低其负责节点在各个时间段所面临的潜在风险。这一目标对于保障企业邮件节点的安全稳定运行及保护企业和用户的信息安全具有至关重要的意义。防御者优化函数可以精确表述为:

$$x_m^*(t) = \arg\min \sum_{t=1}^{24} R_m^{t,\text{enterprise}}, x \geqslant 0 \tag{10}$$

其中,$x_m^*(t)$ 表示防御者 D_m 在时间段 t 的最优防御资源分配策略。防御者通过调整 $x_m^*(t)$,合理分配防御资源来降低 $R_m^{t,\text{enterprise}}$ 的值,从而降低单个云节点的整体风险。

在实际应用中,防御者可以根据用户的风险评估结果,对风险较高的用户优先分配防御资源;通过实时监测用户的行为数据,如登录时间、邮件收发频率等,及时调整防御资源的分配策略;在用户登录高峰期,增加对高风险用户的防御资源投入,以应对可能出现的钓鱼邮件攻击。此外,防御者还可以结合用户之间的信任关系,对与高风险用户有密切联系的用户进行重点保护,从而有效降低云邮件节点的整体风险。

从云邮件服务商的角度来看,其具备对多个相互关联节点的云端邮件节点进行全面监控和管理的能力。与防御者相比,云邮件服务商 D_m 能够获取更全面、更准确的信息,从而能更深入地感知单个节点风险。云邮件服务商了解云端的防御资源分配策略,其感知到的节点的风险更准确。为了实现 D_{cloud} 风险的最小化,云邮件服务商引入了一个节点级别的优化目标,对云端各个时间段的防御资源进行全局优化。优化目标可表示为:

$$x_{\text{cloud}}^*(t) = \arg\min \sum_{t=1}^{24} \sum_{m \in D} R_m^{t,\text{cloud}} \tag{11}$$

其中,$x_{\text{cloud}}^*(t)$ 表示云邮件服务商在时间段 t 内的最优防御资源分配策略。云邮件服务商通过优化 $x_{\text{cloud}}^*(t)$,可以实现对多个相互关联节点之间的防御资源的合理调配,降低节点风险。

云邮件服务商通过分析用户行为数据,把握行为模式与风险特征,并实时监测各个节点的防御资源分配情况,从而能够及时察觉安全威胁并调整防御资源分配。如发现某个节点中用户登录频繁且邮件互动异常但防御资源数量不足,D_{cloud} 可及时从别的节点调配防御资源,以降低其节点风险。

4.2 单节点资源动态分配算法

在云邮件节点的防御过程中,单个企业邮件节点防御资源的合理分配是保障节点安全的关键环节。本节提出了单节点资源动态分配算法 SN-DRA,该算法通过考虑多维度的用户行为因素,实现防御资源的优化配置,有效降低节点的整体风险。算法 1 详细描述了 SN-DRA 的具体实现过程。

算法 1 单节点资源动态分配算法(SN-DRA)

输入:邮件用户登录概率,邮件用户交流信息

输出:防御资源分配策略

1. 初始化 D_m 的防御资源分配列表
2. 根据式(1)计算各个用户之间的信任度
3. while D_m 中存在未分配的防御资源 do
4. for 对每一个时间段 t do
5. 根据式(3)计算节点 D_m 中在第 t 时间段内每个用户 $v_{m|i \in V_m}$ 的风险 $R_{m|i}^t$
6. end for
7. 将风险从大到小排序,更新用户风险列表
8. 从 D_m 的风险列表中选取风险最大 $R_{m|max}^t$ 的邮箱用户 $v_{m|max}$ 并分配防御资源
9. 将 $x_{m|max}^t = 1$ 添加到 D_m 防御资源分配列表
10. end while
11. 根据式(5),结合 D_m 防御资源分配列表计算 D_m 此时的风险总值 R_m
12. 返回 R_m 和 D_m 的防御资源分配列表

首先,初始化 D_m 的防御资源分配列表,并依据式(1)计算邮件用户之间的信任度。信任度是反映用户之间互动关系的重要指标,它综合考虑了用户的邮件交流频率和互动质量。

在计算了用户之间的信任度之后,便进入防御资源分配阶段。首先,检查是否还有未分配的防御资源。如果防御资源尚未完全分配,则根据式(3)计算防御者 D_m 负责节点中每个邮件用户被攻击成功的概率,即每个用户给 D_m 带来的风险。然后,从 D_m 的用户风险列表中选择此时段内风险最大的用户,优先分配防御资源。这样可以确保节点在防御资源有限的情况下,优先保护最容易受到攻击的用户。例如,在某一时间段,用户 G 的风险值在所有用户中最高,那么就优先为用户 G 分配防御资源,以降低其被攻击成功的概率。

在完成一次防御资源的分配后,必须重新计算每个用户的风险值。根据式(5),防御资源的分配可以有效地降低单个

云节点的风险。一个邮箱用户受到保护，同时段内，其他邮箱用户被攻击成功的概率也会发生变化。因此，节点需要根据已分配的防御资源，重新评估每个用户的风险值，并更新用户风险列表。列表中的用户需要根据新的风险值进行排序，确保下一轮资源分配时风险较高的用户能够得到优先保护。例如，为用户 G 分配防御资源后，其他用户风险值发生变化，此时重新计算其他用户的风险值，可能会发现用户 H 的风险值排名上升，成为新的高风险用户，那么在下一轮资源分配时，就会优先为用户 H 分配资源。

在每次资源分配和风险更新后，节点需要检查防御资源是否已经完全分配。如果仍有剩余资源，继续执行上述步骤，直到所有的防御资源被有效分配完毕。这样可以确保资源的分配过程高效且全面，最终实现最优的资源利用。

当所有防御资源被分配完毕后，算法将输出最终的防御资源分配策略和此时 D_m 负责节点的风险总值。防御资源分配策略会明确地记录不同时间段内，各个用户在某时段具体获得的保护。通过该算法，单个云节点能够根据用户行为动态调整防御措施，使得防御资源能够动态且合理分配，有效降低云邮件节点面临的安全风险。

4.3 多节点资源协同分配算法

在云邮件环境中，不同的云邮件节点相互关联且安全威胁各异，单节点的资源分配策略难以从全局视角实现资源的最优利用与风险控制。多节点资源协同分配算法 MN-RCA 旨在打破节点壁垒，实现云端多节点间防御资源的智能调配。以节点 A 中已分配给用户 a 的防御资源为例，从云端全局视角分析，若将该资源重新调配至节点 B 的用户 b，且满足两项核心条件 —— 节点 A 的风险水平不升高（即保持稳定或降低）、云端整体风险显著降低，则执行该跨节点资源转移操作。这一过程需综合评估各节点内用户的风险状况、现有防御资源的分配效果以及资源转移对不同节点和云端全局风险的影响，从而构建一个动态、协同的资源分配体系，提升整个云端邮件节点的安全性与资源利用效率。

算法 2 详细阐释了 MN-RCA 的具体执行流程。

算法 2 多节点资源协同分配算法（MN-RCA）

输入：各个节点的防御资源分配方案，各个节点的邮件用户信息

输出：优化后的跨节点资源调配方案

1. 根据式(3)计算每一个用户的节点风险值
2. 根据式(6)计算每一个用户的云端风险值
3. 记录当前所有节点防御资源分配状态
4. 初始化资源转移列表 transferlist＝Ø
5. for 对每一个节点$D_m \in D$do
6. 找到D_m在所有时间段 t 内的已分配资源用户中给节点D_m所带来风险最小的用户v_m
7. for 遍历v_m的常用联系人所属节点内的所有未分配防御资源的邮箱用户v_{-m}do
8. 计算出防御资源从v_m转移到v_{-m}后系统D_m的风险值R_{-m}
9. 计算出防御资源从v_m转移到v_{-m}后云端D_{cloud}的风险值R_{-cloud}
10. if $R_{-m} \leqslant R_m$ and $R_{-cloud} < R_{cloud}$ do
11. 将资源从v_m转移到v_{-m}
12. 将时间段 t、提供资源用户v_m及收到资源用户v_{-m}记录到 transferlist
13. else if 若还有未遍历过的用户v_{-m}则继续执行 for 循环
14. end if
15. end for
16. end for
17. 返回资源转移列表 transferlist

首先，需对每个用户的风险状况进行全面量化评估。依据已构建的风险评估模型，深度融合邮件用户信息，计算出每一个用户的云端全局风险值。此值综合考虑了用户在整个云端邮件系统中的行为模式、交互关系以及潜在安全威胁等多维度因素，精准反映出用户对全局安全态势的影响程度。同时，计算该用户对所归属节点的风险值，这一数值聚焦于用户在本节点内的活动特征与风险关联，为后续资源分配提供了节点层面的风险参考。

在完成用户风险值计算后，全面记录当前所有节点防御资源的分配状态。遍历每一个节点的防御资源分配策略，了解每个用户所分配到的防御资源数量以及资源的使用状态等关键信息。这些详尽的记录为后续资源转移分析提供了基础数据，确保在资源调配过程中能够清晰掌握各节点的初始状态与资源分布情况。

紧接着，初始化一个资源转移列表，此列表将作为后续存储符合条件的资源转移信息的载体。在正式进入资源转移筛选阶段后，针对每一个节点展开分析。在节点的所有运行时间段内，深入挖掘已分配资源用户中对本节点带来风险最小的用户。该用户的确定并非仅仅基于单一风险指标，而是综合考虑了用户的防御资源分配情况、与节点内其他用户的交互风险传播路径以及在过往时段内对节点安全的实际影响等多方面因素。

一旦确定了风险最小的用户，便针对该用户的常用联系人所属节点内的每一个未分配防御资源的邮箱用户展开深入评估。假设将风险最小用户的防御资源转移至目标用户，在此假设情境下，运用特定的风险计算模型，精准计算出节点在资源转移后的新风险值。该模型充分考虑了资源转移对节点内用户风险传播路径的改变、资源重新分配后的防御覆盖范围变化以及节点整体的安全脆弱性调整等因素。同时，计算这种资源转移对云端全局风险值的影响，其全面反映了资源转移对整个云邮件节点安全态势的宏观影响。

若资源转移后节点的新风险值小于或等于原风险值，并且云端全局风险值相较于初始值有所降低，则表明此次资源转移具备合理性与可行性。此时，果断执行资源从风险最小用户到目标用户的转移操作，并将本次资源转移所涉及的关键信息（包括转移发生的时间段、提供资源的用户以及接收资源的用户等）详细记录到资源转移列表中。这些记录不仅为后续的资源调配效果评估提供了数据支撑，也为节点的安全审计与回溯分析奠定了基础。

反之，若资源转移后的风险评估结果不满足上述条件，且仍存在未遍历的目标用户，则继续在内层循环中寻找下一个可能的资源转移对象。这种循环筛选机制，能确

保对每一个潜在的资源转移可能性进行全面评估，不放过任何一个优化资源配置的机会。当所有节点都完成上述资源转移可能性筛选后，算法将返回最终的资源转移列表。该列表清晰明确地展示了在不同时间段内跨节点的资源优化分配方案，为云节点间的防御资源协同分配提供了具体且可执行的指导策略。通过 MN-RCA 算法，各云节点能够实现防御资源的动态协同调配，有效提升云端邮件系统在面对复杂多变安全威胁时的应对能力，显著降低节点遭受攻击的风险。

5 实验及分析

5.1 实验设计

5.1.1 实验数据集

实验选用高校的真实邮件数据集以及其遭受的真实钓鱼邮件攻击记录作为数据来源。该高校邮件节点涵盖多个学院、行政节点以及科研机构的用户，具有广泛代表性和多样性。真实邮件数据集包含 2018 年全年度 51 个节点的 1490 名用户的登录时间、地点和方式，能反映用户使用习惯和活跃程度；还包含 11719 条单位内用户联系收发邮件的详细信息，包括邮件发送时间、接收时间、发件人、收件人以及邮件内容等，对研究用户之间的通信模式和信任关系至关重要。真实钓鱼邮件攻击记录详细记录了攻击者发起钓鱼邮件的时间以及用户的回复时间，通过分析这些记录，可深入了解攻击者的攻击策略和时间规律，以及用户对钓鱼邮件的响应情况。

5.1.2 实验场景设置

本文设置了 4 个实验场景，以全面对比不同攻击方式和防御模式下的防御效果，探究防御资源分配的最优策略。场景一是基于真实钓鱼邮件攻击数据来模拟攻击并采用分布式防御策略，各节点独立管理防御资源，专注提升单个节点内部的通信安全性，能真实反映实际攻击下分布式防御策略的效果。场景二是随机时间段发起钓鱼邮件攻击并采用分布式防御策略，攻击时间随机分配，模拟攻击的不确定性，以研究分布式防御策略在攻击时间不确定情况下的适应性和有效性。场景三是基于真实攻击数据的钓鱼邮件攻击并采用协同式防御策略，多个节点协同分配防御资源，提升节点内部通信安全性的同时优化跨节点通信安全，用于检验协同式防御策略在应对真实攻击时的优势和效果。场景四是随机时间段的钓鱼邮件攻击并采用协同式防御策略，旨在结合随机攻击时间和协同式防御策略，探究复杂情况下协同式防御策略的性能表现。4 个场景的特征如表 1 所列。

表 1 实验场景特征的对比

Table 1 Comparison of experimental scene features

实验场景	防御模式	攻击模式	用户被攻击概率	跨节点调资源
场景一	分布式	真实数据	历史行为	不支持
场景二	分布式	随机分配	均匀分布	不支持
场景三	协同式	真实数据	历史行为	支持
场景四	协同式	随机分配	均匀分布	支持

在每个场景下，攻击与防御资源数量通过用户覆盖比例量化。攻击规模 α 分别设定为 10%，20%和 30%，以模拟不同规模的攻击情况；防御资源覆盖度 β 从 10%至 90%递增调整，实验时间范围为模拟一天 24 小时，以全面评估不同防御资源数量投入下的防御效果。在 4 个实验场景中，全天的总防御资源量保持固定（即防御资源覆盖度的日均值为预设值，如 10%，30%，50%），各时段的具体资源分配数量由不同方法的算法逻辑决定；本文方法结合用户行为数据（登录概率、信任关系）与风险评估模型，在不同时段下动态分配资源数量；Victor 方法、Wang 方法与 Essia 方法则是将单日防御资源均匀分配至各个时段；Masaki 方法通过分析各时段的历史攻击概率，按攻击发起概率的占比动态分配资源数量，即攻击概率越高的时段获得的资源数量比例越高。

5.1.3 实验评价指标

为科学评估防御策略的有效性，引入 3 个实验评价指标：时段系统损失值（Time Specific System Loss Value，TSLV），全天系统总损失值（Total Daily System Loss，TDSL），以及资源效率提升率（Resource Efficiency Improvement Rate，REIR）。TSLV 指单个时段（如 10:00－11:00）内，云邮件系统因钓鱼攻击出现损失的量化值。在单个时段内，若某个用户被钓鱼攻击成功，则 TSLV 加 1。TDSL 通过整合 24 小时内各时段的 TSLV，反映防御策略在全天候动态攻击场景下的整体防御效果。REIR 是指在拥有同等防御资数量下，协同式防御策略相较于分布式策略的系统损失降低比例。该指标直接体现跨节点资源协同对资源利用效率的优化程度，数值越高表明协同分配策略的优势越显著。

$$REIR=\left(1-\frac{\text{协同式策略损失}}{\text{分布式策略损失}}\right)\times 100\%$$

5.1.4 对比方法

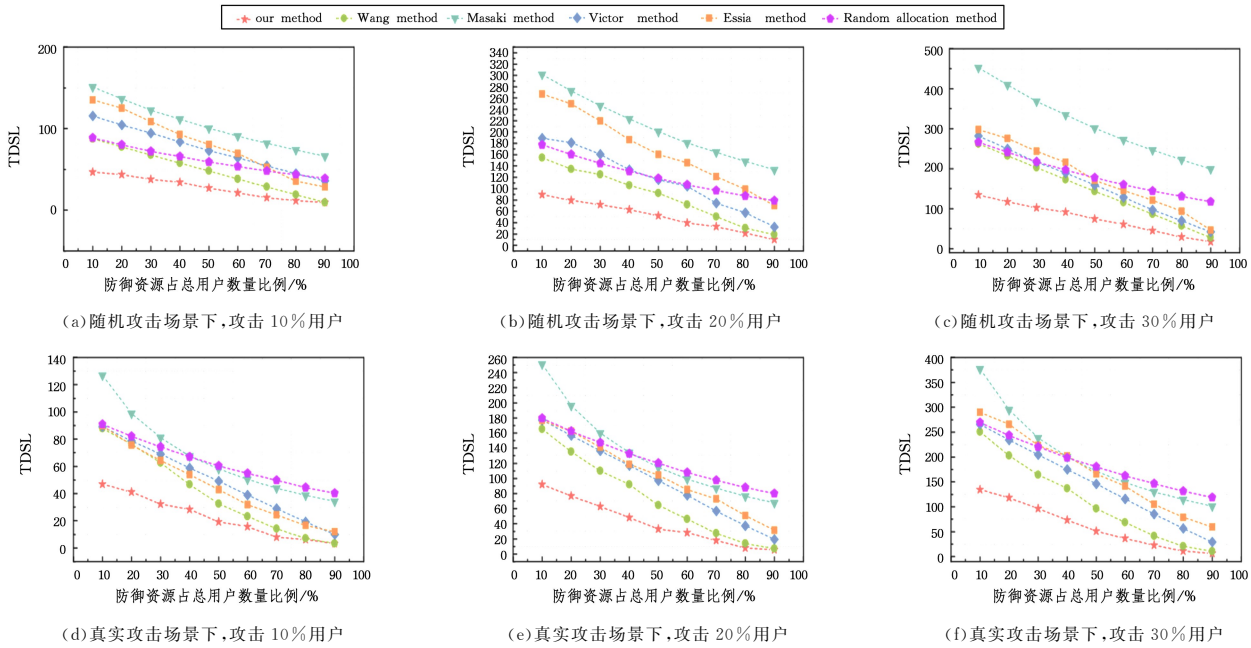
实验选取了 5 种具有代表性的防御资源分配方法作为对比，分别为 Victor 方法[28]、Wang 方法[29]、Masaki 方法[30]、Essia 方法[31]，还引入防御资源随机分配方法作为基准。Victor 方法通过为网络中的节点提供资源来遏制传播过程，定义了预防性资源和纠正性资源，寻找成本最优的资源分配方案，最大限度地加强防御效果。Wang 方法提出基于网络拓扑结构优化资源分配的概念，通过识别网络中的关键节点分配资源，加强遏制效果，专注于在有限预算条件下降低攻击整体传播率。Masaki 方法探讨复杂的优化资源分配问题，定义了两类资源分配方案，在成本约束下寻找最小化适应率和接受率的方案，在性能受限场景下确保总成本最小化，同时使受感染节点的衰减率满足指定约束要求。Essia 方法旨在通过中心性测量方法（度数、接近、介度、特征向量中心性）识别关键节点，并在预算限制内优化资源分配策略来增强网络安全。随机分配方法将所有防御资源在网络中随机分配给每个受保护的用户，不考虑任何节点特征或网络拓扑结构，作为基准

测试，能直观展示其他优化方法在资源分配上的优势。

5.2 实验结果与分析

5.2.1 分布式分配防御资源方法效果对比

在分布式分配防御资源的实验中，对 6 种不同方法在场景一和场景二中的 6 个测试案例进行了全面对比。实验结果如图 3 所示，可以清晰地看出，随着攻击规模的不断扩大，各个方法均导致 TDSL 呈现出增长趋势，这表明攻击规模的增大无疑会给节点带来更大的损失。随着防御资源数量的不断增多，TDSL 也呈现出明显的下降趋势，这充分说明增加防御资源能够有效降低节点损失，提升节点的防御能力。在这 6 个测试案例中，SN-DRA 方法均取得了最低的 TDSL，展现出了卓越的防御效果。具体而言，在 6 个测试案例下，SN-DRA 方法的 TDSL 在各攻击规模下均显著低于对比方法。



(a)随机攻击场景下，攻击 10%用户　(b)随机攻击场景下，攻击 20%用户　(c)随机攻击场景下，攻击 30%用户

(d)真实攻击场景下，攻击 10%用户　(e)真实攻击场景下，攻击 20%用户　(f)真实攻击场景下，攻击 30%用户

图 3　分布式分配防御资源方法效果的对比

Fig. 3　Comparison of the effectiveness of distributed approaches to allocating defense resources

针对不同的攻击规模(10%，20%，30%)，记录了防御资源数量从 10%开始，以 10%为步长递增至 90%的 9 种不同情况下的 TDSL 值。然后，对每个攻击规模下的 9 个损失值求和并取平均，得到该攻击规模对应的 TDSL 均值，具体数值详见表 2 和表 3。

同时，为了直观地展示 SN-DRA 方法的优势，括号内给出了在相同防御资源数量和攻击规模下 SN-DRA 方法相比于对应对比方法 TDSL 所降低的百分比。

表 2　分布式分配资源方法的效果比较(场景一)

Table 2　Comparison of the effectiveness of distributed resource allocation methods(scenario 1)

方法	$\alpha=10$	$\alpha=20$	$\alpha=30$
Our method	22.32	41.34	61.15
The Victor method	49.10 (54.53%)	97.27 (57.45%)	145.91 (58.06%)
The Wang method	39.28 (43.21%)	73.46 (43.72%)	110.31 (44.54%)
The Masaki method	66.65 (66.43%)	131.84 (68.63%)	197.48 (69.01%)
TheEssia method	45.69 (51.06%)	104.87 (60.58%)	170.25 (64.09%)
Random allocation method	62.68 (64.34%)	123.89 (66.67%)	185.74 (67.03%)

表 3　分布式分配资源方法的效果比较(场景二)

Table 3　Comparison of the effectiveness of distributed resource allocation methods(scenario 2)

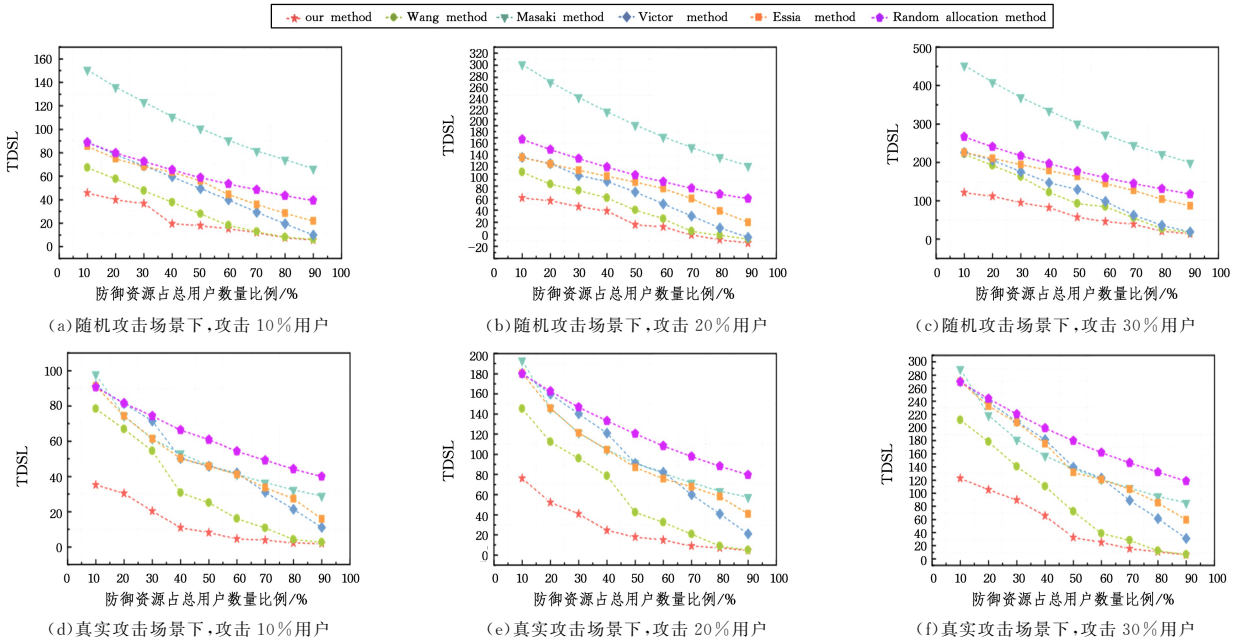
方法	$\alpha=10$	$\alpha=20$	$\alpha=30$
Our method	27.36	50.95	74.56
The Victor method	74.54 (63.33%)	116.53 (56.30%)	159.30 (53.19%)
The Wang method	48.16 (43.21%)	87.01 (41.43%)	144.47 (48.34%)
The Masaki method	103.92 (73.70%)	207.93 (75.47%)	311.90 (76.06%)
TheEssia method	80.98 (66.23%)	168.77 (69.87%)	178.87 (58.34%)
Random allocation method	61.09 (55.20%)	122.32 (58.38%)	183.47 (59.43%)

SN-DRA 方法的 TDSL 显著低于 Victor 方法，因为其不仅考虑了用户之间的沟通次数，还考虑了用户之间的信任程度，以及用户不同时段的登录概率，从而获得了更好的防御资源分配优化效果。SN-DRA 比 Wang 方法更有效，得益于其考虑了用户和用户之间的关系，进而考虑了横向钓鱼攻击情况，能够更好地优化防御资源的分配。SN-DRA 比 Essia 方法更有效，是因为其不仅考虑了邮件用户在邮件社交网络中节点的中心性，更考虑了不同时间段下用户的登录概率，能够更好地进行防御资源的动态分配。Masaki 方法的 TDSL 在所有方法中最高，在分布式分配情况下，其在场景一的表现比在场景二中好，在相同攻击规模下，TDSL 分别降低了 35.86%，36.59%，36.68%，

这得益于其向攻击较频繁的时间段投入了较多的防御资源，因此在对不同时间段的攻击比重不同的真实攻击情况下的效果更好。资源随机分配方法是在两种场景下 TDSL 第二高的方法，因为其不考虑任何因素，将所有不同时间段内的所有用户视为相同个体，完全随机分配防御资源，所以效果不理想。

5.2.2 协同式分配防御资源方法效果的对比

在协同式资源分配方法的实验中，对 5 种不同防御方法在场景三与场景四下的表现进行了深入考查。图 4 直观地展示了各方法 TDSL 的对比情况。随着攻击规模的逐步扩大，所有方法的 TDSL 均呈现上升趋势；而当防御资源投入增加时，TDSL 通常会降低，这充分表明了资源数量在抵御攻击过程中发挥着关键作用。然而，不同方法对资源的利用效率存在显著差异。本文提出的云邮件防御资源分配方法展现出了最优的资源分配效率，尤其是在资源有限的情况下，其 TDSL 始终低于其他对比方法，在实际应用中具备优势。



(a)随机攻击场景下，攻击 10%用户　(b)随机攻击场景下，攻击 20%用户　(c)随机攻击场景下，攻击 30%用户

(d)真实攻击场景下，攻击 10%用户　(e)真实攻击场景下，攻击 20%用户　(f)真实攻击场景下，攻击 30%用户

图 4　协同式分配防御资源方法效果对比

Fig. 4　Comparison of the effectiveness of collaborative approaches to allocating defense resources

表 4 和表 5 详细记录了不同攻击规模下各方法的平均 TDSL 情况。

表 4　协同式分配资源方法的效果比较(场景三)

Table 4　Comparison of the effectiveness of synergistic approaches to resource allocation(scenario 3)

方法	$\alpha=10$	$\alpha=20$	$\alpha=30$
Our method	12.99	27.37	52.51
The Victor method	49.52	99.63	149.30
	(73.75%)	(72.56%)	(64.91%)
The Wang method	32.07	60.14	88.69
	(59.53%)	(54.45%)	(40.76%)
The Masaki method	52.38	103.29	154.85
	(75.20%)	(73.53%)	(66.04%)
TheEssia method	48.94	97.97	154.28
	(73.53%)	(72.05%)	(65.93%)
Random allocation method	62.32	124.05	185.64
	(79.14%)	(77.98%)	(71.74%)

Victor 方法虽能在一定程度上降低 TDSL，但在应对复杂攻击场景时，其表现不及本文方法。深入探究发现，这主要是由于 Victor 方法在资源分配时考虑的因素较为单一，缺乏对复杂攻击环境中多种因素的综合考虑，从而限制了其在复杂场景下的防御效果。Wang 方法侧重于考虑用户登录概率，却忽略了用户之间的社交关系。这一局限性导致在面对跳板攻击和冒用身份攻击等场景时，其无法准确地根据用户之间的关联进行资源分配，使得资源分配效果不够理想，无法充分发挥防御资源的作用。Masaki 方法在掌握一定攻击概率信息时，能够发挥一定的防御效果。但当对攻击者在不同时段的攻击概率掌握不全时，其防御效果急剧下降，TDSL 显著上升。这表明，Masaki 方法对攻击概率信息的依赖程度较高，在信息不完整的情况下难以有效应对攻击威胁。资源随机分配方法由于具有随机分配防御资源的特性，在 4 个场景中关键参数值相同的情况下，TDSL 大体保持一致。这反映出该方法缺乏针对性和策略性，无法根据不同场景的特点进行有效的资源分配，从而在防御效果上表现出明显的局限性。

表 5　协同式分配资源方法的效果比较(场景四)

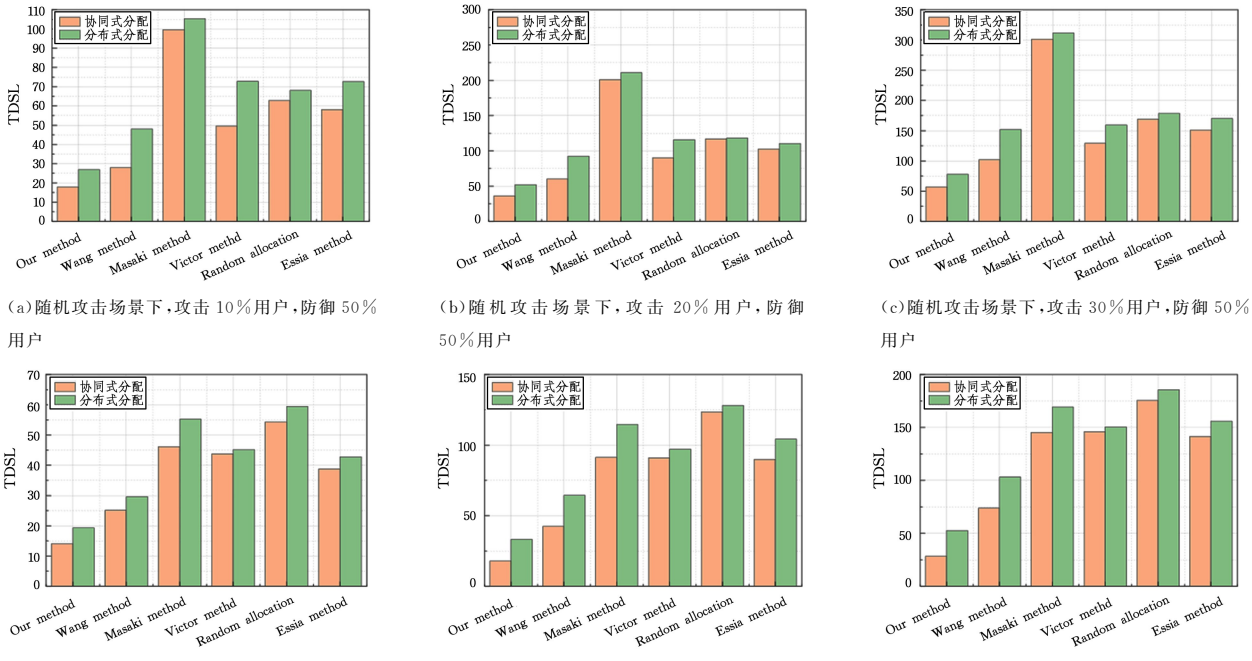
Table 5　Comparison of the effectiveness of synergistic approaches to resource allocation(scenario 4)

方法	$\alpha=10$	$\alpha=20$	$\alpha=30$
Our method	22.21	42.59	65.05
The Victor method	49.31	85.07	122.10
	(54.97%)	(49.95%)	(46.69%)
The Wang method	31.47	62.17	108.33
	(29.40%)	(31.50%)	(39.96%)
The Masaki method	103.81	207.86	311.78
	(78.65%)	(79.53%)	(79.10%)
The Essia method	53.27	100.66	159.56
	(58.28%)	(57.71%)	(59.22%)
Random allocation method	61.10	122.31	183.43
	(63.67%)	(65.20%)	(64.53%)

5.2.3 多节点资源协同分配算法的效果

实验比较了 MN-RCA 在场景三和场景四两种场景下对 5 种防御资源分配方法的提升程度。从图 5 中可以清晰地

观察到，在相同的攻击规模和防御资源覆盖度条件下，协同式分配策略的 TDSL 显著低于分布式分配策略的 TDSL。这一结果有力地证明了，MN-RCA 能够有效整合和调配云邮件节点中的防御资源，极大地提升节点的整体防御能力，从而显著减少节点在遭受攻击时的损失，有效提升防御资源利用率。



(a)随机攻击场景下，攻击 10%用户，防御 50%用户　(b)随机攻击场景下，攻击 20%用户，防御 50%用户　(c)随机攻击场景下，攻击 30%用户，防御 50%用户

(d)真实攻击场景下，攻击 10%用户，防御 50%用户　(e)真实攻击场景下，攻击 20%用户，防御 50%用户　(f)真实攻击场景下，攻击 30%用户，防御 50%用户

图 5　协同式和分布式分配效果的对比

Fig. 5　Comparison of synergistic and distributed distribution effects

表 6 列出了 $\beta=50$ 时，α 从 10 递增到 30 的过程中所有的 REIR。

表 6　MN-RCA 与 SN-DRA 相比的 REIR

Table 6　REIR for MN-RCA compared to SN-DRA

Method	真实攻击场景			随机攻击场景		
	$\alpha=10$	$\alpha=20$	$\alpha=30$	$\alpha=10$	$\alpha=20$	$\alpha=30$
Our method	22.05	41.05	38.73	44.02	25.14	28.69
Wang method	15.24	39.54	29.45	42.03	34.92	32.84
Masaki method	16.41	19.48	16.48	3.92	3.29	2.62
Victor method	2.97	10.32	4.22	26.43	18.71	18.74
Essia method	3.26	13.24	7.95	24.25	19.51	18.63
Random allocation	8.63	3.99	4.40	7.76	2.29	4.28

深入分析各方法在不同场景下的表现，Masaki 方法在场景三的效果优于场景四。这主要是因为 Masaki 方法的核心在于根据攻击概率信息来分配防御资源，在真实攻击场景中，由于攻击数据真实且具有规律性，因此 Masaki 方法能够更精准地把握攻击态势，将更多的防御资源分配到高风险时段和区域，进而有效降低节点损失。例如，在真实攻击场景下，若历史数据显示某几个特定时间段攻击频繁，Masaki 方法会针对性地在这些时段增加资源投入，使得在这些时段内节点抵御攻击的能力增强，TDSL 相应降低。而在随机攻击场景中，攻击时间的不确定性增加，Masaki 方法难以准确预判攻击概率，导致资源分配的精准度下降，防御效果也随之减弱。其他 4 种方法在从分布式分配转变为协同式分配后，均呈现出一定程度的防御效果提升。这是因为协同式分配策略打破了单个节点或节点的资源分配局限，实现了跨节点的资源共享与协同调配。

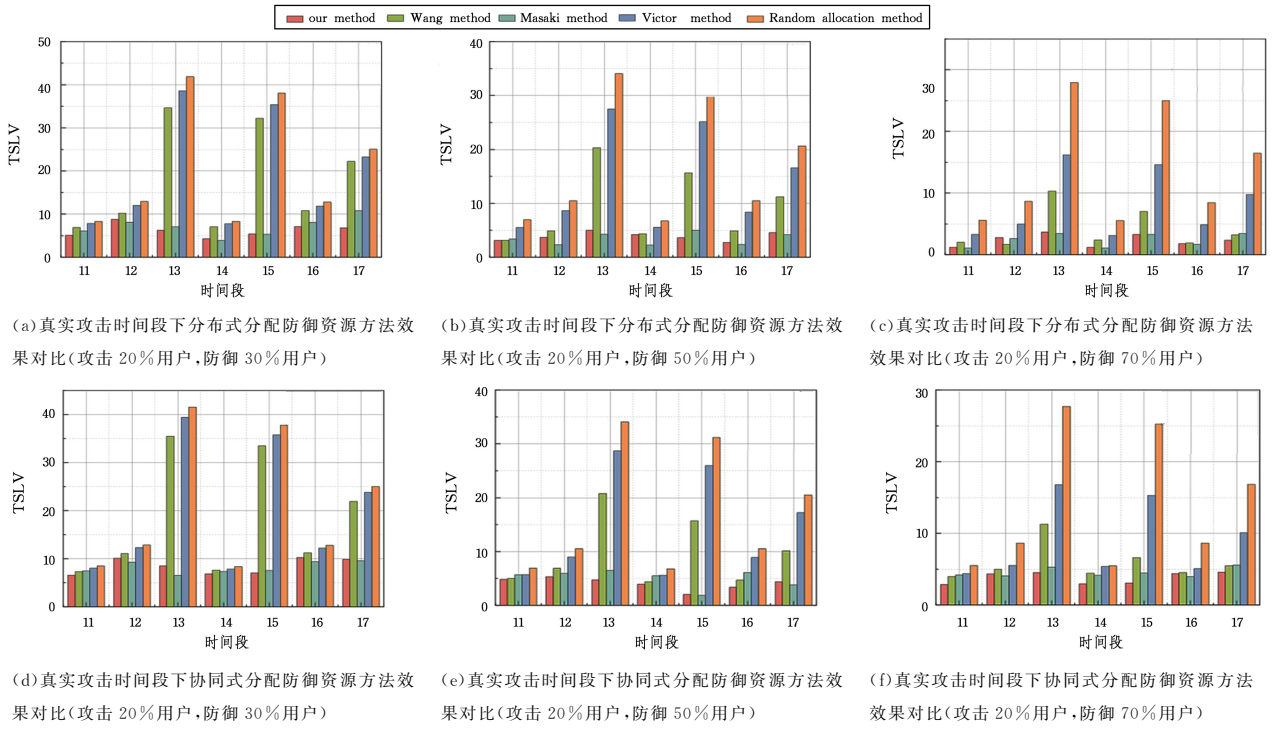
5.2.4　具体时间段下防御策略的比较

在具体时间段的比较研究中，重点探讨了场景一和场景三在 10 时到 17 时之间的 7 个时间段内，各防御资源分配方法的表现，结果如图 6 所示。通过对实验数据的详细分析发现，Wang 方法在分布式分配和协同式分配两种场景下，当防御资源覆盖规模为 30% 和 50% 时，在 13 时、15 时 和 17 时这 3 个时段的 TSLV 明显高于其他时间段。这一现象表明，在这 3 个时段，云邮件系统面临的安全风险高，当前的防御资源投入不足以有效抵御攻击，因此需要加大防御资源的投入。进一步分析 Wang 方法的原理可知，该方法主要基于网络拓扑结构进行资源分配，对用户行为和攻击时间的动态变化考虑不足。在这 3 个高风险时段，攻击方式或攻击目标的变化，使得基于固定网络拓扑结构的资源分配无法满足防御需求，导致节点损失增加。

Masaki 方法在这几个特定时间段下表现出良好的防御效果。深入研究发现，这主要是由于 Masaki 方法自身的资源分配机制，使其在这些时间段投入了大量的防御资源。如前文所述，Masaki 方法会根据攻击概率信息来分配资源，在这几个时间段检测到了较高的攻击概率，从而加大了资源投入。然而，这种资源分配方式也存在一定的局限性，在其他时段，资源可能会因在这几个时段的过度投入而相对不足，导致整体防御效果受到影响。

防御资源随机分配方法在 13 时、15 时和 17 时 这 3 个时间段的防御效果均不理想。这是因为随机分配方法不考虑任何节点特征、网络拓扑结构以及攻击态势等因素，完全随机地

分配防御资源。在这 3 个时间段，攻击规模可能相对较大，而随机分配的防御资源数量难以与攻击规模相匹配，导致防御效果较差，节点损失较高。这也从侧面反映出，科学合理的资源分配策略对于提升云邮件节点防御能力的重要性，防御资源随机分配方法无法有效应对复杂多变的攻击场景。



(a)真实攻击时间段下分布式分配防御资源方法效果对比(攻击 20%用户，防御 30%用户)

(b)真实攻击时间段下分布式分配防御资源方法效果对比(攻击 20%用户，防御 50%用户)

(c)真实攻击时间段下分布式分配防御资源方法效果对比(攻击 20%用户，防御 70%用户)

(d)真实攻击时间段下协同式分配防御资源方法效果对比(攻击 20%用户，防御 30%用户)

(e)真实攻击时间段下协同式分配防御资源方法效果对比(攻击 20%用户，防御 50%用户)

(f)真实攻击时间段下协同式分配防御资源方法效果对比(攻击 20%用户，防御 70%用户)

图 6 真实攻击时间段下资源分配方法效果的对比

Fig. 6 Comparison of the effectiveness of resource allocation methods under real attack time periods

结束语 针对云邮件节点中防御资源分配的难题，本文提出基于用户行为的云邮件防御资源分配方法。该算法构建风险评估模型，设计动态协同分配方案，提升了资源分配的科学性与有效性。实验结果表明，SN-DRA 算法和 MN-RCA 算法在云邮件节点中分配防御资源的效果显著优于现有方法，其能有效降低节点风险，提升资源利用率。然而，该算法在动态环境下的实时响应能力还有提升空间，后续可探索在线调度分配算法，以增强其在动态攻击场景中的适应性，更好地为云邮件节点安全防御技术发展助力。

参 考 文 献

[1] RADICATI. GROUP. Email statistics report 2022—2026 [R/OL]. https://www.radicati.com/wp/wp-content/uploads/2022/11/Email-Statistics-Report-2022-2026-Executive-Summary.pdf.

[2] RAO S, VERMA A K, BHATIA T. A review on social spam detection: Challenges, open is-sues, and future directions[J]. Expert Systems with Applications, 2021, 186: 115742.

[3] MACAS M, WU C, FUERTES W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities[J]. Computer Networks, 2022, 212: 109032.

[4] BOUKE M A, ABDULLAH A, ALSHATEBI S H, et al. The intersection of targeted advertising and security: Unraveling the mystery of overheard conversations[J]. Telematics and Informatics Reports, 2023, 11: 100092.

[5] ALKARAKI J N, GAWANMEH A, FACHKHA C. Blockchain for email security: A perspective on existing and potential solutions for phishing attacks[C]// 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2023: 404-411.

[6] BOUKE M A, ABDULLAH A, UDZIR N I, et al. Overcoming the challenges of data lack, leakage, and dimensionality in intrusion detection systems: a comprehensive review[J]. Journal of Communication and Information Systems, 2024, 39(1): 22-34.

[7] WONGWATKIT R, RAKTHAM M, PHAWANANTHAPHUTI T. Intelligent blacklist security system for protecting spammer in corporate email solution: A case of corporate email service provider in thailand[C]// 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE, 2022: 387-391.

[8] SURWADE A U. Blocking Phishing e-mail by extracting header information of e-mails[C]// 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing(ICSIDEMPC). IEEE, 2020: 151-155.

[9] BOUKE M A, ALRAMLI O I, ABDULLAH A. XAIRF-WFP: a novel XAI-based random forest classifier for advanced email spam detection[J]. International Journal of Information Security, 2025, 24(1): 5.

[10] LI X, ZHANG D, WU B. Detection method of phishing email based on persuasion principle[C]// 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference(ITNEC). IEEE, 2020: 571-574.

[11] HEIDING F, SCHNEIER B, VISHWANATH A, et al. Devising

and detecting phishing emails using large language models[J]. arXiv:2308.12287,2023.

[12] SYMANTEC. Symantec cloud email security [EB/OL]. https://docs.broadcom.com/doc/emailsecurity-cloud-2019-11-service-description-en.

[13] XIAO D,JIANG M Y. Malicious Mail Filtering and Tracing System Based on KNN and Improved LSTM Algorithm[C]// 2020 IEEE International Symposium on Dependable,Autonomic and Secure Computing(DASC). IEEE,2020:222-229.

[14] WEI W,WANG Q,XU H,et al. Highly complex resource scheduling for stochastic demands in heterogeneous clouds[J]. Journal of Grid Computing,2021,19:1-16.

[15] WEI W,WANG Q,YANG W,et al. Efficientstochastic scheduling for highly complex resource placement in edge clouds[J]. Journal of Network and Computer Applications,2022,202:103365.

[16] WEI W,LI H,YANG W. Cost-effective stochastic resource placement in edge clouds with horizontal and vertical sharing [J]. Future Generation Computer Systems,2023,138:213-225.

[17] GILL S S,GARRAGHAN P,STANKOVSKI V,et al. Holistic resource management for sustainable and reliable cloud computing:An innovative solution to global challenge[J]. Journal of Systems and Software,2019,155:104-129.

[18] AHLAWAT C,KRISHNAMURTHI R. Q-learning with function Approximator for clustering based Optimal resource Allocation in fog environment[C]// Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing. 2022:127-135.

[19] JEONG B,BAEK S,PARK S,et al. Stable and efficient resource management using deep neural network on cloud computing[J]. Neurocomputing,2023,521:99-112.

[20] YU B,LI X H,PAN C Y,et al. Edge-cloud collaborative resource allocation algorithm based on deep reinforcement learning [J]. Chinese Journal of Computer Science,2022,49(7):248-253.

[21] GAN D,GE X,LI Q. An optimal transport-based federated reinforcement learning approach for resource allocation in cloud-edge collaborative IoT[J]. IEEE Internet of Things Journal,2023,11(2):2407-2419.

[22] NAWROCKI P,SMENDOWSKI M. FinOps-driven optimization of cloud resource usage for high-performance computing using machine learning[J]. Journal of Computational Science,2024,79:102292.

[23] NEEMA G,KADAN A B,VIJAYAN V P. Multi-objective load balancing in cloud infrastructure through fuzzy based decision making and genetic algorithm based optimization[J]. IAES International Journal of Artificial Intelligence,2023,12(2):678.

[24] YANG Z M,ZUO L L,JI W. Joint optimization method for node deployment and resource allocation based on edge-end collaboration[J]. Chinese Journal of Computer Science,2024,51(S2):665-671.

[25] SHAIK M B,REDDY K S,CHOKKANATHAN K,et al. A Hybrid Particle Swarm Optimization and Simulated Annealing with Load Balancing Mechanism for Resource Allocation in Fog-Cloud Environments [J]. IEEE Access,2024,12:172439-172450.

[26] SENTHIL KUMAR A M,PADMANABAN K,VELMURUGAN A K,et al. A novel resource management framework in a cloud computing environment using hybrid cat swarm BAT (HCSBAT) algorithm[J]. Distributed and Parallel Databases,2023,41(1):53-63.

[27] NARWAL A. Resource Utilization Based on Hybrid WOA-LOA Optimization with Credit Based Resource Aware Load Balancing and Scheduling Algorithm for Cloud Computing[J]. Journal of Grid Computing,2024,22(3):61.

[28] PRECIADO V M,ZARGHAM M,ENYIOHA C,et al. Optimal resource allocation for network protection against spreading processes[J]. IEEE Transactions on Control of Network Systems,2014,1(1):99-108.

[29] WANG M,SONG L. Efficient defense strategy against spam and phishing email:An evolutionary game model[J]. Journal of Information Security and Applications,2021,61:102947.

[30] OGURA M,PRECIADO V M,MASUDA N. Optimal Containment of Epidemics over Temporal Activity-Driven Networks [J]. SIAM Journal on Applied Mathematics,2019:79(3):986-1006.

[31] HAMOUDA E,ELHAFSI M,SON J. Securing Network Resilience:Leveraging Node Centrality for Cyberattack Mitigation and Robustness Enhancement[J]. Information Systems Frontiers,2024,26(1):1-16.

ZHANG Wanyou, born in 1998, postgraduate. His main research interests include big data security and cloud computing security.

SONG Lipeng, born in 1975, Ph.D, professor, Ph.D supervisor. His main research interests include artificial intelligence security and big data security.

(责任编辑:柯颖)