

移动云计算中一种新的跨层信誉机制

于孟洋¹, 林晖¹, 田有亮²

(1. 福建师范大学数学与信息学院, 福建 福州 350117;
2. 贵州省公共大数据重点实验室, 贵州 贵阳 550025)

摘要: 用户在使用各种移动云服务的同时, 面临日益严重的数据泄露和隐私暴露等安全威胁。以移动云计算中的数据安全和隐私保护为研究背景, 将跨层设计与信誉机制相结合, 在节点之间的信誉评估过程中引入MAC(media access control)层和网络层中影响用户信誉的因素, 来识别和管理内部恶意节点。仿真结果表明, 提出的信誉机制能有效地抵御内部诽谤攻击和内部多层攻击, 增强移动终端的可信性, 进而提高移动云服务的数据安全和隐私保护。

关键词: 移动云计算; 安全; 隐私保护; 信誉机制

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018021

New cross-layer reputation mechanism for mobile cloud computing

YU Mengyang¹, LIN Hui¹, TIAN Youliang²

1. College of Mathematics and Information, Fujian Normal University, Fuzhou 350117, China
2. Guizhou Public Big Data Key Laboratory, Guizhou 550025, China

Abstract: Users are facing increasingly serious security threats such as data leakage and privacy exposure while using various mobile cloud services. Based on the data security and privacy protection for mobile cloud computing research background, combining the cross-layer design and credit mechanism, in the node between the introduction of the MAC layer and network layer in the process of credit evaluation of factors affecting user reputation, to identify and manage internal malicious nodes. The credibility of the simulation results show that the proposed mechanism can effectively resist the internal defamation and multilayer attack, enhance the credibility of mobile terminals, thus improve the mobile cloud service data security and privacy protection.

Key words: mobile cloud computing, security, privacy preserving, reputation mechanism

1 引言

移动云计算(MCC, mobile cloud computing)

结合了云计算、移动设备和广布的无线基础设施, 是一种新的计算模式^[1,2]。移动云计算在不同领域广泛应用^[3], 如娱乐、健康、游戏、商业、社交

收稿日期: 2017-12-04; 修回日期: 2018-01-16

通信作者: 林晖, linhui@fjnu.edu.cn

基金项目: 国家自然科学基金资助项目(No.61702103, No.61772008); 福建省引导基金资助项目(No.2016Y0031); 福州市科技局基金资助项目(No.2015-G-54, No.2017-G-79)

Foundation Items: The National Natural Science Foundation of China(No.61702103, No.61772008), Guiding Fund Project of Fujian Province(2016Y0031), Fuzhou Science and Technology Bureau Fund Funding Project(No.2015-G-54, No.2017-G-79)

网络。由于其共享媒介和特殊通信模式的特征,移动云计算容易受到不同的安全和隐私的威胁,尤其是那些由内部恶意节点发起的内部攻击。如今,隐私和安全威胁已经成为移动云计算广泛使用的障碍。然而,现实应用中的移动智能终端、无线网络及第三方移动云服务提供商都无法提供安全有效、可靠的服务和基础支撑,用户在获得丰富的移动云服务的同时,也面临越来越多数据泄露、窃听和隐私暴露等安全威胁^[4,5],尤其是来自内部的诽谤攻击和多层攻击的安全威胁。

作为信任管理的一个关键机制,信誉机制是描述和量化节点行为的一个有效方法。尽管一系列有关信誉机制和基于信誉的信任函数的文献提出,现有的信誉机制是基于特定层调查评估节点的信誉,因此忽略了许多在其他层的信誉关键因素^[6,7]。此外,他们没有考虑隐私保护和用于诽谤好的节点或提高恶意节点信任值的不诚实的推荐。

为了克服上述缺点,本文提出了一种新的跨层信誉机制(NCLRM, new cross-layer reputation mechanism),考虑信誉计算过程中推荐信誉可靠性和隐私保护。这项工作的主要贡献包括以下3个方面。

1) 结合在网络层节点的传递,在MAC层的链路质量和链路冲突概率,跨层的信誉机制可以用来抵御多层攻击、保护隐私,使恶意节点的检测更加有效和准确。

2) 将节点安全相关性的计算方法引入推荐信誉的计算,使推荐的信息和推荐者的可信度更精确。此外,它将进一步加强NCLRM的可靠性和效率,抵御诽谤攻击。

3) 做了大量的仿真实验来检测NCLRM的性能。实验结果表明,在内部诽谤攻击和内部多层攻击的情况下,NCLRM在恶意节点误报率、恶意节点参与率、网络吞吐量方面优于现有机制。

2 相关工作

信誉机制或基于信誉的信任模型在分布式网络的各领域得到广泛研究,用来支持安全、可靠的通信,保证节点间安全协作。

Kim等^[8]在MCC可靠的数据集成、管理与应

用方面,提出了信任管理机制,该机制提出一个方法来量化一个基于移动设备的电话呼叫数据分析的一维信任关系,并且整合了MCC网络用户信任关系。Yan等^[9-11]结合云访问控制与信誉机制,提出了基于信誉的安全访问控制机制。依据访问者的信誉值来控制用户对数据的访问和减少数据访问的风险。Singh等^[12]提出了一个信任评估框架计算在云计算环境下服务提供商的信任。模型考虑3个观点计算最终信任:消费者对服务提供商的自我信任、合作者对服务提供商的信任、第三方对服务提供商的信任。Hammam等^[13]为移动ad-hoc云提出了一个信任管理系统来验证参与者的可靠性。该系统考虑可用性、邻居的评价和反应质量和任务的完整性,通过EigenTrust算法计算节点的信誉信任值。Cao等^[14]针对移动云计算中感知数据的可信性问题,提出了基于信任管理的感知数据和感知用户可信度评估方案,通过设计针对数据或用户的信誉机制或信任管理模型计算数据或用户的信誉值,并通过得到的信誉值判断感知到的数据是否可信。Sicari等^[15]提出一个解决节点的信誉和运行时数据的可信度的架构。该架构是基于混合无线传感器/mesh网络架构,安全验证多点技术的使用提供数据聚合和节点信誉的安全,并允许网络在恶意节点存在的情况下保留聚合数据的可信度。Shen等^[16]提出了一种数据可信度增强的信誉模型,使P2P网络准确地反映节点的信任,并给高服务质量的服务器选择提供指导。模型研究节点信任、信誉和额外的因素之间的关系,并推导出信誉附加因素精确的节点信任度,通过消除附加因素对声誉的影响,真实地反映节点信任。Moati等^[17]提出了一种激励和检测模型,以激励节点在选择过程中的行为。

现有研究成果虽然解决了一些移动云计算安全问题,但仍存在以下不足:1) 基于对单一层次直接观察来评估节点的信誉,忽略了其他层上影响节点信誉度评估的因素;2) 缺少对终端可信性的考虑,很难支持并确保可信移动云数据服务;3) 缺少对用户未来行为的动态预测和有效的用户激励机制,无法动态自适应地调整安全策略,并通过激励用户采取正常行为来减少安全威胁。

3 网络模型和攻击模型

3.1 网络模型

移动云计算作为一种新型计算模式, 结合了云计算、移动设备和无线通信基础设施, 广泛应用于商业、健康和社交网络等领域。图1为移动云计算的总体架构^[10], 包括移动网络、互联网、移动用户、应用服务提供商。在MCC中, 移动用户首先通过基站、无线接入点或其他空中接口连接移动网络来请求云服务。这些请求和移动用户的信息被传送到移动网络的中央处理器, 移动网络运营商可以验证用户的身份、处理数据和提供移动服务。在此之后, 用户的请求通过互联网从移动网络转发到云, 云服务提供商可以为移动用户请求提供相应的云服务。

3.2 攻击模型

移动云计算容易遭受网络外部和内部攻击的威胁, 其中, 内部攻击者由于拥有合法的身份和权限, 外部攻击防御措施不能发挥有效作用, 无法准确区分正常用户和恶意用户; 并且, 合法的身份和权限也使内部攻击者能够轻易获取大量的数据和隐私信息, 导致内部攻击的防御难度和造成的损失都远大于外部攻击。本文主要考虑内部诽谤攻击和内部多层攻击的威胁。

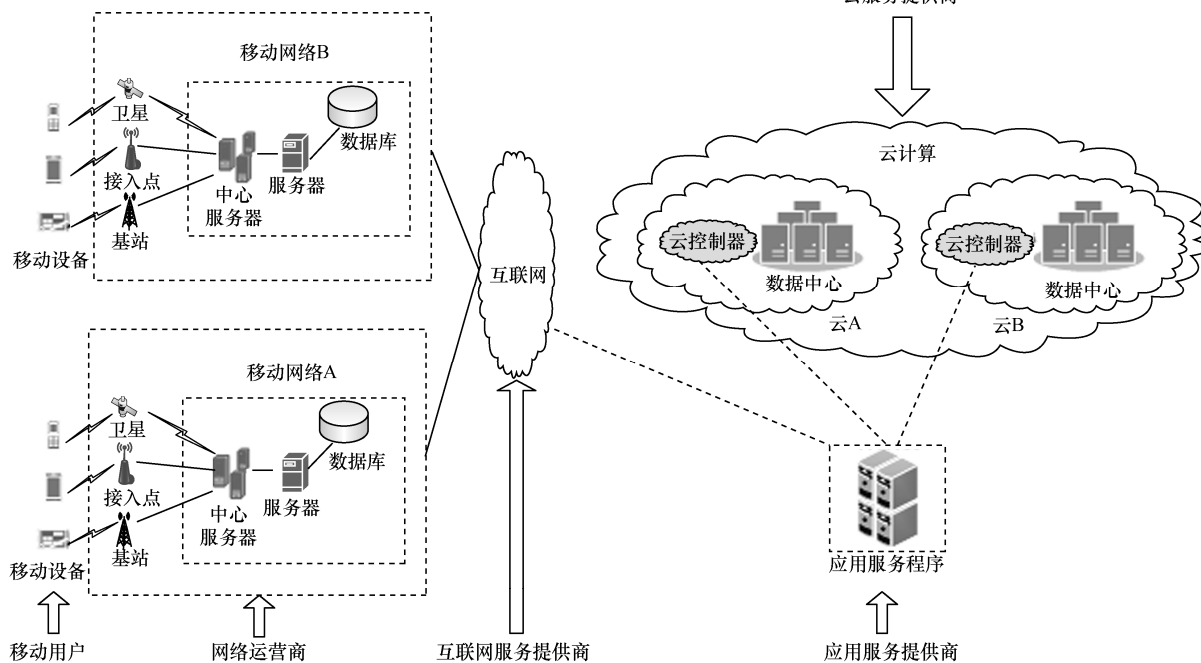


图1 移动云计算架构

4 跨层信誉机制

本文提出一个新的跨层信誉机制 NCLRM。其结构如图2所示, 包括3个部分: 跨层信誉融合中心、信誉数据库和信誉计算模块。信誉计算模块负责不同层的直接信誉计算并存储结果到相应的信誉数据库。然后在跨层信誉融合中心中, 信誉数据库提供直接的信誉到特定层最终声誉融合模块, 用来计算特定层的最终声誉, 还把这个值提供到跨层最终信誉融合模块。最后, 跨层最终信誉融合模块根据不同层次的特定需求, 执行跨层最终信誉融合。

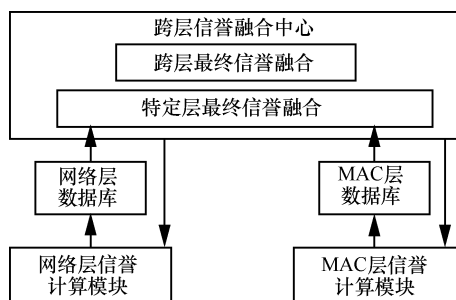


图2 NCLRM 结构

4.1 单层信誉计算

假设 x 和 y 是 2 个邻居节点, x 对 y 的在特定层的最终信誉用 R^{Final} 表示。最终信誉包括 2 个组

成部分,一个是直接信誉 R^{Direct} ,另一个是推荐信誉 R^{Rec} 。直接信誉、推荐信誉和最终信誉在每一层分别计算。此外,最终信誉存储在特定层的最终信誉数据库中,最后提供给跨层信誉融合中心,根据不同层的影响因素执行跨层最终声誉融合。

4.1.1 单层直接信誉的计算

1) MAC 层直接信誉计算

在 MAC 层, x 对 y 的直接信誉 $R_{\text{mac}}^{\text{Direct}}$ 的计算如下。

$$R_{\text{mac}}^{\text{Direct}} = P_{\text{mac}}^{\text{tr}} (1 - P_{\text{mac}}^{\text{col}}) + \alpha_{\text{mac}}^{\text{Direct}} P_{\text{mac}}^{\text{col}} \quad (1)$$

$P_{\text{mac}}^{\text{tr}}$ 是在无线链路 (i, j) 上的成功传输概率, $P_{\text{mac}}^{\text{col}}$ 是在 MAC 层的包舍谋概率, $\alpha_{\text{mac}}^{\text{Direct}}$ 是权重因子,决定了 $P_{\text{mac}}^{\text{col}}$ 对 $R_{\text{mac}}^{\text{Direct}}$ 的影响。 $P_{\text{mac}}^{\text{tr}}$ 的计算如下。

$$\begin{cases} P_{\text{mac}}^{\text{tr}} = (1 - P_{\text{loss}}^{(i,j)})(1 - P_{\text{loss}}^{(j,i)}) \\ P_{\text{loss}}^{(i,j)} = \frac{N_{\text{S,MAC}}^{(i,j)}}{N_{\text{T,MAC}}^{(i,j)}} \\ P_{\text{loss}}^{(j,i)} = \frac{N_{\text{S,MAC}}^{(j,i)}}{N_{\text{T,MAC}}^{(j,i)}} \end{cases} \quad (2)$$

$P_{\text{loss}}^{(i,j)}$ 和 $P_{\text{loss}}^{(j,i)}$ 分别表示无线链路 (i, j) 正向和反向的分组丢失率, $N_{\text{S,MAC}}^{(i,j)}$ 和 $N_{\text{S,MAC}}^{(j,i)}$ 表示在链路 (i,j) 和 (j,i) 已经成功传输的数据分组的数量。 $N_{\text{T,MAC}}^{(i,j)}$ 和 $N_{\text{T,MAC}}^{(j,i)}$ 表示在链路 (i,j) 和 (j,i) 将要传输数据分组的总数。基于其与链路忙碌比率之间的关系 $r_{\text{link-bussy}}$, $P_{\text{mac}}^{\text{col}}$ 计算如下。

$$\begin{cases} r_{\text{link-bussy}} = 1 - \frac{f(P_{\text{mac}}^{\text{col}})\lambda_{\text{idle}}}{f(P_{\text{mac}}^{\text{col}})\lambda_{\text{idle}} + g(P_{\text{mac}}^{\text{col}})\lambda_{\text{suc}} + h(P_{\text{mac}}^{\text{col}})\lambda_{\text{col}}} \\ f(P_{\text{mac}}^{\text{col}}) = (1 - P_{\text{mac}}^{\text{col}})^{\frac{n}{n-1}} \\ g(P_{\text{mac}}^{\text{col}}) = n(1 - P_{\text{mac}}^{\text{col}})[1 - (1 - P_{\text{mac}}^{\text{col}})^{\frac{1}{n-1}}] \\ h(P_{\text{mac}}^{\text{col}}) = 1 + (n-1)(1 - P_{\text{mac}}^{\text{col}})^{\frac{n}{n-1}} - n(1 - P_{\text{mac}}^{\text{col}}) \end{cases} \quad (3)$$

λ_{idle} 、 λ_{suc} 、 λ_{col} 分别表示空闲时长、成功传输时长、碰撞的持续时间。

2) 网络层直接信誉计算模型

x 在网络层对 y 的直接信誉 $R_{\text{network}}^{\text{Direct}}$ 计算如下。

$$R_{\text{network}}^{\text{Direct}} = P_{\text{network}}^{\text{fa}} (1 - P_{\text{network}}^{\text{loss}}) + \alpha_{\text{network}}^{\text{Direct}} P_{\text{network}}^{\text{loss}} \quad (4)$$

$P_{\text{network}}^{\text{fa}}$ 是成功的转发概率, $P_{\text{network}}^{\text{loss}}$ 是节点之间不成功交互的概率,其计算过程如式(5)所示。 $\alpha_{\text{network}}^{\text{Direct}}$ 是权重因子,决定了 $P_{\text{network}}^{\text{loss}}$ 对 $R_{\text{network}}^{\text{Direct}}$ 的影响。

$$\begin{cases} P_{\text{network}}^{\text{fa}} = \frac{N_{\text{network}}^{\text{S}}}{N_{\text{network}}^{\text{T}}} \\ P_{\text{network}}^{\text{loss}} = \frac{I_{\text{F}}}{I_{\text{T}}} \end{cases} \quad (5)$$

$N_{\text{network}}^{\text{S}}$ 是已经成功转发的数据分组数量, $N_{\text{network}}^{\text{T}}$ 是将被转发数据分组的总数, I_{F} 是节点之间失败的交互数量, I_{T} 节点之间交互的总数。

4.1.2 单层推荐信誉计算

本节提出一个推荐信誉计算模型,适用于每个特定层。

在 NCLRM 中,当 x 对 y 的直接信誉计算出来后,被发送到最终的信誉融合模块。然后,根据式(4)的结果,最终声誉融合模块决定是否需要启动推荐信誉查询。

$$R_{\text{mac/net}}^{\text{Final}} = \begin{cases} R_{\text{mac/net}}^{\text{Direct}}, & R_{\text{mac/net}}^{\text{Direct}} > TH_{\text{mac/net}}^{\text{upper}} \\ -1, & R_{\text{mac/net}}^{\text{Direct}} < TH_{\text{mac/net}}^{\text{down}} \\ \text{Query}, & TH_{\text{mac/net}}^{\text{down}} < R_{\text{mac/net}}^{\text{Direct}} < TH_{\text{mac/net}}^{\text{upper}} \end{cases} \quad (6)$$

$TH_{\text{mac/net}}^{\text{down}}$ 和 $TH_{\text{mac/net}}^{\text{upper}}$ ($0 < TH_{\text{mac/net}}^{\text{down}} < TH_{\text{mac/net}}^{\text{upper}} < 1$) 是 $R_{\text{mac/net}}^{\text{Direct}}$ 的下限和上限,当满足条件 $R_{\text{mac/net}}^{\text{Direct}} > TH_{\text{mac/net}}^{\text{upper}}$ 时,则认为该节点不需要进行推荐信誉查询,此时单层的最终信誉 $R_{\text{mac/net}}^{\text{Final}} = R_{\text{mac/net}}^{\text{Direct}}$,其中 $R_{\text{mac/net}}^{\text{Direct}}$ 为 4.1.1 节计算出的单层的直接信誉值,而结果为 Query 则表示要进行推荐查询。

如果需要, x 将向 y 的邻居节点发送查询请求查询 y 的信誉。假设 x 收到 n 个节点($n > 1$)推荐的信誉,设 $\text{REC} = \{N_i | i = 1, \dots, n\}$ 为初始推荐节点集合。推荐信誉计算的详细过程描述如下。

1) 假设只有 2 个推荐者 k 和 k' ,而且它们的推荐意见相互冲突。如果满足式(7),则认为 k 比 k' 更值得信任,令 $R_{\text{mac/net}}^{\text{Rec}} = R_k^{\text{Direct}}$ 。

$$\begin{cases} \theta_{(k,x)} > \theta_{(k',x)} \\ \theta_{(k,x)} = \theta_{(k',x)} \wedge R_k^{\text{Direct}} > R_{k'}^{\text{Direct}} \end{cases} \quad (7)$$

2) 假设有 2 个以上的推荐者,推荐的信誉 $R_{\text{mac/net}}^{\text{Rec}}$ 计算如下。

$$R_{\text{mac/net}}^{\text{Rec}} = \frac{1}{m} \sum_{j=1}^m (\theta_{(j,x)} R_{j,\text{mac/net}}^{\text{Direct}}) \quad (8)$$

4.1.3 计算单层最终信誉

在得到特定层直接和推荐的信誉时，在时间 t_i 特定层的最终信誉计算如下。

$$\begin{cases} R_{t_i, \text{mac/net}}^{\text{Final}} = \varphi_1 R_{t_i, \text{mac/net}}^{\text{Direct}} + \varphi_2 R_{t_i, \text{mac/net}}^{\text{Rec}} \\ \varphi_1 + \varphi_2 = 1 \end{cases} \quad (9)$$

4.1.4 节点信誉更新

单层最终信誉被计算后，在特定层节点 r_i 的最终信誉将会按照式(10)进行更新，并存储于节点 x 。

$$R_{t_i, \text{mac/net}}^{\text{Final}} = \begin{cases} R_{t_i, \text{mac/net}}^{\text{Final}} + 0.1, R_{t_i, \text{mac/net}}^{\text{Direct}} - R_{t_i, \text{mac/net}}^{\text{Final}} \in [-0.5, 0.5] \\ R_{t_i, \text{mac/net}}^{\text{Final}} - 0.1, R_{t_i, \text{mac/net}}^{\text{Direct}} - R_{t_i, \text{mac/net}}^{\text{Final}} > 0.8 \\ R_{t_i, \text{mac/net}}^{\text{Final}} + 0.1, R_{t_i, \text{mac/net}}^{\text{Direct}} - R_{t_i, \text{mac/net}}^{\text{Final}} < -0.8 \end{cases} \quad (10)$$

4.2 跨层最终信誉计算

在 NCLRM 中，当一个特定的层想做一个跨层信誉计算时，它将其需求传递给跨层最终信誉融合模块。然后跨层最终信誉融合模块会查询特定层的最终信誉数据库，执行如式(11)的跨层最终信誉融合。

$$\begin{cases} R^{\text{Final}} = \alpha_1 R_{\text{mac}}^{\text{final}} + \alpha_2 R_{\text{network}}^{\text{final}} \\ \alpha_1 + \alpha_2 = 1, \alpha_1, \alpha_2 \in [0, 1] \end{cases} \quad (11)$$

其中， α_1 、 α_2 分别为 MAC 层和网络层最终信誉值的权重因子。

5 仿真和性能分析

5.1 仿真环境

本文使用 Matlab 对设计的 NCLRM 机制进行仿真实验和性能分析。仿真中选择了以下 3 种指标比较和分析 NCLRM 机制与 ETSCG (evolutionary trust scheme of certificate game) [18] 机制和 SELRM (self-management of reputation mechanism) [19] 机制的性能。仿真实验中，考虑 2 种攻击场景：内部诽谤攻击场景；内部多层攻击场景。

1) 恶意节点误报率 (MFPR, malicious node false present rate): 错误的恶意节点报告占有所有恶意节点报告的比值。

2) 恶意节点参与率 (MPR, malicious node participation rate): 未被识别成功成为转发节点的恶意节点数量与恶意节点总数的比值。

3) 网络吞吐量 (NT, network throughput): 源节点产生的数据分组被成功传输到目的节点的比率。

5.2 信誉机制性能分析

5.2.1 恶意节点误报率

首先，比较 3 种机制的恶意节点误报率。仿真结果如图 3 所示，从图中结果可以发现，随着恶意节点比例的增加，3 种信誉机制的恶意节点误报率也随之增加，但是，本文提出的 NCLRM 机制的恶意节点误报率的增加幅度是最小的。

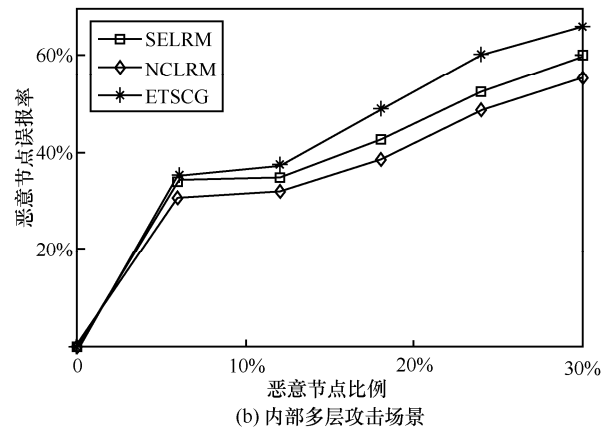
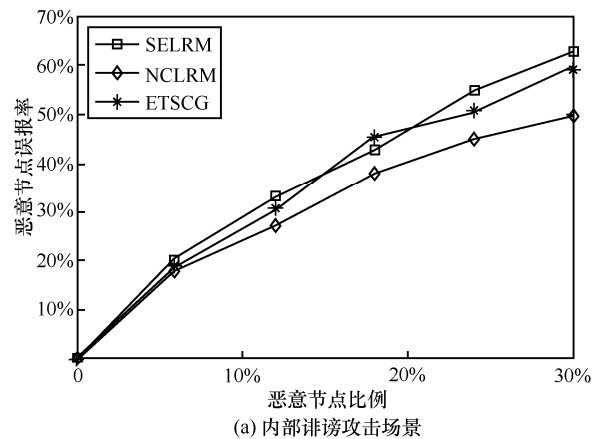


图3 不同场景下的恶意节点误报率

在图 3(a)所示的内部诽谤攻击仿真场景中，本文提出的 NCLRM 机制采用分布式的方法，综合考虑了时间和位置对信誉值评估的影响，提高了用户信誉值评估的动态性和自适应性，进而提高了信誉值评估的准确性；同时，NCLRM 将 MAC 层和网络层中影响用户信誉的因素引入节点之间的信誉评估过程，使信誉值的计算更加准确。与 NCLRM 相比，SELRM 中自主管理机制主要考虑自我感知、策略决策、目标导向、执行这 4 个步骤。而上述 4 个步骤在实际的应用中容易受到网

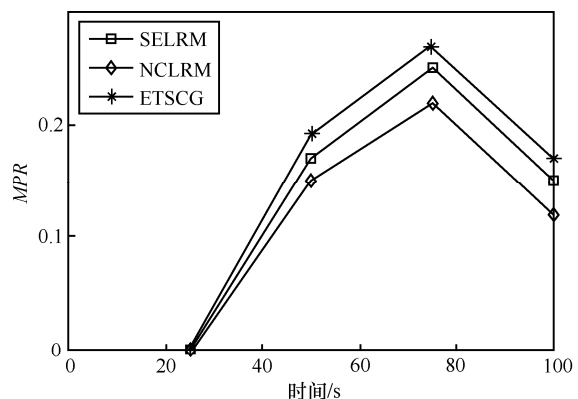
络通信质量、地理位置环境以及用户习惯的影响,在检测的过程中容易导致误报。另外,SELRM 采用自律计算的思想为云计算分布式环境下信誉管理提供思路,以期实现信誉中心的自我管理、自优化等自律特性,然而,如何分辨对数据质量真实性的判断是否准确是一个困难的问题,因此无法有效抵御内部诽谤攻击,从而导致误报。同时,ETSCG 采用的基于证书博弈的进化信任机制主要考虑将虚拟身份验证协调器、身份验证代理和移动用户之间的交互作为一个三阶段博弈,每个玩家的目标都是最大化自己的效用,而信任分配则是通过 G 值学习实现的,存在信誉值更新和获取的延迟问题,无法及时准确地提供最新的用户信誉值,也无法保证传输过程中的数据安全;此外,ETSCG 主要依靠系统保存的服务性能记录和用户的反馈来评估用户和云服务提供者的信誉值,没有提供用户激励机制和反馈可信度的评估,上述这些缺点都使 ETSCG 无法有效抵御内部诽谤攻击,造成误报率的增加。因此,NCLRM 机制的恶意节点误报率的增加幅度是最小的。

在图 3(b)所示的内部多层攻击仿真场景中,由于 ETSCG 中缺乏相应的多层攻击预防机制,因此无法抵御多层攻击,导致在多层攻击场景中,其恶意节点误报率是最高的。SELRM 采用自律计算的思想,虽然可以在一定程度上抵御多层攻击,然而其信誉值评估过程中缺乏准确性、信誉值更新不及时和传输过程中无法抵御篡改攻击等特点,使其多层攻击抵御的有效性低,无法有效快速地识别出恶意节点,从而导致恶意节点误报率增加。与上述 2 种机制相比,NCLRM 专门针对跨层攻击设计了一种跨层信誉机制,以解决移动过程中的信誉损失问题,该机制将 MAC 层和网络层中的影响用户信誉的因素引入节点之间的信誉评估过程,抵御多层攻击。此外,NCLRM 还设计了基于推荐路径的推荐信誉值评估方法,实现了用户的信誉值的动态评估和更新,有效提高了用户信誉值评估结果的准确性和实时性,进而实现有效抵御多层攻击。因此,NCLRM 机制的恶意节点误报率的增加幅度是最小的。

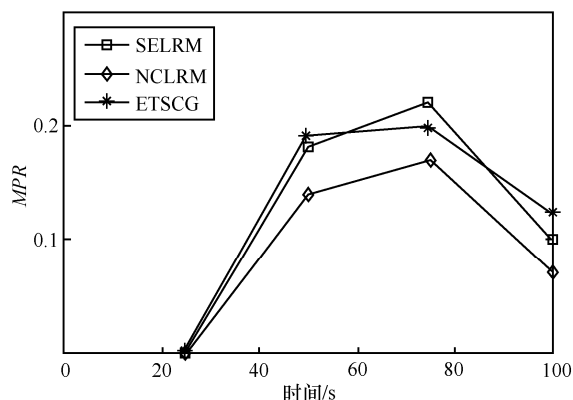
5.2.2 恶意节点参与率

本小节比较了 3 种机制的恶意节点参与率。从图 4 中可以看出,随着仿真实验时间的增长,3 种机制的 MPR 也随之增加,其中,NCLRM 的 MPR

增加得最慢。在仿真的初始阶段,由于缺少对用户行为的积累和信誉值评估的准确性较低,3 种机制的 MIR 都开始上升。随着仿真时间的增加,3 种机制中都积累了一定量的用户行为,对用户信誉值评估的准确性也大大提高了,因此 3 种机制的 MIR 开始下降。



(a) 内部诽谤攻击场景



(b) 内部多层攻击场景

图4 不同场景下的恶意节点参与率

其中,在内部诽谤攻击场景下(如图 4(a)所示),SELRM 和 ETSCG 都提供了用户信誉值评估方法和激励策略,因此都能够识别部分的恶意节点。SELRM 机制的用户信誉值评估方法在准确性和有效性方面优于 ETSCG,因此其 MPR 低于 ETSCG。但是,SELRM 在用户信誉值评估过程中还存在延迟和无法保证传输过程中的数据安全的不足,并且没有提供用户激励机制和反馈可信度的评估。本文提出的 NCLRM 机制在用户信誉值评估过程中的动态性和自适应性,以及采用跨层的信誉计算模式,有效地克服了 SELRM 和 ETSCG 的不足,因此,NCLRM 的 MPR 要低于 SELRM 和 ETSCG。

在多层攻击的场景下(如图 4(b)所示),ETSCG 缺乏相应的多层攻击预防机制,其信誉值评估机制

的有效性和及时性都存在不足,因此它的MPR最高。对于SELRM,由于它的用户信誉度评估结果是集中存放在云端的,因此当用户在同一个云所覆盖范围内运动时,其行为和信誉值评估结果仍旧可以被查询到,因此,相比缺乏相应的移动攻击预防机制的ETSCG来说,在移动攻击场景下,SELRM的MPR要低于ETSCG。但是,由于SELRM中并没有考虑不同云之间的交互,因此,当用户在不同云之间运动时,其行为和信誉值评估结果将不能被传递和查询。而NCLRM采用了分布式的方法,能够有效地解决上述的问题,使用户的信誉值可以快速转移到新的互动区,抵御多层攻击。并且,DRTR在用户信誉值评估结果的准确性和实时性方面大大优于SELRM和ETSCG,因此NCLRM的MPR要低于SELRM和ETSCG。

5.2.3 网络吞吐量

最后,比较3种机制的网络吞吐量。3种机制比较结果如图5所示。从图中结果可以发现,网络吞吐量和时间成正比。然而,不论是在诽谤攻击场景还是在移动攻击场景下,由于时间的增加,3种机制收到的虚假信息越来越多,能够

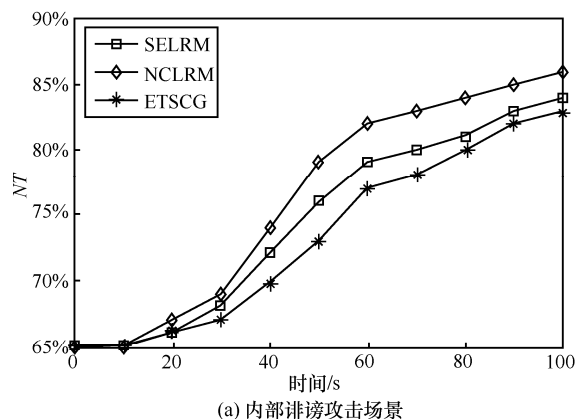
用于准确评估用户信誉度的可靠信息越来越少,3种机制都需要协作节点花费更多的时间建立可靠路径和收集可靠信息。其中,相比SELRM和ETSCG,NCLRM机制设计了有效的推荐信誉评估机制,在评估的过程中动态地建立推荐者集合和推荐路径集合,使NCLRM机制具有一定的网络容错性和生存性,这些都有效地减少了重新建立可靠推荐路径和查找可靠推荐者所花费的时间,从而提高了网络吞吐量,因此,NCLRM机制的网络吞吐量都比SELRM和ETSCG的要高。

6 结束语

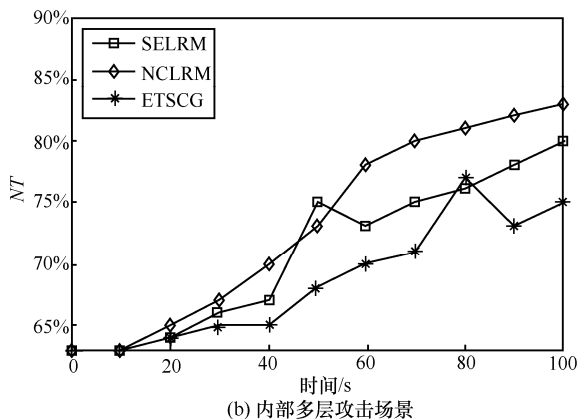
针对移动云计算中面临的数据和隐私安全威胁,尤其是来自内部攻击安全威胁,提出了一种新的跨层信誉机制NCLRM。NCLRM将跨层设计与信誉机制相结合,将MAC层和网络层中的影响用户信誉的因素引入节点之间的信誉评估过程,来识别和管理内部恶意节点,对抗内部多层攻击、诽谤攻击,提供通信过程的安全和隐私保护。仿真结果和性能分析表明,NCLRM在恶意节点误报率、恶意节点参与率、网络吞吐量方面优于现有的ETSCG机制和SELRM机制。

参考文献:

- [1] ZISSIS D, LEKKAS D. Addressing cloud computing security issues[J]. Future Generation Computer Systems, 2012, 28(3): 583-592.
- [2] KHAN A N, KIAH M L M, KHAN S U, et al. Towards secure mobile cloud computing: a survey[J]. Future Generation Computer Systems, 2013, 29(5):1278-1299.
- [3] HUANG D, ZHOU Z, XU L, et al. Secure data processing framework for mobile cloud computing[C]//Computer Communications Workshops. 2011: 614-618.
- [4] LU K, WANG J, XIE L, et al. An eigentrust-based hybrid trust model in P2P file sharing networks [J]. Procedia Computer Science, 2016, 94:366-371.
- [5] FERNANDO N, LOKE S W, RAHAYU W. Mobile cloud computing: a survey[J]. Future Generation Computer Systems, 2013, 29(1): 84-106.
- [6] SEN J. Security and privacy issues in wireless mesh networks: a survey[M]//Wireless Networks and Security. Berlin:Springer, 2013: 189-272.
- [7] WANG H, WU S, CHEN M, et al. Security protection between users and the mobile media cloud[J]. IEEE Communications Magazine, 2014, 52(3):73-79.
- [8] KIM M, SANG O P. Trust management on user behavioral patterns for a mobile cloud computing[J]. Cluster Computing, 2013, 16(4): 725-731.



(a) 内部诽谤攻击场景



(b) 内部多层攻击场景

图5 网络吞吐量

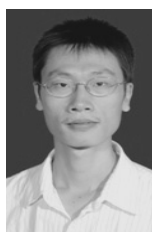
- [9] YAN Z, LI X, KANTOLA R. Controlling cloud data access based on reputation[J]. Mobile Networks & Applications, 2015, 20(6): 828-839.
- [10] YAN Z, LI X, KANTOLA R. Heterogeneous data access control based on trust and reputation in mobile cloud computing[M]//Advances in Mobile Cloud Computing and Big Data in the 5G Era. Berlin: Springer International Publishing, 2017.
- [11] YAN Z, LI X, WANG M, et al. flexible data access control based on trust and reputation in cloud computing[C]//IEEE Transactions on Cloud Computing. 2017.
- [12] SINGH S, CHAND D. Trust evaluation in cloud based on friends and third party's recommendations[C]// Engineering and Computational Sciences. 2014:1-6.
- [13] HAMMAM A, SENBEL S. A trust management system for ad-hoc mobile clouds[C]//The International Conference on Computer Engineering & Systems. 2014:31-38.
- [14] CAO Q H, KHAN I, FARAHBAKHSH R, et al. A trust model for data sharing in smart cities[C]//IEEE International Conference on Communications (ICC2016). 2016: 1-7.
- [15] SICARI S, COEN A. DARE: evaluating data accuracy using node reputation[J]. Computer Networks, 2013, 57(15):3098-3111.
- [16] SHEN H, LIN Y, LI Z. Refining reputation to truly select high-QoS servers in peer-to-peer networks[C]//IEEE Transactions on Parallel and Distributed Systems. 2013: 2439-2450.
- [17] MOATI N, OTROK H, MOURAD A, et al. Reputation-based cooperative detection model of selfish nodes in cluster-based QoS-OLSR protocol[J]. Wireless Personal Communications, 2014, 75(3): 1747-1768.
- [18] LI D, LI M, LIU J. Evolutionary trust scheme of certificate game in mobile cloud computing[J]. Soft Computing, 2017:1-11.
- [19] 吴庆涛, 张旭龙, 张明川, 等. 一种面向云服务的自主信誉管理机制[J]. 武汉大学学报(理学版), 2013, 59(5): 425-430.

WU Q T, ZHANG X L, ZHANG M C, et al. An independent reputation management mechanism for cloud service [J]. Journal of Wuhan University (Science Edition), 2013, 59(5):425-430.

[作者简介]



于孟洋 (1992-), 男, 河南郑州人, 福建师范大学硕士生, 主要研究方向为信息安全。



林晖 (1977-), 男, 福建福州人, 博士, 福建师范大学副教授、硕士生导师, 主要研究方向为信任管理、无线网络信息安全、移动云计算。



田有亮 (1982-), 男, 贵州盘县人, 博士, 贵州大学教授、博士生导师, 主要研究方向为算法博弈论、密码学与安全协议。