移动云计算中基于动态博弈和可靠推荐的传递信誉机制

林晖[1]，于孟洋[1]，田有亮[2]，黄毅杰[1]
（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（贵州大学），贵州 贵阳 550025）

摘 要：移动互联网和云计算的蓬勃发展，涌现出了大量基于移动云平台的服务。用户在使用移动云服务的同时，也将大量用户数据和隐私信息存放在云端，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，针对内部诽谤攻击和移动攻击，首先提出基于动态博弈的推荐激励策略；然后结合该策略，建立可靠推荐信誉评估模型；最后，提出一种新的基于动态博弈和可靠推荐的传递信誉机制。仿真结果表明，所提传递信誉机制能有效地抵御内部诽谤攻击和移动攻击，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；数据安全；隐私保护；动态博弈；信誉机制
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018079

Dynamic game and reliable recommendation based transferring reputation mechanism for mobile cloud computing

LIN Hui[1], YU Mengyang[1], TIAN Youliang[2], HUANG Yijie[1]
1. College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China
2. Guizhou Provincial Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China

Abstract: The booming development of the mobile internet and cloud computing leads to the emerging of many mobile cloud platforms based services. However, since mobile users store lots of data and privacy information in the cloud when they are using the mobile cloud services, they are facing multiple increasingly serious security threats such as data leaks and privacy exposures. The data security and privacy protection was investigated in mobile cloud computing, aiming at the internal bad mouthing attacks and mobile attacks. A dynamic game and reliable recommendation based transferring reputation mechanism was proposed. First, a dynamic game based recommendation incentive mechanism was proposed. Secondly, a reliable recommendation reputation evaluation model was established based on the incentive mechanism. Last, a novel transferring reputation mechanism was proposed that combined the above mentioned incentive mechanism and reputation evaluation model. Simulation results demonstrate the proposed transferring reputation mechanism can defend against the internal bad mouthing attacks and mobile attacks effectively, enhance the credibility of mobile terminals and improve the data security and privacy protection of mobile cloud services.

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

收稿日期：2017-11-08；**修回日期**：2018-02-01
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), Pilot Project of Fujian Province (No.2016Y0031), Project of Fuzhou Science and Technology Bureau (No.2015-G-54, No.2017-G-79)

1 引言

移动云计算（MCC, mobile cloud computing）作为移动学习和云计算的结合体，是一种通过移动互联网络，以移动智能终端为信息接入口，利用云计算技术对移动终端提供所需服务的新型计算模式[1,2]。移动云计算的蓬勃发展，涌现出了大量基于移动云服务，同时也导致越来越多的数据信息和用户隐私出现在网络中[3,4]，面临着越来越多数据泄露、窃听和隐私暴露等安全威胁[5,6]。

数据安全和隐私保护作为移动云计算安全研究中的2个重要内容，受到了广泛的关注，国内外很多学者和机构已经对此进行了大量的研究。但从移动云服务的实际安全需求出发，结合移动云计算的特点，针对内部攻击和移动攻击的数据安全和隐私保护的研究目前还比较少，无法满足移动云计算及其服务的整体发展水平的要求。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远大于外部攻击。与此同时，移动终端的移动性和易受攻击的特点也使通过俘获移动终端来发起移动攻击成为可能，并且难以预防。

综上所述，移动云计算的数据安全和隐私保护问题已经成为阻碍移动云计算及其服务发展的重要障碍，搭建可信的移动云计算平台，确保其能够提供安全可靠的服务和基础支撑，实现可信的信息采集、安全的数据访问和传输，以及提供数据信息的隐私保障尤为重要，是移动云计算安全进一步发展必须要解决的重要挑战。

移动云计算中的数据安全和隐私保护与信任管理和终端用户及无线网络节点的信誉度评估密切相关[7]。终端用户及无线网络节点的信誉度和相互间信任关系的评估能够有效准确地描述节点及用户的行为，了解行为随着时间的演变情况，有效识别出节点的恶意行为和判断出节点未来可能的行为，进而提高移动云数据在采集、传输、存储及访问过程中的安全性和隐私保障。

基于上述分析，本文采用信誉机制和博弈论，提出了一种新的基于动态博弈和可靠推荐的传递信誉机制。本文贡献主要包括以下几点。

1) 提出了一种移动感知的传递信誉机制，解决了移动过程中的信誉丢失问题。该机制使用户或节点的信誉值能够随用户或节点转移到新的互动区，有效抵御了移动攻击。

2) 提出了基于动态博弈的推荐激励策略，使攻击者的攻击收益低于攻击成本，降低了理性攻击者的攻击意愿，实现对内部诽谤攻击的防御。

3) 本文进行了大量的仿真实验来证明所提传递信誉机制的性能。结果表明所提传递信誉机制可以有效抵御内部诽谤攻击和移动攻击，增强移动云计算中的数据安全和隐私保护。

2 相关工作

近些年来，基于移动云计算的社交活动和数据访问越来越频繁，信任管理作为有效评估移动云计算环境下用户行为的关键技术，开始被重视并应用于移动云计算的安全。

Singh 等[7]针对云计算环境下服务提供商的信任问题，提出了一个信任评估模型，通过考虑3个方面的因素来计算最终信任：消费者对服务提供者的自我信任，合作者对服务提供者的信任和第三方对服务提供者的信任。Yan 等[8~10]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。Lin 等[11]提出了一种基于信任管理和机制设计的可信访问控制机制，将新提出的自适应信誉模型，分布式多级安全策略及分级密钥管理协议与移动云计算中的访问控制有机结合起来，从而实现数据的安全访问。Cao 等[12]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来计算数据或用户的信誉值，并通过得到的信誉值来判断感知到的数据是否可信。Lin 等[13]提出了一种将数据分类、情景感知、安全相关性评估等技术有机结合的信誉机制，实现了对内部攻击的有效抵御，增强移动云计算中感知数据的有效性和可信性。Lin 等[14]针对移动云计算中的隐私保护问题，结合信任管理和跨层设计，提出了一种基于可靠推荐和隐私保护的跨层信誉机制，在提高信誉值评估准确性的同时也保障了移动云用户的隐私安全。Kim 等[15]针对移动云计算数据集成，管理与应用方面，提出了相关的信任管理机制。该机制首先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；然后，对整个移动云计算用户间的信任关系进行整合，建立全网的信任关系。Hammam 等[16]针对移动 ad hoc 网络设计了一个信任管理系统，来验证参与者的可靠性。该系统充分考虑网络可用性、邻居节点的评价和反应质量及任务的完整性，通过 EigenTrust 算法计算节点的全局信誉值。最后依据节点的信誉值来识别恶意用户，保障网络的安全。张会兵等[17]针对基于云平台的物联网搜索，将信誉评估机制引入到数据交互过程中，提出了融合主客观要素的动态信誉计算机制。Rajendran 等[18]提出了一种用于评估云服务提供者的可信度的混合模型。该模型采用集中式的机制，将用户和服务提供者的信誉评估结果集中存放在云端的信任管理代理处，并且依靠系统保存的服务性能记录和用户的反馈来评估云服务提供者的可信度。

现有研究成果虽然解决了一些移动云计算安全问题，但仍旧存在以下不足：1) 缺少对内部攻击和移动攻击的考虑；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。针对上述不足，本文有机结合信誉机制和博弈论，提出了一种新的基于动态博弈和可靠推荐的传递信誉机制，通过对用户或节点信誉度的评估来动态识别内部恶意用户、增强移动云服务和数据访问用户或节点的可信度、抵御内部攻击和移动攻击，进而提高移动云计算中的数据安全和隐私保护。

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。与此同时，无线 mesh 网络（WMN, wireless mesh network）作为低成本和高效的解决方案来提供高速的网络接入已被接受和广泛部署。因此，构建基于无线 mesh 网络的移动云计算（WM-MCC, wireless mesh-mobile cloud computing），将是实现移动云计算快速大规模应用的一种可行方案。基于上述分析，本文的研究背景定位于基于无线 mesh 网络的移动云计算 WM-MCC，其架构[2]如图 1 所示，在 WM-MCC 中移动终端与基站（BTS, base transceiver station）连接，通过 mesh 路由器访问 mesh 骨干网；mesh 路由器互相连接，通过网关及有线和无线网络访问移动云平台和移动云服务。

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，传统的外部攻击防御措施不能发挥有效作用，导致内部攻击的防御难度和造成的损失都远远大于外部攻击。与此同时，移动终端的移动性和易受攻击的特点也使移动攻击成为可能，并且难以预防[19]。本文主要考虑内部诽谤攻击和移动攻击的威胁。

4　基于动态博弈和可靠推荐的传递信誉机制

4.1　基于动态博弈的推荐激励策略

本文将动态博弈理论[20]中的委托—代理理论引入信誉机制中的信誉值推荐过程，提出一种新的基于动态博弈的推荐激励策略（DGRI, dynamic game based recommend incentive strategy）。DGRI 中将请求协作的实体作为委托人，将提供协作的交互实体作为代理人。假设交互实体间将经过多轮的博弈。并且，委托人发送协作请求时，代理人的回复为诚实回复和虚假回复 2 种，本文用 Sack={诚实回复(h)，虚假回复(f)} 来表示。在 DGRI 中，如果交

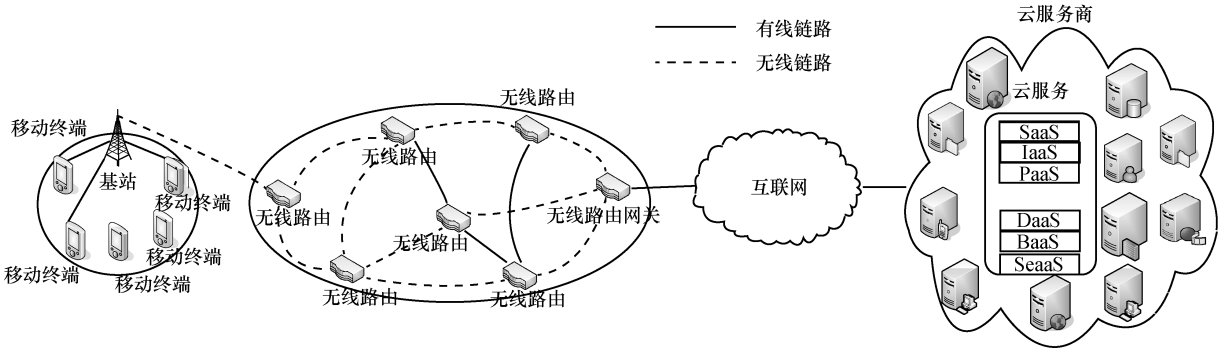


图 1　基于 mesh 网络的移动云计算 WM-MCC 架构

互实体虚假回复，其信誉值会减少，若信誉值低于某个门限值，其他交互实体将不会再与它合作。

当交互实体提供真实回复时，其收益为U_{a}，计算如下

$$U_{\mathrm{a}}=2AP_{\mathrm{d}}R \tag{1}$$

其中，A 为请求协作的实体给协作的交互实体初始的奖励，R 为根据传递的间接信誉值和请求者本地数据库中的直接信誉值计算得到的综合信誉值，R 越大，则实体参与交互的积极性越大；P_{d} 是协作检测率，即正确判断实体存在的概率，P_{d} 计算如下

$$P_{\mathrm{d}}=\frac{N_{\mathrm{s}}}{N_{\mathrm{all}}} \tag{2}$$

其中，N_{s} 和 N_{all} 分别为检测实体存在的正确的次数和总次数，N_{s} 和 N_{all} 存放在本地数据库中。

本文假设所有参与交互的实体都是理性的。在交互过程中，如果提供协作的任意实体 u 给出诚实报告，而任意实体 u' 自己提供虚假回复，这时 u' 的收益为 $3A$，u 收益为–A；如果双方都采用诚实的回复，双方的收益都为 $2A$，如果双方都给出虚假回复，双方的收益都为 0。例如，假设 u_1 和 u_2 进行了 i 次交互，u_1 的收益情况具体分析如下 u_2 和 u_1 的收益计算相同，限于篇幅，本文就只介绍 u_1 的收益。

情况 1 交互实体间都选择相互提供真实回复，则总收益 U_x 为

$$U_x=2A+\left(\sum_{i=2}^{\infty}U_{\mathrm{a}}\right)R=2A+2A\left[\frac{R}{(1-P_{\mathrm{d}}R)}\right] \tag{3}$$

情况 2 若第一次进行虚假回复，后面再进行诚实回复，则总收益 U_y 为

$$U_y=3A-AR+\sum_{i=3}^{\infty}0=3A-AR \tag{4}$$

情况 3 交互用户间一直给虚假回复，从开始就一直给虚假回复，从第一次可能合作后，从第二次开始所有交互实体都不会再对他提供诚实协作，则总收益 U_z 为

$$U_z=3A+\sum_{i=2}^{\infty}0=3A \tag{5}$$

情况 4 先给出诚实回复，下次给出虚假回复，则总收益 U_π 为

$$U_\pi=2A+3AR+\sum_{i=3}^{\infty}0=2A+3AR \tag{6}$$

假设进行了多次博弈时，首先，比较情况 1 和情况 2，当 $U_x>U_y$ 时，即 $2A+2A\frac{R}{1-P_{\mathrm{d}}R}>3A-AR$，且 $0\leqslant R\leqslant 1$，可计算得到在 $R\geqslant\frac{3+P_{\mathrm{d}}-\sqrt{(3+P_{\mathrm{d}})^2-4P_{\mathrm{d}}}}{2P_{\mathrm{d}}}$ 且随 P_{d} 单调递增的，因为 $0\leqslant P_{\mathrm{d}}\leqslant 1$，进一步得到 $R\geqslant 2-\sqrt{3}$。所以当 $R\geqslant 2-\sqrt{3}$，真实回复的策略的总收益是大于情况 2 中的欺骗策略总收益，即 $R\geqslant 2-\sqrt{3}$ 时，选择诚实回复就是占优策略，否则，交互实体会采用虚假回复。

接着，比较情况 1 和情况 3，如果考虑诚实回复未来的收益大于虚假回复的，即 $U_x-U_z\geqslant 0$，可得 $R\geqslant\frac{1}{2+P_{\mathrm{d}}}$，$P_{\mathrm{d}}\geqslant 0$，即 $R\geqslant\frac{1}{2}$。那么考虑双方以后会再进行协作，当 $R\geqslant\frac{1}{2}$ 时采用真实回复是占优策略，否则交互实体会采用虚假回复。

然后，比较情况 1 和情况 4，当 $U_x>U_\pi$ 时，可得 $R>\frac{1}{3P_{\mathrm{d}}}$，且 $0\leqslant P_{\mathrm{d}}\leqslant 1$，即 $R>\frac{1}{3}$。所以，当 $R>\frac{1}{3}$ 时，采用诚实回复是占优策略，否则交互实体会采用虚假回复。

综上分析，考虑长远的收益，所有交互实体都是希望能得到信任，当 $R\geqslant\frac{1}{2}$ 时，相互提供真实回复为纳什均衡。

4.2 传递信誉机制

本节将 DGRI 中得到的纳什均衡结果与推荐信誉评价结合，构建了一种可靠推荐信誉评估模型，并在此基础上，提出了新的基于动态博弈和可靠推荐的传递信誉机制（DRTR, dynamic game and reliable recommendation based transferring reputation mechanism）。

DRTR 包括 3 个部分：直接信誉评估、可靠推荐信誉评估和最终信誉评估。本文假设任意实体 x 和 y 分别表示请求者和服务提供者，x 对 y 的直接信誉评估结果、可靠推荐信誉评估结果和最终信誉评估结果分别用 R^{Direct}、R^{Rec} 和 R^{Final} 表示。最终信誉评估结果将存储在实体的本地数据库中。所有的

实体上都将自动运行 4.1 节中所述的 DGRI 策略。

4.2.1 直接信誉评估

x 对 y 的直接信誉度的评估取决于历史的相互作用和网络信息的动态实时传递，T_n 时刻 x 对 y 的直接信誉度 $R_{T_n}^{\text{Direct}}$ 为

$$R_{T_n}^{\text{Direct}} = \left(\frac{IA_s}{IA_{\text{total}}} \right) \varphi_{T_n} (1 - \varphi_{\text{location}}) \tag{7}$$

其中，IA_s 和 IA_{total} 分别表示实体成功的交互次数和总交互次数。φ_{T_n} 为权重因子，表示截止 T_n 时刻的交互频率对直接信誉评估的影响，计算如下

$$\varphi_{T_n} = \left[1 - \mathrm{e}^{\frac{-NIA_{T_n}}{mn}} \right] \sum_{l=1}^{n} \left(\frac{NIA_l}{m} \cdot \frac{l}{n} \right) \tag{8}$$

其中，m 是一个时间周期内的时间段数，n 是时间周期数。NIA_{T_n} 是 x 和 y 的发生交互的周期数。NIA_l 是在第 l 次周期内的交互数。$\varphi_{\text{location}}$ 表示 x 和 y 之间的实时位置变化对 T_n 时刻直接信誉度评估的影响，计算如下

$$\varphi_{\text{location}} = \mathrm{e}^{-E_{\text{location}} \beta_{\text{location}}} (1 - \mathrm{e}^{-|L - L'| \beta_{\text{location}}}) \tag{9}$$

其中，实时位置和最近的位置分别表示为 L 和 L'，定义 $|L-L'|$ 表示它们的距离。定义 E_{location} 为位置传感误差，β_{location} 为控制位置因子权重对信誉影响的参数。

直接信誉评估算法描述如下。

请求者 y 向 x 发送一个请求消息。

1) 任意实体 x 收到请求消息后，将首先使用式(10)验证请求者 y 的安全级别，如果 y 的安全等级满足要求，则利用式(7)进行直接信誉度评估，反之忽略该请求消息。

$$SL_y = \left\lfloor 5 \left(\frac{1}{n} \sum_{i=1}^{n} R_{T_i}^{\text{Final}} \right) \right\rfloor + 1 \tag{10}$$

其中，$R_{T_i}^{\text{Final}}$ 为在 T_i 时刻计算获得的 y 的最终信誉值。

2) x 将得到的直接信誉度与预设定的门限值上下限 $TH_{\text{direct}}^{\text{upper}}$、$TH_{\text{direct}}^{\text{down}}$ 比较：如果 $(R_{T_n}^{\text{Direct}} > TH_{\text{direct}}^{\text{upper}})$，则最终信誉值 $R_{T_n}^{\text{Final}} = R_{T_n}^{\text{Direct}}$；如果 $(TH_{\text{direct}}^{\text{down}} < R_{T_n}^{\text{Direct}} < TH_{\text{direct}}^{\text{upper}})$，执行本文可靠推荐信誉评估过程和最终信誉评估过程。

4.2.2 可靠推荐信誉评估

如果直接信誉评估不能得出结论，x 将执行基于 DGRI 策略的可靠推荐信誉评估模型，向邻居实体查询 y 的信誉值，并将收到的推荐信誉值进行综合，得出 y 的推荐信誉评估结果。

推荐信誉查询算法描述如下。

1) x 广播查询消息。

2) 任意邻居实体 k 接收到查询消息，k 先执行推荐激励策略和判断 x 的安全性，若 x 的安全级别大于安全等级要求，则进入步骤 3)，反之，k 将忽略这个查询消息。

3) 若 k 有关于 y 的直接信誉值和安全级别信息，则 k 将本地保存的直接信誉值作为直接推荐信誉值反馈给 x；若没有，k 则要向它的邻居实体查询 y 的直接信誉和安全级别信息，并提供基于推荐路径的推荐信誉值。

4) k 评估出综合推荐信誉值，并反馈给 x。

基于 DGRI 策略的可靠推荐信誉评估模型构建过程如下。

假设 x 收到 $n(n>1)$ 个直接推荐信誉值，m $(m>1)$ 个基于推荐路径的推荐信誉值，则 x 按照以下计算式进行 T_n 时刻的综合推荐信誉 $R_{T_n}^{\text{Rec}}$ 计算。

$$\begin{cases} R_{T_n}^{\text{Rec}} = \eta_1 R_{T_n}^{\text{Dir-Rec}} + \eta_2 R_{T_n}^{\text{Path-Rec}} \\ \eta_1 + \eta_2 = 1, \eta_1, \eta_2 \in [0,1] \end{cases} \tag{11}$$

其中，η_1 和 η_2 为权重因子，分别决定了 T_n 时刻的直接推荐信誉值 $R_{T_n}^{\text{Dir-Rec}}$ 和基于传递路径的推荐信誉值 $R_{T_n}^{\text{Path-Rec}}$ 对最终推荐信誉评估的影响。

定义直接推荐者集合为 $DirR = \{dir - rec_i | i = 1, \cdots, n\}$，直接推荐信誉值 $R_{T_n}^{\text{Dir-Rec}}$ 计算如下

$$R_{T_n}^{\text{Dir-Rec}} = \frac{1}{n} \sum_{j=1, j \in DirR}^{n} \left(\frac{sl_j}{sl_{\max}} R_{j:y}^{\text{Direct}} \right) \tag{12}$$

其中，sl_j 和 $sl_{\max}$ 分别为实体 j 的安全等级和最大安全等级。$R_{j:y}^{\text{Direct}}$ 是 j 提供的关于 y 的直接推荐信誉值。

假设 $L_{(i)}, (i = 1, \cdots, n)$ 为推荐路径集合，每条路径包括 j 个交互实体。本文将根据以下的规则选择出最可靠的路径 $\overline{R_{\text{path}}}$。

$$\overline{R_{\text{path}}} = \text{Max}(\zeta_1 R_{L(i)} + \zeta_2 SL_{L(i)}), i = 1, \cdots, n$$

s.t.

$$\begin{aligned} &\zeta_1 + \zeta_2 = 1 \\ &Th_1 < E_{L(i)} < Th_2 \end{aligned} \tag{13}$$

其中，ζ_1 和 ζ_2 分别是对应于路径 $L_{(i)}$ 的信誉值和安全级别的权重因子。Th_1 和 Th_2 是 $E_{L(i)}$ 的阈值。$R_{L(i)}$

和 $SL_{L(i)}$ 分别是路径 $L_{(i)}$ 的信誉值和安全级别。$E_{L(i)}$ 是路径 $L_{(i)}$ 的能量消耗。$R_{L(i)}$、$SL_{L(i)}$ 和 $E_{L(i)}$ 计算如下

$$\begin{cases} R_{L(i)} = \mathrm{Min}\left(\sum_{j=1}^{m} \dfrac{R_j^i}{m}, \min(R_j^i) \right) \\ SL_{L(i)} = \mathrm{Min}(SL_j^i) \\ E_{L(i)} = m \cdot \mathrm{Max}\left(\sum_{j=1}^{m} \dfrac{E_j^i}{m}, \max(E_j^i) \right) \end{cases} \tag{14}$$

R_j^i 和 SL_j^i 分别是第 i 条路径上的第 j 个实体的信誉值和安全等级。E_j^i 是第 i 条路径上的第 j 个实体的的能量消耗。

定义传递推荐者集合为 $\mathrm{PathR} = \{path - rec_j \mid j = 1, \cdots, m\}$，推荐信誉值 $R_{T_n}^{\text{Path-Rec}}$ 计算如下

$$R_{T_n}^{\text{Path-Rec}} = \frac{1}{m} \sum_{k=1, k \in \text{PathR}}^{m} \left[\overline{R_{\text{path}}} R_{k:y}^{\text{Direct}} (1 - \varphi_{x:k,\text{location}}) \right] \tag{15}$$

其中，$\varphi_{x:k,\text{location}} \in [0,1]$ 是 x 和推荐实体 k 之间的位置移动影响因子，可以通过式(9)计算获得。$R_{k:y}^{\text{Direct}}$ 是 k 提供的关于 y 的直接推荐信誉值。

综合推荐信誉计算算法描述如下。

1) x 接收到 n 条直接推荐信息，m 条传递推荐信息的回复消息后，执行步骤 2) 所示的推荐者选择过程。

2) 对于给出回复的 $n+m$ 个推荐者，x 将逐个对其安全性进行检测，若推荐者的安全等级大于安全级别要求，则执行步骤 3)，反之，x 忽略这个回复消息。

3) x 对推荐者进行分类，将推荐者归入推荐者集合 $DirR$ 或推荐者集合 $PathR$。

4) x 计算出 $R_{T_n}^{\text{Dir-Rec}}$，$\overline{R_{\text{path}}}$ 和 $R_{T_n}^{\text{Path-Rec}}$。

5) x 计算综合推荐信誉值 $R_{T_n}^{\text{Rec}}$ 并返回结果。

4.2.3 最终信誉评价

获得直接和推荐的信誉评估结果后，y 的最终信誉值 $R_{T_n}^{Final}$ 计算式为

$$\begin{cases} R_{T_n}^{Final} = \alpha_1 R_{T_n}^{Direc} + \alpha_2 R_{T_n}^{Rec} \\ \alpha_1 + \alpha_2 = 1, \alpha_1, \alpha_2 \in [0,1] \end{cases} \tag{16}$$

其中，α_1 和 α_2 分别为直接信誉值和综合推荐信誉值的权重因子。

5 仿真实验与性能分析

5.1 仿真环境

本文使用 Matlab 对设计的 DRTR 机制进行仿真实验和性能分析。仿真中选择了以下 4 种指标来比较、分析 DRTR 机制、ADAER[17]机制和 TRECS[18]机制的性能。仿真实验中，考虑 2 种攻击场景：内部诽谤攻击场景和移动攻击场景。

1) 恶意节点误报率（FPR, false report rate）：错误的恶意节点报告占所有恶意节点报告的比率。

2) 恶意节点识别率（MIR, malicious identification rate）：路由维护和数据转发过程中被识别出的恶意节点占恶意节点总数的比率。

3) 收敛时间（CT, convergence time）：节点完成对恶意节点的识别和管理所要花费的时间。

4) 推荐效率（RE, recommendation efficiency）：提供可靠推荐者的比率。

5.2 信誉机制性能分析

5.2.1 恶意节点误报率

3 种机制的恶意节点误报率（FPR）的比较结果如图 2 所示。可以看出，随着恶意节点比例的增加，3 种信誉机制的 *FPR* 也随之增加，但是，本文所提 DRTR 机制的 *FPR* 的增加幅度最小。

在图 2(a)所示的内部诽谤攻击仿真场景中，由于 DRTR 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，DRTR 采用了基于动态博弈的激励策略，依据用户的反馈结果的正确与否对用户进行奖励和惩罚，实现有效激励用户提供可靠的信息。与 DRTR 相比，ADAER 中对用户信誉值的评估主要考虑：基于长时间连续检测的数据完整性、时间的衰减、数据提供者是否愿意提供持续性的响应行为这 3 个因素。而上述因素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，导致误报。另外，ADAER 采用的激励策略依据协作用户提供的数据质量真实性信息来支付报酬和激励用户，然而，如何判断数据质量真实性的判断的准确性是一个困难的问题，因此，无法有效抵御内部诽谤攻击，从而导致误报。TRECS 采用集中式的方法来计算和存储用户和服务提供者的信誉值，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，TRECS 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，没有提供激励机制和反馈可信度的评估，上述这些缺点都使 TRECS 无法有效抵御内部诽谤攻击，造成误报率的增加。因此，DRTR 的 *FPR* 增加幅度最小。

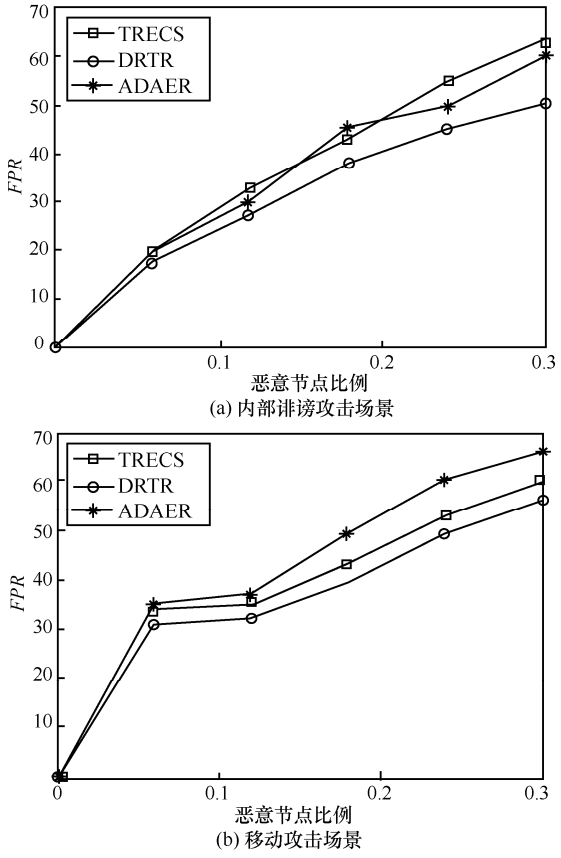


图 2　恶意节点误报率 *FPR*

在图 2(b)所示的移动攻击仿真场景中，ADAER 缺乏相应的移动攻击预防机制，无法抵御移动攻击，导致其 *FPR* 最高。TRECS 采用的集中式的方式，虽然可以在一定程度上抵御移动攻击，但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都使其移动攻击抵御的有效性低下，无法有效快速地识别出恶意节点，导致 *FPR* 的增加。与上述 2 种机制相比，DRTR 专门针对移动攻击设计了一种位置感知的移动信誉机制，以解决移动过程中的信誉损失问题，该机制使用户的信誉值可以快速转移到新的互动区，抵御移动攻击。此外，DRTR 还设计了基于动态博弈的推荐激励策略和基于推荐路径的推荐信誉值评估方法，实现了用户在移动过程中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，进而实现有效抵御移动攻击。因此，DRTR 的 *FPR* 增加幅度最小。

5.2.2　恶意节点识别率

比较 3 种机制的恶意节点识别率 MIR。从图 3 中可以看出随着仿真实验时间的增长，3 种机制的 *MIR* 也随之增加，其中，DRTR 的 *MIR* 增加最快。在初始阶段，由于缺少对用户行为的积累和信誉值评估的准确性较低，因此 3 种机制的 *MIR* 都较低。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，对用户信誉值的评估的准确性也大大提高了，因此，3 种机制的 *MIR* 开始上升。

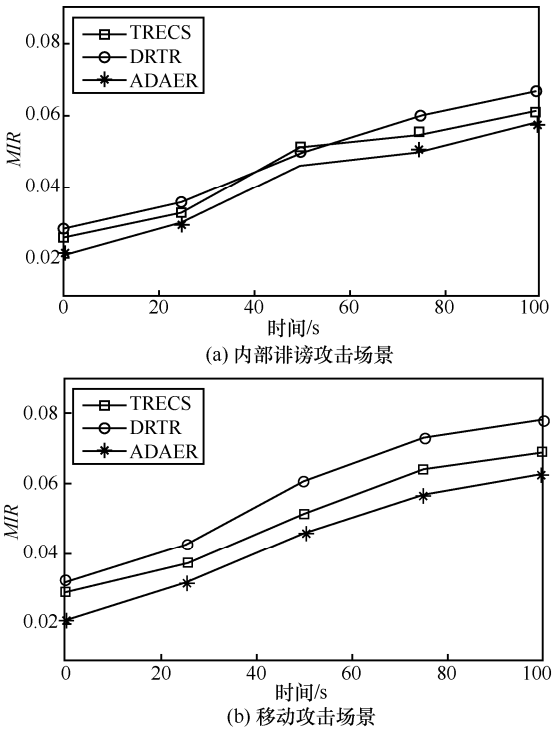


图 3　恶意节点识别率 *MIR*

在图 3(a)所示内部诽谤攻击场景下，ADAER 和 TRECS 中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。TRECS 机制的用户信誉值评估方法在准确性和有效性方面优于 ADAER，因此，其 MIR 高于 ADAER。但是，TRECS 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。本文所提 DRTR 机制在用户信誉值评估过程中的动态性和自适应性，以及采用的基于动态博弈模型的激励机

制，有效克服了 ADAER 和 TRECS 的不足，因此，DRTR 的 *MIR* 要高于 TRECS 和 ADAER。

在图 3(b)所示移动攻击的场景下，ADAER 缺乏相应的移动攻击预防机制，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 *MIR* 最低。对于 TRECS，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 ADAER 来说，在移动攻击场景下，TRECS 的 *MIR* 要高于 ADAER。但是，由于 TRECS 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 DRTR 采用了分布式的方法，能够有效地解决上述问题，使用户的信誉值可以快速转移到新的互动区，抵御移动攻击，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 TRECS 和 ADAER，因此，DRTR 的 *MIR* 要高于 TRECS 和 ADAER。

5.2.3 收敛时间

比较 3 种机制的收敛时间（CT）。3 种机制的 *CT* 比较结果如图 4 所示。从图 4 中结果可以发现，*CT* 和恶意节点的比例成正比，恶意节点的比例越高、*CT* 越长。然而，无论是在诽谤攻击场景还是在移动攻击场景下，由于恶意节点的增加，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去建立可靠路径和收集可靠信息，导致了恶意节点的比例越高 *CT* 越长。其中，相比 ADAER 机制和 TRECS 机制，DRTR 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 DRTR 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 *CT*，因此，DRTR 的 *CT* 都比 ADAER 和 TRECS 的短。

5.2.4 推荐效率

比较 3 种机制的推荐效率（RE）。从图 5 的结果可以发现，不论是在诽谤攻击场景还是在移动攻击场景下，DRTR 的 *RE* 保持一个较平稳的状态，受到仿真时间的影响较小。而 ADAER 和 TRECS 的 *RE* 低于 DRTR，并随着时间的增加不断降低。由于 DRTR 中同时考虑了诽谤攻击和移动攻击，所设计

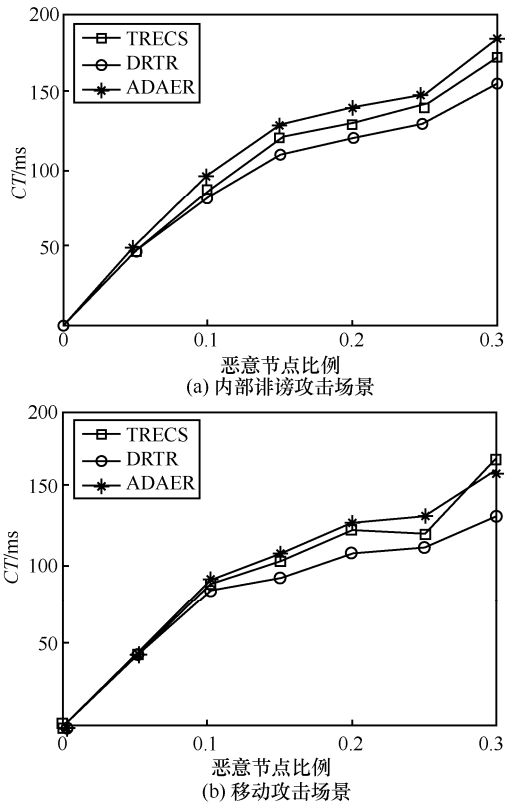


图 4 收敛时间 *CT*

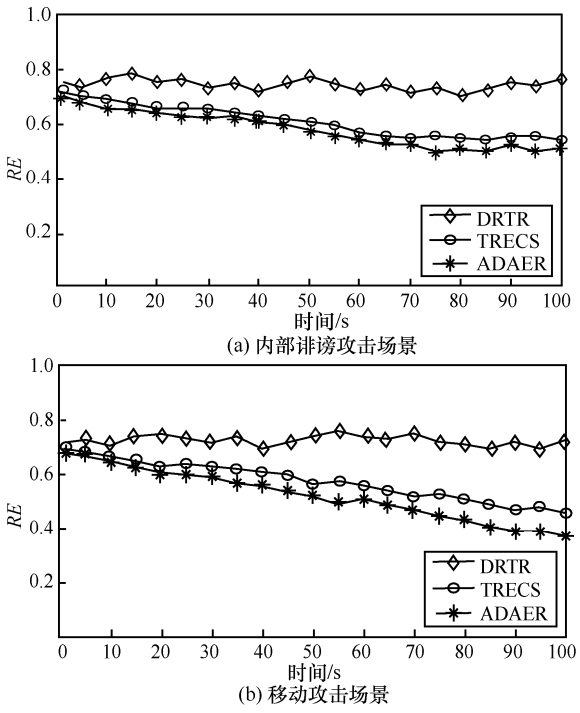


图 5 推荐效率 *RE*

的机制能够有效抵御这 2 种攻击，因此，其 *RE* 性能相对稳定。相比 DRTR 机制，ADAER 和 TRECS 中都缺少提供可靠推荐的方法，因此，它们的 *RE*

性能比 DRTR 差，并且随着时间的增加，不可靠推荐信息扩散的越来越广泛，因此，ADAER 和 TRECSRE 性能随时间的增长而不断下降。

6　结束语

针对移动云计算中面临的数据和隐私安全威胁，尤其是来自内部诽谤攻击和移动攻击的安全威胁，本文有机结合博弈论、位置感知及信誉机制等理论方法，提出了一种新的基于动态博弈和可靠推荐的传递信誉机制 DRTR。DRTR 机制中针对传统信誉机制中无法传递用户信誉值的问题，设计了可靠推荐信誉评估模型；同时，为了激励用户提供可靠的信息，提出了基于动态博弈的推荐激励策略。仿真实验表明，DRTR 机制在恶意节点误报率、恶意节点识别率、收敛时间和推荐效率这 4 个方面的性能都优于现有的 ADAER 机制和 TRECS 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, MAT KIAH M L, KHAN S U, et al. Towards secure mobile cloud computing: a survey[J]. Future Generation Computer Systems, 2013, 29 (5):1278-1299.

[3] FERNANDO N, LOKE S W, RAHAYU W. Mobile cloud computing: a survey[J]. Future Generation Computer Systems, 2013, 29 (1): 84-106.

[4] SHEN H, LIN Y, LI Z. Refining reputation to truly select high-QoS servers in peer-to-peer networks[J]. IEEE Transactions on Parallel Distribute System, 2013, 24: 2439-2450.

[5] LUA K, WANGA J L, XIEA L, et al. An eigentrust-based hybrid trust model in P2P file sharing networks[J]. Procedia Computer Science, 2016, 94:366-371.

[6] 刘浩, 陈志刚, 张连明. 基于社区的移动社交网络安全路由算法设计与实现[J]. 信息网络安全, 2017 (7): 25-31.
LIU H, CHEN Z G, ZHANG L M. A secure routing algorithm of mobile social network based on community[J]. Netinfor Security, 2017, 7: 25-31.

[7] SINGH S, CHAND D. Trust evaluation in cloud based on friends and third party's recommendations[C]//IEEE Engineering and Computational Sciences. 2014:1-6.

[8] YAN Z, LI X, KANTOLA R. Controlling cloud data access based on reputation[J]. Mobile Networks and Applications, 2015, 20(6) : 828-839.

[9] 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, Springer International Publishing, 2017: 65-113.

[10] YAN Z, LI X, WANG M, et al. Flexible data access control based on trust and reputation in cloud computing[J]. IEEE Transactions on Cloud Computing, 2017, 99:1-12.

[11] LIN H, XU L, HUANG X Y, et al. A trustworthy access control model for mobile cloud computing based on reputation and mechanism design[J]. Ad Hoc Networks,2015, 35(C):51-64.

[12] 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.

[13] LIN H, HU J, TIAN Y L, et al. Toward better data veracity in mobile cloud computing: a context-aware and incentive-based reputation mechanism[J]. Information Sciences, 2017, 387:238-253.

[14] LIN H, XU L, MU Y, et al. A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing[J]. Future Generation Computer Systems, 2015, 52:125-136.

[15] KIM M, PARK S O. Trust management on user behavioral patterns for a mobile cloud computing[J]. Cluster Comput, 2013, 16:725-731.

[16] HAMMAM A, SENBEl S. A trust management system for ad hoc mobile clouds[C]//2013 8th International Conference on Computer Engineering & Systems. 2013:31-38.

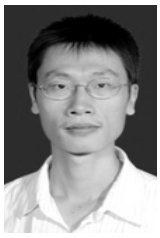
[17] 张会兵, 李超, 胡晓丽, 等. 物联网搜索中主客观融合的动态信誉评估[J]. 通信学报, 2015, 36(12): 106-113.
ZHANG H B, LI C, HU X L, et al. Fusing subjective and objective factors: a dynamic approach to evaluating reputation for IoT search[J]. Journal on Communications, 2015, 36(12): 106-113.

[18] RAJENDRAN V V, SWAMYNATHAN S. Hybrid model for dynamic evaluation of trust in cloud services[J]. Wireless Networks, 2016, 22(6): 1807-1818.

[19] ZHANG J, ZHANG Z, GUO H. Towards secure data distribution systems in mobile cloud computing[J]. IEEE Transactions on Mobile Computing, 2017, 99:1-12.

[20] VASAL D, SUBRAMANIAN V, ANASTASOPOULOS A. A systematic process for evaluating structured perfect Bayesian equilibria in dynamic games with asymmetric information[J]. American Control Conference, 2016:3378-3385.

[作者简介]



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、移动云计算等。

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。

田有亮（1982-），男，贵州六盘水人，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、大数据安全与隐私保护、区块链与电子货币等。

黄毅杰（1990-），男，福建龙海人，福建师范大学硕士生，主要研究方向为无线网络信息安全。