MP2P网下一种基于代理的安全反馈信任模型

曹晓梅[1,3] 朱海涛[1,3] 沈何阳[1,3] 陈贵海[2]
(南京邮电大学计算机与软件学院 南京 210003)[1] (南京大学计算机科学与技术系 南京 210093)[2]
(江苏省无线传感网高技术研究重点实验室 南京 210003)[3]

摘 要 信任问题是移动对等网(Mobile P2P,MP2P)安全中的关键性问题。针对MP2P网与传统P2P网终端设备在编址、通信方式和标识上的差异性以及网络中可能存在的冒名、恶意诋毁、合谋以及"搭便车"等安全问题,提出一种MP2P网下基于代理的安全反馈信任模型(PSTM)。不同类别的代理服务器接入不同类型的终端,以屏蔽网络层终端设备之间的差异性。同时,代理服务器之间对信息的相互备份能够缓解服务器"单点失效"问题。在资源安全选择协议中对反馈方进行身份、资格的认证后进行相似性筛选并加权处理。在多粒度的信任值计算中引入全局节点贡献度和评价可信度,并将直接信任度分为面向节点的与面向资源的来激励移动节点真实地反馈信息。实验表明,PSTM能够减少诋毁以及合谋恶意行为,同时能够抑制"搭便车"行为,从而增加网络善意节点的交易成功率。

关键词 结构化MP2P网,信任模型,代理服务器,安全反馈,相似度加权
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.042

Proxy-based Security-feedback Trust Model in MP2P Network

CAO Xiao-mei[1,3] ZHU Hai-tao[1,3] SHEN He-yang[1,3] CHEN Gui-hai[2]
(College of Computing and Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China)[2]
(Key Laboratory of High-tech Wireless Sensor Network in Jiangsu Province, Nanjing 210003, China)[3]

Abstract Trust problem is the key issue for Mobile P2P (MP2P) network security. In MP2P network, terminal devices' addressing mode, communication mode and identifiers are different to traditional P2P network. Some security issues such as: allusion attack, malicious slander and collusion, "free ride" phenomenon, are even more serious compared to traditional P2P network. Aiming at these above issues, a Proxy-based Security-Feedback Trust Model (PSTM) was proposed in this paper. Different types of terminal devices access to different proxy servers to shield the discrepancy between different terminal equipments on MP2P device access network layer. Meanwhile, proxy servers can reduce the problem of single point failure with the method of related information's backup and recovery. Certificate Feedback Rater's identification and qualification through security resource-selection protocol, then integrate trust information according to similarity of terminal and resource types with weighted method. Furthermore, set global contribution value and evaluation value in multi-granularity trust computation to motivate mobile peers' honest feedbacks. Divide mobile peer's direct trust value into peer-oriented and resource-oriented values to make trust feedbacks more authentic. Simulation experiments show that PSTM can reduce malicious slander and collusion effectively. It also can restrain selfish peers' free ride behaviors and increase successful cooperation rate of high-contributed peers in MP2P network.

Keywords Structured mobile P2P network, Trust model, Proxy server, Security feedback, Weighted by similarity

1 引言

P2P技术的核心思想是利用分布式存储和计算能力来替代集中式处理方式。随着移动网络的不断发展和演进以及移动终端处理能力的不断增强,MP2P网络日趋成熟,并延伸至移动互联网中。信任管理是对传统安全机制的有效补充,是解决MP2P网络中安全问题的有效途径。由于传统的安全手段无法解决MP2P应用中匿名实体之间合作所面临的信任和激励问题,因此节点之间形成信任机制,创造一个透明有序的交易环境显得尤为重要。

目前,已有大量国内外学者对P2P网络的信任问题进行广泛研究,然而其中MP2P信任问题的研究尚处于起步阶

到稿日期:2013-09-01 返修日期:2014-01-04 本文受国家重点基础研究发展项目(973计划)(2011CB302903),国家自然科学基金项目(60873231,61202353),江苏高校优势学科建设工程项目(yx002001)资助。

曹晓梅(1974—),女,博士,副教授,主要研究方向为无线网络安全;朱海涛(1988—),男,硕士生,主要研究方向为无线网络的信任模型,E-mail:zhtstart@qq.com(通信作者);沈何阳(1989—),女,硕士生,主要研究方向为传感器网络数据融合;陈贵海(1963—),男,博士,教授,主要研究方向为无线传感器网络并行计算以及网络安全。

段。文献[1]为处理大量反馈信息而提出 M-trust 方法来对信任数据进行加权融合。为了减少存储开销，每个节点仅仅保留周围节点的综合信任值和评价可信度值于 t_list 表中，同时用 TTL 来及时更新列表，避免了节点频繁退出而造成的信息冗余。然而，文中认为信任值高的节点提供的反馈信息都是可信的，这一假设本身是有误的，不能抵御信任值高节点对其他节点的诋毁行为；同时，t_list 表中信息只能反映主观的局部节点间信任关系，缺乏全局统筹。文献[2]为了更快地聚合可信的信任参考值而提出了基于稳定群组的方法，即将具有相似兴趣或者相似路由方向移动的节点组成群组。文章中通过节点的信号强度判别可信节点成员是否在群组中，并通过这些可信节点获得相对稳定可靠的信任值。然而作者没有考虑到节点在移动过程中信号的强弱会不断变化以及节点的频繁加入和退出，这使得群组内节点并不能实时有效地获取到信任反馈信息。文献[3]提出了一种适合 MP2P 网络环境的动态安全信任模型 DSTM-MP2P。该模型针对节点的信任信息已知的情况，提出基于节点行为的节点类型识别机制；针对节点的信任信息未知的情况，提出基于贝叶斯博弈的节点概率选择策略，然而前一种情况对节点类型的识别过于确定化，没有考虑到节点行为上下文对交易产生的动态变化过程以及信任本身的模糊性以及不确定性。文献[4]提出一种多粒度的信任模型 MGT，该模型的优点是：综合考虑到节点在各个方面的信任值，将时间因子和终端相似度纳入信任值的计算。然而文中对节点评价可信度的更新较为简单并且资源选择协议安全性不高；节点在接收反馈信息时尽管可以通过数字签名识别出冒名节点，但仍易受到其他可信节点虚假反馈信息的干扰。

文献[5,6]分别针对普适环境提出了基于向量机制的信任模型和域间动态开放环境下的信任管理模型 PTM。文献[5]的贡献在于综合考虑了来自信任因子、历史因子、时间因子对信任值的影响，使提出的模型具有较好的动态适应能力。然而由于推荐值的计算只相信邻居节点，计算出来的信任度并不能代表全局性。另外，文中假设的高信任度的推荐者不会提供不可靠的推荐信任本身也是有误的。文献[6]中提出的 PTM 主要采用改进的证据理论进行建模，其主要优点有：很好地体现了信任度随着时间和行为上下文的变化而增减的动态性；没有复杂的迭代计算，适合普适环境下能源节约的应用需求，具有较好的计算收敛性和可扩展性。然而该模型的间接信任度评估通过算术平均获得，没有考虑到推荐信任者本身的差异性。

鉴于上述问题，本文提出一种 MP2P 网下基于代理的安全反馈信任模型 PSTM（Proxy-based Security-Feedback Trust Model）。不同类别代理服务器接入不同类型的移动终端，移动节点加入网络时需要通过本地代理服务器注册或者验证身份，加入网络后只需从代理服务器处查询、获取以及上传信息。前趋与后继代理服务器之间的备份可以缓解“单点失效”问题。代理服务器利用密码学手段通过安全资源选择协议不仅对反馈方身份进行验证，而且对其是否拥有评价的资格进行验证。验证通过后根据评价信息的相似程度对其进行筛选，以减小诋毁、合谋恶意行为对节点信任值的影响。移动节点退出网络时，本地代理服务器将会把该节点提供下载的次数、参与反馈的数目、在线时长、上传文件的数量及大小等参数纳入该节点全局贡献度的计算当中。同时，在多粒度信任值计算方面引入全局评价可信度的概念，将直接信任度分为面向节点与面向资源的，以激励节点真实地反馈对交易资源的信任评价。仿真结果表明，PSTM 能够有效地抵御诋毁以及合谋恶意行为对节点信任值的影响，同时能够抑制节点“搭便车”行为，促进善意节点的交易成功率。

2 基于代理的安全反馈信任模型

信任模型是指建立和管理信任关系的框架，它定义了信任关系的量化表示方法、操作、信任传播途径和计算方法[7]。下面将从设备接入网逻辑框架、移动节点加入与退出网络、移动节点间安全资源选择协议和多粒度的信任值计算这 4 个方面介绍基于代理的安全反馈信任模型。

2.1 设备接入网框架

传统 MP2P 系统结构主要由蜂窝自组网、无线接入网与核心网 3 部分组成[8]。由于 MP2P 网移动终端编址、通信方式以及标识不同，为了屏蔽网络层终端设备之间的差异性，本文在蜂窝自组网的基础上加入一层由代理服务器组成的设备接入网。

代理服务器模拟完全二叉树的结构在设备接入网中的生成。顶层代理服务器（Top Proxy 以下简称 TP）经过运营商的授权负责叶子服务器 ID 的分配、IP 的划分、授权和移动节点黑名单的认证等服务。根服务器扩展出两个左右子服务器，根服务器是左子代理服务器的二叉树前趋结点，而左子服务器是右子服务器的二叉树前趋结点。后继服务器加入网络后，前趋服务器需定期发送备份文件 *Ind*、*Fri* 表（详见下文）给后继服务器。当单个服务器失效时，由于无法周期性发送更新信息给左后继服务器，因此两服务器将反馈此服务器失效给它的树根服务器，树根服务器将重新授权。每棵二叉树所代理的移动终端类型相同（如图 1 所示），相同层不同接入类型的代理服务器之间形成分布式哈希链表（DHT）。此时的终端接入层网络形成纵向为树形分布，横向为 DHT 分布的网络框架。图 1 即为 MP2P 设备接入层的网络逻辑框架图。

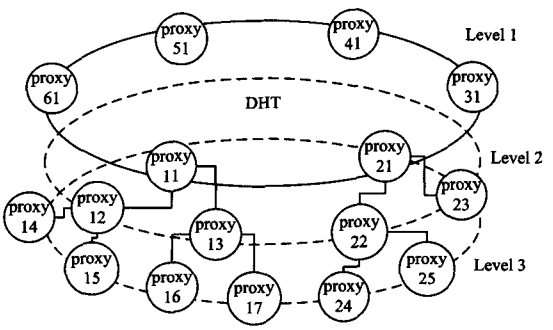


图 1 设备接入层逻辑框架

代理服务器保存资源索引表 *Ind*、信息统计表 *Sta*、注册节点表 *Fri*。*Ind*=(*ID*,*Res*,*type*,*Size*)，*Ind*(*Index*)记录的是处于同一层的代理服务器保存的资源目录情况。*ID* 表示移动节点在 MP2P 网络中唯一的 *ID* 号，*Res* 表示资源名称，*type* 表示资源类型，*Size* 表示资源大小。*Sta*=(*ID*,*IP*,*RFNum*,*TFNum*,*EFNum*,*list*,*oltim*)，*Sta*(*Statistics*)记录的是当前代理服务器所辖移动节点的信息情况。*IP* 表示节点的 *IP* 地址，*RFNum* 表示可提供下载资源的次数，*TFNum* 表示反馈资源信任值的次数，*EFNum* 为反馈节点可信度的次数。节点在本地服务器上传的文件目录记为 *list*，*list*=(*Res*,

$type, Size)$，$oltim$ 为所辖节点在本地服务器的在线时长。$Fri=(ID, Co, Ev, IP, IMEI, e, d)$，$Fri(First)$记录的是在该代理服务器注册的节点信息情况。$Co$ 为注册节点的全局贡献值，Ev 为注册节点的全局评价可信度，IP 表示注册节点当前的 IP 地址，e 为注册节点的公钥，d 为注册节点的私钥。

移动节点存储资源交易表 Det，$Det=(PID, Res, Rtype, Size, Time, Dc, Cr, Tr', Fe, e_p)$。其中 PID 表示资源提供方的 ID，$Time$ 表示交易完成的当前时刻，Dc 为对该资源的直接信任度，Tr'为对资源提供方的直接信任度，Cr 为对资源提供方的间接信任度。Fe 表示该节点收到的其他节点发过来的信任反馈信息，e_p 为资源提供方的公钥。$Fe=(FID, Dc, Ev, h(e_f))$，FID 为反馈节点的 ID，Dc 为反馈节点对资源的直接信任度，$h(e_f)$为反馈节点公钥的哈希值，Ev 为该反馈节点的全局评价可信度。

2.2 移动节点加入与退出网络

由于在 MP2P 网中，节点频繁移动会造成网络逻辑结构和物理结构不匹配(即结构一致性问题)，因此移动节点的加入与退出与传统的 P2P 网有所不同。

(1)当节点首次加入网络时，将 IMEI(International Mobile Equipment Identification)提交给网络覆盖最近的代理服务器，代理服务器将查询 TP，看该设备的 IMEI 是否在黑名单中。该代理服务器对其验证通过后，分配给该节点唯一的 ID；分配 IP 地址；将该节点信息添加到信息统计表 Sta 和信任反馈表 Fri 中；分配该节点公钥 e 和私钥 d(当移动节点丢失后将利用私钥 d 注销其原有 ID 号)。该代理服务器记为该移动节点的 Root 服务器(Root Proxy，以下简称为 RP)。

(2)当节点临时退出网络时，当前代理服务器(Local Proxy，以下简称 LP)将 Sta 表发送给该节点的 RP，RP 将更新该节点的 Co 值。得到 RP 确认后移动节点即可退出网络，LP 将该节点的 Sta 表删除。

(3)当节点再次加入网络时，将提供自己的 ID 和 e 给 LP。LP 将向 RP 进行验证(若该 RP 失效则询问其后继服务器，以避免"单点失效"问题)，验证通过则在 Sta 表中添加该移动节点的信息记录并分配给该节点 IP 地址，同时将此 IP 地址反馈给该节点的 RP。

(4)若节点的严重恶意行为被多方节点所证实(可通过数字签名的方式发送举报信息给 TP)，那么 TP 将此移动节点的 IMEI 拉入黑名单，该节点被强制退出 MP2P 网络。如果节点主动退出网络且不存在严重恶意行为，将向 LP 提供自己的私钥 d。LP 向 RP 验证后将删除其在 Sta 表中的信息。RP 删除其在 Fri 表中的信息，同时向网络广播删除其在 Ind 表中的信息。

2.3 移动节点间安全资源选择协议

该协议为移动节点的申请资源、获取的信任信息、节点间握手交易以及反馈的信任信息提供了时序规范和安全性保障[9]。其中 $()e$ 表示对称加密，$\{\}e$ 表示非对称加密，$[]d$ 表示数字签名，协议相关流程如图 2 所示。

(1)资源申请方通过 3G 通信接口向本地代理服务器(以下用 LP 表示)提出资源查询请求，RID 为申请方身份标识(以下用 R 表示)，查询信息 $Req=(id, Res, Rtype, TTL)$。$id$ 为此次查询号，TTL 为消息生存时间。

(2)$LP(R)$在 Req 信息后加入 $Ttype$、$Timestamp$ 参数。其中，$Ttype$ 为终端类型，$Timestamp$ 为 $LP(R)$收到此信息的时间戳。$LP(R)$通过设备接入网的索引目录对 Ind 表进行资源搜索。

(3)查找到资源后，$LP(R)$根据提供资源方节点的 PID(以下用 P 表示资源提供方)找到其 Root 服务器(以下用 RP 表示)，获取 P 的当前 IP 地址。R 从反馈资源列表中选出一个 P，向 $RP(P)$查询 P 的节点贡献度 Co。符合要求后，通过 IP 地址向 P 发出资源申请请求 $PReq=(RID, RIP, para, Res, Rtype, PK_{req})$，$PK_{req}$ 为此次请求的会话密钥，$para$ 为具体参数要求。P 向 $RP(R)$查询过 R 的全局评价可信度 Ev 和节点贡献度 Co 后，如果同意交易则向 $LP(P)$反馈资源信息 $Rfe=((PID, PIP, port, para)PK_{req}, RIP)$。

(4)R 解密信息后向代理服务器或者群内节点(通过 IEEE 802.11 接口)广播查询对方节点信任度的信息 $poll=(id, PID, RIP, TTL)$，同时向 $RP(P)$发送 $che=(id, RIP, PK_{sec})$。其中，PK_{sec} 为此次查询的会话密钥。

(5)与 P 交易过的节点可以向 $LP(F)$(以下用 F 表示资源反馈方)提交信任反馈信息 $Tfe=((\{FID, Dc, RIP, FRtype, Time|h(d_f)\}e_p, PID)e_f, FIP)$，$LP(F)$根据对称密钥算法解密验证后为其添加 $Timestamp$、$Ttype$ 参数。e_f 为 F 的公钥，e_p 为 P 的公钥。d_f 为 F 的私钥，$h()$为哈希运算，$Time$ 为之前 F 交易结束的时间。

(6)$LP(F)$将通过验证并且处理过的反馈信息 $Tfe=(\{FID, Dc, RIP, Ftype, Time|h(d_f)\}e_p, FIP, Ttype, TimeStamp)$通过设备接入网发送给 $RP(P)$，$RP(P)$根据非对称密钥算法解密验证后对 Tr，$Timestamp$ 以及 FIP 等因素进行相似性检测，将重复数据进行融合。融合后 $RP(P)$根据 FID 从 $RP(F)$获取到 $Ev(F)$值，$Ev(F)$为 F 的评价可信度。最后发送 $Tfe'=(FID, Dc, Ev, Ftype, Ttype, Time|h(d_f))PK_{sec}$ 给 R。

(7)R 解密后通过计算得到 P 的综合信任度，决定是否与之交易。若双方节点确定交易则进入握手阶段。R 根据 P 的 IP 地址和 $Port$ 端口发送握手信息 $challenge(test, PK_{sha})$。$test$ 为任意测试信息。P 接收到该握手信息后再发出自己的相应信息 $response([test]d_P, e_P))PK_{sha}$。

(8)握手成功则进行交易，对数据完整性要求高的用户可以通过资源摘要和$(para)e_P$ 用哈希算法生成 MAC 消息认证码与资源一同发送。

(9)交易完成后，R 更新 $Tr(P)$，$Ev(RF)$。R 可以向 $LP(R)$反馈 $Efe=([((Ev)h(d_f), FID)]d_r, RIP)$。$LP(R)$通过验证后在 Efe 消息后添加 $Ttype$、$Timestamp$ 参数，并发送给 $RP(F)$，$RP(F)$验证后更新 $Ev(F)$。

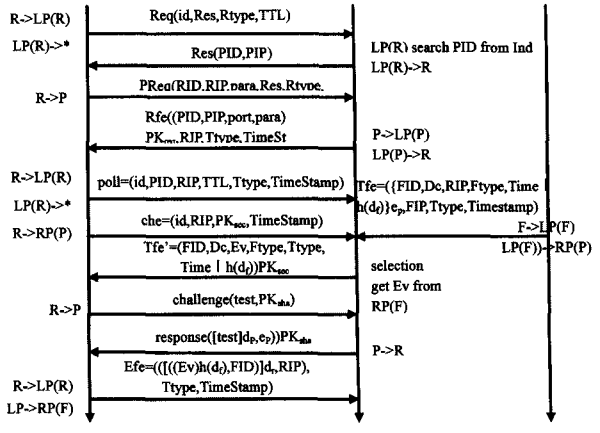


图 2 安全资源选择协议流程图

2.4 多粒度的信任值计算

信任值计算是节点之间信任关系的量化表示方法，按照上节移动节点间安全资源选择协议所提供的时序流程进行计算。为了叙述方便，以下公式计算中用 R 表示资源申请方，P 表示资源提供方，k 表示交易的资源，F 表示反馈方节点。

2.4.1 P 的直接信任度

$$Tr(P)=\begin{cases}Co & (first)\\ Tr' & (\text{else})\end{cases} \tag{1}$$

$$Tr'(P)=\begin{cases}Tr(P)+\omega\cdot(Dc(k)-0.5)^{5m}\cdot Tr(P) & (1\geqslant Dc(k)>0.5)\\ Tr(P)-\omega\cdot(0.5-Dc(k))^{5m}\cdot Tr(P) & (0.5\geqslant Dc(k)>0)\\ Tr(P)\cdot m^{\delta} & (Dc(k)=0)\end{cases} \tag{2}$$

式(1)中 P 的初始直接信任度 $Tr(P)$ 为对方节点的贡献度 $Co(Contribution)$。m 为此次交易安全系数(m 值越大也即风险度越低)，介于开区间(0,1)之间。引入安全系数是为了减少恶意节点通过大量小额交易的成功次数来提升自己的信任度以便进行诈骗的恶意行为。式(2)的 $Tr'(p)$ 为交易后对信任值的更新值(介于[0,1]之间)。如果交易失败，则对此交易资源的满意程度 $Dc(k)$ 为 0，否则将根据 j 节点的服务质量高低使其介于(0,1]区间。交易完成后若发现存在恶意行为，则可以向顶层服务器反馈。ω 为此次行为的权重因子(根据行为上下文而定)。δ 为此次交易失败的惩罚因子，安全系数越低的交易失败后造成的惩罚也就越大。

2.4.2 k 的直接信任度

$$Dc(k)=\frac{1}{m}\sum_{l=1}^{m}\gamma_l\cdot Sc_l \tag{3}$$

式中，m 为 QoS 指标的个数，例如：下载速度、数据完整性、数据真实性、响应时延等等。γ_k 为各指标的权重值，由终端用户自己决定，$\sum_{l=1}^{m}\gamma_l=1$。$Sc_l(score)$ 为交易后根据具体指标对对方节点提供的资源或服务打出的评分值($0\leqslant Sc_k\leqslant 1$)。

2.4.3 P 节点间接信任度

$$Cr(P)=\frac{\sum_{l=1}^{n}Ev(F)\cdot\varepsilon_F\cdot\rho_F\cdot\frac{1}{\Delta t}\cdot Dc(F)}{\sum_{l=1}^{n}Ev(F)\cdot\varepsilon_F\cdot\rho_F\cdot\frac{1}{\Delta t}} \tag{4}$$

$Cr(P)(Credibility)$ 表示关于 P 的资源可信度。Δt 为本次交易与 F 和 P 交易结束之间的时间间隔，n 为符合查询条件的反馈节点数目。$Dc(F)$ 表示 F 反馈的对 P 某资源的直接信任值，$Ev(F)$ 为 F 的全局评价可信度。ε 为终端类型所占权重，终端越相似权重也就越大($0<\varepsilon\leqslant 1$)；ρ 为资源类型所占权重，资源类型越相似权重也就越大($0<\varepsilon\leqslant 1$)。

2.4.4 F 的局部评价可信度

$$Ev(RF)=1-|Dc(R)-Dc(F)| \tag{5}$$

在与 P 完成对 k 资源交易后将计算 F 的评价可信度(evaluation)。$Dc(R)$ 表示 R 对 P 某资源的直接信任值，$Dc(F)$ 表示 F 对 P 提交的反馈信任值。交易完成后节点可以选择上传该局部评价可信度信息至 $LP(R)$。$LP(R)$ 将该反馈信息发送到 $RP(F)$，$RP(F)$ 将按照下列更新公式计算其全局评价可信度：

$$Ev(F)=\begin{cases}Ev'(F)+\varepsilon_R\cdot\varphi(Ev(RF)) & (Ev(RF)\geqslant 0.5)\\ Ev'(F)\cdot Ev(RF)^{\delta} & (Ev(RF)<0.5)\end{cases} \tag{6}$$

$Ev'(F)$ 为 F 更新前的全局评价可信度，初始值为 0.5，$\varphi(x)=\begin{cases}0, & x=0\\ e^{-\frac{1}{x}}, & x\neq 0\end{cases}$。$\varepsilon$ 为终端类型所占权重，终端越相似权重也就越大($0<\varepsilon\leqslant 1$)，δ 为惩罚因子。

2.4.5 P 的综合信任度

$$\mathrm{Re}(P)=\alpha\cdot Tr(P)+\beta\cdot Cr(P)\quad(\alpha+\beta=1) \tag{7}$$

P 的总体可靠度为 $Re(P)$，其中 α、β 为节点信任度以及资源信任度的权重值。α、β 的大小由双方节点交易的历史次数所决定，交易次数多的更相信其主观信任值，而交易少的更相信其间接信任值。因此，在文中令 $\alpha=e^{-\frac{1}{s}}$。其中，s 为双方节点历史交易成功的次数(即 $Dc(k)>0$ 的数目)。

2.4.6 全局节点贡献度

$$Co=Co'+\left[\tau\cdot\frac{\sum_{n=1}^{ResNum}RFNum_n\cdot Size_n}{oltim\cdot(1+\sum_{n=1}^{ResNum}Size_n)}+\pi\cdot Ev\cdot\left(\frac{EFNum+TFNum}{oltim}\right)\right] \tag{8}$$

式中，Co' 表示更新前的节点贡献值，初始值为 0；$RFNum$ 表示提供下载资源的次数；$TFNum$ 表示反馈信任值的次数；$EFNum$ 表示反馈其他节点评价可信度的次数；$Size$ 为节点上传的文件的大小；$Oltim$ 为移动节点在线时长，ζ、π 分别为对其他节点提供服务以及评价行为的权重($\zeta+\pi=1$)。

3 模拟实验结果及分析

3.1 仿真参数设置

为评测 PSTM 抵抗诋毁和合谋两种恶意行为的性能以及抑制“搭便车”行为的作用，本文采用 PeerSim 1.0.5 仿真软件进行仿真，仿真实验参数如表 1 所列。仿真中每隔 30s 更新一次节点的全局贡献度以及评价可信度，每个节点平均每次发送 20 次交互请求。仿真实验设置的场景是文件共享应用，每个节点拥有 8 个文件，硬件环境为 2.0GHz 双核处理器和 2G 内存。

表 1 仿真实验参数

参数	描述	默认值
N	网络节点数	512
M	资源总数	4096
Rtypes	资源类型数目	20
Ttypes	设备类型的数目	10
Time/min	交易时间	30
m	式(1)中的安全系数	0.5
δ	式(2)和式(4)中的惩罚因子	2
Rate of RF	提供下载资源的节点概率	0.4
Rate of TF	反馈资源信任值的节点概率	0.3
Rate of EF	反馈评价可信度的节点概率	0.3
ζ	式(8)中的权重因子	0.6
Threshold	可靠度阈值	0.5

3.2 诋毁恶意行为模拟

模拟诋毁行为对资源交易的成功率时，选取了表现较好的移动 P2P 网多粒度信任模型 MGT[4] 作为对比。节点通过每次交易结束均反馈交易失败(即 $Dc=0$)达到对其他节点的诋毁效果。最后，实验根据诋毁节点所占总节点数的不同比例分别对仿真结果 Rate of Unsuccess.dat 文件进行数据采集，如图 3 所示。

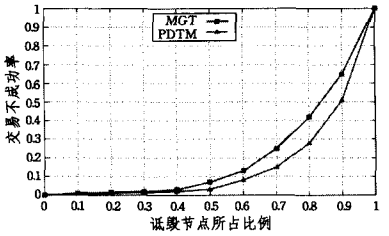


图 3　诋毁行为对交易结果的影响

当恶意节点所占总节点比例小于等于 40%时，两种模型的区别不是很明显，都能达到较为理想的成功下载率。当比例超过 40%时，PSTM 相对于 MGT 的诋毁抑制作用更为明显。PSTM 在计算间接信任度时，根据资源与终端的相似程度以及时间衰变因素为不同节点提交的信任值赋予不同的权值，减少了诋毁行为在计算过程中带来的负面影响。

3.3　合谋恶意行为模拟

模拟合谋行为时，本实验假设网络中 50%与目标节点交易过的节点都互相串通对该目标节点采取贬低和抬高两种恶意行为(前 50 次交易表现为贬低，后 50 次交易表现为抬高)。根据仿真结果 indirect trust. dat 中的数据采样得到这两种行为对该节点间接信任度的影响。为了更好地模拟这两种恶意行为，目标节点在交易 50 次前间接信任度稳步上升($Dc>0.5$)，用以模拟能够给对方节点提供较好的资源的情况，此时的合谋行为表现为贬低该节点的信任度(如图 4 所示)。而在随后的交易过程中，间接信任度逐步下降，用以模拟目标节点由于服务质量的下降而不能提供较好的资源的情况，此时的合谋行为表现为抬高该节点的信任度(如图 4 所示)。从图中可以看出，合谋行为对其间接信任度的影响随着交易次数的增多反而减少。原因在于交易次数越多合谋节点 *IP* 越相似，PSTM 便越能判断其恶意行为，从而减少合谋行为对目标节点信任度的影响。

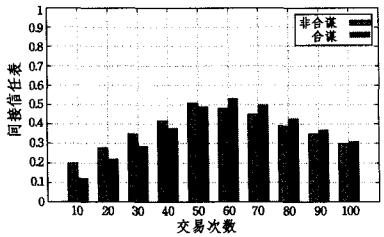


图 4　合谋行为对节点间接信任度的影响

3.4　节点贡献度对搭便车节点的影响

选取网络中 3 种目标节点：贡献较多的节点、贡献一般的节点、“搭便车”节点。为了模拟移动 P2P 网络中节点频繁加入或退出的情况，网络总节点的数目通过 PeerSim1. 0. 5 自带的 Dynamic Network 控制组件依次增加到网络中，3 种目标节点也在不同特定时间加入或退出网络。

如图 5 所示，当网络中存在 64 个节点时，由于节点数目较少，3 类目标节点下载成功率都比较低。但随着网络节点的增加，尤其是增长到 512 个节点时，贡献度较高节点的交易成功率约为 65%，明显高于其他两类节点。这是由于陌生节点在首次向对方节点提出申请时会以其全局贡献度作为直接信任值加以考虑，而对方节点也会参考该申请方节点的全局贡献度以及评价可信度来决定是否与之交易。这就增加了贡献度高的节点交易的成功概率，同时也降低了“搭便车”节点的交易成功率。

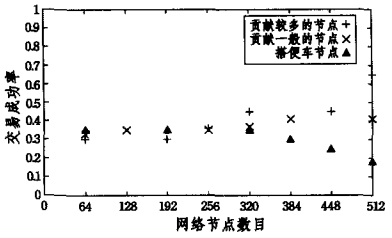


图 5　节点贡献度在不同规模下对交易成功率的影响

结束语　在移动互联网日趋发展的今天，移动用户之间的信任问题具有重要的研究价值。本文提出一种在 MP2P 网络环境下基于代理的安全反馈信任模型 PSTM，主要贡献在于针对 MP2P 网和传统 P2P 网之间终端设备的差异性，给出由代理服务器组成的设备接入网的逻辑框架、移动节点加入与退出网络的流程、移动节点间安全资源选择协议和多粒度的信任值计算方法。实验表明，PSTM 能够有效地抵御诋毁以及合谋恶意行为对节点信任值的影响，同时能够抑制节点“搭便车”行为，促进贡献度高的节点的合作成功率。

后续将深入研究信任信息在设备接入网上的存储方式、哈希映射方式，以提高资源的搜索效率。同时，模型中安全资源选择协议也为代理服务器带来相对较多的信息存储、安全处理与传输时间方面的开销，因此如何提出一个轻量级的安全资源选择协议以适当减少代理服务器的开销也是今后研究的重点。

参 考 文 献

[1] Basit Q, Geyong M. A distributed reputation and trust management scheme for mobile peer-to-peer networks[J]. Computer Communications, 2012, 35(5): 608-618

[2] Wu Xu. A distributed trust management model for mobile P2P networks [J]. Peer-to-Peer Networking and Applications, Springer Science, 2012, 5: 193-204

[3] 李致远. 一种移动 P2P 网络环境下的动态安全信任模型[J]. 电子学报, 2012, 40(1): 1-7

[4] 任艳, 任平安, 吴振强, 等. 移动 P2P 网络中的多粒度信任模型[J]. 计算机工程与应用, 2009, 45(6): 137-140

[5] Jameel H, Hung L, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values[C]// Proc of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005: 674-679

[6] Almenarez F, Marin A, Campo C, et al. PTM: A pervasive trust management model for dynamic open environments[C]// Proc. of the 1st Workshop on Pervasive Security, Privacy and Trust. Boston: IEEE Computer Society Press, 2004: 345-350

[7] 王昕. 基于移动 P2P 的分布式网络信任模型研究[D]. 石家庄: 河北科技大学, 2010

[8] 程久军, 李玉宏, 程时端, 等. 移动 P2P 系统体系结构与关键技术的研究[J]. 北京邮电大学学报, 2006, 29(4): 86-89

[9] 胡建理, 周斌, 吴泉源. 一种 P2P 信任管理安全性协议[J]. 计算机科学, 2011, 38(10): 64-67

[10] 苗光胜, 冯登国, 苏璞睿. P2P 信任模型中基于模糊逻辑的共谋团体识别方法[J]. 计算机研究与发展, 2011, 48(12): 2187-2200

[11] Chin-Chih C, Yen-Chen C. A mechanism for sharing Web serv-

ices in mobile P2P networks[C]//2011 international conference on agricultural and natural resources engineering. Singapore: Advances in Biomedical Engineering, 2011: 251-260

[12] Kokkonen E, Baset S, Matuszewski M. Demonstration of Peer-to-Peer Session Initiation Protocol(P2PSIP) in the Mobile Environment[C]//Consumer Communications and Networking Conference. Las Vegas, NV: IEEE Computer Society Press, 2008: 1221-1222

[13] 陈宏旦. 移动 P2P 网络中的基于 DHT 分层 Chord 算法研究[D]. 重庆: 重庆大学通信工程学院, 2010

[14] Wu Xu, He Jing-sha, Chia - Hu C, et al. A Power Peer-Based Reputation Scheme for Mobile P2P Systems[C]//Proceedings of the 9th International Conference on Algorithms and Architectures for Parallel Processing. Taiwan: Springer-Verlag, 2009: 615-625

[15] 乐光学, 李任发, 陈志, 等. P2P 网络中搭便车行为分析与抑制机制建模[J]. 计算机研究与发展, 2011, 48(3): 382-397

[16] Zou Dong-yao, Gan Yong, Qu Hai-tao. Research of structure consistency between overlay and network layer based on mobile P2P[C] // Computer Science and Information Technology (ICCSIT). Beijing: IEEE Computer Society Press, 2009: 254-258

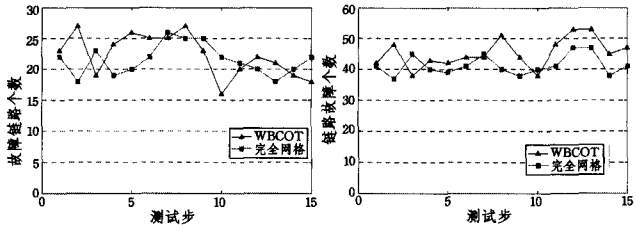
(上接第 183 页)

故障时，重要节点之间仍然可以保持连接，而在相同的条件下，一对一连接机制仅能在平均 63%的链路发生故障时保证相同的结果。两张图均表明 WBCOT 优于有线链路备份中的一对一连接机制。

与此同时，数据波动也表明网络拓扑、重要节点的位置、链路故障以及一些其他的因素对网络的连接性具有重要影响。但是，在相同的网络条件下，WBCOT 对网络持续性的改善程度比有线链路备份高 7%～9%。仿真结果也表明无线备份的灵活性对改善网络连接性具有巨大优势。

4.2 与完全网格连接机制的比较

该实验的停止条件仍为 2 个，且与 5.1 节中的相同。测试数为 15 个。网络拓扑、有线备份连接以及链路故障都是随机产生的。在该实验中，有线备份链路与普通链路具有相同的故障概率。仿真结果如图 4 所示。



(a)停止条件是低于规定值　　(b)停止条件是连接断开

图 4　与完全网格机制的比较结果

图 4 中，黑色线代表 WBCOT 的结果，灰色线代表有线链路备份机制的结果。仿真结果也表明网络拓扑、重要节点的位置、链路故障以及一些其他因素对网络连接性具有重要影响。同时，两条线几乎交织在一起，两种解决方案的性能在每一次测试中都是相近的。这表明 WBCOT 与完全网格连接机制对改善网络连接性具有相似的影响。然而，相比完全网格连接机制需要使用 45 条有线链路来完成有线备份的过程，WBCOT 所需的资源要少很多。

结束语　连接性是代表网络生存能力的重要指标。然而最近人们对它的研究逐渐减少。目前的大多数研究通常假设网络的连接是持续的，有研究假设网络即使会发生故障，也是小范围的故障。然而，当大规模的自然灾害发生时，这种假设就几乎不成立了。

WBCOT 与 FRR、RON 以及任何其他网络生存解决方案都不同。它关注的是提高网络的连接性。它利用无线连接架构的灵活性并根据实际网络上下文环境来动态配置无线备份，同时充分利用有限的无线资源来尽可能保证网络的连接性。性能比较结果表明，WBCOT 比固定的有线备份机制更好。

同时，由于无线连接的故障产生原因与有线链路故障产生原因具有很大的不同(前者往往是无线信号的干扰，而后者通常是物理链路的损坏)，因此在主链路和有线备份链路都发生故障时，无线备份往往能有效避免这种故障，仍然保持正常工作。接下来的工作将从提高 WBCOT 中的网络连接性度量算法以及无线备份建立算法的复杂度性能展开，一个可能的解决方案是结合智能信息处理技术[10]改善相应的算法，使其复杂度降低。

参 考 文 献

[1] Sydney A, Scoglio C, Gruenbacher D. Optimizing algebraic connectivity by edge rewiring[J]. Applied Mathematics and computation, 2013, 219(10): 5465-5479

[2] 褚龙现. 一种改进的半连接查询优化算法[J]. 计算机技术与发展, 2012, 10: 136-139

[3] Atlas A, Zinin A. Basic specification for IP fast reroute: Loop-free alternates. RFC 5286, 2008

[4] Wu Xiao-bo, Zhou Xian-wei, Lin Fu-hong. Dynamic Connectivity in Cislunar Communication Networking Based on Geosynchronous Orbit Relay Satellites[J]. China Communications, 2012, 9(11): 41-53

[5] Zhu Da-jiang, Li Kai-ming, Cesar F, et al. Optimization of functional brain ROIs via maximization of consistency of structural connectivity profiles[J]. Neuroimage, 2012, 59(2): 1382-1393

[6] 杨佳, 郝福珍, 张金霞. 基于可信网络连接的安全 RFID 中间件分析与设计[J]. 计算机工程与设计, 2012, 12: 4465-4470

[7] 秦贵和, 南洋, 陈筠翰, 等. 面向媒体的系统传输网络连接管理策略[J]. 吉林大学学报: 工学版, 2012(4): 963-970

[8] Zhang Yan. Network Optimization-based MPC for Distributed Control Systems[J]. Advanced Composite Materials, 2012, 482-484: 2485

[9] Wang Heng-tao, Zhao Qian-chuan, Jia Qing-shan, et al. Efficient Topology Optimization for a Wired Networked System by Adding Wireless Communication[C]// 2012 American Control Conference(ACC). Montreal, Canada, June 2012: 448-453

[10] 张博, 张涛, 林为民. 基于软交换的智能电网可信网络连接模型研究[J]. 软件学报, 2012(1): 28-33

[11] 郑鹏宇, 何世彪, 张馨月, 等. 一种基于博弈论的无线网状网络信道分配算法[J]. 重庆理工大学学报: 自然科学版, 2013, 27(4): 90-95