

可信普适社交网络研究综述和展望

闫峥, 吴宸梓, 冯伟, 王子龙

(西安电子科技大学网络与信息安全学院综合业务网络理论与关键技术国家重点实验室, 陕西 西安 710071)

摘要: 信任对于陌生人在普适社交网中的交互活动起到了重要作用。它帮助人们克服不确定性、规避风险并做出正确的社交决策。首先, 多方面综述了可信普适社交网络信任管理的研究现状, 并对现有工作的优势与不足进行了分析; 其次, 分析揭示了其关键科学问题和研究方向; 最后, 提出了全面实现可信普适社交网络的研究模型。

关键词: 社交网络; 信任管理; 社交网络安全; 隐私保护

中图分类号: TN929

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00024

Survey of trustworthy pervasive social networking

YAN Zheng, WU Chen-zi, FENG Wei, WANG Zi-long

(State Key Lab of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China)

Abstract: Trust plays an important role in pervasive social networking (PSN) for reciprocal activities among strangers. It helps people overcome perceptions of uncertainty and risk and engages in trust-related social behaviors. The current literature on trust management in PSN was reviewed. The advantages and disadvantages of existing solutions were analyzed. Furthermore, key research issues were presented. A research model was also proposed to achieve trustworthy pervasive social networking comprehensively.

Key words: social networking, trust management, social network security, privacy preservation

1 引言

随着移动计算和移动网络的快速发展, 社交网络逐渐从基于传统的互联网发展到移动领域。个人移动设备(如智能手机等)能够通过移动互联网、蜂窝移动网或无线自组网构建普适社交网(PSN, pervasive social networks), 从而随时随地进行各种社交通信和活动。普适社交网是指由互联网、蜂窝移动网和移动自组织网络等异构网络支撑的普适存在且支持即时社交活动的社交网络。不同于传统的基于互联网的在线社交网络, PSN可以根据不同的社交需求在不同网络间自适应切换, 动态构建社交平台, 高效地支持社交应

用和服务。PSN具有网络自适应性、社交普适性和服务智能性等特点^[1]。5G移动网络将高效融合各种异构网络, 为移动用户提供更便捷和更高质量的网络服务, 普适社交网将成为其应用典范。

移动自组网(MANET, mobile ad-hoc networks)是支持PSN的技术之一。MANET为PSN提供了一种有效的实现平台, 并对传统的在线社交网络进行了有益的扩展和补充。例如, 移动用户可以通过PSN从周围的陌生人中寻求帮助或建议。另外, 由于现代生活中陌生人群集体移动极为常见^[2], PSN可以为用户带来非传统和新型的社交体验, 其价值日益显著, 特别是对“熟悉的陌生人(familiar strangers)”用户而言, 即经常

收稿日期: 2016-01-30; 修回日期: 2016-02-08。通信作者: 闫峥, zyan@xidian.edu.cn

出现在自己附近但并不相识的人^[3]。

社交网络和计算领域已经取得大量优秀的科研成果,目前的研究重心已转向移动领域的社交通信,而基于 MANET 的移动社交网络研究也得到了多个学术组织的关注。例如,美国斯坦福大学 MobiSocial 研究小组开发了基于 MANET 的社交平台 Junction^[4];美国杜克大学开发了帮助用户发布具有位置标签的微博^[5],适于旅游、广告、紧急警报等应用;瑞士 ETH 研发了 AdSocial 普适社交多媒体沟通平台^[2,6];芬兰 Aalto 大学对浮动内容进行了分析研究,探索内容在伺机网络短暂分享的服务质量^[7]。

在工业界,一些公司诸如微软、诺基亚和英特尔已经开始 PSN 领域的研究。微软亚洲研究院开发的 EZSETUP 系统,为移动用户提供发现服务^[8];诺基亚即时社团网提供即时社交平台,支持人们近距离分享各种信息^[9];英特尔伯克利实验室进行的“熟悉的陌生人”项目,扩大了与在公共场所(例如地铁和公交车)定期相遇但不相识的人们的沟通和交流^[3]。

在国内,一些研究团队将普适计算、数据挖掘与社交网络相结合,研究 socially aware computing 和基于社交网络的感知,借助于大规模的社交数据,识别个体行为、挖掘群体交互模式、预测社交行为、智能支持通信和协作^[10,11]。为保护移动社交网隐私,程瑶等^[12]研究了移动社交应用的用户隐私泄露问题;吕志泉等^[13]设计了带陷门的属性加密算法保护社交数据;霍峥等^[14]研究了名为 PrivateCheckIn 的轨迹隐私保护方法。但是,这些项目和研究都没有考虑异构混杂网络融合,而且大部分没有涉及信任和信誉管理,没有充分研究 PSN 的安全和隐私保护。PSN 中有很多问题还未得到深入探讨和实质性突破。

信任在 PSN 用户进行互利交互时起着重要的作用。它帮助人们克服和陌生人进行沟通时产生的不确定性,做出正确的决策从而避免不确定性带来的风险,并促使用户参与到需要高信度的社交活动中。然而,现有的 PSN 项目并未对信任与信誉管理进行充分研究。这里,信任是根据某实体的安全性、真实性、可靠性和其他一些特性而产生的对该实体的信心、信念和期望。信誉是

根据早前与某实体交互的其他实体中获得的直接或间接经验而做出的对该实体信任的评估。信任信誉机制已在多个领域被广泛研究。然而,传统的在线社交网络系统(如 Facebook)和当前的 PSN 研究并未全面地考虑信任,也没有充分地探究如何在 PSN 中对信任进行全面管理。一些相关重要问题,如可信身份识别,PSN 通信数据安全,用户隐私保护,信任关系的评估、演化和增强,不期望信息控制,人机可信交互和恶意社交行为跟踪等,尚未深入研究。显而易见,PSN 的实际应用和部署会带来新的安全挑战,特别是当用户对其隐私和 PSN 安全有较高要求的时候。

2 可信普适社交网研究综述

2.1 信任信誉机制

信任管理涉及搜集有用信息(如用户反馈)、评估信任关系、决策信任、监测和重新评估信任关系,并使以上过程自动化^[1]。信任和信誉机制已经在众多计算机与通信系统中得到广泛研究,例如 MANET、P2P(peer-to-peer)对等网络、网格计算、云计算、社交网络、普适计算和电子商务等^[1,15],但以往的研究成果并不适用于基于异构混杂网络的 PSN 的信任、信誉计算和管理。目前,已开发了许多支持可信通信和协作的信任和信誉系统^[16~18],典型的有 FuzzyTrust 系统^[19]、ebay 用户反馈系统^[20]、PeerTrust^[21]、MANET 的客观信任管理框架^[22]、分布式 P2P 文件信誉系统 Credence^[23]。在分布式系统的信任管理研究中,李建欣等^[24]提出了一种面向网络计算的动态信任管理模型;李致远等^[25]针对 P2P 电子商务中的信任评估问题,提出一种基于信任云的动态安全信任管理模型;针对 P2P 系统中不诚实推荐等问题,文献[26]提出了一种具有激励效果的分布式 P2P 信任管理模型。此外,多种针对 MANET 的信任管理机制也被提出^[27,28];一些研究则根据社交关系对信任进行评估^[29]。

在以上研究中,信任可以被建模并以数值的形式进行表示,但是这些工作不能解决 PSN 信任管理难题,主要体现在:1) 没有考虑如何基于社交行为和经历动态地进行自适应于社交情景的信任和信誉评估;2) 缺乏评估的可信性研究,对各

种恶意攻击(例如女巫攻击、on-off 攻击、独立/协作谣言攻击、矛盾行为攻击、选票作假攻击、以及新来者攻击^[30,31])的抵抗性差;3) 未能有效实现 PSN 信任评估的隐私保护。在之前的工作中,一些在 PSN 中影响信任的因素也未被考虑在内。信任评估需要采集相关个人社交体验、观点和行为数据进行分析,这可能侵犯到用户隐私,而早期研究^[16,19,21,22,29,32]很少将用户隐私作为主要考量来关注 PSN 信息内容信度和社交信誉^[33]。现有的具有隐私保护的信任评估策略计算复杂度相当高,不能灵活支持传统的信任评估理论,可靠性和精确度差,有诸多的局限性^[34-37],因而并不适用于 PSN 的特殊环境。为了确保 PSN 的可信度,还需要对信任信誉管理机制进行进一步的研究。另外,匿名的采用和更改便于用户有效删除其历史行为记录,使信任评估准确度变低,增加了研究难度。研究发现,以评估者历史行为作为评判标准的信誉系统能很好地克服独立/协作谣言攻击^[38-40],集中与分布相结合的复合式信誉系统结构更适用于普适社交网,尤其是普适匿名社交^[38,40]。但以往研究并未全面解决具有隐私保护的可靠信任评估难题^[41]。

2.2 信任和信誉系统的架构

Jøsang 等^[42]将信任/信誉系统分成了2个主要的类型:集中式系统和分布式系统。系统架构决定了在一个信誉系统中信任和信誉评分如何在评估者之间进行交互。很多文献研究 MANET 中的分布式信任评估,但是几乎都没有考虑节点的隐私^[16,17,32],这有可能导致一系列针对特定节点的安全攻击问题,如恶语攻击、谣言攻击等^[43]。一些系统借助博弈论^[21,28,44,45]和贝叶斯分析^[46,47]等工具来表示信誉。它们通常通过计算和公布信誉来强制节点间友好协作以及制裁节点的任何恣意错误行为从而避免节点自私行为。然而,现有的工作很少关注具有隐私保护的信任评估问题。另一方面,实际使用的信誉系统大多会配置一个服务器,服务器可以收集用户的反馈并进行分析来产生信任值(比如 ebay^[20]、雅虎竞拍^[48]以及基于互联网的系统如 Keynote^[49])。然而,这些系统(如 Amazon 和 ebay)大多忽视了用户反馈的可信性,这会对产生的信誉值的可信度造成不良影响。此外,为

了保护用户隐私,一些社交网络中采用匿名方式,而且匿名的更换非常容易,这使用户很容易清除自己的历史行为记录,使准确地进行信誉评估变得更加困难。为了实现 PSN 中准确的信任信誉评估和管理,其信任架构的设计必须要解决上述问题。PSN 中采用混合式信任管理架构可以有效地克服上述2种架构的弱点。在混合式信任管理架构中,信任、信誉评估在 PSN 各节点以匿名分布式进行,但同时也可以得到拥有用户唯一注册身份的中心服务器(如在线社交网站)的支持^[38,50,51],从而使信任、信誉评估更加高效、准确。

2.3 信任信誉管理的信息同步

在大多数 MANET 信誉系统中,节点的信誉在网络中被全局共享。一个节点的信誉可以共享给所有节点从而减少其侦测时间,但维护和传播间接信誉信息会增加节点以及网络的负担。Bansal 等^[52]的 Ocean 系统在进行信任、信誉评估时,仅仅使用直接观测得到的本地信誉而不考虑二手信誉信息,从而减少了间接信誉在节点间交换的通信开销。一些方案^[38,50,51]通过整合本地经验和全局经验来计算本地信誉和全局信誉,并通过部署可信服务器来消除维护和传播信誉信息所产生的额外开销。

信誉的不一致性问题(即不同节点对同一个特定节点给出不同的信誉评估结果)在 MANET 中经常出现,评估主观性以及不同的本地经验都可能导致这一问题。这使从信誉信息中辨别出诚实正确的信誉评估变得非常困难。Hu 等^[53]提出了名为 LARS 的基于本地意识的信誉系统,用来解决自私行为和恶意行为(比如漏包和不公评级)所造成的负面影响。在 LARS 中,一个节点的信誉通过直接监视的信息推导得到,而间接信息不用于信誉评估。在 PSN 中应该避免信誉不一致问题并且消除由于 PSN 节点间多跳信誉传播所造成的用户信誉评估失准。

一些方案^[38,50,51]采用一个信任服务器(TS)来汇总来自各个节点反馈的节点信誉。汇总生成的节点信誉值随后被转发给其他请求节点作为其初始信誉值,请求节点会根据自己的个体经验对其进行修订。这一过程不断地迭代,从而降低了信誉不一致问题造成的不良影响,解决了信誉多跳传播所造成的用户信誉失准问题。可以看到,

不论是在 TS 还是在 PSN 节点, 信誉是根据一手经验和直接投票计算得到的。

2.4 基于信任管理的不期望信息控制

移动用户通过 PSN 获取有用信息的同时, 可能会收到不期望的内容, 例如恶意软件、病毒或木马、垃圾信息、不期望广告, 拒绝服务和分布式拒绝服务攻击等。这些信息可能入侵用户设备、占用设备内存、消耗电池能量、欺骗用户、极大地影响用户社交体验。PSN 不期望信息控制是影响其服务质量的关键因素之一, 这也是 PSN 安全保护的重点。基于信任管理研究信息源和信息内容信度是进行不期望信息控制的有效方法。目前, 已有一些基于信任/信誉管理的反垃圾邮件解决方案^[54], 例如基于用户反馈的 MailTrust^[55]、IRGroupRep^[56], 基于用户历史记录的控制垃圾即时消息发送的 SpimRank^[57]。Tang 等^[58]提出了基于垃圾邮件发送者行为分析的反垃圾邮件方法。一些研究专注于网络垃圾邮件控制, 例如 TrustRank^[59]。Kolan 和 Dantu^[60]提出了基于位置、状态、时间、个体信任、语音特性和信誉分析的垃圾语音过滤机制。但由于 PSN 的特性和对不期望信息判断的主观性, 以上研究成果因通用性差而并不适用, 更不能支持个性化不期望信息控制, 也没有考虑隐私保护。如何在 PSN 中实现通用于异构网络和适用于各种媒体信息的个性化不期望信息控制是研究难点, 加强隐私保护是重点。通过前期研究发现, 基于可信用户对信息反馈、操作和通信流量分析的信任管理系统是解决 PSN 不期望信息控制的有效方法^[61,62]。然而, 现有工作极少关注社交网络中的不期望信息控制。

2.5 隐私保护推荐

推荐系统通常采用信息过滤技术向用户推荐他们所感兴趣的信息。文献[63]提出使用信任来确定推荐权重和对信息进行过滤的推荐方法。可信的推荐者应该和被推荐人有相似的兴趣爱好, 并且具有良好的推荐历史从而证明其推荐的可信性, 推荐过程应该考虑这一信任信息。但是, 大多数推荐系统所考虑的特征都不是用户对隐私数据的分享行为, 而用户对隐私数据的分享行为往往是反映用户在私有数据分享方面偏好的重要线索 (例如用户青睐于在哪些环境中分享哪些数据)。

现有工作极少根据上下文环境针对用户数据隐私保护提供建议和推荐, 特别是在 PSN 中^[64-66]。以往的研究主要致力于探索如何保护用于产生推荐而收集的用户信息, 目的是保护用户隐私不被泄露给推荐服务提供商, 而对于那些能够帮助用户在隐私保护方面做出决策的推荐, 则很少关注。

已有很多实现上下文环境感知或个性化推荐的方案^[67-70]。这些方案一般针对用户的兴趣爱好^[69]或可能感兴趣的信息^[70]推荐好友, 然而, 几乎没有方案针对用户数据隐私保护提供推荐。现有的这些方案大多采用用户-服务器架构, 例如 CoMeR^[67]和 SCAMREF^[68]。其中, AdPriRec 既支持在可信服务器上产生集中式的推荐, 又支持在 PSN 节点端产生分布式的建议^[50]。它使用了环境标识符 ID 来标记上下文环境, 具体环境通过环境参数和参数值来描述。AdPriRec 针对不同的上下文环境对不同的用户数据提供其共享策略, 从而实现具有上下文环境感知的用户数据隐私保护推荐。

现有的文献已经在 MANET 中研究了分布式的信任和信誉评估^[16,17,32]。基于信任/信誉的推荐机制有利于实现节点间的安全交互与合作, 从而维护正常的组网和路由。然而现有工作很少研究如何在 PSN 的服务和应用中对数据隐私保护策略提供推荐^[71]。

2.6 移动社交网络的隐私保护

用户的个人数据和位置信息是隐私保护研究的 2 个关注点^[71-73]。通常的解决方法包括数据加密和密钥分配^[73]以及引入用于发放用户匿名的服务器^[74]。为了验证这些方案的有效性, 研究者们对其抵抗各种攻击的顽健性进行了分析, 这些攻击包括窃听、电子欺骗、消息重放和虫洞攻击等^[74]。很多社交网络应用通过让用户定义自己的隐私策略以及设定有关隐私保护配置来解决隐私保护问题。比如, PeopleFinder 是一款允许用户同他人分享位置信息的社交应用, 用户可以随时改善自己的隐私策略进行位置分享^[75]。Miluzzo 和他的团队对使用传感器的社交网络应用 CenceME^[76]中的隐私问题进行了研究, 该应用允许用户手动选择是否使用手机上的某个传感器, 这意味着用户必须关闭相关的传感器来保护相应

的个人隐私。还有一些方案使用信任管理机制来保护用户隐私,霍峥等^[14]针对签到服务中匿名用户的轨迹隐私泄露问题,提出了名为 PrivateCheckIn 的轨迹隐私保护方法。

2.7 PSN 通信数据访问控制

PSN 安全要求通信数据应由可信用户访问。由于信任关系的易变性和 PSN 的异构性,数据访问密钥管理异常复杂。现有的技术并不能有效地应用于 PSN,具体表现在:1) 传统的基于对称加密和公钥加密的方法由于效率问题并不适用于 PSN^[77];2) 由用户自己制定隐私保护策略、控制自身设备分享个人数据的方法可用性(usability)差^[75,76];3) 模糊化数据的方法不能实现可信数据的访问和应用^[74]。尽管学者们已经提出很多 MANET 中的访问控制方案,但是,它们都没有将信任作为影响访问控制的因素。另外,MANET 安全传输方案集中于链路层和访问控制层,不能支持 PSN 应用层的数据安全及访问控制^[78,79]。自适应于 PSN 异构网络的社交数据访问控制成为未解难题。前期研究表明,信任管理可以有效地与密码学方法结合,采用多维信任评估等级对 PSN 数据进行访问控制是实现 PSN 可信通信的有效途径^[80,81]。

2.8 匿名信任认证

信任在 PSN 中帮助人们克服不确定性、避免不必要的风险并做出正确社交决策。匿名信任认证直接认证信任关系,从而避免透露真实身份和匿名身份,既能实现身份隐私保护,又支持可信社交,是 PSN 中支持安全和隐私保护的关键技术^[82]。区别于传统的匿名通信^[83,84],匿名信任认证和其密钥计算复杂度不随匿名数量线性变化,极大地提高了隐私保护效率和系统可扩展性。目前社交网络经常采用的群访问控制不能有效保护个人隐私^[85]。Ciszkowski 和 Kotulski^[86]应用信誉系统实现具有隐私保护的可靠 MANET 路由搜寻,但未解决匿名信任认证问题。然而,信任评估的身份确定性和匿名认证对身份的隐匿性是一对矛盾体。另外,为确保非关联性,匿名信任认证需要频繁更换密钥对,增大了计算复杂度。如何克服以上矛盾,在保护隐私的同时支持高效实用性,是 PSN 隐私保护研究的一个难题。

3 关键问题和研究方向

PSN 的信任管理涉及很多方面,比如数据安全、用户隐私、PSN 节点间的信任保证、可信身份识别和人机可信交互等。虽然目前有一些关于 PSN 的信任增强技术的方案,但是仍然缺乏综合信任管理架构,也没有实际而有效的方法来全面解决 PSN 中的信任问题。文献研究表明,PSN 信任、安全和隐私问题尚未被广泛探索和深入研究。传统的集中式社交网络系统(如 Facebook)采用基于群的访问控制,不能完全保证用户的隐私^[85],也不能满足即时社交需求,特别是当用户不能连接到互联网而只能和附近的用户进行交互的时候。确保安全和增强隐私的信任管理技术亟需认真研究,这样才能实现易被移动用户接受的值得信赖的 PSN 系统。相关于 PSN 安全、信任和隐私,需要认真解决如下关键科学问题。

1) 自适应密钥管理机制

实现 PSN 通信安全和数据访问控制的密钥应当能够根据用户的信任级别以及社交环境的变化自适应管理。理想情况下,PSN 中的节点可以在不知道对方身份的情况下互相验证对方的信任值。对节点信任值的匿名认证不仅有助于保护隐私,还可以确保 PSN 的可信度。由于 PSN 拓扑结构和用户信任等级的动态变化性,用来进行安全通信的加密密钥需要频繁更换,在这一过程中,PSN 会将新的解密密钥分发给合法用户。频繁的密钥更新与分发会产生大量的通信开销和计算开销,从而导致严重的性能瓶颈。如何安全有效地实现 PSN 中数据访问控制是一难题。现有的研究工作几乎都不能有效地实现 PSN 中的数据访问控制,也不能有效地实现 PSN 成员撤销^[2-9]。过去的密钥管理方案几乎没有考虑采用用户的信任值和环境属性来实现数据的访问控制,因而不能有效地应用在 PSN 系统中^[38,50,51]。

更重要的是,匿名的使用使 PSN 节点可以隐藏自己的真实身份,同时还可以避免恶意的隐私追踪,但这也对系统性能产生了新的挑战,例如节点认证效率问题、密钥管理问题以及信任管理问题。这是因为每次匿名变更,授权中心需要产生一对新的公私钥并对其颁发证书,使节点能够

正常地参与之后的认证和验证活动。此外,对基于过期匿名而评估的信任值应该映射到新的匿名,否则系统会很容易遭到女巫攻击。更严重的是,由于移动设备的电量、存储空间和计算能力有限,密钥的频繁变化和更新以及繁重的身份管理在实际系统中并不适用。因此,PSN 中的信任管理方案在实现隐私保护和安全的同时,需要具有很高的效率。

2) 增强隐私的信任管理系统

PSN 需要能够增强隐私的信任管理系统,该系统应具备环境感知能力并可以被用户轻松接受。普适社交网络需要有一种机制来自动帮助用户进行决策,例如帮助用户确定在什么情况下可以信任另一用户。此外,一般而言,大多数用户希望保护个人隐私并避免恶意追踪。虽然学术界和工业界对 PSN 进行了一些研究,但是如何实现具有隐私保护的实用自治信任管理仍需进一步探索。

3) 不期望信息控制

不期望信息控制在 PSN 中是另一个重要科学问题。人们在不同的环境中以不同的目的进行通信,从而产生大量的通信信息,例如移动终端软件的安装链接、移动服务 URL、网页或是由用户键入的文本信息。然而,当用户期待通过 PSN 接收到有用信息的同时,他们也可能接收到不需要的垃圾信息,例如垃圾软件、病毒或木马、垃圾邮件、网站、垃圾电话、垃圾即时消息、短信网页内容或者 DoS/DDoS 攻击。这些信息强行侵入用户设备,浪费用户时间,占据了设备存储空间,消耗电量从而给用户带来极大困扰。用户应当有方法来确定是否应该信任从 PSN 上接收到的信息并对不期望信息传播进行控制,这使 PSN 不期望信息控制成为了一个重要科学研究问题。

4) 推荐系统

本文期待能够在 PSN 中为用户信任、隐私和安全提供有效、个性化、具有上下文环境感知的推荐系统。PSN 用户隐私保护是一个重要问题,因为对隐私的保护体现了一个实体将自身或是其个人信息隔离并选择性透露的能力。然而用户很难准确判断在不同环境中分享个人数据是否安全合理。另外,隐私是一个主观问题,即便在相同的情景下,不同用户对待隐私的态度和策略也不

同。所以,在 PSN 中针对信任、隐私和安全为用户提供个性化、具备上下文环境感知的推荐系统可以帮助 PSN 用户在社交活动中正确决策,从而有效避免不必要的风险。

显然,任何 PSN 信任管理系统都会遭受很多恶意攻击。现如今,信誉系统可能面临着非人为的不公正评价而导致的信誉评级不公平问题^[20,48]。它们易受到很多潜在攻击,例如女巫攻击、on-off 攻击、独立/协作谣言攻击、矛盾行为攻击、选票作假攻击以及新来者攻击^[30,31]。匿名的使用使追踪恶意行为变得非常困难,从而增加了实现可信信任评估的难度,同时也影响了信誉评估的准确性。Sun 等^[43]提出了一些克服上述攻击的方案,但他们没考虑到实现隐私保护和上下文环境感知会面临的额外挑战。PSN 信任管理应当克服上述这些传统的攻击和挑战,并解决信任管理的顽健性和可信性问题。

4 综合研究模型

4.1 PSN 系统模型

可信 PSN 研究模型如图 1 所示,PSN 系统包含 2 种实体:PSN 节点和服务提供者(SP)(如 Facebook 和 LinkedIn)。PSN 节点彼此间可以进行交互从而完成即时通信或一些在线的社交活动,这种交互可以借助于互联网、蜂窝移动网、MANET 或其他网络来实现;SP 可以通过互联网来提供在线服务,也可以充当信任代理中心(TA)。PSN 中的 TA 具有 PSN 节点所不具备的功能和强大的计算能力,PSN 节点可以信任并将自己的真实身份提供给 TA。TA 收集 PSN 节点用户的社交表现和行为数据从而执行信任和信誉评估。为了节约计算资源及降低处理负载,PSN 节点有可能借助 TA 来完成身份和密钥管理并维护信任关系,从而确保不同情况下的社交安全。为了能够实现 PSN 通信信息的完整性和隐私保护,使用匿名的节点应该能够相互认证。

假设 TA 是可信和可依靠的,并且 TA 会采用安全隐私保护技术来保护节点的隐私数据。这一假设是基于 TA 的商业动机和利益。假设 TA 拥有充足的存储能力和计算能力。PSN 节点除了在 TA 注册,在正常通信时并不需要连接到 TA。PSN

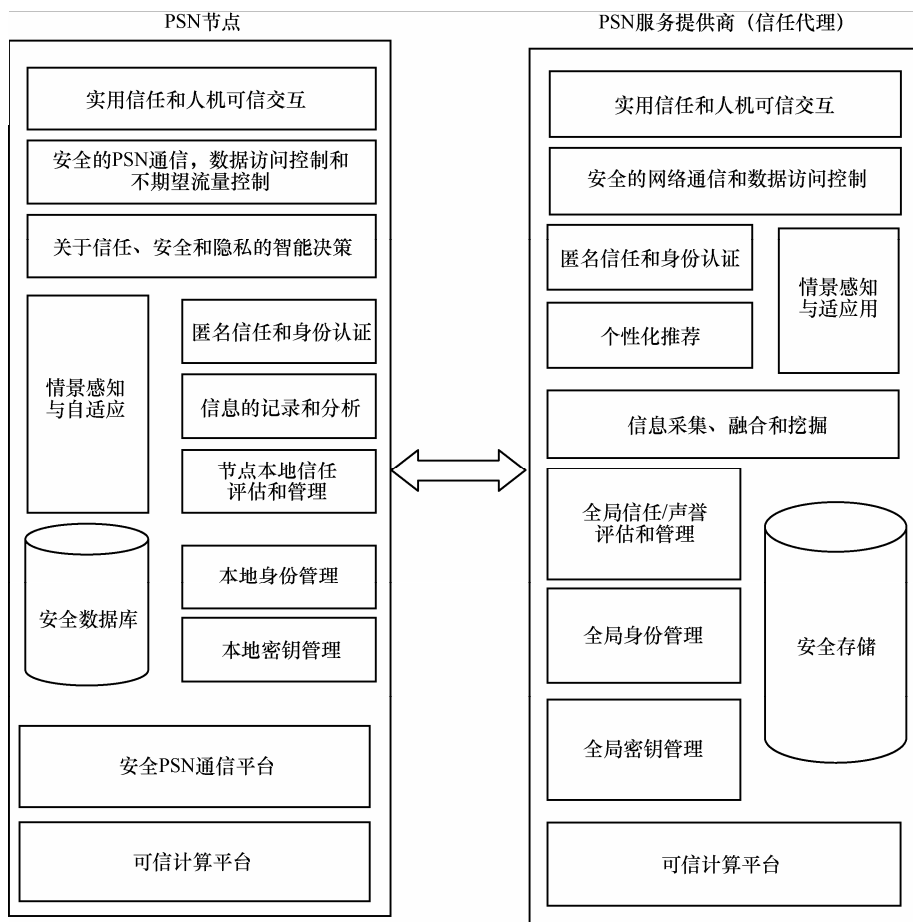


图1 可信PSN研究模型

节点使用自己的唯一真实身份向TA注册，当发生纠纷时，TA可以把节点在PSN中使用的匿名映射到它的真实身份，从而能够解决纠纷。一般来说，PSN中的节点用户可能并不互相信任对方，加上他们彼此大多是陌生人，所以PSN不允许委托行为。这里并不考虑PSN中的支付问题。显然，PSN系统中允许出现多个TA。

4.2 研究目标

基于上述系统模型实现可信普适社交，未来PSN信任管理研究应该实现以下目标。1) 灵活性和综合性：不论PSN中SP或TA是否可以连接，信任信誉管理都应该是灵活而有效的。信任管理系统可以灵活地以集中或分布式的方式进行信任信誉评估。2) 隐私保护：不管是用户数据还是其个人信息，用户的隐私都应该根据PSN用户指定的策略灵活地进行保护。3) PSN通信数据安全：PSN应该能够智能、有效地实现通信数据的访问控制。4) 可信身份管理：系统实体的身份标识(包

括唯一身份信息或匿名)应该能够以一种可信且高效的方式进行认证。5) 系统的安全性和顽健性：PSN的信任管理系统应能够抵抗各种系统攻击从而得到PSN用户的信任。6) 通用性：针对不同PSN应用和服务，信任管理应该是通用和普遍适用的。7) 可用性：信任管理提供了良好的可用性从而易于移动用户接受。

4.3 可信PSN研究模型

为了全面实现可信普适社交网络，本文提出了一个综合研究模型，如图1所示。基于可信计算平台，安全存储和安全互联网、D2D(device-to-device)通信和移动自组网等技术，将研究PSN信任管理的各种机制，包括信任和信誉评估、身份和密钥管理、信息收集和融合、数据分析和挖掘、社交情景自适应机制、个性化和具有情景感知的隐私/信任/安全推荐机制、匿名信任和身份认证、PSN通信数据访问控制和不期望信息控制、人机可信交互和实用信任管理方法。

此外,本文的研究将集成信任评估与 PSN 隐私和安全机制,运用信任评估结果,智能地进行密钥和身份管理、匿名身份和信任认证、数据访问控制和不希望信息控制。

在之前的工作中,提出了支持上下文环境感知、信任/信誉评估、可信推荐、安全通信、不希望信息控制和用户隐私推荐的混合信任管理框架^[38,40,50,51,62,77,80]。同时,为了加强可信度,也提出了一些其他的 PSN 信任管理和隐私保护技术^[41,82]。通过一系列的仿真、原型系统实现和用户使用体验证明了所提出的解决方案的有效性,在分析过程中,主要关注精度、效率、顽健性、可用性和用户接受程度^[38,40,50,51,62]。然而,诸如匿名身份/信任认证、具有隐私保护的社交数据融合和挖掘、人机可信交互等其他关键问题还没有被进一步研究。本文所提出的研究模型能够对未来的可信普适社交网络研究起到指导作用。

5 结束语

社交网络已经从互联网发展到移动领域。PSN 可以通过 MANET、移动网、互联网等网络进行搭建,支持无处无时不在的社交通信,是对传统的社交网络的有益补充。但是现有的研究没有对 PSN 的信任、隐私和安全问题进行深入探讨。本文认为,信任/信誉是解决 PSN 安全和隐私难题的出发点,而传统的信任管理机制由于对 PSN 网络异构特性并不适用,以往的工作很少在考虑信任的同时充分保护用户隐私。本文从信任和信誉机制、信誉系统架构、信任信息同步、不希望信息控制、隐私保护推荐等方面综述了可信普适社交网络研究现状,分析了现有工作的优势与不足,并讨论了实现可信 PSN 的几个关键科学问题,如自适应的访问控制和密钥管理、增强隐私的信任管理系统、不希望内容控制、上下文自适应的安全推荐系统等。此外,为全面实现可信普适社交网,提出了一个综合的信任管理研究模型,该模型有助于结构化、系统化地研究全面而通用的 PSN 信任管理方案。普适社交网是一个全新的应用领域,是未来 5G 移动通信网络的应用典范,将在未来移动网络领域起到重要作用。然而,信任管理对 PSN 成败至关重要。本文对 PSN 的信任、安全和隐私

等问题进行了深入探讨,并展示了部分前期工作和解决方案。要真正实现可信普适社交网络,还有更多的问题和挑战亟待解决,比如匿名身份和信任认证、高效的社交隐私数据保护、自适应上下文环境的自治信任管理、可信的 PSN 通信平台、可用性以及良好的用户体验支持等。

参考文献:

- [1] YAN Z. Trust management in mobile environments-usable and autonomic models[J]. Register, 2013(1): 2.
- [2] GUO Z, YAN Z, WANG F. A methodology to predicate human-being's movement based on movement group[C]//2010 IEEE/ACM International Conference on Green Computing and Communications (GreenCom) and International Conference on Cyber, Physical and Social Computing (CPSCom). c2010: 612-619.
- [3] Familiar stranger[EB/OL]. <http://www.paulos.net/research/intel/familiar-strange/index.htm>.
- [4] Junction, stanford mobisocial group[EB/OL]. <http://openjunction.org/>.
- [5] Microblog[EB/OL]. <http://synrg.ee.duke.edu/microblog.html>.
- [6] SARIGOL E, RIVA O, STUEDI P, et al. Enabling social networking in ad hoc networks of mobile phones[J]. Proceedings of the VLDB Endowment, 2009, 2(2): 1634-1637.
- [7] HYYTIA E, VIRTAMO J, LASSILA P, et al. When does content float? characterizing availability of anchored information in opportunistic content sharing[C]//IEEE International Conference on Computer Communications. c2011: 3137-3145.
- [8] Ezsetup[EB/OL]. <http://research.microsoft.com/enus/groups/wn/mssn.a-spx>.
- [9] AHTIAINEN A, ARVI K K, KASSLIN M, et al. Awareness networking in wireless environments[J]. Vehicular Technology Magazine, 2009, 4(3): 48-54.
- [10] GONG J, TANG J, FONG A C M. ACTPred: activity prediction in mobile social networks[J]. Tsinghua Science and Technology, 2014, 19(3): 265-274.
- [11] YU Z, ZHOU X. Socially aware computing: concepts, technologies, and practices[M]//Mobile Social Networking. New York: Springer, 2014: 9-23.
- [12] 程瑶, 应凌云, 焦四辈, 等. 移动社交应用的用户隐私泄露问题研究[J]. 计算机学报, 2014, 37(1): 87-100.
CHENG Y, YING L Y, JIAO S B, et al. Research on user privacy leakage in mobile social messaging applications[J]. Chinese Journal of Computers, 2014, 37(1): 87-100.
- [13] 吕志泉, 洪澄, 张敏, 等. 面向社交网络的隐私保护方案[J]. 通信学报, 2014, 35(8): 23-32.
LV Z Q, HONG C, ZHANG M, et al. Privacy-perserving scheme for social networks[J]. Journal on Communications, 2014, 35(8): 23-32.
- [14] 霍峰, 孟小峰, 黄毅. PrivateCheckIn: 一种移动社交网络中的轨迹隐私保护方法[J]. 计算机学报, 2013, 36(4): 716-726.
HUO Z, MENG X F, HUANG Y. PrivateCheckIn: trajectory privacy-preserving for check-in services in MSNS[J]. Chinese Journal of Computers, 2013, 36(4): 716-726.

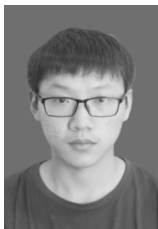
- [15] YAN Z. Trust modeling and management in digital environments: from social concept to system development: from social concept to system development[M]. IGI Global, 2010.
- [16] SUN Y L, YU W, HAN Z, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. Journal on Selected Areas in Communications, 2006, 24(2): 305-317.
- [17] THEODORAKOPOULOS G, BARAS J S. On trust models and trust evaluation metrics for ad hoc networks[J]. Journal on Selected Areas in Communications, 2006, 24(2): 318-328.
- [18] YAN Z, HOLTMANN S. Trust modeling and management: from social trust to digital trust[J]. Examining the Concepts Issues & Implications of Internet Trolling, 2008: 290-323.
- [19] SONG S, HWANG K, ZHOU R, et al. Trusted P2P transactions with fuzzy reputation aggregation[J]. Internet Computing, 2005, 9(6): 24-34.
- [20] RESNICK P, ZECKHAUSER R. Trust among strangers in internet transactions: empirical analysis of ebay's reputation system[J]. The Economics of the Internet and E-commerce, 2002, 11(2): 127-157.
- [21] XIONG L, LIU L. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities[J]. Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [22] LI J, LI R, KATO J. Future trust management framework for mobile ad hoc networks[J]. Communications Magazine, 2008, 46(4): 108-114.
- [23] WALSH K, SIRER E G. Fighting peer-to-peer spam and decoys with object reputation[C]//The 2005 ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems. c2005: 138-143.
- [24] 李建欣, 怀进鹏, 李先贤, 等. DTM:一种面向网络计算的动态信任管理模型[J]. 计算机学报, 2009, 32(3): 493-505.
LI J X, HUAI J P, LI X X, et al. DTM: a dynamic trust management model for internet computing environments[J]. Chinese Journal of Computers, 2009, 32(3): 493-505.
- [25] 李致远, 王汝传. P2P 电子商务环境下的动态安全信任管理模型[J]. 通信学报, 2011, 32(3):50-59.
LI Z Y, WANG R C. Dynamic secure trust management model for P2P e-commerce environments[J]. Journal on Communications, 2011, 32(3):50-59.
- [26] 胡建理, 周斌, 吴泉源. P2P 网络中具有激励机制的信任管理研究[J]. 通信学报, 2011, 32(5): 22-32.
HU J L, ZHOU B, WU Q Y. Research on incentive mechanism integrated trust management for P2P networks[J]. Journal on Communications, 2011, 32(5): 22-32.
- [27] 罗俊海, 范明钰. 基于置信度的 MANETs 主观信任管理模型[J]. 计算机研究与发展, 2010, 47(3): 515-523.
LUO J H, FAN M Y. A subjective trust management model based on certainty-factor for MANETs[J]. Journal of Computer Research and Development, 2010, 47(3): 515-523.
- [28] 郭晶晶, 马建峰, 李琦, 等. 基于博弈论的移动自组织网络的信任管理方法[J]. 通信学报, 2014, 35(11):50-58.
GUO J J, MA J F, LI Q, et al. Game theory based trust management method for mobile ad hoc networks[J]. Journal on Communications, 2014, 35(11): 50-58.
- [29] TRIFUNOVIC S, LEGENDRE F, ANASTASIADES C. Social trust in opportunistic networks[C]//IEEE Conference on Computer Communications Workshops. c2010: 1-6.
- [30] DOUCEUR J R. The sybil attack[C]//The First International Workshop on Peer-to-Peer Systems, Cambridge, MA. Berlin Heidelberg: Springer, 2002: 251-260.
- [31] SUN Y L, HAN Z, YU W, et al. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks[C]//IEEE Conference on Computer Communications Workshops. c2006: 1-13.
- [32] RAYA M, PAPADIMITRATOS P, GLIGOR V D, et al. On data-centric trust establishment in ephemeral ad hoc networks[C]//The 27th Conference on Computer Communications. c2008: 1912-1920.
- [33] YAN Z, NIEMI V. A methodology towards usable trust management[C]//The 6th International Conference on Autonomic and Trusted Computing, Brisbane. Berlin Heidelberg: Springer, 2009: 179-193.
- [34] PAVLOV E, ROSENSCHEIN J S, TOPOL Z. Supporting privacy in decentralized additive reputation systems[C]//The Second International Conference on Trust Management, Oxford. Berlin Heidelberg: Springer, 2004: 108-119.
- [35] YAO D, TAMASSIA R, PROCTOR S. Private distributed scalar product protocol with application to privacy-preserving computation of trust[M]//Trust Management. 2007: 1-16.
- [36] MELCHOR C A, AIT-SALEM B, GABORIT P. A collusion-resistant distributed scalar product protocol with application to privacy-preserving computation of trust[C]//The Eighth IEEE International Symposium on Network Computing and Applications. c2009: 140-147.
- [37] NITHYANAND R, RAMAN K. Fuzzy privacy preserving peer-to-peer reputation management[J]. IACR Cryptology ePrint Archive, 2009: 442.
- [38] YAN Z, CHEN Y, SHEN Y. A practical reputation system for pervasive social chatting[J]. Journal of Computer and System Sciences, 2013, 79(5): 556-572.
- [39] FUJIMURA K, NISHIHARA T. Reputation rating system based on past behavior of evaluators[C]//The 4th ACM Conference on Electronic Commerce. c2003: 246-247.
- [40] YAN Z, CHEN Y, SHEN Y. PerContRep: a practical reputation system for pervasive content services[J]. The Journal of Supercomputing, 2014, 70(3): 1051-1074.
- [41] YAN Z, DING W, NIEMI V, et al. Two schemes of privacy-preserving trust evaluation[J]. Future Generation Computer Systems, 2015(12).
- [42] JØSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems, 2007, 43(2): 618-644.
- [43] SUN Y, HAN Z, LIU K J R. Defense of trust management vulnerabilities in distributed networks[J]. Communications Magazine, 2008, 46(2): 112-119.
- [44] BUCHEGGER S, Boudec J Y L. Performance analysis of the CONFIDANT protocol[C]//The 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing. c2002: 226-236.
- [45] MICHARDI P, MOLVA R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[C]//The Sixth Joint Working Conference on Communications and Multimedia Security. 2002: 107-121.
- [46] BUCHEGGER S, BOUDEC J L. The effect of rumor spreading in reputation systems for mobile ad-hoc networks[C]//WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Net-

- works. c2003.
- [47] 田俊峰, 田瑞. 基于领域和贝叶斯网络的 P2P 电子商务细粒度信任模型[J]. 计算机研究与发展, 2011, 48(6): 974-982.
- TIAN J F, TIAN R. A fine-grain trust model based on domain and bayesian network for P2P e-commerce system[J]. Journal of Computer Research and Development, 2011, 48(6): 974-982.
- [48] RESNICK P, KUWABARA K, ZECKHAUSER R, et al. Reputation systems[J]. Communications of the ACM, 2000, 43(12): 45-48.
- [49] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]//The 1996 IEEE Symposium on Security and Privacy. c1996: 164-173.
- [50] YAN Z, ZHANG P. AdPriRec: a context-aware recommender system for user privacy in MANET services[M]//Ubiquitous Intelligence and Computing. Berlin Heidelberg: Springer, 2011: 295-309.
- [51] YAN Z, CHEN Y. AdContRep: a privacy enhanced reputation system for MANET content services[C]//The 7th International Conference on Ubiquitous Intelligence and Computing, Beijing. Berlin Heidelberg: Springer, 2010: 414-429.
- [52] BANSAL S, BAKER M. Observation-based cooperation enforcement in ad hoc networks[R]. 2003.
- [53] HU J, BURMESTER M. LARS: a locally aware reputation system for mobile ad hoc networks[C]//The 44th Annual Southeast Regional Conference. c2006: 119-123.
- [54] ZHELEVA E, KOLCZ A, GETOOR L. Trusting spam reporters: a reporter-based reputation system for email filtering[J]. ACM Transactions on Information Systems (TOIS), 2008, 27(1): 1139-1141.
- [55] ZHANG J Z, XU W, PENG Y D, et al. MailTrust: a mail reputation mechanism based on improved trustguard[C]//The 2010 International Conference on Communications and Mobile Computing (CMC). c2010: 218-222.
- [56] ZHANG H, DUAN H, LIU W, et al. IPGroupRep: a novel reputation based system for anti-spam[C]//Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing. c2009: 513-518.
- [57] BI J, WU J, ZHANG W. A trust and reputation based anti-spam method[C]//IEEE International Conference on Computer Communications. c2008: 2485-2493.
- [58] TANG Y, KRASSER S, HE Y, et al. Support vector machines and random forests modeling for spam senders behavior analysis[C]//Global Telecommunications Conference. c2008: 1-5.
- [59] WU B, GOEL V, DAVISON B D. Topical trustrank: using topicality to combat web spam[C]//The 15th International Conference on World Wide Web. c2006: 63-72.
- [60] KOLAN P, DANTU R. Socio-technical defense against voice spamming[J]. ACM Transactions on Autonomous and Adaptive Systems (TAAS), 2007, 2(1): 130-138.
- [61] YAN Z, KANTOLA R, SHEN Y. A generic solution for unwanted traffic control through trust management[J]. New Review of Hypermedia and Multimedia, 2014, 20(1): 25-51.
- [62] MA S, YAN Z. PSNcontroller: an unwanted content control system in pervasive social networking based on trust management[J]. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2015, 12(1s): 17.
- [63] O'DONOVAN J, SMYTH B. Trust in recommender systems[C]//The 10th International Conference on Intelligent User Interfaces. c2005: 167-174.
- [64] RESNICK P, VARIAN H R. Recommender systems[J]. Communications of the ACM, 1997, 40(3): 56-58.
- [65] LUO Y, LE J, CHEN H. A privacy-preserving book recommendation model based on multi-agent[C]//The Second International Workshop on Computer Science and Engineering. c2009: 323-327.
- [66] POLAT H, DU W. Privacy-preserving top-n recommendation on horizontally partitioned data[C]//The 2005 IEEE/WIC/ACM International Conference on Web Intelligence. c2005: 725-731.
- [67] YU Z, ZHOU X, ZHANG D, et al. Supporting context-aware media recommendations for smart phones[J]. Pervasive Computing, 2006, 5(3): 68-75.
- [68] ZHANG D, YU Z. Spontaneous and context-aware media recommendation in heterogeneous spaces[C]//The 65th Vehicular Technology Conference. c2007: 267-271.
- [69] 王珣, 高琳. 基于社交圈的在线社交网络朋友推荐算法[J]. 计算机学报, 2014(4): 801-808.
- WANG Y, GAO L. Online social network friends recommendation algorithm based on social network[J]. Chinese Journal of Computers, 2014(4): 801-808.
- [70] 黄震华, 张波, 方强. 一种社交网络群组间信息推荐的有效方法[J]. 电子学报, 2015, 43(6): 1090-1093.
- HUANG Z H, ZHANG B, FANG Q. An efficient algorithm of information recommendation between groups in social networks[J]. Acta Electronica Sinica, 2015, 43(6): 1090-1093.
- [71] ZOURIDAKI C, MARK B L, HEJMO M, et al. Robust cooperative trust establishment for MANETs[C]//The Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks. c2006: 23-34.
- [72] PUTTASWAMY K P N, ZHAO B Y. Preserving privacy in location-based mobile social applications[C]//The Eleventh Workshop on Mobile Computing Systems & Applications. c2010: 1-6.
- [73] CHEN G, RAHMAN F. Analyzing privacy designs of mobile social networking applications[C]//IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. c2008: 83-88.
- [74] BEACH A, GARTRELL M, HAN R. Solutions to security and privacy issues in mobile social networking[C]//International Conference on Computational Science and Engineering. c2009: 1036-1042.
- [75] SADEH N, HONG J, CRANOR L, et al. Understanding and capturing people's privacy policies in a mobile social networking application[J]. Personal Ubiquitous Computing, 2009, 13(6): 401-412.
- [76] MILUZZO E, LANE N D, FODOR K, et al. Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application[C]//The 6th ACM Conference on Embedded Network Sensor Systems. c2008: 337-350.
- [77] CHIN A, ZHANG D Q. Mobile social networking: an innovative approach[M]. New York: Springer, 2014: 195-235.
- [78] YANG H, LUO H, YE F, et al. Security in mobile ad hoc networks: challenges and solutions[J]. Wireless Communications, 2004, 11(1): 38-47.
- [79] LUO H, KONG J, ZERFOS P, et al. URSA: ubiquitous and robust access control for mobile ad hoc networks[J]. IEEE/ACM Transactions on Networking (ToN), 2004, 12(6): 1049-1063.
- [80] YAN Z, WANG M. Protect pervasive social networking based on two-dimensional trust levels[J]. IEEE Systems Journal, 2014(9): 1-12.
- [81] YAN Z, WANG M, NIEMI V, et al. Secure pervasive social networking based on multi-dimensional trust levels[C]//The 2013 IEEE Conference on Communications and Network Security (CNS). c2013: 100-108.

- [82] YAN Z, FENG W, WANG P. Anonymous authentication for trustworthy pervasive social networking[J]. IEEE Transactions on Computational Social Systems, 2016(11): 1-11.
- [83] LIU X, FANG Z, SHI L. Securing vehicular ad hoc networks[C]//The 2nd International Conference on Pervasive Computing and Applications. c2007: 424-429.
- [84] LIN X, SUN X, WANG X, et al. TSVC: timed efficient and secure vehicular communications with privacy preserving[J]. IEEE Transactions on Wireless Communications, 2008, 7(12): 4987-4998.
- [85] KELLEY P G, BREWER R, MAYER Y, et al. An investigation into facebook friend grouping[C]//The 13th IFIP TC 13 International Conference on Human-Computer Interaction, Lisbon. c2011: 216-233.
- [86] CISZKOWSKI T, KOTULSKI Z. Distributed reputation management in collaborative environment of anonymous MANETs[C]//The International Conference on "Computer as a Tool". c2007: 1028-1033.

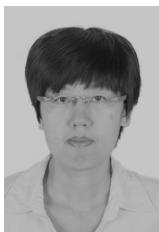


吴宸梓 (1990-), 男, 陕西西安人, 西安电子科技大学硕士生, 主要研究方向为社交网络安全。



冯伟 (1992-), 男, 河北沧州人, 西安电子科技大学博士生, 主要研究方向为信息安全、隐私保护、信任管理。

作者简介:



闫峥 (1972-), 女, 陕西西安人, 西安电子科技大学教授、博士生导师, 主要研究方向为网络与信息安全、信任管理和可信计算、隐私保护。



王子龙 (1982-), 男, 河南新郑人, 西安电子科技大学副教授, 主要研究方向为信息论与密码学。