

移动网络中场景关联的隐私保护机制研究

牛犇, 李凤华, 华佳烽, 何媛媛

(中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093)

摘要: 信息服务的发展已经广泛渗透到人们生活的各个方面, 各种新型服务模式及应用给人们带来便利的同时无形中泄露了隐私信息, 且应用程序的激增和用户需求的多样化给隐私保护带来了更大挑战。结合国内外相关最新研究趋势, 对移动网络中与场景关联的隐私保护问题进行了研究展望。首先介绍了移动网络中场景关联的隐私保护应用场景、服务模型、攻击模型, 以及所面临的隐私威胁; 其次介绍了背景信息、服务质量和资源消耗关联的隐私保护研究现状; 最后提出了背景信息建模与描述、多源背景信息融合方法、移动网络服务中的服务质量描述与建模、基于历史信息的自适应方法、隐私保护中的资源消耗优化算法和多因素均衡的隐私保护机制等研究方向。

关键词: 移动网络; 隐私保护; 背景信息; 服务质量; 能耗

中图分类号: TN929

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00005

Research on scenario-based mechanism in privacy-aware mobile networks

NIU Ben, LI Feng-hua, HUA Jia-feng, HE Yuan-yuan

(State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: The well-developed information services has infiltrated in each part of our daily life, various novel service modes and applications provide us conveniences at the cost of our privacy. This situation becomes more serious with the increasing number of applications and users' requirements. The privacy issues of scenario-based mechanism in mobile networks have been studied based on analyzing the state-of-the-art research trends. The threat and challenges of privacy disclosure caused by the mobile network services, and review the scenarios, service models and attack models were introduced firstly. Followed, a comprehensive study on current status of background information, quality of services, and resource-restricted related privacy preservation were made. Finally, some key technologies on privacy preservation such as background information modeling and describing, multi-background information fusion, quality of services describing and modeling, self-adaptive methods based on historical information, privacy-preserving solutions optimizing energy resources and privacy-preserving schemes equalizing multiple factors etc were posted.

Key words: mobile networks; privacy preservation; background information; quality of services; resource consumption

收稿日期: 2015-09-12; 修回日期: 2015-09-26。通信作者: 李凤华, lfh@iie.ac.cn

基金项目: 国家自然科学基金青年科学基金资助项目(61502489); 国家高技术研究发展计划(“863”计划)基金资助项目(2015AA016007)

Foundation Items: The National Natural Science Youth Science Foundation of China (61502489); The National High Technology Research and Development Program of China (863 Program) (2015AA016007)

1 引言

信息技术、移动通信技术的紧密结合与快速发展,以及智能移动终端软硬件的不断升级与换代,孕育并产生了信息通信技术(ICT, information and communication technology)和各种新的服务模式。移动网络(MNS, mobile network services)已经从众多新的服务模式和应用中脱颖而出,其应用软件随用户需求不断提升的爆炸式增长态势为人们生活带来无微不至的便利。移动网络中的用户不仅可以随时随地获取相关服务(比如订票、购物、查找最近的餐馆、酒店等),还可以发现近邻好友,在某个语义位置签到,分享照片及旅行轨迹等。

然而,移动网络为人们生产和生活带来便利的同时,也会直接、间接地泄漏用户身份、位置、健康状况和银行账号等敏感信息,对用户造成经济、名誉损害,甚至生命威胁。移动网络环境中的安全与隐私泄漏问题已成为社会关注的热点问题。除了传统的网络安全问题之外,移动网络中还存在针对各种类型应用服务的攻击风险,如数据挖掘、与身份有关的攻击等。移动网络中应用种类多样,隐私信息来源众多,这些信息之间相互补充,如果敌手对用户在不同时间、不同空间、不同查询请求以及区域兴趣点分布、社交关系等信息进行收集并做融合分析,用户的个人隐私将

无从谈起,成为透明人。

面对这类威胁,移动网络中场景关联的隐私保护机制全面地控制用户隐私信息的泄漏。由于移动网络日益突显出不同场景中的背景信息复杂化(本文称之为广义背景信息)、隐私保护与服务质量相矛盾和资源利用率不高等特征,移动网络中场景关联的隐私保护机制需要针对以上特征进行系统化研究,以确保用户隐私,更好地服务大众。

2 场景关联的隐私保护机制

2.1 应用场景

以图1为例说明移动中场景关联的隐私保护机制的典型应用场景:一名医生在医院工作时用iPad随时查阅业务信息;下班后使用iPhone接收打折券,使用滴滴打车回家;回家途中使用iPhone查询交通路况,以便优化行车路线或浏览购物优惠信息;睡前通过iPad或iPhone访问病人电子病历和自己的股票行情。

在此过程中,用户享受到了各种移动网络应用服务带来的无限便利,然而隐私泄漏问题也异常严重。如若隐私保护工作不到位,敌手很容易获取用户的身份(从医人员)、工作地点(医院)、家庭住址和喜好(购物、炒股)等信息,可以推演得到用户的休息习惯以实施盗窃、得到用户的行动轨迹以实施跟踪抢劫等,甚至会推理得到该用户的银行账号信息、社会地位和宗教信仰等敏

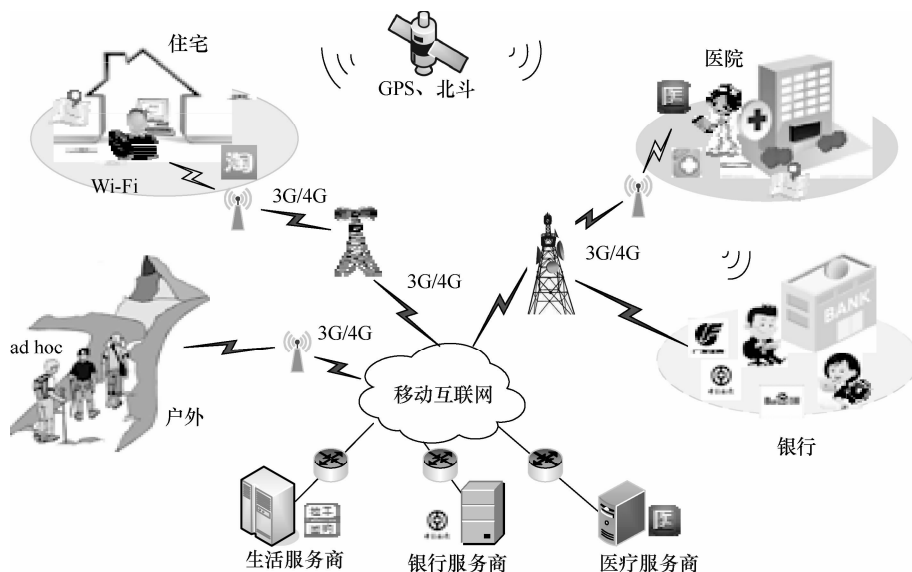


图1 基于移动网络的应用场景

感信息。尤其是敌手如果将上述信息融合分析，对用户的安全和隐私问题将构成异常严峻的威胁。

目前，移动网络环境中敌手对用户个人信息的采集日趋便捷和全面，范围涵盖身份类、交易类（消费与金融活动等）、互动类（网络言论与即时通信等）、社交关系类（通讯录与社交网络等）、观测类（地理位置等）等，各类数据的关联整合可以准确地还原并预测个人的社会生活全貌。长此以往，移动网络中无处不在的隐私泄露风险将严重影响人们对于各种应用服务的热情。因此，亟需研究场景关联的隐私保护机制，力求为用户提供全面的、个性化的隐私保护，从而吸引更多的用户愿意将个人数据提交给智能交通、智能城市等相关服务提供商，进而为人们的日常生活提供更多的便利，形成产业链的良性循环。

2.2 服务模型与攻击者模型

典型的移动网络系统服务模型如图2所示。该模型由4个主要部分构成：移动设备、网络运营商、服务提供商、第三方系统（定位系统、认证系统等）。

1) 移动设备

具备互联网接入和常用存储等功能，通常搭

载各种操作系统的便携式终端，例如智能手机、平板电脑、可穿戴设备等。

2) 网络运营商

进行网络运营和提供服务的实体，不仅需要网络角度知道网络运行状况，还需要从服务角度知道网络运行状况，例如中国移动、中国联通、中国电信、at&t等。

3) 服务提供商

移动互联网服务内容、应用服务的直接提供者，常指电信增值业务提供商，负责根据用户的要求开发和提供适合手机用户使用的服务，例如百度地图、淘宝、微信、Facebook等。

4) 第三方系统

提供移动服务相关应用数据的增值服务，例如，在基于位置的服务中，GPS、北斗等定位系统可以通过用户随身携带的移动智能终端设备（例如智能手机、平板电脑、可穿戴设备等）进行定位，进而获取相关位置服务数据（例如附近餐馆或者距离当前位置最近的银行）。常见的第三方系统包括定位系统、认证系统等。

从网络架构方面考虑，当前方案主要分为集中式网络架构和分布式网络架构。集中式网络架构往往需要依赖一个可信第三方（TTP，

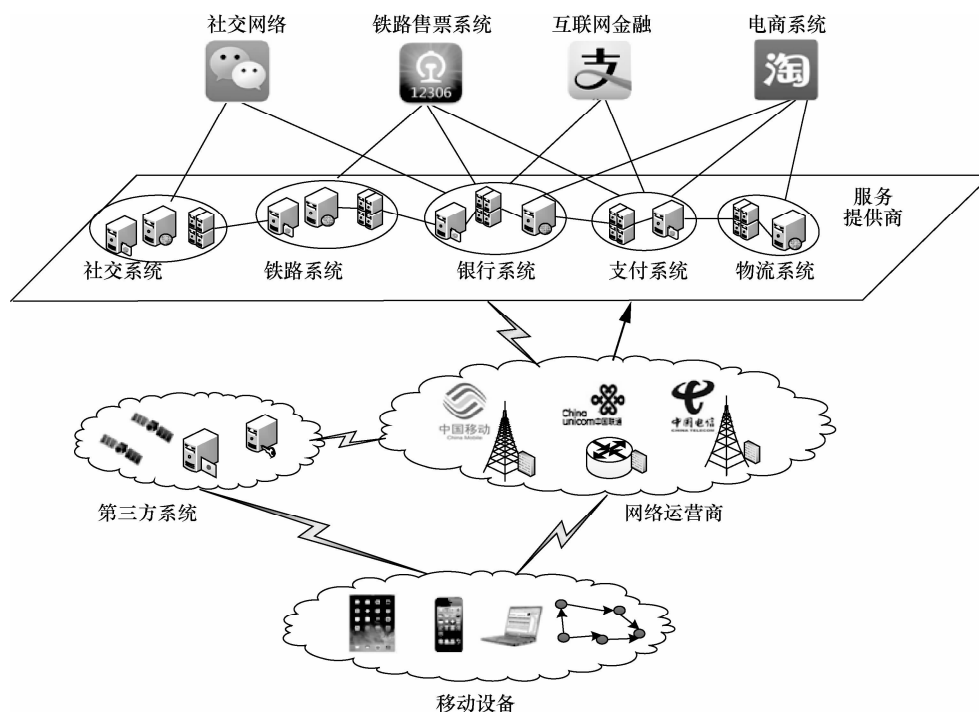


图2 移动网络系统服务模型

trusted third party), 用户将请求的服务内容与身份及当前位置等信息发送给 TTP, 由 TTP 根据用户发送的请求信息及用户当前位置信息做相应处理变换, 之后再连同服务请求内容一起发送给服务提供商。服务提供商对用户的身份信息进行验证, 并将查询到的服务信息返回到 TTP, TTP 经过过滤最终返回给用户。这种网络架构的解决方案存在的隐患相对较多且较为明显, 集中表现在需要可信第三方的支持, 难以提供对用户身份信息的保护, 不能同时保护兴趣信息和位置信息, 不支持连续场景下的隐私保护, 且大都不支持移动设备, 因而不适合在移动互联网中广泛应用。

与此同时, 有一些隐私保护技术并不依赖于 TTP, 其基本思想主要集中于用户和其他用户之间的相互交互, 通过 peer-to-peer (P2P) 或者 encounter-based 等方式实现匿名集的构造, 实现对用户隐私的保护。Chow 等人^[1]提出了一种基于 P2P 的解决方案, 通过用户的相互协作, 用近距离通信标准 (Wi-Fi 或蓝牙技术) 实现用户之间的信息交换, 在考虑用户的最大移动距离的基础上, 实现连续场景下的 k -anonymity, 以保护用户的位置隐私。然而由于用户的移动模式和近距离通信的通信距离限制, 使得用户真实的位置会以较大概率落在匿名集的中心区域。

移动网络中用户隐私发动的攻击行为通常表现为合法用户通过分析传输数据及其传输时间、频率等信息窥探用户隐私的“被动式”攻击和对加密数据进行破坏、解密、伪造或者插入数据标志进行的“主动式”攻击。现有的隐私保护方案主要考虑以下两类攻击模型。

诚实且好奇 (HBC, honest but curious)^[2]攻击模型: HBC 用户能诚实地执行既定方案, 但是, 用户会分析方案执行过程中获得的所有信息, 试图获得对方更多的隐私信息。

恶意 (malicious)^[2]攻击模型: 恶意攻击者可以通过有策略地输入位置、兴趣偏好等恶意信息发起攻击或实行共谋, 多渠道收集用户信息并融合分析以获取用户隐私信息。

2.3 场景关联的隐私保护面临的威胁

在移动网络应用的不同场景中, 敌手可能

获取当前地图上的道路、用户、兴趣点等分布情况, 以及用户查询分布和历史查询情况等背景信息。背景信息是否为敌手所知是大多数基于匿名或混淆等隐私保护方案的一个关键假设。早期的工作往往会忽略背景信息, 认为敌手和用户拥有近似的知识储备, 只在计算能力等方面有所差别。然而, 现实生活中愈发透明化的网络为所有人, 尤其是蓄谋已久的敌手提供了丰富的先验知识, 使他们能够通过搜集、融合分析等方式获取更加复杂的背景信息, 提升获取用户隐私信息的能力。为了更好地保护用户隐私, 需要更加精准的隐私保护方案对用户信息进行细粒度保护, 确保用户在不同场景下使用不同移动网络应用服务时的隐私信息不被泄漏。

移动网络中现有的隐私保护方案在具体实施过程中往往会忽略掉各种应用对服务质量的需求, 以及用户采用不同隐私保护方案时对服务质量的需求和影响 (例如天气预报服务只需要获取用户所处的地区或城市即可, 而滴滴打车等服务则需要获取用户比较精确的位置信息), 而直接提供用户的实时位置和请求内容等信息, 无形中造成了用户隐私的泄漏。尤其是当用户频繁使用多个服务应用时, 多维度的隐私泄漏无疑会使敌手采用关联分析攻击的成功率大增, 使用户隐私信息面临严峻威胁。因此, 服务质量与隐私保护力度的自适应问题已成为基于移动网络的隐私保护技术需要考虑的核心问题之一。

在移动网络环境中, 用户所持终端设备的资源消耗状态不同, 也使得用户当前的隐私保护需求不尽相同。例如, 当用户身处公共场所且智能手机电量不足时 (隐私需求较低, 但需要低运算量和低传输量), 身处户外但有 Wi-Fi 接入时 (不在乎网络流量, 但需要低能耗) 与在家中用 iPad 远程访问医疗信息或银行账号时 (不在乎计算量和网络流量, 但需较高级别的隐私保护) 等, 用户使用的隐私保护方案截然不同。考虑到目前移动网络应用大都集中于智能设备上, 为了达到隐私保护目的, 不同隐私保护方案对智能设备上各种资源的消耗不尽相同。例如, 在智能设备确定的前提下, 基于加解密的隐私保护方案需要相对

较多的计算资源、基于 k -匿名的匿名方案需要较多的存储和传输开销等。基于此，传统的面向某种特定场合或应用的隐私保护方案、通过调整算法参数的隐私保护方案或者多方案堆叠的隐私保护方案将难以应对不断革新的用户隐私需求。尤其当用户面临不同场景时，如何均衡隐私保护效果和资源消耗，以及针对不同场景采用不同的隐私保护方案使对用户隐私信息的保护显得更加有意义。然而，现有的隐私保护方案缺乏对上述诸多因素的综合考虑，难以为用户提供资源优化的隐私保护。

综上，移动网络中场景关联的隐私保护机制旨在针对不同的服务质量需求，以不同的资源消耗代价，对不同的隐私信息采用不同的保护方案，实现不同的隐私保护效果。对此，需要考虑以下3个具有挑战性的问题。

- 1) 如何确保用户在敌手拥有不同背景信息下的隐私保护效果。
- 2) 如何根据用户对移动网络应用的服务质量需求，个性化地提供隐私保护方案。
- 3) 如何基于用户所持移动设备当前的资源

消耗状态提供不同级别的隐私保护解决方案，以提升用户体验。

3 场景关联的隐私保护研究进展

移动网络中的隐私保护受多方面因素影响，现有场景关联的隐私保护机制主要从以下3个方面开展研究：背景信息关联的隐私保护方案、服务质量关联的隐私保护方案和资源消耗关联的隐私保护方案。其中，基于背景信息关联的隐私保护方案研究旨在为不同场景的用户提供各种隐私保护的新方法；服务质量关联的隐私保护方案满足服务质量要求各异的应用或用户需求，实现个性化的隐私保护；同时，考虑到移动终端有限的计算、存储、网络等资源，部分隐私保护方案在设计过程中引入了对资源消耗的优化，试图以较小的资源消耗实现适度的隐私保护效果。表1对现有相关工作进行了详细比对。

3.1 背景信息关联的隐私保护方案

大量文献对移动网络中的隐私保护问题进行了研究，Sweeney^[17]提出了一种 k -匿名技术，通过将每个对象唯一对应的准标识属性进行压缩、

表1 现有相关工作对比

隐私保护方法		是否基于可信第三方	密码方案	匿名	背景信息	服务质量	资源消耗
背景信息	Modeling and Integrating Background Knowledge in Data Anonymization ^[3]	否	否	是	是	是	否
	Local Differential Perturbations Location Privacy under Approximate Knowledge Attackers ^[4]	否	否	否	是	是	否
	位置大数据隐私保护研究综述 ^[5]	—	—	—	—	—	—
	Privacy Risks in Publishing Mobile Device Trajectories ^[6]	否	否	是	是	否	否
服务质量	Quality-of-Protection-Driven Data Forwarding for Intermittently Connected Wireless Networks ^[7]	是	否	否	否	是	是
	A Survey on Wireless Body Area Network: Security Technology and its Design Methodology issue ^[8]	否	是	否	否	是	是
	PrivateCheckIn:一种移动社交网络中的轨迹隐私保护方法 ^[9]	是	否	是	否	是	是
	基于位置服务中的连续查询隐私保护研究 ^[10]	否	否	是	否	是	否
	Exploring the Security Requirements for Quality of Service in Combined Wired and Wireless Networks ^[11]	否	是	否	否	是	否
资源消耗	Resource-Aware Secure ECG Healthcare Monitoring Through Body Sensor Networks ^[12]	否	是	否	否	否	是
	Privacy, Quality of Information, and Energy Consumption in Participatory Sensing Systems ^[13]	否	是	是	否	否	是
	Privacy-aware and Energy-efficient Geofencing through Reverse Cellular Positioning ^[14]	否	是	否	否	否	是
	面向社交网络的隐私保护方案 ^[15]	否	是	否	否	否	是
	A Survey of Green, Energy-Aware Security and Some of its Recent Developments in Networking and Mobile Computing ^[16]	—	—	—	—	—	—

泛化处理,使得攻击者想在匿名数据集中获得目标用户对应的元组之前,必须排除至少 $k-1$ 个元组。Machanavajjhala 等^[18]提出 l -多样性技术,它要求每个数据元组中至少对应 1 种敏感属性值,且在任意一个等价类中每个敏感属性值对应元组数所占比例不能超过规定限度。 k -匿名和 l -多样性在个体隐私保护方案中是简单有效的,但是容易受到同质攻击和背景知识攻击。Li 等^[19]在 k -匿名和 l -多样性的基础上提出了一种 t -closeness 技术,它要求每个等价类中敏感属性值的分布要尽可能地接近整个数据表中的分布,其防止相似性攻击、同质攻击、属性泄露方面的能力与 k -匿名和 l -多样性相比有所提高。

然而,在敌手拥有背景知识的情况下,这些方案无法保证个人的敏感属性值。目前,移动网络应用服务中隐私保护涉及到的背景信息一般指用户的访问时间、查询频率,以及某区域内的用户、道路、兴趣点或者用户查询请求的分布或者密度等信息。为了表达不同种类的背景知识,Martin 等^[20]提出一种通用描述语言,并在此基础上建立多项式时间算法,以度量敏感信息泄露的数目。Chen 等^[21]提出一种多维隐私标准,这种标准能够从多个维度度量敌手可能拥有的背景知识,同时要求数据组织在发布数据的过程中需要将背景知识考虑在内。Rinku 等^[4]对敌手可能掌握的不同类型背景信息进行分类,提出 Perturbation-based 机制,利用混淆方式保护用户的查询隐私。Alireza 等^[6]提出了一种新的匹配算法 Trajectory Finder,该算法通过增加噪声数据的方式有效地防止拥有背景知识的攻击者的攻击,从而保证数据的安全性。Li 等^[3]对敌手背景知识进行建模,结合基于 Kernel 评估机制的通用框架,通过贝叶斯推理技术提出 Skyline(B, t)隐私保护模型,该模型能够抵御拥有不同等级背景知识的敌手的攻击。

在移动网络应用服务的相关场景中,如何模型化攻击者的背景知识是设计隐私保护方案的关键。Zhou 等^[22]对此进行了综述,列举了多种背景知识,包括移动网络的节点属性、目标个体之间的链接关系、节点的度、目标个体的邻居结构、嵌入子图及图的特征等。Hay 等^[23,24]使用目标节

点的邻居结构信息作为背景知识,甚至用户对网络的浏览记录亦可作为攻击者的背景知识。Zou 等^[25]提出了一种 k -自同构图模型对图进行匿名化处理,这种匿名化模型处理的图可以有效地抵御各种基于节点拓扑结构的攻击模式。随后,涌现出了多种基于 k -匿名图和 k -自同构图的图匿名算法^[26-30]。Shen 等^[31]针对采用目标节点的邻居结构信息进行图匹配从而完成隐私发现的攻击模式,提出了一种基于马尔可夫蒙特卡洛的隐私保护方案,将图形匹配与差分隐私保护模型统一在马尔可夫蒙特卡洛模型中,有效地防御了使用邻居拓扑结构进行的攻击。马飞等^[32]综述了社交网络中的隐私保护方案,指出现有的研究主要针对静态社交网络,较少考虑社交网络的动态性。现有大多数隐私保护方案假设攻击者对用户的背景知识的掌握是固定的,然而,在大数据环境下,攻击者获取背景知识的渠道和途径十分广泛,可以持续地收集用户的历史数据从而具备学习用户背景知识的能力。因此,随着攻击者获取背景知识的方式越来越便捷,具备的背景知识越来越丰富,如何设计综合的、有效的、可扩展的隐私保护技术来保护实体、链接和属性隐私等敏感信息将面临越来越大的挑战。

为此,国内外许多学者将背景信息的含义进行了扩展,Niu 等^[33,34]定义背景信息为用户在特定区域发送位置服务请求的概率,并从该背景信息可能被敌手获取的问题入手,分析了隐私保护效果受到的影响,进而利用虚假信息及信息缓存等技术将历史查询信息进行存储以便重复利用,对用户隐私信息实现 k -匿名级别的保护。Niu 等^[2]建立隐私信息匹配方案时,综合考虑用户地理位置和社交关系等背景信息,在保证隐私保护效果的基础上,有效提升匹配效果。王璐等^[5]指出现有的基于概率推测的隐私保护技术不能有效地保护用户的隐私信息,差分隐私是迄今为止针对攻击者的先验知识进行普遍保护的最有效的技术,将差分隐私保护技术应用到背景知识攻击中具有广阔的前景。

差分隐私的研究主要集中在如何添加冗余数据干扰分析结果,主要的技术包括针对整数类型数据的 Laplace 机制^[35]、针对浮点类型数据的 Exponential 机制^[36]以及它们在性能上的改进

Geometric 机制^[37]等。2008 年, 为了解决准标识符和隐私属性存在交叉难以划分的问题, Dwork 提出了 (ϵ -差分隐私) 算法^[38,39], 直接对数据进行噪声处理, 避免攻击者获得真实的数据。近几年, 多种差分隐私保护模型相继被广泛地应用于数据挖掘领域的研究中^[40-43]。然而, 目前差分隐私技术主要应用于离线数据的隐私保护, 针对移动网络中的应用服务场景的差分隐私保护方案少见报道。

现有研究工作中对背景信息的考虑局限于某个特定时段或区域的历史查询概率、查询频率、人口密度以及道路密度等, 而现实生活中背景信息包括周边兴趣点分布、社交关系和时间因素等。为了更好地在不同场景下为用户提供更加精准的隐私保护, 需要将移动网络应用服务中背景信息的传统定义向含义更加丰富的广义背景信息拓展。

3.2 服务质量关联的隐私保护方案

移动网络中, 许多服务供应商积极收集用户的数据, 要求用户不断上传个人数据, 而不提供明确的陈述说明如何使用和共享数据, 这已经引起了对隐私保护的广泛关注。最近, 对 30 个最受欢迎 Android 应用程序的一项调查^[44]表明, 这些应用程序可以访问用户的位置、摄像头和麦克风数据, 其中有 15 个应用向远程广告或分析服务器发送用户信息, 用户隐私面临严峻威胁。然而, 如果用户拒绝将个人数据上传给服务提供商, 将无法享受这些应用提供的个性化服务。因此, 移动网络中的隐私保护亟需服务质量关联的隐私保护方案。

为了提供更好的用户体验, Ickin 等^[45]将情景感知的概念引入移动网络中的隐私保护。Wang 等^[46]关注隐私保护的长期效果, 研究基于情境感知的长期 QoP (quality of protection) 机制, 开发出 QoP 框架, 并将两者结合起来利用情景感知实现服务质量与隐私保护的长期均衡, 为移动网络中的用户提供个性化的隐私保护服务。Wu 等^[7]提出了一种 Trust-Status-Aware 数据转发策略, 在资源受限的移动网络环境下, 防止节点恶意消耗资源, 以提高网络的可靠性。Vikash 等^[8]分析了无线体域网中各种安全技术的优劣, 指出在计算资源和能量受限的环境下, 基于 ECC 的密码方案和生物识别系统具有更高的实用性和安全性,

以及更好的用户体验。Shokri 等^[47,48]提出了一种基于群组的用户隐私保护方案, 当前用户通过将所需查询在群组内转发, 由某一用户替代其向服务运营商发送服务请求, 从而以牺牲服务质量为代价换取隐私保护, 实现对当前用户身份信息、位置信息和兴趣信息的保护。CacheCloak^[49]引入了预测的概念, 通过分析用户历史轨迹等信息, 预测用户下一步的移动, 为用户提供实时的服务, 但预测的准确性直接影响服务质量。针对移动社交网络中假名用户的位置及轨迹隐私泄露问题, PrivateCheckIn^[9]方案设计了一种签到序列缓存机制为缓存的签到序列建立前缀树, 该机制既能保护假名用户的轨迹隐私, 又确保损失签到位置最少, 有效地保证了用户体验。

近几年, 大量文献开始探索服务质量与隐私保护效果之间的内在联系。潘晓等^[10]研究了基于位置服务中连续查询的隐私保护问题, 针对现有的静态匿名算法不适用于连续查询隐私保护, 产生查询隐私泄露、匿名服务器工作代价大等问题, 提出了“-隐私模型”和“-质量模型”来有效均衡隐私保护与服务质量, 实验表明基于该模型的贪心匿名算法可以在 2 ms 内匿名成功, 匿名成功率可达到 98%。Zubair 等^[11]对目前大多数隐私保护方案中安全参数 (例如加密、解密等) 和服务质量 (延迟等) 之间存在的矛盾进行讨论, 提出一种 QoS2 框架, 综合考虑隐私保护效果和服务质量, 在保证安全质量的前提下提高服务质量。Shumin 等^[50]针对社交网络中的用户提出了一个平衡算法来确定用户的隐私设置, 以同时满足用户的隐私需求和效用偏好。Ping 等人^[51]提出了一种增加噪声和分层聚类的数据匿名方法来抵抗概率推理攻击, 给出了关于隐私增益和效用损失的定义, 并利用它们对提出的匿名方法进行评测。Gu 等^[52]给出了关于隐私泄露和效用损失的概念, 并且利用概率论中的散度距离来量化它们。

综上, 现有工作大多需要引入可信/非可信第三方匿名服务器, 虽然方便管理, 但会成为系统瓶颈, 引起单点失效攻击。另外对隐私保护方案的选择不慎也会给终端设备带来严重的资源消耗问题, 很难真正实现隐私保护方案与服务质量的自适应。为了更好地面对复杂的应用场景和用户

在不同场景下对隐私和服务质量的个性化需求问题,需要深入研究隐私保护及其带来的服务质量之间的内在联系,为不同用户在不同场景下提供自适应的隐私保护方案。

3.3 资源消耗关联的隐私保护方案

近年来,资源消耗关联的隐私保护引起了大量研究工作者的广泛关注。Wang 等^[12]对实时健康监控,特别是无线心电数据流监测中的数据安全和隐私保护问题进行研究,建立了兼顾隐私保护效果和资源优化的 BSN (body sensor networks) 框架,该框架为重要的信息(例如关键的心电图数据)分配额外资源进行保护,以高效监测生物医学数据,并且将信息处理和传输整合在一个平台,有助于确保数据安全传输、降低能源消耗和达到最小延迟。Vergara-Laurens 等^[13]针对 PS (participatory sensing) 系统设计混合隐私保护机制,该机制结合数据匿名化、混淆和加密等技术来提高隐私信息保护的质量,并且能够根据属性变量的变化速率动态地调整属性所在区域网格的尺寸大小,进而选择相应的隐私保护方案,以有效地优化能源消耗。Niu 等^[34]从背景信息可能被敌手获取的问题入手,分析了这种潜在问题对隐私保护效果的影响,并利用虚假用户及信息缓存等技术将历史查询信息进行存储以便重复利用,实现以牺牲设备存储为代价换取对用户隐私的保护。Wang 等^[53]在设计群组隐私信息匹配方案时,采用批量验证有效地降低了计算开销。Bareth^[14]通过预测用户和目标位置间的相互关系,对用户前往目标位置过程中发起的多次位置查询复用相似的查询结果,在确保用户隐私安全的基础上,能够有效降低系统开销。Mana 等^[54]设计一种新的密钥共享方案,该方案在保证存储设备中数据的安全和隐私的基础上,降低了数据的存储消耗。Wang 等^[55]提出一种轻量级的数据存储策略,利用秘密共享技术、擦除编号技术和代数签名技术实现传感器数据安全存储和动态完整性检验。Fan 等^[56]利用多重秘密共享技术策略和标准正交向量技术实现数据存储,既保证满足隐私数据安全存储的需求,又降低了能量消耗。吕志泉等^[15]通过设计带陷门的属性加密算法 WT-CP-ABE 和令牌树机制,提出一种

新的社交网络隐私保护方案 PPSNS,该方案能够避免社交网络服务提供商与系统内部非授权用户的合谋攻击,并且有效降低了密文重加密代价,与现有方案相比,在计算代价、移动存储代价等方面有明显优势。Migliardi 等^[16]对移动网络中的安全节能安全(GEAS, green, energy-aware security)模型相关的研究工作进行了综述,认为现有的大多数方案着重提升安全性或降低能耗,而较少文献研究这两者的关系。

此外,无线传感器网络(wireless sensors networks)中的节能和节点安全问题引起了广泛关注,已有大量研究把能源作为相关系统架构的一个基本组成部分。在无线网络环境中,无线传感网络依靠分散在环境中的大量节点,采集周围环境信息。人们将收集到的信息进行融合分析得出结论,并依此采取相应手段。例如,健康监控系统利用无线传感器网络监测病人,收集并汇聚病人实时信息,通过分析所得数据提供相应医疗服务。然而在无线传感网络中,节点的计算、能量等资源是受限的,而能量资源又关系到整个传感网络的生存时间,因此在无线传感网络环境下的隐私保护方案中能量消耗是需要重点考虑的问题。Szewczyk 等^[57]指出,实用 Micadot 节点发送 1 bit 数据消耗能量约 4 000 nJ,处理器执行一条指令需消耗的能量约为 5 nJ,因此减少通信数量可以有效减少能量消耗。Madden 等^[58]提出了一种典型的应用于无线传感网络中的数据融合技术 TAG,通过剔除各个传感节点所感知的冗余信息,在保证数据有效性的前提下,减少各个节点间的数据传输量,有效地节省传感节点能耗,提高了整个传感网络的生存时间。然而该方案没有提供隐私保护机制,在实际应用中,隐私保护机制是不可或缺的,比如在健康医疗系统中,传感节点采集到的病人体温、血压、脉搏等都属于个人隐私数据。Girao 等^[59]和 Castelluccia 等^[60]提出了一种数据融合隐私保护方案,通过利用同态加密,让传感节点在不需要对数据解密的条件下,使数据有效地融合。然而,同态加密的方法开销较大,不适合在资源受限的传感节点中使用。Conti 等^[61]提出了一种提高顽健性的数据融合隐私保护算法,它加强了传感节点的顽健性,而且计算复杂

度和数据传输量都在传感节点可接受的范围内，但是只适用于簇状结构的无线传感网络中。Yang等^[62]提出了一种数据融合隐私保护算法ESPART，它相对于SMART^[63](slice-mix-aggregate)做了相应的改进，采用逐跳(hop-by-hop)的数据融合方式，给每个节点分配随机时间片的办法，避免节点间的数据发生碰撞，并限制节点间串通的数据范围，降低数据丢失对精确度的影响，在与SMART同等隐私保护安全性的情况下，数据传输量减少了50%。

随着时间的推移，在智能终端上实现普适化、个性化、智能化协议、应用和算法已经成为趋势。然而智能设备的软硬件限制和用户需求的进一步精细化阻碍了这一发展趋势，这就要求研究更加合理的解决方案。

4 研究展望

本文首先分析了移动网络中隐私保护面临的威胁和挑战，然后从背景信息、服务质量和资源消耗关联的隐私保护技术3个方面阐述分析了国内外最新研究动态。现有移动网络中场景关联的隐私保护研究方向相对孤立、功能相对简单，难以满足日渐丰富的应用服务和日益激增的用户需求。为了更加推动移动网络应用服务的普及，使其隐私保护技术更加智慧，还需要从广义背景信息在隐私保护方案设计中的应用、隐私保护方案与服务质量自适应、隐私保护中的资源消耗等方面进一步研究。相关研究方向及其关

系如图3所示。

4.1 广义背景信息在隐私保护方案设计中的应用

针对移动网络中应用需求的多样性，需研究广义背景信息的划分和形式化描述，从纵向角度(细粒度背景信息)和横向角度(多元背景信息)对广义背景进行深入探讨，并以广义背景信息可能被敌手获取为切入点，研究基于时空匿名、混淆和虚假信息等技术的隐私方案融合问题，为用户提供更加全面可靠、隐私保护效果灵活多变的隐私保护机制。具体研究内容如下。

1) 广义背景信息描述与建模。从纵向角度，通过研究现有背景信息内容在其他维度的特征，实现细粒度划分，为不同应用场景提供更加精准的参考信息。例如，在基于位置的服务中，常用的以用户查询请求密度或道路密度为代表的背景信息可以根据区域热度(市中心/乡村等)进行更加精准的划分。从横向角度，考虑引入更多对常用背景信息有较大影响的因素，进行形式化描述并进一步拓展背景信息的内涵。例如用户间的社交关系、查询请求的时间分布等都会对背景信息的精准度有较大影响。此类信息的引入势必会给现有背景信息提供有力补充。通过纵横两个维度的拓展，对广义背景信息进行建模，并最终应用到目前主流的隐私保护方案中。

2) 多源背景信息融合方法。基于广义背景信息描述及其模型，分别从用户和攻击者的角度，收集来自不同类型移动网络、不同时期、不同形式和不同结构的背景信息并进行融合分析，研究

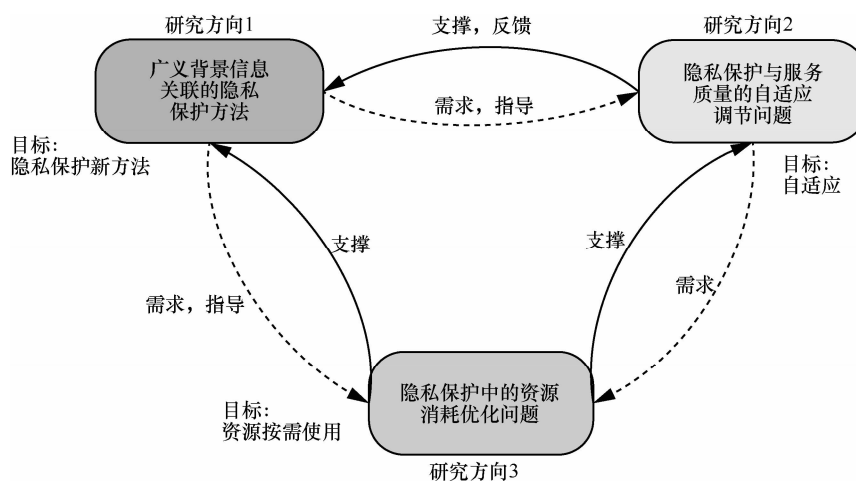


图3 研究方向及其内在联系

多源异构背景信息的聚类融合、异类背景信息的抗关联分析、多维数据属性信息下抗关联分析的隐私数据处理技术、抗关联推断查询的隐私混淆技术等以充分挖掘多源背景信息中潜在的额外价值,进而有针对性地设计隐私保护效果全局最优的隐私保护方案,防止信息融合过程中产生的隐私泄露问题,有效提升隐私保护效果。

4.2 隐私保护与服务质量的自适应问题

针对移动网络应用的服务模式和数据特征,研究影响服务质量的不同因素,并对其进行形式化描述和数学建模;研究利用不同隐私保护方案对服务质量的影响以及两者之间的量化关系,设计面向移动网络应用的服务质量调节算法,构建服务类型与服务质量间的映射关系,并为用户个性化需求的量化分析打好理论基础;针对采用不同隐私保护方案时对服务质量带来的牺牲问题,结合相关因素智能评估用户对特定移动网络应用的服务质量需求,研究基于历史信息的自适应方法。具体研究内容如下。

1) 移动网络服务中的服务质量描述与建模。形式化描述当前移动网络中几种常用的基于数据精确度的服务质量,在此研究工作的基础上,分析其他影响用户体验的因素,例如采用不同隐私保护方案时的响应时间等,通过形式化描述,对移动网络中的服务质量进行定义和建模,为后期的服务质量评价和自适应奠定理论基础。

2) 基于历史信息的自适应方法。在用户端通过个人/群组历史信息复用实现用户端隐私保护、服务质量和资源消耗的均衡,满足用户在不同场景时的隐私保护需求。从用户个人历史信息和其他用户的历史信息两个角度出发,综合研究用户对与该应用类似应用的隐私保护方案选择情况和用户对与该应用类似的其他应用的服务质量需求,设计具有一定参考意义的有效的间接均衡函数,为用户提供基于偏好的自主调节功能,从而实现隐私保护方案和服务质量的自适应。

4.3 基于信息复用的资源消耗优化问题

针对当前移动终端有限的资源,结合用户身处不同场景时对智能终端计算资源、存储资源、网络带宽的需求,设计隐私保护中的资源消耗优化算法,合理优化资源配置,以有限的资源开销最大化地换

取对用户隐私信息的保护。具体研究内容如下。

1) 隐私保护中的资源消耗优化算法。基于移动网络应用服务中用户请求的服务数据的可复用性,研究基于个人历史信息复用或群组缓存信息复用的隐私保护方案,均衡多方面因素对资源消耗的影响,设计隐私保护中的资源消耗优化算法,进一步提高缓存信息复用率,提升用户体验。

2) 多因素均衡的隐私保护机制。通过对不同隐私保护方案与所采用的设备、经由的网络、服务质量需求、资源消耗、期望的隐私保护效果等移动网络服务中常见因素的综合分析,结合已有的研究思路 and 基础,构建多因素均衡的隐私保护机制,在移动网络服务中实现场景关联的隐私保护。

参考文献:

- [1] CHOW C Y, MOKBEL M F, LIU X. A peer-to-peer Spatial cloaking algorithm for anonymous location-based services[C]//The 14th ACM International Symposium on Advances in Geographic Information Systems(ACM-GIS'06), Arlington. 2006: 171-178.
- [2] NIU B, HE Y Y, LI F H, et al. Achieving secure friend discovery in social strength-aware PMSNS[C]//Proceedings of the 34th IEEE Military Communications Conference(MILCOM'15), Tampa. 2015: 962-968.
- [3] LI T C, LI N H, ZHANG J. Modeling and integrating background knowledge in data anonymization[C]//Proceedings of the IEEE 25th International Conference on Data Engineering(ICDE'09), Shanghai. 2009: 6-17.
- [4] RINKU D. Local differential perturbations location privacy under approximate knowledge attackers[J]. IEEE Transactions on Mobile Computing, 2013, 12(12): 2360-2372.
- [5] 王璐, 孟小峰. 位置大数据隐私保护研究综述[J]. 软件学报, 2014, 25(4): 693-712.
- [6] WANG L, MENG X F. Summarization of research on privacy protection of position big data[J]. Journal of Software, 2014, 25(4): 693-712.
- [7] HAGHNEGAHDAR A, KHABBAZIAN M, BHARGAVA V K. Privacy risks in publishing mobile device trajectories[J]. IEEE Wireless Communications Letters, 2014, 3(3): 241-244.
- [8] WU D P, ZHANG H P, WANG H G, et al. Quality-of-protection-driven data forwarding for intermittently connected wireless networks[J]. IEEE Wireless Communications, 2015, 22(4): 66-73.
- [9] VIKASH M, MANSI G, SHRAVAN K U. A survey on wireless body area network: security technology and its design methodology issue[C]//IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS'15), Coimbatore. 2015: 1-5.
- [10] 霍峥, 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.
- [11] HUO Z, MENG X F, HUANG Y. PrivateCheckIn: a method of trajectory of privacy protection in mobile social network[J]. Chinese Journal of Computers, 2013, 36(4): 716-726.
- [12] 潘晓, 郝兴, 孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2010, 47(1): 121-129.

- PAN X, HAO X, MENG X F. Study of continuous queries privacy protection based on location service[J]. Journal of Computer Research and Development, 2010, 47(1): 121-129.
- [11] ZUBAIR M, TARIK T, NIDAL N, et al. Exploring the security requirements for quality of service in combined wired and wireless networks[C]//Proceedings of the International Wireless Communications and Mobile Computing Conference(IWCMC'09), Leipzig. 2009: 73-78.
- [12] WANG H G, PENG D M, WANG W, et al. Resource-aware secure ECG healthcare monitoring through body sensor networks[J]. IEEE Wireless Communications, 2010, 17(1): 12-19.
- [13] IDALIDES J V, DIEGO M, MIGUEL A L. Privacy, quality of information, and energy consumption in participatory sensing systems[C]//Proceedings of the IEEE International Conference on Pervasive Computing and Communications, Budapest. 2014: 199-207.
- [14] ULRICH B. Privacy-aware and energy-efficient geofencing through reverse cellular positioning[C]//Proceedings of the IEEE 8th International Wireless Communications and Mobile Computing Conference (IWCMC'12), Limassol. 2012: 153-158.
- [15] 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 protection scheme for social network service[J]. Journal on Communications, 2014, 35(8): 23-32.
- [16] MAURO M, ALESSIO M, LUCA C. A survey of green, energy-aware security and some of its recent developments in networking and mobile computing[C]//Proceedings of the 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS'14), Birmingham. 2014: 241-246.
- [17] SWEENEY L. K -anonymity: a model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.
- [18] MACHANAVAJJHALA A, GEHRKE J, KIFER D, et al. L -diversity: privacy beyond k -anonymity[C]//Proceedings of the 22nd International Conference on Data Engineering(ICDE'06), Atlanta. 2006: 24-35.
- [19] LI N H, LI T C, VENKATASUBRAMANIAN A. T -closeness: privacy beyond k -anonymity and L -diversity[C]//Proceedings of the 23rd International Conference on Data Engineering(ICDE'07), Istanbul. 2007: 106-115.
- [20] MARTIN D J, KIFER D, GEHRKE J, et al. Worst-case background knowledge for privacy-preserving data publishing[C]//Proceedings of the 23rd International Conference on Data Engineering(ICDE'07), Istanbul. 2007: 126-135.
- [21] CHEN B C, RAMAKRISHNAN R, LEFEVRE K. Privacy skyline: privacy with multidimensional adversarial knowledge[C]//Proceedings of the 33rd International Conference on Very Large Data Bases(VLDB'07), Vienna. 2007: 770-781.
- [22] ZHOU B, PEI J, LUK W S. A brief survey on anonymization techniques for privacy preserving publishing of social network data [J]. SIGKDD Explorations, 2008, 10(2): 12-22.
- [23] HAY M, MIKLAU G, JENSEN D, et al. Resisting structural re-identification in anonymized social networks[J]. Vldb Journal, 2008, 1(1): 797-823.
- [24] HAY M, MIKLAU G, JENSEN D, et al. Anonymizing social networks, TR07-19[R]. Boston: University of Massachusetts, 2010.
- [25] ZOU L, CHEN L, ZSU M T. K -automorphism: a general framework for privacy preserving network publication[J]. Proceedings of the Vldb Endowment, 2009, 2(1): 946-957.
- [26] YING X, WU X. On link privacy in randomizing social networks[J]. Knowledge and Information Systems, 2009, 28(3): 645-663.
- [27] CAMPAN A, TRUTA T M. A clustering approach for data and structural anonymity in social networks[C]//Proceedings of the 2nd ACM SIGKDD International Conference on Privacy, Security, and Trust in KDD (PinKDD). 2008.
- [28] BHAGAT S, CORMODE G, KRISHAMURTHY B. Class-based graph anonymization for social network data[J]. Proceedings of the Vldb Endowment, 2009, 2(1): 766-777.
- [29] CHEN R, MOHAMMED N, WANG K, et al. Privacy-preserving trajectory data publishing by local suppression[J]. Information Sciences, 2013, 231(9): 83-97.
- [30] KANG S, WATT J. The impact of avatar realism and anonymity on effective communication via mobile devices[J]. Computers in Human Behavior, 2013, 29(3): 1169-1181.
- [31] SHEN E, YU T. Mining frequent graph patterns with differential privacy[C]//Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York. 2013: 545-553.
- [32] 马飞, 蒋建国, 李娟. 社交网络隐私保护技术最新研究进展[J]. 计算机应用研究, 2015, 5: 1291-1297.
- MA F, JIANG J G, LI J. The newest research progress of social network privacy protection[J]. Application Research of Computers, 2015, 5: 1291-1297.
- [33] NIU B, LI Q H, ZHU X Y, et al. Achieving k -anonymity in privacy-aware location-based services[C]//Proceedings of the IEEE 33rd International Conference on Computer Communications(INFOCOM'14), Toronto. 2014: 754-762.
- [34] NIU B, LI Q H, ZHU X Y, et al. Enhancing privacy through caching in location-based services[C]//Proceedings of the IEEE 34th International Conference on Computer Communications (INFOCOM'15), Hong Kong, China. 2015: 1017-1025.
- [35] DWORK C. Differential privacy[C]//Proceedings of the 33rd International Colloquium of the Automata, Languages and Programming(ICALP'06). Berlin Heidelberg: Springer-Verlag, 2006: 1-12.
- [36] MCSHERRY F, TALWAR K. Mechanism design via differential privacy[C]//Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science(FOCS'07), Providence. 2007: 94-103.
- [37] GHOSH A, ROUGHGARDEN T, SUNDARARAJAN M. Universally utility-maximizing privacy mechanisms[J]. SIAM Journal on Computing, 2012, 41(6): 1673-1693.
- [38] DWORK C. Differential privacy: a survey of results[C]//The 5th International Conference on Theory and Applications of Models of Computation (TAMC), Xi'an. 2008: 1-19.
- [39] DWORK C. Ask a better question, get a better answer: a new approach to private data analysis[C]//The 11th International Conference on Database Theory (ICDT'07), Barcelona. 2007: 18-27.
- [40] BLOCKI J, BLUMAND A, DATTA A, et al. The johnson-lindenstrauss transform itself preserves differential privacy[C]//Proceedings of the 16th Annual Symposium on Foundations of Computer Science(FOCS'12), New Brunswick. 2012: 410-419.
- [41] BONOMI L, XIONG L, CHEN R, et al. Frequent Grams based embedding for privacy preserving record linkage[C]//Proceedings of the 21st ACM International Conference on Information and Knowledge Management, Maui, Hawaii. 2012: 1597-1601.
- [42] FANAND L, XIONG L. Real-time aggregate monitoring with differential privacy[C]//Proceedings of the 21st ACM International Conference on Information and Knowledge Management, Maui, Hawaii. 2012: 2169-2173.
- [43] ZENG C, NAUGHTON J F, CAI J Y. On differentially private

- frequent itemset mining[J]. Vldb Journal very Large Data Bases a Publication of the Vldb Endowment, 2012, 6(1):25-36.
- [44] ENCK W, GIBERT P, CHUN B G, et al. Taintdroid: an information flow tracking system for real-time privacy monitoring on smartphones[J]. Communications of the ACM, 2014, 57(3): 99-106.
- [45] ICKIN S, WAC K, FIEDLER M, et al. Factors influencing quality of experience of commonly used mobile applications[J]. IEEE Communications Magazine, 2012, 50(4): 48-56.
- [46] WANG W, ZHANG Q. Toward long-term quality of protection in mobile networks: a context-aware perspective[J]. IEEE Wireless Communications, 2015, 22(4):34-40.
- [47] SHOKRI R, PAPADIMITRATOS P, THEODORAKOPOULOS G, et al. Collaborative location privacy[C]//Proceedings of the 8th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems(MASS'11), Valencia. 2011: 500-509.
- [48] SHOKRI R, THEODORAKOPOULOS G, PAPADIMITRATOS P, et al. Hiding in the mobile crowd: location privacy through collaboration[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 11(3): 266-279.
- [49] MEYEROEITZ J, CHOUDHURY R R. Hiding stars with fireworks: location privacy through camouflage[C]//Proceedings of the ACM 15th Annual International Conference on Mobile Computing and Networking(MobiCom'09), Beijing. 2009: 345-356.
- [50] GUO S M, CHEN K K. Mining privacy settings to find optimal privacy-utility trade-offs for social network services[C]//2012 International Conference on Privacy, Security, Risk, Trust and Social Computing. 2012: 656-665.
- [51] XIONG P, PING X. An anonymization method based on tradeoff between utility and privacy for data publishing[C]//International Conference on Management of e-Commerce and e-Government (ICMeCG), Beijing. 2012: 72-78.
- [52] GU Y H, WU W M. A Quantifying method for trade-off between privacy and utility[C]//IET International Conference on Information and Communications Technologies(IETICT), Beijing. 2013: 270-273.
- [53] WANG B Y, LI B C, L H. Gmatch: secure and privacy-preserving group matching in social networks[C]//IEEE Global Communications Conferences(GLOBECOM'12), Anaheim. 2012: 726-731.
- [54] MANA M, FEHAM M, BENSABER B A. Trust key management scheme for wireless body area networks[J]. International Journal of Network Security, 2011, 12(2): 71-79.
- [55] WANG Q, REN K, YU S C, et al. Dependable and secure sensor data storage with dynamic integrity assurance[C]//Proceedings of the IEEE 28th International Conference on Computer Communications (INFOCOM'09), Rio de Janeiro. 2009: 954-962.
- [56] FAN R, PING L D, FU J Q. The new secure and efficient data storage approaches for wireless body area networks[C]//Proceedings of the IEEE International Conference on Wireless Communications and Signal Processing, Suzhou. 2010: 1-5.
- [57] SZEWCZYK R, FERENCZ A. Energy implications of networks sensor designs[EB/OL]. <http://bwrcs.eecs.berkeley.edu/Courses/CS252/Projects/Reports/robert-szewczyk.pdf>.
- [58] MADDEN S, FRANKLIN M J, HELLERSTEIN J M. TAG: a tiny aggregation service for ad-hoc sensor networks[C]//Proceedings of the 5th Symposium on Operating Systems Design and Implementation, New York. 2002: 131-146.
- [59] GIRAO J, WESTHOFF D, SCHNEIDER M. CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks[C]//Proceedings of the 40th International Conference on Communications, Seoul. 2005:3044-3049.
- [60] CASTELLUCIA C, MYKLETUN E, TSUDIK G. Efficient aggregation of encrypted data in wireless sensor networks[C]//Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems(ICMUS'05), San Diego. 2005: 109-117.
- [61] CONTI M, ZHANG L, ROY S, et al. Privacy-preserving robust data aggregation in wireless sensor networks[J]. Security and Communication Networks, 2009, 2: 195-213.
- [62] 杨庚, 王安琪, 陈正宇,等. 一种低能耗的数据融合隐私保护算法[J]. 计算机学报, 2011, 34(5): 792-800.
- YANG K, WANG A Q, CHEN Z Y, et al. A low energy consumption privacy preserving algorithms of data fusion[J]. Chinese Journal of Computers, 2011, 34(5): 792-800.
- [63] HE W, LIU X, NGUYEN H, et al. PDA: privacy-preserving data aggregation in wireless sensor networks[C]//Proceeding of the 26th IEEE International Conference on Computer Communications (ICC'07), Anchorage. 2007: 2045-2053.

作者简介:



牛犇(1984-), 男, 陕西西安人, 博士, 中国科学院信息工程研究所助理研究员, 主要研究方向为网络安全、隐私计算。



李风华(1966-), 男, 湖北浠水人, 博士, 中国科学院信息工程研究所副总工、研究员、博士生导师, 主要研究方向为网络与系统安全、隐私计算、可信计算。



华佳烽(1989-), 男, 湖北黄冈人, 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。



何媛(1985-), 女, 湖北松滋人, 中国科学院信息工程研究所博士生, 主要研究方向为信息安全、隐私保护。