计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190400116

社交传感云安全研究进展

梁俊斌　张　敏　蒋　婵
广西大学计算机与电子信息学院　南宁 530004
广西多媒体通信与网络技术重点实验室　南宁 530004
(15388951803@163.com)

摘　要　社交传感云是由社交网络、无线传感网络与云计算结合产生的一种新型传感云系统,将虚拟社交网络信息世界与现实的物理世界融合在一起,不断为社交用户提供新的服务和应用。社交传感云(Social Sensor Cloud)不仅具备了无线传感网络在收集外界信息方面强大的社交感知能力,还利用云计算技术打破了传统传感器网络在数据处理和存储方面的局限性。但是,由于社交传感器被移动地部署在不可信的社交云环境中,导致现有的社交传感云服务面临许多严重的安全问题,如社交传感器共享数据时容易遭受恶意攻击;不同服务商与用户之间的信誉问题,导致社交传感数据泄露、服务完整性问题等,严重阻碍了社交传感云服务的进一步发展。文中针对目前已有的研究,介绍了社交传感云的产生背景、体系框架、应用领域以及系统新特性,对社交数据安全、社交传感网络安全、社交传感云服务安全的研究现状进行介绍,并分析对比了典型的安全技术方案。此外,文中还讨论了该领域面临的挑战,并对未来的研究方向进行了展望。

关键词:社交传感云;云计算;社交网络安全;数据安全;服务安全
中图法分类号　TP393

Research Progress of Social Sensor Cloud Security

LIANG Jun-bin,ZHANG Min and JIANG Chan
School of computer and electronic information,Guangxi University,Nanning 530004, China
Guangxi Key Laboratory of Multimedia Communication and Network Technology,Nanning 530004, China

Abstract　Social sensor cloud is a new type of sensor cloud system generated by social networks,wireless sensor networks and cloud computing,combines the virtual social networks world with the physical world,and provides new services and applications for social users continuously. It collects external information with the powerful social sensing ability of wireless sensor networks,and solves the limitations of traditional sensor networks in data processing and storage by using cloud computing technology. However,social sensors deployment in untrusted social cloud environment,which causes many serious security issues for social sensor cloud services,such as,malicious attacks when social sensors are sharing data,reputation issues between different service providers and users,social sensor data privacy leaks,service integrity issues. These security issues deeply hinder the further development of social sensor cloud services. For the related research progress of social sensor cloud,this paper introduces the background,the system framework,application fields and new system characteristics of social sensor cloud,and analyzes and compares typical security technology schemes. In addition,the key scientific issues to be solved in this field are discussed,and the future research work is prospected.

Keywords　Social sensor cloud,Cloud computing,Social networks security,Data security,Services security

1　前言

社交传感云是由社交网络、无线传感网络与云计算结合产生的一种新型传感云系统,通过云计算技术对来自社交传感网络节点的数据资源进行计算和存储,实现了虚拟社交网络信息世界与现实物理世界的融合,为用户提供便捷、经济、高可靠性的社交传感云服务[1-3]。

安全是基于云平台提供的所有服务面临的关键性挑战之一,能够为用户提供实时、有效的安全服务是社交传感云的核心问题[4]。首先,社交传感器的移动性使得网络拓扑不稳定[5];其次,在社交传感器传输数据的过程中,社交网络的开放性使得社交传感器容易受到攻击,从而使用户的数据隐私

到稿日期:2019-04-20　返修日期:2019-10-22　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61562005,61762010);广西自然科学基金项目(2018GXNSFBA281169);广西高等学校千名中青年骨干教师培育计划项目(桂教人(2017)49)
This work was supported by the National Natural Science Foundation of China (61562005,61762010),Natural Science Foundation of Guangxi Province, China (2018GXNSFBA281169) and Thousands of Young and Middle-aged Backbone Teachers Training Program for Guangxi Higher Education [Education Department of Guangxi (2017)49].
通信作者:张敏(15388951803@163.com)

得不到保障[6];最后,云服务提供商与社交用户之间存在着不同类型的信誉问题[7-8],以上原因使社交传感云服务安全面临着严峻的挑战。但是,传统的传感云系统无法解决这些由于社交环境因素导致的安全问题,因此需要进一步研究有效的安全机制,以保障社交传感云的安全。

目前,社交传感云服务的应用范围已经很广,越来越多的研究者开始关注与社交传感云相关的安全问题,并提出了不同的解决方案。为了促进社交传感云安全的深入研究,本文第 2 节介绍社交传感云的定义、框架以及应用,强调社交传感云服务安全的重要性;第 3 节概述目前社交传感云的研究进展;第 4 节和第 5 节对社交传感云安全问题进行分类讨论,根据典型的方案进行归纳总结,并分析相关工作的优缺点;第 6 节关注当前的研究热点,进一步指明未来研究的方向;最后总结全文。

2 社交传感云

2.1 社交传感云体系

社交传感云是社交网络、无线传感网络、云计算三者结合而成的新型传感云系统,基于无线传感网络和云计算技术的高速发展,社交传感云成为物联网的核心领域之一。首先,无线传感器网络具有部署迅速、实时性强等优势,它扩展了人们收集外界世界的能力[9]。其次,社交网络在全球迅猛发展,其中社交媒介如智能手机等,作为社交传感器被大范围推广,搭建了一个巨大的社交传感网[10]。最后,社交传感网络与云计算的结合越来越紧密,云计算技术具有强大的数据计算、存储能力,不仅为社交传感网络应用提供了良好的可扩展性,也为解决社交传感网的数据处理提供了新的方法[11]。

在社交传感云中,由社交传感器收集的数据被上传到社交传感网络,通过云端控制传感网实时进行数据采集,利用云计算平台进行数据处理和存储,为不同的社交用户提供最佳匹配的低延迟传感云服务[12-13]。本文研究的社交传感云服务主要从 4 个方面进行研究:效率、数据、虚拟化和服务。图 1 中,社交传感云体系分为 3 个概念层。

(1)社交传感器:Aamir 等认为,除智能手机、平板等可穿戴移动无线设备以外,在社交网络中社交用户贡献自己的个人“数据”,表达自身情况或者事实,都可以被视为社交传感器[3]。其对社交传感器的概念作了进一步的扩展,认为所有包括现代社交网络或者网络媒介中即所有在现代社交网络或者网络媒介中,只要表达了社交用户环境、事件、情况,可以被识别的任何信息来源都称为社交传感器。

(2)社交传感器云(在线社交网络):社交网络的快速增长使用户可以分享他们的社交数据,从而将全球连接为一个整体。近年来在线社交网络不断增加,如 Facebook、Twitter、新浪博客、YouTube 和 Flickr 等,庞大的社交数据存储在不同结构的社交网络中,因此收集不同类型的社交数据是非常具有挑战性的[14]。

(3)社交传感器云服务:社交传感云在云端处理和存储海量数据。为了解决社交网络的隐私问题,并进一步提高云中社交数据的安全,一是在社交网络中预先对数据进行加密处理,二是社交传感器云将不同类型的社交传感器数据经过有效的收集、过滤后,由云端的服务器将接收到的数据经过信任评估等安全机制,再由云平台进行计算和存储,最后根据用户的需求提供各种类型的信息服务,如投入到智能交通、社交传播、军事、地震灾害等应用场景[15-17]。

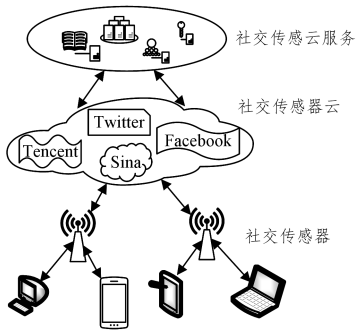


图 1 社交传感云体系结构

Fig. 1 Social sensor cloud system architecture

2.2 社交传感云新特性

回顾近年来有关社交传感云的应用发现,社交传感网络和云计算的结合发挥了极大的作用,但社交传感云在发展的同时也产生了许多新特性以及这些新特性衍化的安全问题。

2.2.1 社交演化性

社交传感云具有在线社交网络的社交演化性,需要针对其复杂的网络结构、群体行为、网络信息进行研究。

(1)社交网络节点的自私性:应该考虑社交传感器的社交特征,社交网络用户可能因为各种原因(资源限制、个人隐私、社交目标)在网络中拒绝合作共享数据[18],如放弃个人数据上传、不进行消息转发等,从而使得数据传输成本增大、传输效率减低,减少了社交数据共享的利益。

(2)社交传播的相互影响:具有社交因素的传感器网络与传统无线传感网络的传播方式不同,这些传感器收集社交数据时应该考虑社交节点的评估,例如通过社交数据的传播延迟来评估两个社交传感器节点之间的正负影响。从物理角度来看,可以根据多跳传感器网络的服务质量(QoS),如带宽、负载和链路之间的物理距离[19],来评估传播延迟;从社交的角度来看,可以根据一个人的行为对另一个人行为的影响来进行量化,反应越快说明延迟越低。综合两者,社交传感的传播延迟可以表示两个用户/传感器之间的交互频率。

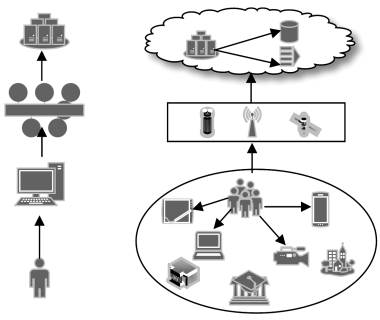
2.2.2 基于系统体系的可扩展性

社交平台的多元化使得社交传感云系统具有很强的可扩展性,如图 2 所示,社交网络已经从图 2(a)所示的单一网络传播模式扩展到图 2(b)所示的多种社交传感设备在多种网络中转播的模式。随着用于存储海量社交传感云数据的云计算与社交网络的结合,不仅使得社交媒体可以融入到社交网络中,还创造了许多具有可扩展性的社交传感云应用程序。

(1)社交场景和设备:社交网络的在线用户量不断增加,应用场景也在不断扩大,随着科技进步,新型的社交设备(社交传感器)不断产生,例如功能愈加丰富的智能手机、平板、智能手表等;

(2)通信设备:针对不同类型的社交传感器和不同的网络,需要提供不同的数据传输接口和设备实现传感层到云端的通信,例如无线卫星、发射塔、光纤等;

(3)云平台:社交传感数据呈现出了更加丰富的属性和更为庞大的数量,因此云服务提供商需要扩展更多的数据中心和数据库,以提供更强的计算、存储能力。



(a)社区网络 (b)社交传感云

图 2 社交传感云演化进程

Fig. 2 Evolution of social sensor cloud

2.2.3 社交传感器与云平台的交互性

社交传感云中社交传感网络的数据量十分庞大,数据类型、功能属性越来越多,不可信社交网络的动态结构更为复杂,因此在管理数据时需要考虑社交传感器与云平台交互性[20]。通过云计算,社交网络用户可以从全球任何地方访问共享资源。

Facebook 和 Twitter 等常见的社交网络帮助全世界数十亿的用户共享互联数据。

(1)数据来源:社交传感器数据是以多种形式从多个源生成的,并且具有不同类型和格式,因此需要不同的定义方法。例如,社交传感器数据非定性特征(如时间、位置等)被抽象为服务的功能属性,定性特征(如价格、信任、覆盖范围等)被抽象为服务的非功能属性。

(2)数据传输:社交传感器是动态部署节点,在有限的时间和范围内移动传感,因此社交传感器的能量和通信能力有限,如何将所有感测数据上传到云平台是一个需要解决的难题。

(3)数据共享:社交传感数据除了由社交传感器收集之外,还来自于社交网络的共享。社交传感网络利用云强大的数据处理能力和数据存储能力,可以进一步扩展社交传感云的服务[21]。因此,在不同社交平台的应用程序中,需要提供不同的访问接口和云数据处理中心。

社交传感云需要将社交网络中的数据处理成服务,而不暴露数据内部结构以及访问数据的形式[3]。社交传感数据需要经过社交传感器和社交网络才能被上传到云端,以进行进一步的处理和过滤,社交传感器与云平台的交互性导致了整个数据收集和管理过程变得十分复杂。

2.3 社交传感云的安全的重要性

随着社交网络的日益发展,社交传感云已经被广泛应用于各种场景,用户需求呈现多样化,因此对安全的要求也逐渐提高。社交传感数据由大规模的社交传感器感知而来,而社交传感器所部署的社交网络环境特性导致其传输的数据容易受到恶意攻击等物理安全问题。社交传感云具备了社交传感网无处不在的物理感知能力和云计算强大的计算和存储能力,与此同时也面临着更大的挑战,包括社交传感网和云计算自身存在的安全问题以及两者融合之后产生的安全问题[11]。

基于社交传感云的新特性,从以下不同角度产生了新的安全问题。

(1)从社交传感器的角度:社交传感器被动态地部署在结构复杂、不可信、虚拟的社交网络中,这为不法分子窃取社交传感云中的用户数据提供了良好的机会。在社交传感云的物理层,许多类型的攻击破坏了数据的完整性和可用性,如在传感层,社交传感器节点可能面临窃听、单节点被俘获、多备份攻击、多节点叛变等攻击[22-23]。

(2)从社交传感云结构的角度:社交传感云结构的特性如社交网络的虚拟化、云平台的可扩展性、数据远程外部存储等,使得社交传感云系统存在着不同层次的安全漏洞。由于社交传感数据格式是异构的,因此社交传感器与社交网络之间需要特定的组件和访问接口进行交互,这种融合带来了新的隐私挑战,如在社交网络中,存在网络欺诈、隐私泄露、恶意信息的传播网络群体性事件等社交安全威胁。

(3)从服务的角度:社交传感云的应用服务虽然为社交用户提供了极大的便利,但同时也产生了一定的安全风险。在社交传播中,虽然社交云将影响目标的端到端传播成本降至最低,但是其中存在的负面影响无法避免[24]。例如,在智能交通系统中,社交云服务虽然会利用社交媒体上产生的大数据提供有用的驾驶导航信息,但是并不能排除虚假信息的存在以及开放的社交媒体网络带来的严重后果,提供共享数据的用户信息也可能遭到泄露,用户个人隐私得不到有效保障。

综上,无论是在哪种应用背景下,社交感云都存在着一定的安全隐患,都可能给社交用户造成安全威胁。1)如何实现虚拟传感器节点的低资源使用并节省物理传感器节点的能量。如果物理传感器节点受到攻击,虚拟传感器仍会将数据传输到虚拟传感器服务平台,从而生成无效数据。2)如何减少冗余误报并防止传感器数据泄露。如果虚拟传感器服务节点受到攻击,物理传感器节点仍会将数据传输到虚拟传感云平台,从而导致数据泄露。

因此,在社交传感器数据的收集、传输、存储过程中,需要研究有效的方案来解决社交传感云中数据传输的低能效和传感器云中数据泄露风险高的问题。社交传感云的安全问题值得关注,我们需要迫切地研究解决方案。

3 社交传感云安全及技术研究分类

社交传感云的发展为人类的生活提供了大量的便利服务。大规模的智能手机、平板、智能手表等无线设备,将摄像头、麦克风、计步器等作为社交传感器,收集大量社交用户的数据信息,并将其传输到云端进行有效处理,为用户提供服务,但是社交传感器在进行数据收集和传输的过程中也存在隐私安全风险。如图 3 所示,经过第 2 节对社交传感云的新特性的分析,将社交传感云服务的安全研究分为两个方面,即社交传感云系统安全和社交传感云服务安全,其中系统安全包括传感层和网络层面临的问题和解决的方案。

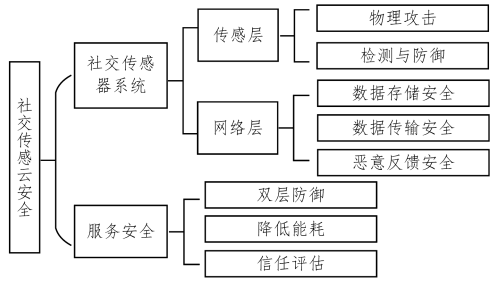


图 3 社交传感云安全研究分类

Fig. 3 Social sensor cloud security research classification

4 社交传感云系统安全的研究进展

社交传感云系统安全包括传感层安全和网络安全,社交传感器在通信时容易受到不同类型的物理攻击,开放性的社交网络环境也面临着节点异常转发等网络传播问题。

4.1 社交传感器的安全研究

4.1.1 物理攻击

在社交传感云背景下,社交网络的本质就是使得多名用户在同一个空间中共存,因此用户的社交传感器在社交场合下容易被攻击。不同类型的物理社交传感器通过 WIFI,433 MHz,Zigbee(2.4G)等技术进行数据传输,这些技术传输数据时面临着不同类型的物理攻击。例如侧信道攻击,指对加密设备进行攻击,使得加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露方法,导致加密电子设备在运行过程中侧信道信息泄露,例如时间消耗、功率消耗或电磁辐射等。

Li 等[25]研发了一个新颖且实用的多模式侧信道击键识别系统(ClickLeak),在社交环境下,将智能手机的加速器和麦克风传感器作为发射器,将计算机作为接收器,获取社交用户在 POS 机输入密码时的击键起始时间,以及该段时间内 Wi-Fi 信号产生的失真,分析信道状态信息(CSI)以推断击键,识别用户密码。根据 CSI 时间序列的临界相位特征,并结合 CSI 幅度和相位波形来构建分类器,以进一步提高 ClickLeak 的性能和准确性。仿真实验结果证明,随着社交网络用户数的增多,ClickLeak 的准确性也会显著提高。

4.1.2 检测与防御机制

传感器云系统中所有数据都存储在远程云服务器中,这给数据安全带来了很高的风险。当采用移动传感器接收器收集传感数据时,复制的接收器攻击会给传感器云系统带来一些严重的问题,如隐私信息泄露或者丢失。因此不仅需要针对传感器节点进行信任评估,还需要建立移动接收器的信任评估[26]。

Wang 等提出了一个全面的可靠数据收集模型来保护传感云系统的安全,其中设计了直接信任、间接信任和功能信任 3 个评估模型来评估传感器和移动接收器的可信度[27]。在直接信任模型中,通过两个社交传感器节点直接的交互(通信能力、剩余能量),以及其他节点的信任推荐来计算信任值。在间接信任模型中,基于传输路由的传播来计算信任值。此外,在功能信任模型中,考虑到当采用移动传感器接收器收集传感数据时,复制的接收器攻击会给传感器云系统带来一些严重的问题,通过为负责数据传输的移动接收器传输存储 ID,对传感云系统中的恶意节点进行检测识别,有效防止了系统复制的移动接收器攻击。

Musaev 等建立了一个山体滑坡信息预测服务系统(LITMUS)[28],通过物理和社交传感器,合并来自气象卫星和地震仪等物理传感器的数据以及社交网络的数据,过滤可靠的物理数据与直接报告山体滑坡的社交媒体数据,以实现高质量和大范围的山体滑坡信息预测。

Lau 等基于在线社交媒体网络,提出了一种大数据收集有效驾驶导航信息系统,即通过社交传感器实时生成有效的驾驶建议[29]。该系统通过收集手机社交媒体用户贡献的包含类型复杂的帖子,基于主题模型的计算方法来收集相关的语义(如交通条件、道路状况、驾驶员条件等),提出了利用社交媒体数据提供导航支持的方案。

4.1.3 方案分析

上述基于接收器的攻击识别系统以及社交传感器的防御系统,都是在社交传感云的背景下,采用社交传感器进行有关数据的感知处理,即收集社交用户共享的帖子,分析处理复杂的交通和道路状况信息,以进一步提高智能交通系统的有效性。这些系统主要采用社交媒体作为社交传感器来提取有效数据信息,模块实施过程相对简单,功能易于实现,但缺乏针对恶意社交传感器产生虚假信息的防御策略[30]。

4.2 网络安全

4.2.1 数据存储以及网络传播安全

目前,为了保护社交共享数据的隐私性,基于云计算的方案一般采用加密和解密数据的方式。在社交传感云中,社交用户共享到社交云中的数据是经过加密的,系统中其他的用户或者云服务商必需具有公钥,才能检索到数据。但是,被获取到的数据可能会遭到恶意泄露,因此需要重新加密。Praveena 等[31]提出了一个在基于云的社交网络上安全存储数据的框架,首先通过用户的私钥对数据进行解密,其次采取代理重加密方案以重新加密数据使其更安全,能够在数据存储于云端之前对数据进行加密,从而进一步保障云中数据的安全。

在线社交网络往往表现出复杂的结构,其中亲密朋友关系和政治对手关系分别呈现了积极影响和消极影响。Guler 等[32]将社会意识融入到以影响为中心的约束下的网络传播中,提出了一个具有正负关系类型的社交传感网络的传播模型,可以提取有关社会和物理现象的信息。通过利用社交传感器观察底层社交中的关系类型,将影响目标的端到端传播成本降至最低,其中传播成本是由社交和物理网络动态引起的;通过研究传播问题,尽量减少传播过程中受到消极影响的人数,并提供影响网络传播参数的因素,如传播延迟、交互频率等。

移动社交网络是一种用于信息共享的即时社交网络,其基于网络的动态性、临时性、开放性,因此依赖网络中节点在传输上的反馈。但是,异常节点的反馈或者恶意行为会降低网络性能,甚至损害网络。

在现有的信任模型中,最终的 ACK 消息是关键因素,Wang 等[33]提出了一个动态信任框架,构建基于信任的路由机制,在机会移动社交网络中设定节点的连通性、适应性和满意度为信任值度量,将贝叶斯算法与该信任值度量方法相结合,提出了一种“双跳反馈方法”,该方法依赖于转发路径中两个中间节点生成的 ACK 消息,而不仅仅依赖于最终目标节点生成的 ACK 消息,验证了节点的诚信度,该方法基于成功传递消息的速率、丢包数、网络负载、异常节点的检测率 4 个标准。该评估方案仅通过检查节点的传播行为来评估该模型的性能。虽然移动节点之间的协作数据传递可以改善移动社交网络中数据传输的性能,但是当存在社交自私节点根据其社会特征和关联来降低合作程度,以实现该节点的社交目标时,数据传输面临在不确定的行为下转发的问题。

针对上述问题,Xia 等[34]提出了一种信令博弈方法(Sig4UDD),研究了行为良好的节点和社交自私节点之间不确定协作对数据转发性能的影响。首先,采用贝叶斯纳算法

中的纳什均衡来分析节点之间的一阶段相互作用。其次，在节点的多阶段相互作用中，建立了一个信任系统来预测社交自私节点的对手类型，并采取适当的行动来最大化它们的效用；设置加权社交距离度量来测量节点之间的全局社交距离，更新社交自私节点的信任。虽然 Sig4UDD 在消息传递成本方面优于其他协议，但是在消息传递延迟方面仅比非合作协议短，以上两个因素导致 Sig4UDD 中的消息传递率比其他算法差。

文献[31-34]从社交传感网络的不同方面研究了节点、网络的信任安全，表 1 列出了各方案的基本思想和优缺点，从中可以看出，在社交传感网络的安全方面需要考虑社交因素对传播节点之间的积极影响和消极影响、社交网络传播性能等。

表 1 方案优缺点对比

Table 1 Comparative analysis of schemes

方案	基本思想	优点	缺点
在社交网络上安全存储数据的框架[31]	在基于云的社交网络上安全存储数据	代理重加密方案用于重新加密，保障了数据的隐私性	检索数据解密需要公钥，能耗较大
正负关系类型的社交传感网络的传播模型[32]	具有正负关系类型的社交传感网络的传播模型	将社会意识融入以影响为中心的约束下的网络传播	异常节点可能会降低网络性能，甚至损害网络
双跳反馈[33]	基于信任路由机制的动态框架	双跳反馈方法，验证了节点的诚信度	面临在不确定的行为下转发的问题
Sig4UDD[34]	信令博弈方法	预测社交自私节点的对手类型，降低了消息的传递成本	消息传递率比其他算法差

4.2.2 现有方案的不足

在社交传感网络环境中，云服务提供商和社交用户之间交互的信任关系是服务交易的基础。但信任关系的建立是一个基于多要素决策的复杂递进的过程，涉及交互历史、信任推荐和信任管理等多方面的信息[30]。在现有的关于社交传感网络的研究中，还存在以下不足。

(1)云计算增强了社交媒体的交互自由，使大多数用户能够通过社交媒体自由分享个人信息以及将信息存储到云计算系统中，如何保证云环境中的用户可以安全地存储和检索共享数据有待解决。

(2)社交媒体上存在大量的错误信息数据，恶意服务提供商提供的这种不值得信赖的服务有可能在社交传感器云上，使得社交用户无法获得安全性高且可靠的服务。

5 社交传感云服务的研究进展

5.1 入侵检测与防御

多数先前的工作从传感云的单层防御角度研究了高效的入侵检测机制。对资源有效的无线传感器网络的研究考虑了检测质量、能耗和控制开销之间的权衡[35-37]。如何从社交传感云的传感层和网络层自下而上地进行入侵检测和防御是一个难点问题。

Anantvalee 等[38]将入侵检测系统(IDS)部署到 MANET 中的平面和集群网络基础设施中，适合 IDS 协同防御传感器集群中的攻击者。Baig[39]提出了一种基于网络流量的攻击识别模型，以便于区分合法和异常攻击流量包。该模型可以在参与检测过程所需的传感器资源集的大小方面提高预测的攻击检测准确度。

在此基础上，Liu 等[40]提出了一个用于保护传感云的节能双层防御方案，优化入侵检测策略以降低能耗并减少传感云中的警报信息，分析了物理传感器节点和虚拟传感器节点在采用监控和防御策略时应如何配合。首先，当所有入侵检测系统(IDS)都有助于检测和报警生成时，传感器节点的消耗相对较高，导致入侵检测期间的可靠性和安全性较低。因此，安装在传感器节点中的每个 IDS 都应该通过学习其他 IDS 来相应地动态调整其策略。此外，采用基于能量约束的演化稳定策略来为 IDS 分配攻击监控和警报生成任务。所提出的机制可以调整物理传感器节点应用在 4 个不同阶段的防御策略，并减少传感云运行 IDS 时的警报消息数，在实现传感云系统安全的前提下进一步节省了能源。

除了满足节能的要求，社交传感云服务的安全性也应该包含身份验证、机密性和完整性等基本要求。Borujeni 等[41]在 P-SEP 协议的基础上，研究了安全服务对基于雾的无线传感器网络生命周期(SFL)的影响，考虑了将受保护数据从雾节点传输到云的安全开销和平均能耗，通过增加网络中的雾节点，没有必要发送所有数据到云端进行处理，仅发送无法在雾节点中处理的数据。与 P-SEP 协议相比，该算法簇头节点和云中的计算量更少，节省了更多的能量。

针对上述社交传感云服务的安全性需求，Zhu 等[42]基于智慧城市研究了在信任辅助传感器云系统(TASC)中关于安全多媒体大数据的应用，提出了两种类型的信任辅助传感器云系统：具有单一信任阈值的 TASC(TASC-S)和具有多个信任阈值的 TASC(TASC-M)。在无线传感器网络中利用超过信任阈值的传感器进行数据的收集和传输，并在可信数据中心进行存储，采用信任评估机制来保障社交数据的源标识、内容完整和隐私等，在进一步处理后给用户按需提供服务，提高了 TASC 中安全多媒体大数据的可靠性。

表 2 列出了文献[40-42]中方案的基本思想和优缺点。可以看出，在保护社交传感云的安全防御方面，不仅需要考虑节能，还需要保障服务的完整性、隐私性和安全性，分阶段进行优化入侵检测使得安全性最大化，但是也需要权衡由此产生的安全开销。

表 2 方案优缺点对比

Table 2 Comparative analysis ofschemes

方案	基本思想	优点	缺点
节能双层防御方案[40]	针对优化入侵检测策略，减少传感云中的警报信息	在 4 个不同段的防御策略，提高安全性，减少 IDS 运行时的警报消息数	分阶段检测导致安全开销较大
SEL[41]	安全服务对基于雾的无线传感器网络生命周期(SFL)的影响	云计算复杂度更少，节省了更多的能量	没有考虑雾节点的隐私性
TASC[42]	基于信任路由机制的动态框架	按需服务，保障社交数据的源标识、内容完整和隐私	按需服务，数据中心安全开销大

5.2 访问控制

基于云计算平台的社交传感云系统，使得社交用户不仅可以远程存储社交传感数据，而具备无处不在、可靠性、高性能、高效率和可扩展性的优势[43-45]。但是，将这些云优势应用于包含敏感信息的巨大感知数据会导致严重的数据安全问题。数据拥有者可能会失去对数据的物理控制[46]，如何加强对数据

拥有者的访问控制来进一步保障系统安全需要进一步的研究。

为了向传感云用户提供高质量的服务,通过研究细粒度的交互控制程序,可以综合解决传感器管理、服务质量控制和系统效率最大化等关键问题[47]。

Dinh 等[48]提出了高效的交互式传感器云(EISC)方案,有效地控制了传感流延迟的低信令开销和高能效。首先,在传感云中设计了请求聚合器,以聚合应用程序的延迟请求,从而最大限度地减少物理传感器所需的工作量并节省能源;其次,聚合器使传感器能够仅运行单个任务,并在为具有不同要求的多个应用程序提供服务时进行调度;最后,方案自动调整传感器的时间安排,其中设计了 QoS 控制器来控制传感流的端到端数据包延迟,以满足所有应用程序的延迟要求。但是,该方案在数据传输延迟和可靠性方面的性能较差。

Rachkidi 等[49]基于不同应用之间共享真实传感器和虚拟传感器的需求,提出了一个资源优化和有效分配(ROED)方案。为减少物理和逻辑传感器的负担,该方案最小化了传感云中虚拟传感器的数量,以及在实现应用 QoS 目标的同时,减少实现物理传感器和逻辑传感器的通信量,节省了传感云的部署成本并降低了基础设施内的数据传输延迟。但是,在部署虚拟机的数量和控制网络成本之间较难进行权衡。

针对上述方案存在的两个问题,Kim[50]提出了一种基于传感云的两阶段博弈方法的高效控制方案,为多种应用提供按需感应服务。该方案包括了数据中心选择算法和传感器激励算法两阶段博弈,模拟用户、数据中心和传感器之间的关系,通过两阶段博弈依次进行交互,并选择最佳策略以最大化其预期收益。

从表 3 可以看出,交互模型设计用于云和传感器节点,以优化物理传感器的资源消耗以及感测流量的带宽消耗。EISC 在物理传感器的能耗、从汇聚节点到传感器云的带宽消耗、数据包传送延迟、可靠性和可扩展性方面实现了显著改进。与现有的 EISC 和 ROED 方案相比,在不同的服务请求速率下,高效传感云控制方案具有更低的服务延迟和更大的系统吞吐量。如何从网络运营商的角度解决社交传感云系统中的网络安全问题值得进一步探索。

表 3 方案优缺点对比

Table 3 Comparative analysis of schemes

方案	服务延迟	平均能耗	吞吐量	部署成本
EISC[48]	较大	较低	较低	较高
ROED[49]	较小	较高	较低	较低
高效传感云控制方案[50]	较小	较低	较高	较高

6 社交传感云安全的研究展望

根据社交传感云的特性以及安全需求,目前已有的研究方案还不够完善,只针对社交传感云部分的层次问题进行研究,如社交传感器面临的侧信道攻击、基于云的社交网络的数据存储框架等,对于社交传感云系统整体安全还需要进一步探索。结合社交传感云的发展,本文提出了未来的研究方向。

6.1 与普适计算相结合

社交网络充当社交感应设备,为访问海量社交传感信息提供了机会。尽管已经存在许多以这种方式利用社交网络工具的应用程序,但是在普适计算服务的背景下,它们系统性地作为社交传感器的开发尚处于起步阶段。将社交传感与普及的 ICT 设备的传统传感手段相结合的前景,使得提供具有更高程度的情境感知的普适应用成为了可能,进一步缩短了数字与物理世界的差距,为用户提供了更全面、更个性化的社交传感云服务。将普适计算服务世界与社交网络和社交感知世界联系在一起,增强了虚拟现实,为社交传感云的安全提供了一个新的发展方向。

6.2 社交传感云系统与雾计算结合

图 4 给出了由传感层、雾设备和云数据中心构成的新型社交传感云体系,将雾计算技术引入社交传感云中,使得社交传感云可以更好地提供便捷、开放式的服务。雾计算是一种新型的边缘计算网络架构,雾设备可以承担一部分社交传感数据的计算和存储,从而将云计算扩展到网格边缘,有效避免了网络拥塞并保护了用户隐私。此外,雾计算通常具有很好的可扩展性,能够及时根据传感层的服务请求进行增量部署,为社交传感云服务的安全提供可靠的保障。

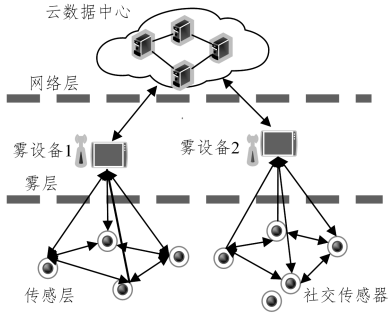


图 4 与雾计算结合的社交传感云体系

Fig. 4 Social sensor cloud system based on fog computing

6.3 虚拟化

基于虚拟化的社交传感云安全主要从社交数据共享传输和虚拟传感层处理的角度保证社交传感云安全。当社交传感器的数据传输到虚拟层时,由于社交传感器节点与传统无线传感器节点的差异性,导致已有的系统架构不完全适用于社交传感云,因此在下一步的研究工作中,可以根据社交传感云虚拟层的特性设计符合其安全需求的软件基础设施,如搭建云数据处理中心、虚拟层管理系统等,为保护社交传感云安全提供有效的方案。

6.4 增加信任

在社交传感云中,信任主要存在于社交网络中。在社交云环境下,从中提取信息、各种社交网络资源可能会在特定的上下文环境中告诉特定关系的强度。除了简单地利用信任作为资源共享的基础外,社交云中的其他决策可以基于社交结构(例如社交云存储或内容交付网络中的复制程度)的分析。这些决策可以根据社交云派生的信任度量,进一步考虑社交传感云系统安全和社交用户感知的可靠性。

未来的研究方向包括:1)构建用于签名网络的多层影响传播方案,结合多层关系类型,多模态传感器观察;2)结合现代社交网络中的实际应用,通过基于阈值的影响模式的积极性和消极性;3)开发用于增强目标节点的感知能力的推理方法。

6.5 绿色通信

能效是未来通信中一个非常严峻的挑战,我们称之为绿色通信。随着互联网、多媒体通信、云计算等业务的发展,通信业能源消耗呈现快速增长的态势,以低能耗为目标的绿色

通信正在成为未来无线通信发展的趋势。但是，移动社交用户提供接入服务所需的能源数量非常高。

(1)由于社交用户可能向社交传感云请求相同的数据，因此云可能会向社交用户提供大量相同的数据，传输重复的数据时在社交传感节点能量、社交网络资源以及云计算资源3个方面形成了浪费。

(2)当多个社交用户同时从云端请求数据时，需要同时将大量数据从云交付给多个社交用户。从云到多个社交用户的大量数据传输也增加了对云的计算资源、存储成本的消耗。

基于以上两个原因，未来需要研究在移动社交用户量不断增加的情况下，如何降低提供社交传感云服务及其网络运营商的能耗，以进一步提高社交传感云的安全以及实现绿色通信服务。

结束语 社交传感云是一个新兴的研究热点。社交传感器产生的社交数据信息量日益增加，需要通过云计算平台进行有效处理。目前社交数据传输过程容易受到恶意攻击，并且存在大量虚假信息，因此社交传感云需要采取合适的过滤方案对来自社交传感器的数据进行有效过滤，并且需要不断完善安全服务机制。目前，针对如何将社交传感器共享的数据有效且实时地传送给最终用户，但不暴露数据收集和管理的复杂性，已经采取了一些措施。但是，所提出的方案一般针对社交网络或云服务平台其中的一个方面，没有深入考虑社交传感云的结构特性。本文首先介绍了社交传感云的体系框架以及数据流，总结了社交传感云的新特性，强调了社交传感云安全的重要性，然后根据社交传感云的数据安全、网络安全、服务安全进行了分类介绍，分析对比了典型方案，探讨了未来社交传感云的发展方向，在与雾计算结合的方面给出了体系结构，为下一步的研究工作提供了参考。

参 考 文 献

[1] ZHU C, LEUNG V C M, RODRIGUES J J P C, et al. Social Sensor Cloud: Framework, Greenness, Issues, and Outlook[J]. IEEE Network, 2018, 32(5): 100-105.

[2] XU Q, SU Z, YU S, et al. Trust Based Incentive Scheme to Allocate Big Data Tasks with Mobile Social Cloud[J]. IEEE Transactions on Big Data, 2017, doi: 10.1109/TBDATA.2017.2764925.

[3] AAMIR T, BOUGUETTAYA A, DONG H, et al. Social-Sensor Cloud Service Selection[C]// IEEE International Conference on Web Services. IEEE, 2017: 508-515.

[4] WANG T, LI Y, JIA W J, et al. Research progress of sensor-cloud security[J]. Journal on Communications J. Communs., 2018, 39(3): 35-52.

[5] GHARINEIAT A, BOUGUETTAYA A, SELLIS T, et al. Crowdsourced Coverage as a Service: Two-Level Composition of Sensor Cloud Services[J]. IEEE Transactions on Knowledge and Data Engineering, 2017: 1384-1397.

[6] CHARD K, CATON S, RANA O, et al. Social Clouds: A Retrospective[J]. IEEE Cloud Computing, 2016, 2(6): 30-40.

[7] REYES R J R, DE MENDONCA F F D, DIAS K L. A Service-Oriented Architecture with Data Virtualization Support for Cloud-Based Wireless Sensor Networks[C]// 2017 VII Brazilian Symposium on Computing Systems Engineering (SBESC). IEEE, 2017: 199-204.

[8] CHANG C, SRIRAMA S N, LIYANAGE M. A service-oriented mobile cloud middleware framework for provisioning mobile sensing as a service[C]// 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2015: 124-131.

[9] RANI S, AHMED S H, TALWAR R, et al. Can Sensors Collect Big Data? An Energy Efficient Big Data Gathering Algorithm for WSN[J]. IEEE Transactions on Industrial Informatics, 2017: 1961-1968.

[10] NAKASHIMA K, YOKOYAMA M, TANIYAMA Y, et al. s3 system: A system for sharing social sensor data and analytical programs[C]// Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services. ACM, 2016: 147-152.

[11] ZENG J D, WANG T, JIA W J, et al. Research progress of sensor-cloud [J]. Journal of Computer Research and Development, 2017, 54(5): 925-939.

[12] PETRI I, DIAZ-MONTES J, RANA O, et al. Modelling and implementing social community clouds[J]. IEEE Transactions on Services Computing, 2017, 10(3): 410-422.

[13] CHATTERJEE S, LADIA R, MISRA S. Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure[J]. IEEE Transactions on Services Computing, 2017, 10(2): 203-216.

[14] AAMIR T, DONG H, BOUGUETTAYA A. Trust in social-sensor cloud service[C]// 2018 IEEE International Conference on Web Services (ICWS). IEEE, 2018: 359-362.

[15] BILECKI L F, FIORESE A. A Trust Reputation Architecture for Cloud Computing Environment[C]// 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2017: 614-621.

[16] BHATT S, KRISHNAMURTHY V. Controlled information fusion with risk-averse CVaR social sensors[C]// 2017 IEEE 56th Annual Conference on Decision and Control (CDC). IEEE, 2017: 2605-2610.

[17] REZVANI M, IGNJATOVIC A, BERTINO E, et al. A trust assessment framework for streaming data in wsns using iterative filtering[C]// 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). IEEE, 2015: 1-6.

[18] CHARD K, CATON S, RANA O, et al. Social cloud: Cloud computing in social networks[C]// 2010 IEEE 3rd International Conference on Cloud Computing. IEEE, 2010: 99-106.

[19] MRABET M, BEN SAIED Y, SAIDANE L A. Modeling correlation between QoS attributes for trust computation in cloud computing environments[C]// Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE, 2017: 488-497.

[20] CHARD K, BUBENDORFER K, CATON S, et al. Social Cloud Computing: A Vision for Socially Motivated Resource Sharing [J]. IEEE Transactions on Services Computing, 2012, 5(4): 551-563.

[21] MADRIA S, KUMAR V, DALVI R. Sensor Cloud: A Cloud of Virtual Sensors[J]. IEEE Software, 2014, 31(2): 70-77.

[22] AIKO Z, NAKASHIMA K, YOSHIHISA T, et al. A Social Sensor Visualization System for a Platform to Generate and Share Social Sensor Data[C]// 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2018, 2: 628-633.

[23] YI X,BOUGUETTAYA A,GEORGAKOPOULOS D,et al. Privacy protection for wireless medical sensor data[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 13(3):369-380.

[24] BIJARBOONEH F H,DU W,NGAI C H,et al. Cloud-Assisted Data Fusion and Sensor Selection for Internet-of-Things[J]. IEEE Internet of Things Journal,2015,3(3):257-268.

[25] LI F,WANG X,CHEN H,et al. Clickleak:keystroke leaks through multimodal sensors in cyber-physical social networks [J]. IEEE Access,2017,5:27311-27321.

[26] JIANG J,HAN G,WANG F,et al. An Efficient Distributed Trust Model for Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228-1237.

[27] WANG T,LI Y,FANG W,et al. A Comprehensive Trustworthy Data Collection Approach in Sensor-Cloud System[J]. IEEE Transactions on Big Data,2018,doi:10. 1109/TBDATA. 2018. 2811501.

[28] MUSAEV A,PU C. Landslide information service based on composition of physical and social sensors[C]// 2017 IEEE 33rd International Conference on Data Engineering (ICDE). IEEE, 2017:1415-1416.

[29] LAU R Y K. Toward a social sensor based framework for intelligent transportation[C]// 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE,2017:1-6.

[30] WANG G,GUI X L. Selecting and Trust Computing for Transaction Nodes in Online Social Networks[J]. Chinese Journal of Computers,2013,36(2):368-383.

[31] PRAVEENA A,SMYS S. Ensuring data security in cloud based social networks[C]// 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA). IEEE,2017,2:289-295.

[32] GULER B,VARAN B,TUTUNCUOGLU K,et al. Using Social Sensors for Influence Propagation in Networks With Positive and Negative Relationships[J]. IEEE Journal of Selected Topics in Signal Processing,2015,9(2):360-373.

[33] WANG E K,LI Y,YE Y,et al. A Dynamic Trust Framework for Opportunistic Mobile Social Networks[J]. IEEE Transactions on Network and Service Management,2017:319-329.

[34] XIA F,JEDARI B,YANG L T,et al. A Signaling Game for Uncertain Data Delivery in Selfish Mobile Social Networks[J]. IEEE Transactions on Computational Social Systems, 2017, 3(2):100-112.

[35] MOOSAVI H,BUI F M. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2014,9(9):1367-1379.

[36] HAN G,LIU L,JIANG J,et al. Analysis of energy-efficient connected target coverage algorithms for industrial wireless sensor networks[J]. IEEE Transactions on Industrial Informatics, 2017,13(1):135-143.

[37] MAHBOUBI H,MOEZZI K,AGHDAM A G,et al. Distributed deployment algorithms for improved coverage in a network of wireless mobile sensors[J]. IEEE Transactions on Industrial Informatics,2014,10(1):163-174.

[38] ANANTVALEE T,WU J. A survey on intrusion detection in mobile ad hoc networks[M]// Wireless Network Security. Boston:Springer,2007:159-180.

[39] BAIG Z A. Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks[J]. Computer Communications,2011,34(3):468-484.

[40] LIU J,YU J,SHEN S. Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds[J]. IEEE Transactions on Information Forensics and Security,2018,13(2):408-420.

[41] BORUJENI E M,RAHBARI D,NICKRAY M. The impact of security services on fog-based WSNs lifetime[C]// 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI). IEEE,2017:984-991.

[42] ZHU C,SHU L,LEUNG V C M,et al. Secure Multimedia Big Data in Trust-Assisted Sensor-Cloud for Smart City[J]. IEEE Communications Magazine,2017,55(12):24-30.

[43] CHARD K,CATON S,RANA O,et al. Social cloud:Cloud computing in social networks[C]// 2010 IEEE 3rd International Conference on Cloud Computing. IEEE,2010:99-106.

[44] KWAK D,LIU R,KIM D,et al. Seeing is believing:Sharing real-time visual traffic information via vehicular clouds[J]. IEEE Access,2016,4:3617-3631.

[45] GONG X,CHEN X,ZHANG J,et al. Exploiting social trust assisted reciprocity (STAR) toward utility-optimal socially-aware crowdsensing[J]. IEEE Transactions on Signal and Information Processing over Networks,2015,1(3):195-208.

[46] DINH T,KIM Y. An efficient interactive model for on-demand sensing-as-a-services of sensor-cloud[J]. Sensors,2016,16(7): 992.

[47] YUAN J,LI X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion[J]. IEEE Access, 2018, 6: 23626-23638.

[48] DINH T,KIM Y. An efcient sensor-cloud interactive model for on-demand latency requirement guarantee[C]// 2017 IEEE International Conference on Communications (ICC). IEEE,2017: 1-6.

[49] RACHKIDI E E,AGOULMINE N ,CHENDEB N,et al. Resources optimization and effcient distribution of shared virtual sensors in sensor-cloud[C]// 2017 IEEE International Conference on Communications (ICC). IEEE,2017:1-6.

[50] KIM S. An Effective Sensor Cloud Control Scheme based on a Two-stage Game Approach[J]. IEEE Access, 2018, PP(99): 20430-20439.

LIANG Jun-bin, born in 1979, Ph. D, professor, Ph. D supervisor. His main research interests include wireless sensor networks, network deployment and optimization.

ZHANG Min, born in 1994, postgraduate. Her research interests focus on wireless sensor networksand cloud computing.