doi: 10.3969/j.issn.1671-1122.2012.05.019

机会物联及其安全性探讨

郭斌[1]，於志文[1]，张大庆[1,2]，王柱[1,2]

（1. 西北工业大学陕西省嵌入式系统技术重点实验室，陕西西安 710072；
2. 法国国立电信学院，法国）

摘 要： 文章简要介绍了机会物联的由来及其内涵，并对其与人类社会之间的双向作用进行了分析，提出了物联网社会性的概念。在此基础上，就机会物联与人类行为的紧密关联进行分析，提出了机会物联所面临的涉及用户安全隐私方面的新的挑战和问题。针对这些新问题，对一些现有的研究工作进行了介绍，并对未来发展方向提出了建议。

关键词： 机会物联；信息传播；安全隐私；人类行为

中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2012）05-0068-02

The Security Challenges of the Opportunistic IoT

GUO Bin[1], YU Zhi-wen[1], ZHANG Da-qing[1,2], WANG Zhu[1,2]

（1. *Shaanxi Key Embedded System Technology Lab., Northwestern Polytechnical University, Xi'an* 710072, *China*
2. *Institute TELECOM SudParis, France*）

Abstract: This article presents the origin and the definition of Opportunistic IoT. Based on the description of the bi-directional effects between human society and the IoT, we propose the concept of the social side of the IoT. The tight-coupled relationship between opportunistic IoT and human behaviors raises a series of issues about user privacy and security. We make a brief review of existing efforts on these issues, and present some guidelines for future research.

Key words: opportunistic IoT; information dissemination; security and privacy; human behavior

1 机会物联

物联网（Internet of Things, IoT）的远景目标在于推动人类社会与物理世界的和谐融合，建立起一套社会化的感知体系。因此，研究物联网与人类学以及社会科学的交叉具有重要的科学意义。就目前而言，对物联网的研究还侧重于射频识别跟踪、服务支持、海量数据分析、安全隐私保护等方面[1]，对物联网社会性方面的研究还比较少见。近年来，笔者一直在从事有关物联网社会性方面的研究，在2011年IEEE物理信息系统和物联网（CPSCom' 11& iThings' 11）国际会议上就物联网的社会性，特别是对个体和群体行为的感知和理解进行了阐述[2]。在此基础上，笔者在《中国计算机学会通讯》2011年第12期上进一步提出了“机会物联”（Opportunistic IoT）的概念[3]，并受邀在2012年五月召开的第十六届IEEE计算机支持协作设计国际学术会议（CSCWD' 12）上就“机会物联”进行主题演讲。

机会物联是以短距离无线通讯技术（蓝牙、WiFi等）为基础，利用智能物体在移动过程中的机会接触（Opportunistic Contact）所构成的具有临时性、自组织（Ad hoc）等特点的机会网络（Opportunistic Networks）来进行信息、资源以及服务的传播与共享。这里指的智能物体包括智能手机、可穿戴设备、汽车等，它们已经成为人们日常生活中的亲密伴侣（如人们驾车出行、携带手机进行日常工作和社会活动），在人类移动的过程中实现机会接触。这里给出一个机会物联的例子：在一个咖啡厅，用户A和其周围一定范围内的用户可以通过移动自组织方式进行自主连接，并进而进行本地通讯和信息共享服务。

如图1所示，人类社会和机会物联网不仅在物理层面上密切相关（如前所述，手机、汽车都是人们日常工作活动的贴身伴侣），在逻辑和计算层面上也彼此关联、相互作用。一方面，由机会物联网获取的大规模实时感知数据，经过计算分析和处理，获得个体和群体行为及交互方面的信息；另一方面，人类社会的各种属性如人类移动性（Human Mobility）[4]、社会网络结构（Social Network Structure）[5]及社会特征（如活跃度Social Popularity、意愿性Social Willingness等）反过来会对有关机会信息传播和共享（如

收稿时间： 2012-03-26

作者简介： 郭斌（1980-），男，山西，副教授，博士，主要研究方向：普适计算、物联网、社群智能；於志文（1977-），男，湖北，西北工业大学计算机学院副院长，教授，博士，主要研究方向：普适计算、社会感知计算；张大庆（1964-），男，河南，教授，博士，主要研究方向：普适计算、社群智能；王柱（1983-），男，河北，博士研究生，主要研究方向：普适计算、机会网络。

代理选择、传输延迟等）造成影响。机会物联网与人类社会的这种紧密相互作用可称为“物联网的社会性（The Social Side of the Internet of Things）”[6]。

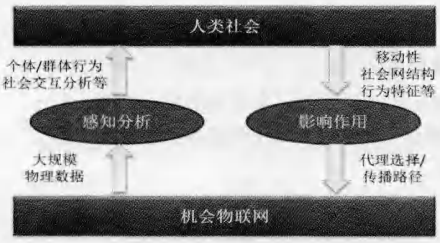

图1 机会物联网与人类社会的双向交互作用

2 机会物联安全性

机会物联基于人们的社会特征及其在在物理世界的交互行为，这为开发一系列创新性的“以人为中心（Human-Centric）”的应用，如社会机缘网络（Opportunistic Social Network）、机会广告传播（Opportunistic Advertising）等提供了可能[6]。然而，从个人设备中抽取和共享个体行为及社会交互特性来开发机会物联服务不可避免的会带来安全和隐私方面的问题。例如，在机会广告传播服务中，一些涉及用户隐私的信息如个体位置和感兴趣地点（Point of Interests）等很容易会被攻击者所获取。这就给机会物联带来了新的挑战，即如何提供可信的机制保护用户数据的隐私及安全，从而提高公众参与的积极性。机会物联所具有的临时性、随机性、匿名性、动态性等特点，使得在随机而遇的计算设备之间构建安全可信的交互机制这一问题更为复杂化。下面就机会物联的安全性涉及到的几个方面（安全、隐私保护及信任）及一些现有的研究进展分别进行说明。

1）安全机制。机会物联环境下，一般无法在智能物体加入网络之前识别其是否为恶意攻击者[7]，也就是说无法保证恶意攻击者不会加入网络，甚至在攻击者加入网络但是尚未表现出恶意行为之前都无法对其进行识别。导致在机会物联网络中，无法实现仅在非恶意设备之间安全地分发密钥。因此，仅仅依赖于加密的认证机制无法满足机会物联对于安全性的要求。较为可行的安全机制是基于机会物联所具有的社会性，将社会网络结构作为安全认证的基础[8]。通过发现智能物体在物理和逻辑上所具有的共性，构建物体社群（Smart Object Community）以增强机会物联网络的安全性。通过社会网络结构增强网络安全性的思路本身并不新颖，其它领域的研究者已经进行过相关的研究，例如基于社会网络结构的垃圾邮件过滤[9]。然而，在机会物联网络下利用社会网络结构却是一项全新而富有挑战性的工作，因为此种环境下基于中心服务器或者在线认证的经典安全机制已不再可行。所以需要综合考虑机会物联网络以及社会网络的特点，研究新的安全机制。

2）隐私保护机制。一般情况下，基于机会物联的应用服务需要获取诸如设备使用者的档案信息（User Profile）、实时位置等隐私数据[3]。攻击者可以基于这些数据进行分析，进而获取用户的行为规律、兴趣偏好等信息，从而使得用户的隐私处于高度危险之中。这就给机会物联带来了新的挑战，即如何在用户贡献数据的同时保证其私密性。针对这一挑战，研究者已经进行了很多探索，提出了多种隐私保护技术与机制。如来自美国达特默斯学院的AnonySense项目[10]提出了一种多层次的用户隐私保护架构，从三个方面实现对用户隐私的保护。首先用户设备可以匿名获取数据采集任务；之后基于时空匿名技术（Spatio-Temporal Cloaking），在保证数据精度的前提下将单个用户的特性向系统隐藏；最后通过k-匿名技术（k-Anonymity）提高用户数据对于应用服务的隐私性。来自匈牙利的研究人员都勒等人提出了一种机会网络环境下基于“隐藏（Hide）”和“虚报（Lie）”的用户档案信息隐私保护策略[11]。用户一方面将自己感兴趣的属性项“隐藏”为不感兴趣；另一方面将自己不感兴趣的属性项“虚报”为感兴趣。然而，对于数据隐私的保护仅仅局限于技术层面的保障可能是不够的，还需要在制度和法律层面对如何使用个人敏感数据的形成相应的规范。

3）信任机制。在机会物联所支持的社会协作应用中，需要利用匿名贡献者来收集或传播数据。在此过程中如果缺乏有效的机制来确定数据源或代理的可信性，则会对应用造成影响。例如，某源节点可能会发送错误信息；某中继节点可能会修改或伪造自己所承担的传递任务。因此，需要引入信任机制来保证信息传播和共享的可靠性。然而，传统的安全方案往往需要集中式的在线信任授权，不能很好的适应机会网络所具有的随机性和分布式的特点。在第三十届INFOCOM国际会议上，来自美国宾夕法尼亚州立大学的研究人员提出一种基于多个设备互相进行位置信息可信性验证的机制，要求互相验证的多个设备处于无线通信范围（如蓝牙作用范围）之内[12]。然而这一机制无法应对集体性攻击，即多个攻击者处于同一位置发起攻击。为此，鉴于机会物联网络和社会网络之间存在的关联，可以通过分析社会网络结构和属性来探索适合机会物联特性的信任模型。此外，还可以借鉴P2P分布式网络和Ad hoc网络中的行之有效的声誉机制来增强机会物联节点间的信任关系[13,14]。

3 总结与展望

机会物联为物联网的研究和发展带来了新的机遇，通过普适计算、物联网技术、与社会科学、认知心理学的交叉融合，感知人类社会的内在活动规律，探索人类行为对机会信息传播和共享的影响，对于物理信息空间与人类社会的和谐融合、互促发展具有积极意义。然而，机会物联的社会性也为人类的数据安全及隐私保护等带来了新的挑战。以社会学、

下转第77页

责任性，出现问题及时追查等；对远程拨号用户必需进行合理的权限限制，在经过认证的连接上应该仅能够行使受限的网络功能与应用。

2.3 安全管理体系

规范化管理是SCADA系统安全的保障。以“三分技术，七分管理”为原则，建立信息安全组织保证体系，落实责任制，明确各有关部门的工作职责，实行安全责任追究制度；建立健全各种安全管理制度，保证SCADA系统的安全运行；建立安全培训机制，对所有人员进行信息安全基本知识、相关法律法规、实际使用安全产品的工作原理、安装、使用、维护和故障处理等的培训，以强化安全意识，提高技术水平和管理水平。

2.4 安全服务体系

建立完善的安全服务体系，进行SCADA系统上线前的安全测评、上线后的安全风险评估、安全整改加固以及监控应急响应，用于保护、分析对系统资源的非法访问和网络攻击，并配备必要的应急设施和资源，统一调度，形成对重大安全事件（遭到黑客、病毒攻击和其他人为破坏等）快速响应的能力。

2.5 安全基础设施

SCADA系统安全防护的基础安全设施主要包括建立基于公钥技术的数字证书体系以及远程容灾备份体系。数字证书体系为SCADA控制中心和站控系统的关键用户和设备提供数字证书服务，实现高强度的身份认证、安全的数据传输以及可靠的行为审计。远程容灾备份体系应尽量采用应用级的容灾备份，且要做好网络链路的冗余和应用的异地接管，如果SCADA系统出现故障时就能够及时、准确地恢复。同时，应制定合理的远程容灾备份策略和进行定期恢复验证，一方面可以验证容灾备份数据的可用性，没有经过验证的备份风险非常大，这样就可以发现备份没有完成、或者备份错误等情况；另一方面也可以锻炼系统管理员的灾难处理能力，避免在出现故障时无从下手[6]。

3 结束语

随着我国基础产业“两化融合”进程的不断加快，SCADA系统的应用日益广泛，其安全防护已纳入国家战略，建立工控SCADA的信息安全防护体系，确保SCADA系统的安全、稳定和优质运行，能更好地为国民经济高速发展和满足人民生活需要服务。（责编 程斌）

参考文献：

[1] 方兰，王春雷，赵刚．SCADA系统结构特点及其脆弱性分析[C]. 全国抗恶劣环境计算机第十七届学术年会论文集，2007.

[2] 兰昆，饶志宏，唐林等．工业SCADA系统网络的安全服务框架研究[J]. 信息安全与通信保密，2010，(03)：47-49.

[3] Joe St Sauver. SCADA Security and Critical Infrastructure[C]. Oregon Infraguard Meeting 2004.

[4] 高国辉．西门子被曝工业系统漏洞 或影响多数工业化国家[N]. 南方日报，2011-6-8.

[5] P.A.S. Ralston et al. Cyber security risk assessment for SCADA and DCS networks[C]. ISA Transactions 46 (2007): 583-594.

[6] 余勇，林为民，邓松，车建华．智能电网中的云计算应用及安全研究[J]. 信息网络安全，2011，(06)：41-43.

上接第69页

行为科学等为指导，对机会物联环境下产生的新安全问题进行深入分析和研究，将为问题的解决提供新的解决思路。同时也应该在制度层面加强对机会物联环境下个体信息的保护，从而促进用户参与，推动物联网这一新兴产业及其创新应用的发展。（责编 程斌）

参考文献：

[1] L. Atzori, A. Iera, G. Morabito. The Internet of Things: A Survey[J]. Computer Networks, 2010, 54(15): 2787-2805.

[2] B. Guo, D. Zhang, Z. Wang. Living with Internet of Things: The Emergence of Embedded Intelligence. Proc[C]. of the 2011 IEEE International Conference on Cyber, Physical, and Social Computing, Dalian, China, 2011.

[3] 郭斌，於志文，张大庆，周兴社．机会物联-兼谈物联网的社会性[J]. 中国计算机学会通讯，2011，7(12)：50-55.

[4] D.R. Choffnes, F.E. Bustamante. An integrated mobility and traffic model for vehicular wireless networks. Proc[C]. of the 2nd ACM International Workshop on Vehicular Ad hoc Networks, 2005, pp. 69-78.

[5] N. Eagle, et al. Inferring Social Network Structure using Mobile Phone Data[C]. Proceedings of the National Academy of Sciences (PNAS), 2007, 106(36):15274-15278.

[6] B. Guo, Z. Yu, D. Zhang, X. Zhou. Opportunistic IoT: Exploring the Social Side of the Internet of Things[C]. The 16th IEEE International Conference on Computer Supported Cooperative Work in Design (CSCWD 2012), Wuhan, China, 2012.

[7] L. Lilien, Z. H. Kamal, A. Gupta. Opportunistic Networks: Research Challenges in Specializing the P2P Paradigm[C]. Proc. 3rd International Workshop on P2P Data Management, Security and Trust, 2006, pp. 722-726.

[8] M. Conti, M. Kumar. Opportunities in Opportunistic Computing[J]. IEEE Computer, 2010, 43(01): 42-50.

[9] J.S. Kong, B.A. Rezaei, N. Sarshar, V.P. Roychowdhury, P.O. Boykin, Collaborative spam filtering using e-mail networks[J]. IEEE Computer, 2006, 39(08): 67-73.

[10] A. Kapadia , N. Tri , C. Cornelius, D. Peebles, D. Kotz. AnonySense: Opportunistic and Privacy-Preserving Context Collection[C]. Proc. of 6th International Conferenfce on Pervasive Computing, 2008, pp. 280-297.

[11] L. D ó ra, Tam á s Holczer. Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks. Proc[C]. of the Second International Workshop on Mobile Opportunistic Networking, 2010, 135-142.

[12] Z. Zhu, G. Cao. Applaus: A Privacy Preserving Location Proof Updating System for Location-based Services. Proc[C]. of IEEE INFOCOM' 11, 2011, pp. 1889-1897.

[13] R. Ma. An incentive mechanism for P2P networks. Proc[C]. of DCS, 2004, 516-523.

[14] J. J. Jaramillo, R. Srikant. Darwin: Distributed and adaptive reputation mechanism for wireless ad-hoc networks[C]. Proc. of MobiCom, 2007.