基于物联网的网络信息安全体系

Network Information Security Architecture Based on Internet of Things

中图分类号：TN91 文献标志码：A 文章编号：1009-6868 (2011) 01-0017-04

刘宴兵/LIU Yanbing
胡文平/HU Wenping
杜江/DU Jiang
（重庆邮电大学，重庆 400065）
(Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

摘要： 物联网是计算机、互联网与移动通信网等相关技术的演进和延伸，其核心共性技术、网络与信息安全技术以及关键应用是物联网的主要研究内容。物联网感知节点大都部署在无人监控环境，并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台，传统网络安全措施不足以提供可靠的安全保障。物联网安全研究将主要集中在物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律的制订等方面。

关键词： 物联网；安全结构；射频识别；隐私保护

Abstract: Internet of Things (IoT) is seen as the evolution of related technologies and applications such as Internet and mobile networks. Future research into IoT will focus on generic technology, information security, and critical applications. Sensor nodes in IoT are deployed in an unattended environment, and the IoT platform is extended on the basis of the sensor network and application platforms in the existing infrastructure. So traditional network security measures are insufficient for providing reliable security in IoT. Future research into IoT security will focus on security architecture, privacy protection mode, law-making, and terminal security.

Key words: Internet of things; security architecture; radio frequency identification; privacy protection

每一次大的经济危机背后都会悄然催生出一些新技术，这些技术往往会成为经济走出危机的巨大推力。

2009年，3G在中国正式步入商业化阶段，各大电信运营商、设备制造商、消费电子厂商都将目光集中在3G市场的争夺。随着3G时代的到来，涌现的一些新技术解决了网络带宽问题，极大地改变了网络的接入方式和业务类型。其中物联网被认为是继计算机、互联网与移动通信网之后的又一次信息产业浪潮，代表了下一代信息技术的方向。

物联网除与传统的计算机网络和通信网络技术有关外，还涉及到了许多新的技术，如射频技术、近距离通信和芯片技术等。物联网正以其广泛的应用前景成为人们研究的热点，同时，云计算作为一种新的计算模式，其发展为物联网的实现提供了重要的支撑。

“物联网”最早由MIT Auto-ID中心Ashton教授1999年在研究射频标签(RFID)技术时提出。2003年，美国《技术评论》提出传感网络技术将是未来改变人们生活的十大技术之首，从此物联网逐渐走进了人们的视野。2005年国际电信联盟发布《ITU互联网报告2005：物联网》。报告引用了“物联网”的概念并指出无所不在的“物联网”通信时代即将来临，世界上所有的物体都可以通过因特网进行信息交互，射频识别技术、传感器技术、纳米技术、智能嵌入技术将得到更加广泛的应用。2009年，美国总统奥巴马与美国工商业领袖举行了一次圆桌会议，对IBM首席执行官彭明盛提出的“智慧地球”这一概念给予了积极评价，并把它上升至美国的国家战略。2009年8月，温家宝总理在无锡考察时提出“感知中国”的发展战略，之后物联网被写入政府工作报告并被正式列为中国五大国家新兴战略性产业之一。

随着物联网在国家基础设施、自然资源、经济活动、医疗等方面的广泛应用，物联网的安全问题必然上升到国家层面。

1 物联网相关概念

由于物联网还处于发展初期，业界对物联网定义尚未达成共识。维基百科中物联网被描述为把传感器装备到电网以及家用电器等各种真实物体上，通过互联网连接起来，进而运行特定的程序，达到远程控制或者实现物与物的直接通信的网络。

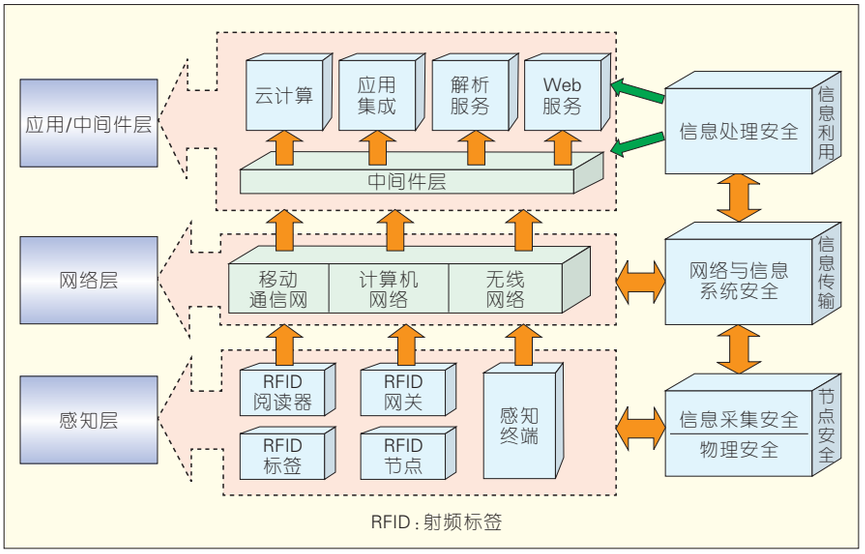
基金项目：信息网络安全公安部重点实验室开放课题(C09608)；重庆市自然科学基金重点项目(2009BA2024)；重庆高校优秀成果转化资助项目(Kjzh10206)

2010年中国政府工作报告把物联网定义为通过信息传感设备，按照约定的协议，把任何物品与互联网连接起来，进行通信和信息交换，以实现智能化识别、定位、跟踪、监控和管理的一种网络[1]。而中国工程院邬贺铨院士认为物联网相当于互联网上面向特定任务来组织的专用网络，即原有通信网络中的一个应用拓展，其突出的特点是包含了一个原有通信网中不存在的底层感知层[2]。

按照人们对物联网的理解，物联网是指在物理世界的实体中部署具有一定感知能力、计算能力和执行能力的嵌入式芯片和软件，使之成为“智能物体”，通过网络设施实现信息传输、协同和处理，从而实现物与物、物与人之间的互联。物联网应该具备3个特征：一是全面感知，即利用RFID、传感器等随时随地获取物体的信息；二是可靠传递，通过各种电信网络与互联网的融合，将物体的信息实时准确地传递出去；三是智能处理，利用云计算、模糊识别等各种智能计算技术，对海量数据和信息进行分析和处理，对物体实施智能化的控制，其中智能处理和全面感知是物联网的核心内容。另外，物联网可用的基础网络有很多，根据其应用需要可以用公网也可以用专网，通常互联网被认作是最适合作为物联网的基础网络。

2 物联网安全问题

随着物联网建设的加快，物联网的安全问题必然成为制约物联网全面发展的重要因素。在物联网发展的高级阶段，由于物联网场景中的实体均具有一定的感知、计算和执行能力，广泛存在的这些感知设备将会对国家基础、社会和个人信息安全构成新的威胁。一方面，由于物联网具有网络技术种类上的兼容和业务范围上无限扩展的特点，因此当大到国家电网数据小到个人病例情况都接到看似无边界的物联网时，将可能导致更多的公众个人信息在任何时候，任何地方被非法获取；另一方面，随着国家重要的基础行业和社会关键服务领域如电力、医疗等都依赖于物联网和感知业务，国家基础领域的动态信息将可能被窃取。所有的这些问题使得物联网安全上升到国家层面，成为影响国家发展和社会稳定的重要因素。



▲图1 物联网的安全层次结构

物联网相较于传统网络，其感知节点大都部署在无人监控的环境，具有能力脆弱、资源受限等特点，并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台，传统网络安全措施不足以提供可靠的安全保障，从而使得物联网的安全问题具有特殊性。所以在解决物联网安全问题时候，必须根据物联网本身的特点设计相关的安全机制。

3 物联网的安全层次模型及体系结构

考虑到物联网安全的总体需求就是物理安全、信息采集安全、信息传输安全和信息处理安全的综合，安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性，因此结合物联网分布式连接和管理(DCM)模式，本文给出相应的安全层次模型(如图1所示)，并结合每层安全特点对涉及的关键技术进行系统阐述[3]。

3.1 感知层安全

物联网感知层的任务是实现智能感知外界信息功能，包括信息采集、捕获和物体识别，该层的典型设备包括RFID装置、各类传感器(如红外、超声、温度、湿度、速度等)、图像捕捉装置(摄像头)、全球定位系统(GPS)、激光扫描仪等，其涉及的关键技术包括传感器、RFID、自组织网络、短距离无线通信、低功耗路由等。

(1)传感技术及其联网安全

作为物联网的基础单元，传感器在物联网信息采集层面能否如愿以偿完成它的使命，成为物联网感知任务成败的关键。传感器技术是物联网技术的支撑、应用的支撑和未来泛在网的支撑。传感器感知了物体的信息，RFID赋予它电子编码。传感网到物联网的演变是信息技术发展的阶段表征[4]。传感技术利用传感器和多跳自组织网，协作地感知、采集网络覆盖区域中感知对象的信息，并发布给向上层。由于传感网络本身具有：无线链路比较脆弱、网络拓扑动态变化、节点计算能力、存储能力

▼表1 传感网组网技术面临的安全问题

层次	受到的攻击
物理层	物理破坏、信道阻塞
链路层	制造碰撞攻击、反馈伪造攻击、耗尽攻击链路层阻塞
网络层	路由攻击、虫洞攻击、女巫攻击、陷洞攻击、Hello 洪泛攻击
应用层	去同步、拒绝服务流等

和能源有限、无线通信过程中易受到干扰等特点，使得传统的安全机制无法应用到传感网络中。传感技术的安全问题如表1所示。

目前传感器网络安全技术主要包括基本安全框架、密钥分配、安全路由和入侵检测和加密技术等。安全框架主要有SPIN(包含SNEP和uTESLA两个安全协议)，Tiny Sec、参数化跳频、Lisp、LEAP协议等。传感器网络的密钥分配主要倾向于采用随机预分配模型的密钥分配方案。安全路由技术常采用的方法包括加入容侵策略。入侵检测技术常常作为信息安全的第二道防线，其主要包括被动监听检测和主动检测两大类。除了上述安全保护技术外，由于物联网节点资源受限，且是高密度冗余撒布，不可能在每个节点上运行一个全功能的入侵检测系统(IDS)，所以如何在传感网中合理地分布IDS，有待于进一步研究[5]。

(2)RFID相关安全问题

如果说传感技术是用来标识物体的动态属性，那么物联网中采用RFID标签则是对物体静态属性的标识，即构成物体感知的前提[6]。RFID是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据。识别工作无须人工干预。RFID也是一种简单的无线系统，该系统用于控制、检测和跟踪物体，由一个询问器(或阅读器)和很多应答器(或标签)组成。

通常采用RFID技术的网络涉及的主要安全问题有：(1)标签本身的访问缺陷。任何用户(授权以及未授权的)都可以通过合法的阅读器读取RFID标签。而且标签的可重写性使得标签中数据的安全性、有效性和完整性都得不到保证。(2)通信链路的安全。(3)移动RFID的安全。主要存在假冒和非授权服务访问问题。目前，实现RFID安全性机制所采用的方法主要有物理方法、密码机制以及二者结合的方法。

3.2 网络层安全

物联网网络层主要实现信息的转发和传送，它将感知层获取的信息传送到远端，为数据在远端进行智能处理和分析决策提供强有力的支持。考虑到物联网本身具有专业性的特征，其基础网络可以是互联网，也可以是具体的某个行业网络。物联网的网络层按功能可以大致分为接入层和核心层，因此物联网的网络层安全主要体现在两个方面。

(1)来自物联网本身的架构、接入方式和各种设备的安全问题

物联网的接入层将采用如移动互联网、有线网、Wi-Fi、WiMAX等各种无线接入技术。接入层的异构性使得如何为终端提供移动性管理以保证异构网络间节点漫游和服务的无缝移动成为研究的重点，其中安全问题的解决将得益于切换技术和位置管理技术的进一步研究。另外，由于物联网接入方式将主要依靠移动通信网络。移动网络中移动站与固定网络端之间的所有通信都是通过无线接口来传输的。然而无线接口是开放的，任何使用无线设备的个体均可以通过窃听无线信道而获得其中传输的信息，甚至可以修改、插入、删除或重传无线接口中传输的消息，达到假冒移动用户身份以欺骗网络端的目的。因此移动通信网络存在无线窃听、身份假冒和数据篡改等不安全的因素。

(2)进行数据传输的网络相关安全问题

物联网的网络核心层主要依赖于传统网络技术，其面临的最大问题是现有的网络地址空间短缺。主要的解决方法寄希望于正在推进的IPv6技术。IPv6采纳IPsec协议，在IP层上对数据包进行了高强度的安全处理，提供数据源地址验证、无连接数据完整性、数据机密性、抗重播和有限业务流加密等安全服务。但任何技术都不是完美的，实际上IPv4网络环境中大部分安全风险在IPv6网络环境中仍将存在，而且某些安全风险随着IPv6新特性的引入将变得更加严重[7]：首先，拒绝服务攻击(DDoS)等异常流量攻击仍然猖獗，甚至更为严重，主要包括TCP-flood、UDP-flood等现有DDoS攻击，以及IPv6协议本身机制的缺陷所引起的攻击。其次，针对域名服务器(DNS)的攻击仍将继续存在，而且在IPv6网络中提供域名服务的DNS更容易成为黑客攻击的目标。第三，IPv6协议作为网络层的协议，仅对网络层安全有影响，其他(包括物理层、数据链路层、传输层、应用层等)各层的安全风险在IPv6网络中仍将保持不变。此外采用IPv6替换IPv4协议需要一段时间，向IPv6过渡只能采用逐步演进的办法，为解决两者间互通所采取的各种措施将带来新的安全风险。

3.3 应用层安全

物联网应用是信息技术与行业专业技术的紧密结合的产物。物联网应用层充分体现物联网智能处理的特点，其涉及业务管理、中间件、数据挖掘等技术。考虑到物联网涉及多领域多行业，因此广域范围的海量数据信息处理和业务控制策略将在安全性和可靠性方面面临巨大挑战，特别是业务控制、管理和认证机制、中间件以及隐私保护等安全问题显

得尤为突出。

(1)业务控制和管理

由于物联网设备可能是先部署后连接网络，而物联网节点又无人值守，所以如何对物联网设备远程签约，如何对业务信息进行配置就成了难题。另外，庞大且多样化的物联网必然需要一个强大而统一的安全管理平台，否则单独的平台会被各式各样的物联网应用所淹没，但这样将使如何对物联网机器的日志等安全信息进行管理成为新的问题，并且可能割裂网络与业务平台之间的信任关系，导致新一轮安全问题的产生。传统的认证是区分不同层次的，网络层的认证负责网络层的身份鉴别，业务层的认证负责业务层的身份鉴别，两者独立存在。但是大多数情况下，物联网机器都是拥有专门的用途，因此其业务应用与网络通信紧紧地绑在一起，很难独立存在。

(2)中间件

如果把物联网系统和人体做比较，感知层好比人体的四肢，传输层好比人的身体和内脏，那么应用层就好比人的大脑，软件和中间件是物联网系统的灵魂和中枢神经。目前，使用最多的几种中间件系统是：CORBA、DCOM、J2EE/EJB以及被视为下一代分布式系统核心技术的Web Services。

在物联网中，中间件处于物联网的集成服务器端和感知层、传输层的嵌入式设备中。服务器端中间件称为物联网业务基础中间件，一般都是基于传统的中间件(应用服务器、ESB/MQ等)，加入设备连接和图形化组态展示模块构建；嵌入式中间件是一些支持不同通信协议的模块和运行环境。中间件的特点是其固化了很多通用功能，但在具体应用中多半需要二次开发来实现个性化的行业业务需求，因此所有物联网中间件都要提供快速开发(RAD)工具。

(3)隐私保护

在物联网发展过程中，大量的数据涉及到个体隐私问题(如个人出行路线、消费习惯、个体位置信息、健康状况、企业产品信息等)，因此隐私保护是必须考虑的一个问题。如何设计不同场景、不同等级的隐私保护技术将是为物联网安全技术研究的热点问题[8]。当前隐私保护方法主要有两个发展方向：一是对等计算(P2P)，通过直接交换共享计算机资源和服务；二是语义Web，通过规范定义和组织信息内容，使之具有语义信息，能被计算机理解，从而实现与人的相互沟通[9]。

4 物联网安全的非技术因素

目前物联网发展在中国表现为行业性太强，公众性和公用性不足，重数据收集、轻数据挖掘与智能处理，产业链长但每一环节规模效益不够，商业模式不清晰。物联网是一种全新的应用，要想得以快速发展一定要建立一个社会各方共同参与和协作的组织模式，集中优势资源，这样物联网应用才会朝着规模化、智能化和协同化方向发展。物联网的普及，需要各方的协调配合及各种力量的整合，这就需要国家的政策以及相关立法走在前面，以便引导物联网朝着健康稳定快速的方向发展。人们的安全意识教育也将是影响物联网安全的一个重要因素。

5 结束语

物联网安全研究是一个新兴的领域，任何安全技术都伴随着具体的需求应运而生，因此物联网的安全研究将始终贯穿于人们的生活之中。从技术角度来说，未来的物联网安全研究将主要集中在开放的物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律的制订等几个方面。

6 参考文献

[1] 2010年政府工作报告 [EB/OL]. [2010-03-15]. http://www.china.com.cn/policy/txt/ 2010-03/ 15/content_19612372_8.htm.
[2] 邬贺铨. 物联网是互联网运用的拓展 更具专业性 [EB/OL]. [2010-03-15]. http://news.163.com/10/1028/15/6K3H05RP00014JB5.html.
[3] 刘宴兵，胡文平. 物联网安全模型及其关键技术 [J]. 数字通信, 2010,37(4):28-29.
[4] 传感器：物联网成引擎 新技术催生新机遇 [N]. 中国电子报, 2010-07-13.
[5] 李晓维. 无线传感器网络技术 [M]. 北京：北京理工大学出版社, 2007: 241-246.
[6] 张福生. 物联网：开启全新生活的智能时代 [M]. 太原：山西人民出版社, 2010: 175-184.
[7] 王帅, 沈军, 金华敏. 电信IPv6网络安全保障体系研究 [J]. 电信科学, 2010,26(7):10-13.
[8] MEDAGLIA C M, SERBANATI A. An Overview of Privacy and Security Issues in the Internet of Things [C]//The Internet of Things: Proceedings of the 20th Tyrrhenian Workshop on Digital Communications, Sep 2-4, 2009, Sardinia, Italy. Berlin, Germany: Springer-Verlag, 2010:389-394.
[9] SAVRY O, VACHERAND F. Security and Privacy Protection of Contactless Devices [C]// The Internet of Things: Proceedings of the 20th Tyrrhenian Workshop on Digital Communications, Sep 2-4, 2009, Sardinia, Italy. Berlin, Germany: Springer-Verlag, 2010: 409-418.

收稿日期：2010-11-10

作者简介

刘宴兵，重庆邮电大学教授、博士；主要研究领域为网络接入控制和网络安全；先后主持基金项目10项，获得国家科技进步奖1项、省部级奖励2项；已发表学术论文50篇(其中SCI收录9篇，EI收录22篇)，出版专著2部，申请发明专利5项。

胡文平，重庆邮电大学通信工程专业在读硕士研究生；主要研究领域为物联网以及移动互联网安全技术。

杜江，韩国仁荷大学计算机学院硕士毕业；重庆邮电大学副教授；研究方向为信息安全；已在核心期刊发表论文20篇。