



信息科学技术学术著作丛书

# 物联网安全

胡向东 魏琴芳 向敏 等著

3



科学出版社

TP393.4/262

2012

信息科学技术学术著作丛书

# 物联网安全

胡向东 魏琴芳 向敏等 著

北方工业大学图书馆



C00272353

科学出版社

北京

## 内 容 简 介

本书是作者从事多年物联网安全相关科研工作实践的结晶。本书较全面、系统、深入地论述了物联网安全的基本理论、专门技术和最新发展。全书共 14 章,内容包括绪论、物联网安全的密码理论、无线传感器网络安全概述、密钥管理、非正常节点的识别、入侵检测、认证、安全成簇、安全数据融合、安全路由、安全定位、物联网中的抗干扰、射频识别的隐私与安全、物联网嵌入式系统的安全设计。

本书可供从事物联网安全和可靠应用的管理决策人员、与物联网安全相关领域应用和设计开发的研究人员、工程技术人员参考,也可作为高等院校物联网工程、信息安全、测控技术与仪器、自动化、通信工程、计算机应用等专业高年级本科生和研究生教材。

### 图书在版编目(CIP)数据

物联网安全/胡向东等著. —北京:科学出版社,2012  
(信息科学技术学术著作丛书)  
ISBN 978-7-03-033913-3

I. 物… II. 胡… III. ①互连网络-应用-物流②互连网络-安全技术  
IV. ①TP393.4②F253.9

中国版本图书馆 CIP 数据核字(2012)第 053334 号

责任编辑:张艳芬 / 责任校对:包志虹  
责任印制:赵 博 / 封面设计:陈 敬

科学出版社出版

北京东黄城根北街 16 号

邮政编码:100717

<http://www.sciencep.com>

深海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

\*

2012 年 4 月第 一 版 开本:B5(720×1000)

2012 年 4 月第一次印刷 印张:22 3/4

字数:436 000

定价:72.00 元

(如有印装质量问题,我社负责调换)

## 作者简介



胡向东(1971— ),博士,教授,中国计算机学会计算机安全专业委员会委员、教育部“工程应用型自动化专业课程体系研究与教材建设委员会”委员,重庆市第二届学术技术带头人,“传感器与自动检测技术”国家精品课程负责人。

主要从事网络化测控及其信息安全、复杂系统建模、仿真与优化等方向的研究工作。作为项目负责人承担国家高新技术研究计划(“863”计划)项目、国家科技重大专项、国家自然科学基金项目等 20 余项,主持重庆市重点教研研究课题等 10 项;在国际、国内重要期刊和会议上发表学术论文 50 余篇,其中 30 余篇被三大检索系统收录;主编普通高等教育“十一五”国家级规划教材《应用密码学》、《应用密码学(第 2 版)》,撰写《传感技术》、《传感器与检测技术》、《智能检测技术与系统》、《物联网安全》等著作 8 部;获重庆市科技进步奖一等奖、三等奖各 1 项,获国家级教学成果奖二等奖 1 项、重庆市高等教育教学成果奖二等奖 1 项;指导学生获全国计算机仿真大赛全国二等奖 2 项、全国大学生“飞思卡尔”杯智能汽车竞赛全国总决赛二等奖 1 项。

## 《信息科学技术学术著作丛书》序

21 世纪是信息科学技术发生深刻变革的时代,一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起,悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展;如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力;如何抓住信息技术深刻发展变革的机遇,提升我国自主创新和可持续发展的能力?这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台,将这些科技成就迅速转化为智力成果,将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上,经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术,微电子、光电子和量子信息技术,超级计算机、软件和信息存储技术,数据知识化和基于知识处理的未来信息服务业,低成本信息化和用信息技术提升传统产业,智能与认知科学、生物信息学、社会信息学等前沿交叉科学,信息科学基础理论,信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强,具有一定的原创性;体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版,能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时,欢迎广大读者提出好的建议,以促进和完善丛书的出版工作。

中国科学院计算技术研究所所长



## 前 言

为加快转变经济发展方式、促进经济结构的战略性调整,引领经济社会走上创新驱动、内生增长、科学发展的轨道,我国正在大力培育和发展战略性新兴产业。战略性新兴产业体现了新兴科技和新兴产业的深度融合,既代表科技创新的重要方向,也代表产业发展的重要方向,具有市场前景广阔、经济技术效益好、带动性强的突出特点。随着“工业化与信息化融合”、“智慧地球”、“传感中国”等理念的提出,物联网作为战略性新兴产业的重要代表性领域,掀起了第三次信息技术浪潮。不断发展的信息技术正在快速地改变着人们的工作模式、生活习惯和思维方式,越来越多的信息安全问题如影随形,物联网的安全和隐私保护问题亟待解决。

物联网作为一个大的产业链,是一个多学科交叉的综合应用领域。尽管科技界、产业界、政府部门以及广大普通民众基于各自不同的背景对物联网有不同的理解和体会,但有一点是共同期待和永恒坚持的,即“没有安全就没有应用,没有应用就没有发展”,在越来越强调生命尊严和生活质量的今天,与人们的生产、生活息息相关的物联网的安全尤其重要!

本书是作者从事多年的物联网安全相关科研工作实践的结晶。本书从提出写作构想、准备资料、总结研究成果,到最终完稿,经历了四年多的艰苦努力与再三凝练,同时深刻见证了物联网技术与产业的快速进步,以及对物联网安全快速增长的需求与期待。基于物联网特有的分布、技术和物权等属性,物联网对攻击者展现出前所未有的吸引力,并暴露出明显的安全脆弱性。与传统信息安全问题不同的是:一方面,传统的信息安全技术难以直接应用于物联网并保证其安全目标的实现;另一方面,物联网安全与国家安全、人身安全、隐私保护等密切相关,涉及物理上实实在在的财物与生命安全,不再仅仅是信息安全问题,而且我国在物联网的关键硬件国产化方面还有很多工作要做,因此物联网的安全备受关注。物联网既是多学科交叉综合应用的产物,又处于技术和产业成熟前的快速发展期,物联网的安全解决方案正处于积极的研究探索阶段,其安全目标的实现任重而道远,目前还没有完全成熟、定型、系统的物联网安全解决方案。本书是当前物联网相关安全方案的系统总结,多角度展示了物联网安全不同专题、不同方向的研究成果,作者希望借此抛砖引玉,启发并催生出更多创新性研究成果,推动物联网安全解决方案尽快走向成熟、趋于完善,早日实现物联网科技惠及民生的美好愿景。

本书由重庆邮电大学胡向东教授组织撰写,第2章由魏琴芳撰写,第5章由胡向东、余朋琴撰写,第7章由胡向东、丰睿撰写,第9章由胡向东、唐贤伦、冯志宇撰

写,第12章由向敏、胡向东撰写,胡向东负责其余章节的撰写和全书的统稿。特别感谢参考文献中所列各位作者,包括未能在参考文献中一一列出资料的作者,正是因为他们各自领域的独到见解和特别的贡献为作者提供了宝贵的参考资料、研究视角和丰富的写作源泉,使作者能够在系统总结本领域科研工作成果的基础上,汲取各家之长,及时形成本书。

参加本书资料搜集整理、仿真实验的还包括王泉、罗志勇博士和万天翔、张力、王雪、赵代娜、崔鹏、尚可、韩恺敏、许宏如、张玉函、白润资、汤其为等研究生;刘宴兵教授为本书的撰写提供了富有建设性的指导和建议。在此对他们付出的辛勤劳动表示由衷的感谢。本书的出版受到重庆邮电大学出版基金资助,并得到国家自然科学基金项目(61170219)、重庆市科委自然科学基金项目(CQ CSTC2009BB2278, CSTC2011jjA40028)、重庆市教委研究项目(113029)、2011重庆市高等学校优秀人才支持计划项目和重庆邮电大学自然科学基金项目(A2011-15、A2011-17)的资助。

物联网安全的内涵丰富、多学科交叉特征明显、技术发展迅速、应用需求多样,对本书的撰写是作者在此领域的一次努力尝试,限于作者的水平 and 学识,书中难免存在疏漏和错误之处,诚望读者不吝赐教,以利修正,让更多的读者获益(huxd@cqupt.edu.cn)。

作者

2011年9月

# 目 录

《信息科学技术学术著作丛书》序

前言

第 1 章 绪论	1
1.1 物联网概念的形成	1
1.2 物联网的体系结构	3
1.3 物联网的关键技术	4
1.3.1 体系架构	4
1.3.2 标识与识别技术	5
1.3.3 通信和网络技术	6
1.3.4 嵌入式系统与硬件	7
1.3.5 数据处理技术	8
1.3.6 信息安全和隐私	8
1.4 待解决的关键问题	9
1.4.1 国家安全问题	9
1.4.2 标准体系问题	10
1.4.3 信息的合法有序使用问题	10
1.4.4 核心技术有待突破问题	11
1.4.5 商业模式完善问题	11
1.5 研究发展现状	12
1.6 物联网安全模型	17
1.7 发展趋势与展望	19
参考文献	23
第 2 章 物联网安全的密码理论	25
2.1 引言	25
2.2 群论	26
2.2.1 群的概念	26
2.2.2 群的性质	26
2.3 有限域理论	27
2.3.1 域和有限域	27
2.3.2 有限域 $GF(p)$ 中的计算	27



2.3.3	有限域 $GF(2^m)$ 中的计算	28
2.4	欧几里得算法及其扩展	33
2.5	AES 对称密码算法	34
2.5.1	加密原理	35
2.5.2	基本加密变换	37
2.5.3	AES 的解密	40
2.5.4	密钥扩展	41
2.6	椭圆曲线公钥密码算法	43
2.6.1	椭圆曲线密码概述	43
2.6.2	椭圆曲线的加法规则	43
2.6.3	椭圆曲线密码体制	44
	参考文献	46
<b>第3章</b>	<b>无线传感器网络安全概述</b>	<b>48</b>
3.1	引言	48
3.1.1	网络模型	48
3.1.2	传感器网络体系结构	50
3.1.3	传感器节点体系结构	51
3.2	无线传感器网络的安全挑战	53
3.3	无线传感器网络的安全需求与目标	54
3.3.1	信息安全需求	55
3.3.2	通信安全需求	56
3.3.3	无线传感器网络的安全目标	57
3.4	无线传感器网络可能受到的攻击分类	57
3.4.1	一般性攻击	58
3.4.2	拒绝服务攻击	59
3.4.3	物理攻击与节点的捕获	61
3.4.4	假冒攻击	63
3.4.5	针对特定协议的攻击	63
3.5	无线传感器网络的安全防御方法	65
3.5.1	物理攻击的防护	66
3.5.2	实现机密性的方法	67
3.5.3	密钥管理	69
3.5.4	阻止拒绝服务	71
3.5.5	对抗假冒的节点或恶意的数据	72
3.5.6	对抗女巫攻击	72

---

3.5.7 安全路由 .....	73
3.5.8 数据融合安全 .....	74
参考文献 .....	75
<b>第4章 密钥管理 .....</b>	<b>79</b>
4.1 密钥的种类与密钥管理的层次式结构 .....	79
4.1.1 密钥的种类 .....	79
4.1.2 密钥管理的层次式结构 .....	80
4.2 密钥管理系统 .....	81
4.2.1 密钥管理系统框架 .....	81
4.2.2 公钥基础设施 .....	82
4.2.3 密钥管理的阶段 .....	83
4.3 密钥的协商与建立 .....	84
4.3.1 Diffie-Hellman 密钥交换算法 .....	84
4.3.2 密钥的建立 .....	86
4.4 密钥的分发 .....	95
4.4.1 分布式物联网密钥的分发 .....	96
4.4.2 层次式物联网密钥的分发 .....	102
参考文献 .....	105
<b>第5章 非正常节点的识别 .....</b>	<b>107</b>
5.1 引言 .....	107
5.2 拜占庭将军问题 .....	107
5.3 基于可信节点的方案 .....	108
5.3.1 系统模型 .....	108
5.3.2 定位信任模型 .....	109
5.4 基于信号强度的方案 .....	110
5.4.1 系统模型 .....	110
5.4.2 可疑节点的发现 .....	110
5.4.3 性能评估 .....	111
5.5 基于加权信任评估的方案 .....	112
5.5.1 网络结构 .....	112
5.5.2 基于加权信任评估的恶意节点发现 .....	113
5.5.3 加权信任评估的性能 .....	114
5.6 基于加权信任过滤的方案 .....	115
5.6.1 网络模型及基本假设 .....	115
5.6.2 符号定义 .....	116

5.6.3	恶意节点发现流程	116
5.6.4	仿真及结果分析	118
5.7	恶意信标节点的发现	120
5.7.1	恶意信标节点的发现方法	120
5.7.2	撤销恶意信标节点	126
5.7.3	仿真与结果分析	129
5.8	选择性转发攻击的发现	130
5.8.1	选择性转发攻击的研究概述	130
5.8.2	网络模型及假设	131
5.8.3	发现方案	132
5.8.4	仿真与结果分析	134
5.8.5	结论	136
	参考文献	136
<b>第6章</b>	<b>入侵检测</b>	<b>138</b>
6.1	引言	138
6.2	入侵检测原理	140
6.2.1	入侵检测技术	140
6.2.2	入侵检测结构	141
6.2.3	决策技术	141
6.3	面向物联网的IDS	142
6.3.1	物联网对IDS的要求	142
6.3.2	物联网的IDS体系结构	143
6.3.3	物联网的IDS分类	146
6.3.4	物联网的IDS组成	148
6.4	发现攻击	153
6.4.1	基于看门狗的包监控方案	153
6.4.2	发现污水池攻击	155
6.5	IDS在TinyOS中的实现	155
6.5.1	模块和接口	156
6.5.2	存储器计算需求	158
6.5.3	实验	158
6.6	基于神经网络的入侵检测方案	160
6.6.1	入侵检测模型的建立	160
6.6.2	仿真与结果分析	162
	参考文献	166

---

<b>第 7 章 认证</b> .....	168
7.1 消息认证 .....	168
7.1.1 目标跟踪方法 .....	169
7.1.2 监控类物联网的安全 .....	172
7.1.3 消息认证协议的进展 .....	173
7.2 广播认证 .....	183
7.2.1 具有 DoS 容忍和故障容错能力的广播认证 .....	183
7.2.2 基于双层过滤机制的 uTESLA 广播消息认证 .....	201
参考文献.....	206
<b>第 8 章 安全成簇</b> .....	208
8.1 引言 .....	208
8.2 国内外现状及发展动态分析 .....	209
8.3 SLEACH 安全成簇方案简介 .....	211
8.3.1 SLEACH 安全成簇原理 .....	211
8.3.2 安全性分析 .....	213
8.4 安全成簇中的关键技术 .....	214
8.5 安全成簇的技术路线 .....	215
8.6 安全成簇算法原理 .....	218
8.6.1 算法基本思路 .....	218
8.6.2 簇头安全选择 .....	218
8.6.3 安全数据通信 .....	219
8.6.4 安全簇维护 .....	220
8.6.5 算法特点 .....	221
8.7 节点安全加入与退出 .....	221
8.7.1 节点安全加入网络 .....	221
8.7.2 异常节点安全退出网络 .....	223
8.7.3 仿真与结果分析 .....	223
参考文献.....	225
<b>第 9 章 安全数据融合</b> .....	227
9.1 引言 .....	227
9.2 基于信誉度评价的安全数据融合 .....	227
9.2.1 安全数据融合模型 .....	228
9.2.2 仿真与结果分析 .....	231
9.2.3 结论 .....	233
9.3 基于模糊数学的安全数据融合 .....	233

9.3.1	概述 .....	233
9.3.2	高效安全数据融合的步骤 .....	233
9.3.3	基于模糊数学的融合算法 .....	234
9.3.4	实验结果与分析 .....	237
9.4	基于逐跳的安全数据融合 .....	238
9.4.1	系统模型 .....	238
9.4.2	安全数据融合协议 .....	239
	参考文献 .....	249
<b>第 10 章</b>	<b>安全路由 .....</b>	<b>251</b>
10.1	引言 .....	251
10.2	安全路由协议的提出 .....	252
10.2.1	路由协议的安全目标 .....	252
10.2.2	针对路由协议的常见攻击 .....	252
10.2.3	防御对策 .....	254
10.2.4	现有安全路由协议 .....	254
10.3	定向扩散路由协议 .....	255
10.3.1	命名机制 .....	256
10.3.2	兴趣的扩散 .....	256
10.3.3	梯度的建立 .....	257
10.3.4	数据的传播 .....	257
10.3.5	路径的建立和加强 .....	258
10.4	定向扩散路由协议的安全性增强 .....	259
10.4.1	问题描述 .....	259
10.4.2	能量高效的定向扩散路由协议设计 .....	259
10.4.3	安全高效扩散路由协议设计 .....	262
10.5	仿真与性能分析 .....	266
10.5.1	仿真环境设置 .....	266
10.5.2	EEDD 性能分析 .....	266
10.5.3	SEEDD 性能分析 .....	268
	参考文献 .....	276
<b>第 11 章</b>	<b>安全定位 .....</b>	<b>278</b>
11.1	定位异常的发现 .....	279
11.1.1	分布知识的建模 .....	279
11.1.2	定位异常的发现问题 .....	280
11.1.3	用分布知识发现定位异常 .....	281

11.2 基于 MDS-MAP 的安全定位 .....	282
11.2.1 概述 .....	282
11.2.2 经典的 MDS-MAP 定位算法 .....	282
11.2.3 安全的 MDS-MAP 定位算法 .....	284
11.2.4 仿真实验分析 .....	286
11.3 具有鲁棒性的安全定位 .....	289
11.3.1 鲁棒性定位 .....	289
11.3.2 基于最小中值平方的鲁棒性拟合 .....	290
11.3.3 采用 LMS 的鲁棒性定位法 .....	291
11.3.4 仿真与结果分析 .....	292
11.3.5 结论 .....	293
参考文献 .....	293
<b>第 12 章 物联网中的抗干扰</b> .....	295
12.1 物联网中的通信 .....	295
12.1.1 通信协议栈 .....	295
12.1.2 通信协议和标准 .....	296
12.2 人为干扰的内涵及网络脆弱性 .....	296
12.2.1 人为干扰的定义 .....	296
12.2.2 人为干扰技术 .....	297
12.2.3 干扰者类型 .....	297
12.2.4 受人为干扰影响的脆弱性 .....	299
12.3 对付干扰的措施 .....	299
12.4 物联网对抗干扰的安全建议 .....	301
12.4.1 预防型对抗措施 .....	301
12.4.2 反应型对抗措施 .....	306
12.4.3 基于移动代理的对抗措施 .....	308
12.4.4 小结 .....	310
参考文献 .....	311
<b>第 13 章 射频识别的隐私与安全</b> .....	313
13.1 引言 .....	313
13.2 无线射频识别系统的工作原理 .....	314
13.3 无线射频识别系统的安全需求 .....	316
13.4 无线射频识别系统中的可能攻击 .....	318
13.4.1 针对标签和阅读器的攻击 .....	318
13.4.2 针对后端数据库的攻击 .....	322

---

13.5	无线射频识别的安全机制	324
13.5.1	物理方法	324
13.5.2	逻辑方法	325
13.6	无线射频识别的安全服务	327
13.6.1	访问控制	327
13.6.2	标签认证	328
13.6.3	消息加密	330
	参考文献	332
<b>第 14 章</b>	<b>物联网嵌入式系统的安全设计</b>	<b>334</b>
14.1	物联网嵌入式系统概述	334
14.1.1	射频识别系统的安全性	334
14.1.2	无线传感器网络的安全性	336
14.2	无线嵌入式系统的脆弱性和防护	337
14.2.1	攻击形式	337
14.2.2	物理安全和防拆装	339
14.2.3	安全固件设计和存储器保护	340
14.3	安全无线嵌入式系统的组件选择	341
14.3.1	安全嵌入式微控制器	341
14.3.2	无线传感器网络节点和有源射频识别标签的微控制器选择	341
14.3.3	无线广播选择	342
14.4	轻量级认证和加密算法	343
14.4.1	对称加密	344
14.4.2	非对称加密	344
	参考文献	345

# 第 1 章 绪 论

## 1.1 物联网概念的形成

随着当代生产力的快速发展,多学科科学技术交叉融合的推动,以及不断增长的应用需求的递进牵引,以“智能化”为核心的物联网应运而生。物联网就是“物品的互联网”(the Internet of things, IoT),可以认为是传统的物流信息化工作的进一步深化与综合,也是传统互联网的使用对象由人及物在应用范围上的延伸和扩展,将互联网的用户终端由个人电脑延伸到任何需要实时管理的物品,其目的是让没有生命、为人服务的物品也能“开口说话”,通过网络实现互联互通,允许人和物在任何时间(anytime)、任何地点(anywhere),使用任何的路径或网络(any path/any network)、任何的服务或业务(any service/any business),与任何的事物或设备(anything/any device)、任何人(anyone)无缝地联系,将聚合(convergence)、内容(content)、知识库(collections)、计算(computing)、通信(communication)和连接(connectivity)等元素集成在一起形成一个有机的整体(见图 1.1),从而加强人与

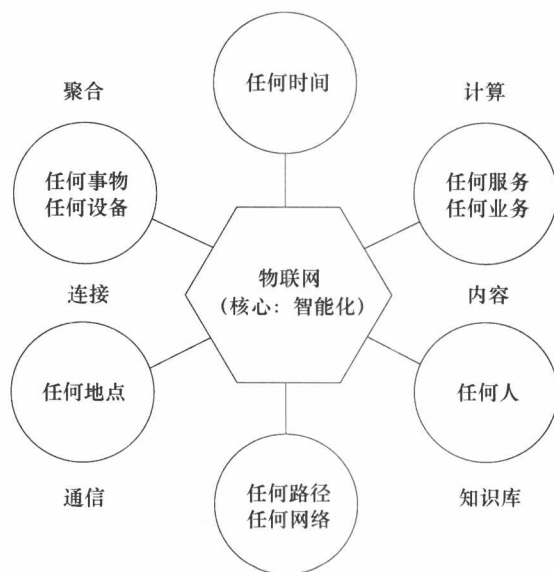


图 1.1 物联网的基本内涵



物、物与物等的信息交流,实现更高的工作效率,节省操作成本,体现“服务的智能化”和“科技惠及民生”的本质<sup>[1]</sup>。

物联网中的“物”是时空范围内存在的、可以被标识和识读的实际(物理)的或数字(虚拟)的实体,它们通常可通过分配的身份(identity, ID)号、名称或位置地址来识别。应用创新是物联网技术的发展核心,国际电信联盟(ITU)于2005年在一份报告中曾描绘“物联网”时代的图景:当司机出现操作失误时汽车会自动报警;公文包会提醒主人忘带了什么东西;回家前先发条短信,浴缸就能自动放好洗澡水等<sup>[2]</sup>。

物联网的概念大致起源于1999年美国麻省理工学院自动识别中心(MIT AutoID Center)给出的“物联网”理念,即在计算机互联网基础上,利用射频识别(radio frequency identification, RFID)、无线数据通信等技术,构造一个覆盖世界上万事万物的网络,以实现物品的自动识别和信息的互联共享;同年,在美国召开的“移动计算和网络国际会议”上还提出“传感网是下一个世纪人类面临的又一个发展机遇”<sup>[3,4]</sup>;2003年,美国《技术评论》将传感网络技术列为未来改变人们生活的十大技术之首;也有人认为,早在1995年比尔·盖茨的《未来之路》一书中已提及物联网的相关概念;2005年,在突尼斯举行的“信息社会世界峰会”(WSIS)上,ITU发布了《ITU互联网报告2005:物联网》<sup>[2]</sup>,正式提出了“物联网”的概念;2009年,IBM公司提出“智慧地球”的概念,在世界范围内掀起了物联网的热潮,发展物联网技术被多个国家列为重大信息发展战略。

物联网从提出至今只有十余年时间,其内涵尚处于快速发展变化过程中,还没有一个统一的定义。目前,较为大家所接受的物联网的基本含义是:通过RFID、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理<sup>[5]</sup>。物联网的核心概念在于“基于网络对物品信息的按需、自动、及时、可靠感知”。一般认为物联网应具备三个基本特性:①及时感知信息,即利用各种可用的感知手段,能实现对物体动态信息的实时采集;②可靠传输信息,即通过各种信息网络与互联网的融合,将感知的信息准确可靠地传递出去;③智能处理信息,即利用云计算等智能计算技术对海量的数据和信息进行分析和处理,以便按需、自动地获取到有用信息并对其进行利用。物联网的本质是通过能够获取物体信息的传感器来进行信息采集,通过网络进行信息传输与交换,通过信息处理系统进行信息加工及决策。

物联网在国内是一个得到广泛认同的概念,并将传感网、物联网和泛在网(ubiquitous network)三者看做是一个递进的包容拓展关系,但国际上习惯将物联网称为泛在网,大概强调的是物联网发展的最终形态。从英文的角度理解,物联网就是物品的互联网,到目前为止,不同领域的专家学者对物联网与互联网的关系有