普通高校物联网工程专业规划教材

物联网安全

任 伟 编著

清华大学出版社

普通高校物联网工程专业规划教材

物联网安全

任 伟 编著

清华大学出版社
北京

内容简介

本书全面而又系统地论述了物联网安全中的部分关键问题及其典型解决方案。全书分为3大部分：物联网感知层安全、物联网网络层安全和物联网应用层安全。物联网感知层安全介绍RFID安全、无线传感器网络安全、物联网终端系统安全；物联网网络层安全介绍近距离无线接入安全（无线局域网安全）、远距离无线接入安全（无线移动通信安全）、接入网安全的扩展讨论、物联网核心网安全（6LoWPAN安全和RPL安全）、物联网服务端安全（云计算安全）；物联网应用层安全介绍智能电网安全、EPCglobal网络安全、基于无线体域网的远程医疗安全、M2M安全。

本书可作为物联网工程、信息安全、计算机科学等专业的研究生或本科高年级教材，对物联网安全领域的研究者具有一定参考价值，对物联网领域的工程技术人员亦具有指导价值。

图书在版编目（CIP）数据

物联网安全/任伟编著. —北京：清华大学出版社，2012.6
（普通高校物联网工程专业规划教材）
ISBN 978-7-302-28503-8

Ⅰ. ①物… Ⅱ. ①任… Ⅲ. ①互联网络—应用—物流 ②互联网络—安全技术 Ⅳ. ①TP393.4 ②F253.9

中国版本图书馆CIP数据核字(2012)第064979号

责任编辑：龙启铭
封面设计：傅瑞学
责任校对：李建庄
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京世知印务有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：12.75　　**字　数**：315千字
版　　次：2012年6月第1版　　**印　次**：2012年6月第1次印刷
印　　数：1～3000
定　　价：25.00元

产品编号：046006-01

前　言

物联网作为国家的战略新兴产业，正在得到大力发展，在国家科技创新、可持续发展和产业升级中具有重要的地位。在工业和信息化部最近发布的《物联网“十二五”发展规划》中，“加强信息安全保障”已成为主要任务之一。但是，目前还没有全面论述物联网安全的相关书籍，因此，无论是信息网络安全领域的科研与教学人员，还是物联网工程领域的技术人员，都急需一本全面讲解物联网安全的书籍。

物联网安全本身涉及的内容极其广泛，本书特精心挑选了其中的关键问题、特色问题、重点问题进行讨论，给出相关的技术、方法和常用的典型方案，并介绍几个特色领域（如 6LoWPAN、智能电网、EPCglobal 网络以及 M2M 领域）的安全研究进展。

作者在写作的过程中特别遵循了以下一些新的思路。

（1）内容编排循序渐进、由浅入深、先总体再局部、兼顾广度和深度。先给出物联网的体系结构以及安全架构，再给出物联网安全问题的共性之处和一般解决思路。然后根据物联网的安全架构（感知层安全、网络层安全和应用层安全），分章节依次探讨特定的安全问题。同时在每一章的介绍中，还遵循先介绍总体架构与安全威胁全貌，后论述典型安全论题的次序。

（2）选材新颖、理论联系实际。选材尽量突出基本的研究问题以及新的进展，理论的论述突出共性和一般原理（如对接入网围绕认证与密钥协商机制来论述、RFID 认证协议、无线传感器网络的密钥管理），实践部分强调新颖性和工程性（如对最新 LTE 加密算法 ZUC、LBlock、NTRU、SMS4、SM3 的解释）。理论与实际结合中，突出网络安全设计方案的一般规律，便于指导将来的安全设计。

（3）注重启发性和对创新能力的培养，包括对一般原理的总结和归纳、协议设计方法的比较和分析，注重对问题本质的提炼。通过每一章的“研究与思考”环节，启发读者思考、提出并解决新的物联网安全问题。爱因斯坦曾经说过：“提出问题往往比解决问题更为重要”。这一环节对于创新教育可能是一次有益的尝试。

（4）注重对国内自主知识产权和自主创新的介绍，包括轻量级分组加密 LBlock、国家密码管理局标准 Hash 算法 SM3，无线局域网安全标准 WAPI、流密码 SMS4、3G 标准 TD-SCDMA、4G 中的流加密算法 ZUC、国产手机操作系统 OMS、北斗卫星导航系统、CMMB 等。由于信息安全的行业特殊性和我国综合国力的提升，介绍这部分相关成果有利于激发读者和相关技术人员对我国自主创新成果的关注，扩大我国自主知识产权成果的影响，促进我国自主知识产权成果的推广和应用。

（5）特别讨论了物联网安全中的几个特色问题，如 6LoWPAN 的安全、智能电网安全、EPCglobal 网络以及 M2M 安全。对从事该方面研究的科研人员以及安全工程技术研发人员有一定的参考价值。

(6) 注重对实践能力的培养和对行业动态的关注。书中给出了多个密码算法便于读者去实现。通过文中对最新物联网科技动态的报道(如 iPhone 集成 RFID 的专利信息),便于把握新的研究动向和应用场景。文中还对国内部分行业领先企业做了介绍,以支持民族产业和扩大自主品牌的影响。

(7) 密码学工具与计算机和网络安全的有机结合。物联网安全问题的解决工具主要是密码学,因为它深刻而且精巧,但是又不囿于密码学方法(有些问题需要来自计算机科学的方法解决)。实际中的网络问题为密码学提供了丰富的问题和需求,刺激了密码学的发展。同时,根据不同的安全问题,应选择与之相适应的安全方案,而不能局限于某一种方法或者工具。本书在两种方法之间力求兼顾,希望能给有密码学背景的读者提供一些实际问题,也给计算机科学背景的读者提供一些密码学工具和密码学思考问题的角度(特别是在云存储安全一节)。

全书共分 13 章:第 1 章是物联网安全概述,第 2 章介绍 RFID 安全,第 3 章介绍无线传感器网络安全,第 4 章介绍物联网终端系统安全,第 5 章介绍近距离无线接入安全——无线局域网安全,第 6 章介绍远距离无线接入安全——无线移动通信安全,第 7 章介绍接入网安全的扩展讨论,第 8 章介绍物联网核心网安全——6LoWPAN 和 RPL 的安全性,第 9 章物联网服务端安全——云计算安全,第 10 章介绍智能电网安全,第 11 章介绍 EPCglobal 网络安全,第 12 章介绍基于无线体域网的远程医疗安全,第 13 章介绍 M2M 安全。其中,第 2～4 章为第 1 部分物联网感知层安全,第 5～9 章为第 2 部分物联网网络层安全,第 10～13 章为第 3 部分物联网应用层安全。带星号的部分为选学内容。

本书面向的主要对象包括从事信息和网络安全研究的科研人员,学习物联网安全相关课程的高等院校信息安全类、物联网工程类、计算机类专业研究生和本科高年级学生,以及从事物联网安全技术研发、应用和管理的工程技术人员。

本书得到了国家自然科学基金面上项目(No. 61170217)、湖北省高等学校省级教学研究项目(2011123,2011125)、山东省计算机网络重点实验室开放课题资助(SDKLCN-2011-01)、中央高校基本科研业务费专项资助项目(090109,110109)的支持,在此表示感谢。感谢长江学者华中科技大学金海教授和长江学者北京邮电大学杨义先教授的指导和教诲。感谢新加坡管理大学邓慧杰(Robert H. Deng)教授的帮助。感谢香港科技大学和美国伊利诺理工大学的老师和朋友们。感谢研究生刘宇靓协助绘制了部分插图。

愿本书的写作能为我国物联网安全的研究以及教学起到抛砖引玉的作用。由于作者水平和学识有限,加之编写时间紧,不足之处在所难免,在此衷心恳请广大读者同行批评指正。

任 伟
中国地质大学(武汉)
2012 年 4 月

目　录

第 1 章　物联网安全概述

1.1　物联网安全概述

1.1.1　物联网概念与发展历程

1. 物联网的概念

物联网(Internet of Things)是一个基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络[1]。它具有普通对象设备化、自治终端互联化和普适服务智能化 3 个重要特征。

另外一个在国内被普遍引用的物联网定义是来自百度百科和互动百科的定义，虽然没有经过官方审定，但是传播范围很广：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、监控和管理的一种网络。

下面先回顾一下物联网的发展历程，然后介绍如何理解物联网概念。括号部分是我们对事件的评论。后面的章节选材和内容组织在某种程度上与这些事件相呼应。

(1) 1998 年，美国麻省理工学院提出了当时被称为 EPC(Electronic Product Code)系统的物联网构想。紧接着在 1999 年，在 EPC 编码、RFID 技术和互联网基础上，MIT 的 Auto-ID 中心提出物联网的概念。2003 年 10 月，非盈利性组织 EPCglobal 成立(这形成了基于 Internet 的 RFID 系统)。

(2) 2004 年，IETF 成立了基于低功耗无线个域网(LoWPAN)的 IPv6 工作组 6LoWPAN，致力于研究在由 IEEE 802.15.4 链路构成的低功耗无线个域网中如何优化运行 IPv6 协议。这为通过 Internet 直接寻址访问无线传感器网络结点(无需通过网关)提供了可能(使得无线传感器网络走向开放并可能成为一种 Web 服务)。

(3) 2006 年，美国国家自然科学基金委员会将信息物理融合系统 CPS(Cyber Physical System)作为重点支持的研究课题。CPS 是一个以通信和计算为核心的集成的监控和协调行动的工程化物理系统，是计算、通信和控制的融合，具备很高的可靠性、安全性和执行效率。CPS 试图突破原有传感器网络系统自成一体、计算设备单一、缺乏开放性等缺点，注重多个系统间的互联互通，强调与互联网的联通，真正实现开放的、动态的、可控的、闭环的计算和服务支持(感知和控制融合使得物联网更加强大，从此控制系统的安全需要重视了)。

(4) 2005 年，国际电信联盟 ITU 发布了《ITU 互联网报告 2005：物联网》。报告指出，世界上所有的物体都可以通过互联网主动进行信息交换。RFID、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，强调 M2M(Machine-to-Machine)通信。2008 年，欧洲智

能系统集成技术平台(EPoSS)在《物联网 2020》报告中分析预测了未来物联网的发展阶段(可见,欧洲的物联网是从电信部门开始主导的,因为 M2M 具有巨大的市场潜力)。

(5) 2008 年 9 月,IPSO(IP Smart Object)联盟成立,推进 IP 在智能物体(Smart Object)中的应用(智能物体可视为一种通用的物联网终端模型,其功能可能是异构的 Hybrid,即具有感知、识别、制动等多重功能)。

(6) 2009 年 1 月,奥巴马就任美国总统后,与美国工商业领袖举行了一次"圆桌会议"。作为仅有的两名代表之一的 IBM 首席执行官首次提出了"智慧地球"的概念。依据奥巴马总统的经济恢复法案,2009 年美国能源部宣布投资 45 亿美元打造基于 M2M 技术的实时双向通信的智能电网。在美国除 M2M(Machine-to-Machine)外,最受关注的物联网应用是智能电网和远程医疗。这两个领域都是奥巴马政府低碳经济和医疗改革政策直接推动的结果(美国研究物联网是从具体应用入手的,重视智能电网、远程医疗等物联网应用)。

(7) 2009 年,欧盟执委会发表题为《Internet of Things-an Action Plan for Europe》的物联网行动方案,描绘了物联网技术应用的前景(物联网上升为整个欧盟的战略行为)。

(8) 2009 年,韩国通信委员会和日本政府 IT 战略本部分别提出了物联网相关战略(韩日的物联网战略)。

(9) 2009 年 8 月,温家宝总理在无锡视察时发表重要讲话,提出"感知中国"的战略构想。在后来的"让科技引领中国可持续发展"的讲话中,将物联网列入战略新兴产业之一,标志着物联网产业发展已经提升到我国的国家战略(我国开始大规模介入物联网)。

对于物联网概念的理解,应该从基本应用需求出发,把握物联网的特点和基本技术。对于物联网的发展和应用,不同的国家有着不同的着力点。美国常常提及智能电网(为了新能源利用、节能减排的需要)、远程医疗、基于 EPCglobal 网络的供应链管理。欧洲常常提及 M2M 应用,从大规模安装无线移动通信的 SIM 卡到智能设备或者监控仪表来促进其发展,以及智能嵌入式实时系统。我国的物联网则涉及范围更加广泛,从传感网和 RFID 的应用入手,到两化融合(自动化和信息化的融合)和 M2M,被认为是一次赶超世界先进信息技术的历史机遇。

物联网的特点是融合了无线网络和有线网络,扩大了接入 Internet 网络的设备的规模(除了计算机外,还有大量的微型计算设备),使得网络连接的范围更广。加上这些设备如传感器结点具有感知外部环境的功能,有些设备如 RFID 具有标识附着的物体的能力,这些设备还可以借助卫星定位系统如 GPS,可被定位和追踪,这些都使得人类具有比以前更加强大的获取信息的能力。如果这些设备还能够具备行动能力,则人类具有比以前更加强大的控制能力。这些使得人类具有前所未有的能力去感知、标识、跟踪、联接、控制、管理地球上的物体的一举一动,好比给地球加上了一个神经系统。这个神经系统有末梢(物联网终端系统)、有传导(网络通信系统)以及处理(如云计算、信息与网络中心等)。

1.1.2 物联网的体系结构

物联网应该具备 3 个特征:

(1) 全面感知,即利用 RFID、传感器、条形码(二维码)、GPS(北斗卫星导航)定位装置等随时随地获取物体的信息。

(2) 可靠传递，通过各种网络与互联网的融合，将物体的信息实时准确地传递出去。

(3) 智能处理，利用云计算等各种智能计算技术，对海量数据和信息进行分析和处理，对物体实施智能化控制。因此，物联网的体系架构通常认为有 3 个层次：底层是用来感知(识别、定位)的感知层，中间是数据传输的网络层，上面是应用层，如图 1.1 所示。

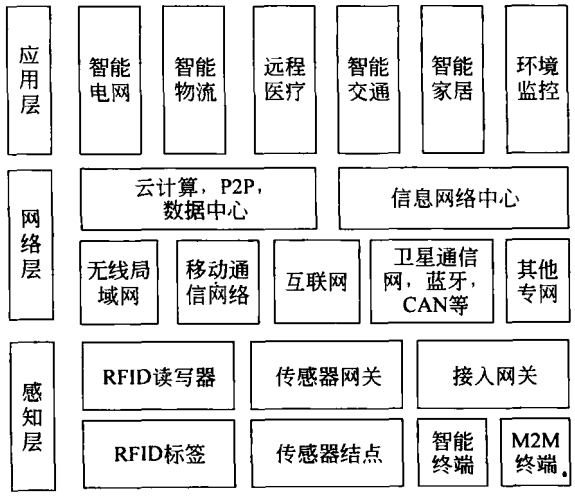

图 1.1　物联网体系架构

感知层包括以传感器为代表的感知设备、以 RFID 为代表的识别设备、GPS(北斗系统)等定位追踪设备以及可能融合部分或全部上述功能的智能终端(手机)等。大规模的感知则构成了无线传感器网络。另外，M2M 的终端设备，智能物体都可视为感知层中的物体。感知层是物联网信息和数据的来源。

网络层包括接入网、核心网以及服务端系统(云计算平台、信息网络中心、数据中心等)。接入网可以是无线近距离接入，如无线局域网、ZigBee、Bluetooth、红外，也可以是无线远距离接入，如移动通信网络、WiMAX 等，还可能其他接入形式如有线网络接入(PSTN、ADSL、宽带)、有线电视、现场总线、卫星通信等。网络层的承载是核心网，通常是 IPv6(IPv4)网络。网络层是物联网信息和数据的传输层，此外，网络层也包括信息存储查询、网络管理等功能。云计算平台作为海量感知数据的存储、分析平台，是物联网网络层的重要组成部分，也是应用层众多应用的基础。

应用层利用经过分析处理的感知数据为用户提供丰富的特定服务，这些服务通常是在具备感知、识别、定位追踪能力后新增加的功能，如智能电网、智能物流、远程医疗、智能交通、智能家居、环境监控等。依靠感知层提供的数据和网络层的传输，进行相应的处理后，可能再次通过网络层反馈给感知层。应用层是物联网信息和数据的融合处理和利用，是物联网发展的目的。

我们认为，物联网中比较有特色的共性网络技术有 3 个：6LoWPAN、EPCglobal 网络和 M2M(Machine-to-Machine)。

(1) 6LoWPAN，主要用于基于 Internet 寻址访问传感器结点，由 IETF 定义，被 IPSO 联盟推广。从广义上讲，可用于在基于 IEEE 802.15.4 的无线个域网链路条件下，

承载 IPv6 协议构成一个广域的大规模的设备(智能物体)的联网。这一技术可视为无线传感器网络的 Internet 演进,其推动者是 IETF 以及 IPSO 联盟。

(2) EPCglobal 网络,主要用于基于 Internet 的 RFID 系统,由 EPCglobal 定义,主要用于广域物体的定位与追踪的物流应用。这一技术可视为 RFID 技术的 Internet 演进,其推动者是 EPCglobal 组织。

(3) M2M,通常是指通过远距离无线移动通信网络(例如 GPRS、TD-SCDMA 等)的设备间的通信,如终端设备与中心服务器间通信的智能抄表,以及两个广域网的设备间的通信(通过中心服务器转接)。M2M 的主要作用是为远端设备提供无线通信接入 Internet 的能力。M2M 很多时候可视为一种接入方式,这种接入方式和无线移动通信网中以人为中心的接入方式不同,M2M 中接入的对象是设备,且这些设备通常是无人看守的(因此 M2M 设备可能是机卡一体的)。当然,广义上 M2M 可泛指所有机器之间的通信,涵盖控制系统间的通信。M2M 通常是移动通信运营商在推动,可视为远距离无线移动通信网络的接入端从以人为中心向以设备为中心演进。

上述 3 种技术之间的关系可以表述如下:

(1) EPCglobal 网络和 M2M 可以融合,即 RFID 读写器通过 M2M 连接到 Internet,然后可访问 EPGglobal 定义的 ONS(Object Name Service)、EPCIS(EPC Information Service)等服务。EPCglobal 网络主要定义了应用层服务的架构。

(2) 6LoWPAN 和 M2M 之间的区别是前者提供了直接的 Internet 寻址能力,而后者可以通过在 M2M 服务器端的网关功能进行寻址,这种寻址类似于一种基于广域无线通信网的网络地址转换(Natural Address Translation,NAT),因为后者可不需要配置 IP 地址,而只需要配置 M2M 标识。6LoWPAN 是协议栈的一个适配层。

(3) 无线传感器结点或者无线传感网网络网关也可以通过 M2M 的 GPRS、特别是 TD-SCDMA 连接到远距离无线移动通信网络的中心结点,然后与 Internet 相连。达到 6LoWPAN 技术类似的效果。M2M 的最大优势是对大规模移动性的支持。

基于上述基本网络技术,根据需求选择适当的终端设备,再合理地选择接入网络和核心网,就可以构造各种新颖的应用。

国际电信联盟(ITU)在 2005 年的物联网报告中,描述了一个物联网应用场景。这是 2020 年日常生活的一天。一个来自西班牙的 23 岁名叫 Rosa 的学生,刚刚同男朋友吵完架,想要独处一段时间。她决定私自驾驶自己的智能汽车去法国阿尔卑斯山的一个滑雪胜地度周末。但是她必须先去修理厂,因为汽车的传感系统提醒她轮胎可能坏了。当她进入修车厂入门通道的时候,基于传感器的诊断工具已经为她的车做了全面检查,并根据检查的结果引导她的车开进一个配备有自动机器人手的专门修理站点。Rosa 下车后去喝杯咖啡,饮料自动售货机知道 Rosa 喜欢冰咖啡,所以在 Rosa 挥舞网络手表付账后得到了一杯她想要的冰咖啡。当 Rosa 回来时,一对新的后轮胎(装有传感器和 RFID)已经安装好了。机器人然后提示 Rosa 新轮胎上与隐私有关的选项,存储在汽车控制系统中的信息是为维护和维修用的,但在汽车行驶中如果周围有 RFID 读写器,这些信息将被读取到。Rosa 不想任何人知道(特别是她男友)知道她去哪里,所以她选择把这些信息设为被保护,防止被无权限的人看到。

终于，Rosa 可以开车去最近的商业街购物了。她想买有内嵌媒体播放器和温度调节功能的单板滑雪服。由于她要去的滑雪场已经通过无线传感器网络监测到雪崩的可能性很小，所以她感到去那里很安全。在通过法国和西班牙边境时，她不需要停留，因为她的车里保存放了她的驾照和护照，在越过边境的时候，这些信息被自动传输到边境控制装置中自动检查放行。

突然，Rosa 从她的太阳镜上收到一个视频寻呼，她赶紧把车停到路边，她看到男友正请求原谅并问她是否想一起度周末。这时她心情正好不错，于是她脱口而出，对导航系统发出了撤销隐私保护的语音命令，这样她的男友就可以看到她现在位置赶过来。

1.1.3　物联网的安全架构

物联网的安全架构可以根据物联网的架构分为感知层安全、网络层安全、应用层安全。应用层安全的研究内容，可能会与感知层安全和网络层安全有交叉，但其关注重点是具有应用特色的安全问题，或者需要在应用层解决的安全问题，如密钥管理问题、隐私保护问题、信任管理问题等。

物联网安全的研究应该突出从物联网应用中找安全需求，从有特色的共性网络技术中找安全问题，从物联网的特点中发现新问题。这里物联网的特点主要是指物联网存在多种形态网络的异构和融合、物联网设备可能具有资源受限的条件、设备可能是大规模且远距离可访问、设备的移动性和可定位追踪等。

从信息安全研究领域角度和信息安全需求角度，这里给出一个物联网安全的总体概貌，如图 1.2 所示。

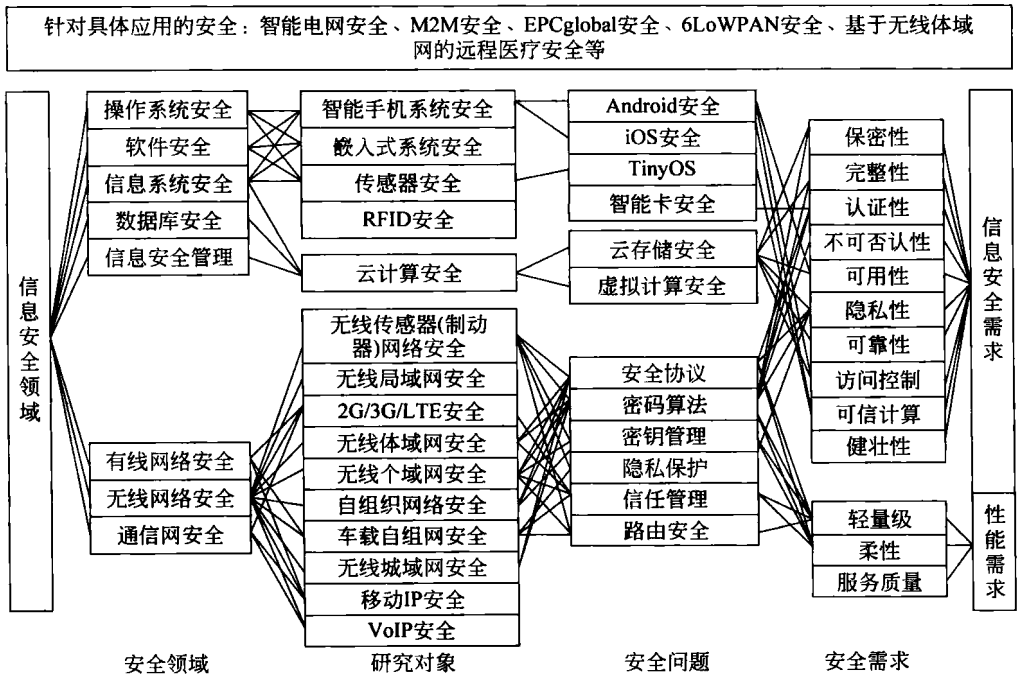

图 1.2　物联网安全的总体概貌

从物联网的架构出发，进行物联网安全的分类，可给出一个物联网安全架构的层次模型，如图 1.3 所示。这也是本书将要论述的主要内容，在每个论题中尽量选取了典型的网络情形和有代表性的安全问题。

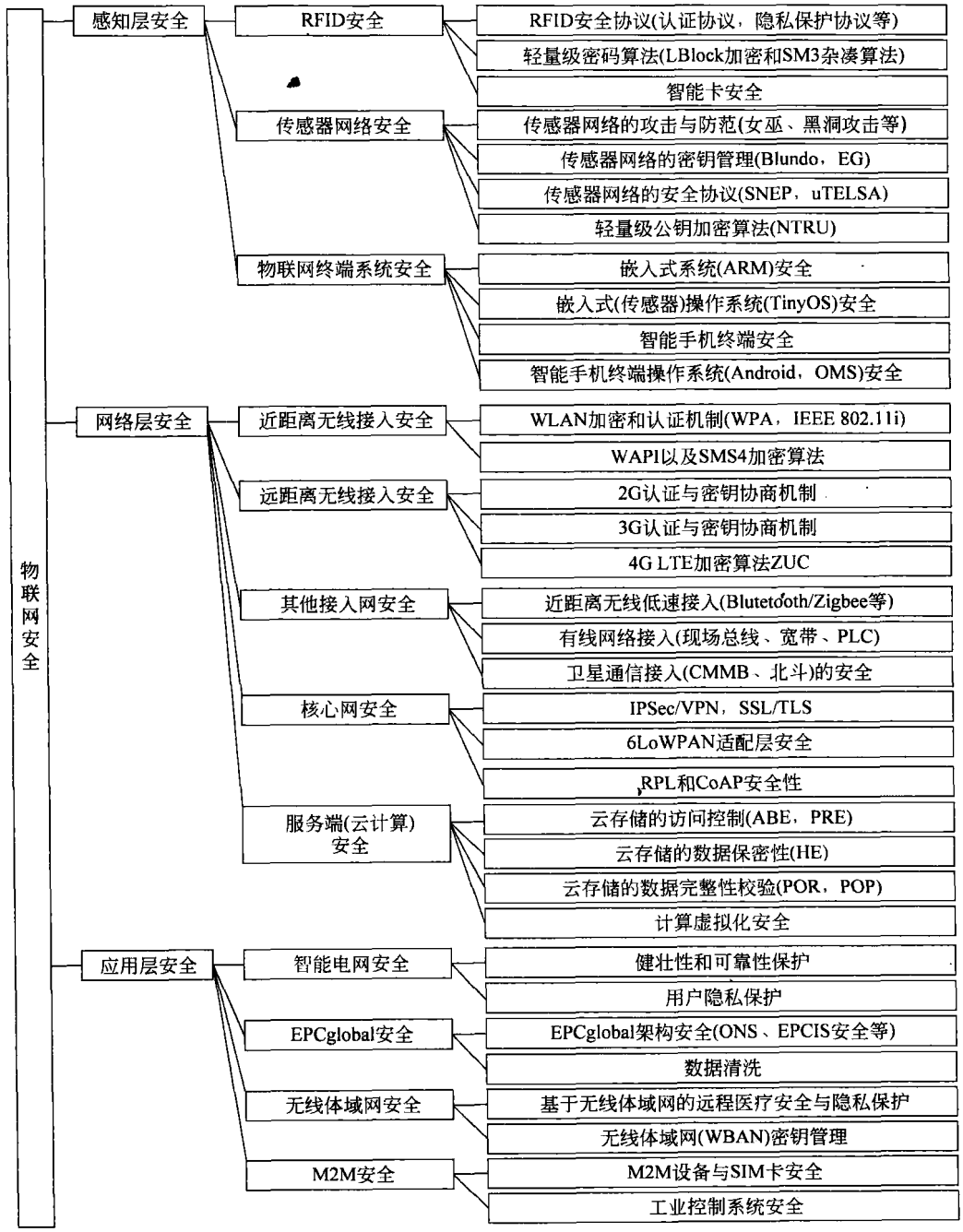

图 1.3　物联网安全架构的层次模型

下面给出一个物联网安全分析与设计的参考流程图，如图 1.4 所示。该流程图从感

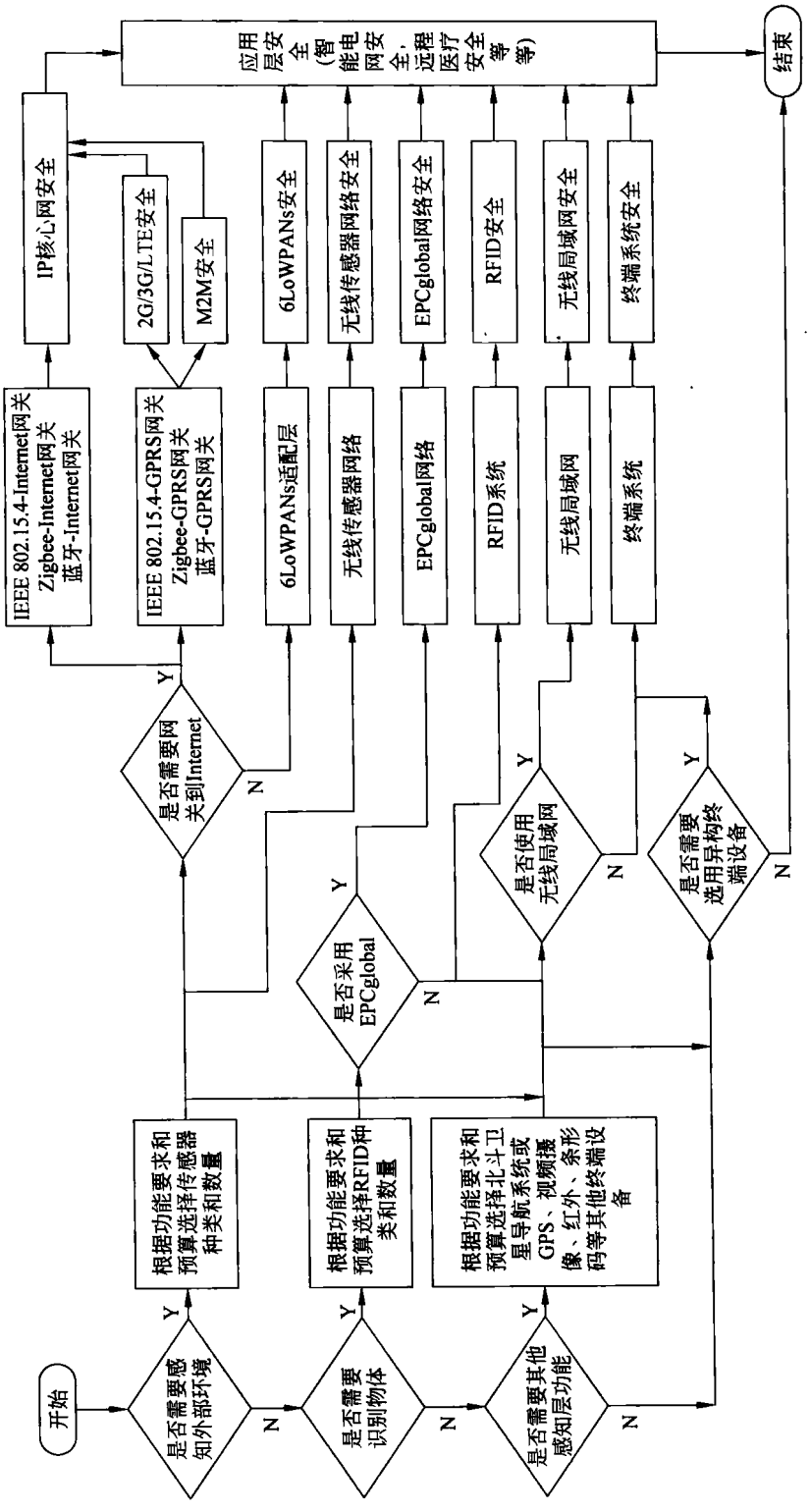

图 1.4　物联网安全设计的参考流程图