高等院校 物联网 专业规划教材

物联网安全技术

贺方成　韦鹏程　付仕明　著

清华大学出版社

高等院校 物联网 专业规划教材

物联网安全技术

贺方成　韦鹏程　付仕明　著

清华大学出版社
北京

内 容 简 介

“物联网”的概念源于互联网，它是互联网实现具体应用化的表现。近几年，物联网开始应用于家庭、农业、军事、医疗、交通等多个领域，给人们的生产和生活带来了便利，但同时物联网信息安全方面也面临巨大挑战。本书以物联网信息安全为出发点，讲解物联网的安全技术与应用，内容包括物联网信息安全概述、物联网信息安全、物联网信息安全密码概述、物联网感知层安全技术分析、物联网网络层安全技术分析、物联网应用层安全技术分析、物联网信息接入安全技术、物联网的网络安全技术、物联网信息安全技术应用、智能家居信息安全系统。本书内容新颖，侧重于物联网信息安全技术和应用案例，讲解前沿物联网安全技术知识，同时融入了全新的物联网研究成果和应用。

本书适合高等院校物联网工程专业的本科生、高职高专院校物联网专业学生作为教材使用，同时也适合物联网相关从业人员及相关领域研究人员参考阅读。

图书在版编目(CIP)数据

物联网安全技术/贺方成，韦鹏程，付仕明著. —北京：清华大学出版社，2018
(高等院校物联网专业规划教材)
ISBN 978-7-302-50785-7

Ⅰ. ①物… Ⅱ. ①贺… ②韦… ③付… Ⅲ. ①互联网络—应用—安全技术—高等学校—教材 ②智能技术—应用—安全技术—高等学校—教材 Ⅳ. ①TP393.408 ②TP18

中国版本图书馆 CIP 数据核字(2018)第 178792 号

责任编辑：汤涌涛
封面设计：常雪影
责任校对：吴春华
责任印制：李红英
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, 010-62791865
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　张：17.75　　字　数：430 千字
版　　次：2018 年 9 月第 1 版　　印　次：2018 年 9 月第 1 次印刷
定　　价：49.00 元

产品编号：079360-01

前　言

随着互联网的普及和计算机行业的飞速发展，物联网逐渐进入大众视野，并已经成为继互联网之后的第三次信息产业热潮，作为国家新产业，被大力发展。在物联网和云计算环境中，由于跨域使用资源、外包服务数据、远程检测和控制系统，使得数据安全和通信安全变得更加复杂，并呈现出与以往不同的新特征，需要研发新的安全技术以支撑这样的开放网络应用环境。因此，物联网安全技术也面临严峻的挑战。针对物联网安全问题，提出解决策略，解决关键问题。

目前，物联网已经被纳入高校教学计划，国内已有许多高校开办物联网专业，物联网安全技术是物联网方向的重要课题，因此，很多高校急需一本系统性的物联网安全技术图书。本书从物联网安全基础、物联网感知安全、物联网传输安全、物联网应用安全、物联网信息安全、物联网网络安全等多个方面对物联网安全问题及典型的物联网安全技术进行了总结和分析。

全书共 10 章，第 1～3 章主要介绍物联网的基本概念、物联网安全的整体结构、物联网安全面临的威胁与防范措施、物联网信息安全密码的体制与分类。第 4～6 章分别介绍物联网感知层、网络层、应用层的安全技术，这也是本书的重点。第 7～9 章介绍物联网信息接入技术、物联网中网络入侵的安全技术(包括系统安全、网络病毒、防火墙、网络防御技术等)、物联网信息安全技术的应用。第 10 章在物联网的应用领域选取智能家居信息安全系统，用具体的应用实例介绍物联网在智能家居安全方面的设计。

在内容安排上，在专业内涵、专业知识领域方面，本书都具有较强的学习针对性。本书采用分层架构思想，由下至上地论述物联网信息安全的体系结构和相关技术，包括物联网与信息安全、数据安全、隐私安全、接入安全、系统安全和无线网络安全等内容。

本书由重庆第二师范学院贺方成、韦鹏程、付仕明根据自身教学经验积累及部分物联网参考资料、文献及自身科研成果撰写而成。为了满足物联网工程专业学者及从业技术人员的学习需求，也为了适应物联网安全发展的需求，作者尽自身所能写成此书，期望本书能对读者起到实际效果，也期望能够为推动我国物联网的发展贡献自身的一分力量。该书支持项目为：重庆市交互式教育电子工程技术研究中心、重庆市儿童大数据工程实验室、重庆市计算机科学与技术重点学科和重庆市计算科学与技术特色专业。本书在编写过程中，还借鉴了国内外物联网的重要研究成果以及案例，在此向相关人员表示敬意和感谢。

由于作者水平和学识有限，加之时间仓促，书中不妥之处在所难免，殷切地希望广大读者及同行专家批评指正。

作　者

目　录

第1章 物联网信息安全概述

学习导读

物联网是现代信息技术发展到一定阶段后出现的一种聚合性应用与技术提升，将各种感知技术、现代网络技术和各种人工智能自动化技术聚合与集成应用，使人与物智慧对话，创造一个智慧的世界。随着物联网技术的广泛应用，物联网的安全性能也受到关注。

1.1 物联网概述

物联网通过装置在各类物体上的电子标签、传感器、二维码采集信息，并通过通信网络将物与物、物与人相连，协同工作，从而给物体赋予智能。物联网是继计算机、互联网之后的第三次信息科技发展浪潮。物联网是互联网的发展演化，并与云计算、大数据等概念相结合，对海量的跨地域、跨行业、跨部门的数据和信息进行分析处理，提升对物理世界、经济社会各种活动和变化的洞察力，实现智能化的决策和控制。

1.1.1 物联网的定义与特点

1. 物联网的定义

物联网是新一代信息技术的重要组成部分，其英文名称是 The Internet of things。顾名思义：“物联网是物物相连的互联网。”这有两层意思：第一，物联网的核心和基础仍然是互联网，是在互联网基础上延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间进行信息交换和通信。因此，物联网的定义是通过射频识别(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相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

2. 物联网的特点

互联网是人与人之间的网络，而物联网是物与物、物与人之间的网络。与互联网相比，物联网具有以下几个特点。

1) 传感信息能力较强

物联网可以利用 RFID、传感器、二维码等技术随时随地获取物体的信息。在物联网中存在许多传感器，每一个传感器都是一个信息源。传感器有不同的类别，不同的传感器所捕获、传递的信息内容和格式会存在差异，传感器按照一定的频率周期性地采集环境信息，每一次新的采集就会得到新的数据。

2) 传递功能较为强大且可靠

互联网信息量规模的扩大会导致信息的维护、查找、使用的困难相应增加，所以从海量的信息中快速、方便地找到具有使用需求的信息就显得尤为重要。物联网可以通过各种电信网络与互联网的融合，将物体的信息及时准确地传递出去。

3) 智能处理功能

物联网可以利用云计算、模糊识别等各种智能计算技术，对海量的数据和信息进行分析与处理，对物体实施智能化的控制。

4) 多角度过滤和分析

对海量的传感信息进行过滤和分析，是有效利用这些信息的关键。面对不同的应用，要从不同的角度进行过滤和分析。

1.1.2 物联网的应用行业

各个行业都对物联网有较大需求，如商场购物、医疗监测、配送中心等，发展物联网并将其应用于这些行业，必然产生很大的经济效益。由于人们更在乎物联网相关产品的收费方式和产品服务，对于技术要求不是很高。所以物联网应当以服务为主，协调好技术成本与收费，这是将来取得效益的关键。相信在未来几年，物联网的产业规模将进入快速增长期。

物联网的应用非常广泛，包括智能家居、智能物流、智能电网、智能交通、智能医疗、智能农业、智能环保、公共安全等多个领域，这些应用的发展将带动相关设备、基础设施和系统集成产业的规模发展。以“十三五”期间规划物联网发展的几个重点行业领域为例，可以看到每个领域都涉及庞大的市场规模，充满了发展机遇。

1. 智能家居

近几年来，随着经济的快速发展和人们生活水平的不断提高，智能家居和安防行业得到了长足的发展，今后更有加大步伐的趋势，特别是智能家居、安防系统的出现，让门禁识别远程监控报警感应视频监控、信息家电、灯光、燃气、烟雾、电力控制等系统通过网络无缝整合对接，实现远程智能控制，并将逐步进入寻常百姓家庭，成为家庭卫士。智能家居走进百姓生活，让民众的生活品质不断提高。另外，它在众多的城市安全、场馆安防等城市公共安防、工业安防、视频监控、交通监控、小区安防等领域的需求更加旺盛。

2. 智能物流

面向物流企业运输管理的“e 物流”系统，就是运用了物联网技术，为用户提供实时准确的货物信息、车辆跟踪定位、运输路径选择、物流网络设计与优化等服务，大大提升物流企业的竞争能力。

3. 智能电网

智能电网，就是利用传感器、嵌入式处理器、数字化通信和 IT，构建具备智能判断与自适应调节能力的多种能源统一入网和分布式管理的智能化网络系统，可对电网与客户用电信息进行实时监控和采集，且采用最经济与最安全的输配电方式将电能输送给终端用户，实现对电能的最优配置与利用，提高电网运行的可靠性和能源利用效率。

智能电网是物联网第一重要的运用，包括很多电信企业开展的“无线抄表”应用，其实也是物联网应用的一种。对于物联网产业甚至整个信息通信产业的发展而言，电网智能化将产生强大的驱动力，并将深刻影响和有力推动其他行业的物联网应用。

4. 智能交通

所谓智能交通，就是利用先进的通信、计算机、自动控制、传感器技术，实现对交通的实时控制与指挥管理。交通智能化是解决交通拥堵、提高行车安全、提升运行效率的重要途径。我国交通问题的重点和难点是城市道路拥堵。在道路建设跟不上汽车增长的情况下，对车辆进行智能化管理和调配，就成为解决拥堵问题的主要技术手段。目前，全国已经有 20 多个省区市实现公路联网监控、交通事故检测、路况气象等应用，路网检测信息采

集设备的设置密度在逐步加大，有些高速公路实现了全程监控，并可以对长途客运、危险货物运输车辆进行动态监管。21 世纪将是公路交通智能化的世纪，人们将要采用的智能交通系统，是一种先进的一体化交通综合管理系统。在该系统中，车辆靠自己的智能在道路上自由行驶，公路靠自身的智能将交通流量调整至最佳状态，借助于这个系统，管理人员对道路、车辆的行踪将掌握得一清二楚。

5. 智能医疗

智能医疗主要体现于医药产品、医药器械、血液和医疗废弃物的电子化管理，远程医疗信息平台。将物联网技术应用于医疗健康领域，可以解决医疗资源紧张、医疗费用高昂、人口老龄化压力等各种问题。例如，借助实用的医疗传感设备，可以实时地感知、处理和分析重大医疗事件，从而快速、有效地做出响应；乡村卫生所、乡镇医院和社区医院可以无缝地连接到中心医院，从而实时获取专家的建议、安排转诊和接受培训；通过联网整合并且共享各个医疗单位的医疗信息记录，从而构建一个综合的专业医疗网络。

6. 智能农业

智能农业包括农业生态环境监测、农业生产精细化管理和农产品与食品安全溯源。物联网的发展，将带动结构调整和产业升级，为新兴产业的腾飞装载上发动机，其中也蕴藏着良好的市场前景和巨大的投资机会。

7. 智能环保

随着经济的发展，人们对生活质量和环境的要求越来越高，为了提高环境监测和管理水平，环保部门可以建设基于物联网的智能环保通信系统。通过建设，形成一个覆盖全区的环境自动监测信息采集网络，实现对重点排污单位防治设施运行状态、主要污染物排放检测数据的自动传输和预警，实现重点流域水环境质量、重点城市环境空气质量自动监测数据实时传输。通过建设一个环境分析系统和交互式的环境监测、环境保护的动态信息发布平台，向政府、公众发布环境信息，实现集环境监测的智能感知、智能处理和综合管理于一体，推进污染减排和环境保护，实现环境与人、经济乃至整个社会的协调发展，促进环境改善。

8. 公共安全

公共安全问题是社会关注的问题。我们可以利用物联网开发出高度智能化的安全防范产品或系统，进行智能分析、判断及控制，最大限度地降低因传感器问题及外部干扰造成的误报，并且能够实现高精度定位，完成由面到点的实体防御与精确打击，进行高智能化的人机对话等功能，弥补传统安全系统的缺陷，确保人民的生命财产安全。此外，物联网也可以用于烟花爆竹销售点监测、危险品运输车辆监管、火灾事故监控、气候灾害预警、智能城管、平安城市建设；可以用于对残障人员、弱势群体(老人、儿童等)、宠物进行跟踪定位，防止走失等；还可以用于井盖、变压器等公共财产的跟踪定位，防止公共财产的丢失。

综上所述，物联网遍及智能交通、环保、公共安全、智能消防、工业监测、卫生医疗、食品、敌情侦察和情报搜集等多个行业领域。但是，物联网虽然已经起步并取得一定的发

展，但未来必将接受严峻的挑战，就像互联网发展时会出现互联网泡沫一样，物联网的发展之路必定也不会一帆风顺。但是物联网时代的到来是大势所趋，未来将出现一系列物联网产品和服务。

1.1.3 物联网的体系结构

目前，公认的物联网的体系结构分为三个层次，分别是感知层、网络层(包括接入网络)和应用层(包括信息、处理、云计算等平台)。如图 1-1 所示为业界常用的物联网体系结构。

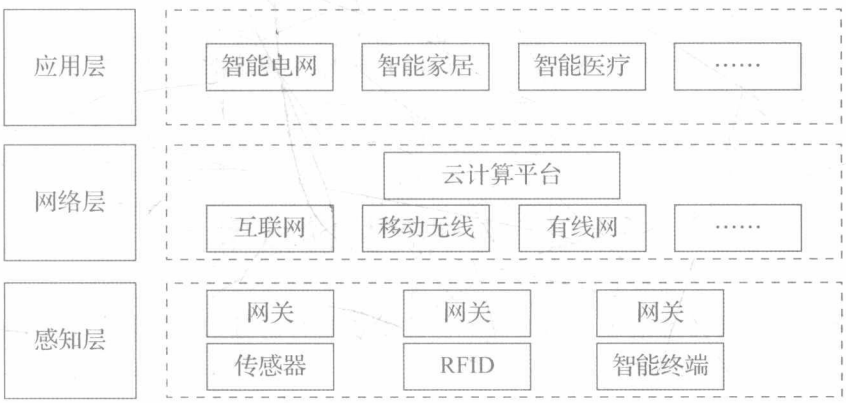

图 1-1 物联网体系结构

1. 感知层

物联网感知层的主要设备包含各种传感器、RFID、智能终端等，这些设备的主要功能是完成用户或者系统所需数据的采集以及提取。传感器网络中常采用的一个簇结构是各个传感器间采用自组网的方式相互连接，并通过接入网关连接到互联网上；RFID 技术又称为射频标签，即带有存储器的电子标签，它主要是通过射频的方式将 RFID 中的信息传递给所需信息的载体或客户，而这种信息的传递主要是通过射频间的通信完成的；智能终端主要包括智能手机、PDA、iPad 等具有智能系统同时又带有无线射频的通信设备，用户可以通过移动网络厂商将数据或者信息远程传送到指定的 Server(服务器)。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。

2. 网络层

物联网网络层又称为传输层，该层的主要功能是完成数据与信息的传递。常见的接入技术包括有线接入以及无线接入：有线接入技术已经十分成熟，该接入技术以其高稳定性被应用于日常生活中；而无线接入技术由于其低廉的部署价格以及接入的便捷性，在业界十分活跃。网络层也可以分为接入网、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(蓝牙)、红外；也可以是无线远距离接入，如移动通信网络 3G/4G/4G+、WiMAX 等；还可能为其他接入形式，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。云计算技术的兴起，为互联网用户提供了更为方便快捷的信息传递方式。总之，物联网技术中网络接入层的主要任务就是完成用户或者系统对感知层数据以及信息的获取。

3. 应用层

物联网应用层主要实现用户根据不同的感知数据做出不同的反应。当前市场上兴起的云电视、智能家居、智能医疗系统等都是物联网技术的广泛应用。物联网应用层的主要作用就是对感知层获取数据信息的应用。应用层对物联网信息和数据进行融合、处理和利用，这也是物联网发展的目的。

总之，物联网体系结构的各层之间，信息不是单向传递的，也有交互、控制等，所传递的信息多种多样，这其中关键是物品的信息，包括在特定应用系统范围内能唯一标识物品的识别码和物品的静态与动态信息。

1.2 物联网关键技术

物联网涉及的新技术很多，其中的关键技术主要有射频识别技术、传感器技术、网络通信技术和云计算(传输数据计算)等。

1.2.1 射频识别技术

射频识别技术，俗称“电子标签”，是物联网中非常重要的技术，是实现物联网的基础与核心。射频技术是一项利用射频信号通过空间耦合(交变磁场或电磁场)实现无接触信息传递并通过所传递的信息达到识别目的的技术。这一技术由三个部分构成：①标签(Tag)，附着在物体上以标识目标对象；②阅读器(Reader)，用来读取(有时还可以写入)标签信息，既可以是固定的也可以是移动的；③天线(Antenna)，其作用是在标签和阅读器之间传递射频信号。当然，在实际应用中还需要其他硬件和软件的支持。

射频识别技术的基本思想是，通过先进的技术手段，实现人们对各类物体或设备(人员、物品)在不同状态(移动、静止或恶劣环境)下的自动识别和管理。由于射频识别无须人工干预，可使用于各种恶劣环境，可用来追踪和管理几乎所有物理对象，所以零售商和制造商非常关心和支持这项技术的发展和应用。比如，沃尔玛公司就成功地将射频技术应用于供应链管理中，高速公路的自动收费系统更是这项技术的最成功应用之一。

射频技术发展面临的主要问题和难点是：①射频识别的碰撞防冲突问题；②射频天线研究；③工作频率的选择；④安全与隐私问题。

1.2.2 传感器技术

要产生真正有价值的信息，仅有射频识别技术是不够的，还需要传感技术。由于物联网通常处于自然环境中，传感器要长期经受恶劣环境的考验，因此，物联网对传感器技术提出了更高的要求。

作为摄取信息的关键器件，传感器是现代信息系统和各种装备不可缺少的信息采集手

段。如果把计算机看作是处理和识别信息的大脑，把通信系统看作是传递信息的“神经”系统，则传感器就是感觉器官。所谓传感器，是指那些对被测对象的某一确定的信息具有感受(或响应)与检出功能，并使之按照一定规律转换成与之对应的可输出信号的元器件或装置。离开了传感器对被测的原始信息进行准确可靠的捕获和转换，一切准确的测试与控制都将无法实现。即使是最现代化的电子计算机，假如没有准确的信息(或转换可靠的数据)和不失真的输入，也将无法充分发挥其应有的作用。

传感器技术的发展与突破主要体现在两个方面：①感知信息方面；②传感器自身的智能化和网络化。

未来传感器技术的发展趋势大致分为以下几个方面。

(1) 向检测范围挑战。

(2) 集成化，多功能化。

(3) 向未开发的领域挑战——生物传感器。

(4) 传感技术、智者为尊——智能传感器(Smart Sensor)。

(5) 发现和利用新材料。

传感器技术是一门综合的高新技术，它集光、机、电、生物医学于一身。可以毫不夸张地说，传感器技术的水平从一个侧面反映了微电子技术、MEMS、纳米技术、光电子技术、生物技术等高新技术的水平。

1.2.3 网络通信技术

无论物联网的概念如何扩展和延伸，其最基础的物物之间的感知和通信是不可替代的关键技术。网络通信技术包括各种有线和无线传输技术、交换技术、组网技术、网关技术等。

其中 M2M 技术则是物联网实现的关键。M2M 技术是机器对机器(Machine To Machine)通信的简称，指所有实现人、机器、系统之间建立通信连接的技术和手段，同时也可代表人对机器(Man To Machine)、机器对人(Machine To Man)、移动网络对机器(Mobile To Machine)之间的连接与通信。M2M 技术适用范围广泛，可以结合 GSM/GPRS/UMTS 等远距离连接技术，也可以结合 Wi-Fi、BlueTooth、Zigbee、RFID 和 UWB 等近距离连接技术，此外还可以结合 XML 和 Corba，以及基于 GPS、无线终端和网络的位置服务技术等，用于安全监测、自动售货机、货物跟踪领域。目前，M2M 技术的重点在于机器对机器的无线通信，而将来的应用则遍及军事、金融、交通、气象、电力、水利、石油、煤矿、工控、零售、医疗、公共事业管理等各个行业。短距离无线通信技术的发展和完善，使得物联网前端的信息通信有了技术上的可靠保证。

通信网络技术为物联网数据提供传送通道，如何在现有网络上进行增强，适应物联网业务的需求(低数据率、低移动性等)，是该技术研究的重点。物联网的发展离不开通信网络，更宽、更快、更优的下一代宽带网络将为物联网发展提供更有力的支撑，也将为物联网应用带来更多的可能。

1.2.4 云计算

云计算(Cloud Computing)是网格计算、分布式计算、并行计算、效用计算、网络存储、

虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物。云计算的基本原理是：通过使计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，企业数据中心的运行将与互联网更加相似。这使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。它旨在通过网络把多个成本相对较低的计算实体整合成一个具有强大计算能力的完美系统，并借助 SaaS、PaaS、IaaS、MSP 等先进的商业模式把这强大的计算能力分布到终端用户手中。

云计算的一个核心理念就是通过不断提高“云”的处理能力，减少用户终端的处理负担，最终使用户终端简化成一个单纯的输入输出设备，并能按需享受“云”的强大计算处理能力。Google 搜索引擎是云计算的成功应用之一。

1.3 物联网安全问题概述

物联网的关键在于应用，物联网应用将深入所有人生活的方方面面。物联网应用中所面临的安全威胁以及安全事故所造成的后果，将比互联网时代严重得多。物联网安全呈现大众化、平民化特征，安全事故的危害和影响巨大。物联网应用中各处都需要安全，安全措施与成本的矛盾十分突出。物联网安全，还必须改变先系统后安全的思路，在物联网应用设计和实施之初，就必须同时考虑应用和安全，将两者从一开始就紧密结合，系统地考虑感知、网络和应用的安全，才能更好地解决各种物联网安全问题，应对物联网安全的新挑战。下面从五个方面阐述物联网信息安全的问题。

1.3.1 物联网安全特征

与传统网络相比，物联网发展带来的安全问题将更为突出，所以要强化安全意识，把安全放在首位，超前研究物联网产业发展可能带来的安全问题。物联网安全除了要解决系统信息安全的问题之外，还需要克服成本、复杂性等新的挑战。物联网安全面临的新挑战主要包括需求与成本的矛盾，安全复杂性进一步加大，信息技术发展本身带来的问题，以及物联网系统攻击的复杂性和动态性仍较难把握等方面。总体来说，物联网安全的主要特点表现在四个方面：大众化、轻量级、非对称和复杂性。

(1) 大众化。物联网时代，当每个人习惯于使用网络处理生活中的所有事情的时候，当你习惯于网上购物、网上办公的时候，信息安全就与你的日常生活紧密地结合在一起了，不再是可有可无的了。如果物联网时代出现了安全问题，那么每个人都将面临重大损失。只有当安全与人们的利益相关的时候，所有人才会重视安全，也就是所谓的“大众化”。

(2) 轻量级。物联网中需要解决的安全威胁数量庞大，并且与人们的生活密切相关。物联网安全必须是轻量级、低成本的安全解决方案。只有这种轻量级的思路，普通大众才可能接受。轻量级解决方案正是物联网安全的一大难点，安全措施的效果必须要好，同时要低成本，这样的需求可能会催生出一系列的安全新技术。

(3) 非对称。物联网中，各个网络边缘的感知节点的能力较弱，但是其数量庞大，而网络中心的信息处理系统的计算处理能力非常强，整个网络呈现出非对称的特点。物联网安全在面向这种非对称网络的时候，需要将能力弱的感知节点的安全处理能力与网络中心强的处理能力结合起来，采用高效的安全管理措施，使其形成综合能力，从而能够整体上

发挥出安全设备的效能。

(4) 复杂性。物联网安全十分复杂，从目前可认知的观点出发可以知道，物联网安全所面临的威胁、要解决的安全问题、所采用的安全技术，不仅在数量上比互联网大很多，而且还可能出现互联网安全所没有的新问题和新技术。物联网安全涉及信息感知、信息传输和信息处理等多个方面，并且更加强调用户隐私。物联网安全各个层面的安全技术都需要综合考虑，系统的复杂性将是一大挑战，同时也将呈现大量的商机。

1.3.2 物联网安全现状

目前，国内外学者针对物联网的安全问题开展了相关研究，在物联网感知、传输和处理等各个环节均开展了相关工作，但这些研究大部分是针对物联网的各个层次的，还没有形成完整统一的物联网安全体系。

在感知层，感知设备有多种类型，为确保其安全性，目前主要是进行加密和认证工作，利用认证机制避免标签和节点被非法访问。感知层加密已经有了一定的技术手段，但是还需要提高安全等级，以应对更高的安全需求。

在传输层，主要研究节点到节点的机密性，利用节点与节点之间严格的认证，保证端到端的机密性，利用密钥有关的安全协议支持数据的安全传输。

在应用层，目前的主要研究工作是数据库安全访问控制技术，但还需要研究其他的一些相关安全技术，如信息保护技术、信息取证技术、数据加密检索技术等。

在物联网安全隐患中，用户隐私的泄露是危害用户的极大安全隐患。所以在考虑对策时，首先要对用户的隐私进行保护。目前，主要用加密和授权认证等方法。通过加密，只有拥有解密密钥的用户才能读取通信中的用户数据以及用户的个人信息，这样能够保证传输过程中不被他人监听。但是，加密数据的使用变得极为不方便，因此需要研究支持密文检索和运算的加密算法。

另外，物联网核心技术掌握在世界上比较发达的国家手中，始终会对没有掌握物联网核心技术的国家造成安全威胁。所以，要解决物联网的安全隐患，我国应该加大投入力度，进一步地开发研究，攻克技术难关，争取早日掌握物联网安全的核心技术。

1.3.3 物联网安全威胁

人们可以通过物联网感知各方面的信息，同时也可以通过物联网实现各种应用。通过互联网，人们可以远程感知和控制类似家电、交通、能源、金融等设施和服务。在物联网提供这些便利的同时，人们也对物联网的强大感到担忧。物联网在网络的每个层次上都存在威胁：感知层方面有终端设备的物理安全、信息的传输安全、隐私泄露等问题，网络层方面有数据破坏、身份假冒及信息泄露等安全问题，应用层方面有身份假冒、非法接入、越权操作等安全问题。目前，国内外对物联网体系架构的研究是三层的架构体系，即应用层、网络层、感知层。下面分别从感知层、网络层和应用层对其面临的安全威胁进行分析。

1. 感知层安全威胁

如果感知节点所感知的信息不采取安全防护或者安全防护的强度不够，则这些信息很可能被第三方非法获取，而信息泄密某些时候可能会造成很大的危害。由于安全防护措施