普通高等教育“十三五”规划教材

物联网安全实践

WULIANWANG ANQUAN SHIJIAN

雷 敏　王 婷　编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

物联网安全是当前社会关注的热点，基于物联网的智能终端各种安全事件频发。本书介绍物联网智能终端和协议存在的安全隐患，并对这些安全隐患进行分析与加固。书中对智能摄像头、智能插座、ZigBee、蓝牙、物联网应用层协议、NFC 等安全问题进行分析，同时还介绍物联网安全分析所需要的工具和基本方法。

本书可作为高校网络空间安全、信息安全和计算机等相关专业学生的课程实验、课程设计、项目实践、项目实训教材，也可用于社会从业人员的学习提高，同时还可作为各培训机构的实践教材。

图书在版编目(CIP)数据

物联网安全实践 / 雷敏，王婷编著 . -- 北京 ：北京邮电大学出版社，2017.7
ISBN 978-7-5635-5103-3

Ⅰ.①物… Ⅱ.①雷… ②王… Ⅲ.①互联网络－应用－安全技术 ②智能技术－应用－安全技术 Ⅳ.①TP393.4 ②TP18

中国版本图书馆 CIP 数据核字（2017）第 108393 号

书　　名：物联网安全实践
著作责任者：雷　敏　王　婷　编著
责 任 编 辑：刘　佳
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：
开　　本：787 mm×1 092 mm　1/16
印　　张：8.5
字　　数：210 千字
版　　次：2017 年 7 月第 1 版　2017 年 7 月第 1 次印刷

ISBN 978-7-5635-5103-3　　定　价：20.00 元

前言

Foreword

Foreword

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，国务院学位委员会正式批准增设“网络空间安全”一级学科，并且首批授予了北京邮电大学等29所大学“网络空间安全一级学科博士点”。如今，许多大学都在努力培养网络安全人才，都在下大功夫、下大本钱，聘请优秀老师，招收优秀学生，建设一流的网络空间安全学院。

优秀教材是培养网络空间安全专业人才的关键。但是，这却是一项十分艰巨的任务，原因有二：一是，网络空间安全的涉及面非常广，至少包括密码学、数学、计算机、操作系统、通信工程、信息工程、数据库、硬件等学科，因此，其知识体系庞杂、难以梳理；二是，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资要求也很高。

随着万物互联的普及，越来越多的物联网智能终端部署，但是物联网系统也存在诸多安全隐患，物联网安全越来越重要。目前理论结合实践的物联网教材较少，为弥补案例教学、实训教学等方面的薄弱环节，本书作者计划出版《物联网安全实践》一书。因为，物联网实践部分在过去的教材中很少涉及，而随着物联网的迅速普及，它已经成为网络空间安全的重要内容之一。因此，开展物联网安全实践研究对网络空间安全人才的培养具有十分重要的现实意义。

本书通过介绍典型的物联网系统存在的安全隐患，分析典型物联网系统智能终端安全案例，通过介绍典型物联网智能终端存在的安全隐患案例让研究人员更好地掌握物联网系统存在的安全隐患。书中选取的案例均是比较典型的案例，此种类型的漏洞在其他物联网中也存在。本书案例不针对某种产品，而且所有的案例仅仅用于教学。

本书针对每种类型的安全漏洞都尽量提出加固建议，宗旨是希望帮助物联网安全的研究人员和物联网系统的研发人员掌握物联网安全漏洞产生的原因和原理，从而找到修补这些安全漏洞的方法，对这些漏洞进行修补。通过本书的介绍希望能让研发人员重视安全，通过学习这些安全漏洞产生的原因让物联网系统的研发人员在研发过程中避免再次出现类似的安全隐患，从而避免物联网系统出现类似的安全漏洞和安全隐患。

本书内容涵盖物联网智能摄像头、智能路由器、智能开关等各种智能家居

设备的安全分析，包含物联网基本概念、物联网系统架构、物联网安全威胁、物联网各种安全分析案例等。

本书第4章和第8章由中国信息安全测评中心王婷编写；其余章节由北京邮电大学网络空间安全学院信息安全中心雷敏副教授编写。在本书编写过程中，中国信息安全测评中心张普含博士、谢丰博士、马洋洋等提供了很多宝贵意见，北京邮电大学多名研究生和本科生实践了书中的案例，在此对他们表示衷心感谢。

本书针对物联网安全，实践内容丰富、新颖，可操作性强，既适合网络空间安全、信息安全等相关专业的学生，也适合物联网安全研究人员、开发人员和有志于进一步提高物联网安全实践能力的读者。

今后随着物联网技术的不断发展，随着NB-IoT和基于LoRa的蜂窝物联网系统的逐步商用，越来越多的物联网终端采用基于LPWAN方式接入物联网，这些物联网设备会产生很多的安全隐患。同时随着工业物联网和医疗物联网等各种物联网应用的逐步发展，物联网系统将会出现更多的安全问题，今后将不断地更新图书内容。

网络空间安全实践教学除需要教材外，还需要用于实践教学的教学环境，本书所有的实验均需在实验环境下完成，本书作者将探索搭建书中所有实验内容所需的实验环境。

由于作者水平有限，书中难免存在疏漏和不妥之处，欢迎读者批评指正。作者联系方式：雷敏，leimin@bupt.edu.cn。

编著者

2016年12月

目录

Contents

第 1 章

物联网概述

1.1 物联网基本概念

物联网(The Internet of Things)是新一代信息技术的重要组成部分,也是“信息化”时代的一个重要发展阶段。物联网,顾名思义,是物物互联网络。相对于互联网,物联网扩展到了任何的物体与其他物体之间的信息交换和通信。

关于物联网,至今没有一个统一的定义,最初提出其概念可以概括为通过射频识别(RFID)技术、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,以实现智能化识别、定位、跟踪、监控和管理的一种网络。

欧盟提出物联网的定义:物联网是未来互联网的一部分,能够被定义为基于标准和交互通信协议的具有自配置能力的动态全球网络设施,在物联网内物理和虚拟的“物件”具有身份、物理属性、拟人化等特征。

国际电信联盟(ITU)在《ITU2015 互联网报告:物联网》中指出:物联网是指通过射频识别技术(RFID)、传感器技术、纳米技术、智能嵌入技术等解决物品到物品(Thing to Thing,T2T)、人到物品(Human to Thing,H2T)、人到人(Human to Human,H2H)之间的互联。

2010 年,温家宝总理在十一届人大三次会议上所做的政府工作报告中对物联网做了如下定义:物联网是指通过信息传感设备,按照规定的协议,把任何物品和互联网连接起来,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。

物联网的起源可追溯至 1995 年,比尔·盖茨在《未来之路》一书中描绘了物联网的雏形,但由于当时设备和技术的限制,物联网并没有受到人们的广泛关注。四年后,美国麻省理工学院(MIT)成立了“自动识别中心(Auto-ID)”,该中心的 Kevin Ashton 教授于 1999 年在研究 RFID 时最早阐明了物联网的基本含义,将“物联网”定义为把所有物品通过射频识别(RFID)和条码等信息传感设备与互联网连接起来,实现智能化管理和识别的网络。

2005 年 11 月 17 日,在突尼斯举行的消息社会世界峰会(WSIS)上,国际电信联盟(ITU)发布了名为《ITU 互联网报告 2005:物联网》的年度报告,扩展了物联网的概念,同时物联网的范围也得到了较大的扩展。世界上所有的物体都能够通过互联网进行积极沟通,物联网也不再仅指基于射频识别(RFID)技术的网络,传感器技术、纳米技术、智能嵌入技术也将得到更加普遍的利用。物联网观念的普及很大程度上受益于此。

2008 年,IBM 提出了“智慧地球”发展战略后,迅速得到了美国政府的高度重视。2009 年,美国总统奥巴马在和工商领袖举行的圆桌会议上做出积极回应,将“新能源”和“物联网”作为振兴美国经济的两大武器,物联网就是在这一年进入快速发展之年。

同年，温家宝总理考察了中科院高新微纳传感网工程技术研发中心，强调在未来物联网的发展中要早一点谋划，早一点攻破其核心技术。欧盟执委会也在2009年发布了欧洲物联网行动计划，描绘了物联网技术的应用前景，提出欧盟政府要加强对物联网的管理，促进物联网的发展。此外，韩国和日本也都于2009年针对本国物联网发展做出相应规划并出台政策。

1.2 物联网系统架构

物联网作为战略性新兴产业的重要组成部分，已成为当前世界新一轮经济和科技发展的战略制高点之一。越来越多的移动终端开始接入企业或家庭网络，全球领先的信息技术研究和顾问公司Gartner预计2016年全球将使用64亿个物联网设备，到了2020年，全球所使用的物联网设备数量将增长至208亿个。

物联网通信技术有很多种，从传输距离上区分，可以分为两类：一类是短距离通信技术，代表技术有ZigBee、Wi-Fi、Bluetooth、Z-wave等，典型的应用场景如智能家居；另一类是广域网通信技术，业界一般定义为低功耗广域网（Low-Power Wide-Area Network，LPWAN），典型的应用场景如智能抄表。

当前，物联网系统架构有两种划分方法，第一种方法是将物联网系统分为感知层、传输层、管控层和应用层的四层架构，如图1.1所示。其中感知层由各种具有感知能力的

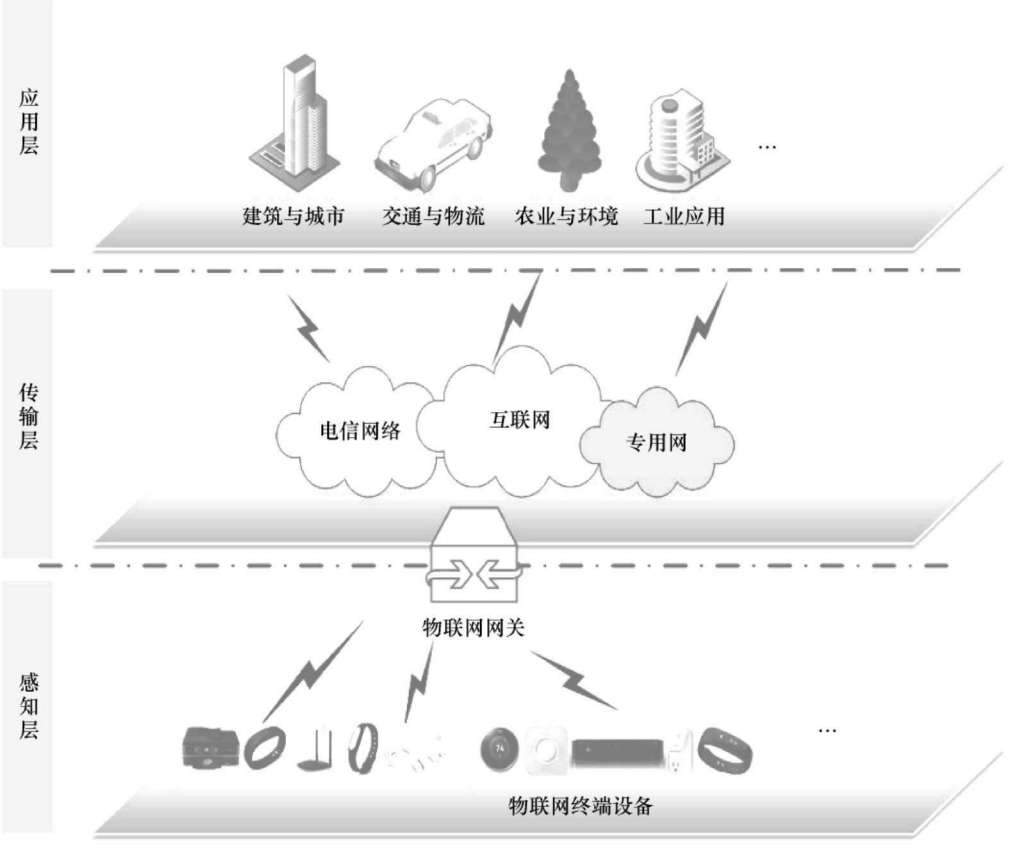

图1.1 物联网系统架构

设备组成，主要用于感知和采集数据。传输层也被称为网络层，解决的是感知层所获得的数据传输问题，是进行信息交换、传递的数据通路，包括接入网与传输网两种。管控层主要接受采集到的数据信息，进行相关的信息存储、处理和控制等事务。应用层根据底层采集的数据，形成与业务需求相适应、实时更新的动态数据资源库，为各类业务提供统一的信息资源支撑，从而最终实现物联网各个行业领域应用，一般情况下也可以将管控层合并划分到应用层。

第二种分类方法是将物联网系统分为海（海量的终端设备）、网（网络通信）和云（云端服务），其中“海”对应感知层海量终端，这些海量终端包括基于 Wi-Fi 协议、ZigBee、蓝牙等短距离无线通信协议的终端，也包括基于 NB-IoT 和 LoRa 等新兴技术的各种智能终端。“网”对应传输层的网络通信，“云”对应管控层和应用层，如图 1.2 所示。其中感知层的智能终端收集各种数据，感知层收集的数据通过网络层传送到应用层，应用层对这些数据进行处理。

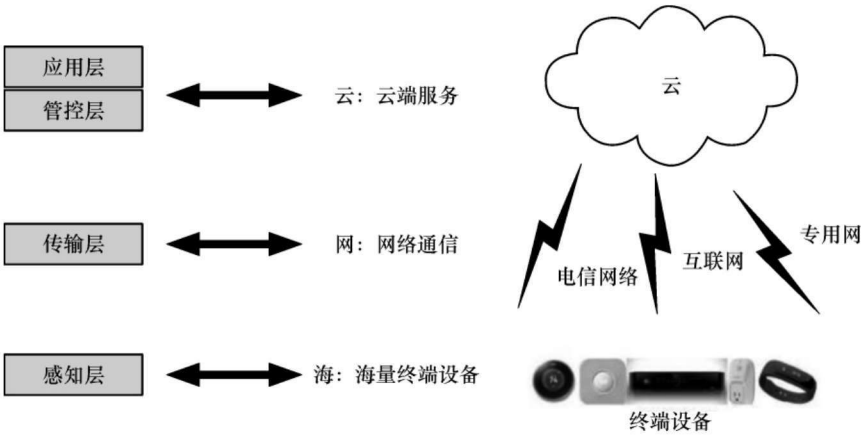

图 1.2　物联网系统架构

1.3　物联网的应用领域

物联网应用涉及国民经济和人类社会生活的各个方面，它将改变人们的生活方式，对整个社会产生深刻变革。下面介绍物联网的主要应用领域。

1. 智能安防

随着智能摄像头的普及和智慧城市的建设，越来越多的智能安防系统应用在城市管理、工厂和学校的监控。联网的智能监控设备通过网络将监控的画面实时传送到智能监控管理平台，智能监控的管理平台对所有已经安装的智能安防设备进行管理，并收集智能安防设备采集的各种实时画面。

智能安防系统的架构如图 1.3 所示，智能安防系统主要用于监控和智慧城市建设与管理等。

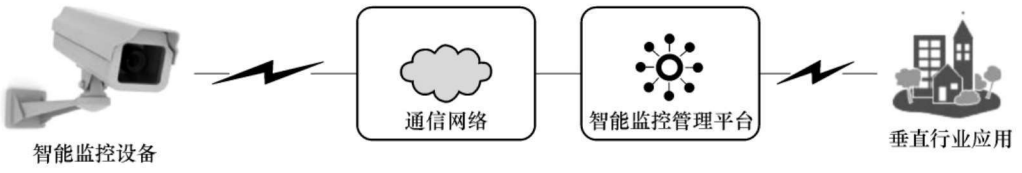

图 1.3　智能安防系统的架构图

2. 家联网

家联网(Home internet)是将家中所有的智能家电,如彩电、冰箱、洗衣机等大家电和各种小家电,如灶具、窗帘、微波炉等连成一个局域网,图 1.4 展示了家庭互联网网络的大致架构,网络节点包括控制点、设备和网关。

控制点是网络中的控制器,如手机、PAD、机顶盒等人机交互设备。设备是服务提供者,如电视、空调、冰箱、烟灶、开关、窗帘等。网关是一种特殊设备,可以含有一般设备的所有属性,也可作为其他设备的代理。控制点、设备和网关都是逻辑设备,某一个物理设备可以同时是设备、网关和控制点。

随着家联网的不断发展,越来越多的设备进入到家联网,除传统使用 Wi-Fi 协议的设备之外,还有很多使用 ZigBee、蓝牙或者其他各种短距离通信协议的设备接入到家庭互联网中。

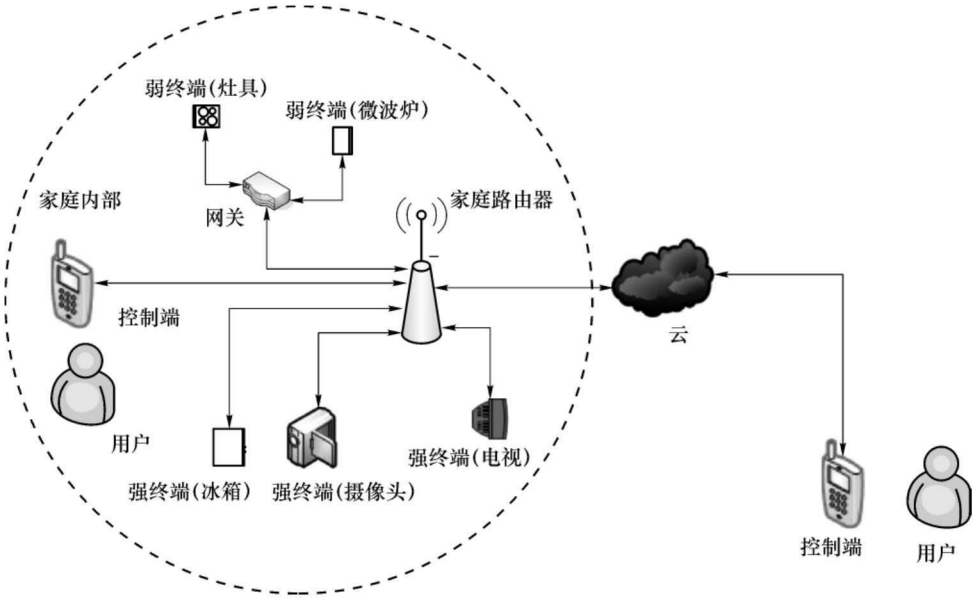

图 1.4　家庭互联网网络构架图

3. 基于 **LoRa** 的物联网系统

LoRa 是 LPWAN(低功耗广域物联网)的一种,目前国内已成立中国 LoRa 应用联盟(简称“CLAA”),旨在推动 LoRa 产业链在中国的应用和发展,建设多业务共享、低成本、广覆盖、可运营的 LoRa 物联网。LoRa 的网络结构如图 1.5 所示,其中 LoRa 的网关可以接入数量众多的终端设备,LoRa 使用非授权频段。

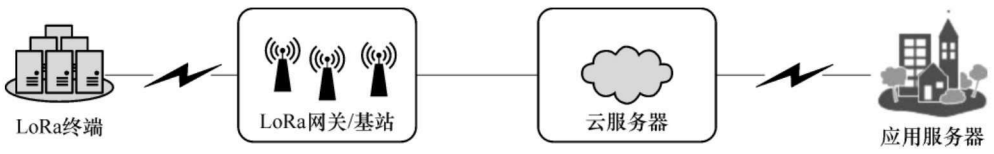

图 1.5　LoRa 物联网

4. 基于 **NB-IoT** 的物联网系统

NB-IoT 是 LPWAN(低功耗广域物联网)的一种，是 2015 年 9 月在 3GPP 标准组织中立项提出的一种新的窄带蜂窝通信 LPWAN 技术。其核心是面向低端物联网终端(低耗流)，适合广泛部署在智能家居、智慧城市、智能生产等领域，NB-IoT 基于现有的蜂窝网络构建，只消耗约 180 kHz，可以直接部署在 GSM 网络、UMTS 网络和 LTE 网络。NB-IoT 使用授权频谱，网络结构如图 1.6 所示。其中 NB-IoT 的智能终端连接到 NB-IoT 基站，基站和 NB-IoT 核心网连接，然后将上传到各种 IoT 的管理应用平台，之后将数据用于各种垂直行业应用。

图 1.6　NB-IoT 物联网系统架构

5. 车联网

车联网(Internet of Vehicles)是当前比较热门的一种物联网的应用领域。车联网由车辆、驾驶员和车载智能系统等多系统组成一个巨大交互网络，用于实时完成车辆之间的通信和交互。在感知层，车辆通过 GPS、RFID、传感器、摄像头图像处理等装置，完成自身环境和状态信息的采集；在网络层，车联网终端收集的各种信息通过网络通信技术，将自身采集的各种信息传输汇聚到应用层或云端；应用层和云端通过计算机和人工智能处理技术，将收集的信息进行分析和处理，从而计算出不同车辆的最佳行驶路线，及时汇报路况和安排信号灯周期，从而能够缓解交通的原理，合理地规划路线等。

1.4　思 考 题

1. 物联网一般分为几个层次，每个层次中涉及哪些技术？

2. 随着物联网技术的发展，物联网典型的应用领域越来越多，请调研物联网的典型应用领域。

3. LoRa 和 NB-IoT 的主要差别是什么？请给出一个典型的行业应用说明两者之间的差别。

4. 物联网对人们的生活带来哪些变化，请举例说明。

第 2 章

物联网通信协议

物联网的智能终端和控制 APP 需要通过通信网络和云端通信，智能终端和云端通信的过程中采用各种通信协议，如物理层/MAC 层、网络层、传输层和应用层。其中网络层所使用的协议和传统的互联网所使用的协议相同。本章主要介绍物联网系统所使用的应用层协议，物理层所使用的安全协议，如 ZigBee、蓝牙等将在后续章节介绍。

2.1 物联网通信协议概述

2.1.1 物联网各层通信协议

物联网各层所使用的通信协议不同，物联网所使用的协议分为物理层、网络层、传输层和应用层四层，每层所使用的通信协议不同。各层所使用的通信协议如图 2.1 所示。

物理层在物联网体系中，也叫接入层，是物联网设备组网和接入网络的基层，它包括蜂窝网络协议 GSM、GPRS、LTE、无线局域网协议 IEEE 802.11、宽带无线 MAN 标准 IEEE 802.16 和低速率个人无线网协议 IEEE 802.15.4 等，还包括近距离通信协议蓝牙、NFC 等。

网络层、传输层和传统的计算机网络中的层次类似。网络层以 IP 协议为主，包括 IPv4 和 IPv6 等，除此之外在 IPv6 的基础上，还提出了专门针对物联网而设计的低速率个人无线网协议 6LoWPAN，以及基于 802.15.4 的低功耗局域网协议 ZigBee 等。网络层对端到端的包传输进行定义，它定义了能够标识所有结点的逻辑地址，还定义了路由实现的方式和学习的方式。

传输层以 TCP 和 UDP 协议为主，这层的功能包括是否选择差错恢复协议还是无差错恢复协议，及在同一主机上对不同应用的数据流的输入进行复用，还包括对收到的顺序错误的数据包的重新排序功能。

应用层负责设备之间应用程序通信服务，是用户日常接触最多的层次。在物联网体系中，除了常规的 HTTP、WebSocket、XMPP 协议之外，还有专门针对物联网应用提出的 CoAP 协议、MQTT 协议等。

物联网应用层所使用的协议很多，包括 HTTP、HTTPS、XMPP、MQTT 等。这些协议都已经被广泛地应用，并且每种协议都有多种代码实现的方法，但是在具体物联网系统架构设计时，需要考虑实际场景的通信需求，选择合适的协议，可以通过 3G/4G 适配性能、LIN 适配性能、计算资源等来进行筛选分析。物联网由于资源受限、网络环境复杂等因素，其应用层的通信协议很难做到既满足低功耗和运算能力的需求，又保证通信数据的安全。本章

对目前具有代表性的 4 种通信协议 HTTP、XMPP、CoAP、MQTT 做一个简单的介绍以及安全性分析。

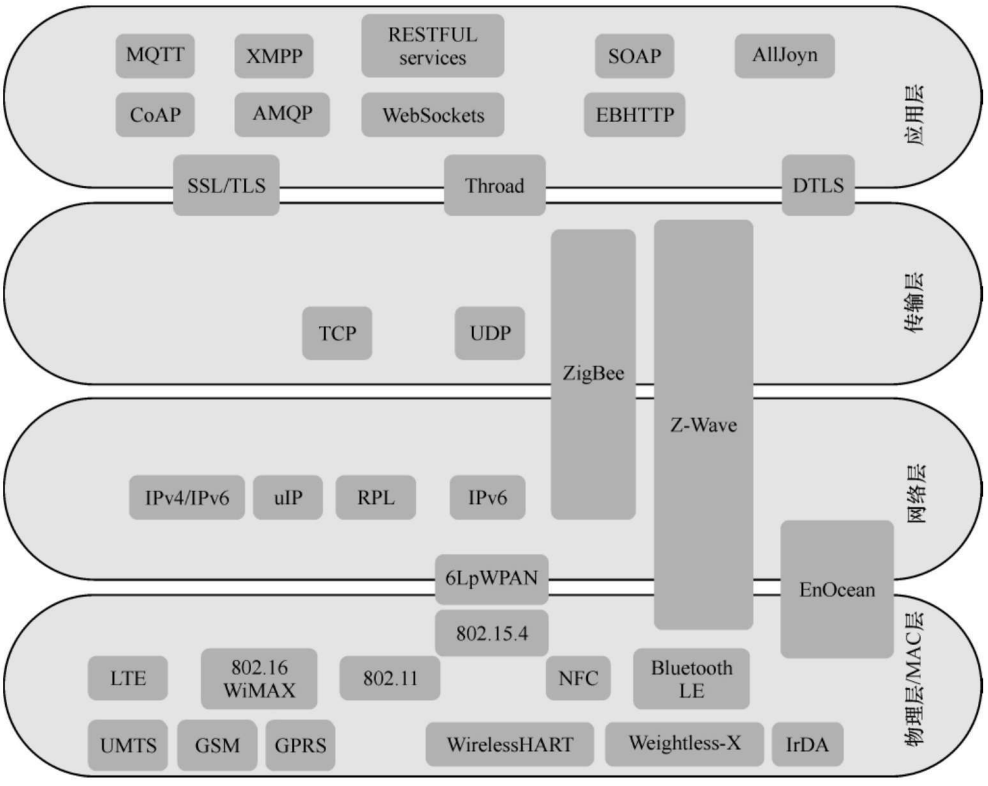

图 2.1　NB-IoT 物联网系统架构

2.1.2　物联网应用层协议比较

物联网应用层有各种不同的协议，每种协议的特点不同，底层所使用的传输协议也不同，表 2.1 总结了物联网所使用的四种不同的应用层协议。

表 2.1　物联网应用层协议比较

协议	HTTP	XMPP	CoAP	MQTT
传输协议	TCP	TCP	UDP	TCP
消息模式	请求/响应	发布/订阅 请求/响应	请求/响应	发布/订阅 请求/响应
2G,3G,4G 适配性能(千级节点)	优	优	优	优
LLN 适配性能(千级节点)	一般	一般	优	一般
计算资源	10 ks RAM/Flash	10 ks RAM/Flash	10 ks RAM/Flash	10 ks RAM/Flash

物联网由于资源受限、网络环境复杂等因素，其应用层的通信协议很难做到既满足低功耗和运算能力的需求，又保证通信数据的安全。本章首先介绍了物联网的架构和物联网的

通信协议框架，然后对具有代表性的应用层协议 HTTP、XMPP、CoAP、MQTT 等做了简要的协议介绍，最后对上述四种应用层协议进行了安全性分析。针对物联网环境下低功耗、低运算能力的需求，提出即满足正常运行的功能，又保证数据的安全的通信协议，是一个值的长期研究的课题。

2.2 HTTP 协议

2.2.1 HTTP 协议介绍

超文本传输协议(HyperText Transfer Protocol，HTTP)是典型的 C/S 通信模式，由客户端主动发起连接，向服务器请求 XML 或 JSON 数据。该协议最早是为了适用 Web 浏览器的上网浏览场景设计的，目前在 PC、手机、PAD 等终端上都广泛应用。现在物联网的通信架构也是构建在传统互联网基础架构之上的。HTTP 协议由于开发成本低、开放程度高，大部分物联网协议采用 HTTP 网络传输，所以很多厂商在构建物联网系统时也基于 HTTP 协议进行开发。

HTTP 的工作过程可分为四步，一次请求/响应的过程称为一个 HTTP 事务。

(1) 客户机与服务器需要建立连接，只要单击某个超级链接，HTTP 的工作开始。

(2) 建立连接后，客户机发送一个请求给服务器，请求方式的格式为：统一资源标识符(URL)、协议版本号，后边是 MIME 信息包括请求修饰符、客户机信息和可能的内容。

(3) 服务器接到请求后，给予相应的响应信息，其格式为：一个状态行，包括信息的协议版本号、一个成功或错误的代码，后边是 MIME 信息包括服务器信息、实体信息和可能的内容。

(4) 客户端接收服务器所返回的信息通过浏览器显示在用户的显示屏上，然后客户机与服务器断开连接。

2.2.2 HTTP 协议安全性分析

HTTP 协议应用在物联网场景存在三个缺陷。

(1) 由于必须由设备主动向服务器发送数据，难以主动向设备推送数据，所以只对简单的数据采集等场景勉强适用，而对于频繁的操控场景，只能通过设备定期主动拉取的方式来实现消息推送，实现成本和实时性都不佳。

(2) HTTP 采用明文传输，并且缺乏消息完整性的检验。研究人员使用网络嗅探的方式就可以轻易获取明文传输的信息，而 HTTP 只在数据包头进行了数据长度的检验，并未对数据内容做验证，研究人员可以轻易地发起中间人攻击。因此 HTTP 在很多安全性要求较高的物联网场景(如移动支付等)是不适用的。

(3) 不同于用户交互终端如 PC、手机，物联网场景中的设备多样化对于运算和存储资源都十分受限，HTTP 协议、XML/JSON 数据格式的解析都无法有效地实现。

针对难以主动向设备推送数据这个缺陷，提出了 WebSocket 的办法。WebSocket 是 HTML5 提出的基于 TCP 之上的可支持全双工通信的协议标准，其在设计上基本遵循 HT-

TP 的模型，对基于 HTTP 协议的物联网系统是一个很好的补充。

针对明文传输问题，可采用 HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer)协议，是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。即 HTTP 下加入 SSL 层，HTTPS 的安全基础是 SSL，因此加密的详细内容就需要 SSL。

2.3　XMPP 协议

2.3.1　XMPP 协议介绍

XMPP 是一种基于标准通用标记语言子集 XML 的协议，它继承了在 XML 环境中灵活的发展性。因此，基于 XMPP 的应用具有超强的可扩展性。经过扩展以后的 XMPP 可以通过发送扩展的信息来处理用户的需求，以及在 XMPP 的顶端建立如内容发布系统和基于地址的服务等应用程序。而且，XMPP 包含了针对服务器端的软件协议，使之能与另一个系统进行通话，这使得开发者更容易建立客户应用程序或给一个配好的系统添加功能。

XMPP 中定义了三个角色，客户端、服务器、网关，通信能够在这三者的任意两个之间双向发生。服务器同时承担了客户端信息记录、连接管理和信息的路由功能。网关承担着与异构即时通信系统的互联互通，异构系统包括 SMS(短信)、MSN、ICQ 等。基本的网络形式是单客户端通过 TCP/IP 连接到单服务器，然后在此之上传输 XML。

由于其开放性和易用性，在互联网及时通信应用中运用广泛。相对于 HTTP，XMPP 在通信的业务流程上更适合物联网系统，开发者不需要耗费过多精力去解决设备通信时的业务通信流程，相对开发成本更低。

2.3.2　XMPP 协议安全性分析

XMPP 虽然优化了通信业务的流程，降低了开发成本，但是在 HTTP 协议中的安全性以及计算资源消耗等问题并没有得到本质的解决。如果物联网智能设备需要保持长时间在线的会话并且要接收云端消息，可采用简单方便的 XMPP 协议。相应的 XMPP 协议存在的安全问题也将带入到该物联网环境中。

如图 2.2 所示，国内某厂商的物联网设备和第三方平台之间使用 XMPP 协议实现会话控制和长连接保持在线，用户通过手机发送指令到云端服务来控制相应的设备。在此场景下，研究人员通过网络嗅探的方式，可以轻易地获取设备与云平台通信明文的完整内容，利用支持 XMPP 协议的普通聊天软件即可模拟设备登录云平台。在搜集了大量的设备与云端通信内容后，可以获得完整的控制业务流程，控制指令集等重要的敏感信息，进一步修改设备 ID 编号即可控制其他在线的任意同款设备。

从示例可以看出，简单地使用 XMPP 协议具有重大的安全隐患，一旦研究人员完全控制设备并发送恶意指令，如空调温度设为 100 ℃、洗衣机高速空转等，都将可能威胁到用户的经济利益和人身安全。