本书由湖南商学院学术著作出版基金资助出版

面向物联网的数据完整性检测与隐私保护

◎ 李超良 著

Data Integrity Detection and Privacy Protection in Internet of Things

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

本书由湖南商学院学术著作出版基金资助出版

面向物联网的数据完整性检测与隐私保护

Data Integrity Detection and Privacy Protection in Internet of Things

◎ 李超良 著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

图书在版编目（CIP）数据

面向物联网的数据完整性检测与隐私保护 / 李超良著 . ——西安 : 西安交通大学出版社，2016.10

ISBN 978-7-5605-9129-2

Ⅰ. ①面… Ⅱ. ①李… Ⅲ. ①互联网络－应用②智能技术－应用③互联网络－隐私权－信息安全－安全技术－研究 Ⅳ. ①TP393.4②TP18③TP393.08

中国版本图书馆 CIP 数据核字（2016）第 265774 号

书　　名	面向物联网的数据完整性检测与隐私保护
著　　者	李超良
责任编辑	魏　杰　贺彦峰
出版发行	西安交通大学出版社 （西安市兴庆南路 10 号　邮政编码 710049）
网　　址	http://www.xjtupress.com
电　　话	（029）82668357　82667874（发行中心） （029）82668315（总编办）
传　　真	（029）82668280
印　　刷	长沙市宏发印刷有限公司
开　　本	880mm×1230mm　1/32　**印张** 4.75　**字数** 115 千字
版次印次	2016 年 10 月第 1 版　2016 年 10 月第 1 次印刷
书　　号	978-7-5605-9129-2/TP · 742
定　　价	58.00 元

读者购书、书店添货、如发现印装质量问题，请与本社发行中心联系、调换。

前　言

物联网是继互联网和移动通信网络之后的世界信息产业发展的第三次浪潮，它是一种物物相连的网络，具有节点计算能力有限、存储空间较小、网络连接不稳定等特点。由于物联网具有广泛的适用空间，其研究与应用近年来受到了国内外政府、学术界和企业界的高度重视。物联网的标签及读写器具有非视距识别的特点，可以利用附着在货物上的标签实现仓储货物高效管理；此外，物联网数据具有信息高敏感性、数据高联系性的特点，因而也必须加强物联网隐私保护研究。

本专著主要关注物联网环境下数据完整性检测及隐私保护问题，研究仓储货物的静态完整性检测、动态完整性检测及隐私保护。具体来说，主要有以下研究成果：

(1)提出了一种基于中国剩余定理、适合于检测仓储系统中批量货物数量完整性的检测协议 CIDA。该检测协议只需要访问一次数据库，时间复杂度为 $O(n)$，就能够实现批量货物数量的快速完整性检测；同时，该协议在检测过程中，能够隐藏货物的真实

信息,较好地保护用户隐私。

(2)研究了当前仓储管理这一物联网应用的特殊状况,针对仓储环境下需要对远程数据进行有效管理的需求提出了一种能进行动态完整性检测的 DRDA 算法。该算法以双线性对为基础,以 MHT 为存储结构,只需要用户及服务器两个实体,不需要第三方参与,就能够实现数据的分布式、动态完整性检测。检测相同大小的数据包时,DRDA 算法所需要的开销比典型的检测算法 DPDP 平均要小 40kB,检测性能较好。

(3)提出了一种 RFID 系统中能检测数据包在通过非安全的通道传输后是否遭受篡改等攻击的数据包完整性检测算法 FBDA。在 RFID 系统中,标签和读写器之间的传输通道通常被认为是不安全的,两者之间传递的数据包可能会遭受攻击。本书采用聚集签名方法实现了一种能够隐藏标签信息、保护物品及其所有者隐私的检测算法 FBDA。在读写器端,FBDA 只需要进行一次比对,就能检测大量数据包在通过不安全的通道时是否遭受了攻击。理论分析和模拟实验表明,与现有的一些解决方法如 DPLK、CC 相比,FBDA 算法在标签端只需要两次哈希运算,性能较好。

(4)将基于同态加密的安全双方隐式比较引入物联网路由数据隐私保护研究中,提出了一种新型的基于同态加密的物联网数据包路由隐私保护方案 PPHE。该方案能保证节点收集的数据信息在最短时间内发送给目标节点。在节点对之间进行相遇概率的比较时,加入冗余数据,构建新的相遇概率集合,隐藏节点之间真实的相遇情况。在选择路由路径时,选择相遇概率较大的节点进行数据传送,从而既实现了数据包的快速传输,也保护了相关

节点的隐私。与同类方案相比,该方案需要的计算时间减少了约1/4。

本专著可作为计算机应用技术、信号与信息处理、模式识别与智能控制等专业高年级本科生、研究生的参考书,也可供从事相关专业研究工作的科研人员参考。

目 录

第1章 绪 论

本章首先对物联网应用系统进行简要描述，然后重点阐述物联网环境下数据完整性检测与隐私保护的概念、技术和特殊要求，简要介绍该领域的研究现状，进而指出本书的主要工作。

1.1 研究背景

1.1.1 物联网发展

物联网的概念最先是比尔·盖茨于1995年在《未来之路》一书中提及的，后来，物联网作为一个专有名词由麻省理工学院自动识别实验室于1999年正式提出，并将其定义为：通过射频识别（Radio Frequency Identification，RFID）和条码等信息传感设备把所有物体与互联网连接起来，实现智能识别和管理功能的网络。互联网实现了人与人（Human to Human，H2H）、人与计算机（Human to Computer，H2C）以及计算机与计算机（Computer to Computer，C2C）的相互连接，而物联网则将互联网的应用进一步扩展和延

伸到物物（Thing to Thing，T2T）之间的信息交换和信息处理。2005 年 11 月 17 日，在突尼斯举行的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布了《ITU 互联网报告 2005：物联网》，正式将物联网称为 Internet of Things，IoT，对物联网概念进行了扩展，提出了采用 RFID 技术、传感器技术、纳米技术、智能终端技术，在任何时刻、任何地点、任何物体之间的相互连接，实现无所不在的网络和无所不在计算。欧盟第七框架下 RFID 和物联网研究项目簇（Cluster of European Research Projects on the Internet of Things：CERP－IoT）于 2009 年 9 月发布的《物联网战略研究路线图》研究报告中提出，物联网是未来互联网的一个重要组成部分，并且将物联网定义为具有动态的基于标准的和可互操作的通信协议且能实现自动配置的全球化网络基础架构。在其定义中，物联网中的“物”都具有自身的标识、物理属性和实质上的个性，使用智能接口，能够实现与互联网的无缝整合。在 2010 年 3 月的政府工作报告中，我国对物联网做了如下的定义：物联网是指通过各种信息传感设备，按照既定的协议，把任何物品与互联网连接起来，进行信息交换和通信，实现智能化识别、定位、跟踪、监控和管理的一种网络，是现有互联网的延伸和扩展。

物联网被认为是继计算机互联网、移动通信网之后的第三次信息产业浪潮。自从物联网概念被提出以来，就受到了世界各国政府、学术界、相关企业的极大关注。在 2012 年第三届中国国际物联网博览会上，航天信息集团董事长于滨曾明确表示，全球物联网市场规模将持续保持 25% 左右的年增长率，到 2015 年将达到 3 500 亿美元的市场规模。美国市场预测研究公司 Forrester 宣称，到 2020 年，世界上“物物互连”的业务，跟人与人通信的业务的比例，将达到 30∶1，仅在机场防入侵系统、电网智能检测等方面的

市场规模就将达到千亿美元。物联网被称为下一个万亿美元级的信息技术产业。因此，世界各主要发达国家和地区以及大跨图公司均十分重视物联网的研究与应用。韩国于2002年4月提出e-Korea（电子韩国）战略；新加坡于2006年提出“智慧国2015”大蓝图；欧盟于2009年6月启动了“物联网行动计划”；IBM公司早在2008年年底就向美国政府提出“智慧地球”战略。中国在物联网研究方面起步较早，研发水平处于世界前列。为支持物联网的深入研究，促进物联网的发展，各级政府和部门相继提出了多种规划，《国家中长期科学与技术发展规划（2006-2020）》和“新一代宽带移动无线通信网”国家科技重大专项中均将传感网列入重点研究领域。2011年工信部制定了《物联网“十二五”发展规划》，重点培养物联网产业100家骨干企业和10个聚集区，实现物联网产业链上下游企业的汇集和产业资源整合。2013年2月，国务院发布了《国务院关于推进物联网有序健康发展的指导意见》，对发展物联网的指导思想、基本原则、发展目标进行了明确规定，并提出了包括“加快技术研发，突破产业瓶颈”“推动应用示范、促进经济发展”等在内的主要任务。2014年2月，全国物联网工作会议在北京召开，提出要突破物联网核心芯片、软件等基础共性技术，加快研发智能传感器、大数据处理、行业应用软件等关键技术，积极推进我国物联网标准国际化工作，提升我国标准的影响力和竞争力。

1.1.2 物联网体系结构

物联网的巨大价值在于物体具有“智慧”，能够实现人与物、物与物之间的沟通，是感知、互联、智能三者的结合。物联网通常可表示成由三个部分组成，即感知层、网络层、应用层，如图1-1所示。感知层即感知部分，主要用于感知对象的各种属性，

如温度、湿度、压力等指标，以二维码、RFID、传感器为主要实现技术。 网络层即传输部分，是对“物体”的识别、传输网络，可以通过现有的各种通信网络如互联网、广电网络等进行数据传输。应用层即智能处理部分，主要采用神经网络、人工智能、数据挖掘、云计算等技术实现对物品的自动控制与智能管理等。

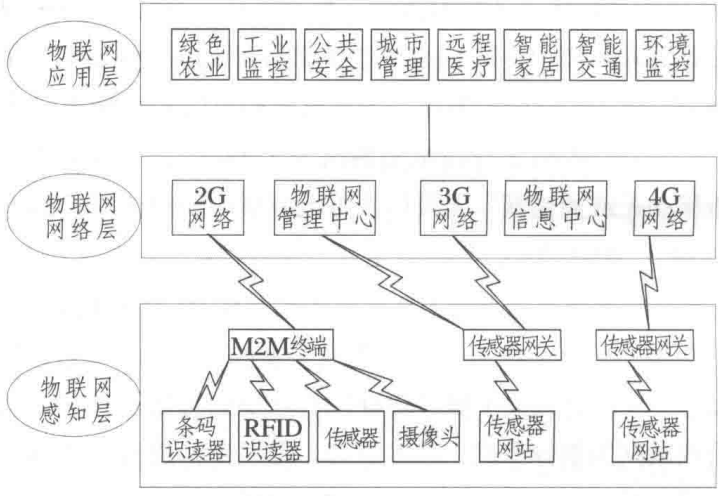

图 1-1 物联网结构图

1.1.3 基于物联网的典型应用

1. 智能家居

物联网是物物相连的网络，可以通过多种智能感知设备按照约定的协议，把任何物品与互联网联系起来，进行信息交换、通信，以实现物品的智能化识别、跟踪、定位、管理、监控。 由于物联网适用的范围非常广泛，因而在包括仓储管理、环境监测、智能城市、智能电网、智能交通等的许多方面都将有广泛的应用。

物联网的应用实例如通过对门禁、温度、湿度、灯光、烟雾等信息的收集、监测，实现对家居环境的智能化管理。 图 1-2 是一

个典型的智能家居环境监控系统图。该系统主要由感知层、网络层、应用层构成。感知层主要获取家居环境中的各种原始信息，通过各种有线或无线的方式传输给智能控制终端。终端再通过移动通信系统将信息发送给用户。用户可以向智能控制终端发送指令以实现对相关对象的远程操作。由于移动通信网络在我国覆盖面广、系统稳定、使用人数众多，因而使用该智能家居环境监控系统实现对家居环境的自动监测，对于提高人们的生活水平具有重要的社会意义，同时也必将带动其上下游产业及相关配套产品的发展，产生巨大的经济效益。

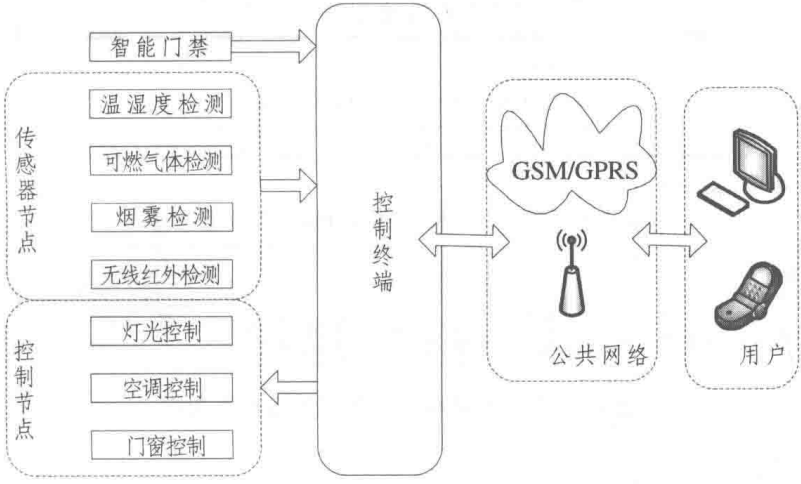

图 1-2 智能家居环境监控系统图

2. 智能电网

我国拥有世界上最大最复杂的电网，如何保证电网安全运行、输变电设备完好，实现电力流、信息流、业务流的高度统一，是目前面临的难题。在解决此类问题上，物联网具有独特的优势。图1-3是一个典型的面向智能电网的物联网应用框架图。系统分为三层：感知层主要感知输电、变电、配电、用电各模块的基础信

息，然后通过光纤或宽带无线接入方式连接数据库，再结合云计算技术，实现海量数据的实时处理，保障电网安全运行。

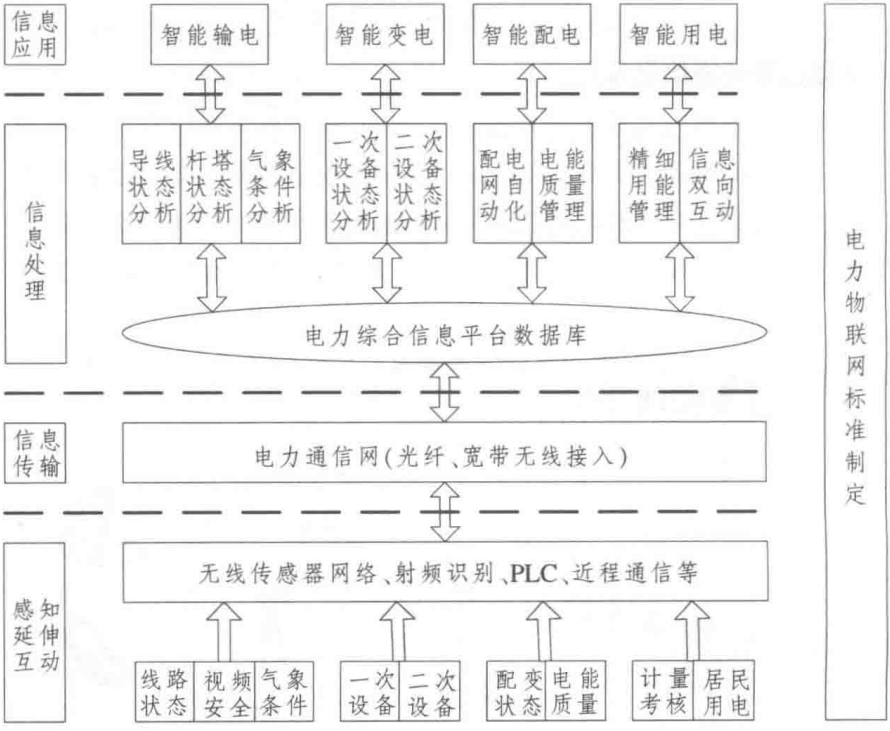

图 1-3 面向智能电网的物联网应用框架图

3. 智能仓储

仓储管理系统是现代物流的主要组成部分，能对流通中的货物进行检测、保管、加工、集散、转换运输方式等处理，是解决现代仓储物品管理问题的一种重要手段。它能够加速货品流转，提高物流效率和质量，提升仓储管理系统水平。在仓储管理中，通过RFID技术，识别附着在物品上的标签（tag），可以实现物联网标签的自动统计，完成货物入库、出库统计，仓储货物数量统计、查找等功能。因此，物联网技术能给我国的仓储行业提供极大的技