RFID 安全协议分析与设计

原变青 ◎ 著

科学技术文献出版社
SCIENTIFIC AND TECHNICAL DOCUMENTATION PRESS

北京经济管理职业学院资助出版

RFID安全协议分析与设计

原变青 著

科学技术文献出版社
SCIENTIFIC AND TECHNICAL DOCUMENTATION PRESS
·北京·

图书在版编目（CIP）数据

RFID安全协议分析与设计 / 原变青著. —北京：科学技术文献出版社，2018.8
ISBN 978-7-5189-4730-0

Ⅰ.①R… Ⅱ.①原… Ⅲ.①无线电信号—射频—信号识别—安全技术
Ⅳ.①TN911.23

中国版本图书馆 CIP 数据核字（2018）第 179396 号

RFID安全协议分析与设计

策划编辑：周国臻　　责任编辑：王瑞瑞　　责任校对：张吲哚　　责任出版：张志平

出 版 者　科学技术文献出版社
地　　址　北京市复兴路15号　邮编 100038
编 务 部　(010) 58882938，58882087（传真）
发 行 部　(010) 58882868，58882870（传真）
邮 购 部　(010) 58882873
官方网址　www.stdp.com.cn
发 行 者　科学技术文献出版社发行　全国各地新华书店经销
印 刷 者　北京虎彩文化传播有限公司
版　　次　2018 年 8 月第 1 版　2018 年 8 月第 1 次印刷
开　　本　710×1000　1/16
字　　数　151千
印　　张　10.25
书　　号　ISBN 978-7-5189-4730-0
定　　价　48.00元

前　言

RFID技术是一种自动识别和数据获取技术。只需将RFID标签附着或嵌入到目标实体，无须直接接触，RFID读写器即可识别该目标实体。随着世界各国对物联网产业的不断重视，作为物联网感知层的关键技术，RFID无论是在技术水平还是在应用规模方面都有了长足的发展。目前，RFID系统已经在产品管理、交通支付、物流管理及票证管理等多个领域形成了一定规模的应用。

由于RFID标签的存储资源和计算能力有限，而且RFID标签和读写器往往工作在开放的无线通信环境下，因此，RFID系统在通信过程中容易遭受窃听攻击、重放攻击、隐私攻击等各种安全威胁。设计并应用高效、安全的RFID协议是实现RFID系统安全的重要保障。

本书首先对物联网和RFID系统分别做了概述，指出了RFID系统存在的安全性问题及主要解决办法；然后介绍了进行RFID安全协议分析与设计所需要的基础知识；最后分别对RFID认证协议、RFID标签组证明协议、RFID标签所有权转移协议及基于云的RFID协议的研究现状进行了总结，详细描述了各类协议的交互模型和安全模型，在对典型协议进行分析的基础上，设计了相关安全协议。

本书的主要创新点如下。

①组证明协议的功能是生成两个或两个以上的标签被一个读写器同时扫描的证据。安全性和效率是设计组证明协议时需要考虑的重点问题。本书在分析组证明协议安全模型的基础上，提出了一个新的读取顺序无关的离线组证明协议，即收到读写器的广播消息后，组内标签可以同时进行计算，具有较高的效率。此外，在标签端使用伪随机数生成器作为生成部分组证明的主要计算方式，使得协议适用于低成本标签的应用场景。随后，对一个典型的标签顺序读取组证明协议进行了安全性分析，发现该协议易遭受异步攻击和主动攻击。本书提出了针对该协议的改进方案，新方案在不降低原协议性能的基础上，安全性有了较大的提高。

②随着物品所有权的转移，其上附着的 RFID 标签的所有权也需要发生转移。安全和隐私问题是标签所有权转移过程中需要研究的重点问题。本书提出了一个新的轻量级单标签所有权转移协议。在 UC（通用可组合）框架下，定义了单标签所有权转移的理想函数，并证明了新协议安全地实现了所定义的理想函数，即新协议满足双向认证、标签匿名性、抗异步攻击、后向隐私保护和前向隐私保护等安全属性。与已有的单标签所有权转移协议相比，新协议中 RFID 标签的计算复杂度和存储空间需求都较低，并且与新旧所有者的交互次数较少，能够更加高效地实现低成本标签的所有权转移。

③在某些应用中，往往需要在一次会话中同时完成一组 RFID 标签所有权的转移。然而，现有的标签组转移方案大多需要可信第三方的支持，并且需要与单独的组证明协议组

合，才能实现标签组所有权转移的功能。本书设计了一个安全高效的标签组转移协议，协议在无可信第三方支持的情况下实现了一组标签所有权的同时转移。然后定义了 RFID 标签组转移的理想函数，并在 UC 框架下证明了新协议的安全性。

④随着 RFID 标签应用规模的不断增长，传统的 RFID 系统由于其有限的计算能力和低效的大规模数据管理模式，已经越来越无法满足 RFID 系统的实际应用需求。为此，学者们提出了基于云的 RFID 体系架构。本书首先分析了云计算环境下 RFID 标签所有权转移的安全和隐私需求，提出了一个基于云的无须可信第三方支持的标签所有权转移协议。新协议将标签信息存储在半可信的云服务器上，并通过在云服务器端采用代理重加密机制来创建标签的新所有权关系。随后，定义了基于云的标签所有权转移理想函数，并在 UC 框架下证明了新协议实现了该理想函数。与传统的标签所有权转移方案相比，新方案在部署成本和可扩展性方面都有较大的优势。

在本书创作过程中，笔者大量参阅了本领域国内外专家学者的论著和科研成果，也得到了很多同行及专家的指导。本书的出版得到了北京经济管理职业学院的资助。在此，一并表示衷心的感谢！由于笔者能力与精力有限，书中难免存在不妥之处，敬请各位读者与专家批评指正。

目　录

1 绪 论

1.1 物联网简介

物联网（Internet of Things，IoT）这个概念最早是由美国麻省理工学院的 Ashton 教授于 1999 年提出的，是指在互联网基础上，依托射频识别（Radio Frequency Identification，RFID）技术，实现物品信息的智能化识别和管理，从而构造一个物品信息共享的实物网络。2005 年，国际电信联盟发布的《ITU 互联网报告 2005：物联网》丰富了物联网的内涵，将物联网感知层技术拓展到了传感网络技术、嵌入式智能技术及微缩纳米技术等领域。如今，物联网是指利用各种感知技术和设备全面获取物理世界的各种信息，通过网络互联完成物与物、人与物的信息交互，从而在现有互联网的基础上构建一个覆盖世界上所有人与物的网络信息系统，以实现对物体的智能化识别、定位、跟踪、管理和控制[1]。

1.1.1 物联网体系结构

从本质上看，物联网是指在现有各种网络基础上，将现实中的所有物体进行连接，以达到控制和管理物体的目的。因此，物联网通常被划分为 3 个层次：感知层、网络层和应用层[2-3]。

（1）感知层

感知层处于物联网的底层，主要解决识别物体、获取物体信息的问题。感知过程分为两部分，首先是通过 RFID 标签和读写器、二维码读写器、传感器、摄像头等感知设备完成数据采集，然后通

过短距离传输网络将采集的信息传送给相应的控制部件。这一层涉及了 RFID、传感器、ZigBee、蓝牙等技术。

（2）网络层

网络层位于感知层和应用层的中间，它基于现有的互联网，融合移动通信网和广播电视网，将从感知层获得的信息正确且快速地传送给上层用户，同时也将用户的指令传送给相应的感知设备。本层主要涉及了 IPv6、2G/3G/4G、Wi-Fi 等远距离有线或无线通信技术。

（3）应用层

应用层处于物联网的最上层，主要是对信息感知层传送的数据进行分析和处理，获得正确的控制和决策信息，以实现既定的智能化应用。这一层涉及了海量数据存储、数据挖掘和人工智能等技术。

此外，由于物联网涉及大量的应用，物联网的管理在物联网中也有举足轻重的作用。公共技术部分负责完成物联网的标识与解析、网络管理、安全管理和服务质量管理。

1.1.2 物联网发展现状

随着物联网技术与其他信息技术的不断融合渗透，物联网技术已由孤立化应用演变为“重点聚焦、跨界融合”的新模式[4]。近年来，世界各国也投入了大量的人力和物力用于物联网技术的研发与应用。

2015 年，美国宣布了以物联网应用试验平台建设为主的智慧城市计划，该计划预计投入 1.6 亿美元。在工业制造领域，美国政府推出了以物联网技术为基础的网络物理系统，还将其作为重点支持项目以重塑美国在工业制造领域的优势。同年，欧盟投入 5000 万欧元成立了物联网创新联盟，该联盟提出了“四横七纵”的体系架构，该架构包括项目设置、价值链重塑、政策导向和标准化四大横向基础支撑，以及家居、智慧城市、农业、交通、可穿戴、环

保和制造七大行业纵深领域。以日韩为首的亚洲发达国家也在不断加大对物联网技术研发的投入。日本提出大力普及农用机器人的农业物联网计划，到2020年该计划的规模预计将达到50亿日元。2015年起，韩国计划投资370亿韩元用于研发物联网核心技术、MEMS传感器芯片及宽带传感设备。新加坡政府则通过制定传感器网络及特定领域产品的标准，为创建统一的物联网体系结构打下良好的基础。

自从2009年提出“感知中国”这个概念以来，物联网已经成了我国的新兴战略性产业。2012年8月，为推进物联网有序健康发展，我国建立了由发展改革委、工业和信息化部等10多个部门共同参与的物联网发展部际联席会议制度，并于2013年9月印发了有关物联网的顶层设计、标准制定、技术研发、应用推广、产业支撑、商业模式、安全保障、政府扶持措施、法律法规保障、人才培养10个专项行动计划。近年来，物联网技术更是进入了高速发展的快车道。据统计，2015年我国物联网产业的市场规模达到了7500亿元，2017年已破万亿元。预计到2020年，中国物联网的整体规模将超过1.8万亿元。目前，我国已初步形成环渤海、泛珠三角、长三角及中西部地区四大区域集聚发展的物联网空间格局，并拥有多个国家级物联网产业发展示范基地，具备了包括芯片和元器件、设备、软件、系统集成、电信运营、物联网服务等在内的物联网产业链。

1.1.3 物联网的安全需求

随着物联网的蓬勃发展，引入物联网设备的种类越来越多，各类设备的性能和功能也千差万别。这些设备的引入，特别是大量具有移动性的智能设备的引入带来了许多新的安全和隐私问题，主要是安全认证问题和隐私泄露问题[5]。

首先，物联网中会引入大量的传感器或者贴有RFID标签的物品，在部署或者使用这些设备时必然会带来认证的问题。虽然传统

网络中有很多成熟的认证协议，但由于这些认证协议大多都是基于计算能力较强的台式机等终端设计的，因此，无法将这些认证协议直接应用到低成本的、计算能力有限的标签或者智能终端设备上。

其次，由于大多数的物联网应用都是采用无线通信的方式进行连接的，故敌手可以通过窃听无线信号的方式来获取各个节点所发送的信息。特别是随着智能手机的大规模普及，人们在日常生活中会经常性地使用自己的智能手机来获取相关的应用和服务，在获取这些应用或者服务的过程中，用户或多或少地需要提供自己的身份信息、地理位置信息等用户敏感的隐私信息，这就造成了用户隐私泄露的风险。例如，有的用户喜欢将自己的旅游、社交等活动发布在自己的微博上，而发布的这些信息中可能含有很多不该被陌生人知道的信息，如用户的家庭住址、工作单位、车牌号等个人隐私信息。如果这些信息被不法分子获取，将会造成很多不必要的损失。

因此，物联网的诞生，给人们的生活和生产带来便利的同时，对系统的安全和隐私保护都提出了更高的要求。解决好安全和隐私保护问题将是物联网技术能否被社会所接受乃至被广泛应用的关键。由于物联网的体系框架还处在不断演进的过程中，所以对于物联网安全和隐私保护的研究也处在不断的演进过程中。当前，大多数关于物联网安全与隐私方面的研究都是基于物联网在不同领域的不同应用场景进行的有针对性的研究。

1.2 RFID 概述

随着贸易市场和交通运输业的发展，物品识别变得越来越重要。第一个物品自动识别技术是条形码技术，该技术至今仍然被广泛使用。然而，使用条形码识别物品存在如下问题：需要将扫描仪近距离对准条形码，而且一次只能扫描一个物品等。RFID 技术的出现正好解决了上述问题。

RFID 是一种自动识别和数据获取技术。通过将 RFID 标签附

着到特定目标实体，如产品、动物和人等，读写器无须直接接触目标实体即可实现对特定目标实体的识别和数据的搜集。通过使用无线电波识别或跟踪附着在物品上的电子标签，RFID 技术完全可以替代条形码来识别物品。此外，RFID 标签还具有成本低、读取距离大、耐磨损、数据可加密与修改等优点。目前，RFID 系统已被部署到不同的应用场景，如自动付款、资产跟踪、供应链和库存管理等领域，成为物联网感知层最为关键和应用最广的技术。

1.2.1 RFID 系统组成

一个典型的 RFID 系统通常由 3 类实体构成：标签、读写器和后台服务器。图 1-1 为 RFID 系统示意。

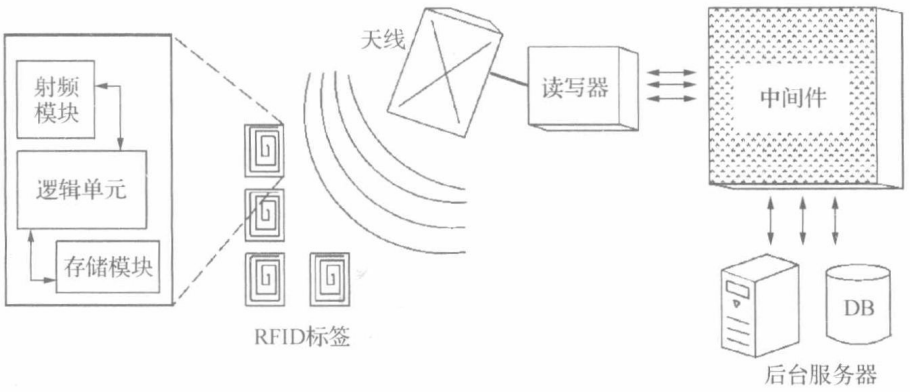

图 1-1 RFID 系统示意

1.2.1.1 标签

标签通常附着在物体上以标识目标对象。它由具有一定计算和存储能力的耦合元件及芯片组成。此外，标签内还包含用于通信的天线。

一般地，根据能量来源不同，可将标签分为被动标签、半被动标签和主动标签[6]。被动标签内部没有电源，它通过接收读写器的电磁波信号驱动其内部电路，从而向读写器回传信号。因此，被

动标签成本较低且体积较小，在市场上有广泛的应用。与被动标签不同，半被动标签提供内部电源。当收到读写器的询问信号时，半被动标签可以使用内部电源驱动标签工作，具有更高的效率。主动标签内含有电池来支持其通信，它可以主动触发通信并具有 100 m 以上的读取距离，但其成本相对较高。

根据工作频率不同，可将标签分为低频标签、高频标签、超高频标签和微波标签[3]。低频标签的工作频率范围为 30 ~ 300 kHz，典型的工作频率有 125 kHz 和 133 kHz。此类标签一般为无源标签，其阅读距离通常小于 1 m。主要适合廉价、省电、近距离、低速及数据量少的识别应用，如动物识别、自动化生产等。高频标签的工作频率范围为 3 ~ 30 MHz，典型的工作频率为 13.56 MHz。此类标签的工作方式与低频标签类似，但其传输速度有所提高。典型应用有无线 IC 卡、电子身份证、电子车票等。超高频标签的工作频率范围为 850 ~ 910 MHz。微波标签的工作频率为 2.54 GHz。这两种标签存储数据量大、阅读距离远且具有较高的阅读速度。目前，低频和高频标签技术已经在物联网中得到了广泛的应用。由于具有低成本及可远距离识别等优势，超高频标签技术将成为未来应用的主流。

1.2.1.2 读写器

RFID 读写器通常由射频模块、控制单元和耦合单元组成，一般有较好的内部存储和处理能力，复杂的计算（如各种密码操作）也可以在读写器中执行。读写器可通过有线或无线的方式和后台服务器相连，通过天线与标签进行无线通信以实现对标签的识别和读写。

1.2.1.3 后台服务器

由于标签在数据存储和处理上的局限性，使得标签内存储的信息非常有限，因此关于物品的业务信息（如生产日期、型号、详

细描述等）通常存储在后台服务器。后台服务器一般具有较强的处理能力，它通过数据库管理其所拥有的读写器和标签的信息。一般地，由于读写器和后台服务器的数据处理和存储能力都比较强，它们之间可以使用各种密码技术或通信协议，因此通常假设读写器和后台服务器之间的通信信道是安全的。

1.2.2 RFID 系统通信模型

RFID 系统通信模型由 3 层组成，从下到上依次为：物理层、通信层和应用层[7]，如图 1-2 所示。物理层主要处理频道分配、物理载波等电气信号问题；通信层定义了读写器与标签之间双向交换数据和指令的方式，主要解决多个标签同时访问一个读写器时产生冲突的问题；应用层主要解决与上层应用相关的内容，包括认证、识别及应用层数据的表示、处理逻辑等。一般我们所说的 RFID 安全协议指的就是应用层协议。

图 1-2 RFID 系统通信模型

1.2.3 RFID 系统安全

由于 RFID 标签的存储资源及计算能力有限，因此复杂的密码运算往往无法在标签端使用。此外，由于读写器通过开放的无线通信环境与 RFID 标签进行交互，使得其通信容易受到窃听、篡改、重放等恶意攻击，也极易导致标签所有者的身份、位置等隐私信息遭到泄露[1]。例如，在超市，粘贴在一个昂贵商品上的电子标签可能被改写为一个便宜的商品的信息；在企业，竞争对手可以在库