RFID 数据管理:算法、协议与性能评测

谢 磊 殷亚凤 陈 曦 陆桑璐 陈道蓄

(南京大学计算机软件新技术国家重点实验室 南京 210093)

摘 要 随着物联网关键理论及技术的发展,RFID 作为物联网的核心支撑技术,成为物联网领域备受关注的研究热点之一.文中以 RFID 的数据管理为切入点,从算法、协议以及性能评测 3 个层面对 RFID 的研究工作进行阐述与分析,着重介绍了 RFID 的防冲突算法、认证与隐私保护协议以及真实环境下系统的性能评测与分析等方面的研究成果及进展.最后展望了未来的研究方向.

关键词 射频识别;数据管理;防冲突算法;认证与隐私保护;性能优化;物联网

中图法分类号 TP393 **DOI 号** 10.3724/SP.J.1016.2013.00457

RFID Data Management: Algorithms, Protocols and Performance Evaluation

XIE Lei YIN Ya-Feng CHEN Xi LU Sang-Lu CHEN Dao-Xu

(*State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing* 210093)

Abstract With the development of critical theories and technologies in Internet of Things (IOT), as a key supporting technology, RFID has become one of the hotspots in the field of Internet of Things. Focusing on RFID data management, this paper describes and analyzes the research work on three aspects: algorithm, protocol and performance evaluation. In this paper, we introduce the research progress in RFID with anti-collision algorithm, authentication and privacy protection protocols, as well as performance evaluation of RFID systems in realistic settings. Finally, we outlook the future research directions and conclude.

Keywords RFID; data management; anti-collision algorithm; authentication and privacy protection; performance optimization; Internet of Things

1 引 言

随着“物联网”时代的来临,新一代 IT 技术将被充分运用在各行各业之中.射频识别(RFID)作为物联网应用的一项核心支撑技术,在学术界与工业界已经得到广泛关注.目前,RFID 技术正在越来越频繁地出现在大量的物联网应用中,包括物流管理、电子支付、RFID 护照、安全访问控制、目标监测与追踪等.随着 RFID 的技术原理被进一步深入理解、廉价的 RFID 组件相继出现以及 RFID 的安全得到保障,RFID 技术将会在物联网应用中发挥越来越重要的作用.

物联网的核心理念是在普适环境下实现“物-物相联”,即通过对物理世界信息化、网络化,将传统上分离的物理世界与信息世界实现互联与整合.这就需要将“智能”嵌入到每一个物理对象当中,并且提供一种有效的、低成本的通信方式,RFID 技术的出现

收稿日期:2012-02-08;最终修改稿收到日期:2012-05-27.本课题得到国家“九七三”重点基础研究发展规划项目基金(2009CB320705)、国家自然科学基金(61100196,61073028,61021062)以及江苏省自然科学基金(BK2011559)资助.**谢 磊**,男,1982 年生,博士,讲师,中国计算机学会(CCF)会员,主要研究方向为传感器网络、RFID 系统、车联网、高性能计算.E-mail:lxie@nju.edu.cn.**殷亚凤**,女,1989 年生,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为 RFID.**陈 曦**,男,1988 年生,硕士研究生,中国计算机学会(CCF)学生会员,主要研究方向为 RFID.**陆桑璐**,女,1970 年生,博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为普适计算、分布式计算、传感器网络.**陈道蓄**,男,1947 年生,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为普适计算、分布式计算、计算机网络.

正好满足了这一需求. RFID 是一种非接触式的自动识别技术,它通过射频信号自动识别目标对象并获取相关数据,识别工作无须人工干预. 作为一种简单的无线系统,RFID 系统只有两个基本器件,一个是阅读器,另一个是标签. 其基本工作原理是:阅读器以广播方式连续向周围发送携带能量的基准信号,感应到能量的标签通过调制电路信号以反射的方式向阅读器返回自身携带的数据,阅读器对接收到的数据进行解码,并传给主机进行处理. 通过上述方式,RFID 系统能够提供有效的身份信息(Identity)和地址信息(Location). 相比于其它智能系统,RFID 系统具有如下鲜明特点:(1)能够实现非接触式的快速自动识别;(2)标签内能够永久存储一定大小的数据;(3)标签内含一定数目的逻辑门能够进行简单的逻辑处理;(4)标签具有普通无线设备的物理属性;(5)标签成本低廉,可以大量部署. 因此,作为物联网感知识别层面的一项关键技术,RFID 技术能够使得物联网中的每一个物体被唯一地识别,并且能够携带规范而具有互用性的信息,在无源的情况下有效实现"被动智能",为"物-物相联"提供根本保障.

在物联网环境下,RFID 系统被部署和应用的根本目的是:针对具体的应用需求,对被标识的物理对象进行合理有效的信息收集,为上层应用提供最基本的数据支持. 因此,任何一种具体的 RFID 应用都依赖于对 RFID 数据实现有效的数据管理. 所谓数据管理是指结合 RFID 系统的应用需求实现有效且有针对性的数据收集、分析挖掘以及数据安全保障等操作. 在现有的物联网体系架构中,数据管理起着承上启下的关键作用:一方面,物联网需要从感知到的海量原始数据中提取有效信息并进行管理,为上层的特定应用提供数据支撑;另一方面,物联网需要结合具体的数据管理需求来组织感知识别层面的众多节点,在网络层面进行优化调度与资源配置,以更有效地指导下层协议与算法的设计实现.

基于上述认识,本文关注 RFID 数据管理问题,以数据管理的核心技术为切入点,分别从 RFID 的防冲突算法、RFID 的认证与隐私保护协议以及真实环境下 RFID 系统数据收集的性能评测与分析 3 个方面对 RFID 数据管理技术的研究与进展进行分析与讨论. 图 1 展示了上述 3 个方面研究问题之间的逻辑层次关系. 其中,研究防冲突算法的目的是为 MAC 层提供一套快速的标签识别机制,实现 RFID 数据管理的高效性;研究安全协议的目的是为数据管理提供基本的安全保障,能够有效地实现认证并且保护用户隐私,实现 RFID 数据管理的可信性;对 RFID 系统进行性能评测与分析,其目的在于验证在真实环境下物理层的关键因素对系统识别性能的影响,确保数据管理的可靠性. 深入探究三者之间的联系,我们发现任一研究问题均对其余二者产生影响:防冲突算法能够提供最根本的数据传输支持,安全协议能够实现必要的安全保障,性能评测能够验证在真实环境下的系统运行性能. 上述三方面研究问题与 RFID 系统协议栈的对应关系如图 1 所示,可以看到三者之间相互联系,又各有侧重.

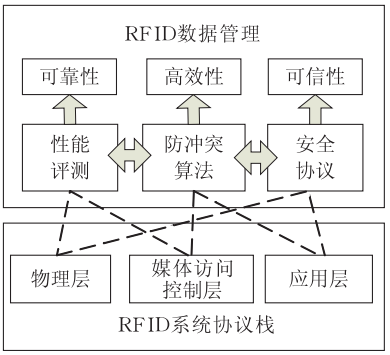

图 1 各研究问题之间的逻辑层次关系

本文第 2 节主要介绍 RFID 的标签识别协议与防冲突算法,着重阐述 RFID 标签识别机制、数目估算机制以及轮询机制方面的研究工作;第 3 节主要介绍 RFID 的认证与隐私保护协议,对 RFID 的安全与隐私问题进行探讨与分析,并对 RFID 安全方面的三类主流技术进行总结;第 4 节对真实环境下 RFID 系统性能的评测与分析方面的研究工作进行介绍;第 5 节对 RFID 数据管理相关的其它开放性问题的研究进展进行总结;第 6 节展望 RFID 未来的研究方向;最后对全文进行总结.

2 RFID 标签识别协议与防冲突算法

2.1 RFID 的标签识别协议

在通常的 RFID 应用中,大量的 RFID 标签往往被广泛地部署在指定区域中. 为了能够快速有效地识别这些标签,阅读器需要在 RFID 标签识别协议中使用一套有效的防冲突算法来逐一读取这些标签. 在无线通信环境下,普通的无线设备主要基于载波侦听多路访问/冲突避免(CSMA/CA)的竞争机制来实现多个设备之间的通信,如 802.11 协议. 与普通的无线节点不同,RFID 标签是极为简单的无线设备,标签上的资源极其有限,不能够自发地通过

调节自身的无线传输机会来避免标签间的传输冲突.具体来说,标签没有足够的处理能力与能源来实现上述竞争机制,避免通信冲突.鉴于 RFID 的系统特点,RFID 标签识别协议需要具备如下性质:(1)简单.由于 RFID 标签上的计算、存储资源极其有限,标签识别协议的处理逻辑(包括执行流程和状态迁移关系)需要尽可能简单;(2)高效.面对大量的 RFID 标签,标签识别协议需要提供轻量级的通信机制,尽可能避免不必要的控制报文的传输,确保传输的高吞吐率与低延迟性.

目前的 RFID 防冲突算法主要分为两大类:基于二进制树的防冲突算法[1-2]和基于 ALOHA 的防冲突算法[3-8].前者利用二叉搜索树,按照递归的方式将冲突的标签集合划分为两个标签子集,对于可能产生冲突的相关标签集合,采用沉默的方式来解决冲突问题.划分子集的方法包括随机二进制树算法和查询二进制树算法.文献[1]提出了一套自适应的基于树形结构的防冲突算法来实现有效的标签识别.文献[2]提出了一套基于查询树结构的智能遍历机制,能够以低延迟的方式实现标签的识别.ALOHA 协议最早被用在分组无线网络中实现随机访问机制.在 RFID 系统中,为了提高标签识别的效率,文献[3-4]提出了时隙 ALOHA 协议来有效解决冲突,实现标签的高效识别.时隙 ALOHA 协议将若干个时隙组织为一帧,在每一帧开始时,阅读器广播帧的长度 f,即当前帧所包含的时隙个数,并通过发送连续的电磁波来激活扫描范围内所有标签.每个标签在接收到帧长 f 之后随机独立地在第 1～f 个时隙中选择一个时隙发送标识符.如果成功,即无冲突发生,该标签进入静默状态;如果有冲突发生,则该标签将继续等待在下一帧中再选择一个时隙重新发送标识符.因此,每一帧的时隙会存在如下 3 种情况之一:(1)空时隙(Empty Slot).没有任何一个标签选中该时隙;(2)单时隙(Singleton Slot).仅有唯一一个标签选中该时隙;(3)冲突时隙(Collision Slot).多个标签选中该时隙.上述每种时隙所包含的信息量各不相同.目前,时隙 ALOHA 协议已经成为 RFID 系统在 EPC-C1G2 标准下使用的通信协议.在表 1 中,我们分别从优缺点两个方面对上述两种防冲突算法进行了比较,总体而言,两者在性能与功能实现方面各有利弊.

对于时隙 ALOHA 协议而言,每一轮所采用的帧长对总体的识别性能至关重要.对于给定的待读标签集合,如果帧长过大,则该帧大部分时隙为空时隙,导致时隙的浪费;如果帧长过小,则该帧大部分时隙会出现标签传输冲突,导致大部分标签需要在下一帧重传.因此,研究者们对该问题进行了深入研究.文献[5]分析了在时隙 ALOHA 协议中采用动态帧长的方法对读取性能的影响.文献[6]基于贝叶斯的概率模型提出了优化动态帧长的决策机制.文献[7]利用马尔可夫过程来对读取过程进行建模,并且由此计算出读取过程中应该使用的一系列优化的帧长.文献[8]进一步针对最大化信道使用效率的目标推导出优化的动态帧长,该文指出,如果每一轮中帧长与当前未读取的标签数相同,则整个信道能够达到最大的使用效率.其原理阐述如下:假设当前标签数目为 n,帧长为 f;由于标签对时隙的选择符合二项分布,则根据二项分布,当前帧中单时隙的期望数目为 $E[n_1]=n\times(1-1/f)^{n-1}$;为了最大化信道的使用效率,即单时隙数目在当前帧中的比例 n_1/f,我们采用求极值的方法计算 f 的取值,即 $\frac{\partial E[n_1]/f}{\partial f}=0\rightarrow f^*=n$,得到此时信道的使用效率为 $n_1/f^*\rightarrow 1/e$.对于上述性质,我们在图 2 和图 3 中给出更为形象的描述.图 2 展示了给定标签数目 $n=100$,帧长 f 变化对信道使用效率的影响.可以看到当帧长 f 由小及大变化时,信道的使用效率逐渐增大后又逐渐减小,在 $f=100$ 时取到最大值1/e.图 3 展示了随着标签数目 n 变化,使用最优帧长 $f^*=n$ 对信道使用效率的影响.可以看到当 n 取值较小时,所达到的最优效率大于 1/e,例如,当仅有一个标签时($n=1$),帧长为 1 可以达到最优效率 100%.当 n 逐渐增大时,其最优效率快速收敛到 1/e.这就意味着,当 $n>5$ 时,每一轮帧长 f 取值为当前待读的标签数 n 时,使用效率趋向于 1/e,可以达到当前每一轮的局部最优效率.如果在识别过程中每一轮都使用该策略,则整体效率可接近 1/e.由于 1/e 是整体效率的上限值,因此当前整体效率接近全局最优.

表 1　两类防冲突算法的优缺点比较

	基于二进制树防冲突算法	基于 ALOHA 防冲突算法
优点	通常使用确定性的算法,算法实现逻辑简单;基于查询树结构的算法不需要存储中间状态变量	使用随机算法,算法实现逻辑简单;平均情况下,标签识别性能良好;随机算法使得各时隙的结果在统计意义上符合一定的概率分布,有助于进行各种统计性分析
缺点	对基于查询树结构的算法,标签识别的时延受扫描范围内标签 ID 的分布以及 ID 的长度影响	算法的随机性导致存在“饿死”问题,某些标签可能永远选择不到单时隙进行传输;最坏情况下,标签识别的时延趋向于$+\infty$,其性能无法保障

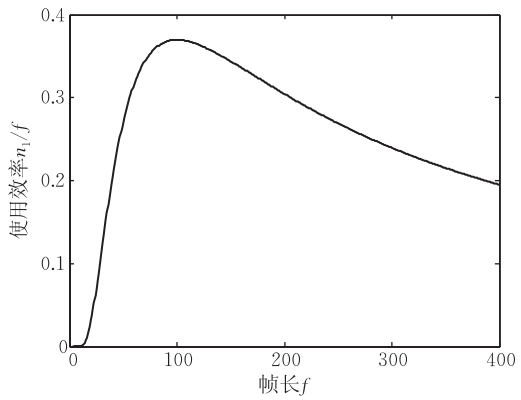

图 2 给定标签数目$n=100$,信道使用效率与帧长 f 的关系

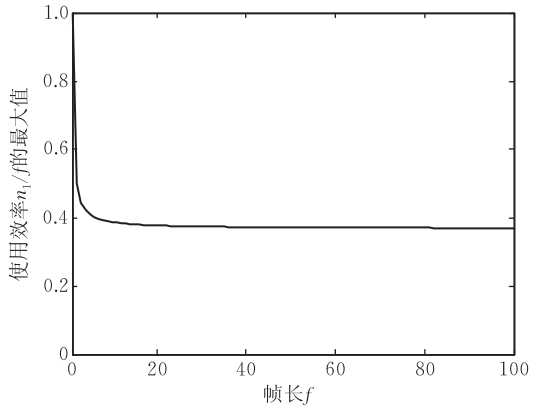

图 3 随着标签数目 n 变化,使用最优帧长$f^*=n$对应的信道使用效率

上述提到的协议与防冲突算法多数是在较为理想的部署环境下得出,并未充分考虑实际应用环境下所遇到的种种难题,例如,标签的频繁移动、多个RFID 阅读器之间的信号干扰、RFID 标签传输的信号衰减以及多径效应等. 因此,一些研究工作开始关注并尝试解决上述问题. 鉴于之前的研究工作大多关注于解决标签之间的传输冲突问题,并未考虑到多个阅读器之间以及标签与阅读器之间的信号干扰,文献[9-10]在多个 RFID 阅读器环境下提出了优化的阅读器激活与调度机制,使得多个阅读器能够协作地识别标签,有效避免信号的传输冲突. 考虑到单个 RFID 阅读器的有效读取范围相对有限,文献[11]利用"时空关联"关系提出了性能高效的连续扫描机制,来实现对大规模部署标签的快速识别. 之前大部分的研究工作主要考虑在相对理想状态下针对静态环境设计优化的标签识别机制,并未考虑移动环境以及传输环境中普遍存在的信号衰减对标签识别性能带来的影响. 有鉴于此,我们针对上述问题开展了相应的研究工作,文献[12]针对移动环境下持续变化的信号衰减情形,基于跨层优化的思路提出了一套 RFID 标签读取性能的概率模型,基于时隙 ALOHA 协议设计出优化的标签识别参数,相比传统的识别机制更为有效地提升了识别的性能.

2.2 RFID 的标签数量估算机制

随着 RFID 应用的进一步拓展,某些应用仅需要获取一些统计性信息来为上层的数据分析以及挖掘提供数据基础. 在这种情况下,RFID 系统不需要逐个识别标签,仅仅需要快速获取扫描范围内标签的统计信息,其中一个关键的信息就是标签数量. 此外,基于动态帧长的时隙 ALOHA 协议也需要估算标签的大体数量来决定动态帧的长度. 因此,近年来出现了很多关注于如何快速、精确地估算标签数目的研究工作,其核心思想主要是使用基于随机算法的时隙 ALOHA 协议来实现估算. 研究者们意识到,尽管时隙 ALOHA 协议是以随机的方式让标签选择时隙进行数据传输,然而从统计意义上来看,整个空时隙、单时隙以及冲突时隙的分布事实上是符合二项分布的. 当对时隙的采样次数足够多时,完全可以基于二项分布规律来估算出实际参与标签的数量. 基于上述思路,文献[13]提出了一套快速而可靠的标签数量估算机制,以一种实用的方式实现了RFID 标签的快速统计. 其主要思想为:假设在某一轮中帧的长度为 f,空时隙的数目会随着实际参与的标签数 n 增加而减少,冲突时隙的数目会随着标签数 n 增加而增加,而单时隙的数目会随着标签数 n 增加先增加再减少, 因此,空时隙(冲突时隙)的数目与标签数存在明确的单调减(增)关系. 该文作者基于二项分布的概率模型给出了空时隙与冲突时隙的数值期望计算公式,提出了空时隙与冲突时隙相结合的估算算法,并通过重复采样的手段有效降低了估算的误差. 研究者们通过进一步研究发现,尽管单时隙数目与标签数目不存在单调关系,无法利用单时隙数目推算出确切的标签数目,但是 3 种时隙的数目结合起来能够指导系统更精确地估算标签数目. 文献[14]根据观察到的 3 种时隙的数目提出了一套后验概率模型,基于最大化后验概率的决策来更精确地实现标签数量估算机制. 上述机制均需要对 3 种时隙进行大量采样来提高估算的精确度,事实上,完全可以借助其它参量来更快速有效地估算标签数目. 我们在文献[15]中提出了一种基于Ball-and-Bin 概率模型的快速估算方法. 其核心思想在于:每个标签会随机选择位置回复,系统可以通过观察第一个标签回复的位置来估算最有可能造成该事件发生的标签数量. 该文从理论上建立了概率模

型，并证明了其正确性和性能的上界. 实验表明，在给定精度要求的情况下，该方法明显快于现有其它方法. 此外，为了解决单个标签被多次读取的问题，文献[16]提出了一套“复制不敏感”的估算机制来实现更精确的标签数量统计. 文献[17]提出了一个自适应的基于划分的估算机制，该机制基于几何分布规律让单个标签选择同一帧中的多个时隙进行传输，使得每个标签有 $1/2^t$ 的概率选择第 $t-1$ 个时隙，有效解决了单个标签被多次读取的问题. 表 2 对上述研究工作的特点进行了总结和比较.

表 2　标签数量估算算法的特点总结与比较

估算算法	与时隙 ALOHA 协议兼容性	估算参考的指标	概率模型
文献[13]	兼容	空时隙与冲突时隙的数目	二项分布
文献[14]	兼容	3 种时隙的数目	基于二项分布的后验概率模型
文献[15]	兼容	第一个标签回复的位置	二项分布
文献[16-17]	不兼容	冲突时隙出现的边缘位置	几何分布

除了对标签数量进行简单估算之外，一些研究工作者开始探究如何在 RFID 系统上实现更为复杂的数据分析与挖掘机制. 文献[18]着力研究面对大量的 RFID 标签，如何在不需要读取所有标签具体信息的前提下快速定位出最热门的标签类别. 该文基于分组测试(Group Testing)的理念，提出了有效的随机算法来解决上述问题. 文献[19]面向流量追踪一类的应用问题，针对动态移动的标签集合提出了保障隐私的快速估算机制. 该机制能够快速统计在时域 (t_1,t_2) 内从地点 A 移动到地点 B 的标签数目，从而在无需读取确切标签 ID 信息的前提下有效地进行流量追踪. 总体而言，目前该方面的研究成果相对较少，随着 RFID 数据管理技术以及相关应用的进一步拓展，基于 RFID 的数据分析与挖掘机制必将得到更为广泛的关注与深入的研究.

2.3　RFID 的标签轮询机制

某些 RFID 应用并不需要获取全部 RFID 标签的标识信息，仅需要对指定集合内的标签进行轮询，来确认标签的状态是存在或丢失. 例如，对仓库管理应用而言，出入库之前管理员需要根据货物清单来清点指定的货物，确定是否存在货物丢失. 在这种情况下，假设所有的货物都贴有唯一标识的 RFID 标签，能否有效地实现标签的轮询机制成为与此密切相关的问题. 最简单直接的方案便是设计一种类似于“点名”的机制：阅读器根据清单内容接连地广播标签的标识符 ID，每传输一个 ID 后，阅读器会等待对应的标签返回一个短暂的响应消息. 如果接收到响应，则推断该标签存在于扫描范围内，否则认为该标签丢失. 然而，上述方案存在如下弊病：(1) 与时隙 ALOHA 协议不太兼容；(2) 长达 96 bit 的 ID 传输使得整体扫描时间过长，降低了系统的效率. 因此，研究者们针对上述问题开展了深入的研究，其目标为基于时隙 ALOHA 协议设计出一套有效的标签轮询机制，尽可能地减少整体扫描时间.

研究发现，在时隙 ALOHA 协议的每一轮中，处于激活状态的标签会“随机”地在帧中选择一个时隙进行传输. 然而，由于标签的简易性，真正的随机性很难得到实现. 事实上，标签的芯片逻辑实现了一个“伪随机”的操作：在每一轮中阅读器广播一个随机数 r，每个被激活的标签接收到 r 后随即结合本地的标识符 ID 进行散列操作，计算出伪随机数 s 作为选定的时隙序号，这里 $s=\mathrm{hash}(ID,r)\bmod f$，$f$ 是帧的长度. 上述的“伪随机性”意味着，对于任一标签，一旦阅读器广播的数值 r 以及帧的长度 f 确定下来，该标签在帧中相应的位置即被确定，这就使得对标签的有效轮询成为可能. 在实施扫描之前，阅读器可以预先根据指定集合内各标签在帧中对应的位置为每个时隙计算出期望的结果：空时隙(0)、单时隙(1)或者冲突时隙(C). 对于某一时隙，如果该时隙期望为单时隙但实际无响应，则表明对应于该时隙的标签丢失；如果该时隙期望为冲突时隙但实际无响应，则表明对应于该时隙的所有标签丢失. 图 4 给出了基于时隙 ALOHA 协议的轮询机制示意图. 如图所示，在标签 A～H 中，虚线标识丢失的标签，实线标识存在的标签. 当标签 E、F 以及 H 丢失时，其对应的时隙实际观察到的状态变成空时隙(0)，此时可以判定标签丢失. 但对于标签 C 丢失的情况，由于标签 B、D 的存在，使得对应时隙实际观察到的状态仍为冲突时隙(C)，未能判断出标签 C 丢失的情况，导致假阳性误判(False Positive). 上述轮询机

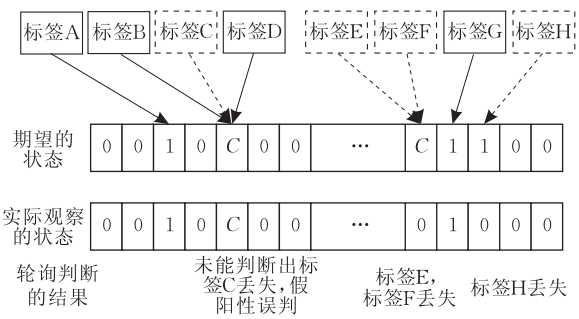

图 4　基于时隙 ALOHA 协议的轮询机制示意图

制为进一步的研究工作提供了一个理论基础.

基于上述认识,文献[20]对面向大规模标签监控应用中的一个重要问题进行了研究:如何在大量标签中快速定位出丢失的标签.该文利用时隙ALOHA协议的伪随机性,基于轮询机制提出了多种协议,能够快速有效地定位丢失的标签.针对由电池供电的大规模主动标签实时信息收集的问题,文献[21]设计了一套高效节能的轮询协议.该协议基于标签排序(Tag-Ordering)的编码方式,使得所消耗的能量比通常的轮询协议下降一个数量级.该协议进一步采用基于分块的布鲁姆过滤器(Bloom Filter)来提高轮询机制的性能,在不影响整体扫描时间的前提下显著降低了能耗.文献[22]针对上述问题进一步提出了基于单级 Hash 与多级 Hash 的轮询机制,显著地降低了信息收集的时间.文献[23]基于轮询协议提出了一套批处理的认证机制,无需通过逐个识别的方式来认证标签.通常情况下,为了实现对大量标签的认证,阅读器需要对标签逐一识别并认证,这种方式需要耗费大量的通信开销与扫描时间.基于轮询协议的伪随机性,该批处理认证机制提出了一套快速的认证算法,能够极大地降低认证的扫描时间与通信开销.由于该机制基于时隙ALOHA的随机算法进行认证,因此存在假阳性误判,但是该机制能够以概率的形式确保未检测到的伪造标签所占比例被控制在指定阈值范围内.上述研究工作的轮询机制都对应于扫描范围内的所有标签,如果仅需要对扫描范围内标签的一个子集进行轮询,这些机制将很难适用.因此,针对大规模标签部署情况下搜索特定标签集合的问题,文献[24]基于布鲁姆过滤器提出了一套两阶段的快速搜索算法,能够在指定的假阳性误判率的范围内有效降低通信开销与时延.总体来说,RFID的轮询机制基于时隙ALOHA协议中的伪随机操作来进行轮询,能够有效避免对标签逐一识别带来的额外开销,但同时也存在假阳性误判的效应,系统可以借助相应的优化机制来降低假阳性误判的概率.

3 RFID的认证与隐私保护机制

3.1 RFID的安全与隐私问题

在物联网应用中,对RFID系统实现有效数据管理的前提在于保障RFID数据的安全性与私密性.RFID系统的安全威胁主要来自于阅读器对标签的非法访问以及伪造标签的存在.对RFID系统而言,其安全问题是指存在伪造标签时,如何有效地对标签进行认证;其隐私问题是指存在恶意阅读器时,如何防止阅读器对标签的非法访问,来有效地保护用户的隐私.在常用的网络安全解决方案中,已经存在成熟的加解密算法如DES、AES、RSA、椭圆曲线密码等,这些算法构成了对称密钥加密以及公开密钥加密中的支撑技术,能够有效地实现加密与鉴别功能,抵制非法读取、伪装哄骗、重放攻击等安全威胁,具有良好的安全性.但实现上述算法需要较多的逻辑处理单元,如AES需要大约20000～30000个逻辑门,RSA、椭圆曲线密码等公钥密码算法则需要更多的逻辑门.而RFID标签受到低成本限制,通常只能拥有大约5000～10000个逻辑门,并且这些逻辑门主要用于实现一些最基本的标签功能,仅剩少许可用于实现安全功能.此外,RFID标签上的存储资源也非常受限,通常标签的EPC区仅能存储96 bit数据,用户区仅能存储512 bit数据.RFID标签极其有限的计算资源难以支持上述复杂的加解密算法的实现.因此,对RFID系统而言,其安全与隐私保障机制所面临的最大挑战在于:如何以一种轻量级的方式在资源极其受限的RFID系统上实现认证与隐私保护协议.下面我们从基于物理方法的安全保护机制、基于对称密钥加密的协议以及基于Hash函数的协议等几个方面来具体阐述相关研究成果.

3.2 基于物理方法的安全保护机制

RFID的隐私问题是由阅读器识别标签时无需认证引起的.在没有隐私保障机制的情况下,阅读器可以随意地对标签进行秘密扫描,获取标签信息;对于无法直接获取信息的加密标签则可以根据反馈的加密信息进行跟踪,获得用户的地点信息,综合整理就形成了对用户个人信息的盘点.为了保护RFID用户隐私,一种简单直接的手段便是基于物理方法的安全保护机制,具体而言,主要包括灭活操作、静电屏蔽、主动干扰以及阻塞法等.

灭活(Kill)操作是一种简单暴力的方法,阅读器通过向标签发送一个指定的PIN码来执行杀死命令,命令执行完后标签就失效了,不再对阅读器的查询做出回应.显然,完全地让标签失效并不是一个合理的解决方案.文献[25]提出可以只让标签中唯一识别码失效而保留产品类型标识码的数据部分,这样就可以避免标签被跟踪,但是该方案使标签失去了唯一标识物品的特性.文献[26]提出采用全新的标识符重新对标签进行标识的方案,原有的标识

符可以在物品被回收等情况下重新被激活使用. 由此来看，灭活操作使标签丧失功能，不可能再被重用，从而阻止对标签的任意读取和跟踪；而需要考虑到重用的场合可以采取休眠(Sleep)机制[26]，原理与前者相似，但是实施休眠机制的标签可以被唤醒再次使用. 静电屏蔽是指将标签放入具有静电屏蔽功能的容器中，使其不能与外界进行电磁耦合，阻止标签被扫描，这种方法需要一个额外的物理设备，如法拉第网罩. 主动干扰是指通过一个设备主动广播干扰信号来阻止或破坏附近的非授权阅读器对标签的读写操作. 文献[27]提出了一套基于掩码的主动干扰机制. 当阅读器在读取标签 ID 时，标签周围的保护设备会同时传输一串掩码序列信号，最终阅读器接收到标识符 ID 与掩码相混杂的信号. 这种机制使得授权的阅读器能够使用该掩码序列有效恢复标签的标识符，而未授权的阅读器由于无法获取该掩码序列的模式，从而无法对接收的混杂信号进行有效恢复. 阻塞法采用一个特殊的阻止标签，通过设定的标签冲突算法来阻止未授权的阅读器读取那些受保护的标签. 文献[28]提出了上述阻止标签的理念，通过编入标签的可修改位来保护隐私，若隐私位为‘0’表示可公开扫描，为‘1’则表示是私有区域. 当阅读器访问私有区域时，采用一个特殊的阻止标签来实行干扰，从而阻止未授权的阅读器非法读取受保护的标签.

3.3　基于对称密钥加密的协议

公开密钥加密算法虽然功能强大，能够有效地实现加密、电子签名等机制，但由于其复杂的计算操作使其根本无法在资源异常受限的 RFID 系统上实现. 因此，RFID 系统往往借助于逻辑较为简单的对称密钥加密算法来实现安全与隐私保障机制. 具体来说，基于对称密钥加密的协议可以用来对标签进行有效认证. 在该协议中，任一标签与阅读器共享一个对称密钥. 算法 1 阐述了使用对称密钥加密算法对 RFID 标签进行认证的过程[29].

算法 1.　使用对称密钥加密算法对 RFID 标签进行认证.

1. 标签向阅读器发送数值 T_i 表明身份.

2. 阅读器生成一个随机的比特串 R，发送至标签.

3. 标签用密钥 k_i 对比特串 R 进行加密，计算 $C=E_{k_i}[R]$，将 C 发送至标签.

4. 阅读器本地计算 $C'=E_{k_i}[R]$，验证是否有 $C=C'$，若是，则标签被成功认证.

上述基于对称密钥加密的协议虽然能够对 RFID 标签实现有效认证，但却无法保护标签的隐私. 由于在步骤 1 标签需要事先将标识号 T_i 发送至阅读器，所有邻近的阅读器都能够读取该标识信息，这种方式完全暴露了标签的隐私；另一方面，如果不发送标识号 T_i，则阅读器很难迅速地定位到对应的密钥 k_i 来支持后续操作. 为了在实现认证的同时保障隐私，事实上存在一种简单直接但性能低下的方法：相比于算法 1，标签无需传输标识 T_i，而是直接根据接收的挑战数 R 发送加密密文 $C=E_{k_i}[R]$. 阅读器接收到加密密文 C 后，在本地遍历所有可能的 k_i 计算 $C_i=E_{k_i}[R]$，如果存在某个 k_i 使得 $C_i=C$，则通常情况下该密钥对应的标签即为当前认证的标签. 假设搜索空间存在 n 个标签，该算法密钥搜索的时间复杂度为 $O(n)$，当 n 数值很大时，其搜索时间开销是巨大的. 针对上述问题，很多研究工作开始关注于如何根据加密密文进行快速的数据搜索. 文献[30]提出了基于对称密钥的加密数据搜索系统. 文献[31-32]也提出了基于加密数据库的查询系统. 我们也在该方面开展了研究工作，文献[33]通过在标签上维护一个单调增的计数器，从而利用二叉搜索方案来进行快速的搜索，将时间复杂度降低至 $O(\log n)$.

在基于对称密钥加密协议中，当密钥 k_i 的长度足够大时(不小于 128 位)，仅仅根据比特串 R 和 C 是很难在短时间内使用普通的计算设备推算出密钥 k_i 的，协议安全性高. 但是，由于 RFID 标签成本的限制，标签内部存储单元通常少于 512 bit，逻辑门的数目也相当受限，实际使用在 RFID 系统中的比特串 R 和 C 以及密钥 k_i 的长度都远小于达到正常安全标准所期望的数目. 例如，德州仪器公司研发了用于汽车防盗系统中的加密 RFID 标签，出于标签成本的考虑，挑战数 R 与密钥 k_i 的长度仅为 40 bit，标签响应结果 C 仅为 24 bit. 在这种情况下完全可以通过逆向工程、密码破解等技术来破解该加密系统. 针对上述问题，研究者们提出了各种轻量级解决方案来保障安全性. 其中，DESL[34]是在传统的加密协议 DES 基础上为适应小型计算设备(如 RFID 标签)要求的一种轻量级的扩展，是一套超低成本的加密算法. HIGHT[35]是一种分组加密算法，它使用 64 位的分组块和 128 位的密钥，子密钥只在加密和解密的运行过程中被生成，对硬件资源的要求很低.

3.4　基于 Hash 函数的协议

相比于对称密钥加密协议，采用 Hash 函数可以在多数情况下实现等效的安全机制，且实现逻辑会大为简化. 因此，近年来很多研究工作关注于在

RFID 系统中采用基于 Hash 函数的协议来实现一套足够轻量级的安全与隐私保障机制. 尽管 Hash 函数的逻辑实现已经相对简单,但是由于 RFID 标签的资源稀缺性,Hash 函数的常用逻辑实现还是超出标签的资源限制. 为此,需要确保实现 Hash 函数的逻辑电路足够简单. 研究发现[20],Hash 数值可以从一个预先存储的随机比特序列中推导:首先,使用离线的随机数生成器以标签 ID 为种子生成一个 200 bit 的随机序列,将其存储在标签内部;该比特序列首尾相连形成一个逻辑上的环结构;当执行 Hash 操作 $H(ID,r)$ 时,即在上述环结构序列中返回第 r 个比特以后一串指定长度的比特序列. 这样,200 个随机比特组成的序列可以返回 200 个不同的 Hash 数值,在通常情况下足够满足一般的应用需求.

基于 Hash 函数的安全协议主要包括 Hash-Lock 协议、随机化 Hash-Lock 协议以及 Hash 链协议等. Hash-Lock 协议[36]使用了 $metaID$(标签密钥的 Hash 值)代替真实的标签 ID,来有效地对阅读器进行认证,从而避免标签信息泄露. 然而,由于 $metaID$ 对特定的标签始终保持不变,因此标签每次响应都使用固定的 $metaID$,容易受到追踪和重放攻击. 随机化 Hash-Lock 协议[37]采用了基于随机数的询问/应答机制:在阅读器请求访问标签时,标签先用伪随机数生成器生成一个随机数 R,然后计算其 ID 和 R 的 Hash 值 $H_{\text{key}}(ID \| R)$,最后将随机数 R 与该 Hash 值发送给阅读器. 阅读器在后台数据库中进行穷举搜索,计算所有 ID 和 R 的 Hash 值 $H_{\text{key}}(ID \| R)$,将匹配成功的 ID 发送给标签,实现解锁. 上述这种方式能够避免标签每次响应固定模式的信息,故而不能对其进行跟踪. 但是,随机化 Hash-Lock 协议不能防止重放攻击. 攻击者完全可以窃听随机数 R 以及对应的 Hash 值 $H_{\text{key}}(ID \| R)$,从而在阅读器查询时重放该响应伪装为该标签. 其次,阅读器端的穷举搜索使得该方法缺乏很强的可扩展性. Hash 链协议[38]是基于共享秘密的询问/应答协议,在该协议中,标签和阅读器共享两个 Hash 函数 G 和 H 以及一个随机的初始化标识符 s_1. 当阅读器请求访问标签时,标签返回当前标识符 $r_k = G(s_k)$,同时更新当前标识符为 $s_{k+1} = H(s_k)$. 阅读器根据获得的 r_k 值查找数据库对标签进行认证,并更新 s 值与标签保持同步. 该方法利用 Hash 函数的"前向安全性"使得标签响应的结果随每次查询不停更新,有效防止了重放攻击. 但是,攻击者可以恶意多次扫描标签,使得标签与阅读器之间失去同步,导致阅读器在认证时无法设定每个可能的标签 ID 需要的计算次数,使系统无法正常工作.

表 3 对上述 3 种方案从效果、适用范围以及标签所需资源 3 个方面进行了具体的比较. 可以看出,3 种方案各有利弊,需要根据具体的应用需求与资源限制条件来选择合理的安全与隐私保障方案. 目前,国内的研究者们也在 RFID 的安全与隐私保障方面开展了深入的研究. 文献[39]分析了已有的各种 RFID 安全机制,重点介绍了基于密码技术的 RFID 安全协议,分析了这些协议的缺陷,讨论了基于可证明的安全性理论来设计和分析 RFID 安全协议的模型和方法. 文献[40]定义了供应链环境下 RFID 通信协议必须满足的安全需求,提出了一个可以满足这些安全需求的通用可组合安全模型,设计了一个可以实现该模型的轻量级 RFID 通信协议.

表 3 3 种方案的比较

	效果	适用范围	标签所需资源
基于物理方法的安全保护机制	标签实现逻辑非常简单,不需要标签自身实现安全与隐私保障	适用于对处理能力非常有限的被动标签进行安全保护的场合	对标签的资源要求非常低,需要额外的设备提供安全隐私保障
基于对称密钥加密的协议	标签实现逻辑较为复杂,能有效实现加密、解密操作	适用于主动标签或处理能力较强的被动标签需要进行加密、解密的场合	对标签资源要求较高
基于 Hash 函数的协议	标签实现逻辑较为简单,具有"前向安全性",不能实现加密、解密操作	适用于处理能力较弱的被动标签需要认证的场合	对标签的资源要求低

3.5 其它解决方案

近年来,为了更有效地防止针对 RFID 系统的黑客攻击,一些研究者开始关注入侵检测系统在 RFID 系统中的应用. 由于 RFID 标签处理能力非常有限,不可能在标签上实现入侵检测的逻辑. 因此,文献[41]基于小型电池装置设计了一套 RFID 守护系统. 该系统集成了多种安全机制,包括密钥管理、访问控制、认证以及审计功能,尽管集成了多种安全功能,该系统却很容易出现单点失效的问题:一旦守护系统被攻克,整个 RFID 网络都被暴露在各种攻击隐患之下. 文献[42]进一步提出了一个入侵检测系统模型 Deckard,用来检测标签所有权的改变. 该系统是 RFID 入侵检测系统的早期研究工作之一. 文献[43]基于 RFID 系统设计了一套入侵检测系统安全框架,在 RFID 阅读器层面以及中间件层面实

现了入侵检测的功能.该系统利用阅读器之间的通信来获取攻击检测所需的审计信息,将 RFID 阅读器作为“看门狗”来从周围的阅读器与标签中收集所需信息,提供了一套更为泛化的安全框架来检测多样化的 RFID 攻击.总体说来,随着 RFID 的进一步广泛应用,RFID 系统的入侵检测方案将会受到越来越多的关注.

4　真实环境下 RFID 系统的性能评测与分析

很多 RFID 的前期研究工作主要考虑在相对理想的传输环境下如何对 RFID 数据收集算法与协议参数进行优化,并通过模拟实验来验证其性能.事实上,对于 RFID 系统而言,真实传输环境中的一些物理因素包括路径损耗、能量吸收、信号干扰等给物理层的信号传输带来了极大的不可靠性,由此对基于防冲突算法的 RFID 数据收集机制的性能也带来了很大的影响.具体说来,真实传输环境下影响 RFID 系统性能的关键因素包括:(1)阅读器的发射功率;(2)能量吸收、路径损耗、多径效应;(3)信号干扰;(4)标签的分布与部署.对阅读器的发射功率而言,功率过小,阅读器有效通信范围减小,使得某些标签无法被激活,或者由于反射信号能量过小,低于信噪比从而使阅读器无法有效识别;功率过大,阅读器有效通信范围增大,使得某些标签反射的信号能量增大,导致标签之间的信号干扰增大.对能量吸收、路径损耗、多径效应而言,这三者都会引起信号衰弱,大幅度降低发射信号到达标签的能量以及反射信号到达阅读器的能量,导致信号难以识别.对信号干扰而言,标签与标签之间、标签与阅读器之间、阅读器与阅读器之间都存在发射/反射信号的干扰,导致比特差错,降低传输效率.对标签的分布与部署而言,标签部署过于密集,会导致阅读器的发射能量被充分稀释,并且反射信号间的干扰与能量吸收会加剧;过于稀疏会导致其超出阅读器扫描范围;而对于单个标签,如果标签平面(即标签天线方向)与能量穿透方向平行,则无法产生足够强度的反射信号,应使标签平面与能量穿透方向尽可能正交.表 4 具体阐述了这些因素对 RFID 系统具体性能参数的影响,包括 RFID 系统的扫描范围、阅读速率以及能量消耗.

表 4　关键因素对系统性能各指标的影响

	扫描范围	阅读速率	能量消耗
阅读器的发射功率	功率过小,阅读器有效通信范围减小;功率过大,阅读器有效通信范围增大	功率过小,使得某些标签无法被激活或有效识别,降低阅读速率;功率过大,使得部分标签反射信号强度增大,导致标签间信号干扰增大,降低阅读速率	功率过小,能量消耗小;功率过大,能量消耗大
能量吸收、路径损耗、多径效应	会引起信号衰减,减小阅读器有效通信范围	使得正常通信范围内某些标签无法被激活或有效识别,降低阅读速率	使得阅读器必须要增加功率来补偿传输中信号能量损失,增加能耗
信号干扰	某些标签反射信号会受到干扰无法被有效识别,阅读器有效通信范围减小	导致传输比特差错,降低阅读速率	阅读器需要合理调整功率来避免过多信号干扰,会改变阅读器能量消耗
标签的分布与部署	标签的密集部署会影响阅读器天线的电磁场分布,改变阅读器有效通信范围	如果使标签天线方向与能量穿透方向尽可能正交,读取效率增大,阅读速率提升;否则,阅读速率下降	标签分布部署不合理会使得阅读器必须要增加功率来提升反射信号强度,增加能耗

上述因素在真实传输环境下的普遍存在性使得理想情况下推导出的算法与优化参数在实际情况下的性能很难得到保障.因此,目前该领域的很多研究工作者关注在真实应用环境下对 RFID 系统实际性能的测试与分析.为了说明物理层差错对 EPC-C1G2RFID 系统的影响,文献[44]给出了模拟实验结果,证明了物理层的比特差错极大地降低了系统的整体性能.文献[45]在真实环境设置下检验了 RFID 系统的读取性能,确定了导致整体性能和可靠性降低的物理层因素.他们发现物理层实际的环境参数以及相关配置参数的设置极大地影响了读取性能,并且由于物理层与 MAC 层没有进行有效整合,导致明显的性能下降.文献[46]利用简单、经验性的实验手段验证了当前 RFID 系统识别标签的各项性能参数,作者通过在不同的传输环境下(包括自由空间、接近水、接近金属环境),改变通信距离检验了各项性能参数.文献[47]针对 RFID 系统给出了一个综合的性能基准,通过这些基准能够描述在真实环境下 RFID 系统的运作效率.文献[48]在真实环境设定下对 RFID 系统性能进行了验证,发现在阅读器的有效探测范围内存在两个不同的区域:主探测区域和次探测区域.主探测区域是指靠近读取

器的一段探测区域,在该区域内具有很高的标签识别概率(接近 100%);次探测区域是指从主探测区域末端延伸至有效识别范围边缘的一段探测区域,在该区域内标签识别率依照线性关系降低为 0. 文献[49-50]研究了在真实传输环境下阅读器发射功率对大规模标签识别性能的影响,通过实验发现,RFID 标签在激活状态与非激活状态之间存在一个中间状态(Lossy State),对识别性能影响很大. 由此作者提出了自动功率调节算法,进一步降低了阅读器的总体能耗与扫描时延. 文献[51]通过真实实验发现,当阅读器功率被调整至合理范围时,可以利用遏止效应(Capture Effect)来有效地将冲突时隙转化为单时隙,由此提出了渐进的扫描算法来优化读取性能. 文献[52]提出了无源 RFID 系统中能量有效的物理层设计方法,在前向链路中为使标签获得更多能量,结合 ASK 调制提出了一种新的用于无源 RFID 系统的能量有效的数据编码方法. 上述研究成果表明,RFID 在 MAC 层、应用层方面的研究需要充分结合物理层的实际传输特性;否则,理想情况下设计出的算法与协议将与实际的情况严重不符,无法达到预期的性能要求.

总体来说,为了有效避免或降低物理环境因素对系统性能各指标的影响,目前的有效方法主要包括以下几个方面:(1)调整阅读器功率. 通过合理调整阅读器功率,补偿信号衰减的同时有效避免干扰,优化系统性能;(2)优化协议参数. 设置优化的协议参数(如帧长、传输速率)来优化读取性能;(3)规划部署方案. 通过调整标签的部署位置、方向以及增加冗余标签的方式来提升识别性能;(4)改善物理层设计. 采用更合理的编码/解码方案以及通信频段来提高数据传输可靠性.

5 其它开放性问题

上述 RFID 数据管理方面的研究工作主要关注如何能够快速、有效地识别标签的标识信息. 事实上,从数据管理的角度来看,除了标签的标识信息,RFID 系统还能够提供一类非常重要的信息,那就是标签的反射信号强度. 通过对反射信号强度数据进行有效处理与合理利用,RFID 系统能够实现定位、追踪以及移动行为感知等机制.

5.1 基于 RFID 的定位机制

目前的定位系统主要包括 GPS(Global Positioning System)定位、蜂窝基站定位、WLAN 定位、传感网定位等. 其中,GPS 定位与蜂窝基站定位主要用于室外定位,WLAN 定位、传感网定位主要用于室内定位. RFID 定位技术以低成本、非接触性通信等特点,有望成为室内定位技术的首选. 目前的室内定位系统大多基于 RSSI(Received Signal Strength Indicator)来辅助定位,其基本原理是:已知发射信号的强度,接收方根据接收到的信号强度,估算出通信双方的距离. 而在实际情况下,无线信号在空间传播时能量的衰减不仅受传播距离的影响,还受到多径效应、传播的方向性、复杂的室内结构、随机流动的人员等诸多不确定因素的影响,利用 RSSI 作为位置感知数据进行室内定位存在较多的困难. 但是由于 RSSI 极易获取,不需要额外的设备,相比于其它定位技术成本非常低,因此当前主流的 RFID 定位技术都是基于 RSSI 进行定位. 其中比较典型的代表是 SpotON 系统与 LANDMARC 系统. SpotON 系统[53]基于阅读器与目标标签构造了一个无线感知环境,通过聚合算法减少信号强度误差,并利用信号传播模型求解阅读器与目标标签的距离,最后利用三角定位算法对目标在三维空间进行定位. 整体而言,SpotON 是一个实验性的原型系统,无论是距离估计还是误差处理都停留在比较粗糙的阶段. LANDMARC 系统[54]在已知位置引入参考标签,通过对比目标标签与参考标签的 RSSI 值,来确定物理坐标关系,最终确定目标标签坐标. LANDMARC 通过将参考标签部署到实际应用场景中,实时同步地对参考标签和目标标签进行能量值测算,可以最大限度减少多径效应以及电离体对电磁波的影响,接近精确的定位效果. 该系统在较少阅读器的条件下提高了系统的定位精度,同时也大大降低了系统成本. 除了使用 RFID 实现定位机制之外,一些研究者开始关注基于 RFID 定位信息的查询技术研究. 文献[55]提出了一种新颖的 RFID 系统框架结构,依靠位置相对固定的标签来定位携带移动式阅读器的监控对象,从而支持高效的移动范围查询. 该文提出了此场景下移动对象位置查询的一种概率模型,并给出了有效的定位方法.

5.2 基于 RFID 的移动行为感知

现有的移动行为监测主要是基于摄像头获取视频图像来实现的,此类方案具有如下缺点:(1)感知设备价格昂贵,一些专业摄像头动辄成百上千元;(2)获取数据量大质低,存在大量冗余数据,无法实时抽取信息与有效利用. 研究者们发现,当人体经过 RFID 阅读器天线与标签之间的空间时,由于人体

的能量吸收作用，被人体遮挡的部分标签的反射信号会存在明显的能量衰减现象. 基于上述认识，文献[56]在不需要移动目标附加任何 RFID 标签的前提下利用 RFID 主动标签阵列设计了一套系统，来有效感知目标对象的移动行为并且挖掘频繁的移动轨迹. 该系统提出了一套实用的容错方法，能够抵消周围普遍存在的噪声信号的影响. 文献[57]进一步基于 RFID 标签阵列提出了一套行为感知方案. 与前者不同的是，该方案大量使用了无源的被动标签，结合少量的主动标签来构建感知系统，并且针对被动标签反射信号的抖动问题提出了有效的除噪方案，更为有效地提升了系统的性价比. 总体来说，上述基于 RFID 的移动行为感知方案由于使用了廉价的 RFID 标签，成本非常低廉，具有良好的可扩展性. 此外，该方案能够以一种轻量级的方式提取移动行为的感知信息，避免产生大量冗余数据，从而有效支持感知数据的实时处理.

6　未来研究方向

虽然 RFID 研究已经取得了一定的成果，但是仍有很多问题需要解决. 当前物联网技术快速演进发展的浪潮，也给 RFID 的理论研究与应用带来了新的发展契机，主要体现在如下几个方面：

(1)“跨层优化”的 RFID 数据管理理论与关键技术. “跨层优化”的理念最早来源于无线网络协议栈的优化设计，其核心思想就是实现两个或更多协议层之间的优化和控制以及相互间信息的交换，从而达到显著改善网络系统性能的目的. 在传感网研究方面，“跨层设计”的思想已经得到了广泛的认可和应用. 然而，由于 RFID 系统设计的简单性以及资源稀缺性，之前很少有研究者提出采用“跨层优化”的思路来研究 RFID 相关的问题. 我们认为，RFID 系统稀缺计算存储资源，物理通信环境中普遍存在噪声、信号干扰以及能量吸收对数据传输的影响，提出了“跨层优化”的必要性，同时也使得“跨层优化”的实现难度进一步提升. 一方面，如果没有引入“跨层优化”来充分考虑各层次之间的影响，相应的理论研究成果很难在实际的应用环境下达到预期的性能；另一方面，稀缺的资源限制使得我们必须要考虑研究轻量级的协议或算法来实现“跨层优化”的目的. 因此，在真实环境下，如何根据物理层传输性状的变化来实现 MAC 层防冲突算法的参数优化，提供快速高效的 RFID 识别机制，是一个值得研究的问题. 针对应用层对数据分析与挖掘的需求，如何利用现有 MAC 层防冲突机制所体现出的有规则的概率分布性，避免无效数据的传输，实现高效的数据处理机制，都是需要进一步研究的问题.

(2) 基于 RFID 物理层特性的轻量级安全与隐私保障机制. 由于 RFID 标签上的计算资源极其有限，无法像常规无线系统一样使用非对称密钥来保障私密性和安全性，从而给 RFID 系统的安全保障带来了极大的困难. 然而，RFID 系统所具有的一些特殊物理属性使得实现更为可靠的轻量级安全与隐私保障机制成为可能. 例如，由于 RFID 标签具有基于能量反射方式通信的特性，使其在物理层的通信存在邻近效应，即只有在阅读器临近范围内的 RFID 标签才能够被实时的访问和读取. 此外，RFID 在物理层通信的信号特征可以用来构造“物理单向函数”：利用物理层的一些特质(如物理信号)来实现类似于 Hash 单向函数的一些性质. 因此，如何利用物理层的邻近效应来有效保障隐私，是一个值得研究的问题. 如何利用“物理单向函数”设计出轻量级的认证算法来识别伪造标签，也是需要进一步研究的问题.

(3) 实际环境下 RFID 系统的优化部署方案. 考虑到真实传输环境中多种因素对系统性能指标的影响，迫切需要研究 RFID 系统在实际环境下的优化部署方案，包括 RFID 阅读器的功率调整、阅读器天线的全方位立体部署、RFID 标签的冗余部署等方案. 具体来说，实际应用情况下由于种种原因总是存在一些死角使得 RFID 标签无法被快速有效地识别. 针对上述问题，如何有效地调整阅读器功率并且合理规划多个天线的部署方案，来尽可能避免识别死角的存在，同时提升并发读取效率，值得研究者们去深入探讨. 此外，通过在单一目标对象上部署多个标签，这样在仅需识别其中一个标签的情况下就能有效识别目标对象信息. 在上述情况下，如何部署合适粒度的冗余标签，在避免死角的前提下有效确保识别效率，也是需要进一步研究的问题.

(4) RFID 应用模式的探索与研究. 由于 RFID 最初的设计目的是用来标识物品，当前 RFID 技术的主流应用还停留在供应链中对货物进行跟踪、管理及监控方面. 如今，RFID 正以独特的优势，逐渐被广泛应用于方方面面，例如防伪、动物识别、反偷窃系统、资产管理、食物药品安全等. 事实上，能否有效地将 RFID 推广到新型的应用中取决于能否结合 RFID 的特性来对其可行的应用模式进行思考. 对

RFID 应用模式的深入探讨主要包括两个层面：以低成本的方式替代现有模式以及探索创新的应用模式. 例如，除了能标识物体之外，RFID 标签自身就是一个小型无线节点，其物理层的传输特性参数如 RSSI、编码方式等为定位、追踪、认证一类的应用模式提供了技术准备；RFID 标签用户区存储空间能够支持 512 bit 以上的存储容量，通常情况下可以存储 32 个以上的汉字或英文字符，在支持索引号的情况下可以存储更多的信息，这就为物联网环境下的信息检索、查询类的智能应用提供了有效保障.

7 总 结

作为物联网的一项关键技术，RFID 在近几年得到了广泛的关注与研究. 本文关注于 RFID 的数据管理问题，从算法、协议以及性能评测 3 个方面出发，分别从 RFID 的标签识别协议与防冲突算法、认证与隐私保护机制以及真实环境下系统的性能评测与分析等方面阐述和分析了 RFID 领域的研究进展. 在此基础上总结并展望了 RFID 未来的研究方向. 总体来说，RFID 数据管理与传统的分布式数据管理不同，后者主要关注于分布式的数据分片存储以及查询优化处理，RFID 数据管理更侧重于物理层、MAC 层与应用层之间的高效耦合，来提升 RFID 数据管理的整体性能；同时，RFID 数据管理与传感器网络的数据管理也存在区别，后者主要关注于对感知数据的网内处理与存储以实现高效节能性，RFID 数据管理则更侧重于对 RFID 标签实现快速、可靠的信息收集与统计，以便有效减少扫描时延并确保鲁棒性.

参 考 文 献

[1] Myung J, Lee W, Jaideep S. Adaptive binary splitting for efficient RFID tag anti-collision. IEEE Communications Letters, 2006, 10(3): 144-146

[2] Pan L, Wu H. Smart trend-traversal: A low delay and energy tag arbitration protocol for large RFID systems//Proceedings of the 28th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'09). Rio de Janeiro, Brazil, 2009: 2571-2575

[3] Maguire Y, Pappu R. An optimal Q-algorithm for the ISO 18000-6C RFID protocol. IEEE Transactions on Automation Science and Engineering, 2009, 6(1): 16-24

[4] Zhen B, Kobayashi M, Shimuzu M. Framed ALOHA for multiple rfid objects identification. IEICE Transactions on Communications, 2005, 88-B(3): 991-999

[5] Schoute F. Dynamic frame length ALOHA. IEEE Transactions on Communications, 1983, 31(4): 565-568

[6] Floerkemeier C. Bayesian transmission strategy for framed aloha based RFID protocols//Proceedings of the IEEE International Conference on RFID. Grapevine, USA, 2007: 228-235

[7] Vogt H. Efficient object identification with passive RFID tags//Proceedings of the 1st International Conference on Pervasive Computing. Zurich, Switzerland, 2002: 98-113

[8] Lee S, Joo S, Lee C. An enhanced dynamic framed slotted ALOHA algorithm for rfid tag identification//Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05). San Diego, USA, 2005: 166-172

[9] Tang S, Yuan J, Li X Y, Chen G, Liu Y, Zhao J. Raspberry: A stable reader activation scheduling protocol in multi-reader RFID systems//Proceedings of the 17th IEEE International Conference on Network Protocols. Princeton, USA, 2009: 304-313

[10] Yang L, Han J, Qi Y, Wang C, Gu T, Liu Y. Season: Shelving interference and joint identification in large-scale RFID systems//Proceedings of the 30th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'11). Shanghai, China, 2011: 3092-3100

[11] Sheng B, Li Q, Mao W. Efficient continuous scanning in RFID systems//Proceedings of the 29th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'10). San Diego, USA, 2010: 1010-1018

[12] Xie L, Sheng B, Tan C C, Han H, Li Q, Chen D. Efficient tag identification in mobile RFID systems//Proceedings of the 29th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'10). San Diego, USA, 2010: 1001-1009

[13] Kodialam M, Nandagopal T. Fast and reliable estimation schemes in RFID systems//Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom'06). Los Angeles, USA, 2006: 322-333

[14] Chen W. An accurate tag estimate method for improving the performance of an rfid anticollision algorithm based on dynamic frame length ALOHA. IEEE Transactions on Automation Science and Engineering, 2009, 6(1): 9-15

[15] Han H, Sheng B, Tan C C, Li Q, Mao W, Lu S. Counting rfid tags efficiently and anonymously//Proceedings of the 29th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'10). San Diego, USA, 2010: 1028-1036

[16] Chen Q, Ngan H, Liu Y, Ni L. Cardinality estimation for large-scale RFID systems. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(9): 1441-1454

[17] Chen Q, Liu Y, Ngan H, Ni L. ASAP: Scalable identification and counting for contactless RFID systems//Proceedings of the 30th IEEE International Conference on Distributed Computing Systems (ICDCS'10). Genova, USA, 2010: 52-61

[18] Sheng B, Tan C C, Li Q, Mao W. Finding popular categories for RFID tags//Proceedings of the 9th ACM Interational

Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'08). Hong Kong, China, 2008: 159-168

[19] Kodialam M, Nandagopal T, Lau W. Anonymous tracking using RFID tags//Proceedings of the 26th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'07). Anchorage, USA, 2007: 1217-1225

[20] Li T, Chen S, Ling Y. Identifying the missing tags in a large RFID system//Proceedings of the 11th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'10). Chicago, USA, 2010: 1-10

[21] Qiao Y, Chen S, Li T, Chen S. Energy-efficient polling protocols in RFID systems//Proceedings of the 12th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'11). Paris, France, 2011: 25

[22] Chen S, Zhang M, Xiao B. Efficient information collection protocols for sensor-augmented RFID networks//Proceedings of the 30th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'11). Shanghai, China, 2011: 3101-3109

[23] Yang L, Han J, Qi Y, Liu Y. Identification-free batch authentication for RFID tags//Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP'10). Kyoto, Japan, 2010: 154-163

[24] Zheng Y, Li M. Fast tag searching protocol for large-scale RFID systems//Proceedings of the 19th IEEE International Conference on Network Protocols (ICNP'11). Vancouver, Canada, 2011: 363-372

[25] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications//Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'02). Redwood Shores, USA, 2002: 454-469

[26] Inoue S, Yasuura H. RFID privacy using user-controllable uniqueness//Proceedings of the RFID Privacy Workshop. MIT, USA, 2003

[27] Lim T, Li T, Yeo S. A cross-layer framework for privacy enhancement in RFID systems. Pervasive and Mobile Computing, 2008, 4(6): 889-905

[28] Juels A, Rivest R L, Szydlo M. The blocker tag: Selective blocking of RFID tags for consumer privacy//Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03). Washington, USA, 2003: 103-111

[29] Juels A. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394

[30] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data//Proceedings of the IEEE Symposium on Security and Privacy (S&P'00). Berkeley, USA, 2000: 44-55

[31] Wang S, Ding X, Deng R H, Bao F. Private information retrieval using trusted hardware//Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS'06). Hamburg, Germany, 2006: 49-64

[32] Yang Z, Zhong S, Wright R N. Privacy-preserving queries on encrypted data//Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS'06). Hamburg, Germany, 2006: 479-495

[33] Tan C C, Li Q, Xie L. Privacy protection for RFID-based tracking systems//Proceedings of the IEEE International Conference on RFID. Orlando, USA, 2010: 53-60

[34] Poschmann A, Leander G, Schramm K, Paar C. New lightweight crypto algorithms for RFID//Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'07). New Orleans, USA, 2007: 1843-1846

[35] Hong D, Sung J, Hong S, Lim J, Lee S, Koo B, Lee C, Chang D, Lee J, Jeong K, Kim H, Kim H, Chee S. HIGHT: A new block cipher suitable for low-resource device//Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'06). Yokohama, Japan, 2006: 46-59

[36] Sarma S E, Weis S A, Engels D W. Radio frequency identification: Secure risks and challenges. RSA Laboratories Cryptobytes, 2003, 6(1): 2-9

[37] Weis S A, Sarma S E, Rivest R L, Engels D W. Security and privacy aspect s of low-cost radio frequency identification systems//Proceedings of the 1st International Conference on Security in Pervasive Computing (SPC'03). Boppard, Germany, 2003: 201-212

[38] Ohkubo M, Suzuki K, Kinoshita S. Hash chain based forward secure privacy protection scheme for low cost RFID//Proceedings of the Symposium on Cryptography and Information Security (SCIS'04). Sendai, Japan, 2004: 719-724

[39] Zhou Yong-Bin, Feng Deng-Guo. Design and analysis of cryptographic protocols for RFID. Chinese Journal of Computers, 2006, 29(4): 581-589(in Chinese)
(周永彬，冯登国. RFID 安全协议的设计与分析. 计算机学报，2006，29(4)：581-589)

[40] Zhang Fan, Sun Xuan, Ma Jian-Feng, Cao Chun-Jie, Zhu Jian-Ming. A universally composable secure RFID communication protocol in supply chains. Chinese Journal of Computers, 2008, 31(10): 1754-1767(in Chinese)
(张帆，孙璇，马建峰，曹春杰，朱建明. 供应链环境下通用可组合安全的 RFID 通信协议. 计算机学报，2008，31(10)：1754-1767)

[41] Rieback M, Crispo B, Tanenbaum A. RFID guardian: A battery-powered mobile device for RFID privacy management//Proceedings of the Australasian Conference on Information Security and Privacy ACISP'05. Brisbane, Australia, 2005: 184-194

[42] Mirowski L, Hartnett J. Deckard: A system to detect change of RFID tag ownership. International Journal of Computer Science and Network Security, 2007, 7(7): 89-98

[43] Thamilarasu G, Sridhar R. Intrusion detection in RFID systems//Proceedings of the IEEE International Conference Military MILCOM. San Diego, USA, 2008: 1-7

[44] Kawakita Y, Mitsugi J. Anti-collision performance of Gen2 air protocol in random error communication link//Proceedings of the International Symposium on Applications and the Internet Workshops. Phoenix, USA, 2006: 68-71

[45] Buettner M, Wetherall D. An empirical study of UHF RFID performance//Proceedings of the 14th Annual International

Conference on Mobile Computing and Networking (MobiCom'08). San Francisco, USA, 2008: 223-234

[46] Aroor S R, Deavours D D. Evaluation of the state of passive UHF RFID: An experimental approach. IEEE Systems Journal, 2007, 1(2): 168-176

[47] Ramakrishnan K M, Deavours D D. Performance benchmarks for passive UHF RFID tags//Proceedings of the 13th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems (MMB'06). Nürnberg, Germany, 2006: 1-18

[48] Jeffery S R, Garofalakis M, Franklin M J. Adaptive cleaning for RFID data streams//Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB'06). Seoul, Korea, 2006: 163-174

[49] Xu X, Gu L, Wang J, Xing G. Negotiate power and performance in the reality of RFID systems//Proceedings of the 8th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'10). Mannheim, Germany, 2010: 88-97

[50] Xu X, Gu L, Wang J, Xing G, Cheung S. Read more with less: An adaptive approach to energy-efficient RFID systems. IEEE Journal on Selected Areas in Communications, 2011, 29(8): 1684-1697

[51] Su W, Alchazidis N, Ha T T. Multiple RFID tags access algorithm. IEEE Transactions on Mobile Computing, 2010, 9(2): 174-187

[52] Wang Hong-Gang, Pei Chang-Xing, Yi Yun-Hui. Energy efficient physical layer design for passive RFID system. Chinese Journal of Computers, 2009, 32(7): 1356-1364(in Chinese)
(王宏刚，裴昌幸，易运晖. 无源 RFID 系统中能量有效的物理层设计. 计算机学报，2009，32(7)：1356-1364)

[53] Hightower J, Borriello G, Want R. SpotON: An indoor 3D location sensing technology based on RF signal strength. University of Washington, Seattle: Technical Report UW CSE 2000-02-02, 2000

[54] Ni L, Liu Y, Lau Y, Abhishek P. LANDMARC: Indoor location sensing using active RFID. Wireless Networks, 2004, 10(6): 701-710

[55] Gu Yu, Guo Na, Yu Ge. Study on processing probabilistic RFID spatial range query based on mobile readers. Chinese Journal of Computers, 2009, 32(10): 2052-2065(in Chinese)
(谷峪，郭娜，于戈. 基于移动阅读器的 RFID 概率空间范围查询技术的研究. 计算机学报，2009，32(10)：2052-2065)

[56] Liu Y, Chen L, Pei J, Chen Q, Zhao Y. Mining frequent trajectory patterns for activity monitoring using radio frequency tag arrays//Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'07). New York, USA, 2007: 37-46

[57] Zhang D, Zhou J, Guo M, Cao J, Li T. TASA: Tag-free activity sensing using RFID tag arrays. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(4): 558-570

XIE Lei, born in 1982, Ph. D., assistant professor. His research interests include sensor networks, RFID systems, vehicular networks and high performance computing.

YIN Ya-Feng, born in 1989, Ph. D. candidate. Her research interests focus on RFID.

CHEN Xi, born in 1988, M. S. candidate. His research interests focus on RFID.

LU Sang-Lu, born in 1970, Ph. D., professor, Ph. D. supervisor. Her research interests include distributed computing, pervasive computing, and wireless networks.

CHEN Dao-Xu, born in 1947, professor, Ph. D. supervisor. His research interests include distributed computing, parallel processing, and computer networks.

Background

This work is partially supported by the National Natural Science Foundation of China under Grant Nos. 61100196, 61073028, 61021062; the National Basic Research Program (973 Program) of China under Grant No. 2009CB320705; the Jiangsu Natural Science Foundation under Grant No. BK2011559.

As the rapid development of technologies for Internet of Things, RFID becomes an emerging technology and expects to grow up in an accelerated pace. In recent years, a great number of researchers have paid much attention to the area of RFID, and have focused on some issues from the anti-collision algorithms, security and privacy-preserving protocol, performance evaluation in realistic settings, etc. However, a lot of issues in this area still have not been addressed well, and many new challenges have been raised. Therefore, focusing on RFID data management, the authors conduct a survey on research progresses in algorithms, protocols and performance evaluation of RFID, and provide a summary of future research issues.