·安全技术· 文章编号：1000-3428(2016)01-0133-05 文献标识码：A 中图分类号：TP393.08

一种快速检测 RFID 丢失标签的方法

梁雪萍[1,2]，马存庆[1,2]，梁颖升[1,2]

（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学，北京 100049）

摘 要： 在时间敏感的大规模射频识别技术（RFID）应用中，为快速地检测出集合中丢失的标签，提出一种基于迭代识别的 RFID 丢失标签检测方法。通过对多轮检测过程中的历史检测信息进行迭代识别，挖掘帧时隙 ALOHA 中空时隙、单响应时隙和碰撞时隙中的信息，使得每一轮检测出存在或者丢失的标签数量明显增加，从而提高整体的检测效率。实验结果证明，相比 IIPS-CM 协议，在不同的丢失率和丢失数量下，该方法都能降低丢失 RFID 标签的平均检测时间，其检测效率也具有较好的稳定性，不随丢失标签数量变化而变化。

关键词： 时间敏感；丢失标签；帧时隙 ALOHA；历史信息；迭代识别；快速检测

中文引用格式： 梁雪萍，马存庆，梁颖升. 一种快速检测 RFID 丢失标签的方法[J]. 计算机工程，2016，42(1)：133-137.

英文引用格式： Liang Xueping，Ma Cunqing，Liang Yingsheng. A Fast Detection Method for RFID Missing Tag[J]. Computer Engineering，2016，42(1)：133-137.

A Fast Detection Method for RFID Missing Tag

LIANG Xueping[1,2]，MA Cunqing[1,2]，LIANG Yingsheng[1,2]

（1. Institute of Information Engineering，Chinese Academy of Sciences，Beijing 100093，China；
2. University of Chinese Academy of Sciences，Beijing 100049，China）

【Abstract】 Due to its low cost and convenience，Radio Frequency Identification（RFID） technology is widely deployed in social life. In time-sensitive large-scale RFID applications，efficient RFID missing tag detection is a key problem. Based on analysis on recent research，a detection method based on iterative update is proposed. The method makes use of history information in each round，and acquires more information in empty slot，singleton slot and collision slot to identify more existing or missing tags，which improves the efficiency of detection. Compared with IIPS-CM protocol，it achieves higher performance as well as good stability under various rates，and does not change the number of missing tags.

【Key words】 time-sensitive；missing tag；framed slotted ALOHA；history information；iterative recognition；fast detection

DOI： 10.3969/j.issn.1000-3428.2016.01.024

1 概述

射频识别（Radio Frequency Identification，RFID）技术是一种非接触式自动识别技术[1]，具有成本低、自动、准确和便捷的特点[2]。RFID 技术还能穿透非金属材料，适应恶劣的工作环境[3]，因此，大量应用到日常生产生活中的很多方面，比如门禁系统、物流管理、仓储系统、医疗安全、供应链管理、智能交通、人员监管和防伪识别等[4-5]。RFID 应用系统一般包括 3 个部分：读写器，标签和服务器。读写器可以与标签交换数据，也可以与后台服务器进行交互验证。标签按照能量供应方式的不同可以分为 3 类：主动式标签，半主动式标签和被动式标签[6]。主动式标签进行内部工作和射频通信都具有独立的能量供应，半主动式标签进行内部工作具有独立能量供应而射频通信时需要耦合能量，被动式标签只能通过耦合能量进行内部工作和射频通信。标签可以存储信息，接收并响应读写器发送的数据。

随着 RFID 技术的普及，RFID 应用系统越来越多，规模也越来越大，单个系统中 RFID 标签的数量可以达到上万级别（大型超市中的标签数目可能达到几十万甚至上百万[7]）。出于成本方面的考虑，大规模 RFID 应用系统中通常采用被动式 RFID 标签，其计算和存储能力受限。在时间敏感的 RFID 应用

基金项目： 国家自然科学基金资助项目（61402470/F020705）；国家“863”计划基金资助项目（2012AA013104，2013AA01A214）；国家“973”计划基金资助项目（2014CB340603）；中国科学院战略先导专项基金资助项目（XDA06010702）。

作者简介： 梁雪萍（1990－），女，博士研究生，主研方向为网络与信息系统安全；马存庆，助理研究员、博士；梁颖升，博士研究生。

收稿日期： 2014-11-18 **修回日期：** 2014-12-22 **E-mail：** xpliang13@lois.cn

系统中,如何高效地检测 RFID 标签集合,发现其中丢失的 RFID 标签,成为一个关键问题。例如在仓库管理中,每个货物都附着一个具有唯一 ID 的标签,工作人员使用读写器对标签进行扫描,跟踪库存信息,包括库存总量以及货物的实时变动。对于检测货物的丢失情况而言,越早发现货物的丢失,越能减少不必要的损失。例如对于每一个标签来说,如果检测时间都减少 0.01 s,那么检测 10 000 个标签,所需的总时间代价就可以减少 100 s。所以在时间敏感的大规模 RFID 应用中,如何快速地检测 RFID 标签集合,发现其中丢失的 RFID 标签是非常重要的。

针对在时间敏感的大规模 RFID 应用中丢失 RFID 标签的检测问题,本文在 RFID 标签检测中常用的帧时隙 ALOHA 框架[8]下,提出一种基于迭代识别的快速检测方法。通过对多轮检测过程中的历史信息进行临时存储和迭代识别,充分挖掘空时隙、单响应时隙和碰撞时隙中隐含的信息,使得每一轮检测出的存在或丢失的标签数量明显增加,从而提高整体的检测效率,并减少发现丢失 RFID 标签的平均时间。

2 背景知识

识别 RFID 应用系统中丢失的 RFID 标签,一般需要检测出所有 RFID 标签的状态(存在或者丢失)。因而,快速检测丢失的 RFID 标签即需要快速地检测 RFID 标签集合。在具有 N 个标签的 RFID 应用系统中,应用服务器存储着所有 RFID 标签的 ID 信息,假设所有的 RFID 标签都是被动型标签,都会正常地响应读写器的命令。

最基本的检测方法“点名”(一问一答),即应用服务器通过读写器,向所有 RFID 标签广播 ID(时间消耗为 T_{ID}),具有该 ID 的 RFID 标签进行响应(时间消耗为 T_R)。如果应用服务器通过读写器收到 RFID 标签响应,那么该标签存在,否则丢失。点名方法总时间消耗为 $N\times(T_{\mathrm{ID}}+T_R)$,检测单个 RFID 标签的平均时间为($T_{\mathrm{ID}}+T_R$)。

最理想的检测方法是“报数”(一问多答),即应用服务器通过读写器,向所有 RFID 标签广播报数命令(时间消耗为 T_C),在之后的 N 个时隙内,N 个 RFID 标签依次响应。服务器查看每一个报数时隙内的响应情况,从而可以判定相应的 RFID 标签是否存在。报数方法的总时间消耗为($T_C+N\times T_R$),检测单个 RFID 标签的平均时间近似为 T_R,远小于点名检测方法。

事实上,RFID 应用系统中的 RFID 标签数量是变化的,其 ID 取值通常很大并且不连续。为了实现上述报数方法,需要将这些 ID 映射到一个连续的且元素取值较小的空间内。通常采用散列函数实现上述映射,但由于散列函数不能完全避免冲突,即不能实现一一映射,因此 RFID 标签响应时也会发生碰撞[9],导致读写器无法识别,因而无法实现上述理想的报数检测方法。现有的 RFID 标签检测方法只能尽可能接近理想的报数方法,通常需要通过多轮的报数过程才能完全检测出全部 RFID 标签的状态。

帧时隙 ALOHA 是一种基于报数原理的典型框架。应用服务器通过读写器向 RFID 标签发送帧长度 f 和随机数 r;RFID 标签根据收到的(f,r)和自身 ID,计算 $s=H(ID,r)\bmod f$(H 为散列函数,mod 为模运算)并在第 s 个时隙内发送响应;应用服务器分析比较 f 个时期内预期的响应情况和通过读写器收集到的实际响应情况来判断相应的 RFID 标签是否丢失。相比于另一类基于树形结构的检测方法[10-11],此类基于 ALOHA 的方法具有更高的检测效率,因而广泛应用于大规模 RFID 应用系统中。

3 相关研究

对于国内外已有的丢失 RFID 标签检测研究,按照检测结果的确定程度,检测方法可以分为确定型和概率型 2 类。确定型方法[10-12]以 100% 的概率确定标签是否丢失,而概率型方法[13]以小于 100% 的概率确定标签是否丢失。

文献[13]提出了可信读写器协议(Trusted Reader Protocol,TRP),但只能以概率 α 判定 n 个标签中是否有多于 m 个标签丢失,而不能确定出丢失标签的数量及 ID 信息,不适用于需要明确丢失标签详细信息的应用场景。文献[12]提出 5 种检测协议,其中的迭代无标识协议(Iterative ID-free Protocol,IIP)检测每个 RFID 标签的平均时间为0.86 ms。文献[8]提出在分布式应用中,多个读写器在应用服务器的控制下进行独立的、并行的检测过程,但其协议都存在需要估算丢失标签数量和采用固定帧长度等问题。

文献[14]分析发现了 IIP 协议检测效率随丢失率(丢失 RFID 标签所占比例)升高而下降的问题,提出具有稳定检测效率的 IIPS 协议,并进一步基于对丢失率的动态计算,提出 IIPS-CM 协议和 IIPS-CP 协议,其检测效率随丢失率升高而提高。例如,0.1% 的低丢失率下丢失 RFID 标签的平均检测时间为 0.86 ms,而 80% 的高丢失率下平均检测时间约为 0.62 ms。其中 IIPS-CM 协议对丢失率的计算更为稳定,其检测效率也相对更稳定。文献[7]提出对主动式标签的快速检测方法。

本文重点研究在时间敏感的 RFID 应用系统中丢失 RFID 标签的确定型检测方法。针对大规模的

被动型 RFID 标签集合,尽可能挖掘更多的标签状态信息,减少 RFID 标签的平均检测时间,从而快速识别出丢失的 RFID 标签。

4　历史检测信息的迭代识别

在现有的基于帧时隙 ALOHA 的丢失 RFID 标签检测方法中[13-14],通常只考虑了本轮检测过程中获取到的信息,即在每一轮执行过程中,根据本轮各个时隙的状态识别存在或丢失的标签。而当开始执行下一轮时,一般只保留了上一轮结束后已经识别出存在的标签和丢失标签的集合,其他信息(例如每个时隙的状态)通常都会被舍弃。事实上,从这些被丢弃的信息中,可以进一步提取出更多 RFID 标签的状态信息,从而提高检测效率。

对历史信息进行迭代识别的场景如下:

(1)第 M 轮检测,预期某时隙中标签 i、标签 j 都响应,实际上也检测到响应,但无法确定是标签 i 还是标签 j 进行了响应;第 $N(N>M)$ 轮检测,如果判断出标签 i 存在,那么迭代到第 M 轮中即可判定标签 j 丢失。

(2)第 M 轮检测,预期某时隙中标签 i、标签 j 都响应,实际上也检测到响应,但无法确定是标签 i 还是标签 j 进行了响应;第 $N(N>M)$ 轮检测,如果判断出标签 i 丢失,那么迭代到第 M 轮中即可判定标签 j 存在。

通过利用历史信息,能够从每一轮检测中获取更多 RFID 标签存在或丢失的信息,从而减少协议执行的轮次。迭代识别的过程在高性能的应用服务器实现,这些简单运算的时间消耗可以忽略。

迭代识别历史检测信息的详细过程为:应用服务器保存每一轮的帧长度、随机数、每个时隙的状态和其他信息。当第 i 轮协议执行结束后,利用新的识别结果对历史检测结果进行迭代识别,即从第 1 轮开始再次开始检测,一直到第 i 轮,然后再次从第 1 轮检测到第 i 轮,直到对第 i 轮连续两次检测都没有识别出新的存在或者丢失的 RFID 标签为止。

5　丢失 RFID 标签的快速检测方法

针对已有研究中检测效率最高的 IIPS-CM 协议,本文基于多轮执行的帧时隙 ALOHA 框架,提出一种对历史检测信息进行迭代识别的快速检测方法。应用服务器需要维护 4 类集合:第 i 轮开始时的未识别标签集合 S_{U_i},已识别为存在但未被停止的标签集合 S_{P_i},已识别出丢失的标签集合 S_{A_i}和已识别为存在且被停止的标签集合 S_{S_i}。初始状态时,集合 S_{U_1} 中为数据库中所有的标签,而集合 S_{P_1},S_{A_1} 和 S_{S_1} 为空。第 i 轮协议的执行过程如下:

(1)读写器选择最优帧长度 f_i,并生成随机数 r_i,同时计算向量 $[\boldsymbol{u}_s]_{f_i}$ 和向量 $[\boldsymbol{p}_s]_{f_i}$,分别表示第 s 个时隙内预期收到的来自集合 S_{U_i} 和 S_{P_i} 中标签的响应数量;读写器将参数 f_i,r_i 和预期帧状态向量(f_i 比特,表明每个时隙是否为碰撞时隙)发送到其覆盖范围内的所有标签。

(2)每个标签计算出自己应该进行响应的时隙位置 $s=H(ID,r_i)\bmod f_i$。如果该时隙为碰撞时隙,再计算 $H'(ID,r_i)$,并以一定的概率(通常为 50%)确定是否在该时隙内进行响应。

(3)读写器开始从 0 到 f_i-1 个时隙的计时,标签在对应的时隙内发送响应消息。

(4)当 f_i 个时隙结束时,应用服务器根据实际标签的响应情况进行分析,可以分为 2 种情况:

1)情况 1(C_1):对于非空时隙 s,如果 $u_s=1$ 且 $p_s=0$,则集合 S_{U_i} 中预期响应的 1 个标签是存在的。

2)情况 2(C_2):对于空时隙 s,如果 $u_s>0$ 且 $p_s=0$,则预期响应的 u_s 个标签是丢失的。

将识别出的存在标签和丢失标签分别放入集合 S_{P_i} 和 S_{A_i} 中,并将其从集合 S_{U_i} 中移除。

(5)应用服务器对历史检测信息进行迭代识别过程。

(6)读写器根据检测结果构造 f_i 比特的停止命令向量,并将该向量广播至其覆盖范围内的所有标签。对于已经识别出存在并且被停止的标签,将其从集合 S_{P_i} 移动到 S_{S_i}。

(7)读写器检查集合 S_{U_i},如果其为空,则检测结束,集合 S_{A_i} 中的 RFID 标签确定丢失;否则,令 $S_{U_{i+1}}=S_{U_i}$,$S_{P_{i+1}}=S_{P_i}$,$S_{A_{i+1}}=S_{A_i}$,$S_{S_{i+1}}=S_{S_i}$,继续进行第 $i+1$ 轮检测过程。

上述检测方法中需要计算出最优的帧长度 f_i。假设 S_{U_i} 和 S_{P_i} 中标签数量分别为 N_{U_i} 和 N_{P_i},某时隙中有 k 个响应来自于 S_{U_i} 或 S_{P_i} 中标签的概率分别是:

$$P_u(k)=\binom{N_{u_i}}{k}\left(\frac{1}{f_i}\right)^k\left(1-\frac{1}{f_i}\right)^{N_{u_i}-k}$$

$$P_p(k)=\binom{N_{p_i}}{k}\left(\frac{1}{f_i}\right)^k\left(1-\frac{1}{f_i}\right)^{N_{p_i}-k}$$

用 $M_u(n,k)$ 和 $M_p(n,k)$ 分别表示预期 n 个来自 S_{U_i} 和 S_{P_i} 中标签的响应中实际收到 k 个的概率,则有:

$$M_u(n,k)=\binom{n}{k}(1-P_{M_i})^k P_{M_i}^{n-k}$$

$$M_p(n,k)=\begin{cases}1 & n=k\\ 0 & n\neq k\end{cases}$$

用 $P_u(z,n,k)$ 和 $P_p(z,n,k)$ 分别表示预期有 n 个响应来自 S_{U_i} 和 S_{P_i} 中的 z 个标签,但实际收到 k 个响应的概率,则有:

$$P_u(z,n,k)=P_u(z)\cdot P_z^n\cdot M_u(n,k)$$

$$P_p(z,n,k)=P_p(z)\cdot P_z^n\cdot M_p(n,k)$$

其中,P_z^n 表示预期会有 z 个标签响应的碰撞时隙中,

经过 50% 的概率转化,实际预期收到 n 个响应的概率。

假设集合 S_{U_i} 中 z_1 个标签和集合 S_{P_i} 中 z_2 个标签同时映射到时隙 s 中,其中预期分别有 n_1 和 n_2 个进行响应,而读写器实际收到 k_1+k_2 个响应的概率(其中 k_1 个来自于集合$S_{U_i}S_{U_i}$)为:

$$P(z_1,n_1,k_1,z_2,n_2,k_2)=P_u(z_1,n_1,k_1)\cdot P_p(z_2,n_2,k_2)$$

那么步骤(4)中的 2 种可以识别的标签存在或者丢失的时隙出现的概率分别为:

$$P(C_1)=\sum_{z_1=1}^{N_{u_i}}\sum_{z_2=0}^{N_{p_i}}P(z_1,1,1,z_2,0,0)$$

$$P(C_2)=\sum_{z_1=1}^{N_{u_i}}\sum_{n_1=1}^{z_1}\sum_{z_2=0}^{N_{p_i}}P(z_1,n_1,0,z_2,0,0)$$

第 i 轮通过帧时隙 ALOHA 方法预期识别出的标签总数量为:

$$\begin{aligned}N_{A_i}&=f_i\Big(\sum_{z_1=1}^{N_{u_i}}\sum_{z_2=0}^{N_{p_i}}P(z_1,1,1,z_2,0,0)+\sum_{z_1=1}^{N_{u_i}}\sum_{n_1=1}^{z_1}\sum_{z_2=0}^{N_{p_i}}P(z_1,n_1,0,z_2,0,0)\cdot n_1\Big)\\&\approx\frac{c_{u_i}\rho_i f_i}{2}\left(e^{-\rho_i}+e^{-\frac{\rho_i}{2}}(1-P_{M_i})+P_{M_i}e^{-\frac{(1-c_{u_i}P_{M_i})\rho_i}{2}}\right)\end{aligned}$$

其中,ρ_i 为负载因子,即待检测的标签总数与帧长度的比值;P_{M_i}为丢失率,即丢失标签与待检测标签的比值。令 $F(\rho_i)=c_{u_i}\rho_i\left(e^{-\rho_i}+e^{-\frac{\rho_i}{2}}(1-P_{M_i})+P_{M_i}e^{-\frac{(1-c_{u_i}P_{M_i})\rho_i}{2}}\right)$,第 i 轮中读写器与标签通信的总时间消耗为:

$$T_i=f_i\times t_s+2\left\lceil\frac{f_i}{96}\right\rceil\times t_{\text{tag}}\approx 0.45f_i$$

出于公式推导需要,忽略步骤(5)中检测出的存在或者丢失的标签数量,则单个标签的平均检测时间为:

$$T_{A_i}\approx\frac{T_i}{N_{A_i}}\approx\frac{0.45f_i}{\frac{1}{2}f_iF(\rho_i)}=\frac{0.9}{F(\rho_i)}$$

为使平均时间 T_{A_i}取最小值,应使 $F(\rho_i)$取最大值。根据数值方法,可以计算出最优帧长 f_i。

6 仿真实验与结果分析

为了对比分析 IIPS-CM 协议和本文方法在不同标签丢失率和丢失数量下的执行效率,设计了 2 个实验进行仿真分析。根据 Philp I-Code 系统[15],读写器向标签发送一个长为 96 bit 的 ID 消息需要 2.4 ms(即 $t_{\text{tag}}=2.4$ ms),RFID 标签向读写器发送短响应消息的时间为 0.4 ms(即 $t_s=0.4$ ms)。每一个实验数据都是 20 次实验结果的平均值。

实验 1 假设待检测标签总数为 10 000 个,标签集合的丢失率从 0 增加至 90%,分别使用 IIPS-CM 协议和本文方法进行仿真。

通过 2 种方案的对比,即可得出迭代优化的算法性能,2 种方案的平均检测时间曲线如图 1 所示。

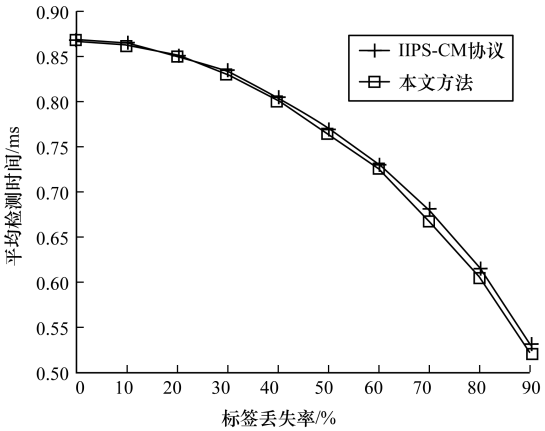

图 1 不同丢失率下平均检测时间对比

通过对比可以发现,本文方法在不同的丢失率情况下基本都能实现平均检测时间的减少,即具有更高的检测效率。特别是在丢失率比较高的情况下,效果更为显著。

实验 2 假设丢失率为 80%,通过调整标签总数改变丢失标签的数量,对比 2 种方案的检测效率。其次,假设丢失率为 0.1%,进行类似实验。

图 2 和图 3 为 2 项实验平均检测时间的曲线图。

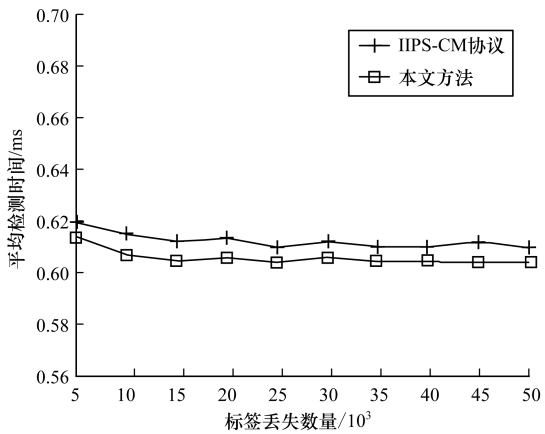

图 2 不同丢失数量下(丢失率 80%)平均检测时间对比

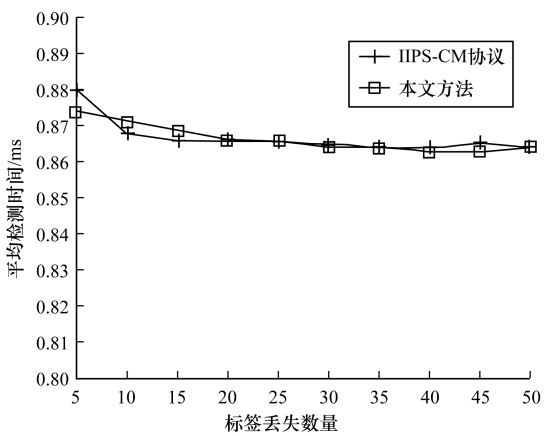

图 3 不同丢失数量下(丢失率 0.1%)平均检测时间对比

由实验结果可以看出,当丢失率为 80% 时,本文方法的检测效率均高于 IIPS-CM 协议;当丢失率为 0.1% 时,2 种方法检测效率差别不大。在相同丢失率的情况下,本文方法的检测效率是稳定的,不随丢失标签数量变化而变化。

综上分析,在不同的标签丢失率和丢失数量下,本文方法中单个标签的平均检测时间减少,具有更高的检测效率,且检测性能具有较好的稳定性。

7　结束语

通过对历史检测信息进行迭代识别,本文提出一种丢失 RFID 标签的快速检测方法。实验结果证明,相比于已知最高检测效率的 IIPS-CM 协议,本文方法具有更高的性能。下一步工作将探索如何进一步提高丢失 RFID 标签检测方法的效率。

参考文献

[1] 颜　元,武岳山,熊立志. RFID 系统多标签碰撞检测方法探索与测试[J]. 移动通信,2011,35(15):35-39.

[2] 刘　丹,魏　鹏,谭　杰,等. 一种 RFID 多标签碰撞检测方法[J]. 小型微型计算机系统,2009,30(9):1890-1894.

[3] 胡玲敏. RFID 系统的防碰撞算法研究[D]. 杭州:杭州电子科技大学,2012.

[4] Luo Wen, Chen Shigang, Qiao Yan, et al. Missing-tag Detection and Energy-time Tradeoff in Large-scale RFID Systems with Unreliable Channels [J]. IEEE/ACM Transactions on Networking, 2014, 22(4): 1079-1091.

[5] Khanam S, Mahbub M, Mandal A, et al. Improvement of RFID Tag Detection Using Smart Antenna for Tag Based School Monitoring System [C]//Proceedings of International Conference on Electrical Engineering and Information & Communication Technology. Washington D. C., USA: IEEE Press, 2014: 1-6.

[6] Chawla V, Dong Sam-Ha. An Overview of Passive RFID[J]. IEEE Communications Magazine, 2007, 45(9): 11-17.

[7] 张士庚,刘光亮,刘　璇,等. 大规模 RFID 系统中一种能量有效的丢失标签快速检测算法[J]. 计算机学报,2014,37(2):434-444.

[8] Zhang Rui, Liu Yunzhong, Zhang Yanchao, et al. Fast Identification of the Missing Tags in a Large RFID System [C]//Proceedings of the 8th Annual Communication Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks. Washington D. C., USA: IEEE Press, 2011: 278-286.

[9] 刘金艳,冯全源. 无线射频识别多标签防碰撞算法综述[J]. 计算机集成制造系统,2014,20(2):440-451.

[10] 周　清. 射频识别(RFID)技术中防碰撞算法的研究[D]. 无锡:江南大学,2012.

[11] 吴　楠. 一种树型结构的 RFID 防碰撞算法研究[D]. 长春:吉林大学,2014.

[12] Li Tao, Chen Shigang, Ling Yibei. Identifying the Missing Tags in a Large RFID System [C]//Proceedings of the 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York, USA: ACM Press, 2010: 1-10.

[13] Tan C C, Sheng Bo, Li Qun. How to Monitor for Missing RFID Tags[C]//Proceedings of the 28th International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2008: 295-302.

[14] Ma Cunqing, Lin Jingqiang, Wang Yuewu. Efficient Missing Tag Detection in a Large RFID System[C]// Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK: [s. n.], 2012: 185-192.

[15] NXP Semiconductors. I-code Smart Label RFID Tags[EB/OL]. (2004-01-30). http://www.nxp.com/documents/data_sheet/SL092030.pdf.

编辑　顾逸斐

(上接第 132 页)

[17] 刘长龙,赵毅强,史亚峰,等. 基于侧信道分析的硬件木马建模与优化[J]. 华中科技大学学报:自然科学版,2013,41(2):53-57.

[18] 张　鹏,王新成,周　庆. 基于电磁辐射信号分析的芯片硬件木马检测[J]. 电子学报,2013,42(2):341-346.

[19] Kumar P, Srinivasan R. Detection of Hardware Trojan in SEA Using Path Delay [C]//Proceedings of IEEE Conference on Electrical, Electronics and Computer Science. Washington D. C., USA: IEEE Press, 2014: 1-6.

[20] Li J, Lach J. At-speed Delay Characterization for IC Authentication and Trojan Horse Detection [C]// Proceedings of IEEE International Workshop on Hardware-oriented Security and Trust. Washington D. C., USA: IEEE Press, 2008: 8-14.

[21] Chakraborty R S, Bhunia S. Security Against Hardware Trojan Attacks Using Key-based Design Obfuscation[J]. Journal of Electronic Testing, 2011, 27(6): 767-785.

[22] Schrittwieser S, Katzenbeisser S, Kieseberg P, et al. Covert Computation——Hiding Code in Code Through Compile-time Obfuscation[J]. Computers & Security, 2014, 42(1): 13-26.

[23] Xiao K, Tehranipoor M. BISA: Built-in Self-authentication for Preventing Hardware Trojan Insertion[C]//Proceedings of IEEE International Workshop on Hardware-oriented Security and Trust. Washington D. C., USA: IEEE Press, 2013: 45-50.

[24] Bhunia S, Abramovici M, Agrawal D, et al. Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution[J]. IEEE Design & Test, 2013, 30(3): 6-17.

[25] Zhang X, Tehranipoor M. RON: An On-chip Ring Oscillator Network for Hardware Trojan Detection[C]// Proceedings of DATE'11. Washington D. C., USA: IEEE Press, 2011: 1-6.

[26] Salmani H, Tehranipoor M, Plusquellic J. A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time[J]. IEEE Transactions on Very Large Scale Integration Systems, 2012, 20(1): 112-125.

编辑　索书志