Journal of Computer Applications
计算机应用,2014,34(1):99 - 103
ISSN 1001-9081
CODEN JYIIDU
2014-01-10
http://www.joca.cn

文章编号:1001-9081(2014)01-0099-05
doi:10.11772/j.issn.1001-9081.2014.01.0099

内嵌安全机制的 RFID 防碰撞策略

李　佳*,郑义平,刘春龙
(广东工业大学 计算机学院,广州 510006)
(*通信作者电子邮箱 rose6263@126.com)

摘　要:当前的射频识别(RFID)系统只是简单地将防碰撞算法和安全机制粗糙地融合在一起。在分析经典自适应动态防碰撞算法的基础上,提出了一种内嵌安全机制的防碰撞策略。该策略将先序遍历机制、布尔运算双向认证协议内嵌入其中,解决了传统 RFID 系统标签识别效率较低、成本过高的问题,同时具有较高的安全性优势。与后退二叉树、动态自适应、二叉树搜索等算法进行比较,结果表明该策略能大大降低系统搜索的次数,提高标签的吞吐率。

关键词:射频识别;防碰撞算法;安全机制;自适应二叉树遍历;布尔运算
中图分类号:TP301.6　　**文献标志码**:A

RFID anti-collision strategy of embedded safety mechanism

LI Jia*, ZHENG Yiping, LIU Chunlong
(*Faculty of Computer, Guangdong University of Technology, Guangzhou Guangdong* 510006, *China*)

Abstract: The current Radio Frequency IDentification (RFID) system just simply integrates the collision algorithm and security mechanism together. Based on the analysis of classical adaptive dynamic anti-collision algorithm, an anti-collision strategy of embedded security mechanism was proposed. It combined the first traversal mechanism and Boolean mutual authentication protocol to solve the problem that traditional RFID tag identification system is not efficient and has high cost; it also has high security. Compared with the backward binary, dynamic adaptive and binary tree search algorithms, the proposed strategy can greatly reduce the times of the system search and improve the label throughput.

Key words: Radio Frequency IDentification (RFID); anti-collision algorithm; security mechanism; adaptive binary tree traversal; Boolean operation

0　引言

近年来,很多学者尝试把安全机制和防碰撞算法结合在一起。张晖等最早提出了新型安全机制下的 RFID 防冲突算法[1],将物理方法和密码机制相结合,通过将 Hash 锁放入阅读器中使用来节省门电路。丁治国等提出的基于码分多址和防碰撞功能的 RFID 安全认证协议[2],利用码分多址技术的保密性、抗干扰性和多址通信能力,结合认证密钥和 Hash 函数[3],设计了一种具有防碰撞功能的安全认证协议;余松森等提出了融合安全与反碰撞的 RFID 处理机制[4],采用的方法是将轻量级的随机密钥双向认证和动态时隙 ALOHA 协议进行融合。然而这些机制都是简单地将安全协议与防碰撞算法结合在一起,效率较低,随着标签的增加,信道占用率较高,吞吐率变低;数据在传输的过程中容易被窃听 ID,隐私被刺探,安全性不高;而且防碰撞效果差,花费时间较长,不宜大规模使用;同时又由于安全性达不到实用级别,需要另外的安全协议来加以保护,这样增加了成本,极大地降低了 RFID 系统运行的质量。

本文提出了一种新的轻量级高安全性防碰撞策略,该方法将自适应二叉树遍历算法与布尔运算双向认证协议相融合,得到一种新的防碰撞策略,该算法在解决了标签碰撞问题的同时,具有较高的安全性。对于在图书馆、流水线、快递服务、散货堆场等应用场合,已能提供足够的安全级别,适用于大数量、高效率、低成本的物联网系统。

1　RFID 系统相关原理

1.1　自适应二叉树遍历机制

在系统读写识别之前,该机制相当于在碰撞标签堆中利用遍历规则整理出一个有序的队列,从而使标签拥挤状态变成有序状态。自适应二叉树遍历机制[5-6]的搜索过程是根据先序遍历规则,在收集到的所有碰撞标签中,根据碰撞位特征采取向前搜索策略,直到遇到一个可以识别的标签为止;同时再采取后退方式,返回上一查询指令节点,继续搜索直至识别完阅读器工作区域内所有碰撞标签。主要步骤如下:

1)阅读器根据曼彻斯特编码方法得到所有识别标签的碰撞位,得到一个查询指令栈。

2)查询指令栈取出栈顶指令 Query(X,N) 命令(X 为碰撞位查询码,N 为标签碰撞的最高位),检测所有标签的碰撞位。

3)检测有无碰撞位编码符合条件的标签,若有两个以上响应,在符合条件的标签中重新执行曼彻斯特编码检测,根据是否连续位调整碰撞位查询码,并修改 N 值,得到下一次查询命令 Query 所需的参数,继续搜索直到出现一个碰撞位或者无碰撞位。

收稿日期:2013-06-24;**修回日期**:2013-09-10。　**基金项目**:广东省教育部产学研结合项目(2011B090400348,2010B090400436)。
作者简介:李佳(1987 -),男,湖北黄冈人,硕士研究生,主要研究方向:智能监控;　郑义平(1985 -),男,广东湛江人,硕士研究生,主要研究方向:知识管理;　刘春龙(1988 -),男,湖南衡阳人,硕士研究生,主要研究方向:智能监控。

4)若有一个碰撞位,可以根据约定直接先后识别两个标签(二进制位上取值具有互斥性,非 0 即 1);若无碰撞,则直接识别单个标签,处理完后回跳到父节点,得到下一次查询命令 Query 所需的参数。

5)重复进行请求与检测过程,直到查询栈中无查询命令时结束。

算法充分利用返回式搜索[7]和自适应二进制搜索的优点,并根据检测碰撞位是否连续动态生成多分支进行分治,只查询碰撞位的方法,减少了冗余,提高了系统效率。

先序遍历二叉树操作的递归算法在二叉链表上实现:

```
Status PreOrderTraverse( BiTree T, Status( * Visit)(TElemType e)){
  if (T){
    if (Visit(T -> data))
      if (PreOrderTraverse(T -> lchild, Visit))
        if (PreOrderTraverse(T -> rchild, Visit))
          return OK;
        return ERROR;
  }
  else
    return OK;
}                                          //PreOrderTraverse
```

1.2 基于布尔运算的双向认证安全协议

布尔运算是计算机最简单、最擅长、最快速的运算,具有无可媲美的优势,布尔运算贯穿该策略。

1)标签收到阅读器发出的命令数据,与 ID 编码进行布尔运算,命令数据与标签生成的随机数进行布尔运算[8]。

2)在阅读器中根据先建立好的 Hash 函数的索引,然后解码在后台数据验证,采用索引布尔运算的思想查找 ID,可提高验证速度。

3)后台数据库采用布尔运算的结果更新响应标签的记录。

现有协议标签中门电路较多,成本过高;而且动态 ID 机制中标签与数据库更新不同步造成了安全隐患。本文利用布尔运算,提出一种新的认证协议——基于布尔运算的低成本双向认证机制(如图 1 所示)。将 Hash 模块放在阅读器中,标签上无需集成 Hash 函数模块,只需要异或门电路和随机数生成器,通过布尔异或运算加密保证 RFID 系统通信安全[9-10],简单可行,适宜于低成本电子标签。

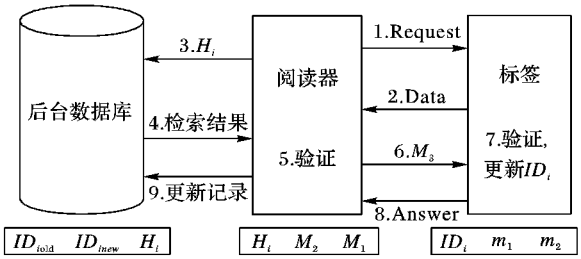

图 1 基于布尔运算的双向认证协议模型

2 内嵌安全机制的防碰撞策略

2.1 策略的基本思想

RFID 技术利用无线射频方式在阅读器和标签之间进行非接触双向数据传输来达到目标识别与数据交换的目的,电子标签的二进制唯一标识的 ID 可以构成一棵完全二叉树。而在阅读器作用范围内同步响应阅读器信号的标签的 ID 构成一棵不完全二叉树。阅读器根据信号冲突的情况反复对二叉树的分枝进行裁剪,快捷安全地找出这棵二叉树的结构,最终完成信息交换。

1)在修剪二叉树过程中,只需要根据碰撞位的不同来进行识别,省去了非碰撞位的遍历,缩减查询范围,减少冗余。

2)综合运用曼彻斯特编码、栈队列技术、二叉树先序遍历、后退式算法经典部分及采用独立分治并行处理思想,实现标签的有序识别。

3)动态自适应策略,根据碰撞位前缀是否连续,动态选择,碰撞前缀中出现连续 n 个碰撞位时采取 2^n 叉树分裂的策略(n 为大于等于 2 的正整数)。

4)短暂锁定机制,阅读器接收到标签所发的信息后,会暂时锁定,不再发出和接收任何标签命令。标签成功发送完信息后进入暂时休眠状态不再重复发送,阅读器开始进行内部的防碰撞处理,处理完后会逐步将结果发送到已识别的标签。

2.2 策略准备工作

传统的都是通过来回多次请求命令实现交互通信的做法,在源头上将阅读器与标签之间的通信信道暴露出来,本文则将加密的 ID 编译出来之后,直接在阅读器中完成处理,最终只需要返回结果即可,减少来回请求次数。这种设计有利于标签简单化,低成本化,把重心放在阅读器上,便于后续的维护升级,使系统生存能力增强。

1)请求命令 Request(Null, m_1):阅读器发出同步广播请求信号命令作用范围内的所有标签(m_1 为随机数)。

2)查询命令 Query(X,N):X 为曼彻斯特编码检测到的碰撞位前缀,参数 N 为冲突的最高位,在读写器的内部,查询命令不断按照先序规则搜索碰撞位生成的二叉树,直到检测至无碰撞或只有一个碰撞位为止;否则不断根据曼彻斯特编码调整 X 和 N 值,继续搜索。

3)应答命令 Answer(*Data*)(*Data* 是标签内部经布尔运算加密之后的数据):其作用是收到请求命令的标签对阅读器作出应答,将数据信息返回给阅读器。

4)锁定命令 Lock():阅读器收到作用范围内的标签响应后,会自动进入到锁定状态,暂时不接收外界任何消息。

5)$h(x)$、$f_k(x)$:分别表示标签能够运行的 Hash 函数和带密钥的 Hash 函数[11]。

6)在标准稳定环境中内存记录安全,阅读器与后台服务器之间信道安全,阅读器与标签之间信道不安全。

2.3 策略流程

内嵌机制处理流程如图 2 所示。

策略举例详细描述步骤如下:

第 1 步 系统进行初始化,阅读器发出同步广播请求命令 Request(Null, m_1),其中:m_1 为随机数比特串,$m_1 \in R\{0,1\}^k$(k 为 ID_i 等位的整数)。本例中有 8 个标签响应,如表 1 所示。

表 1 标签编号及其 ID

编号	ID	编号	ID
Tag_1	10100011	Tag_5	00100011
Tag_2	00101010	Tag_6	11101011
Tag_3	10101011	Tag_7	01100010
Tag_4	10100010	Tag_8	01101011

第 2 步　在读写器的作用范围内,满足条件的标签 Tag_i 在收到命令之后,生成一个随机比特串 $m_2 \in R\{0,1\}^k$(m_2 同 m_1,均为随机串)作为临时会话私钥,计算 $H_i = h(ID_i)$,$M_1 = ID_i \oplus m_2$,$M_2 = f_{ID_i}(m_1 \oplus m_2)$,然后将响应消息 H_i、M_1、M_2 等数据 Answer($Data$) 给阅读器。

第 3 步　阅读器收集完响应标签数据之后,自动调用 Lock 命令,进入暂时锁定状态。并将收集到的响应标签 $Data$ 数据,传送到后台进行安全验证。

第 4 步　服务器利用阅读器收集到的数据,进行如下安全验证:

a) 服务器根据 H_i 检索数据库,如果没有找到对应的 H_i,就终止本次会话,继续下一个任务;如果找到 $H_i = H_{i\,\mathrm{old}}$,则计算 $M_1 \oplus ID_{i\,\mathrm{old}} \rightarrow m_2$,然后判断 $M_2 \stackrel{?}{=} f_{ID_i}(m_1 \oplus m_2)$。

b) 若 $M_2 = f_{ID_i}(m_1 \oplus m_2)$,则阅读器验证通过,计算 $M_3 = ID_i \oplus m_2$,然后通过 Request(Null, M_3) 命令将 M_3 发送给标签。

c) 标签 Tag_i 计算并判断 $ID_i = M_3 \oplus m_2$,如果不相等,标签就保持当前存储的 ID_i 不变,发送 Answer(Error) 给阅读器,终止本次会话;若相等,则标签验证通过,更新并存储的 ID_i,$ID_i \oplus H_i \oplus m_1 \oplus m_2 \rightarrow ID_i$,同时发送 Answer(Success) 命令给阅读器。

d) 阅读器收到 Answer(Success) 命令后,开始更新后台服务器数据库中应答标签的记录,令 $ID_{i\,\mathrm{old}} \leftarrow ID_i$,$H_{i\,\mathrm{old}} \leftarrow H_i$,$ID_{i\,\mathrm{new}} \leftarrow ID_i \oplus H_i \oplus m_1 \oplus m_2$,$H_{i\,\mathrm{new}} \leftarrow h(ID_{i\,\mathrm{new}})$,安全验证通过。

第 5 步　继续对验证通过的标签进行防碰撞处理。阅读器将消息 $Data$ 数据传递给后台服务器中防碰撞处理机制。

第 6 步　对收集到的数据进行解码处理,得出标签 ID。根据曼彻斯特编码规则,分离出碰撞位 ID_{coll} 和非碰撞位 $ID_{N\mathrm{coll}}$。本例中作用范围内 8 个碰撞标签,曼彻斯特编码为 ??10?01?,碰撞位为 $D_7D_6D_3D_0$,碰撞最高位为 D_7,如表 2 所示。

表 2　碰撞标签及其碰撞位 $D_7D_6D_3D_0$

编号	ID	编号	ID
Tag_1	1001	Tag_5	0001
Tag_2	0010	Tag_6	1111
Tag_3	1011	Tag_7	0100
Tag_4	1000	Tag_8	0111

第 7 步　在阅读器后台中根据碰撞位进行有序化列队处理,碰撞位构成的二叉树如图 3 所示。

第 8 步　碰撞位从高到低次为 $D_7D_6D_3D_0$,由于 D_7D_6 是连续碰撞位,$2^2 \leqslant 4 < 2^3$,所以动态选择四叉树搜索,确定四个分支(11)(10)(01)(00)(按照先序,根、左到右的顺序,先 1 后 0,高位到低位约定),并将搜索分支命令入栈。

第 9 步　阅读器从堆栈中获取栈顶查询指令 Query(00, 7),所有待命的第七、六位是 00 的标签响应,这里是标签 Tag_5、Tag_2 响应。再次解码 Tag_5、Tag_2 得到新的编码数据为 0010?01?,由于有二位冲突位且不连续,故选择二叉树搜索,最高冲突位为 D_3,得到下一次查询命令 Query(0,3)、Query(1,3),并将命令入栈。

第 10 步　从栈顶取出 Query(1,3) 命令,开始在 Tag_5、Tag_2 中搜索,只有 Tag_2 符合条件,故将 Tag_2:00101010 进入有序队列。

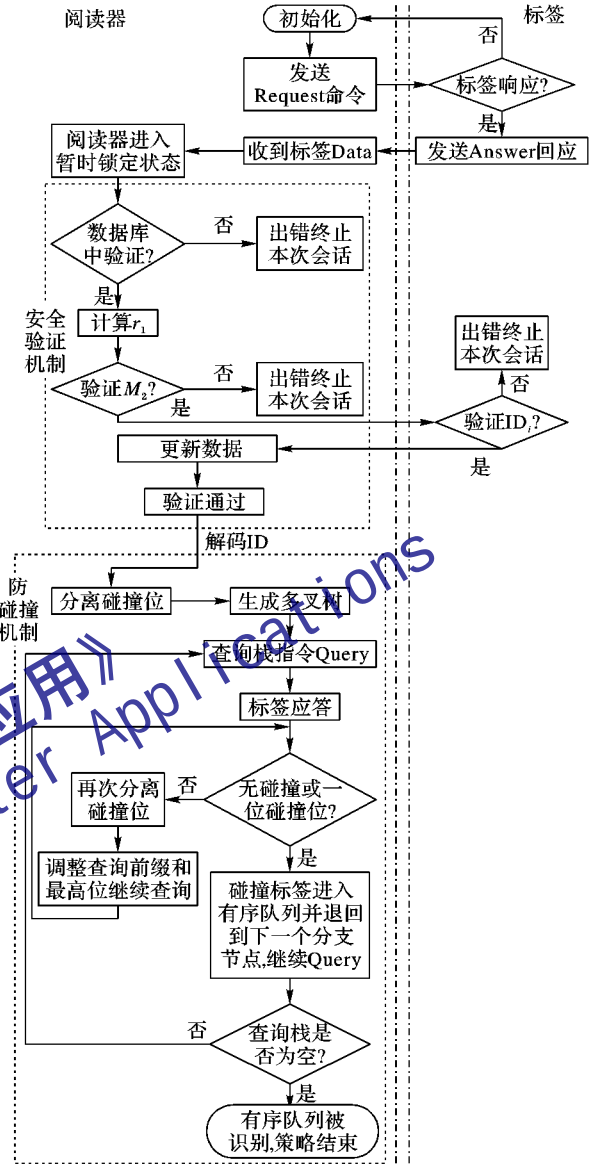

图 2　内嵌机制流程

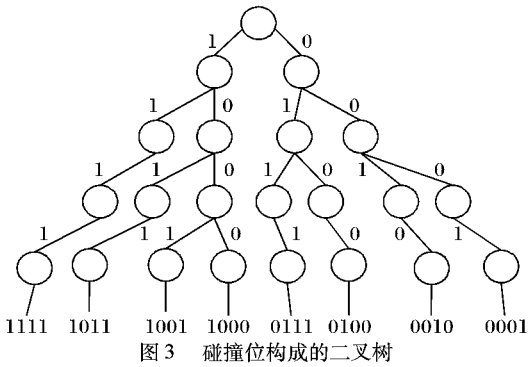

图 3　碰撞位构成的二叉树

第 11 步　从栈顶取出 Query(0,3) 命令,开始在 Tag_5、Tag_2 中搜索,只有 Tag_5 符合条件,故将 Tag_5:00100011 进入有序队列。

第 12 步　算法采用回跳方式,从栈顶中取出查询指令 Query(01,7) 开始继续搜索,标签第七、六位是 01 的满足条

件，这里只有 Tag_8:01101011，Tag_7:01100010，解码得 0110?01?，这种情况与 Tag_5、Tag_2 处理方式相似，同第 10 ~ 11 步，先后将 Tag_8、Tag_7 进入有序队列。

第 13 步　继续回跳执行，从栈顶中取出查询指令 Query(10,7)，待命标签第七、六位是 10 的响应，这里有标签 Tag_4:10100010，Tag_3:10101011，Tag_1:10100011 符合，解码得到新的编码数据为 1010?01?，由于有二位冲突位且不连续，故再次选择二叉树搜索，最高冲突位为 D_3，得到下一次查询命令 Query(0,3)、Query(1,3)，并将命令入栈。

第 14 步　从栈顶调取 Query(1,3) 开始在 Tag_4、Tag_3、Tag_1 中搜索，只有 Tag_3 符合，故将其入列。

第 15 步　回跳取出 Query(0,3) 继续查询，有 Tag_4、Tag_1 符合，解码得 1010001?，只有一位碰撞位，可以直接识别，先后将 Tag_1、Tag_4 入列。

第 16 步　回跳执行，从栈顶中取出查询指令 Query(11,7)，待命标签第七、六位是 11 的，这里只有标签 Tag_6，由于没有发生碰撞，直接将 Tag_6:11101011 进入防碰撞有序队列。

第 17 步　至此所有标签均排队完毕，最后的有序防碰撞队列为 Tag_2、Tag_5、Tag_8、Tag_7、Tag_3、Tag_1、Tag_4、Tag_6，陆续被读写，完成本例整个 RFID 系统数据交换工作。

3　策略分析

3.1　特点分析

本文所提出的策略主要有以下特点：

1)重阅读器轻标签。传统的防碰撞算法都是通过读回多次 Request 请求命令实现阅读器标签间的交互通信，这样不仅使得标签的成本很高，而且在源头上将通信信道暴露出来，不太合理。本文做法是将阅读器收集到的数据进行解密，得到 ID 标识号，直接在阅读器中完成有序列队处理，最终只需要一次将结果返回即可，不需要来回多次请求应答，使通道处于较安全状态，即只需 Request、Answer 两个命令的传送。这种设计有利于标签简单化，成本降低，把处理重心放在阅读器和后台上，便于后续的维护的升级，利于超大批量的标签系统运作，生存能力加强。

2)内嵌安全机制。通过布尔运算加密的方式将安全机制融合在防碰撞处理之前，一方面先行过滤掉攻击和假冒的无用标签，减轻碰撞处理的压力；另一方面提高标签的生存能力，通过加密的随机数和布尔运算打乱前后的信息逻辑，使得无法推测通信以前的信息，保证通信的安全性。并且通过双向认证的方式来验证消息的可靠性，确保标签、阅读器合法，不被修改。表 3 给出了该策略与几种其他的协议安全性能对比。

3)高性价比。在轻量级的 RFID 解决方案中，利用较简单的标签结构，能为整个系统节省非常可观的费用，同时也能兼顾较高的安全系数。不同策略下的标签成本对比见表 4。

表 4 中：l 表示 ID 比特长度，k 为正整数，l_{pin} 表示文献[3]中密钥的长度，l_c 表示时隙计数器长度，l_s 表示认证密钥的长度，l_{hash} 表示文献[1]中 Hash 变换结果长度，l_{kill} 表示文献[1]自毁装置长度，l_{ID_i} 表示文献[1]假名或随机数长度，l_{spr} 表示文献[2]扩频装置，l_{upd} 表示更新 ID 长度，l_{sv1}、l_{sv2} 分别表示文献[8]中嵌入标签生成的不同秘密值比特长度，Loop 表示文献[1]中循环计数器，Crc 表示校验码算法，Match 表示匹配比较函数，Prng 表示随机数发生器，Spr 表示扩频运算，Hash 表示哈希函数，Rotl 表示向左循环移位运算，Xor 表示异或运算，Con 表示连接运算，Mod 表示模运算，PUF 表示物理不可克隆机制[12-13]，其中长度较小的存储，包括标签中的一些堆栈、队列等小存储空间和少量布尔运算不考虑。

由表 4 可看出：当有标签数目增加时，同等条件下本文策略成本优势将更加明显。

表 3　策略安全特性对比

功能协议	隐私保护	重传攻击	追踪攻击	数据同步	阻断篡改	密钥更新	认证方式	防碰撞
Hash-lock	√	×	×	×	×	×	单	×
Hash 链	△	×	√	×	×	×	单	×
文献[1]协议	√	√	△	×	×	×	双	√
文献[2]协议	△	√	√	△	√	√	双	√
文献[4]协议	△	√	√	×	×	×	单	√
文献[8]协议	△	√	×	△	×	△	单	×
本文策略	√	√	√	√	△	√	双	√

注：√表示提供，×表示不提供，△表示一定条件下提供。

3.2　本文策略的仿真分析

本文策略防碰撞算法将经典的二叉搜索树、后退机制、动态自适应多分支等优点结合在一起。二叉搜索树防碰撞过程就是一个不断修剪二叉树的过程，利用曼彻斯特编码分离出碰撞位，后期处理时只需对标签碰撞位进行搜索，这样减少了搜索冗余；后退是搜索时通过记忆栈和回跳机制，只对分支中待命的标签进行搜索，路径不再重复操作，再一次缩小范围，提高效率；动态自适应多分支分治机制，是当出现连续 n 个碰撞位时，采用 2^n 个分支的查询命令，减少了曼彻斯特编码和调整查询指令 Query 的次数，进一步提高效率。

实验中假定分配的叉数不大于 4，识别过程中探测一个碰撞位的有 M 次，阅读器识别搜索次数可以表示为：

$$S(N) = S(N_{2-array}) + S(N_{4-array}) \approx (5N/3 - 2M) + \left(\sum_{i=0}^{\lfloor \log_4(N/3) \rfloor} 4^i \right)$$

本文算法吞吐率可表示为：

$$e = N/S(N) = \frac{N}{\frac{N}{3}[2(3-M)-1] + \sum_{i=0}^{\lfloor \log_4(N/3) \rfloor} 4^i}$$

为了对比本文策略的防碰撞性能，用 C 语言编写算法流

表 4　不同策略标签端成本对比表

类型	协议	存储空间	计算量	门电路数	复杂度
融合机制	文献[1]协议	$l + l_s + 2l_{hash} + 2Kl_{ID_i} + l_{kill}$	KPrng + KLoop + KMatch	1 700 ~ 2 500	高
	文献[2]协议	$l + l_s + l_{spr}$	Prng + Match + Spr	1 700 ~ 3 000	高
	文献[4]协议	$l + l_s + 4l_c$	Mod + 5Xor + 4Con + 2Crc + Prng	545 ~ 1 090	中
	本文策略	$l + l_s + l_{hash} + l_{upd}$	Prng + 2Match + Hash	545 ~ 1 090	中
单独机制	文献[3]协议	$l + l_{pin} + l_s$	Crc + Prng + 2Hash	1 700 ~ 3 000	高
	文献[8]协议	$l_{sv1} + l_{sv2}$	5Rotl + 5Xor + 2PUF	545 ~ 800	中

程,对二叉搜索树、后退式二叉树搜索算法、动态自适应和本文策略防碰撞算法四种算法进行 Matlab 仿真,在均匀情况下,作用范围内有 N 个标签,平均每次传送的二进制码长度为 L,分别统计搜索总次数和总比特数,最后取 50 次结果平均值。标签长度 $n = 8$ 时,防碰撞搜索次数结果如图 4 所示,防碰撞吞吐率结果如图 5 所示。

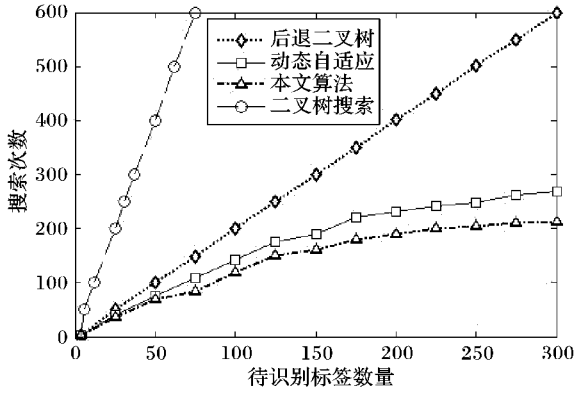

图 4　策略防碰撞搜索次数仿真对比结果 ($n = 8$)

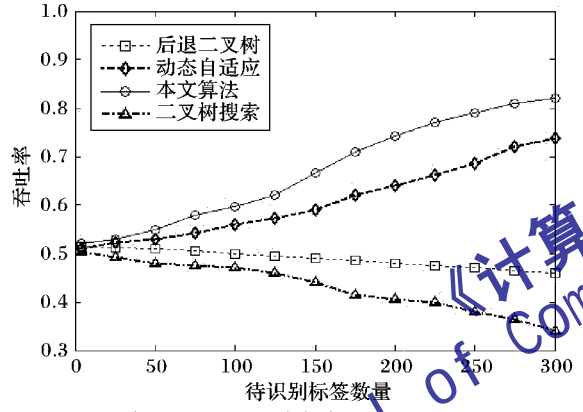

图 5　策略防碰撞吞吐率仿真对比结果 ($n = 8$)

仿真结果表明,当标签数目较少时,本文策略防碰撞效果并不明显,当数目不断增加时,搜索效果只是比后退机制好一些,但是传输比特位会比较显著。这是因为二叉树先序遍历机制采用的是只在碰撞位中遍历,并且有回退机制避免了搜索路径的重复,自适应多叉树策略对碰撞位前缀搜索做了优化,同时利用搜索索引采用布尔运算来匹配,提高了查找的运算速度。

当有巨量标签、标签的长度增大时,本文策略传输的比特位就会非常有优势。以后还可以通过阅读器升级,增加并行分组识别,效果将会更好。

4　结语

本文提出了一种轻量级的内嵌安全机制的 RFID 防碰撞策略,该方案巧妙地将经典动态自适应机制、先序遍历算法和布尔双向认证机制融合在一起,提高了防碰撞效率,降低了系统成本,具有一定的防重传、防篡改、防跟踪、防阻断的安全特性,简单高效,可靠实用。实验结果表明该处理策略能够减少碰撞时隙,提高吞吐量和防碰撞质量,在处理大量标签、较长 ID 标签环境中优势更为突出,具有良好的发展基础和应用前景。后续,在防碰撞过滤和识别处理等方面需要进一步的优化探索,采用基于 PUF 的物理不可克隆功能模块也是 RFID 系统发展的方向,以不断提高识别系统的安全性水平。

参考文献:

[1] ZHANG H, HOU C H, WANG D H. An anti-collision algorithm for a new RFID security architecture[J]. Microcomputer Information, 2008, 24(9-2): 165 – 167. (张晖, 侯朝焕, 王东辉. 一种新型安全机制下的 RFID 防冲突算法[J]. 微计算机信息, 2008, 24(9-2): 165 – 167.)

[2] DING Z G, ZHU X Y, LEI Y K. An RFID authentication protocol based on CDMA and anti-collision function[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2010, 27(3): 397 – 402. (丁治国, 朱学永, 雷迎科. 基于码分多址和防碰撞功能的 RFID 安全认证协议[J]. 中国科学院研究生院学报, 2010, 27(3): 397 – 402.)

[3] CHIEN H Y, CHEN C H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards [J]. Computer Standards & Interfaces, 2007, 29(2): 254 – 259.

[4] YU S S, ZHAN Y J, CAI Q L, *et al*. RFID processing mechanism integrating security and anti-collision[J]. Computer Engineering, 2011, 37(10): 254 – 259. (余松森, 詹宜巨, 蔡庆玲, 等. 融合安全与反碰撞的 RFID 处理机制[J]. 计算机工程, 2011, 37(10): 254 – 259.)

[5] SUN W S, HU L M. Anti-collision algorithm for adaptive multi-branch tree based on regressive-style search[J]. Journal of Computer Applications, 2011, 31(8): 2052 – 2055. (孙文胜, 胡玲敏. 基于后退式搜索的自适应多叉树防碰撞算法[J]. 计算机应用, 2011, 31(8): 2052 – 2055.)

[6] XU H f, JIANG H, LIU Z. An improved adaptive anti-collision algorithm in RFID[J]. Computer Engineering, 2012, 38(17): 290 – 293. (徐海峰, 姜晖, 刘振. 一种改进的 RFID 自适应防碰撞算法[J]. 计算机工程, 2012, 38(17): 290 – 293.)

[7] PUPUNWIWAT P, STANTIC B. A RFID explicit tag estimation scheme for dynamic framed-slot ALOHA anti-collision [C]// WiCOM 2010: Proceedings of the 2010 6th International Conference on Wireless Communications Networking and Mobile Computing. Piscataway, NJ: IEEE Press, 2010: 1 – 4.

[8] BASSIL R, EL-BEAINO W, KAYSSI A, *et al*. A PUF-based ultra-lightweight mutual-authentication RFID protocol [C]// Proceedings of the 2011 International Conference on Internet Technology and Secured Transactions. Piscataway, NJ: IEEE Press, 2011: 495 – 499.

[9] LI H. Design and analysis of the light-weight mutual authentication protocol for RFID[J]. Journal of Xidian University: Natural Science, 2012, 39(1): 172 – 178. (李慧贤. 轻量级 RFID 双向认证协议设计与分析[J]. 西安电子科技大学: 自然科学版, 2012, 39(1): 172 – 178.)

[10] DUC D, PARK J, LEE H, *et al*. Enhancing security of EPC global Gen-2 RFID tag against traceability and cloning [EB/OL]. [2012-10-10]. http://autoidlabs.org/uploads/media/AUTOID-LABS-WP-SWNET-016.pdf.

[11] CHO J-S, YEO S-S, KIM S-K. Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value [J]. Computer Communications, 2011, 34(3): 391 – 397.

[12] HE Z Q, ZHENG Z X, DAI K, *et al*. Low-cost RFID authentication protocol based on PUF[J]. Journal of Computer Applications, 2012, 32(3): 683 – 685, 698. (贺章擎, 郑朝霞, 戴葵, 等. 基于 PUF 的高效低成本 RFID 认证协议[J]. 计算机应用, 2012, 32(3): 683 – 685, 698.)

[13] RUHRMAIR U, MUNCHEN T, DROR G, *et al*. Modeling attacks on physical unclonable functions [C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM Press, 2010: 237 – 249.