DOI:10.16644/j.cnki.cn33-1094/tp.2022.11.001

基于RFID的隐私保护协议*

任雪萍，蔡培伟，郭远凯，范　扬

(杭州电子科技大学信息工程学院，浙江 杭州 311305)

摘　要：基于射频识别的医院婴儿管理系统,存在婴儿信息等隐私泄露的安全隐患。针对这个问题,基于分组思想,设计了一个新的RFID协议。该协议能实现基于RFID的匿名双向认证协议,可以实现婴儿手环标签和阅读器之间匿名的进行双向认证与协商会话密钥,并防止攻击者通过丢失的阅读器获取隐私信息。本协议能够抵御常见安全攻击。通过复杂度分析,证实了本协议更适用于低性能的标签。

关键词：无线射频识别(RFID)；安全攻击；安全隐患；认证协议；分组

中图分类号:TP301　　**文献标识码:**A　　**文章编号:**1006-8228(2022)11-01-04

RFID-based privacy protection protocol

Ren Xueping, Cai Peiwei, Guo Yuankai, Fan Yang

(*School of Information Engineering, Hangzhou Dianzi University, Hangzhou, Zhejiang 311305, China*)

Abstract: In the hospital infant management system based on RFID, there are potential security risks such as the leakage of infant information. Aiming at this problem, a new RFID protocol is designed based on the idea of grouping. Based on the protocol, anonymous two-way authentication and negotiation of session keys between the baby hand ring tag and the reader can be implemented, which prevents attackers from obtaining private information through a lost reader. This protocol is resistant to common security attacks. The complexity analysis confirms that this protocol is more suitable for low performance tags.

Key words: radio frequency identification (RFID); security attack; potential security risks; authentication protocol; grouping

0 引言

无线射频识别(radio frequency identification,RFID)作为一种新型的自动识别技术在物流管理,工业自动化,商业自动化,交通运输控制管理等众多领域得到了广泛的应用,在不远的将来将进行产品级大规模应用进入日常生活。如果说标准问题与标签价格是阻碍RFID技术推广所面临的两个难题,那么安全与隐私问题便是RFID这项技术是否能够进行行业应用的关键。由于RFID标签强大的追踪能力,RFID的广泛应用,也势必给消费者带来新的隐私威胁问题[1,2]。这种环境下隐私保护问题必将越来越受到人们的重视,对RFID安全协议进行研究具有重要的意义。研究RFID隐私保护协议,有利于保护系统的安全性、保护信息传输的安全性,推动RFID技术的普及。

1 相关研究

目前,已经有许多认证技术方案被提出来用于保护RFID系统用户的安全和隐私。根据所采取的措施,可以分为物理机制方案[3]和加密机制[4]方案。

物理机制方案主要有:Kill命令机制、静电屏蔽、阻塞法等。

“Kill命令机制”是在设计标签时使之能够接受一个Kill命令。带标签的产品在卖点扫描结账后,向标签发出该命令,使标签自动失效。

完全杀死标签可以完美地阻止扫描和追踪,但对于消费者来说,牺牲了RFID标签所有售后利益。在

收稿日期:2022-04-19

***基金项目:**浙江省·大学生创新创业项目“基于分组的RFID隐私保护协议设计”(S202113279004)

作者简介:任雪萍(1978-),女,浙江宁波人,硕士,讲师,杭州电子科技大学副教授,主要研究方向:分布式数据结构、无线通信。

通讯作者:蔡培伟(2000-),男,浙江江山人,本科,主要研究方向:信息管理。

很多情况下，标签不能被杀死。

阻塞法依靠编入标签识别码的可修改位来保护隐私性，这一位称为隐私位，为0表示可以公开扫描，为1表示是私有。阻塞法依赖树遍历反冲突协议来起作用。除此之外，由于不可靠的RFID传输，可以造成阻塞的失败。随着阅读器的发展，可以利用信号强度等特征来过滤阻塞信号。

加密机制方案根据标签有没有被分成多个小组，这些方案可分为两类：基于分组的方法和不分组的方法。

不分组传统的认证方法，通常采用位逻辑运算符，哈希函数和伪随机数字生成器(PRNG)，对称密钥加密，数字签名和零知识隐私模型等技术来实现安全和隐私保护的目的。

在文献[5]中提及Sarma等人于2003年设计提出了基于哈希函数的Hash-Lock认证机制。该认证机制将通信中的数据用哈希函数进行隐藏。但是，该协议也有较多的安全漏洞。因此，Hash-Lock协议并不能满足系统安全性要求。

根据能不能为标签提供字段级的保护，基于分组的方法又可以分成两类。

部分基于分组的方法，读写器或者可以获取标签的整体信息，或者不能获得任何信息。Avoine等人提出的基于分组的认证协议在可扩展性和隐私保护中得到了较好的权衡。但是该协议存在严重缺陷。Farzana等人提出一个用于大规模RFID系统的基于分组的认证协议。但是该协议标签信息保护没有达到字段级，而且系统的可扩展性有限。

另一类基于分组的协议，提供分类保护。分类保护协议确保合法读写器仅获得标签的部分授权信息。为了解决这个问题，H.Ning等人为RFID系统提出了一个可扩展的分布式密钥组身份认证协议(KAAP)[6]。通过分析，号称该协议具备抵制外部和内部攻击的能力。但是，在KAAP协议里读写器的角色被事先设定，很难改变。这个特性限制了该协议的可扩展性。

X.Ren等人提出了一个可扩展的分类保护RFID认证协议(SAAP)[7]。系统分析表明该协议在保证良好性能和较好可扩展性的同时，能抵制内外部的各种攻击。如同不分组的协议，这两个协议的隐私模型也假设攻击方没有破译标签的能力。

2 改进的RFID隐私保护协议

2.1 初始条件及符号含义

协议执行的初始条件包括以下几个方面。

标签组：在本课题里，标签根据类型的不同被分成N个组，每个小组里标签个数不同。其中考虑到医院同时能够接纳的产妇和婴儿的个数有限。这两种类型的在用标签数目固定。(出院婴儿和产妇的标签物理销毁)。每个标签组有唯一的组密码KG_i，组内标签共享这个密码。每个标签组共享一个标签标识(ID)池SET_i。

$$SET_i = \{ID_{i,1}, ID_{i,2}, ID_{i,3}, \cdots, ID_{i,s}\}$$

其中$1 \leqslant i \leqslant N$，s是系统设置的参数。任意两个标签组不共享任何一个ID，也就是当$\forall i \neq q$时，$SET_i \cap SET_q = \varnothing$。

标签：每个标签保存有组密码KG_i，在授权的读写器和标签之间共享的唯一密码KT_j，以及标识符$ID_{i,x}$。$ID_{i,x}$从SET_i集合中随机选出一个ID。

读写器组：读写器根据功能被分成M个组，每个组内的个数各不相同。读写器组对于标签组有一个授权访问密码组KEY_{MN}，用来指示该组读写器对于某个标签组里的标签有哪几个字段的访问权。

读写器：每个读写器对于有访问权限的标签组有一个秘密信息集合$\sigma_i = \{KG_i, \{KT_j, 1 \leqslant j \leqslant s\} | 1 \leqslant i \leqslant M\}$，保存有该读写器所在的读写器组相关的授权访问密码组KEY_{pN}，其中p表示该读写器所在的组别。

发行者：发行者初始化各个系统参数(N-标签组数，M-读写器组数，s-标签组最多标签的个数)。给每个标签组分配一个组密码KG_i和一个标识符集。初始化授权访问密码组KEY_{MN}，把每个读写器允许访问的标签组的相关信息集和授权访问密码组KEY_{pN}写入该读写器。其中p表示该读写器所在的组别。该协议描述中使用的符号及其含义如表1所示。

表1 协议中的符号及其含义

符号	含义
N	标签组数
M	读写器组数
s	标签组最多标签的个数
KG_i	每个标签组唯一的组密码
SET_i	每个标签组共享的一个标签标识(ID)池
$ID_{i,x}$	标签标识
KT_j	在授权的读写器和标签之间共享的唯一密码
KEY_{MN}	读写器组对于标签组的一个授权访问密码组
σ_i	允许访问的标签组的相关信息集
H_1	利用它要访问的标签组密码KG_i，采用对称加密算法加密随机数
H_2	收到信息的标签，用自身的组密码KG_i，解密
H_3	利用授权的读写器和标签之间共享的唯一密码K_j加密K_{ij}

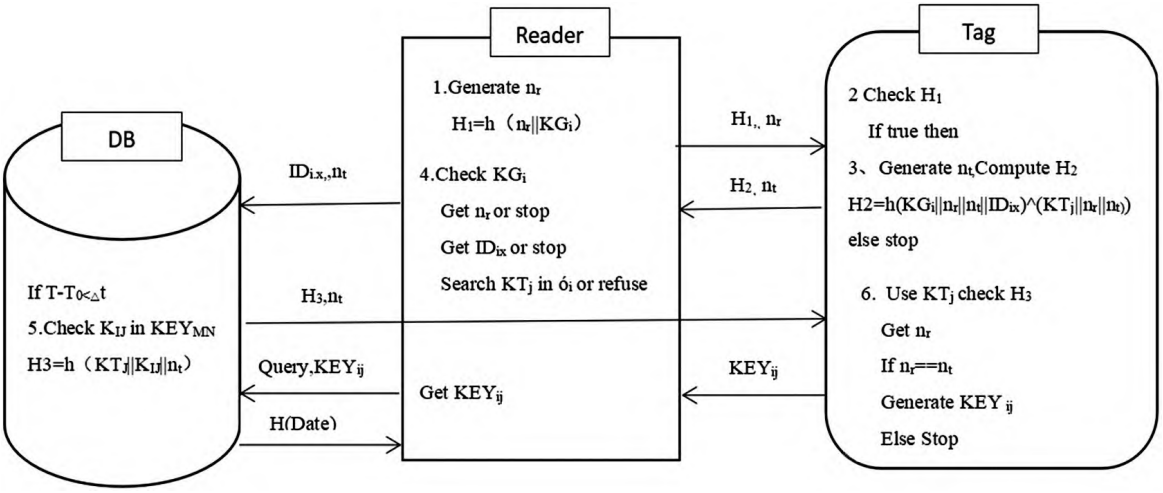

图1 基于RFID的隐私保护协议

2.2 认证过程

新设计的隐私保护协议认证过程如图1,详情如下。

⑴ 读写器产生一个随机数n_r,利用它要访问的标签组密码KG_i,采用对称加密算法加密随机数,并把加密后的结果发给标签。

⑵ 收到信息的标签,用自身的组密码KG_i,解密。如果可以解密则转⑶继续,否则不予理会,直接结束。

⑶ 标签先产生一个随机数n_t,接着利用KG_i和对称加密算法加密n_r,n_t和$ID_{i,x}$这三个数连接后的值,用KT_j和对称加密算法加密n_r和n_t这二个数连接后的值,最后把获得加密后的值发给读写器。

⑷ 读写器在秘密信息集中,查找有没有KG_i可以解密第一个数。如果没有,就结束认证。否则,查看解密后的第一部分是不是n_t,如果不是,结束认证,否则得到$ID_{i,x}$。然后在σ_i中,查找跟$ID_{i,x}$关联的密码,搜索合适的KT_j,进行解密。如果存在着这样一个密码KT_j,则接受该标签转⑸,否则拒绝。

⑸ 在授权访问密码组KEY_{MN}中,找出合适的K_{ij},利用KT_j和对称加密算法加密K_{ij}和n_t的连接值,把结果发给标签。

⑹ 标签收到信息后,用KT_j解密,获得随机数和授权访问码。如果随机数与n_t不符,则结束,否则根据授权访问码,允许该读写器访问本标签相应字段的值,把相信字段的信息加密后发给读写器。

⑺ 特殊情况,遇到婴儿出院,需要先在读写器和婴儿的标签之间通讯,获得其母亲的信息。读写器再和产妇的标签通信获得其相关信息,一致后,读写器发出通过的信号,放行,同时他们的标签物理销毁。

⑻ 读写器每隔5分钟主动发出请求验证信号时,如果婴儿的标签位置无反馈或反馈数据异常时,发送警报,提醒医护人员注意。

⑼ 婴儿需要离开病房去检查时,用特定的读写器去读取婴儿标签,先检查是否有医疗检查预约,若有则验证抱婴儿人的身份,若身份验证通过则暂时关闭该标签报警系统。检查科室有相应的扫描读写器,当该标签进入时即刻反馈婴儿位置信息。当回到病房区域后读写器扫描到该标签时同样自动开启报警系统。估计路程时间,若超过规定时间还没到达指定区域,发警报给医护人员,医护人员询问相关联系人,一定时间内未联系上则报警。

3 安全性和复杂度分析

3.1 安全性分析

⑴ 防窃听攻击

协议中,读写器和标签之间的信道,读写器和后端数据之间的信道,所有真实消息均经过对称加密算法后传递,基于随机数的堆成加密算法保证了攻击者即使在信道中窃听到了传递的消息,也无法恢复出消息的真实内容。

⑵ 防篡改、假冒攻击

协议中,如果攻击者截获了加密后的值,由于攻击者只能在标签和读写器之间的无线信道中窃听到一个加密的值,信息截获后相应的读写器或标签无相应的反馈。而本协议是双向认证的,所以攻击者伪造消息企图假冒标签通过读写器的认证是困难的,实施篡改无法通过服务器认证。因为非法读写器没有访问后端认证服务器的权限,因而无法获取标签ID等信息,即攻击者假冒读写器没有意义。

⑶ 防重放攻击和跟踪

协议中读写器产生的随机数Nr每次通信中都是不相同的，因此每次通信发送响应的消息也不同。这样一方面，有效防止攻击者根据通信中固定的输入消息对标签进行跟踪；另一方面，即使攻击者获取到了某一次的通信消息，在下次通信时伪装成标签对读写器产生正确的应答消息是困难的，仍然无法通过对方认证。

3.2 复杂度分析

在新协议中，只使用了哈希函数和简单的异或运算，相较于分布式挑战–应答协议，新协议在标签中只进行了一次哈希运算且不需要集成伪随机数发生单元，降低了标签的成本，提高了效率。此外，相较于大部分RFID认证协议的3–5步认证，新提出的协议需要六步实现认证，虽然步骤增加，但协议在安全性上有非常大的提升。

假设数据库中存储了N个标签的信息，那么完整地执行一次本协议，后端数据库最少执行一次哈希运算和一次比较，最多执行N次哈希运算和N次查找；标签执行一次哈希运算；读写器只需产生一次伪随机数。假设协议中选取的哈希函数输出以及标签ID的长度均为L，那么每次通信信道中传输的数据长度为2L，标签的空间复杂度为2L。执行一次本协议最多需要在后端数据库中进行N次哈希运算和N次查找，虽然随着系统中标签数量的增加会增加认证服务器的负担，但这从本质上不会对RFID系统的效率造成太大影响，因为本协议可用于分布式数据库环境，可以分散存储和计算。

针对上述安全问题以及协议执行所需步骤，将文中提出的协议与几种经典认证协议进行比较，如表2所示。

表2 协议比较

	防窃听	防假冒	防篡改	防重放	防跟踪	协议执行步骤
Hash–Lock协议	×	×	×	×	×	6
KAAP协议	√	√	√	×	√	5
文中提出的改进协议	√	√	√	√	√	6

注√：可以满足解决该安全问题；×：不能解决该安全问题

3.3 协议模拟

使用的开发工具为IntelliJ IDEA(以下简称IDEA)，使用的数据库为MySQL数据库，使用的数据库管理软件为Navicat for MySQL，开发环境配置为JDK1.8，使用JAVA按照RFID隐私保护协议进行程序设计实现协议的模拟。读写器有非法读写器和合法读写器。而合法读写器又可细分为产房读写器、药房和检查科读写器。

标签分为产房标签和药房标签。只有当读写器为合法读写器且是相对应的标签的读写器时才可根据自己的权限访问数据库从数据库中取得权限所对应的信息，如图2所示；否则访问失败。

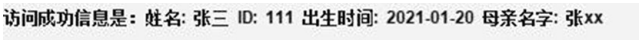

图2 产房标签访问成功

以产房读写器读取产房标签为例(其他操作指令的程序设计与此相近)，通过点击下发“读取标签中的数据存储区”指令在IDEA中的JAVA代码实现，如图3所示。

```
        String info="";
        if ( reader.visit(tag).equals("1")) {
            try {
                info=connect.connect( type: "1", id: "111");
            } catch (Exception ex) {
                ex.printStackTrace();
            }
            label.setText("访问成功信息是："+info);
        } else {

            label.setText("访问失败");
        }
        myFrame.add(label);
    });
```

图3 控制程序段

新建一个信息提示框，通过点击按钮，获取相应属性的reader和tag，根据点击后的reader和tag进行访问，通过标志为1来确认此次访问是成功的，访问成功后，因为每个相同类型的标签id均不同，去数据库查询相应条目，获取相应的访问字段内容，展示在提示框中。具体的应用场景模拟如图4所示。

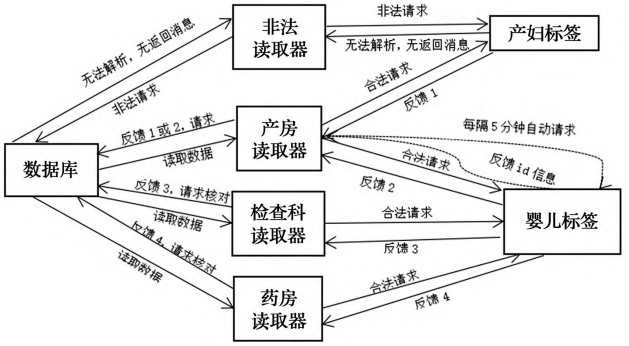

图4 基于RFID的隐私保护协议应用场景模拟

(下转第9页)

变化曲线，如图7所示，NMPC的曲线相对AMPC更加平滑一些，这表明NMPC控制器在加速度执行和速度追踪方面表现得更为平稳，在保证车辆行驶安全性的前提下，可以提供更好的舒适性和稳定性。

4 结束语

本文通过对车辆横向动力学进行合理建模，引入车道检测模块，基于传统模型预测控制理论，建立了自适应MPC和非线性MPC两种控制器，实现了车道保持辅助系统，实验结果表明：在发生车道偏离时，所设计的LKA系统可以及时帮助驾驶员调整前轮转向，回归车道中心。此外，NMPC模型相对于AMPC模型具有更平滑的加速度和速度指令，一定程度上给予乘客更好的稳定性和舒适性。但是NMPC要求处理系统的计算性能较高，花费时间较长，未来将从实时性与稳定性两者综合的角度出发，进而实现高性能、高效率的LKA系统控制方案。

参考文献(References):

[1] 房泽平，段建民，郑榜贵．智能四轮转向车辆稳定车道线保持串级控制[J]．信息与控制，2016，45(4)：8

[2] 吴乙万，朱越，李凡．基于主动转矩分配的电动车车道保持辅助控制方法[J]．科技导报，2018，36(5)：7

[3] Bing Z, Meschede C, Chen G, et al. Indirect and Direct Training of Spiking Neural Networks for End-to-End Control of a Lane-Keeping Vehicle[J].Neural Networks, 2020,121:21-36

[4] 施卫，张晨．基于LQR算法的车道保持控制策略[J]．智能计算机与应用，2021，11(1)：5

[5] 董婷．基于改进预瞄驾驶员模型的车道保持系统[J]．汽车实用技术，2019(24)：3

[6] Marino R, Scalzi S, Netto M. Integrated Driver and Active Steering Control for Vision-Based Lane Keeping[J]. European Journal of Control,2012,18(5):473-484

[7] 罗莉华．基于MPC的车道保持系统转向控制策略[J]．上海交通大学学报，2014，48(7)：6

[8] Huang Y, Chen Y. Vehicle Lateral Stability Control Based on Shiftable Stability Regions and Dynamic Margins[J]. IEEE Transactions on Vehicular Technology, 2020(99): 1-1

[9] Mulliken, Robert S. Magic Formula, Structure of Bond Energies and Isovalent Hybridization[J]. Journal of Physical Chemistry,1952,56(3):295-311

[10] T Holzh ü ter. Simulation of relay control systems using MATLAB/SIMULINK[J]. Control Engineering Practice, 1998,6(9):1089-1096

(上接第4页)

4 结束语

本研究针对基于射频识别的医院婴儿管理系统，基于分组思想，设计了一个新的RFID协议。该协议具有分类保护和可扩展性。通过安全性讨论证明了协议的安全性，本协议能够抵御常见安全攻击。通过复杂度分析，证实了本协议更适用于低性能的标签。分析表明，与其他相关协议相比：该协议在抵抗各种内外部攻击（内部攻击、重放攻击、跟踪攻击、欺骗攻击和DOS攻击）的同时，能进行医护正常交流，能实现母婴身份验证，能日常预防婴儿被盗（假设暴力剪开标签可以确保物理毁坏，无法回复信息）。该协议将大幅度提高医疗领域的安全管理，可节省原本需要的人力物力成本，创造经济价值，改善社会风气。

参考文献(References):

[1] 刘彦龙，白煜，滕建辅．RFID分布式密钥阵列认证协议的安全性分析[J]．计算机工程与应用，2014

[2] 卿斯汉．安全协议[M]．北京：清华大学出版社，2002

[3] 刘旷．一种RFID隐私保护双向认证协议[EB/OL]．(2009)．https://www.eefocus.com/communication/169402

[4] 周世杰，张文清，罗嘉庆．射频识别(RFID)隐私保护技术综述[J]．软件学报，2015，26(4)：960-976

[5] 王海春，李灿，邓珊．基于混沌加密的RFID认证协议设计[J]．超星期刊，2015

[6] H. Ning, H. Liu, J. Mao, Y. Zhang. Scalable and distributed key array authentication protocol in radio frequency identific-ation-based sensor systems[J]. IET Communi-caTions,2011,5(12):1755-1768

[7] XuepingRen,MingJiang,TingWu,XianghuaXu,YinglongGe. A Scalable Authentication Protocol with Classified Protection in RFID-based Systems[J]. Ad Hoc & Sensor Wireless Networks,Vol.31:151-172