一种基于射频识别技术的物资安全保障方案设计与应用

林亚忠，万任华，林村河，王　苓，顾金库

[摘要]　目的：设计并应用一种基于射频技术的物资安全保障方案。方法：事先约定了 RFID 标签的编码格式，只有 PDA 通过无线方式与基地数据库连接才能获取 RFID 标签内容；同时在 PDA 与 RFID 标签之间建立双向认证机制，防止未授权的阅读器和假冒的标签参与会话。结果：在卫生分队执行机动卫勤保障任务动态补充物资过程中应用该方案后，保证了物资的安全运输。结论：在确保物资应急保障的安全性和可靠性方面有较大应用价值。

[关键词]　RFID；卫勤保障；信息编码；安全认证
[中国图书资料分类号]　TN925+.1；R318.6　[文献标识码]　A　[文章编号]　1003-8868(2011)09-0010-03

An Application and Design for Safety Material Support Program Based on Radio Frequency Identifier

LIN Ya-zhong[1], WAN Ren-hua[1], LIN Cun-he[1], WANG Ling[2], GU Jin-ku[3]
(1.The 175th Hospital, Southeast Hospital of Xiamen University, Zhangzhou 363000, Fujian Province, China; 2.The 92nd Hospital of PLA, Nanping 353000, Fujian Province, China; 3.Dept. of Computer Science, Xiamen University, Xiamen 361005, Fujian Province, China)

Abstract　Objective To design and apply a material security program based on RFID technology. Methods The program agreed on encoding format of RFID tag in advance, in which PDA could access the content of RFID tags only by connecting with the base database wirelessly. At the same time, mutual authentication mechanism was established between the PDA and the RFID tag, which prevented unauthorized tags and readers from participating in the session. Results The safe of military supplies transportation was assured after the program was applied in the implementation of mobile medical support tasks. Conclusion The program has great application value for ensuring the safety and reliability of material emergency support. [Chinese Medical Equipment Journal, 2011, 32(9): 10-11, 18]

Key words　RFID; service support; information coding; security authentication

1　引言

应急机动卫生分队作为医院卫勤机动力量具备独立行动和执行任务能力，适应于执行战时卫勤和平时突发事件保障任务需要。卫生分队的物资管理系统通常采用射频识别(radio frequency identifier，RFID)技术，在外出机动执行保障任务时，可通过手持 PDA 来管理物资的使用，在任务结束后再与医院后台数据库进行同步，减少了手工的参与，大大地提高卫生分队物资管理的自动化程度。然而，现代高科技信息化局部战争使医疗物资呈现出高消耗特征[1]，同时运输工具的多样化使得跨地区执行军事任务成为常态，卫勤保障地点往往离后方基地库房较远，直接从战备库房运输医疗物资显然不切实际，只能就近采购，战备物资的应急补充在所难免。传统应急物资采购的 RFID 标签通常包含物资的详细信息，容易受到监听和攻击。为安全起见，应急采购物资的 RFID 标签信息应避免使用明码。针对这一现状，本文提出一种基于 RFID 技术的物资安全保障方案，在该方案中，标签的具体内容保存在后方数据库中，PDA 通过事先约定的 RFID 标签编码，与后方军用网络建立无线连接来获取射频标签的物资内容，同时在 PDA 与 RFID 之间建立一种双向认证机制，防止未授权的阅读器和假冒的标签参与会话，确保了物资应急保障的安全性和可靠性。

基金项目：南京军区重点课题(08Z021)；南京军区“十一五”计划课题项目(06MA99)
作者简介：林亚忠(1973-)，男，高级工程师，博士，硕士生导师，主要从事计算机图像处理和卫勤信息化方面的研究工作，E-mail：yzlincqh@tom.com。
作者单位：363000　福建漳州　解放军 175 医院（厦门大学附属东南医院）(林亚忠、万任华、王　苓)；353000　福建南平　解放军 92 医院(林村河)；361005　福建厦门　厦门大学计算机科学系(顾金库)
通讯作者：万任华，E-mail:yqwyywrhua@tom.com

2　RFID 技术简介

射频识别技术是一种通过使用辐射电磁场来传输和读取数据的技术。通过将射频电子标签粘贴在车辆、包装箱或单元物品上，就可以实现对在运或货架上物资等相关信息的自动存储和传递[2-3]，通常 RFID 技术可获取 10 cm 以上距离(高频 13.56 MHz 标签)乃至几十米以上距离(超高频 915 MHz、2.4 GHz 标签)电子标签中的信息，然后通过软件进行格式转换并存入数据库。近年来，RFID 技术凭借其非接触、可重复使用和快速读取等优点，广泛应用于军事物流领域。

3　基于 RFID 技术的安全保障方案

图 1 是我们借鉴移动 RFID 服务架构体系[4]建立的安全保障模型。在该模型中，RFID 标签存储的电子编码唯一标识了其对应的物资编码信息，就如同互联网中的 IP 地址用来标识网络中的一台计算机一样；PDA 用来承担 RFID 标签的数据采集、信息传输与获取；基站可以是军用卫通车，也可以是通过 AP 访问的一个无线网络，用于连接军方内部网络；军方

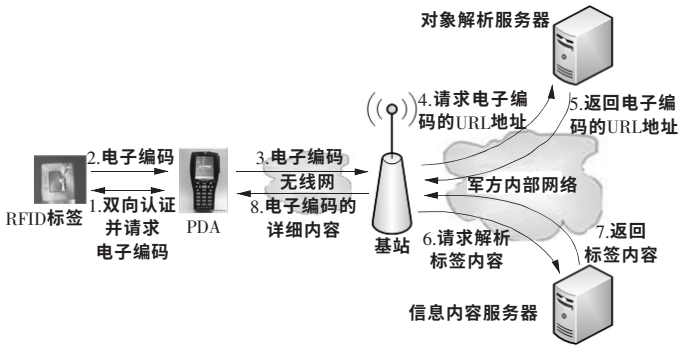

图 1 基于 RFID 技术的安全保障方案

内部网络设置有 2 种服务器，即对象解析服务器和信息内容解析服务器。其中，对象解析服务器用于返回 RFID 标签电子编码的统一资源标识符(URL)地址；信息内容服务器用来提供与电子标签对应的详细内容。对于一般访问模式，用户首先利用 PDA 扫描物品上的 RFID 标签，获取标签信息的电子编码，电子编码通过无线方式发送到后方军队网络，然后通过网络中的对象解析服务器获得对应的 URL，最后，利用给定的 URL 从信息内容服务器获得电子编码对应的物品内容，并返回给 PDA。

在上述模型中，从 2 个方面来保障物资的安全，首先，通过约定一种军事物资 RFID 标签的编码格式，标签内只存有物资的编码，而具体的物品信息则在军方后端数据库内保存，PDA 需要通过无线方式连接到后方网络才能获得物资的具体内容；另外，在 RFID 标签和 PDA 之间建立一种基于哈希函数双向认证机制，只有经过授权的阅读器和真实的标签才能进行会话。下面我们从设计安全的电子编码格式和双向认证协议 2 个方面入手，研究、讨论基于 RFID 技术的安全保障方案如何确保物资应急保障的安全性。

3.1 设计安全的电子编码格式

在安全方案中，应急保障战备物资所用的射频标签是经过特殊处理的，通常由军方和厂商约定解决。考虑到这类标签可以唯一确定某一类具体物资，但是又不能单独靠 PDA 得到详细的物资信息，将 RFID 标签的编码设计由版本号、域名管理和序列号组成。其中域名管理描述了与此电子编码相关的厂商信息，可用于加快内容检索速度；序列号唯一标识某种物资信息，如表 1 描述了护理箱射频标签上的编码情况。为防止

表 1 某个护理箱上 RFID 标签的电子编码

版本号字段(2 位)	域名管理(16 位)	序列号(30)
01	1000101001010111	(简写为 S)

这种简单编码被截获和利用，该文引入一串二进制随机数据，并与原域名管理编码进行简单的逻辑运算，从而实现对数据的加密。首先，在卫生分队和厂商之间约定一个“<序列号，二进制随机数据>”映射表。针对每个电子编码序列号，都有一个唯一的二进制随机数与之对应，在标签写入前，先用真实的电子编码与该随机数据数进行异或，然后将其结果写入 RFID 标签，代替原有电子编码中的域名管理字段，使得普通的 PDA 无法正确读出标签信息，只有装有反向解密软件的 PDA 才能透过逆变换，获取标签的真实数据。以表 1 域名管理字段为例，与序列号 S 对应的二进制随机数为 0011110101011010，则写入射频标签域名管理字段的值应为它们的异或值 1011000011101101。

该方法简单且易实现。对于带有这一约定映射表的我方 PDA 来说，只需通过简单的异或运算便可获得真正的电子编码，并进行下一步的查询。而对敌方来说，在不知道该映射表的前提下，对于每一位编码都有 0、1 两种可能，其破解代价达到 2^{16}=65 536 种，从而可以有效地保证电子编码的安全性。

3.2 设计安全的双向认证协议

近年来，国际标准化组织出台了 ISO/IEC 29176 等移动 RFID 保护隐私协议来确保智能移动终端与 RFID 标签之间的信道安全，很多学者和组织在移动 RFID 系统的安全与隐私保护方面做了大量研究[5-7]，并取得一定成果。其中，文献 [5]提出的零知识双向认证方法比较典型，它确保了信息拥有者在不泄露标签 ID 的情况下，通过一次一换的随机会话密钥(random session key，RSK)和时间戳(date timestamp，DT)，实现了 PDA 与 Tag 标签之间的双向认证。然而，该方法中随机数由 RFID 标签生成，不仅增加了成本，而且运算速度慢；加上时间戳 DT 是明文传输，也容易被假冒，不能完全实现所谓的零知识认证。因此，本文提出一种改进的双向认证协议。通过在 PDA 与 Tag 之间共享一个单向 Hash 函数 H、拥有极小的初始时间戳、初始共享密钥(shared key，SK)以及对原 Tag 进行简单异或等运算，实现 PDA 与射频标签间的双向安全认证。大致步骤为：

(1)PDA 向 Tag 发送随机数 r 和 Query 认证请求。

(2)Tag 使用自己的 ID 和 SK 计算 $a_1=ID\oplus H(r\oplus SK)$，发送 a_1 给 PDA。

(3)PDA 计算 $ID'=a_1\oplus H(r\oplus SK)$，在数据库中查找是否有这样的 ID'，如果有，Tag 则通过初步认证，之后 PDA 产生一个随机数 RSK，计算 $b_0=DT\oplus H(SK)$，$b_1=RSK\oplus H(DT\oplus SK)$，$b_2=H(ID\oplus RSK\oplus SK)$，并发送$\{b_0,b_1,b_2\}$给 Tag。

(4)Tag 收到$\{b_0,b_1,b_2\}$，首先，用 SK 计算 $DT=b_0\oplus H(SK)$，恢复出 DT。如果恢复的 DT 比以前保存的大，则认为其正常并保存，否则停止验证；然后，用 SK 计算 $RSK'=b_1\oplus H(DT\oplus SK)$，$b_2'=H(ID\oplus RSK'\oplus SK)$，如果 $b_2'=b_2$，说明 $RSK'=RSK$，通过对 PDA 的验证；最后，计算 $a_2=H(r\oplus SK\oplus RSK\oplus DT)$，并发送 a_2 给 PDA 作为应答，该应答既确认收到 RSK，又证明 Tag 是整个认证会话的参与者。如果 DT 不正常或者 RSK 无效，则 Tag 忽略此次收到的消息，持续保持静默。

(5)PDA 收到 a_2，并计算 $a_2'=H(r\oplus SK\oplus RSK\oplus DT)$，如果 $a_2=a_2'$，则对 Tag 的认证通过，否则认证错误，从而完成双向身份认证。图 2 为其认证流程示意图。

在该认证过程中，Hash 函数的单向性确保了从认证消息中无法获取 SK、标签 ID、时间戳 DT 等敏感信息；采用的共享 SK 使得 PDA 和 Tag 可以对收到的消息进行正确性和完整性验证，从而确保认证消息、时间戳 DT 和 RSK 的机密性；时间戳既可以作为认证的参照，又可以作为会话序号，防止重放攻击；认证采用双向认证的机制可以有效防止未授权的阅读器和假冒的标签参与会话，增加认证的安全性。与基于传统加密算法相比，该双向认证在 (►►下转第 18 页►►)

站姿医护人员：30 min 时，站姿医护人员所在区域的温度和相对湿度数值明显下降，空气流速数值略微上升，处于“舒适”等级；60 min 时，站姿医护人员所在区域的空气流速数值不变，温度和相对湿度数值进一步下降，仍处于“舒适”等级。“舒适”等级的最大关联度值 0.932(60 min)>0.902(30 min)，站姿医护人员 60 min 时的热舒适性感觉优于 30 min 时的热舒适性感觉。

6　结论

(1)试验前急救车舱室外空气质量处于高温高湿条件，由于舱壁的阻挡，舱室内空气流速小于舱室外，舱室内人体热舒适性小于舱室外人体热舒适性。

(2)开启制冷空调 30 min 时，舱室内卧姿伤病员、坐姿伤病员、站姿医护人员的热舒适性评价等级分别达到“最舒适”和“舒适”等级；60 min 时舱室内人员的热舒适性感觉进一步提高。

(3)30 min 和 60 min 时，卧姿伤病员的热舒适性略优于坐姿伤病员和站姿医护人员，且左侧卧姿伤病员的热舒适性优于右侧。

总之，综合考虑舱室空气质量的各因素指标的关联作用，采用灰色关联度的方法评价常规条件下舱室空气质量对人体热舒适性的影响，依据最大关联度来判断人体热舒适性等级，既能确定舱室内不同区域人员的热舒适性等级，又能对同等级人员的热舒适性感觉进行比较。评价结果与试验时人员实际热舒适性感觉相一致，且更为准确地对人体热舒适性感觉进行了量化，结果直观。

[参考文献]

[1] 龙升照，黄端生，陈道木，等. 人-机-环境系统工程理论及应用基础[M]. 北京：科学出版社，2004，8：160-216.

[2] 纪秀玲，李国忠，戴自祝. 室内热环境舒适性的影响因素及预测评价研究进展[J]. 卫生研究，2003，32(3)：295-299.

[3] GJB 6805—2009 野战卫生舱室微环境质量要求和评价方法[S].

[4] GB/T 18883—2002 室内空气质量标准[S].

[5] GB 50019—2003 采暖通风与空气调节设计规范[S].

[6] 徐小林，李百战，罗明智. 室内热湿环境对人体舒适性的影响分析[J]. 制冷与空调，2004(4)：55-58.

[7] 殷　平. 冰蓄冷低温送风系统设计方法(1)：室内计算参数、舒适感、室内空气品质[J]. 暖通空调，2004，34(5)：59-65.

[8] 苗　平. 湿空气对人体舒适性的影响 [J]. 洁净与空调技术，2003(4)：13-16.

[9] 周西文，马爱华，王　雨. 湿热和热舒适性与空调节能的探讨[J]. 山西建筑，2008，34(6)：245-246.

[10] 王德刚. 机动卫生装备舱室微环境质量要求与评价方法研究[D]. 北京：军事医学科学院，2008：12-71.

[11] 刘思峰，郭天榜，党耀国，等. 灰色系统理论及其应用[M]. 2 版. 北京：科学出版社，1999，10：40-77.

(收稿：2011-04-20　修回：2011-05-28)

(◀◀上接第 11 页◀◀)

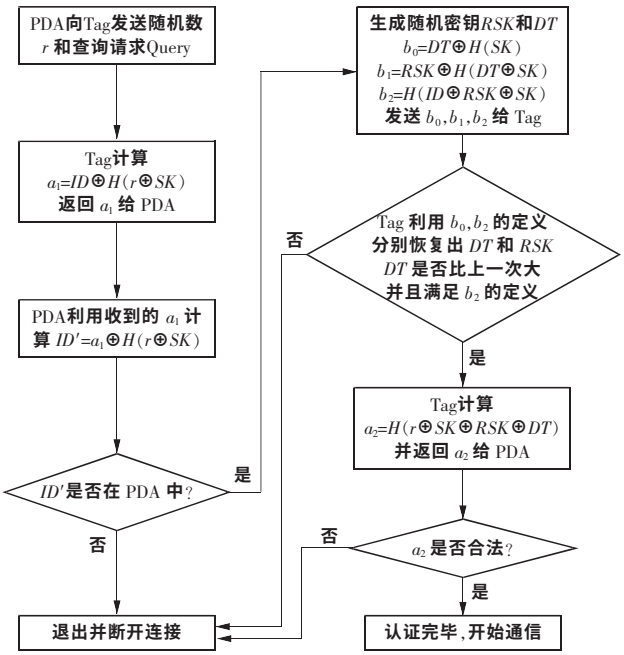

图 2　PDA 与 Tag 认证流程示意图

计算量和通信量上对 RFID 标签是适度的，并可针对应用的不同需求，选择不同 Hash 函数等加密变换。

4　结语

本文提出一种基于 RFID 技术的物资安全保障方案，在方案中事先约定了 RFID 标签的编码格式，PDA 只有与后方数据库连接、解析才能获得应急保障物资的详细内容；同时在 PDA 与 RFID 之间建立基于哈希函数的安全双向认证机制，实现了射频标签与 PDA 读卡器之间编码的安全读取与通讯，从而较好地解决了卫生分队外出应急保障中物资应急供应的安全。

[参考文献]

[1] 杨腾驰，刘勋海. 伊拉克战争物资保障的基本特点及其对我军的启示[J]. 军事经济研究，2003(6)：8-11.

[2] 陈斗雪，黎毅明，陈一天，等. 无线射频识别一起在制造业中的应用[J]. 计算机工程与设计，2006(8)：17.

[3] 赵宏涛. 论 RFID 在军事物流中的应用 [J]. 物流科技，2005(28)：45.

[4] 吴华森，张有光，王赵波. 移动 RFID 系统架构及标准体系研究[J]. 2009(12)：40-43.

[5] 常振华，陈　越，邵　婧，等. 一种 RFID 隐私保护双向认真协议[J]. 2008(15)：80-82.

[6] 唐志军，何怡刚. 基于隐私保护的超高频移动无线识别(RFID)系统安全性研究[J]. 中国安全科学学报，2009(12)：108-114.

[7] I.J Jung Kim，Eun Young Choi，Dong Hoon Lee. Secure Mobile RFID system against privacy and security problems[C]//Security，Privacy and Trust in Pervasive and Ubiquitous Computing Third International Workshop on. Istanbul：2007：67-72.

(收稿：2011-03-14　修回：2011-06-15)