一种应用于军事物流领域的无源 RFID 标签的身份认证方法

林亚忠[1],万任华[1],林村河[1],王 苓[1],郝 刚[2]
(1.解放军 175 医院,厦门大学附属东南医院,福建漳州 363000;
2.厦门大学计算机科学系,福建厦门 361005)

[摘要] 目的:设计一种针对无源 RFID 标签的身份认证方法。方法:考虑到无源标签的弱计算能力,使用简单高效的哈希函数进行运算比较。结果:实现了阅读器与 RFID 标签之间的双向身份认证,从而保障了物流运输的安全。结论:该方法可以有效地增强战时环境下军事物资 RFID 标签的安全性。

[关键字] 射频识别技术;军事物流;哈希函数;身份认证
[中国图书资料分类号] TP391;R318;R82 [文献标识码] A [文章编号] 1003-8868(2012)02-0033-03

Identity Authentication Method for Passive RFID Tags in Field of Military Logistics

LIN Ya-zhong[1], WAN Ren-hua[1], LIN Cun-he[1], WANG Ling[1], HAO Gang[2]
(1. The 175th Hospital of the PLA, the Southeast Hospital Affiliated to Xiamen University, Zhangzhou 363000, Fujian Province, China; 2. Computer Science Department, Xiamen University, Xiamen 361005, Fujian Province, China)

Abstract Objective To design an authentication method for passive RFID tag. Methods Taking the weak computing ability of passive tags into account, the simple and efficient Hash function was used for computing and comparing. Results Two-way authentication between the reader and RFID tags was realized, which could protect the safety of our military logistics. Conclusion This method can effectively improve the security of the RFID tags of military supplies during the war.[Chinese Medical Equipment Journal,2011,33(2):33-34,40]

Key words radio frequency identification; military logistics; Hash function; identity authentication

1 引言

RFID 技术又称射频识别技术,是一种通过射频信号自动识别目标并获取相关信息的技术。由于其具有体积小、操作简单、无接触式感应等特点,已被广泛地应用于物流运输领域[1]。军事物流是在战争状态下开展的一种特殊形式的物流活动,它利用 RFID 技术可方便地对军事物资的存储、运输、分发等过程进行有效监督。自动化识别提高了物资管理的效率,减少了不必要的浪费,军事物资被及时、准确地运输到战场前线,从而为战争的胜利提供了可靠的保障。但是,RFID 技术的使用也为敌方干扰提供了可乘之机,主要威胁概括为 2 个方面:(1)敌方使用自己的 RFID 阅读器在一定距离内读取我方军事物资类别,从而进行有针对性的打击,摧毁我方重要物资,在战场上占得先机;(2)如果敌方占有我方一个物流基地后,由于物流基地存在网络与后方指挥所相连,敌方通过使用我方基地的 RFID 读取设备去读取一些虚假的 RFID 芯片信息,将直接干扰我方后端数据库信息,影响指挥所的物资配送。这 2 个方面的威胁都会对我军的战略部署起消极作用。为此,在军事物流领域引入 RFID 的身份认证机制是十分必要的,具有非常重要的现实意义。

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,博士,硕士生导师,高级工程师,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;万任华(1965—),男,主任医师,院长,主要从事医院和卫勤信息化管理方面的研究工作。
通讯作者:万任华,E-mail:yqwyywrhua@tom.com

2 RFID 技术

2.1 RFID 技术介绍

RFID 技术是一种利用射频信号经空间磁场耦合实现无接触信息传递,并通过所传递的信息达到自动识别目标的技术[2-3]。一个 RFID 系统通常由 RFID 阅读器、RFID 标签(内含 RFID 芯片)和后端数据库组成。RFID 阅读器可以是灵活移动的手持设备,也可以被安装在门或其他固定的设施上,在军事物资到达后,阅读器内的天线与 RFID 标签内的天线进行通信,从而对物资进行快速扫描和识别,并与后端数据库进行交互。目前,RFID 标签分为无源型、半无源型和有源型标签等 3 种。无源型标签由 RFID 阅读器发出的能量来驱动通信,标签内部无电池,适合在较短范围内进行信息传递,价格低廉;半无源型标签含有电池,用于维持芯片内部的易失性内存,这种类型的标签仍由阅读器发出的能量来激发;有源型标签是一种比较昂贵的标签,它内部的电池由于主动发送一定频率的信号,当阅读器的射频信号和该信号耦合时,便可进行通信。后端数据库用于记录所有军事物资的类别、数量以及具体使用信息等,它随着物资的储存、运输和分发,处于不断的更新过程中,使得指挥所对部队物资情况能有全面的了解,从而进行有效地调配。

RFID 技术较之传统的条形码技术,在效率、识别距离、容量、耐用性方面有较大的提高[4]。在效率方面,条形码读取器一次只能读取一个条形码,且常常需要多于 1 s 的时间,而 RFID 阅读器可同时读取多个 RFID 芯片信息,且需要的时间更短;在识别距离方面,条形码技术为几厘米到十几厘米,RFID 技术可以到几米的距离;在容量方面,条形码技术含有的信息量极小,通常只记录了货物的类别,并且是只可读不可写,RFID 的容量可以达到兆字节的数量级,并可进行自由读

写；在耐用性方面，条形码标签易磨损，易受恶劣环境影响，导致无法读取结果，RFID 芯片抗污染性强，本身的外壳可以很好地保护芯片。虽然在价格方面 RFID 芯片要高于条形码，但 RFID 技术的优点是条形码技术无法比拟的，所以 RFID 技术在物流管理方面发挥着越来越重要的作用。

2.2　RFID 技术在战场的应用情况

RFID 技术已广泛应用于美国的军事物流领域，在伊拉克战争和阿富汗战争中取得了良好的实战效果。在 1991 年的海湾战争中，美国 2 万多个集装箱由于标记不明需要打开登记并重新进行封装运输，极大地降低了物流配送的效率。在战争结束后，仍然有 8 000 多个未使用的集装箱物资，造成了大约 20 亿美元的浪费。反观伊拉克战争，由于采用了 RFID 技术来追踪 4 万个物资集装箱的流动，使得物资在储存、运输、分送过程中得到有效的管理，给前线作战部队提供了可靠的后勤保障。与海湾战争相比，伊拉克战争海运量减少了 87%，空运量减少了 88.6%，战略支援装备动员量减少了 89%，战役物资储备量减少了 75%，为美国国防部节省了几十亿元的开支，满足了战场对军用物资的需求。在阿富汗战争中，美国在军队物资上贴有无源型 EPCGen2UHF 标签，用于仓储追踪；同时货物集装箱采用了 433 MHz 有源型 RFID 标签，运输途中标签被沿途 RFID 固定阅读器读取，对集装箱实时跟踪，有效地实现了对军事战略物资的合理管控。

2.3　RFID 技术存在的安全问题及改进

随着 RFID 技术在军事物流领域的普及，它的安全问题也变得越来越重要。由于 RFID 标签可以在一定范围内接收到 RFID 阅读器发出的信号，在战争条件下，敌方可以利用 RFID 阅读器在物资运输途中获取对方物资信息，对物资进行有针对性的打击，另外还可以预测对方的战略意图，使对方陷入不利局面；同时，若敌方攻占了对方在前线的物流中转基地，利用基地中、后端数据库联网的 RFID 阅读器读取虚假的 RFID 标签，便可轻而易举地扰乱对方后端数据库的信息，这种伪装的信息将对后方指挥所的物流管理产生消极的影响。

针对 RFID 技术的安全问题，致力于推动 RFID 电子产品标准的 EPCglobal 所制定的新标准中包含了“Kill”命令[5]，通过使用此命令可以使 RFID 标签丧失功能，使阅读器无法读出标签内的数据。但是，“Kill”命令是不可逆的操作，如果在军事物流领域中使用，必须在物资到达前线物流中转基地并被分发完毕后方可进行，但在物资运输途中仍会受到敌方的窃听。IBM 公司开发了一种“裁剪标签”技术，可以将标签上的天线扯掉或刮除，使标签不能被随意读取，使用这项技术，尽管天线不能再用，但 RFID 阅读器仍然能够直接读取标签内容。鉴于无源 RFID 标签计算能力弱且价格低廉，预计在不久的将来会在军事物流领域得到广泛地应用。因此，可以利用无源 RFID 标签简单高效的双向身份认证机制，实现在战场环境下对标签信息的有效保护，为物流的合理配送提供安全保障。

3　一种新的 RFID 身份认证方法

3.1　身份认证方法

身份认证方法是确认操作者身份的过程而产生的解决方法[6]。目前，身份认证方法主要分为 3 种：(1)根据信息来证明身份，例如常见的用户名/密码登录。每个用户的密码由用户自己设定，只有用户自己才知道。只要能够正确输入密码，系统就认为操作者是合法用户，密码泄露是该方法常见的问题。(2)根据所拥有的物品或设备来证明身份，常见的如动态口令卡。动态口令技术是一种让用户密码按照时间或使用次数不断变化、每个密码只能使用一次的技术，用户使用时只需要将动态口令卡上显示的当前密码输入系统，即可实现身份认证，由于每次使用的密码必须由动态口令卡来产生，只有合法用户才持有该卡，所以只要通过密码验证就可以认为该用户是可靠的，而用户每次使用的密码都不相同，即使密码被获取了，也无法通过下次身份认证。(3)根据独一无二的身体特征来证明身份，例如指纹、虹膜等，通过可测量的身体特征或行为进行身份认证，具有较强的安全性。

3.2　应用于军事物流领域的无源 RFID 标签的身份认证方法

为了防止敌方阅读器读取无源 RFID 标签内的信息，同时为了防止敌方利用我方阅读器读取虚假 RFID 标签，进而干扰后端数据库数据，本研究提出一种针对无源 RFID 标签的简单高效的身份认证方法，根据所知道的信息来证明自己的身份，将信息输入 hash 函数进行少量的运算，使用较短的时间达到阅读器与标签双向身份认证的目的。如果认证通过，阅读器就可以操作无源标签内的数据了，如果计算得到的结果错误，则断开连接。

双向身份认证的原理：每一个数字设备，包括阅读器和无源 RFID 标签，内部都存在一个唯一的数字序列 ID，用于标识自己的身份，另外这些设备内还保存有一个唯一的 2 位数数字 m，该数字也可叫做滑动窗口。hash 函数的定义是平方取中法的变种，将输入的数字序列 ID 进行平方运算，然后利用滑动窗口 m 从得到的结果中进行截取，2 位数 m 中第 1 位数字用于标识截取的第 1 个数字所在的位置，第 2 位数用于标识截取的长度，通过该 hash 函数运算后得到 1 个数字串，将该数字串与保存在数字设备内的结果进行比较，如果相等，则表示身份认证通过；否则，退出并断开连接。具体流程图见图 1。

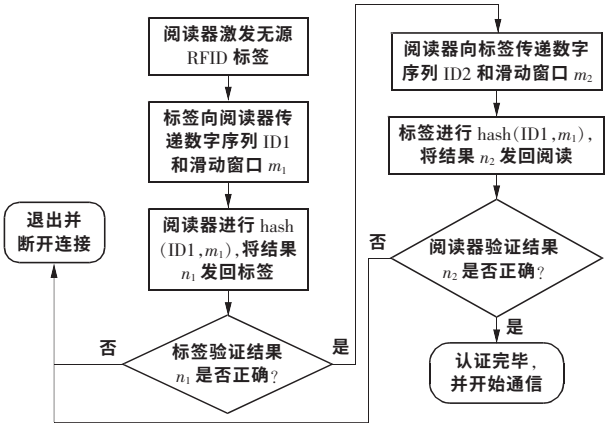

图 1　身份认证流程图

假设无源 RFID 标签数字序列 ID=1 234，m=25，在阅读器激发标签后，标签将(ID,m)发送到阅读器，如果阅读器是我方的设备，则它必然知道 hash 函数的形式，阅读器利用该函数进行运算，1 234×1 234=1 522 756，然后利用滑动窗口 m 进行截取，得到数字序列 52 275，将该数字串发送回标签，标签将数字串与内部存储的数字串进行比较，如果相同，则 RFID 阅读器认证完毕，继续认证标签。双方均认证完毕后，就可以开始通信了。

无源 RFID 标签是一种具有弱计算能力的标签，以上 hash 函数的设计简单高效，认证过程进行了一次整数乘方运算和一次截取运算，花费时间　(►►下转第 40 页►►)

机气道压力、呼出潮气量和折叠风箱的变化，说明开放性囊内吸引装置对麻醉机的机械通气功能没有影响。随着麻醉机吸气期与呼气期周期性更替，开放性囊内吸引装置的储气囊相应地呈现缩小与膨大的变化，气流向颈口内吹动棉丝或棉丝摆动不明显，说明储气囊内气体外逸不明显。

本院吸入麻醉的应用较普遍，8 台麻醉机使用了 1 a 时间没有出现与开放性囊内吸引装置相关的故障。麻醉中气体抽样检测发现，在使用开放性囊内吸引装置后第 2 个储气囊的颈内麻醉废气（氧化亚氮、异氟醚或七氟醚）浓度均接近于零。

4　讨论

19 世纪 60 年代后期，手术室内麻醉废气污染问题得到了广泛的重视[8]。迄今为止，麻醉废气对健康的潜在危害还没有确定性结论，一般认为有以下 4 个方面：(1)影响心理行为，包括听力、记忆力、理解力、读数字能力及操作技能等；(2)影响慢性遗传学，包括慢性中毒、致突变、致畸和致癌作用；(3)影响生育功能，包括生殖能力、交配行为、胚胎流产、胎儿致畸、先天异常、产后存活及行为表现，这是手术室女性工作人员最关注的问题；(4)器官毒性，包括肝、肾、脑功能损害。目前，以 AGSS 为代表的手术室净化装置在临床中得到越来越多的应用，它的应用可以减少 90%以上的手术室内麻醉废气污染，使麻醉机的临床应用风险得到有效控制，同时也积极地推动了吸入性麻醉药的发展。在发达国家，每一个手术室都有完善的 AGSS，以保证吸入性麻醉药对手术室的空气污染最小化。洁净的手术室环境不但能使手术室工作人员在整个麻醉过程中保持清醒的头脑，而且能更有效地保障手术室工作人员的健康。由于受到设备条件的限制，国内麻醉废气清除设备远远落后于国外发达国家，因此，因地制宜地研制开放性囊内吸引装置具有积极的临床意义。

在开放性囊内吸引装置的结构中，第 2 个储气囊的颈口保持开放，其内部的透气管保证气流顺畅，吸引器连接管的吸引端位于第 1 个储气囊的颈内，远离麻醉机废气排放口，因此，大气不能压瘪储气囊，负压就不会传至麻醉机呼吸回路内，也不会增加气道阻力，从而不会危及患者安全。在麻醉机呼气期，麻醉废气瞬间快速排出，第 1 个橡胶储气囊具有暂时储存已排出的麻醉废气和缓冲气流的作用，并且只吸出已排出的麻醉废气，而不影响麻醉机呼吸回路内的正常运行气体，但囊内吸引端并不能在呼气瞬间及时把麻醉废气完全吸出，余下的麻醉废气可以暂时进入第 2 个储气囊内；在麻醉机吸气期，囊内吸引端继续吸引储气囊内的剩余麻醉废气，使麻醉废气在没有到达第 2 个储气囊的颈口之前就基本上被吸出；如此反复，就可以顺利地使用小口径加强软管将较大量的麻醉废气排出手术室外，故手术室工作人员无麻醉废气污染之虞。

中心负压吸引终端是排放麻醉废气的动力源，负压吸引力范围一般为-0.03~-0.07 MPa，或吸引流量为 30 L/min，只要中心负压吸引终端条件完好，储气囊内的麻醉废气就不会明显外逸，而负压不足可以导致麻醉废气吸出不完全。由于麻醉机呼吸回路的差异性设计，不同麻醉机产生的麻醉废气量相差甚大，如果麻醉机废气排出量较大，则第 1 个储气囊的容积也要相应增加。为了保证麻醉废气污染最小化，临床应用前必须调试开放性囊内吸引装置，结果以第 2 个储气囊的颈口没有气体流出为宜。

开放性囊内吸引装置没有增加麻醉机的复杂性，它的不足之处是影响麻醉机外观和增加了一些噪音。

总之，开放性囊内吸引装置具有利用废物、制作简单、使用及维护方便的优点，经临床应用证实，效果良好，安全可靠，特别适用于具有中心负压吸引终端和通风系统的洁净手术室。使用开放性囊内吸引装置后麻醉医师不必再担心麻醉废气污染手术室的问题。

[参考文献]

[1] 中华医学会麻醉学分会. 关于处理麻醉气体泄漏的专家共识[J]. 临床麻醉学杂志，2009，25(3)：194-196.

[2] Irwin M G，Trinh T，Yao C L. Occupational exposure to anaesthetic gases：a role for TIVA[J]. Expert Opin Drug Saf，2009，8(4)：473-483.

[3] 王　艳，褚艳梅. 手术室的麻醉废气污染调查与干预对策[J]. 现代保健：医学创新研究，2007(8)：75-76.

[4] Smith F D. Management of exposure to waste anesthetic gases[J]. AORN J，2010，91(4)：482-494.

[5] 蔡定球，潘　琳，汪小海，等. 自制麻醉废气清除装置临床实用性研究[J]. 医疗卫生装备，2008，29(5)：97-98.

[6] 胡雁东，梁晋彬，宋晋华. 介绍一种麻醉废气排除装置[J]. 中国医疗器械杂志，2009，33(1)：67-68.

[7] 梁以钊，黄文祥，谭宏峰，等. 麻醉机废气排除装置的改进[J]. 医疗装备，2007，20(5)：5-6.

[8] 张书芳. 中心吸收在麻醉排污中的应用[J]. 中国医疗器械杂志，1995，19(6)：356-357.

（收稿：2011-03-30　修回：2011-05-09）

（◀◀上接第 34 页◀◀）

较短，适合在此类标签上部署，可以有效地抵御前文提到的 2 种威胁，为军事物资的安全运输提供了可靠保障。

4　结语

RFID 技术是目前较先进的自动识别技术，将它应用在军事物流领域，极大地提高了军事物资管理效率。但是，随着 RFID 技术的应用普及，安全问题也随之而来。本文针对无源标签的弱计算能力，提出专门针对无源 RFID 标签的身份认证方法，通过使用简单的 hash 函数实现对阅读器和 RFID 标签之间的双向身份验证。实践证明，该方法可以有效地防止战争情况下附有无源标签的军用物资在传输过程中信息被窃取的风险，也可在一定程度上阻止虚假 RFID 标签对后端数据库的干扰，保障了军队物流体系得以安全实施。

[参考文献]

[1] 李　波，刘震宇，谢胜利. RFID 在现代军事领域的应用探讨[J]. 计算机与电信，2006(7)：16-23.

[2] 李苏剑. 无线射频识别技术(RFID)理论与应用[M]. 北京：电子工业出版社，2004.

[3] 申秀兰. RFID 技术在物流中的应用[J]. 条码与信息系统，2006(1)：15-17.

[4] 邵永哲，杨　健，李小将，等. 基于 RFID 技术的军事物流系统构建流程与安全[J]. 物流科技，2009，32(8)：82-85.

[5] 刘长波. RFID 普及遭遇安全问题[J]. 中外物流，2006(8)：90-91.

[6] 施　锋. 信息安全保密基础教程[M]. 北京：北京理工大学出版社，2008.

（收稿：2011-03-28　修回：2011-12-01）