安全的航空物品管理RFID系统

邓淼磊[1,3] 马玉军[2] 石金娥[1] 周利华[3]
(解放军信息工程大学理学院 郑州 450001)[1] (南阳理工学院网络中心 南阳 473004)[2]
(西安电子科技大学计算机学院 西安 710071)[3]

摘 要 在航空物品管理中应用无线射频识别(RFID)技术将带来极大的便利。提出了一个航空物品管理RFID系统模型,对其中存在的安全问题进行了分析,给出了相应的解决方案。并设计了一个应用于航空物品管理的RFID认证协议,该协议可以抵御多种安全威胁。协议的实现基于随机置换函数和异或运算,具有较高的效率。

关键词 无线射频识别,航空物品管理,认证协议,安全
中图法分类号 TP309 **文献标识码** A

Secure RFID System for Aviation Goods Management

DENG Miao-lei[1,3] MA Yu-jun[2] SHI Jin-e[1] ZHOU Li-hua[3]
(Institute of Science, PLA Information Engineering University, Zhengzhou 450001, China)[1]
(Network Information Center, Nanyang Institute of Technology, Nanyang 473004, China)[2]
(School of Computer, Xidian University, Xi'an 710071, China)[3]

Abstract Radio frequency identification (RFID) technology will greatly facilitate aviation goods management. A RFID system model for aviation goods management was proposed and the main security solutions were presented. An authentication protocol for RFID was also designed in this context. The proposed protocol is invulnerable to a number of malicious attacks. The implementation of the protocol is based on random permutation functions and XOR operations, has higher efficiency.

Keywords Radio frequency identification, Aviation goods management, Authentication protocol, Security

无线射频识别(RFID)是一种非接触式自动识别技术,目前已被广泛应用于工业自动化、商业自动化、交通运输控制管理等众多领域。除了传统的应用外,RFID技术还可以用来对航空物品进行自动化管理[1,2],实现对航空物品信息的自动采集、追踪、信息共享和管理,从而大幅提高工作效率,降低管理成本。

在文献[3,4]中,对未来航空RFID系统的应用和结构进行了描述,但对其中存在的安全问题没有给出具体的解决方案。本文提出了一个具体的应用于航空物品自动化管理的RFID系统模型;对其中存在的安全问题进行研究,提出了解决方案;并设计了一个应用于航空物品管理的安全的RFID认证协议。

1 航空物品管理RFID系统模型

航空物品管理RFID系统如图1所示。它由两个子系统构成:机载RFID系统和地面RFID系统。其中地面RFID系统主要包括各个机场RFID处理系统(简单起见,图1中只包含了两个机场RFID处理系统)和航空公司RFID处理系统。

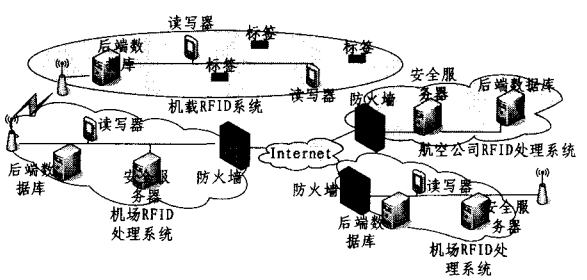

图1 航空物品管理RFID系统

机载RFID系统主要由RFID标签、RFID读写器、RFID后端数据库以及地面通信用天线设备构成。机载RFID系统用于对已经装载到飞机上的物品进行管理。对于需要地面RFID系统协助处理的问题,机载RFID系统的后端数据库把信息发送给临近进场的RFID处理系统,做进一步处理。RFID后端数据库负责对机载读写器进行配置,并负责建立和维护与机场RFID处理系统的无线连接。由于机载RFID系统要与不同国家和地区的机场RFID处理系统进行通信,为了方便地支持各种无线通信标准,机载的后端数据库和各个机场的后端数据库之间的通信使用软件定义无线电[5]

到稿日期:2009-12-02 返修日期:2010-02-10 本文受"十一五"国防科技预研项目资助。
邓淼磊(1977—),男,博士生,主要研究方向为安全协议设计、RFID安全技术,E-mail:dmlei2003@163.com;马玉军(1978—),男,讲师,主要研究方向为计算机网络安全;石金娥(1967—),女,副教授,主要研究方向为应用数学;周利华(1942—),男,教授,博士生导师,主要研究方向为计算机网络安全理论与技术等。

(Software Defined Radio,SDR)实现。SDR 的可编程性可为众多不同类型的无线通信系统提供较好的支持。

机载 RFID 系统中,从 RFID 标签读取的信息根据需要或者由机载的后端数据库处理,或者由机场的后端数据库处理,或者由航空公司 RFID 处理系统处理。其中的每一个 RFID 处理系统都可以根据需要把标签信息转发给其他相关的 RFID 处理系统处理。机场 RFID 处理系统中的后端数据库除了对机载 RFID 系统发来的信息进行处理外,还在物品装机或者卸下飞机时,处理机场 RFID 读写器读取的标签信息。提供认证、授权和审计等服务的安全服务器保证了网络连接的安全性。地面各个 RFID 处理系统之间通过 Internet 进行互联,并在各个系统的边界设置防火墙,以防止非法的访问和其他形式的网络攻击。

2 存在的安全问题及解决方案

在航空物品管理 RFID 系统中,存在的主要安全问题及其解决方案如下:

(1)机载和机场 RFID 系统中读写器对标签的安全识别问题。RFID 读写器和标签间的无线通信方式存在许多安全隐患,攻击者可以进行物理攻击、偷听攻击、重发攻击等;而且 RFID 标签设备只具有有限的计算能力、有限的存储空间和有限的电源供给,这些局限性对 RFID 安全问题的解决带来了特殊的要求。常见的 RFID 硬件安全机制有 Kill 命令[6](Kill Command)、阻塞标签[7](Blocker Tag)、夹子标签[8](Clipped Tag)、假名标签[6](Tag Pseudonyms)、天线能量分析[6](Antenna Energy Analysis)等。与基于物理方法的硬件安全机制相比,基于密码技术的软件安全机制更受到人们的关注。其主要研究内容是利用各种成熟的密码方案和机制来设计和实现符合 RFID 安全需求的协议,例如 Hash-Lock 协议、随机化 Hash-Lock 协议、Hash 链协议、LCAP 协议等。这已经成为当前 RFID 安全研究的热点[9]。本文在第 3 节设计了一个低成本的 RFID 认证协议,以解决 RFID 读写器对标签的安全识别问题。

(2)SDR 安全。为了支持多种无线通信标准,每到一个新的地点,机载无线通信设备就需要重新配置,使得与当地使用的无线通信标准兼容。保证 SDR 的安全就是指要确保相应软件的授权安装和激活、授权的配置管理以及授权的软件更新。对无线通信软件模块可以进行数字签名,这样使用者就可以验证它的完整性以及来源。在图 1 中,机载 RFID 系统中的后端数据库除了负责处理 RFID 读写器发送的标签信息外,还安装有基于 SDR 的无线通信设施。后端数据库负责 SDR 的配置管理,因此它需要获悉临近机场的 GPS 位置和可用的无线连接,从而在多种可用的无线通信标准之间进行正确切换。后端数据库中还应当安装认证模块和访问控制模块,以确保只有授权的实体才能对其进行访问。机场 RFID 处理系统中的后端数据库也具有类似的功能和设置。

(3)机载 RFID 系统和机场 RFID 系统间无线连接的安全。这两个系统中都存在相应的无线通信设备,当它们进行连接时,便构成了一个无线局域网络。无线局域网的开放性导致了它比有线介质更容易受到干扰、窃取和破坏。这里可以采用 IEEE802.11i 协议[10]来加强它们之间连接的安全性能。IEEE802.11i 主要从认证与加密两个方面来加强无线局域网络的安全性。在认证方面,802.11i 使用了 IEEE802.1x,EAP 和动态密钥管理,提供了双向认证和密钥管理功能。在数据加密方面,802.11i 定义了 TKIP,CCMP 和 WRAP 等 3 种加密机制。802.11i 提供的这些安全机制能够很好地满足这里的安全需要。

(4)地面各个 RFID 处理系统间相互连接的安全。地面各个 RFID 处理系统之间通过 Internet 进行互联,运用虚拟专用网(VPN)技术可以保证它们之间连接的安全。这里采用比较成熟的基于 IP Security(IPSec)的 VPN 技术。VPN 通过隧道实现网络互联,它支持用户安全管理,并且能够进行网络监控、故障诊断。

3 RFID 认证协议

本节设计一个 RFID 认证协议,以解决 RFID 读写器和标签的相互认证问题。RFID 读写器的处理能力和存储空间都比较大,而 RFID 标签通常没有微处理器,仅由数千个逻辑门电路组成。RFID 标签有限的计算能力和存储空间以及有限的电源供给都给 RFID 安全协议的设计提出了特殊的要求。一般的 RFID 安全协议都要求是轻量级的。

3.1 安全威胁

RFID 读写器和标签间的无线通讯方式面临许多安全威胁。在航空物品管理 RFID 系统的应用中,具体的安全威胁主要包括如下几种:

(1)窃听攻击。由于读写器和标签之间是无线通信,攻击者可以中途读取读写器和标签之间通信的有效信号,试图获取一些秘密信息。

(2)伪造攻击。伪造攻击也称为克隆攻击。攻击者使用窃听到的标签发射的信号,仿制能够发射相同信号的标签,并使用伪造的标签来标识伪造物品,从而达到非法的目的。

(3)重传攻击。重传攻击也称为回放攻击,它是攻击者通过中途截取读写器和标签之间通信的有效信号,之后将该有效信号在 RFID 系统中重传从而对系统进行的一种攻击。攻击者进行重传攻击的目的是假冒成读写器从而追踪标签,或者假冒成标签从而欺骗读写器。

(4)追踪攻击。攻击者根据协议消息,把某个标签同其他标签一直区分开来,从而进行追踪。

不失一般性,这里假设从 RFID 读写器到后端数据库的通信是安全的,并且在设计的协议中把读写器和后端数据库视为一个整体对待。

3.2 系统设置

读写器(包括后端数据库)和每个标签预先共享的参数有:

(1)T_{ID}。这是标签的唯一性身份标识,$T_{ID}\in\{0,1\}^l$。每个标签都和读写器共享一个不同的身份标识。在协议的执行过程中,需要保证 T_{ID} 的秘密性。

(2)k_1,k_2。这是读写器和标签间共享的两个秘密密钥,$|k_1|=|k_2|=l$。不同的标签和读写器共享的密钥是不相同的。

(3)随机置换函数 F。$F:\{0,1\}^l\rightarrow\{0,1\}^l$,可以使用线性反馈移位寄存器(LFSR)来构造函数 F[11]。由于 F 的构造是公开的,因此攻击者也能够构造出 F。

在读写器端,除了共享参数外,还另外存储有两个随机

数：r_n 和 r_{n+1}，$r_n \in \{0,1\}^l$，$r_{n+1} \in \{0,1\}^l$。r_n 是执行本轮协议时读写器发送的随机数，在成功完成本轮协议后，读写器在执行下一轮协议时将向标签发送 r_{n+1}。

在标签端，除了共享参数外，还包含另外一个随机置换函数 P，$P:\{0,1\}^l \rightarrow \{0,1\}^l$。这里 P 函数是由物理防克隆函数(PUF)[12]构造的。PUF 函数具有物理防克隆特性；即使每个标签中的 P 函数具有相同的物理结构，对于相同的输入，每个标签中的 P 函数也将生成不同的输出。这样，如果攻击者攻陷了一个标签，它也不能制造出一个与被攻陷标签行为完全一样的标签。读写器中存储的 r_n 和 r_{n+1} 具有如下关系：$r_{n+1}=P(r_n)$。

3.3 协议描述

用 R 表示读写器，用 T 表示标签，设计的认证协议如图 2 所示。描述如下：

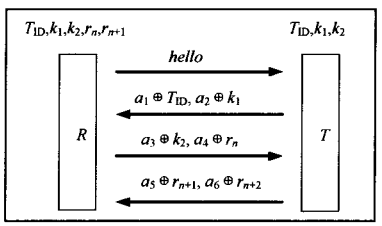

图 2 RFID 认证协议

(1)$R \rightarrow T$：R 向 T 广播“*hello*”消息。

(2)$T \rightarrow R$：T 生成一个随机数 a_1，然后计算出另一个随机数 $a_2=F(a_1)$，向 R 发送消息 $a_1 \oplus T_{ID}$ 和 $a_2 \oplus k_1$。

(3)$R \rightarrow T$：令 $m_1=a_1 \oplus T_{ID}$，$m_2=a_2 \oplus k_1$；R 在数据库中查找一条记录，使其满足 $F(T_{ID} \oplus m_1)=k_1 \oplus m_2$。如果查找不到这样的记录，那么协议停止。否则 R 计算 $a_3=F(a_2)$ 和 $a_4=F(a_3)$，向 T 回复消息 $a_3 \oplus k_2$ 和 $a_4 \oplus r_n$。

(4)$T \rightarrow R$：令 $m_3=a_3 \oplus k_2$，$m_4=a_4 \oplus r_n$；T 计算 $a_3=F(a_2)$，验证 $k_2=a_3 \oplus m_3$ 是否成立。如果成立，那么 T 通过对 R 的认证(这是因为只有合法的 R 拥有密钥 k_2)；然后 T 计算 $a_4=F(a_3)$，$a_5=F(a_4)$，$a_6=F(a_5)$ 以及 $r_n=a_4 \oplus m_4$，$r_{n+1}=P(r_n)$，$r_{n+2}=P(r_{n+1})$，并向 R 发送消息 $a_5 \oplus r_{n+1}$ 和 $a_6 \oplus r_{n+2}$。

(5)R：令 $m_5=a_5 \oplus r_{n+1}$，$m_6=a_6 \oplus r_{n+2}$；R 计算 $a_5=F(a_4)$，$a_6=F(a_5)$ 以及 $r_{n+1}=a_5 \oplus m_5$，$r_{n+2}=a_6 \oplus m_6$。R 检查计算得到的 r_{n+1} 值和存储的值是否相等。如果相等，那么 R 通过对 T 的认证(这是因为只有目标标签 T 才能生成 r_{n+1})，并用 r_{n+1} 和 r_{n+2} 的值分别更新数据库中存储的 r_n 和 r_{n+1} 的值：$r_n \leftarrow r_{n+1}$，$r_{n+1} \leftarrow r_{n+2}$。

3.4 安全分析

设协议的攻击者为 A，A 具有一般 RFID 安全协议攻击者的能力。下面说明设计的协议能够抵御 3.1 节描述的各种攻击。

(1)窃听攻击

在这种攻击中，攻击者 A 窃听读写器和标签间的通信，以期望获悉诸如标签的唯一性身份标识、密钥等秘密信息。

在设计的协议中，所有传输的秘密信息都和一些随机数进行了异或运算，而且这些随机数在每轮协议运行中都不相同。根据香农的理论[13]，通过异或加密保证了这些秘密信息的安全性。另外，由于 A 不知道 F 函数的种子(即标签生成的随机数 a_1)，这样即使 A 知道 F 函数的构造，对 A 也没有任何帮助。

(2)伪造攻击

在这种攻击中，A 通过模仿 P 函数的行为或者其他物理方法来克隆标签。

在设计的协议中，P 函数是基于 PUF 电路实现的，它能够防止对标签的物理攻击。并且这样的 P 函数具有防克隆特性；如果 A 通过某种方式把一个合法标签中的内容复制到一个伪造的标签中，由于不存在两个具有相同行为特征的 PUF 电路，伪造的标签将不能模仿原始标签的行为。

(3)重传攻击

在这种攻击中，A 或者重传标签发送过的消息以假冒成标签，或者重传读写器发送过的消息以假冒读写器。

在设计的协议中，当读写器接收到最后一条消息，通过对标签的认证后，就对存储的 r_n 和 r_{n+1} 值进行更新。这样 A 如果重传旧的标签消息，将不能通过 R 的认证。

另一方面，由于标签每次生成的随机数都不相同并且对 A 保密，这样 A 如果重传旧的读写器消息，将不能通过 T 的认证。

(4)追踪攻击

假设 A 企图追踪标签 T。如果 A 能够持续地把 T 与其他标签区分开来，A 就攻击成功。A 的这种攻击通常是通过重复使用一个能使 T 产生固定答复的询问来实现的。在设计的协议中，由于 T 每次生成的随机数都不相同，A 的这种攻击显然不能成功。

结束语 本文描述的航空物品管理 RFID 系统，本质上是一个通用的航空管理 RFID 系统，它不仅可以用来对航空物品进行自动化的管理，通过修改相应数据，还可以用于其他航空事物的自动化管理，例如对乘务人员或乘客进行跟踪和定位，对飞机维护和检修人员进行认证以及对各种维修工具进行管理等。

随着 RFID 技术在航空中的应用，它的安全性必将引起各界的关注。本文针对应用中存在的安全问题提出了解决方案；设计的 RFID 认证协议可以实现标签和读写器的双向认证，并且标签和读写器端的运算都比较简单，从而具有较高的效率和安全性。

参 考 文 献

[1] Ouyang Y, Hou Y, Pang L, et al. An Intelligent RFID Reader and Its Application in Airport Baggage Handling System [C]// 4th International Conf. on Wireless Communication, Networking and Mobile Computing. New York: IEEE Press, 2008: 1-4

[2] Luo M, Liu W, Aw L L, et al. Evaluation of enabling RFID technology on the operation visibility in MRO plant [C]//4th IEEE Conf. on Industrial Electronics and Applications. Singapore: IEEE Press, 2009: 2540-2545

[3] Falk R, Kohlmayer F, Kopf A, et al. High-assurance SDR based avionics RFID system [C]// SDR 07 Technical Conference and Product Exposition. Berlin-Heidelberg: Springer-Verlag, 2007: 11-17

[4] Chang Y S, Oh C H, Whang Y S, et al. Development of RFID Enabled Aircraft Maintenance System [C]// International on Industrial Informatics. New York: IEEE Press, 2006: 224-229

[5] Mar J, Kuo C C, Lin Y R, et al. Design of software-defined radio

channel simulator for wireless communications: case study with DSRC and UWB channels [J]. IEEE Transactions on Instrumentation and Measurement, 2009, 58(8): 2755-2766

[6] Garfinkel S L, Juels A, Pappu R. RFID privacy: an overview of problems and proposed solutions [J]. Security & Privacy Magazine, 2005, 3(3): 34-43

[7] Juels A, Rivest R L, et al. The blocker tag: selective blocking of RFID tags for consumer privacy [C]// 10th Conf. on Computer and communications security. Washington: ACM Press, 2003: 103-111

[8] Karjoth G, Moskowitz P A. Disabling RFID tags with visible confirmation: clipped tags are silenced [C]// ACM Workshop on Privacy in Electronic Society. Alexandria: ACM Press, 2005: 27-30

[9] 邓森磊，马建峰，周利华. RFID匿名认证协议的设计 [J]. 通信学报，2009，30(7)：20-26

[10] IEEE Std 802.11i™ Amendment 6: Medium Access Control (MAC) Security Enhancements [S]

[11] Goldreich O. Foundations of Cryptography [M]. Cambridge: Cambridge University Press, 2001

[12] Bolotnyy L, Robins G. Physically unclonable function-based security and privacy in RFID systems [C]// 5th Conf. on Pervasive Computing and Communications. Washington: IEEE Press, 2007: 211-220

[13] Shannon C. Communication Theory of Secrecy Systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715

(上接第 91 页)

会造成控制应用的实时性不佳；(2)大的延迟比波动会带来较大比率的线程或连接数调整，增加系统开销，从而对请求延迟造成影响。

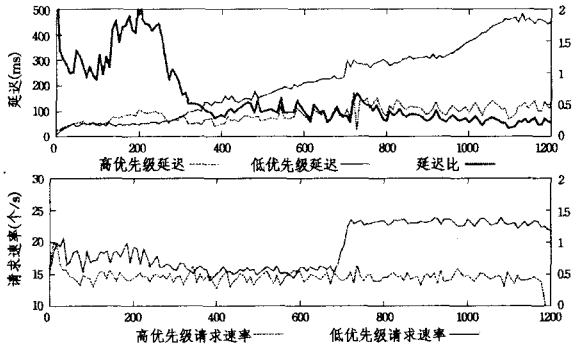

图 5 低优先级请求变化时的比例延迟保证

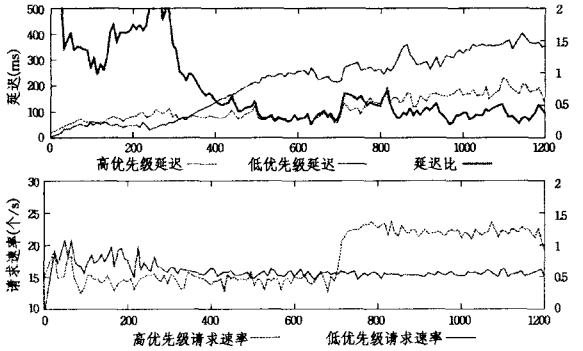

图 6 高优先级请求变化时的比例延迟保证

结束语 本文研究了基于多层 Web 应用的区分服务，提出并实现了一种支持比例延迟保证的多层 Web 应用的多输入多输出模型。通过系统辨识建立系统状态空间模型，并在此基础上完成了状态反馈控制器的设计。最后，在 Windows 平台下，修改了 Apache 源码以及 Tomcat 的 Servlet，并分别采用 TPC-W 基准进行了实验，验证了系统模型的有效性，实现了比例延迟保证。但同时实验结果也暴露了很多的不足。下一步工作应该更加深入研究多层 Web 应用，并寻找更贴近该系统的数学模型及其控制器的设计。

参 考 文 献

[1] Mogul J C. Operating systems support for busy internet servers [C]// Fifth Workshop on Hot Topics in Operating Systems (HotOS-V). Orcas Island, WA, 1995

[2] Barford P, Crovella M. Generating representative web workloads for network and server performance evaluation[C]// Measurement and Modeling of Computer systems. 1998: 151-160

[3] Diao Y, Hellerstein J L, Parekh S, et al. Modeling differentiated dervices of multi-tier Web applications[C]// 14th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). 2006

[4] Kamra A, Misra V, Nahum E M. Yaksha: A self-tuning controller for managing the performance of 3-tiered web sites[C]// Proceedings of the Twelfth International Workshop on Quality of Service (IWQoS 2004). Montreal, Canada, 2004

[5] Liu Xue, Heo Jin, Sha Lui, et al. Adaptive Control of Multi-tiered Web Application Using Queueing Predictor[C]// Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS 2006). Vancouver, Canada, 2006

[6] Karlsson M, Zhu Xiaoyun, Karamanolis C. An adaptive optimal controller for non-intrusive performance differentiation in computing services[C]// International Conference on Control and Automation (ICCA 05). 2005

[7] Diao Yixin, Hellerstein J L, Parekh S, et al. Controlling Quality of Service in Multi-tier Web Applications[C]// Proceedings of the 26th IEEE International Conference on Distributed Computing Systems(ICDCS 06). 2006

[8] Liu Xue, Zhu Xiaoyun, Padala P, et al. Optimal Multivariate Control for Differentiated Services on a Shared Hosting Platform [C]// Proceedings of the 46th IEEE Conference on Decision and Control (CDC'07). New Orleans, LA, 2007

[9] Hellerstein J L, Diao Yixin, Parekh S. Feedback control of computing systems[M]. Wiley-IEEE Press

[10] Bezenek T, Cain H, Dickson R, et al. Characterizing a Java Implementationn of TPC-W[C]// 3rd Workshop On Computer Architecture Evaluation Using Commercial Workloads (CAECW). Toulouse, France, January 2000