文章编号：1005-8451（2015）02-0079-04

基于物联网的铁路客票系统及其安全策略的探讨

周泽岩
（中国铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：本文分析铁路客票系统的局限性，根据物联网的3层体系结构，设计一套基于物联网技术的铁路客票系统，能有效解决系统操作效率低下的问题，提高旅客的通行效率。并对信息安全问题进行分析，提出整体的信息安全体系架构。

关键词：铁路客票系统；物联网；安全策略；信息安全
中图分类号：U29-39 **文献标识码：**A

Railway Ticketing and Reservation System and its security strategy based on Internet of Things

ZHOU Zeyan
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: This paper analyzed the limitations of the existing Railway Ticketing and Reservation System, designed a new Railway Ticketing and Reservation System based on the technology of the Internet of Things, solved the problem of low operation efficiency, improved the efficiency of traffic passenger, analyzed the problems of information security, put forward the information security solution.

Key words: Railway Ticketing and Reservation System; Internet of Things; security policy; information security

近些年，随着高速铁路建设的迅速发展，铁路依然是人们主要的出行方式，为了满足铁路客运的高密度运营需求，亟待提高铁路客票系统的工作效率和自动化水平，铁路客票系统与物联网的结合将是铁路信息科技发展的必然结果。

1 物联网

物联网是指通过射频识别（RFID）、红外感应、全球定位、激光扫描等信息传感设备，按约定的协议，把任何物体与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络[1]。

从通信对象和过程来看，物联网的核心是物与物、人与物之间的信息交互，物联网的基本特征可概括为全面感知、可靠传输和智能处理[2]。

（1）全面感知：利用无线射频识别、二维码、定位器、传感器等技术随时随地对物体的信息进行采集和获取；

（2）可靠传输：通过电信网络和互联网等信息网络，对接收到的信息进行实时传输，实现物体的信息共享与交互。

（3）智能处理：利用各种智能计算技术（云计算、模糊识别等），对海量的感知数据和信息进行分析和处理，实现智能化的决策和控制。

物联网的体系结构划分为3层：感知层、网络层和应用层，如图1所示。感知层，用于感知和识别物体，采集和获取物体信息。网络层，作为数据信息传输的基础设备，包括电信网、互联网等通信网络。应用层，是将物联网技术与各行业领域的专业技术相结合，实现各种智能化的解决方案，例如智能家居、智能交通、智能工业控制等。

2 铁路客票系统的局限性

中国铁路客票发售与预订系统（简称铁路客票

收稿日期：2014-10-08
作者简介：周泽岩，工程师。

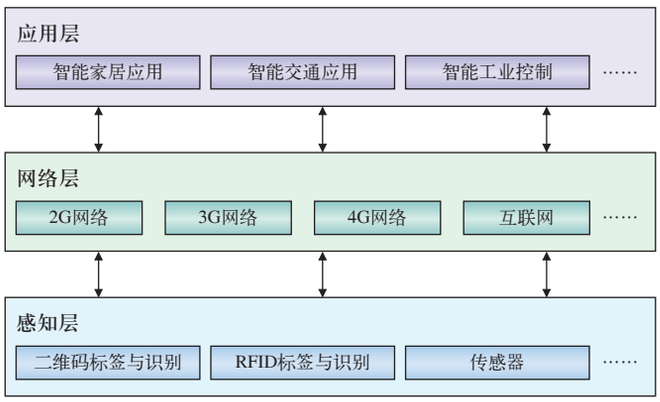

图1 物联网体系结构图

系统）从 1996 年开始建设，先后完成 6 次升级，覆盖全国的客票系统实现了全国联网异地售票，形成了铁总中心、地区中心、车站 3 层网络架构，各层之间通过客票专网相连 [3]。随着电话订票、互联网购票、网银在线支付等功能的实现，客票系统已基本实现管理与发售的现代化，但节假日出行期间旅客购票难、验票、取票、检票效率低下的问题仍然存在。造成操作效率低的主要原因是现有的纸质磁票是接触式识读方式 [4]，旅客需要逐个进行手工操作，验票、检票速度受到很大限制，而且纸质磁票的信息容量很有限，无法较好地适应现代高速铁路客运的需求。

鉴于铁路客票系统验票检票等环节操作效率低的问题，可以考虑采用基于射频识别技术的票制，它是一种非接触式的自动识别技术，具有通信速率快，支持读写、信息容量大，安全性高等特点，可以使得旅客通行效率显著提高。基于射频识别技术的产业链已初步形成，成本也在逐年降低，在铁路客票系统中使用具有广阔的应用前景 [5]。

3 基于物联网的铁路客票系统

根据物联网的 3 层体系结构，结合铁路客票系统自身的特点，本文设计了基于物联网的铁路客票系统，其体系架构如图 2 所示。感知层，主要是各种含 RFID 读写器的客票系统终端设备，用于无线接收票据的数据信息，对基于 RFID 技术的票据进行读写操作，包括窗口售票、自动售票、自动检票、进站验票、到站补票、便携补票等设备；网络层，主要是客票终端设备将票据的数据信息通过客票专网传输给应用层，并将反馈数据信息传输给业务终端，包括客票局域网、客票终端无线网和客票广域网等；应用层，主要对收集的数据信息进行有效的处理，并对终端的业务请求做出回应，实现的客票系统的智能化运作。

本文提出采用客票系统云计算中心作为物联网应用层的核心方案。客票系统云计算中心主要由 4 部分组成，即基础设施层、虚拟化层、平台层和业务层。基础设施层，由服务器设备、存储设备、网络设备等组成；虚拟化层，由网络资源池、存储资源池、计算资源池等组成；平台层由软件硬件资源管理、虚拟计算管理、虚拟资源管理等组成；业务层，由客票系统的核心业务模块构成，内容包括计划调度、订票管理、退票管理、统计分析、票卡管理、数据维护、财务结账等功能模块。

物联网和云计算中心的结合将彻底改变铁路客票系统的应用模式 [6]。

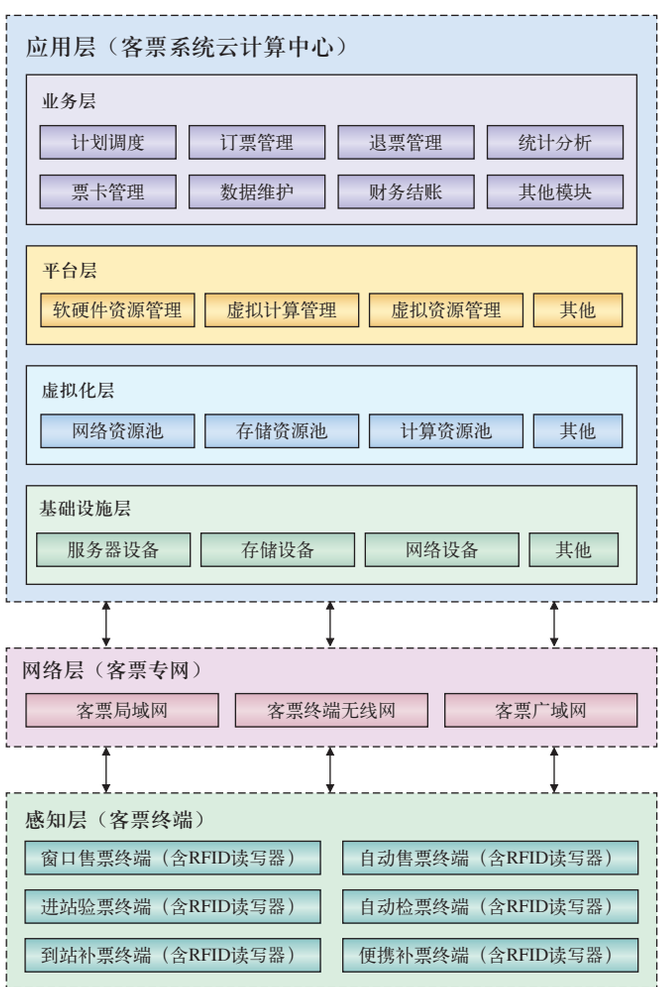

图2 基于物联网的铁路客票系统体系架构示意图

4　安全风险

感知层主要负责收集票据的数据信息，并对基于 RFID 技术的票据进行读写操作。面临的安全挑战主要包括伪票识别、伪造终端节点接入、网关节点被恶意控制、终端节点被恶意控制、感应数据信息被劫持、对终端节点的拒绝服务（DOS）攻击等。

网络层主要包括客票局域网、客票广域网、客票终端无线网。网络层面临的安全挑战与传统的网络安全类似，主要包括传输安全和数据安全。传输安全，关注传输数据信息的保密性和完整性；数据安全，关注敏感数据信息不要被劫持，例如列车调度信息，席次信息、余票信息以及旅客姓名及身份证号等。

应用层由一个云计算中心构成，用于收集客票业务数据信息，处理各种客票业务，并将响应结果回馈给客票业务终端。其面临的安全挑战主要包括伪造身份请求信息、病毒入侵防范、黑客恶意渗透、机密信息泄露、访问权限控制，移动设备接入控制，以及云计算中心遭受自然灾害等。

5　安全体系架构

根据上述安全策略的分析，针对基于物联网的铁路客票系统的体系架构，本文提出“一个中心，三重防护”的安全策略，即一个“客票安全管理中心”和“应用层防护、网络层防护和感知层防护”的三重防护。客票安全管理中心，内容包括统一的安全管理平台、安全监控平台、病毒防护系统、PKI 认证系统和安全审计系统；三重防护，包括应用层安全防护、网络层安全防护、感知层安全防护，具体内容如图 3 所示。

5.1　客票系统安全管理中心

安全管理中心是整个客票系统安全体系的核心，具有最高级别的管理权限。安全管理中心主要由如下系统组成。

（1）统一的安全管理平台

通过统一的安全管理平台，可以对客票系统的所有服务器、业务终端、安全设备、网络设备实现统一管理与调度，最大限度的保证资源的合理利用，主要包括用户管理、资源管理、虚拟机管理、映像管理、资源调度管理、虚拟数据中心管理和系统管理等。

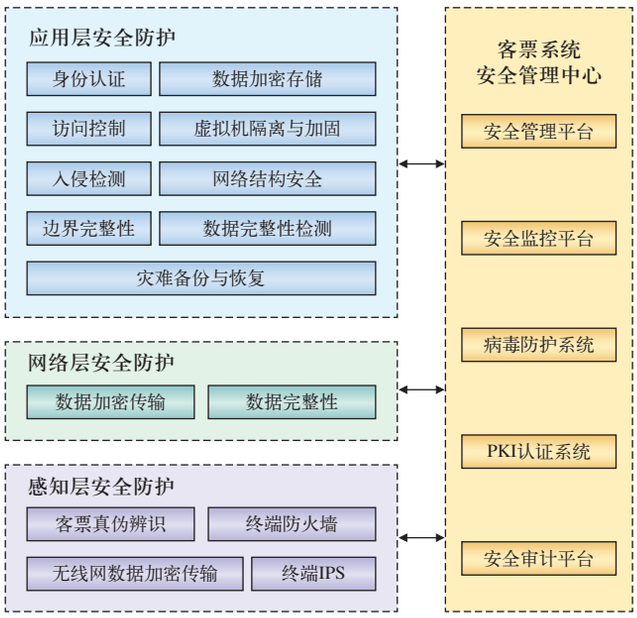

图3　基于物联网的铁路客票系统安全体系架构示意图

（2）统一的安全监控平台

通过统一的安全管理平台，可以对客票系统的所有服务器、业务终端、安全设备、网络设备实现统一安全监控，全面了解各类设备的运行状况，及时发现设备故障并及时报警，极大地提高了网络监控预警能力和事故响应处理速度。

（3）统一的病毒防护系统

对于铁路客票系统这样大型的信息系统，防病毒系统的统一性和完整性是避免病毒蔓延传播的重要一环。为了保证防病毒系统的一致性、完整性和自升级能力，统一的病毒防护系统负责病毒库的自动分发、自动升级、集中配置和管理、统一事件和告警处理，形成整个铁路客票系统范围内病毒防护体系。

（4）统一的 PKI 认证系统

基于物联网技术的铁路客票系统环境下的 PKI 认证系统，与传统的 PKI 认证系统类似，具有用户申请，申请审核，证书签发，证书吊销，证书管理，密钥管理，用户管理等功能，通过使用 CA 证书满足作为密钥管理平台的所有需求。

（5）统一的安全审计系统

相对于传统 IT 系统，基于物联网技术的铁路客票系统增加了很多的自动识别的数据信息和非人为

操作的访问，使得日志信息对于日常运行维护、安全事件追溯、案件调查取证等显得更为重要。建立统一安全审计中心，保障铁路客票系统日志信息的准确性和完整性。

5.2 应用层安全防护

针对应用层的各种安全挑战，采用统一身份授权认证机制，并建立多重的身份认证机制，能有效拒绝伪造身份的请求信息；应用层的访问控制主要在客票系统云计算中心实现，将传统的访问控制技术（自主访问控制、强制访问控制）和基于角色的访问控制相结合[7]，可以实现对访问权限的有效控制；各个设备安装防病毒软件，并与安全管理中心一致，可以有效控制病毒的入侵；增加网络边界完整性检查设备，可以对移动接入设备的有效控制；数据的加密存储、虚拟机的隔离与加固都能有效的防治机密信息的泄露；构建灾难备份与恢复系统，在突发自然灾害时，可以保证客票系统的业务连续性和数据完整性。

5.3 网络层安全防护

基于物联网的铁路客票系统，增加了很多自动识别业务终端，数据信息要通过客票专网进行频繁传输，因此保证传输的保密性和完整性显得尤为重要。为了保证传输安全，借鉴虚拟专用网(VPN)技术，使感知层的客票业务终端和应用层的客票云计算中心的数据传输过程中，获得足够的加密保护。

5.4 感知层安全防护

感知层主要是包含 RFID 自动读写功能的客票系统终端设备，应当安装安全软件，例如统一的防病毒软件、单机防火墙以及单机入侵检测（IPS）等。对于铁路客票系统的特性，终端设备应具有伪票识别功能，如自动检票机对持伪票的人员应果断闭闸并进行报警，窗口售票系统对伪票进行识别，并提示不能进行退票或改签操作；对 RFID 标签的票卡，通过无线网传输数据要进行加密处理，拒绝伪造终端节点接入，有效避免网关节点被恶意控制、终端节点被恶意控制，以及感应数据信息被劫持等；感知层的终端设备有很多非接触式的自动识别交互信息，一旦交互信息被黑客劫持利用，就可以对终端节点展开拒绝服务（DOS）攻击，针对这一特点，需要对终端节点的资源进行有效监控，如果资源使用超标，就应当给出提示信息并报警，能有效防止拒绝服务（DOS）攻击造成的感应层节点瘫痪。

6 结束语

本文设计了基于物联网技术的铁路客票系统，并就其安全体系架构提出了一套解决方案。铁路客票系统未来的发展，必将与物联网、云计算、大数据、秘密数据挖掘、安全多方计算等技术相结合，彻底改变现有的工作模式，也将面临着新的安全挑战，让未来的铁路客票系统变得更加高效、便捷、智能、安全和可靠。

参考文献：

[1] 郎为民 . 大话物联网 [M]. 北京：人民邮电出版社，2013.
[2] 徐小涛，杨志红 . 物联网信息安全 [M]. 北京：人民邮电出版社，2012.
[3] 朱建生，单杏花，周亮谨，刘春煌，等 . 中国铁路客票发售与预定系统 5.0 版的研究与实现 [J]. 中国铁道科学，2006(11).
[4] 史天运，王　成 . RFID 技术在铁路客票系统中的应用 [J]. 中国铁道科学，2009（11）.
[5] 王　成，史天运，蒋秋华，等 . 基于 RFID 技术的铁路长期票和储值卡应用 [J]. 铁路计算机应用，2008（5）.
[6] 周泽岩，马超群，付卫霖，张　彦 . 铁路客票系统云计算模式及其安全策略的研究 [C]. 第八届中国智能交通年会优秀论文集，2013.
[7] 冯登国，张　敏，张　妍，等 . 云计算安全研究 [J]. 软件学报，2011，22（1）.

责任编辑　陈　蓉