基于CDMA2000的智能卡操作系统的测试技术研究

郭 琨,李代平,郭鸿志,梅小虎
(广东工业大学 计算机学院,广东 广州 510006)

摘 要:智能卡操作系统是智能卡资源的管理者,它将智能卡芯片内各种硬件与用户所要求的应用系统密切结合起来,是整个卡片的灵魂。随着智能卡的应用越来越广泛,对其操作系统的质量要求也越来越高,因此必须对其进行全面的、高质量、高效率的测试。文中介绍了基于CDMA2000 1xEV-DO网络的手机智能卡操作系统结构,分析了其主要测试内容并给出了该系统的测试方案。为提高其测试效率,采用了自动化测试技术,对自动化测试工具的设计原理做了简单介绍,并最终完成了测试。

关键词:智能卡;芯片操作系统;软件测试;EVDO卡
中图分类号:TP311.56 **文献标识码**:A **文章编号**:1673-629X(2010)09-0250-04

Research on Chip Operating System Testing Technology Based on CDMA2000

GUO Kun, LI Dai-ping, GUO Hong-zhi, MEI Xiao-hu
(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Chip operating system is the manager of smart card resource, it attachs the hardware of the smart card and applications required by users, it is the soul of the entire card. With the use of smart card are increasingly more widely, the quality requirements have become more sophisticated, so it is necessary to perform a comprehensive test. This paper first introduces the chip operating system based on CDMA2000 1xEV-DO Network, then the test scheme and test content of COS in CDMA2000 is discussed, and its automatic testing technologies and methods is introduced. In the end, the test of COS is successfully completed.

Key words: smart card; chip operating system; software test; EVDO card

0 引 言

随着智能卡在各个领域的应用迅速增长,对其智能卡操作系统(Chip Operating System,COS)质量的要求也越来越高。软件测试是软件质量保证的关键阶段,是对软件设计和编码的最终检查。据统计,目前在软件开发总成本中,用在测试上的花销要占30%~40%[1],对于COS这种商业性质很高的软件,测试所占的比例将会更大。COS一般是紧紧围绕着它所服务的智能卡的特点而开发的,与那些常见的微机上的操作系统相比较而言,COS在本质上更加接近于监控程序,而不是一个通常所谓的真正意义上的操作系统[2]。鉴于COS的特殊性,目前还没有专门的测试方法应用于COS的测试,并缺乏系统的能适用于实际开发过程的测试理论。文中针对CDMA2000 1xEV-DO网络环境下的智能卡(以下简称EVDO卡)COS的特点,首先介绍了EVDO COS的系统结构模型,给出了测试用例的设计方法,自动化测试工具的设计,并最终完成对其的整体测试。

1 EVDO COS系统结构

EVDO COS是智能卡资源的管理者和安全保密的基础,其主要功能是控制智能卡与外界的信息交换[3],管理智能卡内的存储器并在卡内部完成各种命令的处理,要求具有良好的可维护性、可扩展性、高安全性、较小的模块相关性。图1为本设计的系统模型结构,它的体系结构模型划分为微内核层、逻辑功能层以及应用层,下层依次向上层提供相应接口。

收稿日期:2010-01-18;**修回日期**:2010-04-23
基金项目:广州市自然科学基金(2008-GX-015)
作者简介:郭 琨(1985-),男,江西萍乡人,硕士研究生,研究方向为智能卡芯片操作系统;李代平,教授,研究方向为智能卡芯片操作系统、网络并行计算。

由于底层芯片的差异性,本设计采用微内核结构,对不同芯片的驱动进行搜集和编写,对其相同的部分进行提取,实际生产时只需要替换相应的底层驱动程序便可完成移植,所以具有较好的可移植性和扩展性[4]。逻辑功能层主要有四大模块,其中通信管理模块实现与外部的数据通信,接受读写设备发出的命令,并将命令的响应按格式发送出去;命令解释模块负责解析卡片与终端之间交互的信息指令,并作出相应的处理,最终通过 I/O 接口返回响应状态和响应数据;文件管理模块是 COS 的重要模块之一,EVDO 卡上的数据或应用是以文件的形式存放在 FLASH 中的,该模块负责组织、管理和维护卡片内存储的所有的数据,并实现文件系统初始化,文件内容的查找、更新以及删除等操作;安全管理模块是智能卡 COS 中最为核心的模块,它对智能卡内数据提供安全保障,同时也对外提供安全定义,主要内容包括了网络与用户的鉴权算法、文件的访问策略、加密解密算法以及安全报文处理等。应用层在卡上主要实现了增值业务应用,本系统实现的超级号簿可以提供多个扩充电话簿来存储大容量电话号码,并提供了对 EVDO 卡中所有号码的各种检索方式,以及号码编辑、短信群发等功能。

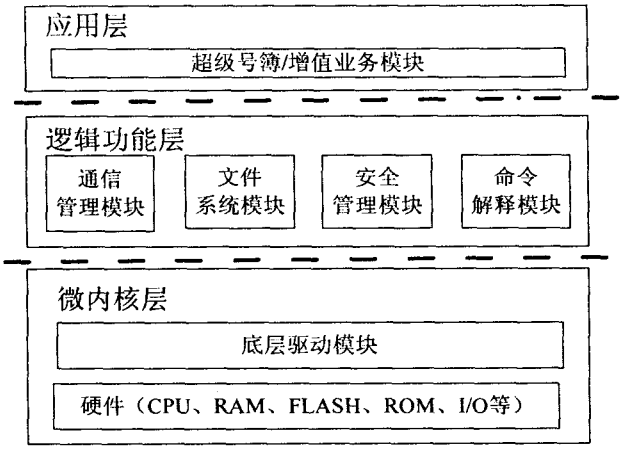

图 1　EVDO 卡 COS 系统结构模型

2　智能卡通信机制

依照 ISO/IEC 7816－3 标准[5],EVDO 卡采用了 T=0(字符传输)协议,卡与终端是通过命令－响应对来进行信息交换的。COS 接受命令报文并对其进行处理,然后将处理结果作为响应报文返回给终端。应用协议数据单元(APDU)即为终端与卡之间一次通讯传输的最小信息单位,它要么包含有命令信息(C－APDU),要么含有响应信息(R－APDU)。

C－APDU 由两部分组成:一个必备的连续 4 字节的命令头和一个可变长度的条件体,数据域的长度由 Lc 表示,期待卡所返回的响应报文的最大长度由 Le 指定。R－APDU 由一个可选的条件体以及必备的 2 字节状态码 SW1|SW2 组成,两者结构如图 2 所示。

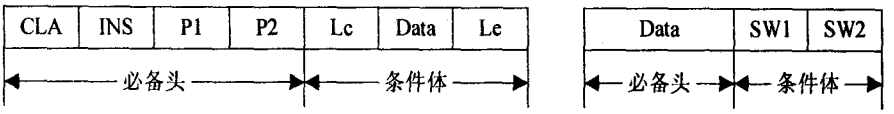

图 2　C－APDU 和 R－APDU 命令结构

3　EVDO COS 的测试内容

3.1　COS 测试的主要内容及方案

EVDO COS 的开发采用传统的瀑布式开发方法[6],依照其系统结构模型,COS 的测试主要包括以下几项内容: COS 应用逻辑测试、协议一直性测试、坚固性测试以及兼容性测试。其中后三项为 COS 测试不同于一般软件测试的地方。

应用逻辑测试,也就是 COS 的基本功能测试,它是 COS 测试最主要的任务,主要包括命令测试、文件测试、命令描述测试、命令响应测试及超级号簿测试。各测试项主要内容见表 1。

表 1　COS 测试主要内容

测试项	主要内容
文件测试	文件标识测试、专用文件测试、基本文件测试、选择文件方法测试
命令测试	包含 SELECT、VERIFY PIN、RUN CAVE 等 29 条命令的测试
命令描述测试	映射规则测试、定义和编码测试
命令响应测试	对错误命令的响应测试、卡返回的状态字节测试
超级号簿测试	终端能否正确显示超级号簿业务菜单,相应功能能否实现

坚固性测试[7]检测 EVDO 卡在恶劣环境和大量使用时运行的能力。其中数据防插拔保护测试主要针对正常环境下采用正确的命令序列执行正常操作,COS 写 FLASH 时,突然断电,EVDO 卡是否能够保证卡内数据的完整性不被破坏。若命令未能成功执行,则需要对卡中的数据进行检查,看是否与执行前完全一致,如果不一致说明卡的防插拔功能未能实现,反之,防插拔功能是有效的。另外,智能卡使用 FLASH 作为存储介质,在进行数据操作时候需对卡反复进行大量的擦写,容易导致其过度损耗,为了保证卡能够长期使用,因此有必要对智能卡进行寿命测试。

智能卡与终端遵循相同的协议是保证它们之间进行正常通信的前提,因此必须测试 COS 对于协议的实

现情况。

开发EVDO COS的最终目的就是使各式各样插入EVDO卡的手机终端能在电信运营商提供的网络中进行正常通信,实现卡与手机的正常交互,因此还必须测试EVDO卡与不同终端的兼容性。该项测试主要通过在实网环境中选择不同品牌的CDMA手机对EVDO卡进行使用,验证其是否能实现电信基本功能,如通话、发送短信等。

依照软件测试[8]的相关理论,各项测试内容与测试阶段及所使用的测试技术对应见表2。

表2 COS的测试阶段

测试内容	测试阶段	测试技术
应用逻辑测试	单元测试 集成测试 系统测试	灰盒测试
协议一致性测试	系统测试	黑盒测试
坚固性测试	系统测试	黑盒测试
兼容性	验收测试	黑盒测试

EVDO卡的测试方案设计如下:首先,进行需求分析,对各项测试内容编写测试用例;编码完成后,在代码走查的基础上,利用Keil软仿真环境并采用递增式组装的方式进行单元测试;COS软掩膜后,利用自主开发的自动化测试工具,通过读写器进行脚本测试;最后,在实网环境下,使用软掩膜卡,选用不同型号的CDMA手机,对其进行兼容性测试以及超级号簿业务测试,并测试其电信基本功能。

3.2 COS测试用例设计

不同于一般的软件,COS具有嵌入性[9],其开发必须严格遵守相关的国际和行业标准,使得COS测试不能照搬常规的软件测试方法[10]。依据COS自身特点,可将其测试结构[11]分为四部分:第一部分详述测试的目的;第二部分包含该项测试的定义和应用性;第三部分列举了COS应满足的需求,与相关协议、标准的一致性;最后一部分规定了实际的测试步骤。

依据图3所描述的测试结构,以命令测试中的

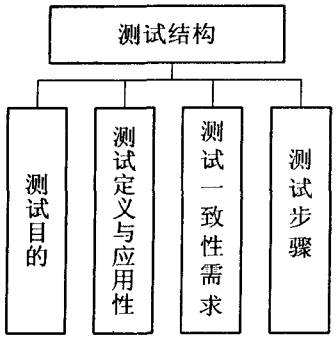

图3 COS测试结构

GET RESPONSE命令为例,可设计其测试用例如表3所示。

表3 GET RESPONSE命令测试用例

测试项	GET RESPONSE命令测试
测试目的	验证GET RESPONSE命令是否正确执行
测试定义和应用性	验证GET RESPONSE命令操作是否符合以下要求
测试一致性需求	1)GET RESPONSE命令必须在相关命令执行后立即执行(在命令/响应对和命令GETRESPONSE之间不应该发出其他命令)。如果没有按照这一次序,卡应该发送状态信息"未诊断出来的技术问题"作为GETRESPONSE的响应 2)由于EVDO卡激活后MF已被选中,GET RESPONSE允许作为EVDO卡激活后的第一条命令
预置条件	EVDO卡连接到ME模拟器上
测试步骤	1) 终端复位EVDO卡 2) 发送GET RESPONSE命令,第5,6字节标识当前选中的为MF文件 3) 发送STATUS命令 4) 发送GET RESPONSE命令,返回一个错误的状态字"6F00"-标识为未诊断的错误
预期结果	期望结果与相应步骤相同

4 EVDO COS的自动化测试

4.1 自动化测试技术的引入

由于COS的软件版本不断更新,每次更新完成后又要重复之前的测试过程,在保证测试的质量的同时提高测试效率,EVDO COS测试引入了自动化测试[12]方法。

自动化测试可以带来以下好处:

1)不需要人工干预,可以运行更多更频繁的测试,大大缩短了测试时间;

2)可对程序的新版本运行已有的测试。自动化测试可在很短的时间内将以前的测试重复一遍,而且自动化测试能重复多次相同的测试,可以获得测试的一致性;

3)可以迅速地对测试结果进行分析,以便开发人员更快地修改测试中所发现的问题。

因此,在COS测试中引入自动化测试技术是非常必要的。

脚本技术是实现软件测试自动化的有效手段[13]。测试脚本对测试用例给以形式化的描述,通过脚本代码的可重用性可以提高测试的可重复性,大大减少测试人员的工作量,提高软件测试的质量和可维护性。由于智能卡与终端通信的基本单元为APDU,因此大部分测试项均可通过终端向COS发送C-APDU,并

依据卡所返回的 R－APDU 与预期结果相比对来进行测试。在实际的测试实施中，只需将测试步骤使用 C－APDU 的格式来描述，便可形成简单的 APDU 测试脚本。

以下简单描述了 GET RESPONSE 命令的测试脚本，括号内为该条指令的期望返回状态字。

```
// GET RESPONSE 命令测试脚本
//具体过程
//1.复位
_R.R
//2.发送 GET RESPONSE 命令，第 5,6 字节标识当前选中的为 MF 文件
A0 C0 00 00 17 (9000)
//3.发送 Status 命令
A0 F2 00 00 17 (9000)
//4.发送 GET RESPONSE 命令，返回一个错误状态字 6F00
A0 C0 00 00 17(6F00)
```

通过单个的测试脚本可以实现一项或多项测试用例的测试，把多个测试脚本按照一定的规则组合在一起就可以实现整个 COS 各项功能的测试并实现自动化。

4.2 自动化测试工具 APDUTOOLS

为解决计算机与各种读卡器之间的互操作性问题，人们提出了 PC/SC(Personal Computer/Smart Card)规范作为读卡器和卡与计算机之间的标准接口，实现不同生产商的卡和读卡器之间的互操作性。Microsoft 在其 Platform SDK 中实现了 PC/SC，作为连接智能卡读卡器与计算机的一个标准模型，提供了独立于设备的 API，并与 Windows 平台集成，它提供了 30 多个函数，以下为常用的几个：

SCardEstablishContext：用于建立将在其中进行设备数据库操作的资源管理器上下文；

SCardListCards：获取以前被用户引入系统的所有智能卡列表；

SCardConnect：连接到一张卡；

ScardTransmit：向智能卡发送命令；

SCardDisconnect：结束一个连接；

SCardReleaseContext：释放资源管理上下文。

APDUTOOLS 便是基于 PC/SC 所实现的一个黑盒自动化测试工具，它支持各种不同的读卡器，将卡与终端进行连接，实现它们之间的交互。测试人员既可在命令编辑区输入单个的 APDU 指令，也可通过文件导入已编写好的测试脚本。该工具可对 COS 执行每条 C－APDU 指令后所返回的状态字以及数据与预先给定的期望结果进行比较，并生成测试报告，便于开发人员对错误进行改正。

APDUTOOLS 还支持单步调试功能，可以帮助测试人员对错误进行精确的定位。在针对需求编写测试用例之后可使用 APDUTOOLS 对 COS 进行单元测试和集成测试。

5 结束语

依据文中所述方法对各项测试内容设计测试用例后，将其转换为脚本格式，依照测试方案，利用自动化测试工具 APDUTOOLS 在单元测试和集成测试中进行了 EVDO COS 的应用逻辑测试，在系统测试中测试了协议一致性、坚固性，最后在验收测试中测试了 COS 与不同手机终端的兼容性。经过反复测试，开发的 EVDO COS 通过了第三方测试。

参考文献：

[1] 李　翔.智能卡研发技术与工程实践[M]. 北京：人民邮电出版社，2003.

[2] 王爱英.智能卡技术[M].第 2 版.北京：清华大学出版社，1996.

[3] der Chipkarten H, Rankl W, Effing W. 智能卡大全[M].王卓人，王　锋，编译. 北京：电子工业出版社，2002.

[4] 梅小虎，李代平，郭广义，等.CDMA2000 芯片操作系统安全部分的研究与设计[J].计算机应用，2009(11)：2917－2919.

[5] ISO 7816－3. Identification Cards Integrated Circuit(s)cards with contacts－Part 3：Electronic signals and transmission protocols[S].[s.l.]：International Electrotechnical Commission，1997.

[6] 李代平.软件工程[M].第 2 版. 北京：清华大学出版社，2008.

[7] Watkins J，贺红卫，杨　芳.实用软件测试过程[M].北京：机械工业出版社，2004.

[8] Jorgensen P C.软件测试[M].第 2 版.韩　柯，杜旭涛，译.北京：机械工业出版社，2003.

[9] Broekman B, Notenboom E. 嵌入式软件测试[M].张君施，张思宇，周承平，译.北京：电子工业出版社，2000.

[10] 张利华.智能卡操作系统开发中的测试技术[J].计算机工程与设计，2004，25(6)：901－902.

[11] GSM11. 17. Digital cellular telecommunications system (Phase 2＋)Subscriber Identity Module (SIM) conformance test specification[M].[s.l.]：[s.n.]，1998.

[12] Dustin E, Rashka J, Paul J. Automated Software Testing：Introduction，Management，and Performance[M].[s.l.]：Addison Wesley Professional，1999.

[13] 周章慧，王同洋，吴俊军，等.智能卡操作系统自动测试中的脚本技术[J].计算机工程与设计，2008，29(8)：2068－2071.