

SCA 系统中以太网设备组件的设计与实现

李兰花¹, 王 玲¹, 施峻武^{2,3}, 雷鹏斌¹, 黄子鸿¹

(1 湖南师范大学 物理与信息科学学院, 湖南 长沙 410012;

2 国防科技大学 电子科学与工程学院, 湖南 长沙 410073;

3 中国电子科技集团公司第五十四研究所 通信网信息传输与分发技术重点实验室, 河北 石家庄 050081)

摘 要: 软件通信体系结构(SCA)作为美军 JTRS 投巨资制定的技术规范,是未来各军兵种无线通信系统都将遵循的一体化结构. SCA 系统中定义的设备组件是底层物理硬件设备的软件抽象,为上层波形应用和服务提供统一的设备接口. 这使上层波形应用的开发无需关心底层硬件设备的实现细节,从而摆脱底层硬件特性的制约,实现波形的可移植和可重用. 由此阐述了以太网设备组件的具体应用背景,并提出了基于 SCA 规范的以太网设备组件的设计和实现方法,为 SCA 系统中其他设备组件的开发也提供了参考.

关键词: 软件通信体系结构;以太网;设备组件;软件无线电

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2016)03-0041-05

Design and Implement of Ethernet Device Component in SCA system

LI Lan-hua¹, WANG Ling¹, SHI Jun-wu^{2,3}, LEI Peng-bin¹, HUANG Zi-hong¹

(1 School of Physics and Information Science, Hunan Normal University, Changsha 410012, China;

2 National University of Defence Technology, Changsha 410073, China; 3 Science and Technology

on Information Transmission and Dissemination in Communication Networks Laboratory,

The 54th Research Institute of China Electronic Technology Group Corporation, Shijiazhuang 050081, China)

Abstract: Software Communications Architecture (SCA) as the heavily invested technical specifications set by the JTRS, it is the integration of structure to be followed by all the services and arms in the future wireless communication systems. The device components defined in the SCA system is software abstraction to underlying physical equipment, and provide a unified device interface for the upper waveform applications and services. This makes the upper waveform application development no need to care the implementation details of the underlying hardware equipment, so it can get rid of the restriction of the underlying hardware characteristics, and realize the portable and reusable waveform. This paper expounds the concrete application background of the Ethernet device components, and put forward the design and implement method for Ethernet device component based on SCA specification, it also provides a reference for the development of other device components in SCA system.

Key words: SCA; Ethernet; device components; software radio

1 引言

SCA 是一个与具体实现无关的开放式架构,为软件无线电的实现提出了具体的设计结构和实现规范,其目标是减少系统的开发时间,提高波形组件的

可移植性,节约系统部署成本,2015 年 1 月 SCA4.1 规范的最新草案已发布^[1].

标准化的 API 对于实现 JPEO JTRS 软件的可移植性和可重用性至关重要. JTRS APIs 通过指定语言和语义保证波形应用程序和服务的设置可以不管

JTRS 组件内部的实现细节,从而使一个波形应用程序可以重复用到不同大小、任务或部署的软件无线电平台,方便在软件无线电系统中部署新的功能,降低系统的维护成本.图 1 所示为将 JTRS APIs 聚合后部署到 JTRS 平台,这时 JTRS APIs 可以划归到三类范畴:原始 API、设备组件、服务组件.

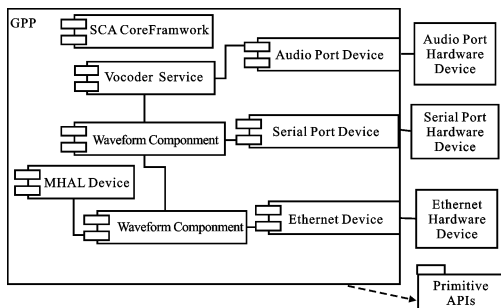


图 1 JTRS 系统的 GPP 平台

原始 API 是一些常见的 API,包括基本的数据类型和数据传输接口,其他设备和服务接口可以继续使用这类接口功能,避免了 API 功能的重复定义.设备组件是底层物理硬件设备的软件抽象,向上层波形组件提供符合 JTRS 接口规范的统一设备接口,这使得波形应用程序无需关心底层硬件的实现细节.同时,设备组件需要根据平台的不同架构和需求设计具体实现.服务组件不像设备组件需要绑定平台上特定的硬件资源,它与其他组件提供一些通用的功能.本文通过设计符合 JTRS 接口规范的以太网设备组件为上层应用程序和服务提供统一的底层通信支持和通用的设备 API.

2 SCA 软件平台及设备组件的设计

2.1 基于 SCA 的 SDR 软件平台架构

基于 SCA 的 SDR 的软件平台架构^[2]满足模块化波形组件的可重构和灵活配置.该软件平台包括了底层硬件环境的支撑,基于 SCA 规范搭建的软件操作环境以及 SCA 应用层的波形组件.由操作系统、分布式处理中间件和 SCA 核心框架构成的软件平台能够实现如下功能:一方面,为波形开发和系统管理等上层开发软件提供统一的接口和服务;另一方面,对底层数据的传输和 GPP、FPGA、DSP 等处理器将进行统一管理.SDR 软件平台架构如图 2 所示.

SCA 系统的开发主要包括了核心框架的设计、组件的开发、系统的集成.核心框架已有较为成熟的产品,往往不需要重新设计.组件的开发则包括了设备组件的开发和波形应用组件的开发,这是平台设

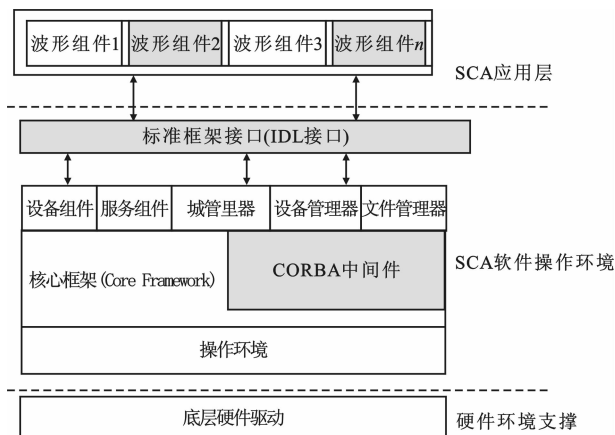


图 2 SDR 的软件平台架构

计开发的重点内容.系统的集成是将核心框架和各组件集成在一起进行运作,包括了数据的分布式处理,组件的管理,系统服务的提供等.

2.2 SCA 系统设备组件的设计

SCA4.0 提出了轻量级组件^[3]的设计,使系统框架功能可以适应不同产品和任务的需求.在之前的 SCA 版本中接口功能十分完备,常常超出了实际的需要,浪费了大量的资源,增加了开发成本,如需求分析、设计决策、开发时间、软件集成和测试和遵从性测试.SCA4.0 规范中提出新的继承方式——选择性继承,在针对不同应用平台时,可自适应地选择需要继承的接口,这使得组件功能相对于之前的 SCA 规范更为灵活,也是实现轻量级组件的途径.开发人员可以通过预编译和 IDL 指令定义特定的组件选择性继承接口.

对于轻量级组件的实现,可参考 SCA 规范中各组件的继承关系,以 Device 接口为例,通过 IDL 指令和预编译配置接口继承,只有在定义了标识符时,接口才被继承,例如只有在定义了 TESTABLE 时 TestableObject 接口才需要被实现,因此通过控制 Device 接口的继承方式就能控制设备组件的大小.定义 V222_COMPAT 时就能和 SCA2.2.2 版本兼容.

```
interface Device : LifeCycle
# if defined ( INTERROGABLE ) || defined ( V222_COMPAT ), DeviceAttributes # endif
# if defined ( CONNECTABLE ) || defined ( V222_COMPAT ), PortAccessor # endif
# if defined ( CONFIGURABLE ) || defined ( V222_COMPAT ), PropertySet # endif
# if defined ( TESTABLE ) || defined ( V222_COMPAT ), TestableObject # endif
```

设备组件的具体设计包括了两个方面:一是设

计设备组件端口,用以实现逻辑设备与其他组件之间的连接通信;二是根据 SCA 规范中 API 的定义来开发设备组件的具体实现,然后编译文件.在 SCA 体系结构中,采用统一建模语言(Unified Modeling Language,UML)搭建图形化接口,并用接口定义语言(Interface Definition Language,IDL)定义接口.IDL 定义接口可以被编译成不同编程语言用于具体实现的开发,所以 SCA 规范中都是采用接口方式对组件进行描述.

3 以太网设备组件的设计

3.1 以太网设备的端口对象设计

以太网设备组件端口^[4]是以太网设备组件与外界的数据通信口.在 SCA 体系中组件通过 User 端口和 Provider 端口两类端口实现数据交换.端口具有方向性,组件的 User 端口用于将数据向外传输给相连组件,并管理组件间的端口互联.组件的 Provider 端口则被其他组件调用,用于接收其他组件的传入数据,随后由端口内的数据处理函数对传入数据实现进一步处理.图 3 中给出了以太网设备端口定义,其他组件就是通过端口来与以太网设备组件进行数据交互的.

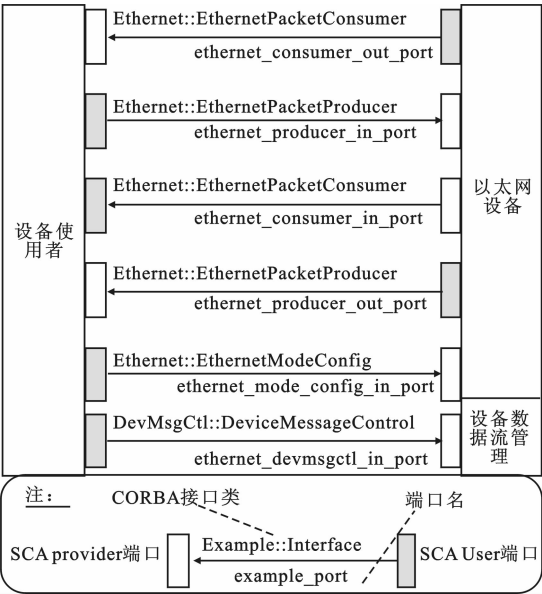


图 3 以太网设备端口定义

端口的具体功能是由它实现的特定接口提供,接口是组件对外公布的一系列的操作和属性,其他组件可以通过接口对组件的功能进行调用.以太网设备组件作为底层以太网硬件设备的封装,它的基本功能就是从硬件设备获取和发送数据包,这是通过继承通用数据包接口来实现的,如 Packet、DeviceIO.

根据 JTRS APIs 规范,以太网设备组件端口对象包括了两个基本接口和五个扩展接口,如图 4 所示.EthernetPacketConsumer 接口用于设备用户在流控操作下向以太网硬件端口传输数据;EthernetPacketProducer 接口用于设备用户从以太网硬件端口获取数据;EthernetModeConfig 接口用于获取和配置以太网模式,包括无模式、标准模式、组播、混杂模式;EthernetMulticastConfigExt 接口用于以太网设备组播模式的实现;EthernetPromiscuousConfigExt 接口用于以太网混杂模式的实现;EthernetHeaderConfig 接口是设备用户用来获取和设置以太网帧头;EthernetMacAddress 接口是设备用户用来查询以太网设备的 MAC 地址.

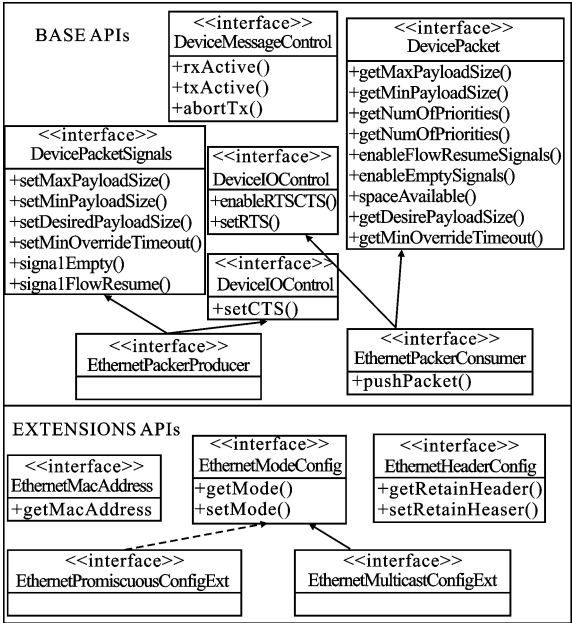


图 4 以太网设备组件的 JTRS API

3.2 以太网设备组件的 API 实现

SCA 规范中设备继承关系按功能划分为 Device (如 I/O 设备、串口设备等基本逻辑设备)、LoadableDevice(可加载设备)、ExecutableDevice(可执行设备).以太网设备作为基本的 I/O 逻辑设备组件,直接继承 Device 接口.在 Device 接口中可选择性定义以太网设备组件需要实现的接口功能.以太网设备组件中还聚合了如下功能:以太网模式配置功能、组播模式实现、多播模式实现、以太网帧头的获取和配置功能以及以太网设备的 MAC 地址查询.图 5 为以太网设备组件的 UML 图.

4 以太网设备组件的功能实现

4.1 功能需求

基于 TCP/IP 的以太网是一种标准开放式的网

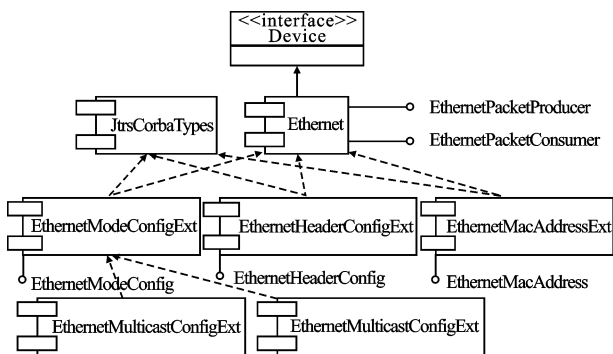


图5 以太网设备组件的UML图

络^[5],由其组成的系统兼容性和互操作性好,资源共享能力强,数据的传输距离长、传输速率高.同时,它还具有低成本、易组网的特点,与计算机、服务器的接口十分方便,因此受到了广泛的技术支持.不同的协议层对数据包有不同的称谓,在传输层叫做段(segment),在网络层叫做数据报(datagram),在链路层叫做帧(frame).TCP/IP的以太网帧的封装过程:首先,用户数据经过TCP程序,添加TCP头生成TCP段;然后,TCP段经IP程序生成IP数据包;最后,IP数据包经以太网驱动程序添加以太网首部和尾部,生成以太网帧.数据封装成帧后发到传输介质上,到达目的主机后每层协议再剥掉相应的首部,最后将应用层数据交给应用程序处理.

利用TCP/IP标准的以太网进行软件无线电电台通信组网时,可能存在特定的数据处理问题.由于每部电台可加载多个波形,同时连接上波形控制终端和网络管理终端.因此,当电台连接的终端发起数据传输,这些数据包可能拥有不同目的IP地址,这时电台以太网设备需要接收所有流经它的数据包,再将数据包交由路由服务组件确定发送路径.

本文设计的以太网设备通过采用TCP/IP协议^[6]中原始套接字方式实现抓取不同协议、不同目的地址的数据包功能.原始套接字的应用具有两大特点,一是可以直接操作从链路层至应用层的数据IP包,当原始套接字在数据链路层直接抓取以太网帧时,能够抓取到不经过系统处理的数据,完整地保留有以太网帧头,这将方便对传输数据的进一步分析,根据数据包类型和数据源地址,进行下一步的数据传输的判断.二是原始套接字是直接使用IP协议的非面向连接的套接字,它既可以使用bind()和connect()函数进行地址绑定,bind()函数指定源IP地址,connect()函数指定目的IP地址,并使用write和send函数发送数据包;也可以不使用地址绑定,

此时在接收数据时将所有协议匹配的IP数据包传递给这个原始套接字,发送数据的源IP由发送接口的主IP地址填充,目的IP地址由数据发送函数sendto或sendmsg在函数参数中指定.

4.2 数据处理流程

以太网设备组件主要采用数据流速控制和发送请求/允许请求控制来保证数据的有效传输.这两类机制主要是用于硬件设备和上层应用程序处理数据速率的匹配.下面给出了以太网设备组件处理数据的两个过程.

(1)从底层硬件设备接收数据,传递给数据接收组件.

首先,当以太网设备监听到有数据流进来,以太网设备组件向数据接收组件(如路由组件等)发送使能控制指令enableRTSCTS和enableFlowResumeSignal,然后接收底层硬件设备传来的数据,随后通过一次握手(即发送请求/允许请求)操作,以太网设备组件向接收组件发送数据.如果中途出现接收组件内存不足而无法接收更多数据时,数据传输就会中断,直至接收组件拥有至少一个最大有效载荷大小(MaxPayloadSize)的空间时,接收组件向以太网设备组件发出恢复数据流信号,以太网设备组件继续接收底层数据发送给接收组件.图6给出了该过程的序列图.

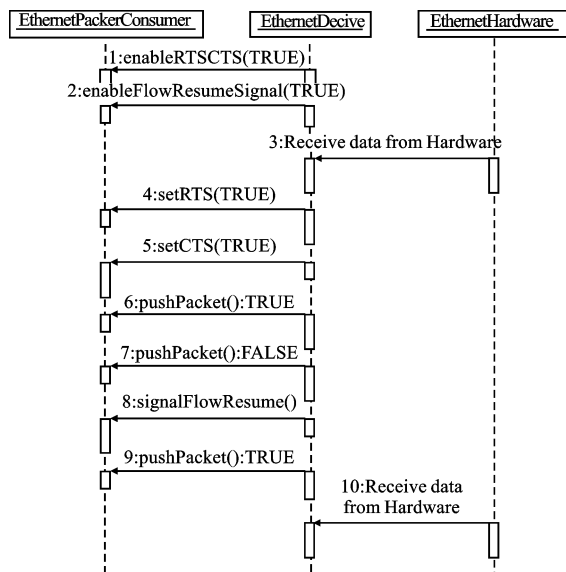


图6 以太网设备组件数据传输序列图

(2)从相连组件获得数据,交由底层硬件设备传输.

当相连组件需要通过以太网传输数据时,第一步是向以太网设备组件发送使能控制信号enableFlowResumeSignal和enableRTSCTS.第二步经过一

次握手操作后,相连组件开始向以太网设备组件推送数据。第三步当以太网设备组件接收一定的数据后,中断相连组件的传输,将数据传递给底层硬件设备。随后,当以太网设备组件拥有至少一个 MaxPayloadSize 的空间时,它会向相连组件发出恢复数据流信号,数据继续传输。

5 结束语

本文设计的以太网设备组件满足 SCA 规范定义,能够广泛应用于软件无线电台通信组网。在基于 TCP/IP 协议的以太网硬件上实现了有效的封装,为上层波形应用程序和服务提供了统一的以太网接口。在组件内部的数据处理上采用了数据流速控制和发送请求/允许请求控制两类机制,实现了数据的有效传递。本文中以太网设备开发,为 SCA 系统中其他设备组件的开发也提供了参考。

参考文献:

- [1] Magsombol C, Jimenez C, Stephens D R. Joint tactical radio system-application programming interfaces [C] // Military Communications Conference, MILCOM 2007. Orlando, IEEE, 2007: 1-7.

- [2] 范建华,王晓波,李云洲. 基于软件通信体系结构的软件定义无线电系统[J]. 清华大学学报:自然科学版, 2011,51(8):1031-1037.
- [3] JTRS JPEO. Software communications architecture specification, Version 4.0 [EB/OL]. (2001-12-19). [2015-06-11]. <http://jpeojtrs.mil/sca/Pages/portabilityguidelines.aspx>, 2012.
- [4] 邓伟,王玲,施峻武. DSP 上 SCA 波形组件接口的实现[J]. 世界科技研究与发展, 2012, 34(3): 423-426.
- [5] 顾霞萍,赵伟,王宜怀,等. 无线传感网络与以太网无缝结合的应用研究[J]. 微电子学与计算机, 2011, 28(6): 79-83.
- [6] 汤宏萍,王竹平. 嵌入式 TCP/IP 协议栈的设计与实现[J]. 微电子学与计算机, 2008, 25(6): 168-170.

作者简介:

李兰花 女,(1989-),硕士研究生. 研究方向为软件无线电. E-mail:lilanhua@163.com.

王玲 女,(1962-),教授,博士生导师. 研究方向为现代网络与通信技术、信息安全、非线性电路与系统.

施峻武 男,(1977-),博士研究生,讲师. 研究方向为软件无线电.

雷鹏斌 男,(1990-),硕士研究生. 研究方向为软件无线电.

黄子鸿 男,(1990-),硕士研究生. 研究方向为软件无线电.

(上接第 40 页)

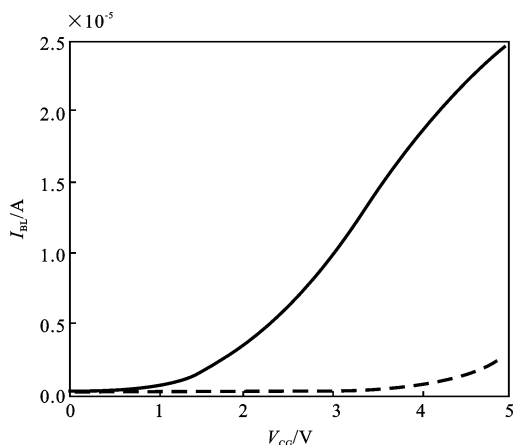


图 13 探针测试结果

大,需要经验积累,但是攻击方式直接,对安全有很大威胁,并且可以和失效分析等仪器和方法相结合,有很多值得研究的切入点。

实验一的探测方法可以明显观测 EEPROM 中单个浮栅晶体管的位置与结构,从而省去某些情况下需要对芯片进行完整逆向分析的繁琐步骤;第二个探针探测攻击方法虽然对 PAD 制作要求高,但是探测少量信息时效果明显。

参考文献:

- [1] Skorobogatov S. Flash memory bumping attacks [C] // International Conference on Cryptographic Hardware & Embedded Systems. Berlin, Springer-Verlag, 2010:158-172.
- [2] Skorobogatov S P. Semi-invasive attacks: a new approach to hardware security analysis [D]. Cambridge, UK: University of Cambridge, 2005.
- [3] Samyde D, Skorobogatov S, Anderson R, et al. On a new way to read data from memory [C] // IEEE Security in Storage Workshop. USA, Maryland, IEEE, 2002:65-69.
- [4] Brown D W, Brewer J E. Nonvolatile semiconductor memory technology: A comprehensive guide to understanding and using NVSM devices [M]. USA, Hoboken: Wiley IEEE Press, 1997.

作者简介:

程鹏 男,(1990-),硕士研究生. 研究方向为针对非易失性存储器的物理攻击技术.

E-mail:chengp12@mails.tsinghua.edu.cn.

白国强 男,(1963-),博士,副教授. 研究方向为应用数学、编码密码学和密码算法的芯片集成技术.