基于 QEMU 的 CAN 总线节点仿真器①

裴建国 李 曦 (中国科学技术大学 计算机科学与技术学院 安徽 合肥 230027;
中国科学技术大学 苏州研究院 江苏 苏州 215123)

摘 要: 汽车控制网网络的开发需要引入一套满足软/硬件协同设计需求的低成本开发工具链,其中硬件仿真器是最重要的工具之一。硬件仿真器为软件开发提供功能验证,缩短整个嵌入式系统的开发周期。在开源仿真器平台 QEMU 和虚拟局域网技术的基础上,实现一款仿真粒度更细的 CAN 总线节点仿真器 CES,并搭建一个满足汽车控制网络软/硬件协同设计需求的 CAN 总线仿真网络。

关键词: CAN 总线; CES; 虚拟局域网技术; 功能仿真

CAN Bus Node Emulator Based on Qemu

PEI Jian-Guo, LI Xi (Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China; Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou 215123, China)

Abstract: The development of vehicle control network is a difficult problem at present. Because it needs a lot of cheap toolchains,which must meet the requirement of hardware/software co-design. In the toolchains, hardware emulator plays an important role. The emulator provides funcation verification for the development of software and shortens the development period of embedded system. For the development of vehicle control network, this paper proposes an emulator based on QEMU and virtual local area network at the same time introduces a way of building CAN bus network by the emulator. It's called CES and achieves the function simulation of the hardware environment of the CAN bus network node.

Keywords: CAN bus; CES(can-emulation-system); virtual local area network; function simulation

1 引言

Wolfhard E. Lawrenz[1]指出未来汽车设计的难点是汽车控制网网络的设计,简称车控网,其开发周期较长,开发难度大。为缩短开发周期,减小开发难度,车控网需要一套符合软/硬件协同设计需求的工具链,其中硬件仿真器是这个工具链中最重要的工具之一。一般而言,硬件仿真器首先要仿真车控网中的硬件寄存器环境,其次要具有验证车控网中应用软件功能的能力。目前,CAN 总线[2]在车控网中使用较为普遍,所以本文研究基于 CAN 总线的硬件仿真器。

CAN 协议分为数据链路层和物理层,其中数据链路层又分为逻辑链路控制子层和媒体访问控制(MAC—Medium Access Control)子层。CAN 总线仿真器需要仿真:

1) CAN 总线节点的硬件环境

2) CAN 总线仲裁机制

基于 PowerPC 处理器的 MPC555 微控制器[3]是车控网节点的常用芯片之一,它的 CAN 总线接口是其附带的外部设备 TouCAN。QEMU [4]是一款开源仿真平台,支持 PowerPC 处理器的功能仿真,但目前不支持 TouCAN 设备的仿真,本文将基于 QEMU 仿真平台开发 CAN 总线节点仿真器 CES,它是通过在 QEMU

① 基金项目:苏州市 2008 年度第十二批科技发展计划(软件专项资金)(SGR0806)
收稿时间:2010-03-25;收到修改稿时间:2010-05-25

上添加 TouCAN 仿真模块 TCE(TouCAN emulator)实现的，QEMU 结构如图 1 所示。

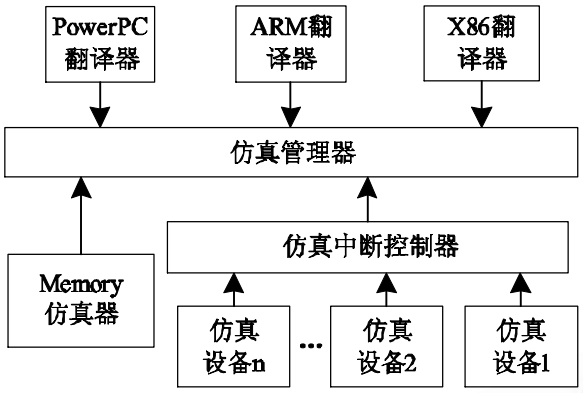

图 1　QEMU 的软件结构

本文第二节分析目前 CAN 总线网络仿真的研究现状。第三节描述 CAN 总线节点仿真器 CES 的具体实现。第四节分析 CES 网络的可靠性。第五节描述 CES 仿真器的使用方法。

2　相关工作

目前针对 CAN 现场总线仿真的主要研究热点可以分为数学仿真，时序仿真和系统级仿真。数学仿真的研究重点是 CAN 总线网络性能的分析方法，例如 DSPN 仿真模型[5]的主要作用就是对 CAN 现场总线的实时性做理论分析。系统级仿真的研究重点是 CAN 总线网络通讯行为的模拟，其仿真粒度是节点级，粒度较粗，因此不提供节点的硬件寄存器环境，例如 Lab Windows CVI[6]就是由美国国家仪器公司开发的一款可应用于 CAN 总线应用层协议分析的系统级仿真工具，它不满足车控网的软/硬件协同设计需求。时序仿真的研究重点是 CAN 总线时序信号的模拟，其仿真目标是 CAN 总线的时序信号，不向软件提供硬件寄存器环境，例如 LANTIRN CEU TPS[7]仿真器就是一款针对总线时序信号的仿真工具。

WANG Jianqiang[8]在 2009 年指出仿真是车控软件系统功能验证的重要手段之一，也是目前的研究热点。Binks[9]在 2003 年指出现有网络仿真器的缺点，例如缺乏信息交互，仿真粒度较粗，不提供寄存器级的细粒度仿真，不满足软/硬件协同设计需求等。

3　CAN总线网络的功能仿真

3.1 CAN 总线仿真网络的搭建

CAN 总线仿真网络由若干个 CAN 仿真节点组成，简称 CES 网络，其拓扑结构如图 2 所示。

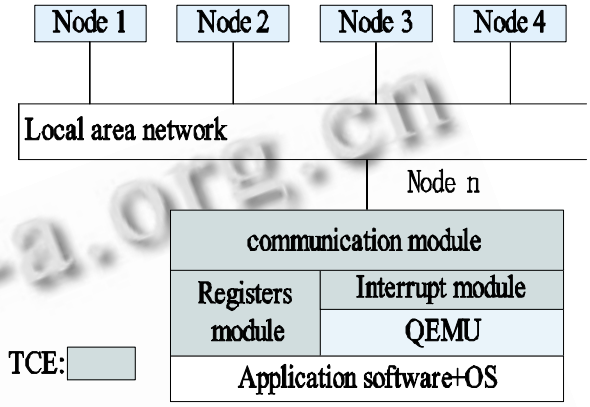

图 2　CES 网络

TCE 的寄存器模块仿真 TouCAN 的寄存器功能，中断模块仿真 TouCAN 的硬件中断行为，通讯模块仿真 CAN 总线节点的通讯行为。

3.2 TouCAN 设备介绍

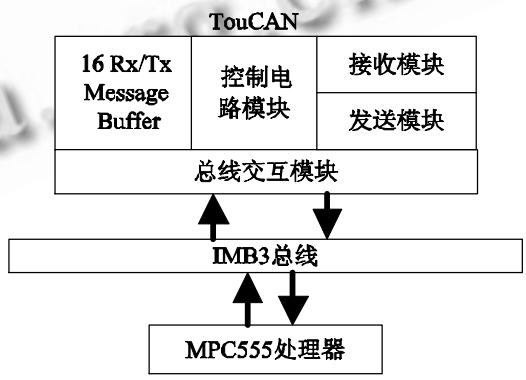

图 3　MPC555 芯片的 TouCAN

TouCAN 的结构如图 3 所示，总线交互模块是 IMB3(intermodule bus3)总线接口，控制电路模块的功能是控制设备的运行模式，主要有低功耗模式和非低功耗模式，消息发送和接收模块的功能是控制 CAN 协议帧数据在传输介质中的传输过程，16 个

Message Buffer 是 TouCAN 和上层软件交互 CAN 协议数据帧的接口。从 TouCAN 的功能仿真角度出发，TCE仿真的重点是TouCAN的寄存器接口和CAN总线仲裁机制。

3.3 TouCAN 寄存器接口的仿真

TCE 要仿真的 TouCAN 寄存器接口是表 1 所示的寄存器列表。TCE 先通过 QEMU 的 I/O 注册函数 cpu_register_io_memory 注册 TouCAN 所有硬件寄存器的地址空间，再分别解析寄存器的功能。

表 1 TouCAN 寄存器列表

寄存器名	在 I/O 地址空间中的地址
TCNMCR	0x307080~0x307082
CANTCR	0x307082~0x307084
CANICR	0x307084~0x307086
CANCTRL0	0x307086~0x307088
PRESDIV	0x307088~0x30708A
TIMER	0x30708A~0x30708C
RXGMSKHI	0x307090~0x30792
RXGMSKLO	0x307092~0x307094
RX14MSKHI	0x307094~0x307096
RX14MSKLO	0x307096~0x307098
RX15MSKHI	0x307098~0x30709A
RX15MSKLO	0x30709A~0x30709C
ESTAT	0x3070A0~0x3070A2
IMASK	0x3070A2~0x3070A4
IFLAG	0x3070A4~0x3070A6
RXECTR	0x3070A6~0x3070A8
MBUFF	0x307100~0x3071F0

3.4 CAN 总线仲裁机制的分析

CAN 总线仲裁机制定义在 CAN 协议的 MAC 子层中，任何一个 CAN 总线节点发送的报文都能被总线中其它节点监听和应答，当总线空闲时，总线网络中任何节点均可发送报文，若有多个节点同时发送报文，就会出现总线冲突问题。MAC 采用的总线仲裁机制是带优先级的载波监听多路访问/冲突避免机制(CSMA/CA)，核心思想是高优先级消息优先发送，具体流程如图 4 所示。

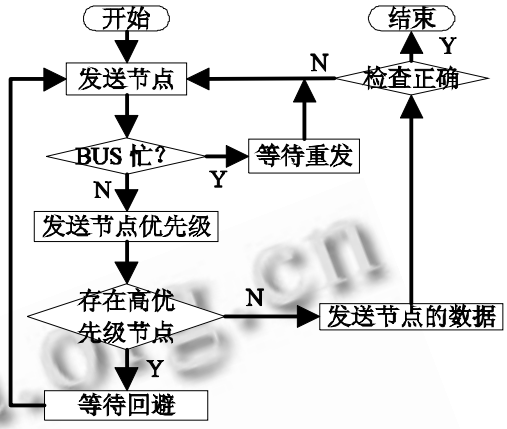

图 4 CAN 的 CSMA/CD 通信机制流程

3.5 CAN 总线仲裁机制的仿真

一般而言，CAN 总线网络节点数都小于 120 个[10]，而局域网的节点数可以达到 254 个，所以可通过局域网技术仿真 CAN 总线网络的拓扑结构和通讯行为。CES 利用局域网的 UDP 协议[11] 模拟 CAN 总线网络的通讯行为，并在虚拟局域网环境下，实现 CAN 总线仲裁机制的仿真。

为模拟 CAN 的总线仲裁机制，CES 引入一个令牌环竞争算法。该算法将总线控制权抽象为令牌环，发送数据帧的节点抽象为拥有令牌环的节点，其他监听节点都抽象为无令牌环的节点，CES 网络中所有节点均可通过消息优先级竞争令牌环，最终实现 CAN 总线仲裁机制的仿真。

为实现 CSMA/CA 机制中高优先级消息优先发送行为的仿真，CES 对 CAN 协议数据帧进行了封装，加入令牌环竞争信息，即消息优先级，具体消息格式如图 5 所示。

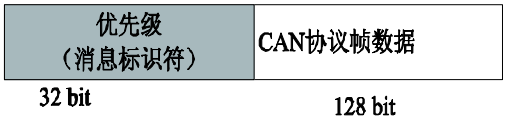

图 5 CES 网络中的消息格式

CES 网络的令牌环竞争算法嵌入在 TCE 的消息发送和接收流程中，其中发送流程如图 6 所示，接收流程如图 7 所示。

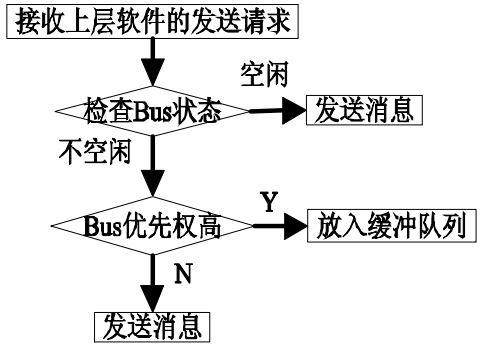

图 6　CES 的消息发送流程

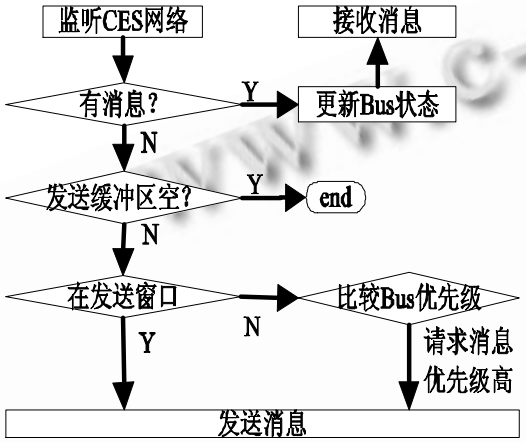

图 7　CES 的消息接收流程

CES 网络中的每个节点都保存 Bus 状态，即当前总线的优先级，仅当消息优先级大于总线优先级时，该消息所属节点才能抢占总线，广播消息，其他监听节点在收到该消息后，立即更新 Bus 状态。上一个拥有令牌环的节点边发送消息，边监听网络中，有无更高优先级的消息，在监听到高优先级消息时，就主动放弃总线控制权。

CES 中的任何节点都可能有连续发送多个分片 CAN 协议帧的需求， CES 为减少这种节点频繁竞争令牌环的开销，引入了发送窗口的概念：

发送窗口：刚抢占到总线的节点持续拥有总线控制权的时间。

4　CES网络可靠性分析

CES网络是基于不可靠的UDP数据传输协议实现的，鉴于此，本节将设计两个实验详细分析该网络的可靠性。一个实验分析 CES 网络的吞吐量，另一个实验分析 UDP 网络丢包率，实验结果表明 CES 网络是可靠的，满足通讯软件功能验证的需求。

在 CES 网络的节点中，成功发送 CAN 协议数据帧的时间 T 包括:嵌入式操作系统的中断响应时间 Ti，中断处理时间 Tisr，中断恢复时间 Tr，其中 Ti 和 Tr 大小和嵌入式操作系统平台相关，而 CAN 总线中断处理程序的执行时间 Tisr 和操作系统平台相关性不大。

$$T = Ti + Tisr + Tr \quad (1)$$

为测量 Tisr 大小，本文首先在 QEMU 的 I/O 地址空间中设计一个高精度计时器用于测量时间，该计时器利用宿主机处理器时钟周期计算时间。其次，在 QEMU 的 Powerpc 平台上，执行一个简单 CAN 中断处理程序 9 次，实验的结果如表 2 所示，而该程序的算法流程如下：

```
void can_interrupt(){
 初始化寄存器地址;
 设置相关功能寄存器;
 读取消息缓冲区状态寄存器;
 for(扫描 Message buffer){
     判断 Message buf 是接收/发送;
     }
}
```

表 2　CAN 中断处理时间 Tisr

实验序号	执行时间
1	1ms
2	5ms
3	4ms
4	2ms
5	3ms
6	25ms
7	27ms
8	37ms
9	17ms

在程序的执行过程中，会随机碰上更高优先级的中断，所以 Tisr 变化很大，本文在此假定它是一个符合均匀分布的随机变量，通过公式(4)，计算 Tisr 大于 1ms 的概率是 0.84。公式(2)和(4)中的 a 表示最小执行时间，b 表示最大执行时间，EX 表示 Tisr 的期望执

行时间，DX 表示 Tisr 的方差,公式(4)是锲比雪夫不等式，p 表示概率。

$$EX = \frac{a+b}{2} = 19\ ms \tag{2}$$

$$DX = \frac{(b-a)\times(b-a)}{12} = 108\ ms \tag{3}$$

$$p\{|X-EX|\le z\} \ge 1-\frac{DX}{z\times z} \tag{4}$$

$$\Rightarrow\ p\{x\in[1,37]\} \ge 1-\frac{108}{18\times 18} = 0.67$$
$$\Rightarrow\ p\{Tisr > 1ms\} \ge 1-0.33\div 2 = 0.84$$

$$T = Ti + Tisr + Tr > Tisr \ge 1ms \tag{5}$$

由公式(5)可知，CES 网络中的节点发送 CAN 协议帧的时间开销 T 都大于 1ms，而根据公式(6)可计算出 CES 的最大网络吐吐量 f 是 20kb/s，其中 CTU 是图 5 中的消息大小。

$$f = (1000/T)*CTU \tag{6}$$

$$T > 1ms$$
$$\Rightarrow\ f < 20\times 1000\div 1024\ kb/s$$
$$\Rightarrow\ f < 20\,kb/s$$

针对 CES 网络可靠性的问题，拟通过分析 UDP 局域网吞吐量和丢包率关系的方法进行评估，一般而言，丢包率越低，可靠性就越高。本文首先选择一个消息发送节点和两个接收消息的节点，然后让发送节点广播 CTU 大小的消息，统计发送频率，而接收节点统计消息丢失率，实验结果如图 8 所示。CES 网络吞吐量 f 远小于 112kb/s，所以网络是可靠的。

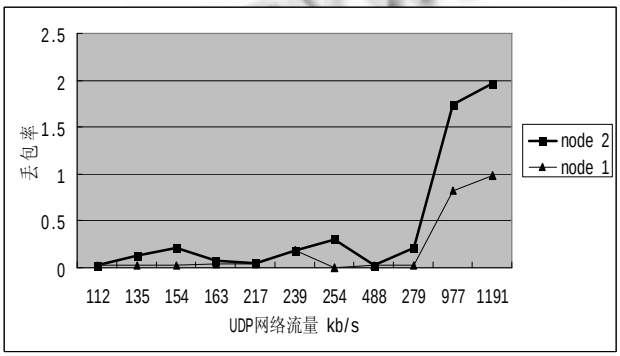

图 8 CES 网络可靠性分析

5 CES仿真器的使用

CES 的编译、使用方法和 QEMU 一样，都可以通过 kernel 选项执行二进制可执行文件。在本实验室 OSEK COM 通讯协议栈的开发过程中，我们利用 CES 功能仿真器对该通讯协议栈进行了功能验证。

OSEK COM 通讯协议栈和操作系统一起被编译成二进制镜像文件 software.bin，CES 通过 kernel 选项执行 software.bin，操作命令如下：

```
qemu-system-ppc --kernel software.bin
```

在局域网中，选择若干台机器，如图 10 所示，每台机器都利用 CES 仿真一个 CAN 总线节点，图 11 是消息发送节点的 CES 执行结果。

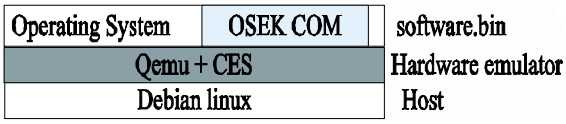

图 10 CAN 总线仿真节点

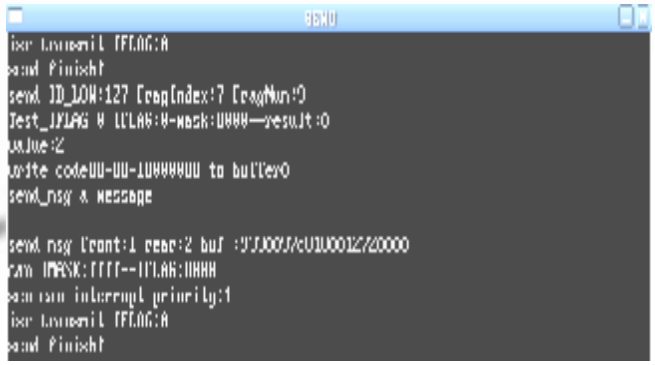

图 11 消息发送节点

本文的通讯协议栈分为消息发送中断响应例程、消息接收中断响应例程、消息缓冲寄存器识别例程、CAN 协议帧封装例程、CAN 协议帧解封例程、远程请求帧的处理例程、消息接收例程和消息发送例程几个子功能模块。我们在 CES 网络中，利用该通讯协议栈进行消息的发送和接收，验证它的各个子功能模块，第一次验证的结果如

表 3 所示。

表 3　通讯协议栈的功能验证结果

功能模块	是否正确
消息发送中断响应例程	正确
消息发送例程	正确
消息接收例程	不正确
消息接收中断响应例程	正确
CAN 协议帧解封例程	不正确
CAN 协议帧的封装例程	正确
远程请求帧的处理例程	不正确
消息缓冲寄存器识别例程	正确

6　总结与展望

本文以 MPC555 的 TouCAN 设备为仿真目标，在 qemu-0.9.1 上设计了 TouCAN 仿真模块 TCE，实现 CAN 总线网络节点的功能模拟，最终实现 CAN 总线节点功能仿真器 CES。为基于 CAN 总线的车控网设计，提供一个基本满足软/硬件协同设计需求的工具。本文的后续工作是在 qemu-0.11.5 上实现 TCE 仿真模块，并向 QEMU 开源社区提供 CES 模块的补丁。

参考文献

1 Lawrenz W. Network Development Techniques. IEE Colloquium on Vehicle Networks for Multiplexing and Data Communication, Dec 19, 1988:5/1－5/8.

2 BOSCH. CAN Specification Version 2.0. 1991.

3 Motorola. MPC555/MPC556USER'S MANUAL. October 2000.

4 Bellard F. QEMU, a Fast and Portable Dynamic Translator Proc. USENIX Annual Tech. Conf.,FREENIX Track, 2005:41－46.

5 刘君华.虚拟程序编程语 LabWindows/CVI 编程.北京:电子工业出版社, 2001.

6 韦雪洁,刘金梅,姚晓琼,李国洪. CAN 总线通信过程实时性能的仿真计算.兵工自动化, 2008,27(6):40－42.

7 Beat J. Programmable real time bus emulation with real time data update. 38th Annual Autotestcon Conference, Huntsville, Al 2002.

8 Wang JQ, Li SB, Huang XY, Li KQ. A Driving Simulation Platform Applied to Develop Driver Assistance Systems. IEEE Vehicle Power and Propulsion Conference, 2009.

9 Binks DFJ. IS EMULATION ENOUGH. Fourth International Conference on 3G Mobile Communication Technologies, London, UK, June 2003:134－138.

10 饶志强,严国萍,阮幼林,叶念愈. 基于 CAN 的最大总线长度和节点数求解方法.通讯和计算机, 2007,4(4):5－8.

11 Stevens RW. Internetworking Wth TCP/IP vol.II: Design implementation and Internals (Second Edition) . Addison-Wesley, 1994:96－99.