文章编号：1005-8451（2013）10-0050-05

CRH2型动车通信网络协议分析系统的设计与实现

于庆坡，谭献海
（西南交通大学 信息科学与技术学院，成都 610031）

摘 要：列车控制网络是面向控制的一种连接车载设备的网络通信系统，是分布式列车控制系统的重要组成部分，它能够通过信息的实时交互来实现对列车各种车载设备的通信、管理与控制等。通信协议是网络运行的最基本的保障，协议实现情况的好坏对于网络以及列车的正常运行都有重要的意义。本文对CRH2型车通信网络协议实现情况的分析方法进行了研究，并且设计了协议实现情况的分析工具，分析内容包括协议报文封装的分析，协议工作流程的分析，不同应用报文封装的分析，不同应用工作流程的分析等。

关键词：列车控制网络；ARCNET协议；协议分析
中图分类号：U285.5 ： TP39 **文献标识码：**A

Design and implementation of Protocol Analysis System on CRH2 EMU communication network

YU Qingpo, TAN Xianhai
(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: Train control network was a control-oriented network communication system which connected different kinds of device in the train. It was also an important part of distributed train control system. It could implement communication, management and control to train device by real-time communication. The protocol was the basic ensure for the network work. The implementation situation of protocol was of significant meaning to the network and the train operation. This paper studied on the analysis method of the implementation for the protocol of CRH2 EMU communication network, designed a tool which helped to achieve this object. The analysis was contained analysis to the packet encapsulation of the protocol, analysis to the work flow of the protocol, the analysis to the application packet encapsulation and the analysis to the work flow of different application.

Key words: train control network; ARCNET protocol; protocol analysis

随着现代列车朝高速化、自动化和舒适化的方向发展，越来越多的信息由此而产生，并且迫切需要在机车车辆之间互相传输与交换。因此列车控制网络的作用也越来越突出，而列车网络有序的运行要有相应的协议作为支撑，协议实现情况的好坏对于列车网络乃至列车的运行都有着重要的意义。对协议在列车网络中实现情况进行分析，有利于减少安全隐患，保障列车的安全运行和旅客的人身财产安全。本文对运行在CRH2型车通信网络上的ARCNET协议的实现情况进行了分析，包括协议报文封装的分析和协议工作流程的分析等。

网络协议分析指的是对某种已知协议或未知协议进行分析，该技术在网络安全领域应用广泛，比如在漏洞发掘中，工作人员要对某种协议的报文格式进行分析，之后按照该协议的报文格式构造畸形报文，最后进行FUZZING测试，当然构造畸形的报文的针对性越好，测试效果就会越显著。另外在入侵检测方面，协议分析也有着重要的地位。在列车网络协议分析方面，有文章对MVB（Multifunctional Vehicle Bus）总线的实时协议进行了分析，在基于列车通信网（TCN）实时协议和网络管理的研究和实现的文章中，对TCN实时协议从变量服务和协议以及消息服务和

收稿日期：2013-03-01
作者简介：于庆坡，在读硕士研究生；谭献海，副教授。

协议两方面进行了分析，文献[4]对WTB（Wire Train Bus）和MVB总线协议数据进行了分析，并且分别设计了MVB协议数据分析软件和TCN协议数据分析软件，文献[5]对TCN协议的一致性进行了测试，而ARCNET协议作为CRH2型车通信网络的重要协议，是网络通信的重要保障，而对该协议在网络中实现情况的分析相对较少，对于该协议的分析无论是对于以后ARCNET协议的深层次的开发，还是保障列车网络的有序运行以及列车的安全，都有着重要的意义，因此有必要对该协议在CRH2型动车网络上实现的情况进行分析。

1　CRH2通信网络协议分析需求分析

随着列车需要实时交互的信息的增多，在列车网络中传输的信息量也越来越大。网络工作情况的好坏关系到不同信息能否很好的交互，而协议作为网络运行的最基本的保障，有必要对网络协议的实现情况进行分析。对协议实现情况的分析大致包括协议不同帧格式封装的分析，协议工作流程实现的分析，封装在协议中的应用报文的分析以及不同应用的工作顺序的分析。要完成这几方面的分析，需要设计一个通信网络协议分析系统，并且该辅助系统应该包含以下几个模块。

1.1　ARCNET帧格式封装分析

ARCNET协议包含5种不同的帧格式，该模块的功能是在WINPCAP捕获到报文后对其进行解析，然后将其与标准的ARCNET协议帧格式进行对比，判断其是否符合规范要求。

1.2　ARCNET协议工作流程分析

该模块的功能是根据不同帧格式报文的发送接收顺序来判断分析ARCNET协议的工作流程。

1.3　封装在ARCNET协议帧中不同应用的分析

由于不同的应用信息封装在ARCNET协议的PAC帧的DATA字段中，因此该模块的功能是将封装在DATA字段中的内容解剖出来后，解析其封装并与规范进行比较，看是否符合规范中要求的应用报文封装格式。

1.4　不同应用报文工作流程分析

由于在CRH2型车中传输的信息各种各样，这些应用报文都有一些工作流程和时序，因此该模块的功能是根据不同应用报文的收发顺序判断各种应用的工作时序，进而与标准进行比较以判断是否同标准的要求相一致。

2　CRH2通信网络协议分析系统的设计

2.1　协议分析的基本思想

协议分析将获取到的报文视为具有严格定义格式的数据流，并将报文按照与封装相反的顺序层层解析出来，然后根据协议的标准对解析结果进行分析，其中标准的协议报文中包含了若干预先定义好的字段，协议分析的重点在检查当前数据包的各个字段值是否符合标准的期望值或在合理的范围之内。由此可见，协议分析就是根据协议标准报文字段中的期望值和合理值的相关知识，来判断是否出现了非法的网络流量[7]。在该项目中利用以太网来仿真ARCNET网络，所有的ARCNET协议报文都是封装在以太帧的数据字段中，用以太帧的类型字段来区分不同的ARCNET协议帧格式。因此可以借助不同的以太网的类型来区分不同的帧格式并进行分析。具体的以太网报文封装格式如下：

源地址	目的地址	类型	数据	CRC校验

2.2　ARCNET协议帧格式封装分析模块

ARCNET协议规范有5种帧格式，分别是令牌帧（ITT），空闲缓冲区询问帧（FBE），确认帧（ACK），否认帧（NAK），数据帧（PAC）。ARCNET 5种不同的帧格式如下：

（1）ITT报文

ALERT	EOT	DID	DID

ARCNET不管是哪种帧格式，都由ALERT来引导，类似于ETHERNET中使用的前导码，ITT帧中的EOT是传输结束控制符（04hex），后跟的2个字节都是目的节点标识符，即后继工作站的逻辑地址，重复使用的目的是增加可靠性。

（2）ACK报文

ALERT	ACK

ACK是ASC字符集中的确认字符（06hex），该报文中没有目的节点是因为这种帧格式是广播发送的。

（3）NAK报文

ALERT	NAK

NAK是ASC字符集中的否认字符（15hex）。这种报文也是广播发送的。

（4）FBE报文

ALERT	ENQ	DID	DID

该帧的ENQ是ASC字符集中的询问字符(05hex)，后跟2个重复的目的节点地址同样是为了增加传输的可靠性，

（5）PAC报文

ALERT	SOH	SID	DID	DID	CP	DATA	CRC	CRC

SOH是ASC字符集中的标题开始字符(01hex)，SID代表源站点，CP（连续指针）指示工作站在存取器中找到的传输数据的起点，2个重复目的节点同样是为了增加传输的可靠性，数据字段DATA的长度是可变的，从1个byte到508个byte不等，CRC为校验字段，对DATA进行校验，以实现DATA的可靠传输。

协议帧格式的分析过程如下：首先在搭建好的ARCNET网络仿真平台上加入分析节点，利用WINPCAP抓包工具来捕获在网络中传输的数据包，然后根据以太网帧格式中的类型字段来区分不同的帧格式，根据不同的类型做不同的处理。以PAC帧的分析为例，其余的帧格式分析与此类似。首先将PAC帧从以太帧的数据字段解剖出来，然后将其封装格式与标准的协议封装格式进行比较，依次读取每个字段的内容进行分析判断，看其是否是非法的字段信息，最后将报文信息写入到一个文件中，写入到文件中的信息包括：报文的类型，报文的到达时间，报文的长度，报文封装是否符合规范等。

该模块通过不同帧格式的分析，可以判断项目中开发的协议的报文封装是否符合标准的要求，同时可以将分析过程中发现的问题及时地向开发人员反映，这样便于提高协议开发的正确性。

2.3 协议工作流程分析模块

ARCNET网络的工作原理和令牌环网有些相似，由令牌控制各个节点数据的发送权限，节点在收到令牌后才有发送数据的资格，节点在收到令牌后，决定是否发送数据，如果没有数据发送，则将令牌传递到下一站，如果有数据发送，则先向目的节点发送FBE帧，询问对方是否有足够的缓冲区来接纳发送的数据，如果收到肯定应答ACK则向其发送PAC帧，即数据帧，如果收到否定应答NAK，则释放令牌，对方对接收到的报文进行校验，如果通过校验，则向发送方发送ACK确认帧，否则什么都不发送让发送方等待超时。由于每个节点的时隙有限，因此发送方如果在规定的时间内没有收到令牌则将令牌释放。

协议的工作流程分析步骤如下：在界面上有每种类型的帧对应的图形标识，如图1所示。在捕获到报文后，根据报文的类型将该类型的报文对应的图形标识发生变化。以ITT报文为例，在捕获到ITT类型的帧后，在界面上使其图像标识发生变化，如图2所示。同理，在捕获到FBE帧后，FBE帧的图像标识也会发生变化。因此可以在协议工作过程中，根据不同类型的帧对应的图像标识的变化来分析协议的工作流程是否与协议规范要求的工作流程相一致。

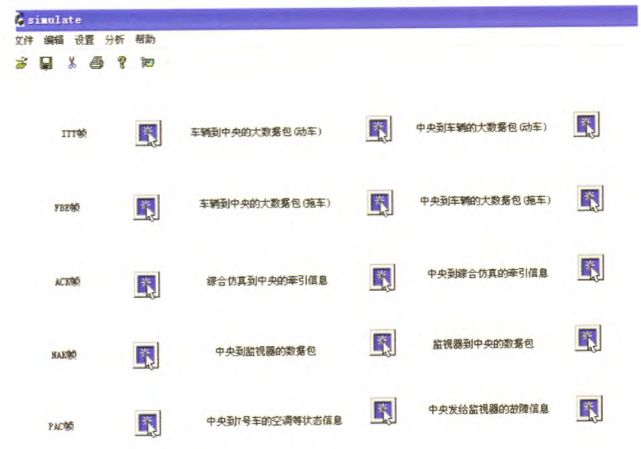

图1 协议工作流程的验证图

图2 捕获到ITT报文后对应标识的变化

通过对协议工作流程的分析，可以判断协议的工作流程是否同标准规定的要求相一致，便于提高协议开发的正确性，同时对于协议在列车网络中有条不紊的运行也有着重要的作用。

2.4 封装在ARCNET协议中的不同应用报文分析模块

在项目规范中应用报文的封装格式是：首先不同的应用信息封装在HDLC协议的信息字段中，然后将整个HDLC协议报文作为ARCNET协议PAC帧中DATA字段

中的内容封装在ARCNET协议的PAC帧中，再将整个PAC帧的信息封装在以太帧的DATA字段中。分析过程为在捕获到报文后，首先从以太报文中解剖出DATA字段中的内容，判断其是否符合PAC帧的封装格式，然后从PAC帧中解析出其DATA字段中的数据，判断是否符合HDLC协议的封装格式，如地址字段的内容是否正确等，然后将报文的信息写入文件。具体的分析流程如图3所示。

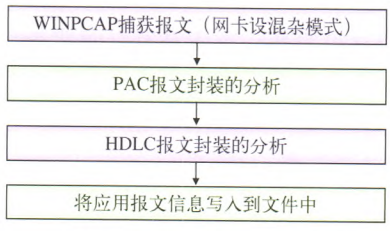

图3　应用报文的封装分析流程

对不同应用报文的封装分析，可以判断不同类型的应用报文的封装是否有与规范中相违背的不合法的字段，这对于提高应用报文封装的精确度有着重要的意义，同时由于在列车中传输的报文多种多样，不同的报文起着不同的作用，因此良好的应用报文封装对于列车正常运行也有着重要的影响。

2.5　不同应用报文工作流程分析模块

正常顺序下应用报文的交互如图4所示，非正常顺序下应用报文的交互如图5所示。

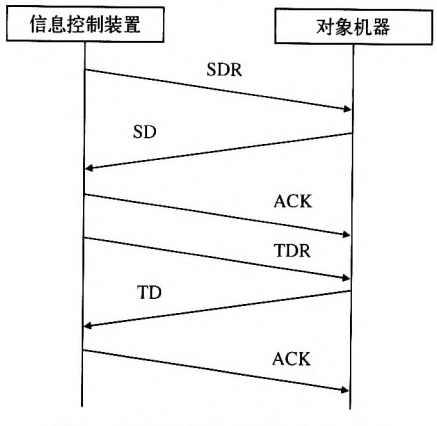

图4　正常顺序下应用报文的交互

注：信息控制装置指中央司控台，对象机器指中央终端或监视器

在列车网络中包含不同的应用报文，比如车辆发送给中央司控台的报文，中央司控台发送给车辆的报文，中央发给监视器的报文等。应用报文的工作流程分析过程是：首先利用WINPCAP

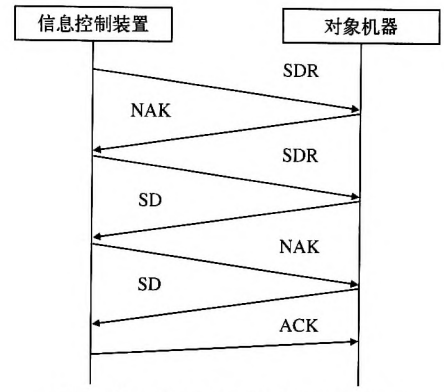

图5　非正常顺序下应用报文的交互

捕获到数据包后，根据应用报文的类型来改变界面上该类型报文对应的图形标识，然后根据不同图形标识的变化来分析不同应用的工作流程是否与标准上要求的工作流程相一致。以车辆信息控制装置向对象机器发送牵引请求信息为例，首先车辆信息控制装置向对象机器发送牵引请求信息（SDR），在捕获到这种类型的报文后，该类型的报文对应的图标会发生变化，如图6所示，若通过校验，对象机器会返回状态信息（SD），车辆信息控制装置在收到状态信息后对其进行校验，若是状态信息通过校验，则向对象机器发送ACK确认帧，因此可以根据不同图像标识的变化过程来判断应用报文的工作流程。

图6　收到牵引请求信息后图标的变化

应用报文的工作流程的分析对于列车协议实现的分析同样重要，在列车的运行中，不同的装置要交互信息，同时这些交互有一定的顺序，对于这些工作流程的分析对于保证列车的正常运行非常重要，对应用工作顺序的分析也可以判断出其是否符合标准的要求。

3　系统的测试

3.1　系统测试环境

硬件环境：

（1）Cisco SL224 10/100 M交换机；

（2）计算机CPU P4 2.0 GHz，内存2 G及以上，标准以太网卡；

（下转P58）

到模型中，使模型更加合理和完善，更准确地描述信息的传播过程，还需要进一步研究。相信随着更多的实证研究支持，可以为网络舆论的预测和引导提供更好的支撑。

参考文献：

[1] 刘 俊，金 聪，邓清华．无标度网络环境下E-mail病毒的传播模型[J]. 计算机工程，2009，35（21）：131-133，137.

[2] 张彦超，刘 云，张海峰，程 辉，熊 菲．基于在线社交网络的信息传播模型[J]. 物理学报，2011，60（5）：1-7.

[3] 许晓东，肖银涛，朱士瑞．微博社区的谣言传播仿真研究[J]. 计算机工程，2011，37（10）：272-274.

[4] 杨春霞，胡丹婷，胡 森．微博病毒传播模型研究[J]. 计算机工程，2012，38（15）：100-103.

[5] 丁 飞，刘 云，司夏萌，张彦超．舆论话题的传播与竞争[J]. 系统仿真学报，2009，21（23）：7660-7664.

[6] 孙庆川．人际信息传播模型及其模拟[D]. 上海：上海大学，2009.

[7] 刘 丰．基于微博的突发事件检测和信息传播建模[D]. 哈尔滨：哈尔滨工业大学，2011.

[8] 郑 蕾，李生红．基于微博网络的信息传播模型[J]. 通信技术，2012，45（2）：39-41.

[9] Mislove A, Marcon M, Gummadi K P, et al. Measure-ment and Analysis of Online Social Networks[C]. Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. [S. l.]：ACM Press, 2007.

[10] Fu Feng, Liu Lianghuan, Wang Long. Empirical Analysis of Online Social Networks in the Age of Web 2.0[J]. Physical A, 2008, 387（2）：675-684.

责任编辑 方 圆

（上接P53）

软件开发环境：

（1）编译器要求：Visual C++ 6.0；（2）操作系统：Windows XP Professional SP3；（3）通信中间件：Winpcap-4-0-1.exe, wpdpack. zip；（4）通用运行库：<ANSI stdio, stdlib, winpc-ap>。

3.2 系统的测试

在部署好环境后，运行协议分析软件，点击设置菜单下的“设置网卡”子菜单，进行网卡的设置，在分析菜单下面有“协议帧格式分析”，“协议工作流程分析”，“应用报文封装分析”和“应用报文工作流程分析”等子菜单，点击任何一个便开始不同功能的分析，在涉及到报文封装分析的部分，会生成一个名为“packet.txt”的文件，文件中包含报文封装相关的信息，前面已有所阐述，若要停止分析，可直接点击分析菜单下的“停止分析子菜单”。经过系统的测试，协议报文封装和工作流程以及应用报文封装和工作流程都符合规范的要求，从而检验了项目中所开发协议的正确性，达到了协议实现分析软件的功能

4 结束语

本文对运行在CRH2型列车控制网络上的ARCNET协议实现情况进行了分析，具体涵盖了协议本身5种帧格式的封装正确与否的分析以及协议工作流程的分析，封装在协议PAC帧中的应用报文封装格式的分析以及不同应用报文工作流程的分析。这种分析对于验证协议的实现和协议的进一步开发以及对列车控制网络有条不紊的运行都有着重要的意义。

参考文献：

[1] 路向阳．列车通信网络的发展与应用综述[J]. 机车电传动，2002（1）：5-9.

[2] 倪文波，王雪梅．高速列车网络与控制技术[M]. 成都：西南交通大学出版社，2011.

[3] 管 婷．TCN实时协议和网络管理的研究与实现[D]. 成都：西南交通大学，2011.

[4] 王兵兵．WTB和MVB协议数据分析软件设计[D]. 武汉：华中科技大学，2011.

[5] 王克举．TCN协议一致性测试研究[D]. 上海：同济大学，2007.

[6] 高 渊．协议识别与分析技术[D]. 上海：同济大学，2007.

[7] 中国南车株洲电力机车研究所．列车网络系统随车技师教材[Z].2008.

[8] 张曙光．CRH2型动车组[M]. 北京：中国铁道出版社，2008.

责任编辑 方 圆