Design and Implementation of the Software of Net Protocol Parse

Hao-Fei Xie, Yan-Bin Wu, Ping Wang
Chongqing University of Posts and TelecommunicationsKey Laboratory of Network control & Intelligent Instrument, Ministry of Education, Chongqing 400065, China
e-mail Wu1979121@yahoo.com.cn

Abstract: Based on the analysis of the communication model of the EPA protocol and the operational principle of the EPA data frame. A software structure for high efficiency EPA protocol *parser are designed, the system state engine, the protocol parser and the design process of EPA parser* are discussed in detail. Finally, the function test are taken, also, the test result indicated that the designed software can analysis network information with high efficiency in real time, reached the expected effect.

Keywords: EPA;system state engine;protocol parse

EPA 协议解析器的设计与实现

谢昊飞，吴艳彬，王平
重庆邮电大学 网络控制技术与智能仪器仪表教育部重点实验室 重庆 400065
E-mail Wu1979121@yahoo.com.cn

【摘要】本文分析了 EPA 协议的通信模型、EPA 数据帧的工作原理，设计了一种高效的 EPA 协议解析器的软件体系结构，深入讨论了系统状态引擎、协议解析器和 EPA 解码器的设计过程。文章最后进行了功能测试，测试表明开发的 EPA 协议解析器在网络流量、报文的时序、报文的完整性、UDP 下层的解码方面不仅能达到与 Ethereal 一样的效果，而且能解析 EPA 协议的所有报文。

【关键词】EPA 协议；系统状态引擎；协议分析；

1 引言

21 世纪初，工业以太网成为工业界研究的热点，各国开始了对工业以太网标准的争夺。2004 年我国提出的 EPA（Ethernet for plant automation）标准成为 IEC SC65C 组织的公用可用规范 PAS（Publicly Available Specification）。2007 年，EPA 被国际电工委员会 IEC 发布成为国际标准 IEC61158 的第 14 种类型。目前，基于 EPA 标准的工业产品在越来越多应用到各个控制领域中，而大量工程应用迫切需要协议分析工具提供EPA数据的分析，确保工程正确应用。协议分析是网络领域上非常关注的、也是发展较快的一个研究课题，它侦听控制网络的数据流量、设备运行状态、分析网络报文与协议的符合度、诊断网络故障，为工程的应用提供了极大的便利。

资助单位：国家 863/CIMS 资助项目子项目项目名称：EPA 网络监测分析软件；编号：2006AA040307-01。

为了保证数据捕获实时性、数据分析的实时性和系统的可靠性，本文中设计的 EPA 协议分析器采用了 Winpcap 开发包和多线程技术，在用户界面和底层的网络适配器间建立两个独立快速环形缓冲队列管理发送和接收报文，此外，还引入软件状态机，保证了软件可靠地执行。

2 EPA 协议分析

EPA 协议模型是在以太网和 TCP/IP 基础上提出来的改进结构，共六层：物理层、数据链路层、网络层、传输层、应用层和用户层，如图 1 所示。物理层和数据链路层仍然以太网的总线的物理层规范和用带碰撞检测的载波侦听多址访问（CSMA/CD）的总线机制。但是在数据链路层和网络层间，增加通信调度实体，进行各种报文的错时发送机制，确保通信的确定性。网络层和传输层保

978-1-935068-01-3 © 2009 SciRes.

留传统的 IP、ARP、ICMP、IGMP、UDP、TCP 协议。在应用层，EPA 协议增加了 EPA 套接字映射实体、EPA 应用访问实体和 EPA 系统管理实体，前者进行 EPA 报文的缓冲区的管理，后面的完成 EPA 过程数据和控制信息传递。EPA 用户层采用 IEC 61499-1、IEC 61499-2、IEC 61499-4 协议定义的“工业过程测量和控制系统用功能模块”和 IEC61804-1、IEC61804-1-2 协议定义的“过程控制用功能块”[1]。

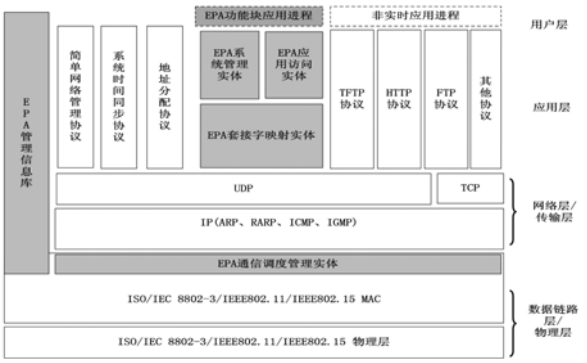

图 1. EPA 协议模型

为了支持快速 EPA 报文的处理，EPA 标准采用 0x88CB 类型标识 EPA 报文[2]，它与标准的以太网帧的区别如图 2 所示。EPA 帧由目的地址、源地址、帧类型（0x88CB）、IP 头、UDP 头、EPA 头、EPA 数据区和 CRC 校验码组成。EPA 头占 8 个字节，serviceID 字段占一个字节，标识 EPA 应用层服务类别；Length 字段占两个字节，标识 EPA 应用层实体报文的长度，包含报文头的长度；MessageID 字段占两个字节，标识服务的调用序列。

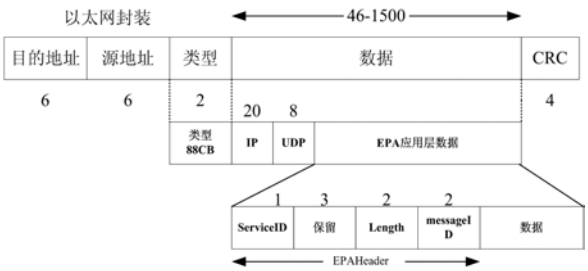

图 2. EPA 报文帧格式

3 EPA 协议分析软件设计

EPA 协议分析软件的总体结构如图 3 所示。它包括协议解析器功能模块、系统状态引擎、EPA 解码器、过滤器、环形缓冲器和信息数据库 6 个模块。

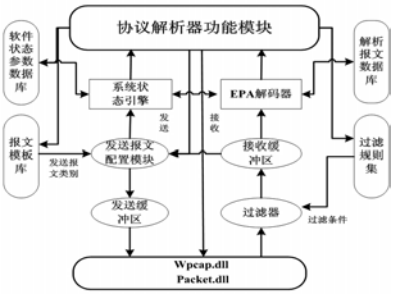

图 3. EPA 协议分析软件总体结构

协议解析器主界面收集关于EPA网络中各种数据报文、网络故障信息、并统计流量、分析 EPA 报文特征以及提供相关控制功能。系统状态引擎是整个软件控制的中心，它探测缓冲器、EPA 解码器、主界面和数据库的相关属性，完成状态机的切换。缓冲器由接收缓冲区和发送缓冲区组成，它们各自通过一个环形的队列来完成。为了保证协议分析的实时性，接收缓冲区和发送缓冲区由分别由两个独立的线程进行管理。EPA 解码器主要完成对 EPA 报文的符合性分析，并将分析好的摘要信息和详细信息提交给主界面，进行显示。信息数据库由报文模板库、解析报文数据库、软件状态参数数据库和过滤规则集组成。它们共同完成信息过滤，原始数据的重放等功能。

3.1 系统状态引擎设计

系统状态引擎考虑了软件启动时的初始化状态、无工作任务的空闲状态、出现异常情况下的故障状态、系统的正常工作的运行状态、数据的发送状态、数据的接收状态、程序的退出状态以及定时器的超时状态，它保证整个软件在状态间完成正常的切换，从而确保软件的可靠运行。

软件在刚刚开始执行时候，它会首先进入初始化状态，检查上一次软件执行的工作状态，初始化接收和发送缓冲区队列、定时器列表、过滤规则集、报文模板库、解析报文数据库、软件状态参数数据库。接着，它进入空闲状态。没有人为的控制启动执行功能的话，它维持本状态，如果启动成功且正常打开网络适配器，那么就进入运行状态，否则说明系统出了大的故障，应该交给故障状态处理。运行状态开始了网络的侦听，如果收到网络报文的话，那么会很快进入到接收状态，根据界面提供的规则集，实时分析 EPA 网络流过的各种报文数据。在某些情况下，用户可能还需要发送相关的控制命令，

那么系统就会发送状态。当发送数据长时期发送失败或接收报文数次不能正常传递给监控界面时，那么就会引发超时状态。故障状态实时监控整个状态机的相关资源利用情况，当出现资源分配冲突或者缺乏某种资源的时候，那么会停止相关的功能，如果问题十分严重，难以维持程序的运行，那么导致退出状态。退出状态，清理已经分配的资源，避免系统出现严重的崩溃状况，系统状态图如图 4。

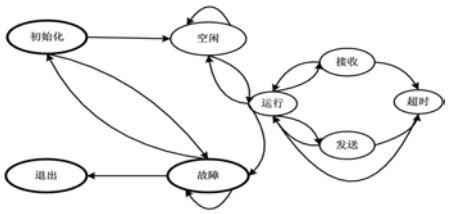

图 4. 系统状态机

3.2 协议解析器功能模块设计

协议解析器的功能包括 6 个子模块：流量统计、设备状态监控、协议摘要分析、协议层次结构分析、协议过滤和报文发送配置模块，如图 5 所示。

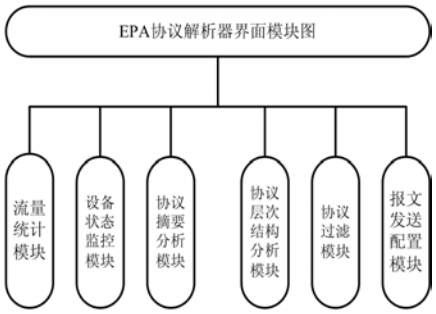

图 5. EPA 协议解析器界面模块图

流量统计模块实时地监控网络的EPA信息和非EPA 信息，统计网络的上行流量、下行流量以及相关错误信息。

设备状态监控模块将自动探测网络各个EPA设备位置，并分析当前设备的工作状态。EPA 网络中设备可以处于准备状态、就绪状态、周期报文发送状态和非周期报文发送状态。它能够帮助用户实时地分析设备的运行状况，远程定位系统的运行故障。

协议摘要分析模块从接收缓冲区实时解析获取报文，判断出报文的帧类型、捕获报文的准备时间、通信关系节点信息和报文主要功能，并这些信息交给监控主界面动态显示。

协议层次结构分析模块是对协议摘要分析模块更加详细解析。当用户需要查看更加具体的内容时，可以通过摘要分析模块的索引自动关联相应的报文，并从数据帧、IP、传输层、应用层和用户层 5 个方面给出报文的语法和语义。

协议过滤模块的功能十分丰富，它可以根据报文的 MAC 地址、IP 地址、协议类型、端口，应用层特点，甚至是用户自定义的字段进行过滤。为了支持较为复杂的过滤规则，协议过滤模块支持若干过滤规则组合过滤。

报文发送配置模块为高级用户提供额外的调试诊断功能。用户可以根据自己的需要定制各种类型报文，或选择模板库中报文，或使用接收的报文组装特制报文，驱动下层的发送线程来进行网络调试。

3.3 EPA 解码器设计

由于 EPA 协议是在以太网和 TCP/IP 协议栈的基础上的改进模型，因此它的解析原理与 TCP/IP 是类似的。它启动接收线程，不停地将 Winpcap 接收的报文送至过滤器中，过滤器处理完后将报文送至接收报文环形缓冲区。上层界面发送监控命令后，EPA 解码器会立即分析报文，首先根据以太网头的长度/类型字段，可以确定帧数据将交由上层哪种协议进行处理。一旦捕获的帧类型是 0x88CB，则认为是 EPA 报文，接下来把后移 14 个字节，进行 IP 头的分析，根据 IP 头的协议字段，确定 IP 数据将交由上层何种协议处理，对 EPA 报文而言，IP 协议的如果是 17，既交由 UDP 协议处理。接着后移 20 字节就是 UDP 头，根据 UDP 头的端口号以确定应用层协议。对 EPA 报文而言，UDP 协议的端口是 0x88BC，根据 EPA 头的 ServiceID 字段，确定 EPA 应用层协议。如果 ServiceID 是 4，则交由 EPA 的设备声明服务报文处理。最后接下来再后移八字节，则是 EPA 设备声明报文的起始位置。根据设备声明报文的结构定义，确定对应的字段的值。其他 EPA 报文使用类同的分析方法。整个解析过程如图 6 所示。

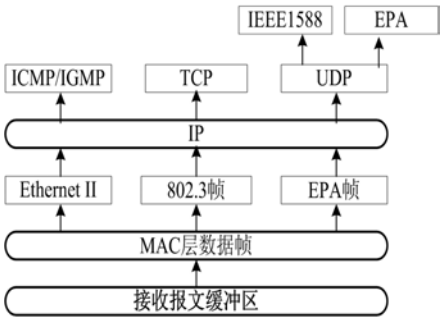

图 6. EPA 解码的层次结构

978-1-935068-01-3 © 2009 SciRes.

4 测试结果

本文提出的协议分析器已经实现，目前应用于我们实验室的 EPA 的网络监测，实验室开发 EPA 标准设备和 EPA 测试平台的调试过程。实验室的 EPA 网络用于设备的开发，设备协议的各种测试。EPA 协议分析器测试环境如图 7。EPA 协议解析器通过双绞线接入 EPA 网络，该测试环境包含 2 个 EPA 标准设备，1 个 EPA 待测设备，一个时间同步测试设备，时间同步测试服务器。EPA 协议解析器能够实时的捕获和解析该网络上的所有报文。

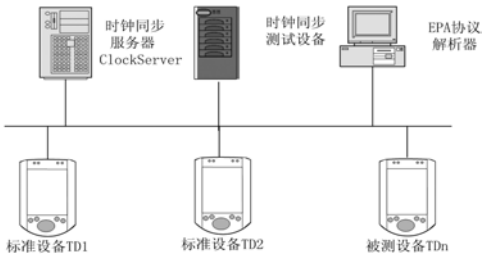

图 7. EPA 协议分析器测试环境图

4.1 功能测试结果

文中所开发的协议解析器，与 Ethereal（当前流行的一种计算机网络调试和数据包嗅探软件[3]）的测试结果相比较，在网络流量、报文的时序、报文的完整性、UDP 下层的解码方面不仅能达到 Ethereal 一样的效果，而且能解析 EPA 标准涉及的所有协议。Ethreal 和 EPA 协议解析器的功能比较如图 10。

表 1. 功能比较图

能够解析 / 协议类别	EPA 协议解析器	Ethreal
ARP、ICMP、IP	支持	支持
TCP\UDP	支持	支持
SNMP、HTTP、DHCP、		支持
PTP	支持	
IEEE1588	支持	支持
EPA 应用层协议	支持	否
EPA 调度协议	支持	否

4.2 数据包捕获性能测试

在性能测试过程中，用 sniffer 以全速向 PC 机发送报文为 130byte 的 UDP 数据包，发送时常为 10 秒。在测试环境中同时运行运行 EPA 协议分析器和 Ethrea 不再接入其它设备，防止干扰测试数据。两种软件就截获的数据包的统计的结果如图 10 所示。

表 2. 两种测试工具测试性能的比较

数据 / 类别	Sinffer 发送	EPA 协议解析器接收	Ethreal 接收
数据包	74432	74432	74433
总比特数	9973888	9973888	9974018
平均速率	946978b/s	793855b/s	793865b/s
发送时长	10.532333s	12.563861s	12.2563856s

通过观察图 10 可知，EPA 协议分析器的实际截获率为%100，实际捕包时长和 Ethreal 的捕包时长相差仅差 4 个微妙，所以该协议解析器满足实际需要。

5 结束语

通过分析测试结果，可知该协议解析器达到了稳定性，可靠性，实时性，一致性的要求。所以该测试器满足实际需要。由于本软件采用的是协议树加特征字的方法，因此有很强的扩展性，后续工作就是要完成不同协议插件接口，当有新的协议出现，可以通过插件的方式快速的实现协议的解析。

References(参考文献)

[1] [国家质量技术监督局，中国人民共和国国家标准“用于工业测量与控制系统的 EPA 系统结构与通信规范”，GB/T 20171-2006, 2006] China State Bureau of Quality and Technical Supervision, China State Standard “EPA System Architecture and communication Specification for use in industrial control and measurement systems”, GB/T 20171-2006, 2006, [S].

[2] Page15. 冯冬芹，徐皑冬，梅格，国际电工委员会/公共可用规范第 62409 号文件，实时工业以太网，第一版，国际电工委员会/第 65 工作组，2005：第 15 页 Feng Dong-qin, Xu Ai-dong, Mei Ke, IEC/PAS 62409, Real time Ethernet EPA (Ethernet for Plant Automation) [S] Version 1, IEC/65C, 2005

[3] 王丽萍，孙 蕾 基于 Ethereal 开源代码构建协议解析器的方法研究 [J] 计算机技术与发展 2007-10 1673-629X(2007)10-0027-04 Sun li ping，sunlei Study on Establishment of Protocol Parser Using Ethereal Public Code Computer Technology and Development 2007-10 1673-629X(2007)10-0027-04