文章编号:1671-4598(2016)02-0084-04 DOI:10.16526/j.cnki.11—4762/tp.2016.02.023 中图分类号:TP393 文献标识码:A

航天测控网实时数据流量监控与分析技术

谢文杰[1],周晓凡[1],栾晓文[2],周荣娟[1]
(1.中国人民解放军 63615部队,新疆 库尔勒 841001;
2.中国人民解放军 63610部队,新疆 库尔勒 841001)

摘要:航天测控网实时数据是航天发射中最重要的试验信息,实时数据交换直接影响着任务的顺利实施;由于航天中心采用自定义网络协议,商业软件不能够对协议数据进行有效监控和深入分析;根据航天测控网体系结构和业务特点,设计了被动式网络数据监控方案,采用专用硬件和底层驱动程序进行网络高速数据采集,实现了基于开源软件Wireshark的航天测控实时包数据交换协议(PDXP)的具体解析;实验结果表明,提出的实时数据监控和分析技术具备强大的数据包捕获和过滤能力,同时便于扩展网络协议,可以对航天中心各类传输信息进行监控和分析,为航天测控网数据监控、性能评估、故障诊断提供有效手段。

关键词:航天测控网;实时数据;网络协议;监控;分析

Real-time Data Traffic Monitoring and Analysis Techniques for China's TT&C Network

Xie Wenjie[1], Zhou Xiaofan[1], Luan Xiaowen[2], Zhou Rongjuan[1]
(1. Unit 63615 of PLA, Korla 841001, China; 2. Unit 63610 of PLA, Korla 841001, China)

Abstract: The real-time data in China's TT&C network is the most important experiment information about space launch. The real-time data exchange plays a pivotal role in the process of the space flight mission. The application data encapsulated by custom-built network protocols used in the space center is not able to be effectively monitored and deep analysed with commercial software. A passive network data monitoring scheme is designed according to the features of TT&C network architecture and traffic, using dedicated hardware and low-level drivers for network to acquire high-speed data. A analyser for Packet Data eXchange Protocol (PDXP) that is one of real-time application protocols of TT&C network is developed specifically based on open source software Wireshark. Experimental results show that the techniques presented above with powerful capabilities of packet capture and filtering and good expansibility of protocol can be used to monitor and analyse various TT&C network traffic as an effective means of monitoring data, evaluating performance and diagnosing fault in space center.

Keywords: TT&C network; real-time data; network protocol; monitoring; analysis

0 引言

随着一体化试验信息系统的规划建设,航天测控网实现了设备的IP接口改造和试验信息的IP化传输。航天测控网作为航天飞行试验任务信息交换、处理和应用的基础平台,承担着实时数据、语音、视频、文件等各类业务信息的传输,对圆满完成任务的跟踪测量、指挥控制、效果评估起着重要的保障作用。相对于先前的HDLC(high-level data link control,高级数据链路控制规程)点对点电路数据交换方式,网络IP数据包交换系统结构复杂、业务应用综合、信息流量巨大,掌握网络运行性能和服务质量、调整网络状态、排除网络故障的难度变大,必须加强对网络的监控和分析。

网络监控包括对网络设备状态的监控和网上传输数据的监控两个方面。航天测控网随设备安装配置了相应的网络管理系统(例如华为公司的iManger U2000),能够监控和管理路由器、交换机等重要设备,但是航天中心对网络传输数据、尤其是高层应用实时数据仍然缺乏有效的监控和分析手段。目前,航天测控信息传输采用了基于TCP/IP协议族定制的多种应用层数据交换协议,市场上现有商业软件只能完成对数据包中标准协议单元的解析,而无法对自定义的专用协议单元进行具体的数据分析[1]。另一方面从任务实际看,参试测控系统和设备之间的实时数据传输约定优先级最高,对任务的顺利进行影响最大,是任务实施过程中航天中心需要重点监控和保障的信息。只有紧密结合航天测控网的体系结构和业务特点,设计和部署网络数据监控系统,开发专用的实时数据分析软件,才能满足航天飞行试验任务需求。

1 网络数据监控方案设计

航天测控网管理要求高,网络技术状态严格受控。为此,采用独立的硬件和软件,主要以网络侦听的方式进行数据采集和分析,这种被动监控方法最大限度减少对网络设备的影响,也不会在网络上增加额外的数据流量。

1.1 系统组成

航天测控网数据监控与分析系统的硬件组成如图1所示。它以千兆高速交换机为核心,包括各种功能计算机、存储设备、网络分流器(TAP)、网卡。系统按照功能划分为数据采集、数据存储和数据分析三部分。监控工作站一般安装有双网卡,一块网卡与被监控网络的交换机(或路由器)连接,另一块网卡与监控交换机连接,能够采集和存储被监控网络的数据包。监控工作站必须具备初步的数据分析能力,既可以捕获流

收稿日期:2015-08-14; 修回日期:2015-10-10。

作者简介:谢文杰(1972-),男,湖南湘乡人,在读硕士研究生,工程师,主要从事测控网络及数据处理技术方向的研究。

经目标端口的所有数据包，也可以根据协议、IP 地址、端口等过滤接收的网络数据包，实现对特定应用和特定方向通信状况的监控。分析工作站主要在事后从数据包文件中提取出满足研究需要的网络数据集，对网络数据集对象进行挖掘分析和综合统计，获取有关任务过程和网络问题的完整信息和有针对性的结论。大容量、高速网络存储设备，用来集中保存监控工作站捕获的网络数据包和分析工作站产生的结果数据文件。

航天测控网由局域网、城域网和广域网组成，采用核心层、汇聚层、接入层三层结构设计。在不同层级网络信息出入口位置，安装固定的计算机进行长时间监控，获取任务过程中网络通信的典型数据集。在各个网络内部，根据故障排查、性能测试等工作需要，可在特定位置使用分流器或镜像端口灵活接入监控工作站，采集网络局部短时通信流量，以便实时监控和分析网络状态。

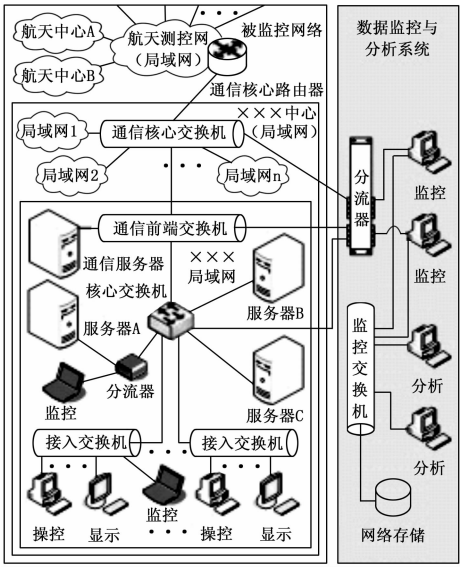

图 1　航天测控网数据监控与分析系统组成

1.2　数据采集

从硬件和软件的设计上满足复杂、高速交换网络中数据采集的灵活性、可靠性需求。

1.2.1　镜像端口数据复制

对网络进行数据监控时一般采用交换机端口镜像方式[1-2]，监控工作站直接与交换机镜像端口连接，但是更多情况下是通过分流器来获取网络流量。分流器作为网络流量采集专用设备，采用 ASIC 专用芯片设计，可以完成多端口线速流量复制。同时分流器在硬件上采取特殊措施，可以保证在设备掉电或故障时不中断和干扰被监控网络的正常通信。高端的分流器还具备多网段、分组式流量复制汇聚功能，有的甚至支持负载均衡、包过滤功能，非常适合于大型网络多结点采集、多监控输出的应用。如图 2 所示，分流器对全部采集流量按端口分成 3 组管理，将从各个子网采集的 4 个单一业务类型、低速数据流量汇聚成 1 个流量输出；将从主干链路上得到的 1 个多业务类型、高速数据流量复制成 3 个流量输出，每个输出流量可以包含全部或部分输入流量；对于带宽合适的输入流量直接输出。通过分流器不仅能够满足不同目标同时监控的需求，还减轻了监控工作站高速流量实时采集的压力。

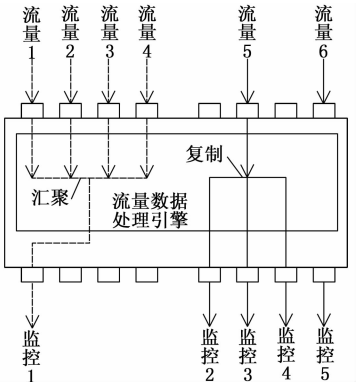

图 2　分流器流量复制和汇聚

1.2.2　底层驱动程序捕包

系统监控工作站采用高性能网卡加 WinPcap 库的方式捕获数据包。WinPcap 是一个基于 Windows 平台、用于捕获网络数据包并进行分析的开源函数库，具有与 Unix/Linux Libpcap 类似的体系结构和 API 接口。WinPcap 将网卡设置成混杂（Promiscuous）工作模式，使网卡工作在侦听状态，网卡驱动程序就会强行接收途经网卡的所有数据包[3]。网络捕包程序需要经过网卡缓存到内核空间、内核空间到用户空间两次内存复制才能取到网络数据包，在网络太忙、机器速度较慢时会存在丢包问题[2-3]。采用 WinPcap 中 NPF 过滤机制，允许用户及早在核心层对数据包进行过滤，只将用户关心的数据提交给用户程序，减少了数据传送量，提高了捕获性能。

1.3　数据分析

航天测控网传输的信息既有测量、引导、指控等实时数据，又有语音、视频数据和非实时的文件数据。其中实时数据使用了航天中心自定义的多种网络高层协议，并且是航天中心最为关心的一类信息，所以航天测控网数据分析必须以应用层实时数据为重点。数据分析分为实时数据分析和事后数据分析。实时数据分析识别从网络底层到高层数据包所使用的协议类型，并分析出各层协议的字段、特征字串、版本等信息，对应用层实时数据关键参数内容进行解析。事后数据分析能够针对应用、协议、端口和设备，对不同时间段和网络位置采集的网络数据集进行综合统计和分析，主要有数据包时间和空间分布分析、端到端通信分析、异常数据分析、实时数据流量统计、实时数据传输中断、延迟和乱序分析等。实时数据流量识别和协议解析是实现实时数据监控和分析的前提和基础。

1.4　系统特点

实时数据监控与分析系统充分考虑了航天测控网网络结构的复杂性、应用的多样性和运行的可靠性，在设计上有以下特点：

1）工作时仅从被监控网络获取数据包拷贝，生成的新的数据流量不进入被监控网络，几乎不占用被监控网络对象的资源，不影响被监控网络的路由和交换工作。

2）采用长时、定点监控与短时、机动监控相结合，既能保证对网络核心位置重点监控，又能以对网络局部监控作为补充，达到全面掌握网络工作状态、迅速处置网络故障的目标。

3）网络数据分析涵盖网络通信协议的低层到高层，以高层航天飞行试验任务实时数据分析为主。自动识别不同格式实时数据流量，对实时数据的参数特征（标志字段、帧/包长等）、分布特征（数据在时间和空间上的出现情况）、性能指标（如丢包/帧率、吞吐量、传输速率等）进行分析和统计。

2 实时数据分析实现方法

根据约定，测控设备与航天中心间，航天中心与航天中心间的实时数据传输采用包数据交换协议（Packet Data eXchange Protocol，PDXP）。下面简要介绍 PDXP 协议及协议分析的实现方法。

2.1 Wireshark 开源代码获取及安装

Wireshark 是运行于 Windows 及类 Unix（包括 Linux）平台上的一个具有图形化用户接口的包捕获和分析工具，其前身为著名的 Ethereal 软件。Wireshark 支持对一千余种协议进行深度解析，采用 pcap 文件格式及其扩展版本 pcap-ng 存储网络信息。重要的是 Wireshark 软件是开源的，在 GNUGPL 通用许可证的保障范围内，使用者可以免费取得该软件及其源代码，并可以根据自身的需要对 Wireshark 进行定制或扩展[4]。利用 Wireshark 的开放性，可以编写专用协议解析程序插件实现对 PDXP 格式数据包的分析。Wireshark 是用 C 语言编写的，在进行二次开发前需要安装软件工具和配置开发环境，基于 Windows 系统搭建开发平台的详细方法与过程可参考文献[4]。

2.2 PDXP 协议

PDXP 协议是基于 TCP/IP 协议模型分层结构定义的应用层数据交换协议，通信双方以结构化数据包的形式采用数据主动推送方式进行数据交换，并完成数据的封装与解包。PDXP 协议可以采用组播和单播两种传输方式进行数据传输，传输层采用 UDP 协议。

PDXP 协议格式如图 3 所示，应用数据包由包含若干标志字段的包头和数据域组成，数据域可以按相应帧格式传输起飞零点、雷达数据、光学数据、遥测参数、轨道数据、设备状态等各种实时信息。

图 3 PDXP 协议格式

2.3 协议分析

Wireshark 定义了规范的开发框架[5-6]，按照规范语法格式定义 PDXP 协议格式结构，正确解析协议中各字段的意义。将编写的 PDXP 协议分析插件代码静态编译到主程序 libwireshark. dll 内或单独编译为 DLL。编写 C 程序插件的主要步骤和关键代码如下：

1）协议注册。

通过调用 proto _ register _ protocol（）函数向主程序注册一个名为 PDXP 的协议解析器；使用 hf _ register _ info hf []数组定义和保存协议中需要解析的各个字段，调用 proto _ register _ field _ array（）函数把字段信息注册到 PDXP 协议下面，proto _ register _ subtree _ array（）函数将相应的项和值添加到协议树下面。

2）协议提交。

```
proto _ reg _ handoff _ PDXP（void）{
  heur _ dissector _ add（" udp"，dissect _ PDXP _ heur，proto _ PDXP）；
```

上面代码中 dissect _ PDXP _ heur 为 PDXP 协议解析函数名称，proto _ PDXP 是第一步中注册得到的协议标识。heur _ dissector _ add（）函数将 dissect _ PDXP _ heur 所代表的解析器挂载到 Wireshark 协议树的 UDP 结点上面，告诉系统 UDP 数据包由 dissect _ PDXP _ heur 解析模块来处理。

3）协议分析。

dissect _ PDXP _ heur（）函数中的代码就是 PDXP 协议解析器具体要做的工作。函数具备深度包检测（DPI）功能，通过综合分析端口号、协议特征串、协议语法等进行应用流量识别。接下来将 PDXP 数据包包头各个字段的信息详细解析出来，还可以根据需要对 Data 域中的有效载荷进一步分析，如对匹配某些特征或参数的数据包进行特殊处理。最后调用 col _ set _ str（）、proto _ tree _ add _ item（）等函数将数据包分析过程中得到的信息在 Wireshark 界面上显示出来。

3 实例验证

在某航天中心计算机局域网通信前端交换机的镜像端口，使用 Wireshark 采集一段网络流量数据，并保存为 .pcap 文件。在 Wireshark 中注册 PDXP 协议分析插件，对网络数据包文件进行解析，查看实时数据分析结果。

3.1 协议注册验证

如果 PDXP 协议分析插件注册成功，那么 PDXP 协议将被添加到 Wireshark 所支持的协议集合中，通过图 4 所示界面可以查询到包括 PDXP 在内的所有软件支持的协议。

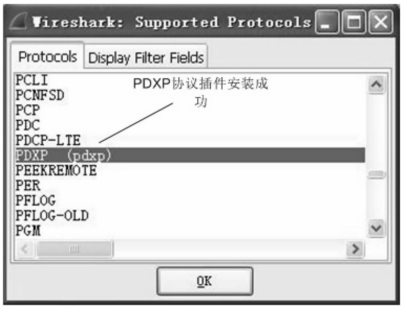

图 4 Wireshark 支持的协议

3.2 实时数据监控与分析结果

在没有安装 PDXP 协议解析插件时，Wireshark 对包含实时数据的网络数据包只能够分析到 UDP 协议层，封装在 UDP 报文中的 PDXP 协议数据单元被整体当作 UDP 报文数据，以一段不易理解的十六进制代码的形式显示在界面中，效果如图 5 所示。安装 PDXP 协议解析插件之后，Wireshark 继 UDP 报文解析之后分析 PDXP 数据包，在数据包细节显示区域可以看到 PDXP 包头中的 VER、MID、SID 等字段，字段的内容有的直接以对应的数值显示，有的被解释成更有意义的字符串显示，效果如图 6 所示。在实现 PDXP 协议分析的基础上，借助于 Wireshark 强大的数据包过滤、信息统计、图形展示功能，

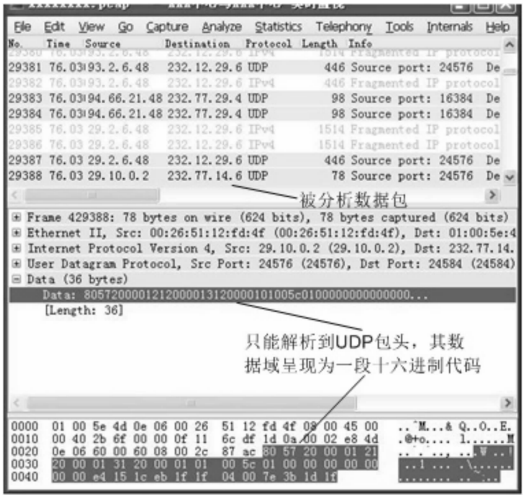

图 5　未安装 PDXP 协议解析插件时的数据包分析结果

图 6　PDXP 数据包分析结果

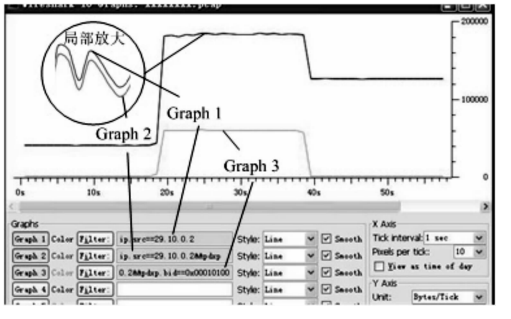

图 7　通信服务器输出带宽时间分布曲线

能够获得更多、更有价值、更有针对性的测控网实时数据交换信息，为及时发现网络和应用问题、快速定位网络故障提供有力的指导和帮助。在 Wireshark IO Graph 中使用显示过滤器对某通信服务器的输出带宽进行分析，如图 7 所示，其中 Graph1 为全部数据的带宽，Graph2 为实时数据的带宽，Graph3 为起飞零点数据的带宽。从图形中可以直观地看出实时数据占用了服务器绝大部分输出带宽，在大约 20 s 时服务器输出带宽有一个大幅跃升，且在 20～40 s 左右服务器输出带宽出现一段由起飞零点数据造成的矩形台阶。通信服务器输出带宽的变化反映了以起飞零点信号的到来为航天飞行试验任务启动标志，通信服务器由通信保持转换为数据转发状态。

4　结束语

航天飞行试验任务日益繁重，参试系统和设备不断增多，网络问题突发的概率逐渐变大，加强对航天测控网实时数据传输情况的监控和分析，对提高任务组织指挥效率、保障任务实施过程顺利圆满具有重要意义。本文根据航天测控网的层次结构，设计了一种高效适用的高性能硬件加软件的网络数据监控方案，提出了基于 Wireshark 的实时数据分析实现方法。与采用专用设备（如探针）相比，本文所述技术成本较低、容易实现，尤其是针对航天中心不同类型业务数据能够方便地增加新的协议分析程序。后续，需进一步做好实时数据的深入挖掘和分析工作，使监控系统在网络数据交换、网络性能评估、网络故障诊断、网络异常报警等方面发挥重要作用，为航天测控网保持高性能、高可靠性和高可用率提供技术手段。

参考文献：

[1] 白　冰，王　丹. 基于简单网络管理协议的运载火箭网络监控系统研究 [J]. 导弹与航天运载技术，2013 (3)：69－72.

[2] 汪立东，钱丽萍. 网络流量分类方法与实践 [M]. 北京：人民邮电出版社，2013.

[3] 王　攀，王远峰，张顺颐. IP 流量统计方法及实现 [J]. 南京邮电学院学报，2002，22 (2)：53－58.

[4] 罗青林，徐克付，臧文羽，等. Wireshark 环境下的网络协议解析与验证方法 [J]. 计算机工程与设计，2011，32 (3)：770－773.

[5] Creating Your Own Custom Wireshark Dissector [EB/OL]. http：//www. codeproject. com/KB/IP/custom _ dissector. aspx，2010－12－25.

[6] How to Generate Wireshark Dissectors using TSN. 1 Compiler [EB/OL]. http：//www. protomatics. com/Wireshark _ dissector. Html，2010－12－25.

[7] WinPcap. The Windows Packet Capture Library [EB/OL]. http：//www. winpcap. org，2012－02－15.

[8] 宋政斌，郭晓玲，于　艳. 网络监听技术在飞行试验机载测试中的应用与研究 [J]. 计算机测量与控制，2009，17 (10)：1917－1919.

[9] 李　臻，杨雅辉，张广兴. 大业务流识别方法研究综述 [J]. 计算机应用研究，2011，28 (1)：6－9.

[10] Angela Qrebaugh. Wireshark&Ethereal Network Protocol Analyzer Toolkit [M]. Syngress Publishing，Inc，2007.

[11] 谢　鲲，张大方，文吉刚，等. 基于 WinPcap 的实时网络监测系统 [J]. 湖南大学学报，2006，33 (2)：118－121.

[12] Chris Sanders. Wireshark 数据包分析实战（第 2 版）[M]. 诸葛建伟，陈　霖，译. 北京：人民邮电出版社，2013.

[13] Yoram Orzach. Wireshark 网络分析实战 [M]. 古宏霞，孙余强，译. 北京：人民邮电出版社，2015.

[14] 彭　城. 基于 Wireshark 的协议分析研究与扩展实现 [D]. 成都：电子科技大学，2007.

[15] 林　川，施晓秋，胡　波. 网络性能测试与分析 [M]. 北京：高等教育出版社，2009.