文章编号：2096-1472(2016)-11-45-03

基于主动节点的跨平台网络监控系统设计与实现

许劭庆，马 彪，安海英
（国网吉林省电力有限公司，吉林 长春 130021）

摘 要：电力企业内部网络监控设备众多，品牌性能各不相同，网络监控难度也越来越大。为了解决不同平台的网络设备监控的难题，本文以跨平台技术为基础，设计了由网络资源设备、主动节点、监控信息库构成的跨平台网络监控系统。系统设计了基于主动网络的动态数据采集算法实现数据的周期性采集，采用主动报文的形式将信息发送给监控平台服务端，通过构造主动节点实现数据的采集和传送控制。本系统于2015年在国网吉林省电力有限公司开始应用，实现了对电力系统不同网络设备进行状态监控集中管理，极大的提高了运维效率。

关键词：主动节点；数据采集；主动报文
中图分类号：TP393.07 **文献标识码**：A

Design and Implementation of the Cross-Platform Network Monitoring System Based on Active Nodes

XU Shaoqing,MA Biao,AN Haiying
(*Jilin Electric Power Co.,Ltd.,Changchun* 130021,*China*)

Abstract: In power enterprise,the huge amount of internal network monitoring equipment with varieties of brands and performances,makes it more and more difficult to monitor the network.In order to solve the problems of network equipment monitoring on different platforms,this paper designs a cross-platform network monitoring system based on cross platform technology,which is composed of network resource equipment,active node and monitoring information base.This system design realizes the periodic data collection based on the dynamic data acquisition algorithm of active network,and it sends the active message to the monitoring server platform in the form of active packet. It realizes the acquisition and transmission of control data by constructing active node.This system has applied in Jilin Power Co.,Ltd.at 2015.The system can monitor and manage the different network devices in power system and improve the efficiency of operation and maintenance.

Keywords:active node;data collection;active packet

1 引言(Introduction)

随着信息技术的发展和网络规模的扩大，企业内部的网络结构也日益复杂，电力企业也不例外，各类网络监控设备种类繁多，这些设备品牌、性能、操作系统各不相同，日志和告警格式也各式各样。对这些设备的网络监控难度也越来越大,网络监控已经成为现代企业信息化建设的难点。近年来，网络监控技术也从传统的集中式转变为分布式、单点代理转向多层次。这些新型监控技术的产生，为解决电力企业的网络监管问题，提供了很好的技术手段[1,2]。

本文设计基于主动节点的跨平台网络监控系统，对电力企业不同平台的网络设备进行监控，方便电力企业实现网络维护和监控。系统采用主动节点和监控平台为基础，采集各类数据。通过主动报文的形式发送给监控平台服务端，并进行展示，实现对电力企业网络设备的集中监控，提高运维效率。

2 系统的总体设计(General design)

网络监控是指对网络运行状态数据进行实时采集、分析、预测，并对网络运行状态实施控制。由于电力企业的网络系统涉及到许多不同平台基础的网络设备，为此在系统的设计过程中采用跨平台设计。根据电力企业内部的网络设备监控的具体需求，基于主动节点的跨平台网络监控系统的系统总体架构设计如图1所示。

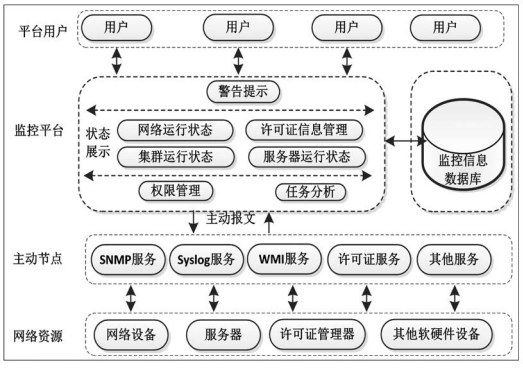


图1 跨平台网络监控系统构架图

Fig.1 Skeleton diagram of cross-platform network monitoring system

由图1可以看出，基于主动节点的跨平台网络监控系统主要由网络资源设备、主动节点、监控系统和系统使用用户四部分构成。网络资源设备包括交换机、路由器、终端监测设备、各类服务器，以及其他的软硬件设备等。主动节点是各类监控服务的载体，为SNMP、WMI、Syslog等服务提供运行基础。主动节点采用主动报文的形式与监控系统进行通信，将各类消息传送至监控系统。主动节点上的主动服务对本地的各类对象和其他节点的网络资源进行管理。监控系统根据主动节点采集的数据为用户提供网络运行状态信息、服务器运行状态信息、集群状态信息等，实现各类告警信息的提示，并为用户提供权限管理和任务分析等功能，同时将各类信息存入监控系统数据库[3]。

3 主动节点设计(Design of active nodes)

3.1 主动节点功能

主动节点是指被安装监控代理的网络设备，是网络监控系统的核心部件，具有管理非主动节点和被监控系统管理的双重身份。主动节点的所有功能都是通过节点上运行的主动代理服务实现的，包括命令的获取、数据的采集和告警的处理等[4-6]。主动代理的具体功能结构如图2所示，其包含的功能如下：

(1)获取和接收网络监控中心的各类指令，执行对网络节点的监控、异常数据采集和数据回传。

(2)根据网络监控中心的指令，实现对本地服务库的管理、配置等。

(3)接收主动报文，并对主动报文进行解析，并执行主动报文中的主动代码。

(4)依据SNMP协议，调用本地SNMP服务和WMI服务，实现对周围非主动节点和网络设备的管理。

(5)对采集的数据，根据一定的策略进行分析、过滤和压缩，消除冗余数据，降低会出数据的流量，减少监控系统的计算任务量。

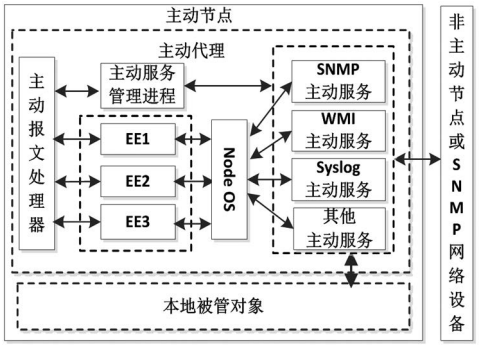


图2 主动节点结构

Fig.2 Active nodes structure

3.2 主动报文处理

当主动节点受到一个主动报文后，主动报文处理器首先对报文的类型进行判断。如果报文的类型不在主动节点处理的范围内，则这个报文就会被丢弃。如果报文能够被节点识别，则节点会根据报文类型进行相应的处理。如果接收到的是普通数据采集报文。则主动节点接收到此报文后，首先对主动报文进行安全认证，认证通过后，主动报文处理器将其发送到相应的数据采集主动环境中。主动环境依据主动报文的主动代码，完成相应主动服务的启动工作，并进行数据采集。如果接受到的报文是主动服务库管理数据报文，则主动报文处理器会将此报文发送给主动服务管理进程。主动服务管理进程根据主动报文中的主动代码管理主动服务库，实现对主动节点各类服务的动态增加、删除和修改等功能[7]。

4 主动报文的设计(Design of active packet)

在基于主动节点的跨平台网络监控系统中，主动报文负责传输节点间的主动程序和相关数据，是监控系统中数据传输的重要载体。与传统的网络数据报文相比，主动报文的特点在于主动报文中含有可以执行的主动代码。主动IP信包是主动报文的一种。本文采用主动IP信包的方式来构造主动报文。主动IP信包，在传统IP数据报文的基础上，增加了一种携带主动代码的机制，具体方法是在IP数据报文的选项域中插入主动代码。从而将传统的IP网络升级为主动网络。主动IP信包由IP头、专用头和载荷三部分组成，报文的具体结构如图3所示。

IP头			专用头				
源地址	目的地址	IP选项	版本号	类型	前地址	类型相关头	载荷

图3 主动IP信包结构

Fig.3 Active packet structure

在主动IP信报中，IP头由源地址、目的地址和IP选项三部分内容构成，IP头的内容与TCP/IP协议中的内容是一致的，从而实现与IP数据包的兼容。主动报文的核心组成部分为专用头，它由版本号、报文类型、前地址和类型等部分构成。版本号代表着IP信包的版本，类型对转发程序和相关的代码、协议等内容进行标识。报文的类型直接影响着报文其他内容的容量。前地址用于传递主动代码，为主动报文经过的上一跳的网络节点地址。报文中的载荷部分对传输层是透明的，包括着网络应用层的各类信息。主动IP信包的最大特点在于它能够对传统的IP数据包进行兼容，能够在传统的IP数据包中嵌入主动代码，这位主动网络与传统网络的兼容提供了基础。

5 数据采集方法(Data collection method)

获取网络运行状态监控的基础数据的关键就是网络运行状态数据的采集。只有获取了足够的数据，网络监控人员才能在这些基础之上对网络运行的状态进行分析、预警和进一步的控制[8]。为了实现更好的采集和传送网络监控数据，本文设计了基于主动网络的数据采集和传送方法。

5.1 基于主动网络的数据采集算法

针对网络监控系统的数据采集问题，本文设计了基于主动网络的动态数据数据采集算法，算法的流程如图4所示，算法描述如下：

第1步：假设t为主动节点的采样周期，则每间隔t秒，主动节点就会对网络设备的各种状态进行一次重新采样。

第2步：对监控系统中的每一个监控设备都设定一个固定的数据采集周期，用T表示，设备的采集周期T应不小于主动节点的采样周期t。T的值要等于节点采用周期t的平均值。主动节点每间隔T秒向监控中心上报一次网络的运行状态数据。

第3步：对有特殊性能要求的指标，设定数据监控的规则和阀值。主动节点每间隔t秒就会按照性能指标规则重新计算一次性能状态数据，如果指标数值超过阀值，则将性能数据上报至网络监控中的监控系统中。

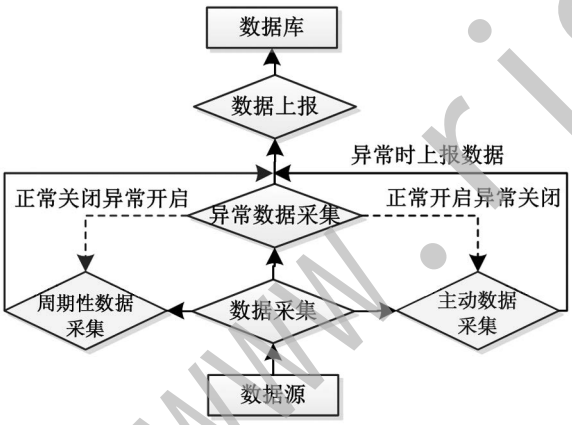


图4 基于主动网络的动态数据采集算法

Fig.4 Dynamic data acquisition algorithm of active network

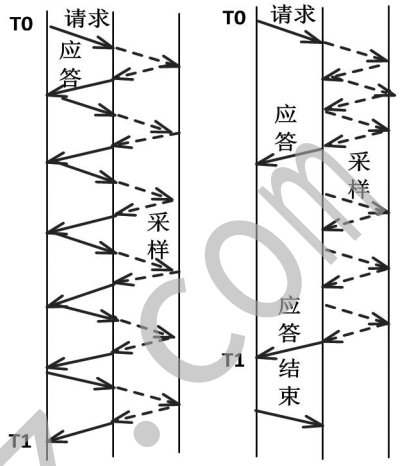
第4步：若网络运行状态的特定指标性能产生异常，则该指标性能数据的采集方式由周期性采样变为主动数据采集方式进行，并实时将性能及状态数据传送至网络监控中心。

第5步：若网络监控人员要对某一项特定的性能指标进行监控，则向节点发送主动报文，将此项指标的采集方式由周期性采集转变为主动式实时采集方式。观察完毕后，则再次发送主动报文，将数据采集方式有主动采集转变为周期性采集。

5.2 算法对比分析

本文提出的数据采集算法与传统的数据采集算法相比较，具有较强的优势。对比过程如图5所示。其中开始时间用T0表示，结束时间用T1表示。将两种算法在T1—T0的时间间隔内分别从网络流量和网络数据有效率两方面进行比较。

在数据传输过程中，数据包包括IP头、UDP头和状态数据等部分。假定每个数据包中IP头、UDP头、运行状态数据和请求数据各算一个单位的数据，则进行如图5所示对比。



(a)传统数据采集算法　(b)本文数据采集算法

图5 数据采集算法比较

Fig.5 Comparison of data acquisition algorithm

(1)网络流量分析。在T1至T0内，采用传统采集算法所消耗的网络流量为3*2*6/(T1−T0)=36/(T1−T0)，采用本文数据采集算法所消耗的网络流量为3*3/(T1−T0)=9/(T1−T0)，由此可见本文设计算法的消耗的网络流量小。

(2)网络数据有效率分析。在T1至T0内，采用传统采集算法传输的数据有效率为1*6/(3*2*6)=1/6，采用本文数据采集算法传输的数据有效率为2/(3*3)=2/9，由此可见本文设计算法在数据传输过程中，数据有效率更高。

6 结论(Conclusion)

本文以跨平台技术为基础，设计了由网络资源设备、主动节点、监控信息库构成的跨平台网络监控系统。设计了基于主动网络的周期性数据采集算法，采用主动报文的形式将信息发送给监控平台服务端，通过构造主动节点实现数据的采集和传送控制。实践证明，该系统能成功的不同平台的网络设备进行监控，提高电力系统的运维效率。

参考文献(References)

[1] Thomas R,Christel B,Martin R.Wireless Security Situation Awareness with Attack Identification Decision Support[C].2011 IEEE Symposium on Computational Intelligence in Cyber Security(CICS).Paris:IEEE,2011:144−151.

[2] XIE Li−Xia,Wang Ya−chao,YU Jin−bo.Network Security Situation Awareness Based on Neural Networks[J].

Journal Tsinghua University:Science & Technology, 2013,23(12):1750-1760.

[3] HANG Tong-qing,ZHUANG Yi.An Approach to Real-Time Network Security Situation Prediction[J].Journal of Chinese Computer System,2014,35(2):303-306.

[4] 崔杰,李陶深,兰红星.基于Hadoop的海量数据存储平台设计与开发[J].计算机研究与发展,2012,49(l):12-18.

[5] 丁琳琳,等.基于Map-Reduce的海量数据高效Skyline查询处理[J].计算机学报,2011,34(10):1786-1796.

[6] 丁治明,高需.面向物联网海量传感器采样数据管理的数据库集群系统框架[J].计算机学报,2012,35(6):1175-1190.

[7] 刘靖龙,刘颖,张思东.基于RTL8169网卡的零拷贝技术研究与实现[J].计算机技术与发展,2011,35(1):67-69.

[8] 肖光华.网络监听技术的研究与应用[D].上海:同济大学计算机科学技术学院,2006.

作者简介：

许劭庆(1974-)，男，本科，高级工程师.研究领域：软件开发.

马 彪(1962-)，男，本科，高级工程师.研究领域：计算机网络.

安英海(1976-)，男，本科，高级工程师.研究领域：软件开发.

(上接第56页)

image file后使用win32DiskImager.exe来把Linux image刻录到SD内，在开发板上电后，打开putty.exe,当系统boot起来后输入root并按下enter就可以登入系统。

(2)在DE1-SoC开发板上实现ARM/HPS到FPGA的通信。首先我们需要先搭建一个Qsys硬件系统；然后需要写一个完成相应功能的C语言代码(主要是结合开发板完成地址的映射和寄存器配置及功能实现)，我们主要是写了一个可控制小车左转、右转，以及前进后退的控制程序；其次是创建Makefile文件，制定编译工程的一系列规则(可根据案例把文件名和地址改为自己的文件名和地址即可)；最后打开embedded文件中的Embedded_Command_Shell.bat,输入cd切换路径，然后输入自己的文件位置，输入make即可在原文件中生成一个空白文档形式的可执行文件。打开Putty.exe就可以，用u盘把生成的可执行文件拷入优盘，然后把开发板上电，输入相应的命令把此文件存入Linux路径下的root即可。然后在Quartus中下载FPGA硬件sof文件，最后在串口终端输入“./+生成的文件名即可”。我们主要用ARM控制FPGA的GPIO口。

(3)在DE1-SoC开发板上提供了一块视频解码芯片ADV7180,此块解码芯片是基于I2C总线协议的传输。当外置摄像头扫描到物体时首先会生成YCbCr格式的图像，然后存入SDRAM,接着Ycbcr格式通过解码生成RGB格式，通过VGA接口在显示屏上显示图像。

(4)在DE1-SoC开发板上提供了一块24位的音频解码芯片WM8731,此块解码芯片是基于I2C总线协议的传输。通过锁相环分频后，控制声音模块，将固定乐曲的音调用MIF Maker生成MIF文件存入ROM中，在数码管上显示乐谱，通过外置蓝牙音箱进行声音放大。

(5)硬件小车模块主要是通过L298模块来驱动直流电机控制小车模块的移动，通过FPGA端口的GPIO口的控制信号来给小车移动的相应信号。电源主要采用电池给开发板供电，然后通过降压后又给电机以及相应模块供电。

参考文献(References)

[1] Lazaro J L,Garci J C,Mazo M.Distributed Architecture for Control and Path Planning of Autonomous Vehicles,2001(03):112-116.

[2] Liu Wanli,Wang Zhankui,Zhu Hua.Novel Method of Trajectory Tracking and Posture Stabilization for Mobile Robot[S.I.].IEEE Press,2010.

[3] Regional objects based image retrieval[A].Proceedings of the 2011 Chinese Control and Decision Conference(CCDC),2011.

[4] 何燚,张翼飞.基于双目视觉的移动机器人避障算法仿真研究[J].计算机仿真,2013(02):21-24.

[5] 汪明磊.智能车辆自主导航中避障路径规划与跟踪控制研究[D].合肥工业大学,2013.

[6] 武丽.基于图像传感器的黑线提取及抗干扰算法研究[J].电子技术应用,2012(02):11-13.

[7] 崔瑾娟.移动机器人路径规划技术现状与展望[J].安阳师范学院学报,2013(02):11-15.

[8] 胡永仕,张阳.基于遗传模糊算法的智能车辆避障路径规划研究[J].福州大学学报(自然科学版),2015(02):16-20.

[9] 阮晓芳.多路超声波机器人的模糊避障研究[J].计算机测量与控制,2012(12):51-53.

[10] 友晶科技.Altera DE1-SoC培训教材[M].友晶科技,2002.

[11] 毛星云,冷雪飞.OpenCV3编程入门[M].电子工业出版社,2015.

[12] 张茜.智能车辆的轨迹跟踪控制方法研究[D].哈尔滨工业大学,2015.

作者简介：

陈亮亮(1982-)，女，硕士，讲师.研究领域：信息处理，微电子技术应用.

刘玉莹(1972-)，女，硕士，副教授.研究领域：信息处理.

詹 春(1975-)，女，硕士，副教授.研究领域：信息处理.