DOI: 10.19783/j.cnki.pspc.181031

调度数据网厂站侧网络监测装置设计

王豫宁[1]，魏 霞[1]，刘 波[2]，田易之[1]

(1.新疆大学电气工程学院，新疆 乌鲁木齐 830047；2.乌鲁木齐职业大学，新疆 乌鲁木齐 830002)

摘要：为提高调度数据网接入层厂站对网络故障和异常行为的自我判断能力，提出了一种网络监测装置的设计方案。方案基于镜像数据监听技术，采用 Ping 程序检测厂站内各联网设备的数据链路通断状态，使用开源 Linux 数据包捕获工具 Tcpdump 作为监听实现途径，并制定了多端点监听下基于非剥夺式的静态优先级调度算法的任务调度机制。通过分析监测结果中的源 IP 地址、目标 IP 地址、通信时间和传输数据量，判断网络内是否存在非法通信操作、数据传输隧道断开和 DoS 攻击等异常行为。测试结果表明，装置的设计方案是可靠且有效的，能够对网络故障和异常行为作出较为准确的判断，有助于增强厂站对自身网络运行状态信息的识别与掌控能力。

关键词：电力调度数据网；厂站；安全监测；网络流量；旁路监听

Design of network monitoring device for power dispatching data network at power station

WANG Yuning[1], WEI Xia[1], LIU Bo[2], TIAN Yizhi[1]

(1. College of Electrical Engineering, Xinjiang University, Urumqi 830047, China;
2. Urumqi Vocational University, Urumqi 830002, China)

Abstract: A network monitoring device is designed to improve the ability of the power station, which belongs to the access layer of power dispatching data network, to make accurate self-judgements on network faults and abnormal behaviors. Based on mirrored data monitoring technique, the device uses Ping to detect the data link on-off state of other connect-to-network devices and Tcpdump to capture data packages. In addition, a task scheduler for multiple endpoints monitoring based on non-deprivation static scheduling is designed. With the monitoring results of source and destination IP addresses, communication time and amount of transported data, the monitoring device can make judgements on the existing of abnormal situations such as illegal communication, data channel interruption and DoS attack. Testing results have verified that the device is reliable and effective, and can make accurate judgements on network faults and abnormal behaviors, which helps to enhance the ability of the power station to identify and control the working condition of its own network.

This work is supported by Natural Science Foundation of Xinjiang Uygur Autonomous Region (No. 2017D01C030). "Single-phase Fault Monitoring and Diagnosis Location for Low-voltage Distribution Network based on Big Data"

Key words: power dispatching data network; power station; safety monitoring; network traffic; bypass monitoring

0 引言

随着信息以及网络技术的迅速发展和广泛应用，信息安全形势愈发严峻，电力行业对信息安全问题的重视程度也日益提高，越来越多的网络安防技术开始在电力系统中得到应用。

近年来，国家电网公司逐步加大对电力二次系统安全防护措施的建设投入力度，并对智能电网调度控制系统中存在的安全隐患进行集中检查和整改[1-4]，重点加强调度数据网接入层厂站掌控网络运行状态，抵御黑客及恶意代码攻击侵害的能力。鉴于目前接入层厂站尚不具备对其自身调度数据网络的运行状态进行监测的功能，需要设计开发一类专用设备来满足这一功能需求。

文献[5-6]中所描述的基于简单网络管理协议(Simple Network ManagementProtocol, SNMP)的网络监测方法在传统商用以太网当中应用广泛，通过

基金项目：新疆维吾尔自治区自然科学基金项目(2017D01C030)“基于大数据的低压配网单相故障监测与诊断定位”

SNMP 服务的数据流量统计功能监测小型局域网运行状况的理念，源自网络数据流量能够反映网络行为状态特征的以太网监测理论。然而，尽管目前调度数据网中绝大部分的网络设备能够提供 SNMP 服务，基于此项技术的网络监测方法也不宜推广使用。根本原因在于目前主流的 SNMP 版本的安全机制过于薄弱，仅通过设置用户权限口令来阻挡非法操作。设备开启 SNMP 服务后，其他运行状态参数同样可以被监视和修改。一旦权限口令被非法窃取，则口令拥有者可以任意地对设备进行读写操作，更改设备状态，从而使调度业务无法正常有序地进行[7]。因此，在实际的电力调度现场中，除非特别必要，SNMP 服务均处于禁用状态。

文献[8]中研究了基于 Netflow 技术的网络监测方法，该方法同样关注网络数据流量。Netflow 特有的数据流输出格式在监测大型企业级局域网或城域网时优势明显。然而，接入层厂站侧的调度数据网通常规模较小，数据流量较低，应用 Netflow 技术不仅很难体现其优势，还需额外配置能够支持该技术的昂贵监测设备。因而从经济角度考虑不宜采用 Netflow 技术进行厂站侧的网络状态监测。

本文在分析调度厂站的局域网故障与异常行为种类和特征的基础上，提出了一种较为经济可行的基于旁路监听技术的网络安全监测装置设计方案。测试证明该装置能够稳定运行并对调度数据网厂站侧常见的链路故障和数据量异常等情形作出较为准确的判断，有助于增强厂站对网络运行状态的掌控能力。

1 工程应用需求分析

在 220 kV 省调直调厂站内，由调度终端节点采集到的调度数据依次经历安全大区交换机、纵向加密网关认证装置和路由器等网络设备，最终通过光传输线路送至调度主站[9-10]。根据调度控制系统数据传输规范，不同类型的调度业务数据的流向应当是确定的，即包含了调度信息的数据报文的发送源地址和接收目的地址都应当是合法且对应的调度终端或主站前置机的 IP 地址[11-12]。而非法的通信行为必定会产生包含非法 IP 地址的数据报文，这类报文的检测对于厂站排查非法通信异常具有重要的参考价值。

通信数据量也是一个重要的网络异常判断指标，正常调度过程中产生的数据量应当稳定在某一范围内，而网络异常状况往往也能通过流量的变化得到反映[13]。例如目前常见的资源消耗型 DoS 网络攻击通常采取持续不断地向主站 SCADA 服务器或数据中心发送无用的大体积数据包的做法，引起短时间内数据量的急剧升高[14]；若某条数据传输隧道发生故障，则该条链路上的数据量会迅速降至一个极低的数值甚至归零[15]。因此厂站需要通过监测数据量来初步判断是否发生网络异常。

通过以上分析，将解决的问题归纳为：获取厂站侧调度数据网各节点的流量信息，并根据异常流量的特征判断是否有网络故障或异常行为的发生。

2 基于旁路监听的监测方法

2.1 监测装置总体设计

监测装置的模块结构与安装位置见图 1，参考了传统商用以太网流量监测领域中基于旁路监听的局域网监测方法，由数据链路状态检测模块、数据帧监听模块和监听结果分析模块组成。

监测装置通过普通网线与交换机直接相连。数据链路状态检测模块负责检查厂站内各网络设备的数据链路的通断情况，数据帧监听模块负责监听目标设备的镜像数据，监听结果分析负责统计相关信息，作出对网络运行状态的判断。

监测装置使用基于 BCM2837 微处理器的嵌入式硬件平台，以专门针对 ARMv7 及其以上芯片架构设计开发的基于 Linux 4.4.38 内核的 Ubuntu MATE 16.04.2(Xenial)为操作系统，编程语言为 C 语言。

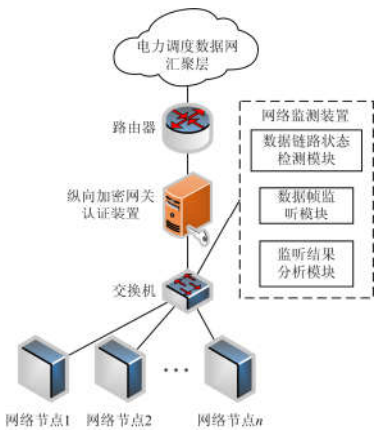


图 1 网络监测装置架构及安装位置

Fig. 1 Structure of network monitoring device and its installation location

2.2 相关网络技术支持

2.2.1 端口镜像技术

目前，厂站侧配置的主流交换机支持端口镜像技术，这项技术能够将流经交换机的镜像源端口的数据帧全部复制并转发至本机的镜像目的端口。其他监听设备连接至该镜像目的端口后便能够获取所

有被复制的数据帧[16]。

在调度数据网中应用端口镜像技术的优势在于数据帧的复制与转发过程均由交换机的内部处理程序完成，不占用任何网络带宽，不会影响调度业务数据帧的正常转发[17-18]；而考虑到厂站交换机的实际数据处理能力，开启端口镜像功能后产生的额外数据处理负荷对这些设备性能造成的负面影响仍在可以接受的范围内。因此，可以利用端口镜像技术，选取合适的监听手段获取数据帧内部的相关信息，并通过分析这些信息最终得到各网络节点的流量状况。

2.2.2 Tcpdump 数据帧监听技术

Tcpdump 是 Linux 环境下一款非常经典的开源网络数据采集分析工具。该程序能够抓取并解析流经指定网络接口上的数据帧，用户可以根据自身需求指定程序的输出格式和内容，进而仅浏览数据帧中的关键信息。图 2 展示了调度数据网中的标准数据帧格式。

IEEE 802.3 首部	IP 首部	TCP 首部	104规约报文	CRC校验

图 2　104 规约报文在以太网数据帧中的封装格式

Fig. 2 Encapsulation format of IEC104 in Ethernet frame

IEC60870-5-104 传输规约是电网调度自动化系统中使用的标准以太网调度通信协议，属于应用层协议[19]。由于 Tcpdump 仅能解析基本的传输层、网络层和数据链路层协议[20]，因此无法仅通过该工具知晓即使处于明文状态的具体调度业务信息。然而，一些包含在 IP 首部中且对流量统计至关重要的信息仍然可以通过这一工具获取。

2. 3 监测程序模块设计

在端口镜像技术和数据帧监听技术的支持下，实现对网络数据流量的监测便成为可能。开启交换机的端口镜像功能，监测装置在连接至交换机的镜像目的端口后便能够等效地监听镜像源端口的所有数据，通过对监听内容的分析便可统计出流量信息。

根据上述的监测方法，将监测程序按照数据链路状态检测模块、数据帧监听模块和监听结果分析模块三个部分分别进行设计。

2.3.1 数据链路状态检测模块

任何一个具有价值的流量监测结果的产生前提是数据传输链路能够正常地工作。因此，在开始流量监测前，需要对厂站内的调度终端、交换机、纵向加密网关认证装置、路由器和光传输设备的数据链路通断状态进行检测，只有在这些设备的数据链路都保持畅通时才进行下一步的监听操作。

检测的方法是利用网络诊断工具 Ping 程序，当上述被测设备均能够正常地 Ping 通且没有发生数据包丢失时，认为该设备的数据链路畅通，否则产生数据链路故障告警[21]。

Ping 程序的原理和使用方法都较为简单，在此不作赘述。

2.3.2 端点状态描述机制

由于“节点”这一术语通常用于网络拓扑结构研究，以下在论述与数据帧监听和分析相关的研究内容时使用 TCP 术语“端点”一词替代“节点”。

为方便其余模块的设计，参考 Moore 状态机的运行过程进行如下定义[22]：

(1) 每一个被监测端点都具有三个状态：监听就绪态、正在监听态以及结果分析态。

监听就绪态表明该端点最近一次的监听结果已经被分析统计完毕，可以进行下一次监听；

正在监听态表明该端点正在被监听；

结果分析态表明该端点最近一次的监听已经完成，生成的监听结果尚未被分析统计完毕。

三种状态之间的迁移如图 3 所示。

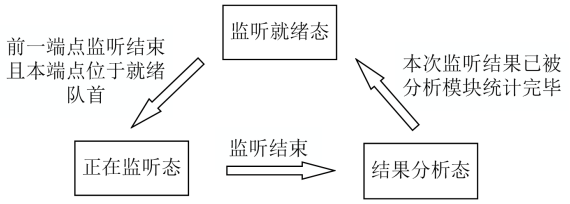


图 3　端点状态迁移示意

Fig. 3 Transfer of endpoint state

(2) 就绪队列与后备队列

为管理处于不同状态的端点，保证监测有序进行，设置两个数据存储结构：就绪队列与后备队列。

就绪队列仅存储处于监听就绪态的端点，后备队列可存储监听就绪态和监听完毕态的端点。

2.3.3 数据帧监听模块

数据帧监听模块(以下简称监听模块)的主要功能就是生成每个端点的监听结果，为监听结果分析模块(以下简称分析模块)提供数据来源。

考虑到本次设计的监测装置对实时性要求并不苛刻，为降低监听任务执行时的复杂程度，监听程序每次运行时仅对一个端点进行监听。具体流程见图 4。

每个端点被监听的内容如下：

(1) 该端点发送的所有数据的目的端点地址、发送时间和数据量；

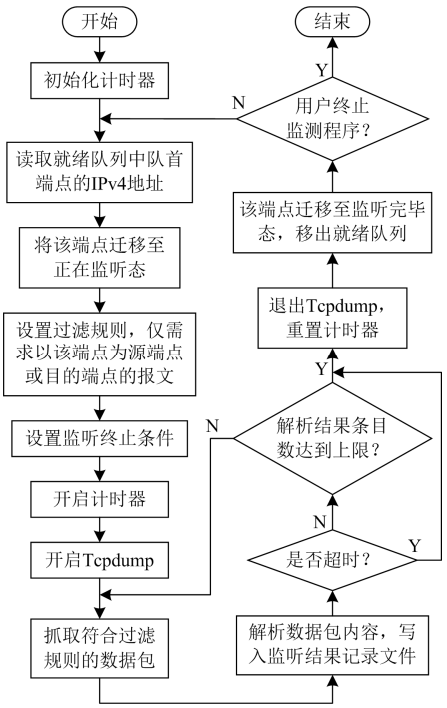


图 4 监听流程图

Fig. 4 Flowchart of monitor progress

(2) 该端点接收的所有数据的源端点地址、接收时间和数据量。

由于调度数据网实质上就是调度信息在不同调度部门间进行交互的平台，而信息的交互又是以数据在不同的端点间进行传输为体现。因此监听以上信息足够支撑对当前调度数据网的活动行为做出判断。

考虑到监听程序需要抓取到数量足够多的数据包才能使得解析出的数据具有可分析统计的价值，因而在设置监听终止条件时，首先需要考虑设置数量终止条件，当解析结果的条目数量超过限定值时终止监听。

然而，若被监听端点的数据吞吐量过低，则达到数量监听条件所需的时间有可能过于漫长，因此还需要设置优先级更高的时间终止条件，在监听超时后立刻结束监听。

本模块中有关端点状态的部分代码如下：

```
switch(endpoint_state){
  case monitor_rdy:
    if (act == tcpdump_on) {
      endpoint_state = monitoring;…… }
  case monitoring:
    if (act == tcpdump_off) {
      endpoint_state = monitor_over;…… } }
```

2.3.4 监听结果分析模块

分析模块的主要功能是通过分析监听模块生成的监听内容，获取被监听端点的数据流向以及吞吐量，进而判断调度数据网内有无非法访问或可能导致数据异常的网络行为。

图 5 展示了分析模块的工作流程。

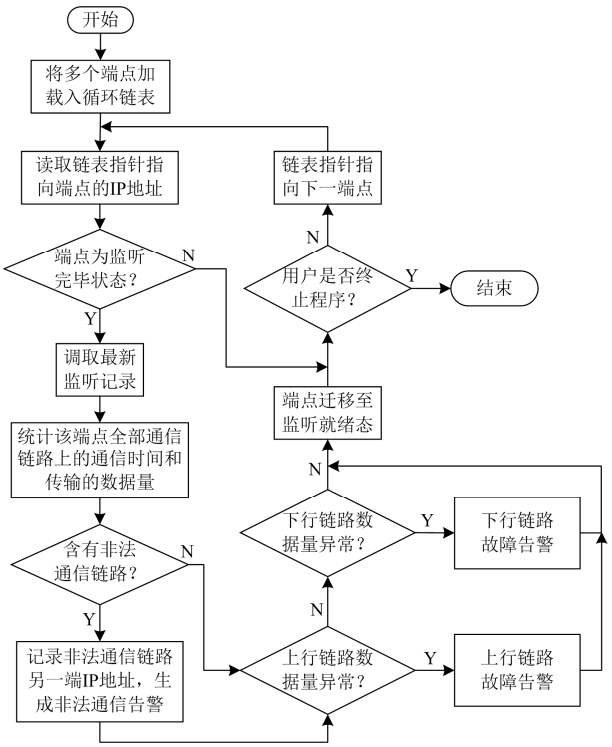


图 5 轮询分析流程图

Fig. 5 Flowchart of polling analysis

分析模块在调取到某个处于监听完毕状态下的端点最新的监听结果后，统计其中的数据链路建立情况，归类所有与被监测端点有过数据交互的 IP 地址、通信时间以及传输的数据量。随后判断这些 IP 地址是否在被测端点被允许访问的范围内，若不在这一范围内则被视为非法通信，产生告警信息。

对于合法的数据链路，按照上行与下行方向检查其传输的数据量是否存在异常，数据量过高或过低都会触发故障告警，通知用户对链路所经历的其他网络设备进行检查，是否存在影响调度数据正常传输的故障。

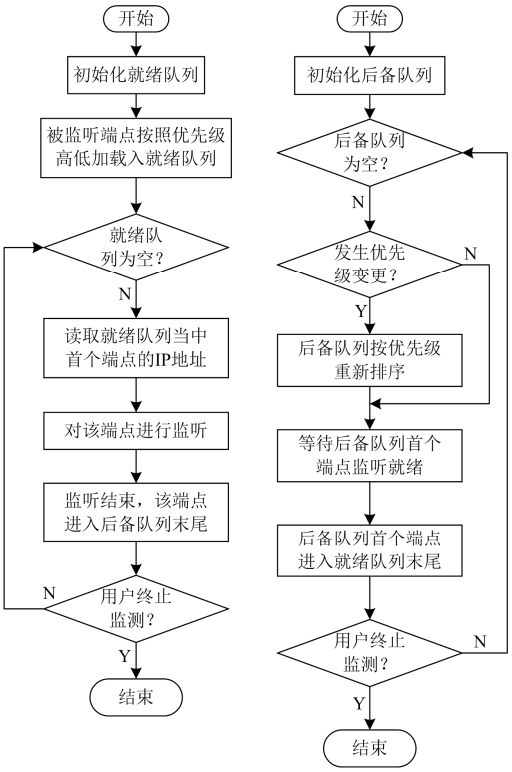
分析模块中有关端点状态的部分代码如下：

```
switch(endpoint_state){
  case monitor_over:
    if (act == analysis_done) {
      endpoint_state = monitor_rdy;
…… }
```

2.3.5 任务调度策略设计

在实际现场中，交换机与多个调度终端相连，而每个调度终端所传输的业务数据对于传输时延或数据完整性的要求并不完全相同，因而可以制定出各个端点的监听优先级，按照非剥夺式的静态优先级调度算法对不同端点的监听进行任务调度[23-25]。

任务调度流程如图 6 所示。



(a) 就绪队列运行流程　(b) 后备队列运行流程

图 6 监听任务调度流程

Fig. 6 Flowchart of monitoring task dispatching

正常状态下，监听程序在监听开始前先将各端点的 IP 地址按照其监听优先级由高至低进行排序，并将排序后的地址依次加载至就绪队列。随后监听程序读取就绪队列中的首个端点的 IP 地址对其进行监听。监听结束后，将该端点的状态变为结果分析态并转入后备队列末尾，监听程序继续读取就绪队列中的下一个端点开始监听。

结果分析态的端点在后备队列当中等待其上一次监听结果接受分析模块的分析统计，完毕后重新转为监听就绪状态等待进入就绪队列。

当某个端点的监听正在进行时，若后备队列中其他端点的监听优先级发生了变更，则对后备队列中的所有端点按照优先级重新进行排序。重新排序后优先级最高的端点在变为监听就绪态后进入就绪队列的末尾。

由于监听结果分析的持续时间基本固定，不随端点监听优先级的变更而发生明显变化，而且远远低于监听过程通常所消耗的时间。因此监听结果分析可以按照常规轮询的方式进行调度，仅检测处于结果分析态的端点并在其监听结果分析完毕后将其迁移至监听就绪态。

3 装置性能测试及结论

监测装置的最终设计目的是使厂站能够掌握调度数据网的运行状态，增强其网络异常自诊能力。因此，测试监测装置的性能时，人为设置一些厂站中常见的故障或异常状况，并重点关注监测装置能否对这些状况作出准确的判断。

在调度子站中，仿照正常的调度数据网厂站侧拓扑结构临时搭建测试专用网络，内含若干个测试用调度终端。通过配置交换机、纵向加密装置以及路由器的相关参数，建立各测试终端与主站前置机 10.53.1.61 之间的数据传输链路，确认双方通信正常后开始进行测试。

首先测试监测装置的数据链路通断状态检测功能。关闭调度终端 53.121.20.13 与 53.121. 20.13 的网络端口访问权限，并限制路由器的数据转发功能，模拟调度终端和光传输数据链路故障情形。测试结果见表 1。

表 1 数据链路状态检测结果

Table 1 Detection result of data link state

IPv4 地址	代表设备	检测结果
53.121.20.13	网络节点 1	数据包完全丢失
53.121.20.18	网络节点 2	数据包完全丢失
53.121.20.3	交换机	网络正常
53.121.20.41	纵向加密网关	网络正常
53.121.60.1	路由器	网络正常
10.53.1.61	调度主站前置机	数据包完全丢失

无论是拒绝访问还是限制转发，由 Ping 命令发出的数据包都无法越过故障点，故而返回“数据包完全丢失”的回显内容。

通过参考监测装置对各设备数据链路通断状态的判断结果，结合调度数据网厂站侧的拓扑结构，可以得出数据链路中断故障的诊断结论(见表 2)。

其次测试流量监测功能。同数据链路通断检测一样，流量监测仅是实现监测装置最终设计目的的手段，因而测试时仍需关注监测装置能否对网络异常状况作出相应的警示，具体流量数值是否精确并不影响对网络状态作出肯定的判断。

对处于正常工作状态的测试终端节点进行如下异常状态设置。

(1) 节点 53.121.20.13 不做任何处理，使其正常工作，作为其他节点的对照组。

(2) 关闭纵向加密网关认证装置中与节点 53.121.20.18 相关的数据传输隧道。

(3) 仿照常见的 DoS 攻击行径，通过节点 53.121.20.21 向主站额外发送大量无用数据。

(4) 节点 53.121.20.22 向主站前置系统中另一个不允许被其访问的前置机地址发送数据。

表 3 记录了流量监测功能的测试结果。

节点 53.121.20.18 的数据传输隧道被关闭后，来自调度主站的信息无法到达交换机。监测装置也就无法监听到任何由主站发送给节点 53.121.20.18 的数据帧，进而根据过低的数据量作出“上行链路数据量过低”的告警信息。

表 2 常见的数据链路检测结果及故障诊断结论

Table 2 Common detection result of datalink and error causes

各网络设备的数据链路状态监测结果					故障原因
网络节点	交换机	纵向加密网关	路由器	调度主站前置机	
网络正常	网络正常	网络正常	网络正常	数据包完全丢失	光传输或主站前置机故障
数据包完全丢失	网络正常	—	—	—	调度终端故障
—	数据包完全丢失	—	—	—	交换机故障
—	网络正常	数据包完全丢失	—	—	纵向加密网关故障
—	网络正常	网络正常	数据包完全丢失	—	路由器故障

注：表 2 中的“—”表示该项检测结果不影响故障诊断结论。

表 3 流量监测测试结果及告警信息

Table 3 Test result of network traffic monitoring and warning information

源 IP 地址	目的 IP 地址	通信起止时间	单向通信时长/s	应用层协议载荷数据量/Byte	告警信息的内容
53.121.20.13	10.53.1.61	22:07:13-22:10:55	202	1 692	无告警
10.53.1.61	53.121.20.13	22:07:11-22:10:54	203	715	
53.121.20.18	10.53.1.61	22:10:15-22:15:14	299	320	上行链路数据量过低
10.53.1.61	53.121.20.18	—	—	—	
53.121.20.21	10.53.1.61	22:15:15-22:16:05	50	71 643	下行链路数据量过高
10.53.1.61	53.121.20.21	22:15:16-22:16:05	49	144	
53.121.20.22	10.53.2.32	22:18:27-22:23:26	299	163	非法通信行为

注：1) 表 3 中“—”表示监测装置无法获取该项的有效数据。

2) 在调度厂站内，上行链路指自交换机至调度主站间的数据链路，下行链路指自调度终端节点至交换机间的数据链路。

节点 53.121.20.21 向主站发送了大量的无用数据，而主站仅对有效的调度数据进行回应，故而造成监听程序抓取到的数据包数量在较短的时间内便达到限定值。经过分析，监测装置判定下行链路的数据量过大，发出“下行链路数据量过高”的告警信息。

节点 53.121.20.22 尝试向不被允许访问的地址发送数据后被监测装置发现，并作出“非法通信行为”的告警。

通过测试可以看到，监测装置对所设置的网络异常状态均作出了较为准确的判断，说明基于旁路监听的流量监测方法是有效的且可靠的，其监测的结果能够反映出网络中存在的某些异常状态。然而，目前调度数据网中存在着多种因素能够造成链路数据量过高或过低。例如针对厂站的路由协议攻击能够过滤由主站发往特定调度终端的数据，从而触发上行链路数据量过低告警。由于本文在设计监测装置时并未对这些因素进行细致区分，因此告警信息仅局限于数据量的高低表征。若要进一步探明导致流量异常的原因，则需要监听数据流的网络端口号，通过分析不同端口号中流过的数据量大小来确定网络中是否存在非法攻击等行为。

以上的测试结果表明，监测装置能够对厂站侧调度数据网当中所发生的链路故障、数据量异常和非法通信等状况作出较为准确的判断，厂站可以参考监测装置提供的信息对调度数据网的运行状态有一个基本准确的了解。在实际的网络故障或异常行为发生时，厂站通过来自调度主站的告警信息并结合监测装置的诊断结论，可以更好更快地做出反应，恢复电力调度业务的正常进行，这也符合了监测装置设计开发的最终目的。

4 结语

本次调度数据网厂站侧网络监测装置的设计，

主要通过监测网络流量的方法，分析判断调度数据网运行状态并告知厂站，从而达到提高厂站对调度数据网运行状态相关信息的掌握程度，特别是增强对网络故障的诊断能力和网络异常行为的识别能力的最终目的，进一步保障了调度数据网的安全运行。

监测装置的设计方案中也存在着不少局限性，例如其监听任务的调度优先级的确定以及链路通行数据量高低阈值的设置都依赖于人的经验判断，并且需要设计相关措施保证监听过程的数据安全性等，这些问题都有待在后续的改进中解决。鉴于目前调度数据网厂站侧的网络监测手段还比较少，因此该装置具有良好的开发应用前景。

参考文献

[1] 孙大雁, 许祖锋, 苏大威, 等. 基于调度与变电站一体化系统的分布式故障诊断[J]. 电力系统自动化, 2016, 40(23): 125-130.
SUN Dayan, XU Zufeng, SU Dawei, et al. Dis-tributed fault diagnosis based on dispatch and substation integrated system[J]. Automation of Electric Power Systems, 2016, 40(23): 125-130.

[2] 高昆仑, 辛耀中, 李钊, 等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化, 2015, 39(1): 48-52.
GAO Kunlun, XIN Yaozhong, LI Zhao, et al. Development and process of cyber security protec-tion architecture for smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 48-52.

[3] 任晓辉. 电网调控自动化系统运行状态在线监视与智能诊断研究及应用[J]. 电力系统保护与控制, 2018, 46(11): 156-161.
REN Xiaohui. Research and application of operating states of grid dispatching and control system[J]. Power System Protection and Control, 2018, 46(11): 156-161.

[4] 徐彪, 尹项根, 张哲, 等. 电网故障诊断的分阶段解析模型[J]. 电工技术学报, 2018, 33(17): 4113-4122.
XU Biao, YIN Xianggen, ZHANG Zhe, et al. A staged analytical model for power system fault diagnosis[J]. Transactions of China Electrotechnical Society, 2018, 33(17): 4113-4122.

[5] 李澄, 陆玉军, 王宁, 等. 智能变电站远程虚拟终端访问系统设计与实现[J]. 电测与仪表, 2016, 53(13): 123-128.
LI Cheng, LU Yujun, WANG Ning, et al. Design and implementation of a remote access system of virtual terminal for the smart substation[J]. Electrical Measurement & Instrumentation, 2016, 53(13): 123-128.

[6] 杨花卫, 王云山, 王立强. SNMP 在机载网络化测试系统中的应用[J]. 测控技术, 2014, 33(4): 98-101.
YANG Huawei, WANG Yunshan, WANG Liqiang. Application of SNMP in airborne networked test system[J]. Measurement & Control Technology, 2014, 33(4): 98-101.

[7] 杨芳南, 刘春. 基于 SNMP 的应用进程监控系统研究与实现[J]. 北京交通大学学报, 2016, 40(5): 35-39.
YANG Fangnan, LIU Chun. Research and imple-mentation of application process monitoring based on SNMP[J]. Journal of Beijing Jiaotong University, 2016, 40(5): 35-39.

[8] 丁圣勇, 闵世武, 樊勇兵. 基于 Spark 平台的 NetFlow 流量分析系统[J]. 电信科学, 2014, 10(5): 48-51.
DING Shengyong, MIN Shiwu, FAN Yongbing. A large scale Netflow analysis system based on Spark[J]. Telecommunications Science, 2014, 10(5): 48-51.

[9] 周雅. 智能化电力调度数据专网建设方案研究[J]. 电力系统保护与控制, 2015, 43(6): 133-137.
ZHOU Ya. Analysis on intelligent construction scheme for power dispatching data network[J]. Power System Protection and Control, 2015, 43(6): 133-137.

[10] 彭志强, 张琦兵. 电网调度自动化系统信息品质分析新方法及其应用[J]. 电力系统保护与控制, 2018, 46(4): 150-157.
PENG Zhiqiang, ZHANG Qibing. A new method of information quality analysis of power grid dispatching automation system and its application[J]. Power System Protection and Control, 2018, 46(4): 150-157.

[11] 樊陈, 倪益民, 窦仁晖, 等. 智能变电站一体化监控系统有关规范解读[J]. 电力系统自动化, 2012, 36(19): 1-5.
FAN Chen, NI Yimin, DOU Renhui, et al. Inter-pretation of relevant specifications of integrated supervision and control systems in smart substa-tions[J]. Automation of Electric Power Systems, 2012, 36(19): 1-5.

[12] BO Zhiqian, LIN Xiangning, WANG Qingping, et al. Developments of power system protection and control[J]. Protection and Control of Modern Power Systems, 2016, 1(1): 1-8. DOI: 10.1186/s41601-016-0012-2.

[13] 李芹, 卢长燕, 霍雪松, 等. 电力调度数据网测试模型[J]. 电力系统自动化, 2015, 39(1): 187-193.
LI Qin, LU Changyan, HUO Xuesong, et al. Test models of electric power dispatching data network[J]. Automation of Electric Power Systems, 2015, 39(1): 187-193.

[14] RETINA J, ELIZABETH N E. Network's server monitoring and analysis using Nagios[C] // 2017 International Conference on Wireless Communications, March 22-24, 2017, Chennai, India: 1904-1909.

[15] 宁剑. 电力调度自动化运行管理规程修订解读[J]. 中国电力, 2017, 50(11): 54-58.

NING Jian. Revision interpretation of code for operation and administration of power dispatching automation system[J]. Electric Power, 2017, 50(11): 54-58.

[16] 刘鹏, 盛万兴, 吕广宪, 等. 基于旁路技术的 IEC 61968 消息监管及交互测试方案[J]. 电力系统自动化, 2018, 42(6): 92-97.
LIU Peng, SHENG Wanxing, LÜ Guangxian, et al. Bypass technology based solution to message supervision and exchange test of IEC 61968[J]. Automation of Electric Power Systems, 2018, 42(6): 92-97.

[17] 潘竹虹, 许卓斌. 信息采集网络支撑系统的设计与实现[J]. 厦门大学学报(自然科学版), 2016, 55(3): 426-433.
PAN Zhuhong, XU Zhuobin. Design and implementation of network supporting system for information acquisition[J]. Journal of Xiamen University (Natural Science), 2016, 55(3): 426-433.

[18] 王政军, 董晓梅, 俞小怡. 基于旁路监听的数字资源评估系统的设计与实现[J]. 图书情报工作, 2015, 59(9): 52-57.
WANG Zhengjun, DONG Xiaomei, YU Xiaoyi. An availability perception study of library resources and mechanism analysis[J]. Library and Information Service, 2015, 59(9): 52-57.

[19] 徐洪伟, 李伟, 叶海明, 等. 基于信息流监测与解析的遥控缺陷诊断技术应用[J]. 电力系统保护与控制, 2017, 45(23): 136-142.
XU Hongwei, LI Wei, YE Haiming, et al. Application of remote control defect diagnosis technology based on information flow monitoring and analysis[J]. Power System Protection and Control, 2017, 45(23): 136-142.

[20] 赵宁, 谢淑翠. 基于 dpdk 的高效数据包捕获技术分析与应用[J]. 计算机工程与科学, 2016, 38(11): 2209-2215.
ZHAO Ning, XIE Shucui. Analysis and application of the high performance data packet capture technology based on dpdk[J]. Computer Engineering & Science, 2016, 38(11): 2209-2215.

[21] FALL K, STEVENS W R. TCP/IP 详解卷 1: 协议[M]. 吴英, 张玉, 许昱玮, 译. 北京: 机械工业出版社, 2016.
FALL K, STEVENS W R. TCP/IP illustrated: vol 1 the protocols[M]. WU Ying, ZHANG Yu, XU Yuwei, trans. Beijing: China Machine Press, 2016.

[22] 李国柱, 马波, 张君华. 有限状态机在一键式测量系统中的应用[J]. 测绘通报, 2016(2): 120-122.
LI Guozhu, MA Bo, ZHANG Junhua. Design and implementation of one-click surveying system based on finite state machine[J]. Bulletin of Surveying and Mapping, 2016(2): 120-122.

[23] 李静梅, 王雪, 吴艳霞. 一种改进的优先级列表任务调度算法[J]. 计算机科学, 2014, 41(5): 20-23.
LI Jingmei, WANG Xue, WU Yanxia. Improved priority list task scheduling algorithm[J]. Computer Science, 2014, 41(5): 20-23.

[24] 徐久强, 张鹏宇, 张佳观, 等. 基于变采样周期的 CPS 多重优先级调度研究[J]. 电工技术学报, 2017, 32(5): 193-199.
XU Jiuqiang, ZHANG Pengyu, ZHANG Jiaguan, et al. Research on cyber-physical systems multiple priority scheduling based on a variable sampling period[J]. Transactions of China Electrotechnical Society, 2017, 32(5): 193-199.

[25] 张晓雪, 牛焕娜, 赵静翔. 含微电网的配电网优化调度[J]. 电工技术学报, 2017, 32(7): 165-173.
ZHANG Xiaoxue, NIU Huanna, ZHAO Jingxiang. Optimal dispatch method of distribution network with microgrid[J]. Transactions of China Electrotechnical Society, 2017, 32(7): 165-173.

收稿日期：2018-03-31； 修回日期：2018-08-25

作者简介：

王豫宁(1992—)，男，通信作者，硕士研究生，主要研究方向为以太网数据检测与采集研究； E-mail: zdh20112102209@163.com

魏 霞(1977—)，女，硕士，副教授，主要研究方向为现场总线、工业以太网技术的开发及应用； E-mail: 30462111@qq.com

刘 波(1977—)，男，硕士，讲师，主要研究方向为火力发电厂调度自动化系统维护。E-mail: 974525189@qq.com

(编辑 张爱琴)