引用格式：贺振华, 李锡瑞, 蒋超. 网络嗅探技术在时频诊断中的应用[J]. 时间频率学报, 2021, 44(2): 113-119.

# 网络嗅探技术在时频诊断中的应用

贺振华[1]，李锡瑞[2]，蒋超[1]

（1. 61920部队，成都 610505；
2. 中国科学院 上海天文台，上海 200030）

**摘要：**时频系统监测参数多，结构复杂，数据处理环节多，故障排查困难。本文首先介绍了典型时频系统结构及故障诊断难点，深入研究了网络嗅探诊断技术，提出了时频故障排查方法和基于网络嗅探器的数据故障排查方法，设计了基于网络嗅探技术的时频故障诊断软件，最后分析了该方法在某时频系统中的故障诊断应用。

**关键词：**网络嗅探技术；氢原子钟；故障诊断
**DOI：**10.13875/j.issn.1674-0637.2021-02-0113-07

# A fault diagnosis method of time-frequency equipment based on network sniffing technology

HE Zhen-hua[1], LI Xi-rui[2], JIANG Chao[1]

(1. Troops 61920, Chengdu 610505, China;
2. Shanghai Astronomical Observatory, Chinese Academy of Sciences, Shanghai 200030, China)

**Abstract:** Time-frequency system has many monitoring items, complex structure, multi-step data processing links. It's difficult in troubleshoot for time-frequency system. This paper introduces the typical time-frequency system structure and fault diagnosis difficulties, studies deeply the network sniffing diagnosis technology, proposes the time-frequency fault diagnosis method and the data fault diagnosis method based on network sniffer, designs a time-frequency fault diagnosis software based on network sniffer technology, and finally analyzes the application of this method in a time-frequency system.

**Key words:** network sniffing technology; hydrogen maser; fault diagnosis

## 0 引言

时间频率系统作为信息系统的重要组成部分，已经广泛应用于通信、卫星导航、电力传输、航空航天等各个领域。时间频率系统的健康程度决定信息系统的工作状态，时间频率系统出现故障，将对信息系统运行造成致命的损害。时间频率系统的故障诊断和排除已成为信息系统维护的重要内容和关键步骤。

时频系统结构复杂，设备精密，核心参数多，上下级设备配合紧密，容易出现设备故障且故障原因不易定位的问题。基于网络嗅探技术研究出一套快速有效、定位准确的诊断方法，可以在监控软件的设

收稿日期：2020-11-20；接受日期：2021-01-12
基金项目：国家自然科学基金资助项目（U1731130）

备监测与控制功能失效时迅速诊断排除故障[1-4]，从而提高时频系统可用度。

# 1 典型时频系统结构及故障诊断难点

## 1.1 时频系统结构

时间频率系统是信息系统的重要组成部分，为信息系统提供准确、稳定、可靠的时频信号。典型的时间频率系统一般由高精度时间频率源、频率切换、时码产生、信号放大、比相监测、监控等关键设备组成。高精度时间频率源是整个系统频率基准的核心，可以为其他设备产生标准时间频率信号，要求高的系统往往采用氢原子钟作为时间频率基准；频率切换设备可以选择主用时钟源，并且实现主、备时钟源间的无缝切换，确保时频信号可靠不中断；时码产生设备可以向标准时间溯源，再结合本地时间频率源频率信号产生本地时间信息及时标信号；信号放大设备可以把频率信号、时标信号进行数量扩充和强度放大，用以输出给其他设备；比相监测设备可以对时间频率系统各设备产生的时间频率信号进行相位比对监测，确保信号输出的正确性；监控设备用来监控所有时间频率设备的状态工况[5]。典型的时间频率系统构成如图 1 所示。

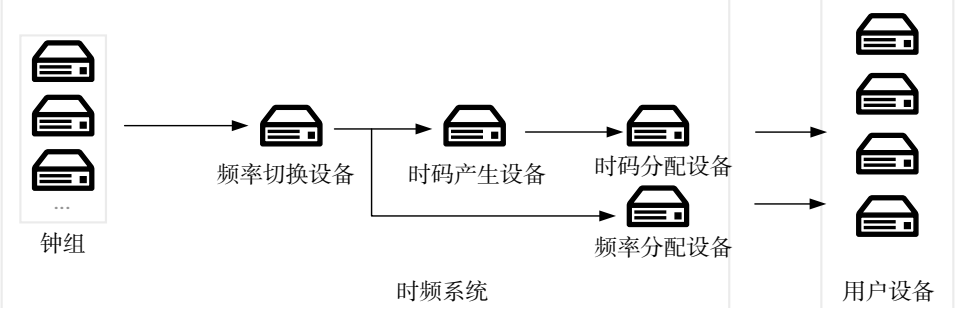


图 1 典型时间频率系统构成图

## 1.2 时间频率系统运行要求

时间频率系统作为信息系统的核心和运行基础，其可靠性直接决定了信息系统的可靠性，这对时间频率系统的运行和维护提出了较高要求。时间频率系统的运行要求包括：

① 信号输出准确性：要求输出信号具备较高的频率准确度。

② 信号输出稳定性：要求输出信号具备较高的频率稳定度。

③ 可靠性：系统要保持较高的可用度，一般采用多台关键设备热备份运行。

④ 自评估能力：系统可以对自身设备状态进行评估，并且可以自动选择主用设备并进行切换。

⑤ 无缝切换性：切换过程应当确保信号不发生跳变，用户感受不到设备的切换。

由于时间频率系统运行要求较为苛刻，系统构成较为复杂，冗余设备较多，因此故障发生后难以对其精准定位。尤其是大部分故障诊断方法均需要中断系统开展故障定位，会对系统可靠性造成影响，降低系统可用度。

## 1.3 时间频率系统故障处置要求

根据时间频率系统故障对其信号输出造成的影响，故障主要可以分为 3 类：

1）信号输出功能失效：此类故障发生时系统已停止输出信号，或时频信号发生跳变，造成系统可用度降低。

2）关键设备单点运行：此类故障发生时，虽然信号可以暂时输出，但由于关键设备已处于单点运行，主备切换功能已经失效，若此时主用设备也失效，将恶化为第 1 类故障。

3）监控软件监控功能失效：在此故障中，信号产生和输出设备均正常，但监控功能失效，可能导致故障向第 2 类或第 1 类恶化。

对于第 1 类故障，此时信号已中断，已经对系统可用度造成影响，而第 2 类和第 3 类故障发生时，系统仍正常输出信号，此时的快速诊断和故障排除可以避免故障向第 1 类故障恶化，对提升系统可用度和可靠性具有重要意义。

### 1.4　故障诊断难点

对于后两类故障的诊断排除，难点共有两个：首先是时频系统很复杂，部分设备输入输出逻辑交联在一起，故障难以快速定位；其次是此时系统仍然输出信号，无法中断系统对故障进行排查，因此需要在系统运行过程中获取监控数据，这也对故障诊断提出了较高要求。针对这两个难点，采用网络嗅探方法对后两类故障进行诊断，是一种有效的诊断方法。

## 2　网络嗅探技术

网络嗅探器，是一种在网络上收集和分析数据的技术。采用网络嗅探技术进行信息系统监控和故障排查，可以不影响原系统的正常运行，在系统不中断的情况下获取原始运行网络数据并进行分析，便于多设备的信息系统数据监控和故障排查。

### 2.1　嗅探流程

通过网络嗅探抓取数据包，并将数据提取至应用程序中，这个过程需要对网络物理层到应用层进行协调设置。在以太网中，数据包的流通流程为：

① 物理层：数据自一个节点在网线和交换设备中传输至另一个节点。

② 数据链路层：节点的网络适配器（网卡）筛选属于自己且正确合法的数据帧重构成数据包送入操作系统的协议栈。

③ 网络层至运输层：操作系统的协议栈通过这两层中的协议判断到来的数据包的目标（操作系统、应用程序）。如果数据包合法，操作系统通过端口将数据包重构成报文送入应用程序[6–8]。

当网络的物理条件满足后，数据才会来到嗅探器中，首先到达的地方就是网卡，网卡将数据（Bits 流）变成数据帧的形式，开始进行判断接收。当数据经过数据层链路后，还要通过操作系统协议栈的审核，系统协议栈在开发环境中设置混杂模式，就可以接收从驱动层来的各种数据，最后通过嗅探软件在应用程序层中解析获取数据[9–11]。

在采用网络嗅探获取数据时，可以采用区别于目标计算机的其他计算机进行数据抓取，也可以在本机直接抓取。考虑到在对时频系统进行故障诊断时，为了便于数据抓取，可以直接将嗅探软件部署于监控计算机本地，这样不需要对系统网络进行改造就可直接进行抓取[12]。

### 2.2　嗅探机制

由于操作系统的分层机制，造成了网络嗅探的复杂性。为了确保操作系统的稳定，用户无法直接使用内核的资源，用户只能在用户模式的层次上使用自己的内存和其他资源，各类用户操作也只有通过一定的转换才能到达核心层，这隔离了用户对操作系统的直接影响，但是也加大了计算机资源的负荷。由于不同操作系统的差异，其数据的过滤捕获机制往往也存在差异。Unix 类型的操作系统中主要的截获机制有：BSD 类系统中的 BPF 机制，SVR4 中的 DLPI 机制以及 Linux 中的 SOCK_PACKET 类型套接字，而在 Windows 操作系统下，因为 Windows 系统没有提供对链路层直接操纵的接口，需要利用系统提供的网络驱动程序接口规范（Network Driver Interface Specification，NDIS）机制开发中间驱动程序来完成

对数据包的截获，并且，Windows 操作系统还提供了接口程序 SPI，因此可以利用 SPI 截取数据包[13]。

# 3 基于网络嗅探技术的时频故障诊断软件设计

运用网络嗅探技术可以对时频系统的监控计算机进行网络数据包的抓取，通过监控计算机这个中心节点获取时频系统中各设备的数据流并解析其内容，最终通过数据分析实现系统故障的诊断。

## 3.1 设计目标

在基于嗅探技术的时频诊断软件中，软件对流经监控系统的所有设备数据进行监视，充分发挥软件的监督作用。根据时频系统常见故障特点和运行要求，对于诊断软件的具体设计目标如下：

① 监控全面：应能够对所有时频系统监控数据进行监测。

② 安全性高：故障诊断的过程不影响时频系统运行，不会对原系统产生干扰。

③ 操作性强：人机交互应当友好，操作方便。

④ 定制灵活：时频设备数据种类多，需要对部分重要数据进行监控和分析时，可以进行灵活定制，以节约监控资源、突出分析重点[14]。

## 3.2 功能组成

根据软件设计目标，可以分析出软件设计的主要功能如图 2 所示，具体包括：

① 网络嗅探：通过嗅探器对以太网中数据包进行捕获，将这些信息提交给数据分析引擎。

② 数据分析：对已经捕获的数据进行应用层的协议分类，并应用相对应的分析策略进行处理。分析内容包括：数据源及目的地址是否正确、数据长度是否正确、数据格式是否符合协议、关键参数是否符合逻辑等。

③ 参数设置：可以对监听的网口、端口进行设置，以获取感兴趣的数据。

④ 数据显示：对监听数据报的数量、来源 IP 及端口、目的 IP 及端口、报文内容进行显示。

⑤ 数据存储：对需要分析的数据进行存储[15]。

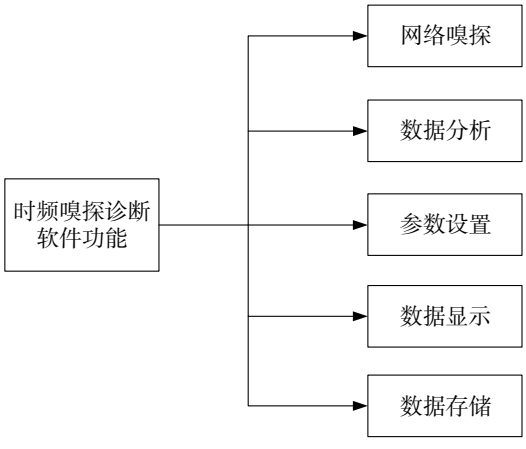


图 2 软件功能示意图

## 3.3 总体结构

整个网络诊断系统功能示意图如图 3 所示，根据其功能和物理位置分为 3 个主要的模块：

① 网络嗅探器：可以实现对网络数据包的监听、捕获。软件安装在被监控时频系统的监控计算机上，通过绑定网卡实现数据的接收。

② 协议分析引擎模块：对抓取的数据进行应用层协议分析，并应用相对应的分析策略进行处理。

③ 监控台模块：实现操作交互、数据显示和数据存储功能。

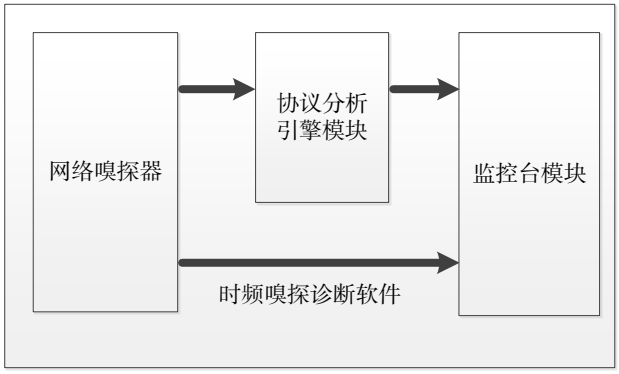


图 3　软件功能示意图

### 3.4　时频系统适应性设计

网络嗅探方法适用于采用以太网进行数据传输和监视控制的时频系统，但串口作为成熟的工业传输接口，也广泛应用于信息系统之中，针对这类时频系统可以通过改造数据传输网络以使结构更加优化。

串口在使用过程中，具有以下缺点：连接不便、对于多设备节点不便于拓扑扩展；串口尺寸较大，不利于走线；串口易损毁，不能热插拔，不便于系统断路调试等。通过串口服务器将串口网络转换为以太网网络，可以有效地克服上述缺点。

串口服务器可以把多路串口线路转换为以太网网络，其主要具备两大功能：

① 数据传输形式转换：串口服务器可以将设备输出链路由串口转换为网络链路，通过网卡和设备相连接。监控系统在监控软件编写过程中，可以通过串口服务器的驱动程序采用逻辑串口监控设备，也可以直接使用网络编程方法监控设备，方法灵活多样。

在采用网络编程方法监控设备时，通过访问串口服务器设置的 IP 地址连接到串口服务器，再通过不同的端口号便可访问到该串口服务器上连接的各设备。

② 进行多点数据交换：串口服务器可以同时连接多个串口设备，起到网络交换机的作用，从而使一台监控系统同时监控多台设备，由于串口服务器连接监控系统的一端为网口，在监控设备数量较多时，还可以采用交换机连接多台串口服务器，扩展快速简便。

采用串口服务器监控串口设备的连接示意图如图 4 所示。

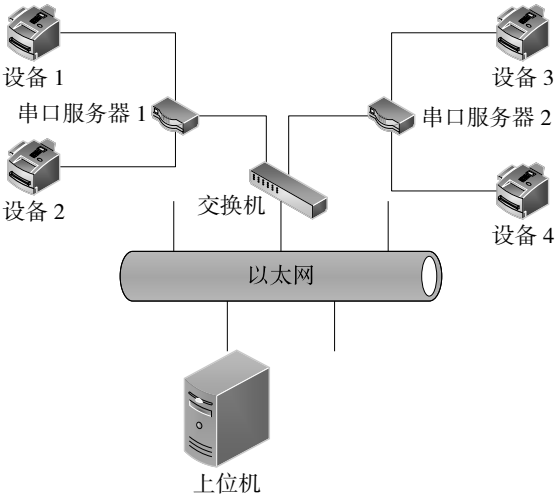


图 4　串口服务器监控示意图

此外，采用串口服务器进行时频系统监控，可以使数据通过网卡收发，从而可采用网络嗅探技术监

测数据情况。

## 4 典型故障诊断方法

采用网络嗅探器，可以对 1.3 节中后两类故障进行较为快速的诊断定位。下面将以某典型时间频率系统为例，分析该系统设备故障的诊断定位方法。

### 4.1 相位调整失败故障

该故障发生时，时频监控系统可以正常更新钟组数据，但发送相位和频率准确度调整指令后，钟无法执行指令。该故障可能为由于备钟故障造成的第 2 类故障，也可能是监控软件错误造成的第 3 类故障。

在某时间频率系统中，通过报文分析，可以发现软件发送的目的地址端口与设备实际地址端口不一致，如图 5 所示，根据报文解析，指令发送的目的地址和端口为：202.127.24.186:4001，但实际设备端口为 4002，故造成故障发生。由此定位故障为软件设计出现问题，无法根据实际配置的串口向钟组发送控制指令。

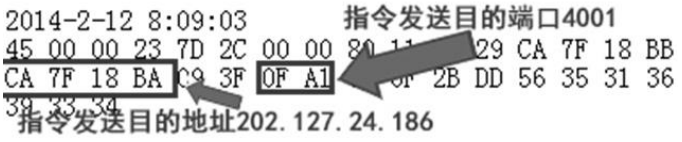


图 5 频率调整指令发送地址及端口

### 4.2 监控失败故障

该故障现象是时频监控计算机对某台钟源的数据停止更新，对钟的控制指令失效。该故障发生的原因主要有 3 种：线路接口松动、监控软件端口选择错误、钟源监控系统损坏。若由于线路出现问题或钟源监控系统损坏，则故障为第 2 类故障；若由于软件端口选择错误，则故障为第 3 类故障。

该故障发生时，首先应当检查线路、接口和通信设备，确保数据传输链路正常。若传输线路正常时仍然存在故障，采用嗅探器检查故障原因。

若通过嗅探器判断数据收发正常，则时频监控系统故障。启动网络嗅探软件抓取原始数据报文，通过分析报文中的 IP 地址、端口号等内容判断软件故障原因。

若通过嗅探器判断软件发送数据正常，但钟源未反馈数据，则可定位故障于钟源监控系统，此时可直接对该钟进行维修。

例如，某时频监控软件对钟源监控过程中发生该故障。在确定线路正常后，启动网络嗅探软件对数据包进行分析。通过分析可以看出，当选择该钟端口 B（对应网络端口为 202.127.24.186：4010，如图 6 所示）为主端口时，数据可以正常通信，但当设置端口 A（对应网络端口为 202.127.24.186：4001）为主端口时，数据无法更新，因此推断为钟源监控系统故障。

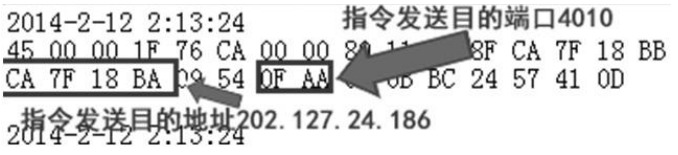


图 6 时频监控软件指令发送地址及端口

### 4.3 监控误报警故障

该故障发生时，时频监控系统可以更新设备数据，但会频繁出现报警。该报警与设备工作状态不符，

为误报警。发生该故障时，一般为软件故障，为第 3 类故障。

某时频监控软件对 3 台钟源频繁出现报警现象，通过查看各钟与故障分析，发现监控报警与实际原子钟运行状态不符。通过网络嗅探软件分析原始数据包，发现在发送过程中出现数据包不完整现象，如图 7 所示，根据报文解析内容，该指令完整的数据报文长度为 70 个字节，但部分报文长度仅为 46 字节。

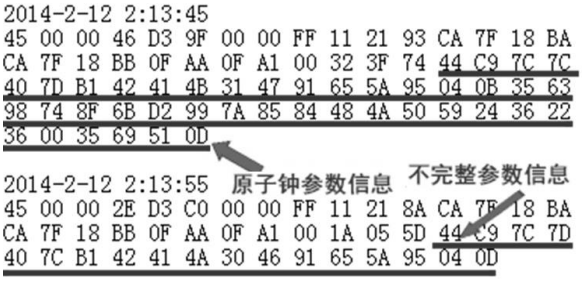


图 7　数据报文中原子钟参数信息

由图 7 分析出该故障产生原因为：时频监控软件接收到不完整的钟源监控数据后直接进行数据解析，导致对不完整数据内存之后的内容进行了解析，最终产生错误参数并发生报警。修改时频监控软件后该故障消除。

## 5　结语

时间频率系统是信息系统的重要组成部分，对时间频率系统进行故障诊断，存在无法中断排查和难以定位的特点。网络嗅探技术可以实现计算机数据包的抓取和数据分析。采用网络嗅探技术，可以快速诊断定位时频系统故障，并且对部分功能失效的系统进行不间断排查，从而提高时频系统可用度，最终确保信息系统的稳定运行。

## 参考文献：

[1] 张洋. 基于局域网的嗅探器发现技术的研究[J]. 微计算机信息, 2005, 21(23): 33-35.

[2] 梁理, 黄樟钦, 侯义斌. 网络信息侦听系统的研究与实现[J]. 计算机工程与应用, 2002, 38(17): 184-186+226.

[3] 刘琦, 李建华. 网络内容安全监管系统的框架及其关键技术[J]. 计算机工程, 2003, 29(2): 287-289.

[4] KOTZ D, ESSIEN K. Analysis of a campus wide wireless network[J]. Wireless Networks, 2005(11): 115-133.

[5] 上海天文台. SOHM-4 型氢原子钟技术说明书[K]. 2008.

[6] 李佳静, 徐辉, 潘爱民. 入侵检测系统中的协议分析子系统的设计与实现[J]. 计算机工程与应用, 2003, 39(12): 152-155.

[7] 温研, 王怀民, 胡华平. 分布式网络行为监控系统的研究与实现[J]. 计算机工程与科学, 2005, 27(10): 13-16.

[8] 李晓莺, 曾启铭. NDIS 网络驱动程序的研究与实现[J]. 计算机应用, 2002, 22(4): 60-61.

[9] 谭思亮. 监听与隐藏: 网络侦听揭秘与数据保护技术[M]. 北京: 人民邮电出版社, 2003.

[10] VISHKIN U. Deterministic sampling-a new technique for fast pattern matching[J]. SIAM Journal on Computing, 1991, 20(1): 22-40.

[11] BAEZA-YATES R, GONNET G H. A new approach to text searching[J]. Communications of the ACM, 1992, 35(10): 74-82.

[12] 刘振宪, 王津涛, 侯德, 等. 基于原始套接字的网络安全研究与实现[J]. 计算机工程与设计, 2006, 27(5): 768-770+779.

[13] 连一峰, 王航. 网络攻击原理与技术[M]. 北京: 科学出版社, 2004.

[14] 陈烽华, 张代远. 基于 RawSocket 技术的改进 Sniffer[J]. 计算机时代, 2007(5): 22-23.

[15] 董玉格. 攻击与防护(网络安全与实用防护技术)[M]. 北京: 人民邮电出版社, 2002.