# 大型设备监控系统通信协议①

赵 炯, 凌 浩, 王 军

(同济大学 机械与能源工程学院, 上海 201804)

**摘 要**: 针对大型设备监控系统在远程通信过程中大数据量传输及部分数据高实时性要求的特点, 设计一种基于 TCP 的应用层通信协议, 实现底层监测设备与监控中心间的可靠通信. 协议提出了从监测设备到监控中心的安全登录方法, 并能够根据实际需求, 完成对个别参数或部件信息地实时传输. 该协议具有较大的灵活性、可扩展性和安全性, 能够满足大型设备监控系统中采集设备和监控中心之间的数据传输需求.

**关键词**: 通信协议; 远程监控; 安全登录; 实时传输; 海量数据

## Communication Protocol of Monitoring System of Large Facility

ZHAO Jiong, LING Hao, WANG Jun

(School of Mechanical Engineering, Tongji University, Shanghai 201804, China)

**Abstract**: Aiming at achieving reliable communication between the underlying device and the monitoring center, a new application layer protocol based on TCP is designed to deal with the huge amounts of data transmissions and high real-time requirements of some data. The protocol proposes secure login method from the acquisition device to the remote monitoring center, and it can complete transmitting real-timely specific parameters and components according to the actual requirements. The protocol has great flexibility, scalability and security, which can meet the demand of data transmission between the acquisition device and the monitoring center in the monitoring system of large facility.

**Key words**: communication protocol; remote monitoring; secure login; real-time transmission; massive data

大型设备(如位于港口码头的斗轮机、卸船机等)在地理上往往具有分布零散的特点, 企业难以有效对这些设备进行统一管理. 因此, 设计一套针对大型设备的远程监控系统来实现对大型装备的状态监测, 故障诊断和远程维护就显得十分有意义[1].

在整个监控系统中, 通信网络是监控中心与采集设备之间的桥梁. 好的通信协议对于系统的高效和可靠运行起着至关重要的作用. 本文所设计的通信协议就是为了解决在对大型设备进行监测的过程中海量数据传输和实时性要求之间的平衡问题.

## 1 监控系统结构

整套监控系统主要由两部分组成: 监控中心和机载系统(主要是监测设备). 监控中心实现了以下功能: 对监测数据进行处理, 获取有效信息, 对设备的状态进行监测; 将获取的信息发布到网页上, 用户可以通过浏览器远程登录系统, 在线查看和管理各个设备; 实现对个别部件和参数的实时动画显示. 安装于机载端的监测设备(黑匣子)可以通过多种方式(包括以太网、485 总线、CAN 总线等)采集数据, 然后将数据进行暂存并通过无线通信的方式传输到监控中心. 另外, 本系统建立了用户到现场设备的 VPN 通道, 实现用户对设备的直接访问和管理. 整个监控系统的方案如图 1 所示.

## 2 通信协议设计

在通信协议中, 主要可以分为两类: 基于文本的通信协议(如 HTTP 协议)和基于字节的通信协议(如 TCP 协议). 鉴于文本型通信协议具有可读性高、易于扩展、便于解析的特点, 而同时字节型协议所暴露的局限性越来越大, 本文即是设计一种基于文本的网络通信协议.

① 收稿时间:2015-09-07;收到修改稿时间:2015-11-11

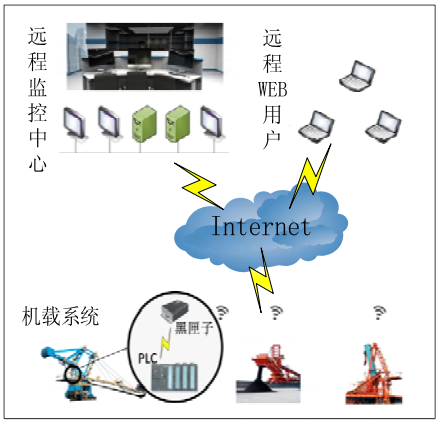


图 1　监控系统整体结构

### 2.1 通信方式

整套监控系统基于 TCP/IP 协议进行数据传输，下层使用 TCP 协议. 监控中心使用固定 IP 地址，机载系统通过 3G/4G 方式接入互联网，并以客户端形式登录到监控中心. 为提高服务器运行安全性，服务器仅开放 80 端口来处理与客户端的通信. 通信双方采用长连接形式，如果通信过程出现一方意外断开，客户端需要以一定时间间隔尝试重连，直到连接重新建立为止[2].

在通信过程中，协议要求对每个命令请求包，都必须应答，通过在应答包中添加与命令包一致的 ID 号来保证命令与应答的一一对应. 而对于监测数据包，则在其出现错误时才发送错误包，告知客户端进行重发，每个数据包有连续的 ID 号，当出现错误时监控中心的服务器根据前一个接收到的包 ID 来推出发生错误的包.

### 2.2 协议基本格式

本协议采用统一的基本格式. 无论数据包、命令包、应答包都是在基本通信格式框架内进行制定、修改. 协议基本格式由三部分组成，分别是：请求行、首部、正文. 通信协议的基本格式如图 2 所示[3-5].

| | |
|---|---|
| 请求行 | COMMAND VERSION\r\n |
| 首部 | username=xx\r\n<br>length=xx\r\n<br>commandno=xx\r\n<br>\r\n |
| 正文 | data |

图 2　协议基本格式

报文的第一部分是请求行，请求行由两个字段组成. 第一个字段是命令(COMMAND)字段，事实上，COMMAND 并不是代表命令，而是用来表示这个包是用来做什么的，它可以是命令、应答也可以是数据. 第二个字段是版本号(VERSION)，目的是在协议版本升级后能够区分以前版本的协议(在下文中使用 002 为版本号). 在行末的回车换行符，表示一行的结束.

报文的第二部分是首部，首部是以“属性=值\r\n”的格式，首部的行数并不限定，每行的长度也不限定，只要通信双方按照首部格式商定即可. 首部的结束是以一个空行来判定的. 在首部字段中有 length 字段，用来表示数据段的长度. 如果没有数据，那么长度字段为 0.

报文第三个部分是正文部分，即数据域. 数据部分的长度由首部字段中的长度确定. 正文部分可选，在一些情况下没有正文部分.

## 3　通信交互方式

### 3.1 客户端登录

客户端登录服务器分为两种情况，初始化登录和正常登录. 两者的区别在于初次运行时，服务器内尚未存有该设备的具体信息，只有设备的序列号，序列号是每台设备唯一的识别号. 客户端需要将自身的序列号、默认用户名、密码、配置等信息提交给服务端. 服务器用其存储的序列号和收到的设备序列号进行匹配. 如果匹配成功，则会存储设备的信息，并会生成一个新的用户名和密码，返回给客户端. 随后，客户端就会退出登录状态，并重新进行登录，此时就进入正常登录状态. 其工作流程见图 3 所示[6].

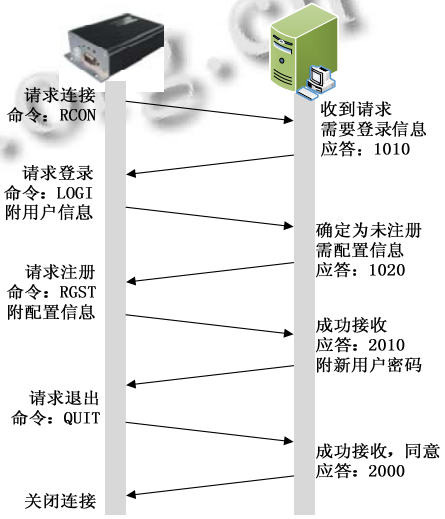


图 3　用户初次登录

在正常登录时，客户端将自身的用户名和密码发送至服务器后，服务器会查询数据库确认该客户，并返回确认信息. 随后双方就进入正常通信状态. 其过程如图 4 所示.

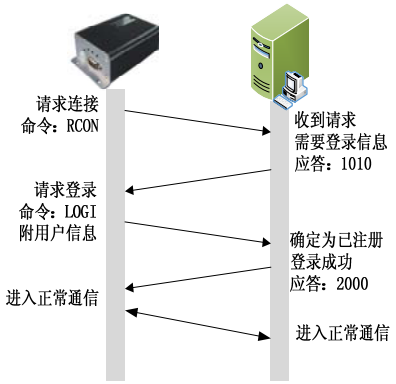


图 4 用户正常登录

### 3.1 数据传输

正常通信时，主要的任务是客户端向服务器发送监测数据. 数据包格式如图 5 所示.

| | |
|---|---|
| 请求行 | DATA 002\r\n |
| 首部 | username=xx\r\n<br>date=xx\r\n<br>length=xx\r\n<br>number=xx\r\n<br>datatype=xx\r\n<br>datalevel=xx\r\n<br>\r\n |
| 正文 | data |

图 5 数据包格式

在每次发送数据时，都带有用户名，目的是为了让服务器再次进行确认，保证数据源的正确性. 另外，数据包还必须带有时间戳，时间戳的格式为：year-month-day hour: minute: second. number 字段是表示数据包的 ID 号，用于数据包的出错重传. datatype 字段是为了区分不同的采集数据，本系统的采集数据包括 GPS 数据和 PLC 数据等. 对于不同的数据，设置成相应值即可. 例如，对于 PLC 采集数据设置 datatype=plc. datalevel 只有在数据类型为 PLC 采集数据时才会有，用来区分不同重要性的数据. 为平衡大数据传输与数据实时性问题，将 PLC 监测数据分为两级. 一级数据主要为开关量，其数据量较少，一般在几百个字节，实时性要求高，设置 datalevel=1；其余数据设为二级数据，其数据量大，可以达到几万个字节，但是实时性要求较低，设置 datalevel=2. 通过这种方式可以保证重要数据实时性的同时，最大程度地利用网络带宽来传输数据.

### 3.2 命令与应答

客户端和监控中心可以通过命令接口发送命令信息或进行命令应答. 命令和应答过程并不会影响正常的数据传输.

#### 3.2.1 实时功能

在本系统中，设计了对于某项参数或部件的实时动画显示功能. 这项功能不同于一般的数据传输，而是以一种命令和应答的方式. 当客户端在收到实时数据的命令时，开始尽最大努力采集并发送该参数或部件的有关数据. 而当用户停止该功能的时候，客户端能够迅速切换回正常通信状态. 其命令格式如图 6 所示.

| | |
|---|---|
| 请求行 | RETM 002\r\n |
| 首部 | begin=1\r\n<br>length=0\r\n<br>parameter=xx\r\n<br>number=xx\r\n<br>\r\n |
| 正文 | |

图 6 实时数据包格式

当用户查看某个参数或是部件的实时显示功能时，系统会发出 RETM(real-time)命令，表示开始传输实时数据并设置 begin=1；如果想结束传输，则发送 begin=0. parameter 字段表示哪个部件或参数需要传输的实时数据，在本项目中已预设几个数据需要进行实时传输，并且将这几类数据进行编号，parameter 的值就是所编号的值.

客户端对于该种命令的应答中包含的数据就是所需要的实时数据. 其格式如图 7 所示.

| | |
|---|---|
| 请求行 | 2130 002\r\n |
| 首部 | length=xx\r\n<br>number=xx\r\n<br>\r\n |
| 正文 | data |

图 7 实时数据应答包

#### 3.2.2 通信命令

通信命令有四个字符组成. 括号内的英文为命令代码.

1) 访问控制命令

① 连接请求(RCON)

用于连接初始的时候，客户端向服务器请求登录，无正文.

② 请求登录(LOGI)

用于客户请求登录服务器时使用. 登录命令包格式如图 8 所示. 登录密码放置在数据域并对其进行加密处理[7].

| | |
|---|---|
| 请求行 | LOGI 002\r\n |
| 首部 | length=0\r\n<br>username=xx\r\n<br>\r\n |
| 正文 | password=xx（加密） |

图 8 请求登录包

③ 初始请求登录(RGST)

用于初始向服务器发送登录请求.

④ 退出登录(QUIT)

用于客户端向服务器请求退出登录, 只有在初始化登录时才会请求退出, 无正文.

2) 传输参数命令

① 数据传输(DATA)

用于客户端向服务器发送数据的命令.

② 实时数据传输(RETM)

用于服务器请求某个实时动态数据.

3) 服务配置命令

①修改参数(CHAG)

用于服务器请求修改客户端或是 PLC 的参数. 每条命令只能进行一项参数的修改.

②查询(QURY)

用于服务器向客户端查询配置参数. 所有的配置信息都通过首部进行发送.

③等待(NOOP)

用于在连接没有信息往来的时候, 查看连接状态, 维护通信连接, 起到心跳包的作用. 该命令由客户端主动发起.

3.2.3 通信应答

通信命令的响应是由四个数字构成. 每一位数字都有其意义, 第一位确定响应是好的, 坏的还是不完全的, 通过检查第一位, 通常就能够知道大概要采取什么措施. 第二位表示是在什么环节中进行应答. 第三位是具体描述应答的细节, 视实际情况而定. 最后一位是保留位, 留待扩展[8].

1) 第一位有四个值:

1xyz 表示包已接收, 需后续处理;

2xyz 请求已被接收, 并处理;

3xyz 客户端错误;

4xyz 服务端错误.

2) 第二位同样有四个值:

x0yz 关于认证登录过程;

x1yz 关于请求;

x2yz 关于数据;

x3yz 格式错误.

本协议中所涉及的应答码如表 1 所示.

表 1 应答码表

| 应答码 | 描述 | 应答代号 |
|---|---|---|
| 1010 | 命令接收, 需登录信息 | NEED_LOG |
| 1020 | 命令接收, 需配置信息 | NEED_COF |
| 2000 | 命令成功接收并执行 | RECV_SUC |
| 2110 | 查询命令执行完成 | QURY_SUC |
| 2120 | 修改命令执行程完成 | CHAG_SUC |
| 2130 | 实时数据传输 | REAL_TIME |
| 2200 | 数据已经收到 | DATA_RECV |
| 3300 | 客户端无法识别, 格式有误 | CLIT_FORM |
| 4000 | 登录信息有误 | LOG_WROG |
| 4010 | 配置信息有误 | COF_WROG |
| 4100 | 服务器无法处理请求 | SERV_QURY |
| 4200 | 服务器无法处理数据包 | SERV_DATA |
| 4300 | 服务器无法识别, 格式有误 | SERV_FORM |

## 4 结语

本文根据在设计大型设备监控系统过程中所提出的需求, 设计了一种专用网络通信协议. 该协议实现了海量数据的快速传输, 根据数据的重要性进行分类传输, 保证不同实时性要求的数据都能满足传输的要求. 此外, 还设计了登录、验证功能以及实时数据传输的功能. 该协议简单明确, 具有高可靠性、可扩展性和安全性, 可以满足大型设备监控系统的传输需要.

## 参考文献

1 赵炯,熊肖磊,周奇才.自动化控制系统中通信协议设计研究.计算机工程,2002,28(8):85-85.

2 娄华平,孙运强,范广.远距离无线通信在监控系统中的应用.科技情报开发与经济,2006,16(17):229-230.

3 胡丽霞,赵光宙.基于分层结构的远程监控系统通信协议的设计.机电工程,2007,24(1):28-30.

4 贾本凯,庄卉,王国平,郭随平,陈志禄.卫星小站远程监控系统通信协议设计与实现.计算机测量与控制,2012,20(8):2240-2243.

5 聂晓旭,于凤芹,钦道理.基于Protobuf的数据传输协议.计算机系统应用,2015,24(8):112-116.

6 戴宁.基于 TCP/IP 协议的网络通信服务器设计[硕士学位论文].西安:西安电子科技大学,2014.

7 朱益飞,赵一鸣.基于身份的密码体制在即时通信协议中的应用.计算机应用与软件,2007,24(5):163-165.

8 史蒂文斯.TCP/IP 详解卷 1:协议.北京:机械工业出版社,2000:316-331.

9 Chen JWT. Design of networked control systems with packet dropouts. IEEE Trans. on Automatic Control, 2007, 52(7): 1314-1319.