

面向 OPC 监控平台的 Modbus/TCP 协议网关研究

陈 伟,方 群,王宏伟

(安徽师范大学 数学计算机学院,安徽 芜湖 241003)

摘 要:工业以太网两设备之间通信的协议主要是 Modbus/TCP 协议。对传统 Modbus 协议和 Modbus/TCP 协议数据帧的格式进行分析,特别为了保证工业以太网 OPC 监控系统数据的安全性和可靠性,提出网络接口冗余切换算法和网络接口 MAC 地址绑定,能保证 OPC 监控系统的实时安全性。在 Modbus/TCP 协议的工业以太网上实现水泥 OPC 监控系统,以 OPC Server 系统和 OPC Client 系统,两个子系统实现工业机器的参数和数据的控制,并在互连网上进行动态显示。根据动态的数据和参数,对机器进行有效的控制和操作,也可以进行远距离的查询数据,确保整个系统和机器的安全。

关键词:OPC 技术;Modbus 协议;Modbus/TCP 协议;冗余切换;MAC 地址

中图分类号:TP391

文献标识码:A

文章编号:1673-629X(2013)08-0075-04

doi:10.3969/j.issn.1673-629X.2013.08.019

Research on Modbus/TCP Protocol Gateway Faced OPC Monitoring Platform

CHEN Wei,FANG Qun,WANG Hong-wei

(College of Mathematics and Computer, Anhui Normal University, Wuhu 241003, China)

Abstract:Industrial Ethernet communication protocol between two devices is mainly on the traditional Modbus/TCP protocol. Modbus protocol and Modbus/TCP protocol data frame format is analyzed, particularly in order to ensure the security and reliability of the data in industrial Ethernet OPC monitoring system, put forward the network interface redundancy cotangent conversion method and network interface MAC address binding, can guarantee the real-time and safety of OPC monitoring system. In industrial Ethernet of Modbus/TCP protocol, realize cement OPC, OPC Server system and OPC Client system, implementing industrial machine parameters and data control, and displaying in the Internet dynamically. According to dynamic data and parameters, the machine can be effective control and operation, also remote data query, ensure the safety of whole system and machine.

Key words:OPC technology;Modbus protocol;Modbus/TCP protocol;redundancy switch;MAC address

0 引 言

随着工业化的进程和互联网的发展,计算机技术、通信技术和电子技术的融合,工业控制网络技术的不断提高,工业控制网络在实际工业控制中发挥至关重要的作用。计算机监控系统软件在早期的集中监控的方式下不断发展为全分布式,计算机监控系统设备通信协议由传统的 TCP/IP 协议发展为 Modbus/TCP 协议,而基于微软 COM/DCOM 技术^[1]的 OPC 是数据的采集技术,OPC Client 和 OPC Server 进行数据交换^[2]。在 Windows 系统下为工业控制监控系统提供了统一的接口,不同的厂商只要遵循 Windows 系统下 COM/

DCOM 和 OPC 技术标准就可以实现设备网络连接^[3]。

在传统的连接网络时须要选择 TCP/IP 协议,使得用户之间能相互进行网络互连就可以保证网络通讯畅通,而可靠的网络协议是网络设备用来通信的一套规则,也可理解为一种双方都可以接受的公用语言,但是传统的以太网网络数据传输实时较差,因为以太网发送数据是随机性的^[4]。在传统 Internet 网络层使用的协议为 IP 协议,而传输层使用的协议是 TCP 协议,就构成了传统的常用 Internet 网络的 TCP/IP 协议,而在工业控制领域为工业控制开发的 Modbus 协议和传统的 TCP/IP 协议基础上开发出现在的工业标准协议 Modbus/TCP 协议, Modbus/TCP 协议是应用于工业

收稿日期:2012-10-11

修回日期:2013-01-12

网络出版时间:2013-04-08

基金项目:国家自然科学基金资助项目(61201252);安徽重点产学研资助项目(KJ2011A148)

作者简介:陈 伟(1983-),男,安徽桐城人,硕士研究生,研究方向为网络信息安全、对等网络;方 群,硕士生导师,副教授,研究方向为对等网络、可信网络、网络中马式过程。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130408.1600.030.html>

控制器上的一种通信协议标准,传统的 Modbus 协议大多运行在 RS-232 串行链路上,而 Modbus /TCP 作为基于 TCP/IP 协议的 Modbus 实现,具有更好的可靠性、灵活性和扩充性。Modbus/TCP 通信协议应用于开发网关协议可以监控自动化设备的参数,通过网关内的集成硬件模块和其它总线以及 I/O 模块网络连接以太网。为了提高网关的安全性以及网络接口冗余备份技术的实现原理,提出快速冗余切换和备份的算法,为了增强系统的安全性提出了 MAC 地址的绑定和 IP 防火墙的过滤。

1 相关知识

Modbus 协议^[5]最早生产为工业过程控制研发的一种工业控制通信协议,也是施耐德公司为工业控制开发的一种工业协议,当工业控制网络用 Modbus 协议在链路上通信时,工业设备的控制器要知道设备的物理地址来识别发送来的 Modbus 消息报文,主要是硬件的操作通过 Modbus/TCP 协议决定产生何种操作。需要回应设备控制器将产生反馈信息并用 Modbus 协议通过工业以太网网络发送给其他与本设备控制器之间的通讯。Modbus 协议将通信设备控制器规定为主工业控制器(MASTER 设备)和从工业控制器(SLAVE 设备),整个系统主要是主控制器,主控制器可向从控制器发送消息请求,从设备控制器不断地检测是否有主设备发送消息,每个从设备都有自己的物理地址编号,最多可以达到 254 个,通过 Modbus 协议多达 24 种总线命令实现主工业控制器设备和从工业控制器设备之间的设备参数和实时数据的交换。

Modbus 消息帧^[6,7]控制器在 Modbus 协议的工业控制网络上具有两种标准的通信方式:ASCII 和 RTU 通信。在 ASCII 方式中,每个 Modbus 消息中的每 8 位字符分别分成 2 个 ASCII 字符进行发送。在 RTU 方式中,Modbus 消息中每 8 位字符包含 4 位十六进制字符进行发送。ASCII 的优点是允许各个字符的传输间隔在 0.5 秒到 1 秒之间而且具有高可靠性;RTU 方式比 ASCII 方式传输的优点是速度快,数据传输的实时性高,在相同的时间条件下,RTU 方式比 ASCII 方式可以传送更多的数据,但是每个 Modbus 消息必须是连续的数据流进行传输,保证数据消息快速传输。ASCII 消息帧采用 LRC 校验而 RTU 消息帧采用 CRC 校验,数据传输在目前 Modbus 工业控制网络系统中大部分采用 RTU 方式。

Modbus 消息帧中分:地址域、功能代码域、数据域。Modbus 消息帧中有专门的地址域,这个专门的地址域主要用于设备之间判定 Modbus 消息是否发给本主控制器设备的地址和发送给其他从控制器设备的地址,

通过这个地址域可以和从控制器设备之间通信,当消息由主控制器设备发给从控制器设备时,功能代码域主要作用是从控制器设备和主控制设备通信时需要执行哪些具体的操作;功能代码域还可以正常回应主控制器的请求和某些错误的信息,如果主控制器设备和从控制器设备通信没有发生任何错误信息,则从控制器设备返回的数据域包含请求的数据,如果发生错误信息,返回的数据域包含一个异常代码,并记录该数据域进行下一个数据域的传输,主控制器设备有专用的应用程序可以用来判断由从控制器设备反馈的异常代码,进行重传或进一步判断操作。

Modbus/TCP 协议是由施乐公司开发的以太网应用层协议,该协议将 Modbus 报文信息封装到 TCP 报文中,而 TCP 协议是面向连接的协议,是可靠传输协议,能保证工业以太网数据的可靠传输。Modbus/TCP 协议非常易于实现^[8],不仅因为简单易于实现而且 Modbus/TCP 协议是在基于 Modbus 应用协议基础上发展起来的,兼有 Modbus 协议的性质,Modbus 应用协议的数据传输,主要通过传统网络协议 TCP/IP 协议来传输,对用户来说是透明的,对工业控制自动化来说 Modbus/TCP 协议已经成为工业控制网络的标准协议之一。

图 1 为 Modbus/TCP 协议模型。

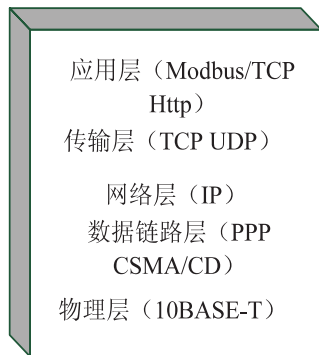


图 1 Modbus/TCP 协议模型

Modbus/TCP 协议是基于 TCP 协议的面向连接的一种协议并且数据在传输时可以并发操作,多个数据包可以独立地在同一连接上传输;而 TCP 协议也支持并发连接,可以提高数据传输的效率,也可以把每个单独的数据包封装在 TCP 协议报文中连接,而传统的 TCP 协议连接的辨别、控制操作容易实现,这也是 TCP 协议的优点,而实现的封装数据包是单独的,就可以单独地控制数据包的传输,单独地封装数据包就可以方便地增加防火墙过滤操作及其他的安全措施,增强 Modbus/TCP 协议网络的安全性、可靠性,使整个的工业控制网络具有高安全性和可靠性。

Modbus/TCP 协议在应用层使用的 TCP 连接的端口号是 502,通信的方式采用 C/S 模式,有四种服务:

Modbus 请求、Modbus 指示、Modbus 应答、Modbus 证实(见图2)。



图2 Modbus/TCP 客户机/服务器模式

MBAP 报文头是 Modbus/TCP 协议在 TCP/IP 协议上的 Modbus 应用数据的一个单元,MBAP 报文头中的一个字节单元标识符取代 Modbus 链路上使用的 Modbus 地址域,地址域主要是用于设备之间通信,每个设备有唯一的物理地址、IP 地址。可以透明通过交换机、路由器等网络互连设备和其他局域网的设备互连,使用 Modbus 地址域可以提高设备通信的效率。

Modbus 协议在工业以太网中传输数据时要保证数据的完整性、传输数据的正确性,所以在 Modbus 协议数据单元中操作 Modbus 请求、Modbus 响应。Modbus/TCP 报文中功能码本身就可以完成数据正确性的验证,而对于 Modbus/TCP 报文的数据部分需要对其数据的完整性进行验证,保证接收方能够快速地识别数据包边界,提高数据传输的效率,使工业实时性提高,即使将报文分成多个信息传输也能保证其数据的完整性,所以有了这些的验证可以确保 Modbus/TCP 协议传输的报文的正确性和可靠性。

图3为 Modbus TCP/IP 数据帧格式。

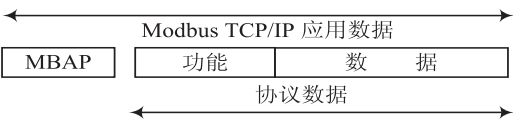


图3 Modbus TCP/IP 数据帧格式

2 Modbus/TCP 网关的可靠性和安全性

工业以太网的可靠性保证是网络的冗余,主要有快速生成树冗余(RSTP)、环网冗余(RTM)和主干冗余(TTM),这些可以提高网络的可靠性,常用的冗余方法是网络链路进行冗余备份和设备网络皆空进行冗余。安全性保证主要是 MAC 地址绑定和 IP 防火墙。

2.1 网络接口的冗余备份实现

网络接口的冗余备份是一种容错防错的机制,为了实现冗余备份,网络设备可以设计多个网络接口,这些端口具有相同的物理地址和网络参数,某一端口在通信时出现问题,可以通过软件的冗余切换保证网络快速恢复^[9,10]。网络接口冗余备份技术是系统中有两个以上网络接口,每个网络接口占有不同的中断号,用来中断切换网络接口。

驱动程序处于数据链路层的 LLC 层(逻辑链路控

制层),数据链路层的 MAC 层(介质访问控制层)完成数据在物理链路上的通信,为了提高工业以太网的可靠性,采用冗余备份设计思想,设计网络接口的数据结构^[11]。

```
typedef struct netcon {
    Struct netcon * next; //指向下一个网络接口
    Uint32 netcon_id; //网卡 ID 号
    Uint32 state; //网卡的状态
    Struct eth_addr macaddr; //网卡的物理地址
    Uint32 ipaddr; //IP 地址
    Uint32 netmask; //网络子网掩码
    struct ip_addr gw; //网关
    Uint32 mtu; //最大传输单元
    Void( * input)(struct prxbuf * p, uint16 len6);
    //网络接口接收函数
    Void( * output)(struct ptxbuf * p, const uint16 * len6)
    //网络接口发送函数
} Network;
```

2.2 冗余切换算法

冗余切换是保证数据正确的传输,首先由接口软件不停地对网卡接口进行轮询,判断传输的数据是否存在异常情况,如果出现有异常情况网络接口就进行切换。网卡控制器假设有一个阈值为 100ms,当 100ms 内没有检测到有效的脉冲,它会自动清除寄存器为 0;说明网卡有故障。中断就会触发冗余切换及时激活备份网卡。在中断处理中,通过周期性地调用 mac_check() 函数来判断网络接口的状态。流程图见图4,代码如下^[12]:

```
Struct netif * mac_check()
{
    Struct netif * netif;
    Uint8 lineZT=0; //初始化寄存器状态为 0
    Char * macValid//网络接口指针
    LineZT = netif_isValid( macValid );//检查当前网络接口状态是否异常
    If( lineZT=0 )
    {
        netif=netif_switch( macValid );//切换、激活备份网络接口
        netif_setup( &netif );
        macValid=netif; //macValid 指向备份网络接口
    }
}
```

netif_isValid() 函数来获取当前网络接口的状态,当网络接口出现异常时,就立即调用冗余切换函数 netif_switch() 备份网络接口参数,激活备份网络接口,并将 macValid 指向该网络接口,获取故障网络接口的参数,使两个网络接口保持参数的一致性。

2.3 网络接口的 MAC 地址的绑定

在工业以太网上数据的安全是不可忽视的,特别

是监控数据,如果监控下的实时数据发生错误,将会发生巨大的损失,所以安全性是联网设备都面临的问题。Modbus 网关响应客户机的请求时,连接都是用 TCP/IP 的端口号来识别,一般工业以太网都是允许特定的主机进行访问,为了保证数据传输的安全性,将网络接口 MAC 地址绑定到交换机端口上,使交换机的每个端口一一对应,保证“非法”的网络接口不能传输数据。

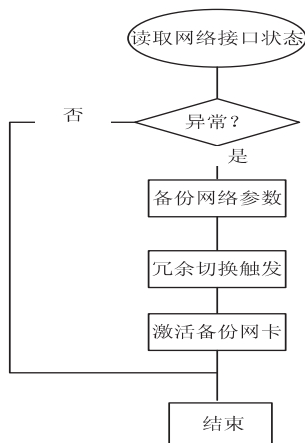


图 4 冗余切换流程图

3 性能测试

系统以水泥 OPC 监控系统为背景,OPC Server 和 OPC Client 部署在工程师站上,OPC Client 采集端负责采集 OPC Server 数据,而 OPC Client 接收端部署在 Window 2008 服务器上负责向 SQL2005 中写入数据,采集端和接收端中间部署 4572 网关,保证工程师数据的安全性,网关串口 (RS232) 连接在工程师站上,RJ45 通过二层交换机连接到 Window 2008 服务器主机网卡上。此系统在 OPC Client 采集端到 OPC Client 接收端数据通信加入网关,是以工业以太网 Modbus/TCP 协议。

测试是采用 Modbus/TCP 通信协议,在初始化随机指定一个激活通信网络接口,网络接口以 200 帧/s 速率通信 1h,通过 sniffer 抓包软件对通信数据进行分析,当一个网络接口出现故障,备份网络接口会自动切换。因为 Modbus/TCP 协议使用的是 TCP 协议,通过在 ping 命令查询网卡接口的状态,在不断测试中没有出现 ping 中断,说明冗余切换成功。假设故障检测周期为 50ms,通过测试主机以 50ms 和 100ms 的周期发送 TCP 测试包,此过程网关以 100ms 的周期自动冗余切换。TCP 数据包的丢包率低说明冗余切换算法具有

较高的性能^[12]。

图 5 为 OPC 监控系统现场部署。

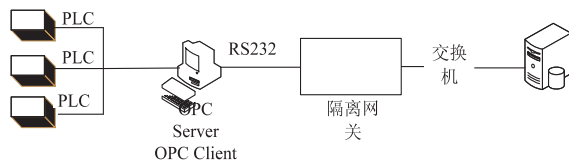


图 5 OPC 监控系统现场部署

系统在 Modbus/TCP 网关通过冗余切换算法保证了数据的安全可靠性,使得整个局域网内可以安全地访问实时采集的数据。

4 结束语

OPC 技术是一项工业标准,特别在工业实时控制上对数据的安全性要求比较高,Modbus/TCP 协议是工业过程控制一个通信标准协议。冗余切换算法可以提高 Modbus/TCP 协议网关的安全性和可靠性。

参考文献:

- [1] OPC Foundation. OPC DA2.05a Specification[S/OL]. 2002. <http://www.opcfoundation.org>.
- [2] Stallings W. SNMP 网络管理[M]. 胡成松,汪凯,译. 北京:中国电力出版社,2001.
- [3] 白金东. OPC 技术在 Modbus/TCP 工业以太网控制系统中的实现与研究应用[D]. 南京:南京工业大学,2005.
- [4] 张文超,李京. OPC 技术在工业以太网控制系统中的应用[J]. 自动化仪表,2004,28(3):88-91.
- [5] 龚克. Modbus 协议及其 PC 机实现[J]. 福建电脑,2004(7):21-22.
- [6] Modbus-IDA. MODBUS Application Protocol Specification V1.1a[S/OL]. 2004-06-04. http://www.Modbus.org/docs/Modbus_Application_Protocol_V1_1a.pdf.
- [7] Modicon Modbus Protocol Reference Guide, Release 1.0[M]. USA:MODICON, Inc., 1998.
- [8] 邓心茹,丁建兴,杨翼,等. Modbus/TCP 工业以太网的现状与发展[J]. 工业控制计算机,2004(9):14-16.
- [9] 刘利强,戴运桃,周卫东. 基于 VxWorks 的双端口网卡智能双冗余驱动[J]. 电子技术应用,2006(7):64-66.
- [10] 田炜,刘利强,袁赣南. VxWorks 环境下双网卡冗余备份技术的实现[J]. 自动化技术与应用,2003,22(7):32-34.
- [11] Stevens W R. TCP/IP 详解卷 2:实现[M]. 范建华,胥光辉,译. 北京:机械工业出版社,2000.
- [12] 吴万涛. 基于工业以太网的 Modbus 网关研究与设计[D]. 南京:河海大学,2008.

(上接第 69 页)

- 802.22 networks[C]//Proc. of IEEE GLOBECOM. [s.l.]: [s.n.], 2008:1-6.
- [12] Kloeck C, Jaekel H, Jondral F K. Dynamic and local combined

pricing, allocation and billing system with cognitive radios [C]//Proc. of IEEE DySPAN'05. [s.l.]: [s.n.], 2005:73-81.

面向OPC监控平台的Modbus/TCP协议网关研究

作者：[陈伟](#)，[方群](#)，[王宏伟](#)，[CHEN Wei](#)，[FANG Qun](#)，[WANG Hong-wei](#)

作者单位：[安徽师范大学 数学计算机学院, 安徽 芜湖, 241003](#)

刊名：[计算机技术与发展](#)

ISTIC

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013(8)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201308019.aspx