工控网络通信协议解密的实现

梁建武 施荣华 杜 伟 中南大学信息工程学院(410075)

Abstract

This paper presented a new model for breaking code to communication network protocol which is very simple and practical and solved effectively the new problem of heterogeneous PLC networks,meanwhile,which is practical effect for user saving investment.The key technique used in hardware component of breaking code and serve software were analyzed in detail.Through the analysis of the program,the scientific practicability of the method is verified.

Keywords:heterogeneous network,API function,protocol,break code

摘 要

针对工控网络的特点,提出了一种对通讯网络协议解密的新模型,该方法简单实用,有效地解决了异构 PLC 工控网络互联新问题,同时为用户节省投资具有现实意义。本文详细分析了解密的硬件设计和软件编制过程使用的关键技术,通过对模型的设计理论和框架的分析,印证了用该技术的科学实用性。

关键词:异构网络,API 函数,协议,解密

目前,世界各大厂商都相继推出自己独特的工控网络产品,它们自成体系、软件通讯协议互不兼容。不同协议的网络互联,能否实现设备的无缝联接,成为目前自动化领域最关心和最迫切的问题[1]。同时也是解决重复引进,造成大量资金浪费的新问题。这就引出了如何对 PLC 工控网络通信协议解密的新课题。

本文对世界上应用最广泛的几种自动化控制及其工业以太网的通信机制进行了分析研究,提出一种破译工控网络过程协议的新思路,此法已在几家大型的企业投入使用,解决了大型企业 PLC 工控网的异构,同时由于对协议的解密,避免了重复引进上位监控部分的硬件和软件。

1 工控以太网模型分析

对工控网络系统,分为工业设备过程、逻辑控制的专用设备和对生产工作进行监控与管理的设备两级,分工的不同决定其体系的软硬件资源和运算能力与分布的不均等,而进程的客户/服务器模型能很好的适应这种现象。从技术上考虑,因网络通信完全是异步的,所以不知道何时发起一次进程通信,相互通信进程之间既不存在父子关系,又不共享内存缓冲区,因此它们的通讯协议是一个黑箱。

为了简化问题,一般从特定的串口通讯开始,它们有一个共同点就是过程控制级和监控级都有 RS232 串口的通讯。由于不知道什么时候发起一次进程通信,故必须编制一个基于 API 函数的线程等候程序。一旦有通讯就能监控通讯协议的内容,先试用和过程控制级连接。将会收到其发出的通信协议。有的是传送数据的请求或部分数据内容,过一会儿重复以上内容,一般重复三次后,就会接到出错信息。和监控级联接时现象差不多。很明显它们通讯的一种应答模试,只有一方传递数据请求得到应答时才会进行正常通讯,以便传递以下的数据。

为了解决这个问题,必须保证过程控制级和中心监控级能正常通讯的情况下去捕捉它们之间互相应答的内容,然后再对内容分析、处理、确认通信的协议规则,故在软件上采用两个通信线程监控程序接收来自过程控制级和中心监控级的传送协议。在硬件上大胆提出信号分流关键技术:把过程控制级串口发送线(S)接到解密通信接收机的串口 1 的接收线(R)上,再把监控级的发送线(S)接到通信接收机的串口 2 的接收线(R)上,再把地线连起来,如图 1 所示。

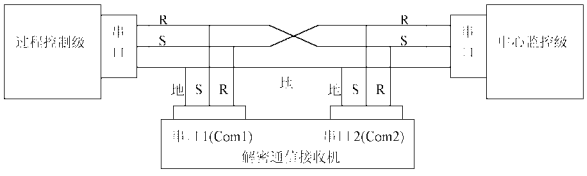

图 1 通信协议硬件解密模型

2 通信协议解密实现

以美国某公司的系列 PLC 为对象原型,对 PLC 工控网通信码解密的具体方法:

2.1 硬件设计

按连接图 1 通信协议硬件解密模型连接好,其中解密通信接收机就是一般的兼容计算机即可(一般都带有两个串口 Com1、Com2)它的目的就是接收来自过程级和监控级两处发送的信号,也就是它们互答的通讯的协议。

2.2 软件设计

通信服务软件中,采用面向对象技术,其语句均采用对象封装技术便于代码重用以及协议升级[2]。

初始化串口 Com1 和 Com2,配置串口参数,并打开两个串口(程序略)。

建立两个读串口的函数 ThreadProc1 和 ThreadProc2。这两个是接收过程控制级和监控级信号的多线程全局函数,表面上看是同时运行,互不干扰。实际是分时片运行的。只有充分利用多线程访问的关键技术,才不会丢失信号。它们均从 CwinThread 线程类中继承而来,首先创建两个全局函数:

```
UINT ThreadProc1 (LPVOID param)
UINT ThreadProc2 (LPVOID param)
```

这两个读线程函数结构一样,以下就是 ThreadProc1 线程函数,用 API 函数写的原程序:

```
UINT ThreadProc1 (LPVOID param)
{ unsigned long nBytesRead;          //定义保存接收信号变量
```

* 国家自然科学基金项目"计算机网络分布资源认证存取控制问题的研究"批准号:60173041

```
while(test)
{ SetCommMask(hCom1,EV_RXCHAR);//EV_RXFLAG}; //设置通信检测事件。检测到。
    if(WaitCommEvent(hCom1,&dwEvent,NULL)) //检测通信事件。
    {  ::Sleep(t);                          //准备读串口!
    ClearCommError(hCom1,&dwError,&cs);//获取缓冲区字节数。
    if(cs.cbInQue)
        {if (!ReadFile (hCom1,input,cs.cbInQue,  &nBytesRead, NULL)) //读串口
        { return 0;                          //读串口失败! }
          else{ receiveData=CString(input,nBytesRead); //读串口成功!");
        ::PostMessage(hWndUpdate,WM_USERUPDATE,0,0);}}}
        PurgeComm(hCom1,PURGE_RXCLEAR); }
        return 1; }
```

然后在初始化程序驱动这两个线程：

```
AfxBeginThread (ThreadProc1,hWndread,THREAD_PRIORITY_NORMAL);AfxBeginThread(ThreadProc2,hWndread,THREAD_PRIORITY_NORMAL);
```

2.3 调试与数据分析

启动解密程序后，就会收到过程控制级和监控级应答信号，收到的源信息用一般的编辑软件看不到（一般显示是乱码），它们的通信码很多不是可见字符的 ASCII 码，要采用专用的 UltraEdit 编辑软件浏览。在监控级对过程控制级发读信号时，则会接受到监控级和过程控制级的信号。通过对过程控制级的不同地址单元读不同的数据个数。表 1 为监控级读过程控制级 4 号单元的整数时，解密机接收的来自监控级和过程控制级的信号。

表 1　为监控级读过程控制级信号

信号源＼字节	0	1	2	3	4	5	6	7	8	9	10	11
来自监控级	01	00	0F	00	02	00	A2	02	04	89	00	00
来自过控级	00	01	0F	00	02	00	05	06	8A			

就不难发现监控级的协议格式：

第 6 字节为功能码 A2 为读，第 7 字节为读数据个数 2（字节数表示），第 8 字节为过程控制级的所读单元地址编号 4，第 9 字节为数据类型（89 为整数）。

过程控制级返回的协议格式：

最重要的是返回数据，通过与监控对比，不难发现从第 6 个字节可始为返回的数据，整数是两个字节（H 高位在前，L 低位在后），数据的计算为 256＊H+L（注意有的机型最高位要屏蔽），紧跟数据后就是一个校验码。

在监控级对过程控制级发写命令时，格式类似，其第 6 字节功能码为 AA，要发的数据附在最后。

表 2 为监控级向过程控制级 0 号单元写一个整数时，解密机接收的来制监控级和过程控制级的信号。表 2 的第 12、13 两字节为写入的整数（一个整数占两个字节），和读的格式一样。过程控制级返回的第 6 字节为校验码。

表 2　为监控级向过程控制级写入信号

信号源＼字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13
来自监控级	01	00	0F	00	02	00	AA	02	00	89	00	00	05	06
来自过控级	00	01	0F	00	02	00	7B							

若在过程控制级改变 PLC 地址号时，不难发现前两个字节表示源和目的的机器编号（00，01）。以上只讲了一些主要的破译过程，共它细节略。

3　结束语

通过以上的模型（硬件和软件）分析，对很多工控网络的通信协议都可以解密。这样根据协议就可以编制异构工控网的通信程序和工控 DCS 的监控程序，把不同的 PLC 工控网进行无缝连接；同时还可以不要厂商的监控级（一般要几十万元），对于大型的控制流程有的要好几台监控机，可想效益是可观的。在实际运用中已达到预期的实效。在自动控制领域具有较高的实用价值和应用前景。

参考文献

1　Yee K S.　Numerical solution of initial boundary value problems involving Maxwell's equations in isotropic media[J].IEEE Trans. Antrnnas and Propagation,1996,14(3):302~307

2　Anthony J,Jim O. Windows 网络编程技术[M].北京：机械工业出版社，2000

［收稿日期：2004.8.5］