第 11 卷第 2 期
1995 年 6 月

广 西 科 学 院 学 报
Journal of the Guangxi Academy of Sciences

Vol. 11, No. 2
Jun., 1995

⑥ 23-29

计算机数字通信数据的截取及通信协议的破译

Intercepting the Data of Computer Digital Communication and Interpreting the Communication Protocol

TN919.3

杨 磊
Yang Lei

（广西计算中心 广西南宁 530022）
(Computing center of Guangxi, Nanning, Guangxi, 530022)

A

摘要 介绍了一种截取计算机数字通信数据的硬件电路和软件程序以及破译通信协议的方法。

关键词 计算机数字通信 数据截取 通信协议 破译 计算机通信 数据通信

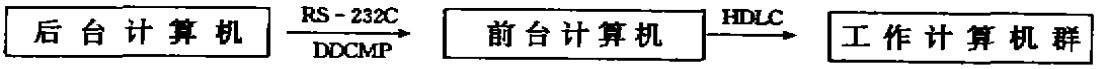
Abstract This paper introduced the hardware and software of intercepting the data of computer digital communication and a method of interpreting the communication protocol.

Key words Computer digital communication, Intercepting data, Communication protocol, Interpreting

计算机数字通信数据的截取及通信协议的破译工作不仅在国防科技上有重大的意义，在经济建设中也常常起着重要的作用。我们曾遇到一套从国外引进的计算机监控系统，其后台机为陈旧且性能不稳定的 FE300 计算机，急需用 PC 机替换。要完成这一工作，首先必须破译原 FE300 与前台机的通信协议。

1 通信数据的截取

原计算机监控系统如图：

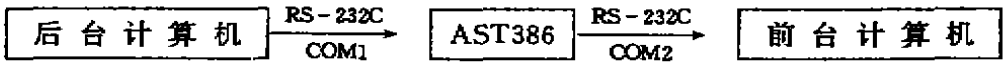


FE300

我们要替换的是 FE300 机及其上的软件系统。原前后台机是以 RS-232C 口连接，双方遵守 DDCMP 协议进行通信。DDCMP 协议只定义了信息的格式，而具体每条信息的意义则

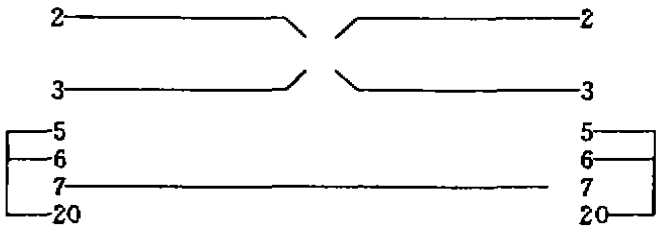
1995-04-18 收稿。

要根据具体的应用来定义。我们所需破译的就是每条信息的实际意义。破译每条信息的意义首先要截取到原前后台机通信的内容，然后根据在通信过程中整个系统的反应来判断每条信息的意义。因为按 DDCMP 协议的通信只有在线路畅通时才能进行下去，故要截取通信内容必须在不影响原前后台机正常通信的情况下进行。经过探索我们找到了这一方法，即用一台 386 计算机插入原前后台机之间（如下图），该机同时接收双方来的信息将它们存入硬盘并转发给另一方，可在保证原通信进行的同时获取通信的内容。



1.1 硬件

AST 386 与后台机和前台机的连线一样的，如下图：



1.2 软件

在 AST 386 上运行的通信软件的设计思想是分别读取两个串口的信息，将其先放在内存并从另一串口转发出去，等到截取的信息到一定数量时再将它们一起做为一个文件存入硬盘。由于两方向的数据传送是同时进行的，因此在存储信息时必需标明其来源。最好的方法是用 00 或 01 表示信息由 COM1 或 COM2 来，并将 00 或 01 做为一个字节存于该信息字节后以标明该字节的来源。例如，先从 COM1 接收到 08 后从 COM2 收到 07，再从 COM1 收到 09 后收到 COM2 的 06，这样存储的信息为 0800070109000601（十六进制）。在读取信息时按两个字节一组即可同时读取信息及其来源。

用汇编语言编写的截取并转发程序名为 YYB.ASM，在 DOS 提示符下可用 C>YYB SJ.DAT 命令执行（SJ.DAT 为用户命名的接收数据的文件名），YYB.ASM 源程序清单如下：

```
STAC    SEGMENT PARA STACK 'STACK'
        DB 256 DUP (0)
STAC    ENDS
DATA    SEGMENT PARA PUBLIC 'DATA'
T11     DB '* * * * 通信系统 * * * * $'
T12     DB '请输入消息数 : $'
FCB     DB 36 DUP (0)
DTA     DB 0
INDA    DB 60010 DUP (0)
;       存放接收数据的缓冲区
COM     DW 1
```

```
NUMB    DW 20000
;       收入字符的个数
MEMBS   DW 1
MEMBE   DW 1
MEMW    DB 0

DATA    ENDS
CODE    SEGMENT PARA PUBLIC 'CODE'
START   PROC FAR
        ASSUME CS: CODE
        PUSH DS
        MOV AX , 0
        PUSH AX
        MOV AX , DATA
        MOV ES , AX
        ASSUME ES: DATA
        MOV SI, 5CH
        MOV DI, OFFSET FCB
        MOV CX, 12
        CLD
        REP MOVSB
        MOV DS , AX
        ASSUME DS: DATA
        MOV AX , DATA
        MOV DS , AX
        ASSUME DS : DATA
; 设置磁盘缓冲区
        MOV DX , OFFSET DTA
        MOV AH, 1AH
        INT 21H
; 打开文件，文件名为执行该软件的命令行中的第一个参数
        MOV DX , OFFSET FCB
        MOV AH, 0FH
        INT 21H
        CMP AL, 0
        JZ CON
        JMP EDD
CON:    MOV WORD PTR FCB+0CH, 0
        MOV WORD PTR FCB+0EH, 1
```

```
        MOV FCB+20H, 0
; 两串口波特率设为 4800
        MOV AH , 0H
        MOV AL , 0C3H
        MOV DX , 0H
        INT 14H
        MOV AH , 0H
        MOV AL , 0C3H
        MOV DX , 1H
        INT 14H
        MOV BX, OFFSET INDA
        MOV MEMBS , BX
        MOV MEMBE, BX
; 设置显示模式
        MOV AH , 0
        MOV AL , 6
        INT 10H
        MOV AX , 600H
        INT 10H
        MOV DH , 1
        MOV DL , 1
        MOV AH , 2
        MOV BH , 0
        INT 10H
; 显示提示
        MOV AH , 9
        MOV DX , OFFSET T11
        INT 21H
        MOV DH , 1
        MOV DL , 40
        MOV AH , 2
        MOV BH , 0
        INT 10H
        MOV AH , 9
        MOV DX , OFFSET T12
        INT 21H
        MOV AH , 0CH
        MOV AL , 08H
        INT 21H
```

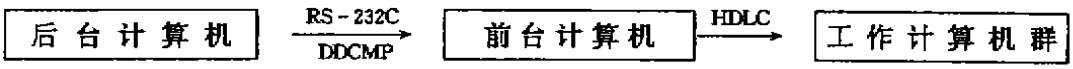
```
        MOV BX, OFFSET NUMB
        SUB AH, AH
        MOV DH , 2
        MOV DL , 1
        MOV AH , 2
        MOV BH , 0
        INT 10H
        MOV BX, OFFSET INDA
REPP:
RE:
; 读串行口状态
        MOV AH, 3
        SUB DX, DX
        MOV DL , BYTE PTR COM
        INT 14H
        AND AH, 1
        CMP AH , 1
        JE GOO
; 有输入则跳到 GOO 处理，否则读取另一串行口状态
        XOR BYTE PTR COM , 1
        JMP RE
GOO:
; 读取串行口输入
        MOV AH , 02H
        SUB DX, DX
        MOV DL , BYTE PTR COM
        INT 14H
; 将读入的内容及串口号写入内存单元
        MOV BYTE PTR [BX], AL
        INC BX
        MOV BYTE PTR [BX], DL
        INC BX
; 将该串口读入的内容从另一串口转发出去
        MOV AH, 1H
        XOR DL, 1
        INT 14H
        MOV AX, NUMB
        DEC AX
        JZ EDDS
```

```
; 接收不够 20000 个字符则跳回 REPP 继续接收下一字符，否则跳出循环
; 到 EDDS
        MOV NUMB, AX
        JMP REPP
EDDS:   MOV BYTE PTR [BX], 0FEH
        MOV MEMBE, BX
        MOV AX, OFFSET INDA
; 将 40000 个字节写入文件，文件名为执行该软件的命令行中的第一个参数
        MOV DX, 40000
RTN:    PUSH DX
        MOV BX , AX
        MOV DL, BYTE PTR [BX]
        PUSH AX
        MOV AL, DL
        PUSH CX
        MOV CL , 4
        SHR AL , CL
        ADD AL , 30H
        PUSH AX
        PUSH CX
        PUSH DX
        PUSH BX
; 将字符写入文件
        MOV BX, OFFSET DTA
        MOV [BX], AL
        MOV DX, OFFSET FCB
        MOV AH, 15H
        INT 21H
        POP BX
        POP DX
        POP CX
        POP AX
        MOV AL, DL
        SHL AL, CL
        SHR AL, CL
        ADD AL, 30H
        PUSH AX
        PUSH CX
        PUSH DX
        PUSH BX
; 将字符写入文件
        MOV BX, OFFSET DTA
```

```
        MOV [BX], AL
        MOV DX, OFFSET FCB
        MOV AH, 15H
        INT 21H
        POP BX
        POP DX
        POP CX
        POP AX
        POP CX
        POP AX
        INC AX
        POP DX
        DEC DX
        CMP DX, 0
        JNZ RTN
; 未写够 40000 个字符则循环
; 将最后字符写入文件
        MOV BX, OFFSET DTA
        MOV BYTE PTR [BX], 1AH
        MOV DX, OFFSET FCB
        MOV AH, 15H
        INT 21H
; 将文件关闭存入硬盘
        MOV DX, OFFSET FCB
        MOV AH, 10H
        INT 21H
EDD:    NOP
        RET
START   ENDP
CODE    ENDS
        END START
```

2　通信协议的破译

用前面介绍的方法可得到前后台机通信的内容。用它对照通信过程中整个系统的反应，经过反复的实验和研究，我们最终破译了每条信息的意义，并按原来协议开发出新的软件系统，成功地用一台 AST 386 替换 FE 300。新的系统结构图如下：



AST386