

基于 WINPCAP 的 GOOSE 报文捕获分析系统研究

张 晔

(无锡供电公司, 江苏 无锡 214000)

摘 要: WinPcap(Windows packet capture)网络开发包是一个免费、基于 Windows 平台、访问网络链路层的工业标准工具, 它允许各种应用程序绕过协议栈捕捉并传送网络数据包。基于 WINPCAP, 可以很方便地开发面向通用对象的变电站事件(GOOSE)报文的捕获分析系统, 本文介绍了整个系统的设计思路以及实现方法, 该系统可以捕获以太网中的 GOOSE 报文, 进而根据 ASN.1/BER 对报文进行解码并分析。

关键词: 变电站自动化; WinPcap; GOOSE; 报文捕获

0 引言

面向通用对象的变电站事件(GOOSE)是 IEC61850 标准的一个亮点, 其出发点是功能的分布式实现^[1]。GOOSE 的应用是一个较为繁琐的工程, 在实际工程调试过程中, 对 GOOSE 报文的解析是一个必不可少的步骤, 主要包括跳闸命令准确性以及时间特性。因此, 开发一个捕获和分析 GOOSE 报文的系统是非常有必要和有价值的。

WinPcap(Windows packet capture)网络开发包是一个免费、基于 Windows 平台、访问网络链路层的工业标准工具, 它允许各种应用程序绕过协议栈捕捉并传送网络数据包, 同时还包括一些其他功能, 如包过滤、网络流量统计以及远程捕获等。此外, 由于 WinPcap 中还提供了发送以太网原始数据包的功能, 因而它非常适合于开发 GOOSE 报文的捕获分析系统^[2]。本文介绍了整个系统的设计思路以及实现方法, 该系统可以捕获以太网中的 GOOSE 报文, 进而根据 ASN.1/BER 对报文进行解码并分析。

1 技术选择

1.1 以太网络的控制

本系统是基于以太网的应用程序, 其很重要的一个方面就是对于以太网层的控制操作, 这是其他上层应用的一个重要基础。

由于 GOOSE 数据包都是直接建立在以太网链路层之上的, 在 ISO 7 层协议中与 IP 协议处于同等的位置, 因而不能使用 TCP/IP 协议发送和接收, 必须

采用更底层的以太网通信函数——WinPcap。

WinPcap 有捕获数据包、发送数据包、统计网络流量 3 个主要功能。捕获数据包的基本流程如下:

(1) 通过接口函数 `pcap_findalldevs_ex` 枚举所有可用的网络设备。

(2) 根据枚举返回的网络设备名称打开一个设备, 对应接口函数为 `pcap_open()`。

(3) 如果需要, 设置数据包的过滤条件, 对应接口函数为 `pcap_setfilter`。

(4) 捕获原始的数据包, 有 2 种方法: 一种方法是以回调函数的方式由接口 `pcap_loop` 或 `pcap_dispatch` 完成, 其基本方法是底层收集数据包, 当满足一定的条件 (timeout 或者缓冲区满), 就调用回调函数, 把收集到的原始数据包通过数据缓存区交给用户; 另一种方法是 `pcap_next_ex()` 的方法, 每当一个包到达以后, 接口 `pcap_next_ex()` 就会返回, 返回的数据缓冲区中只包含一个包。本文中采用 `pcap_next_ex` 的方法^[2]。

1.2 开发平台的选取

Visual C++6.0 是微软公司基于 C++ 语言的一套面向对象的功能强大的 IED 可视化快速开发工具。它提供了面向对象的应用程序框架 MFC(Microsoft Foundation Class: 微软基础类库), 大大简化了程序员的编程工作, 提高了模块的可重用性。Visual C++ 可以帮助用户直观地、可视地设计程序的用户界面, 可以方便地编写和管理各种类, 维护程序源代码, 提高了开发效率^[3-4]。

同时 Visual C++6.0 对于系统底层有着很好的

兼容性，在开发中低层的调用十分方便。因此，本文使用 Visual C++6.0 来开发本系统。

2 GOOSE报文解析

GOOSE解包的最关键部分就是关于APDU部分的解析。APDU的解析，主要是对于Control Block Reference、StateNumber、Sequence Number、Test、Config Revision、Needs Commissioning、Number

Dataset Entries的解析。其中每一部分在数据包中均是以“标识”+“后续数据长度”+“数据”的形式体现的。“标识”依次为：0x80、0x81、0x82、0x83、0x84、0x85、0x86、0x87、0x88、0x89、0x8A。在程序中设置了一个字符型的指针data，指向APDU部分的第一个字节，依次把每一部分解析出来^[5-7]。
GOOSE报文帧结构^[8-10]如图 1 所示。

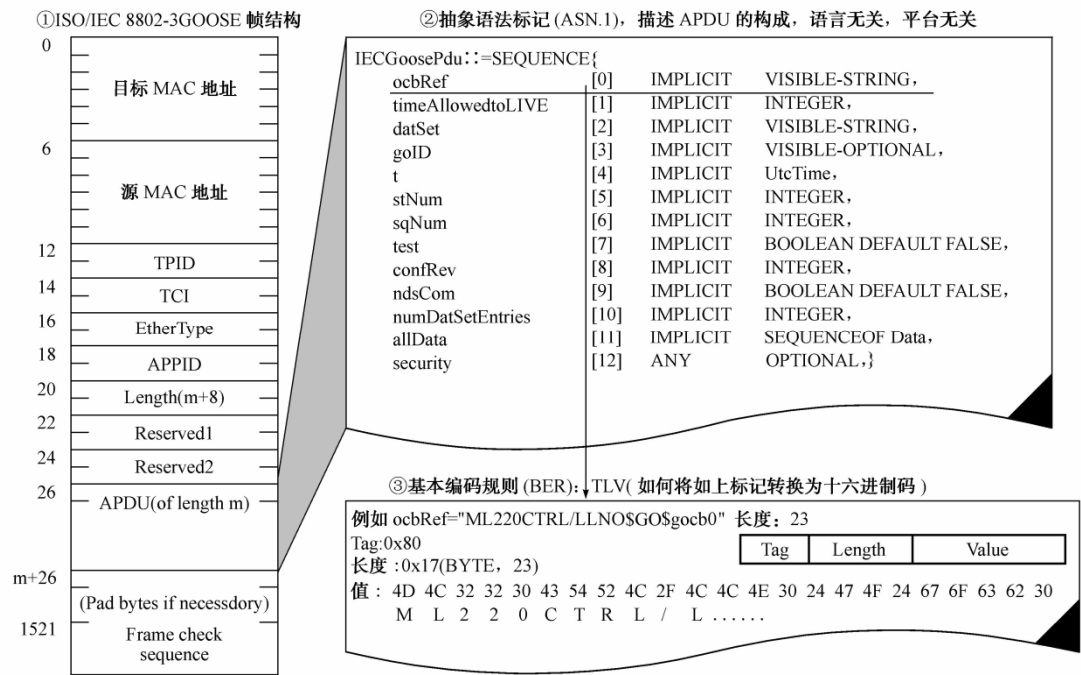


图 1 GOOSE 数据帧结构及解析

3 程序设计与开发

3.1 帧头结构定义

由于 GOOSE 报文帧头部分长度固定，可以使用一个结构来与之对应：

```
struct ListData
{
    char ID[10];
    char TotalPacket[10];
    bool Falg;
    char ethertype[20];
    char src_mac[19];
    char dst_mac[19];
    char Len[10];
    char ASDU[64];
    char packet[127];
    char fourier[600];
};
```

};
3.2 程序流程

- (1) 程序首先进行初始化，包括可用的网卡信息和捕获的数据包信息。
- (2) 然后，程序可以列举可用网卡信息，实现函数为：
if (pcap_findalldevs(&AllDevs, errbuf) == -1)
用户可以通过网卡选择按钮来选择准备使用的网卡，
- (3) 在获取可用的网络设备之后，程序先通过接口函数 pcap_open_live 打开网络接口设备，实现函数为：
if((adhandle=pcap_open_live
(this2->AdapterName,65536,1 ,10,errbuf)) == NULL)
- (4) 调用 pcap_next_ex 捕获以太网数据，实现函数为：

```
res=pcap_next_ex(adhandle,&header,&data);
```

每当捕获到一个数据包时，接口函数 pcap_next_ex 就会返回，然后启动 GOOSE 报文过滤机制，如果报文类型 EtherType 为 0x88B8，则通过消息将数据回传给界面线程。界面线程便会将其显示在列表中。

(5) 如果用户点击此条报文，程序将按照协议将GOOSE报文原文和解析结果一起显示出来，包括以太网帧长度，源MAC地址，目的MAC地址，以太网类型，报文时标及品质，以及开关动作命令^[11-12]。

程序流程框图和报文解析结果如图 2、3 所示。

程序流程框图和报文解析结果如图 2、3 所示。

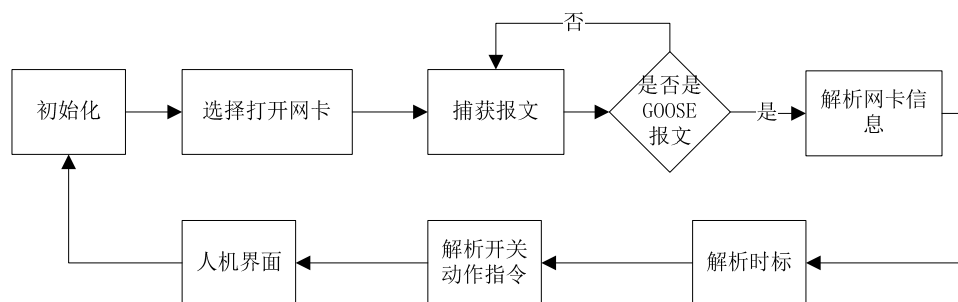


图 2 程序流程框图

报文内容	报文解析
FF FF FF FF FF FF 23 5A -- A0 B3 5F E5 88 B8 00 01	以太网帧长度:284
01 0E 00 00 00 00 61 82 -- 01 02 80 07 67 6F 63 62	源MAC地址:23:5A:A0:B3:5F:E5
52 65 66 81 05 00 00 00 -- 4E 20 82 07 64 61 74 61	目的MAC地址:FF:FF:FF:FF:FF:FF
53 65 74 83 04 67 6F 49 -- 64 84 08 49 1B FA 8A AF	以太网帧类型:IEC GOOSE
5C 28 00 85 05 00 00 00 -- 00 01 86 05 00 00 00 00	时标:2008-11-13 9:59:38.957917 timequality:00
07 87 01 00 88 05 00 00 -- 00 00 01 89 01 00 8A 05	BOOLEAN:0
00 00 00 00 1E AB 81 84 -- 83 01 00 84 03 03 00 00	时标:2008-11-13 9:59:39.915835 timequality:00
91 08 49 1B FA 8A AF 5C -- 28 00 83 01 00 84 03 03	BOOLEAN:0
00 00 91 08 49 1B FA 8A -- AF 5C 28 00 83 01 00 84	时标:2008-11-13 9:59:40.873752 timequality:00
03 03 00 00 91 08 49 1B -- FA 8A AF 5C 28 00 83 01	BOOLEAN:0
00 84 03 03 00 00 91 08 -- 49 1B FA 8A AF 5C 28 00	时标:2008-11-13 9:59:41.831670 timequality:00
83 01 00 84 03 03 00 00 -- 91 08 49 1B FA 8A AF 5C	BOOLEAN:0
28 00 83 01 00 84 03 03 -- 00 00 91 08 49 1B FA 8A	时标:2008-11-13 9:59:42.789587 timequality:00
AF 5C 28 00 83 01 00 84 -- 03 03 00 00 91 08 49 1B	BOOLEAN:0
FA 8A AF 5C 28 00 83 01 -- 00 84 03 03 00 00 91 08	时标:2008-11-13 9:59:43.747505 timequality:00
49 1B FA 8A AF 5C 28 00 -- 83 01 00 84 03 03 00 00	
91 08 49 1B FA 8A AF 5C -- 28 00 83 01 00 84 03 03	

图 3 GOOSE 报文解析

4 结束语

GOOSE 报文解析是数字化变电站继电保护调试的主要手段，本文基于 WinPcap 开发了 GOOSE 报文的捕获分析系统。

首先研究了 WinPcap 开发包网络控制的数据抓包的技术细节，提出了实现方案。然后分析了 IEC61850 规约中 GOOSE 原理及报文结构，并通过实际报文对照加以印证。最后使用 Visual C++6.0 进行程序的编写和功能的实现。

经验证，该系统能够捕获以太网中的 GOOSE 报文，进而能够根据 ASN.1/BER 对报文进行解码并分析，在实际工程调试过程中有着巨大应用潜力。

本文研究还存在很多有待深入探索的问题，比如可以在本文的技术原理基础上完成该系统向嵌入式开发平台的移植，实现一套完善的手持式 GOOSE 测试工具，甚至于完成此工具的产品化研究。本文旨在研究该方案的可行性程度，并给相关研究提供技术性参考，希望能对中国的数字化变电站建设做出贡献。

参考文献：

- [1] IEC 61850 Communication networks and system in substation[S]. 2004.
- [2] WinPcap:The Windows packet capture Library[EB/OL].[2007-06-28].<http://www.winpcap.org/>.
- [3] 孙鑫，余安萍. VC++深入详解[M].北京：电子工业出版社。

版社, 2006.

- [4] 雷斌, 杨建华, 黄超, 等. Visual C++6.0 网络编程技术[M].北京: 人民邮电出版社, 2000.
- [5] 范建忠,马千里. 基于 WINPCAP 的 GOOSE 报文捕获分析工具开发[J]. 电力系统自动化,2007,31(23):52-56.
- [6] 何仰赞,温增银. 电力系统分析(第三版)[M].武汉:华中科技大学出版社, 2002.
- [7] 殷志良,刘万顺,杨奇逊,等. 基于 IEC61850 的通用变电站事件模型[J]. 电力系统自动化, 2005, 29 (19): 45-50.
- [8] 王松,陆承宇. 数字化变电站继电保护的 GOOSE 网络方案[J].电力系统自动化, 2009, 33 (3): 51-54.
- [9] 窦晓波,周旭峰,胡敏强,等. IEC 61850 快速报文传输服

务在 VxWorks 中的实现[J]. 电力系统自动化, 2008, 32(12): 43-44.

- [10] 范建忠,马千里. GOOSE 通信与应用[J]. 电力系统自动化,2007,31(19): 85-90.
- [11] 张世强. 基于 61850 规约的保护装置 GOOSE 报文测试工具的开发[D]. 保定: 华北电力大学,2009.
- [12] 李慧萍,鲁晓帆,张凯. 基于 WinPcap 的数据包捕获技术的研究[J]. 网络安全技术与应用, 2010(8): 31-32.

作者简介:

张 晔(1979-), 女, 江苏泰州人, 工程师, 现在江苏无锡供电公司从事供用电管理工作, E-mail : zhang_ye1111@hotmail.com。