

基于Wireshark的智能变电站MMS告警功能设计及实现

王 宇, 栾庆武, 岳 蔚

(国电南瑞科技股份有限公司, 江苏 南京 211106)

摘要: Wireshark 是一款强大的网络协议分析开源的跨平台软件, 几乎包含了所有主流的网络通信报文, 但对于智能变电站, 其在 MMS 报文分析方面仍有很多不足。通过分析 Wireshark 的设计架构、处理流程、MMS 服务及帧格式等, 给出了基于 Wireshark 开发的适用于智能变电站的 MMS 告警功能的方案及实现过程, 展示了基于该方案的 MMS 告警功能的运行结果, 达到了预期目的。基于开源软件进行二次开发, 为开源软件在电力系统中的应用提供了一种新的思路, 对于智能变电站的通信协议分析 also 具有重要意义。
关键词: 智能变电站; Wireshark; MMS 报文; BER 编码

Design and development of MMS alarm function of intelligent substation based on Wireshark

WANG Yu, LUAN Qingwu, YUE Wei

(NARI Technology Co.,Ltd., Nanjing 211106, China)

Abstract: Wireshark is a powerful open source cross platform software for network protocol analysis, Almost all mainstream network communication messages are included, But for intelligent substation, there are still many deficiencies in MMS message analysis. By analyzing the design architecture and processing flow of Wireshark, MMS service and frame format, the scheme and development process of MMS alarm function for intelligent substation developed based on Wireshark are given, and the operation results of MMS alarm function based on this scheme has achieved the expected purpose. This design is based on the secondary development of open source software, which provides a new idea for the application of open source software in power system, and is also of great significance for the analysis of communication protocols in intelligent substations.

Key words: intelligent substation; Wireshark; MMS packet; BER code

0 引言

华东电网公司于2007年在国内率先开展了智能电网可行性研究^[1], 2009年3月国家电网提出要“建设坚强的智能电网”^[2], 智能电网逐渐成为国家电网发展的一个新方向^[3]。IEC 61850标准凭借其开放性、互操作性和扩展性等特点成为智能电网信息通信体系的重要组成部分

分^[4]。制造报文规范 (Manufacturing Message Specification, MMS) 是由国际标准化组织 (ISO) 工业自动化技术委员会ISO/TC184开发的智能设备间交换实时数据和监控信息的一套独立的国际报文规范^[5], 是应用层的一个协议标准, 主要用于生产设备间控制信息的传送^[6]。为制造设备入网方便, IEC 61850标准把

MMS引入电力系统自动化中,将间隔层及变电站层的通信采用抽象通信服务接口(Abstract Communication Service Interface, ACSI)映射到MMS^[7]。MMS服务建立过程中存在链路初始化失败问题,信息交互过程中存在误码、丢包和流量突发等问题^[8],这些都影响到智能变电站的稳定运行。Wireshark是一款免费开源的应用较为广泛的网络协议分析软件^[9],在智能变电站网络协议分析中得到广泛应用。Wireshark内置的通信协议分析器可对智能变电站中使用到的SNTP、PTP、IEC104协议、GOOSE协议、SV协议和MMS协议等进行嗅捕、分析,但在分析方面仍存在一些不足。例如不能对协议状态进行判断,不能对MMS报文中某些语义异常进行判断^[10],不能按客户端/服务器端统计报文帧及流量等,智能变电站中应用Wireshark被这些不足大大限制。本文深入研究了Wireshark协议分析器的两种设计方法及其流程、网络数据包的内容检测方法^[11],在此基础上提出了基于Wireshark的MMS报文分析功能的方法,并针对性地进行设计及实施,最后对有效性进行验证。

1 Wireshark分析

Wireshark是一款强大的网络协议分析开源的跨平台软件^[12],是一个遵循在GNU GPL许可证的开源网络协议分析软件^[13],在许可证保障范围内,使用者可以获得免费的源代码,并拥有对源代码进行修改及定制化的权利。目前Wireshark拥有的协议分析器超过1 700种,所有重要的网络通信协议几乎都包含其中。

1.1 Wireshark架构

Wireshark是模块化设计,架构如图1所示^[14],包括8个功能模块。

GUI:图形组块,用于参数输入、分析展示等。Wireshark支持GTK和Qt两种工具对图形窗口进行开发。

CORE:核心组块,采用调用函数的方法连接其他模块。

Epan:数据包分析引擎,包括4个子模块^[15]

(Protocol-Tree、Dissectors、Dissectors-Plugins和Displays-Filters),新的协议分析器放在该模块中。

Wiretap:读写捕获的报文文件,读写格式包括libpcap、pcapng或者其他类型的文件格式。

Capture:抓包引擎接口,从底层网络捕获数据包,通用的捕获接口由WinPcap提供,能从多种网络类型的接口(包括ATM网、令牌环网和以太网等)抓捕数据包。

Dumpcap:捕捉引擎组块,对报文进行捕捉,执行需要提升权限。

WinPcap:不同平台的包捕捉以及过滤支持功能库,支持Linux和Windows系统。

Utilities:共用组块,提供处理时间、字符等函数。

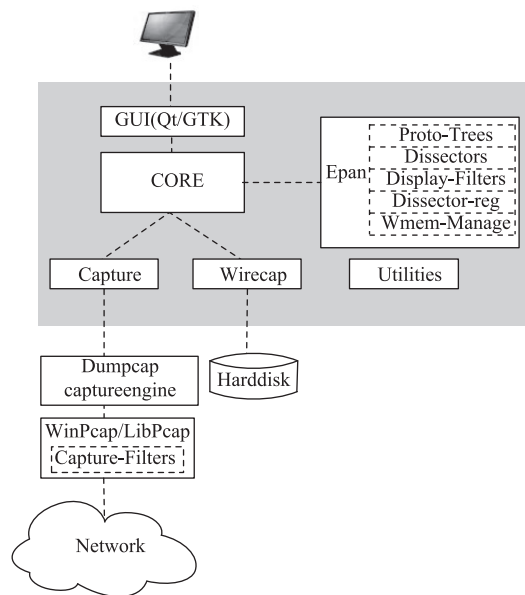


图1 软件架构

Fig. 1 Software architecture

1.2 Wireshark流程分析

Wireshark在分析前先进行初始化,初始化包括部分全局变量初始化、GTK初始化和协议分析器初始化等,Epan模块是初始化的重点。

Wireshark初始化结束后进入报文处理流程,程序把捕获的报文写入临时文件。解析处理时,程序依次从包列表读取数据包,并将从数据包中提取的数据写在数据结构中,Wireshark以

一棵协议树的形式对数据进行分析，一个协议的上级节点为父节点，具有相同父节点的协议成为兄弟节点，Wireshark采用协议的特征字识别拥有同样父协议的兄弟节点协议^[16]。解析顺序为Frame层、Ethernet层、IP层、TCP层和应用层。

核心ACSI通信协议栈主要采用的是基于MMS+OSI+TCP/IP+以太网的协议栈实现通信，即ACSI对象和服务模型映射到MMS的对象和服务模型^[17]。

MMS规范位于ISO/OSI七层模型的第七层应用层，是一个非常庞大的协议集。

MMS基于TCP/IP连接的传输机制，传输过程包括TCP/IP应用层（对应OSI的应用层、表示层、会话层），服务器端口号102，对应关系如

图2所示。



图2 TCP/IP结构与OSI模型对照

Fig. 2 Comparison of TCP / IP structure and OSI model

在应用层解析阶段，程序根据编码规则逐级拆解，最终解析到MMS报文，至此全部报文解析结束。

以图3所示的MMS原始报文为例，程序依次对报文进行解析，解析完成一个层次就会建立一个节点链表，如图4所示。

字节	原始报文															
0000	EC ^[b4]	8E	B5	A7	65	A1	B4	4C	C2	64	66	0D	08	00	45 ^[b2]	00
0010	00	8F	AE	6C	40	00	40	06	AA	C3	0A	64	66	0D	0A	64
0020	66	64	00 ^[b3]	66	E5	D5	59	38	A3	6E	7C	67	92	57	50	18
0030	07	D3	10	07	00	00	03 ^[b4]	00	00	67	02 ^[b5]	F0	80	01 ^[b6]	00	01 ^[b7]
0040	00	61 ^[b8]	5A	30	58	02	01	03	A0 ^[b9]	53	A3 ^[b10]	51	A0 ^[b11]	4F	A0 ^[b12]	27
0050	30	25	A0 ^[b13]	23	A1 ^[b14]	21	1A ^[b15]	0C	43	42	31	30	30	30	31	33
0060	43	54	52	4C	1A ^[b16]	11	43	53	57	49	33	24	43	4F	24	50
0070	6F	73	24	4F	70	65	72	A0 ^[b17]	24	A2 ^[b18]	22	83 ^[b19]	01	00	A2 ^[b20]	09
0080	85	01	02	89	04	13	D5	C0	07	86 ^[b21]	01	00	91 ^[b22]	08	5D	81
0090	92	6F	0B	A5	E3	3F	83 ^[b23]	01	00	84 ^[b24]	02	06	00			

图3 MMS 报文

Fig. 3 MMS packet data

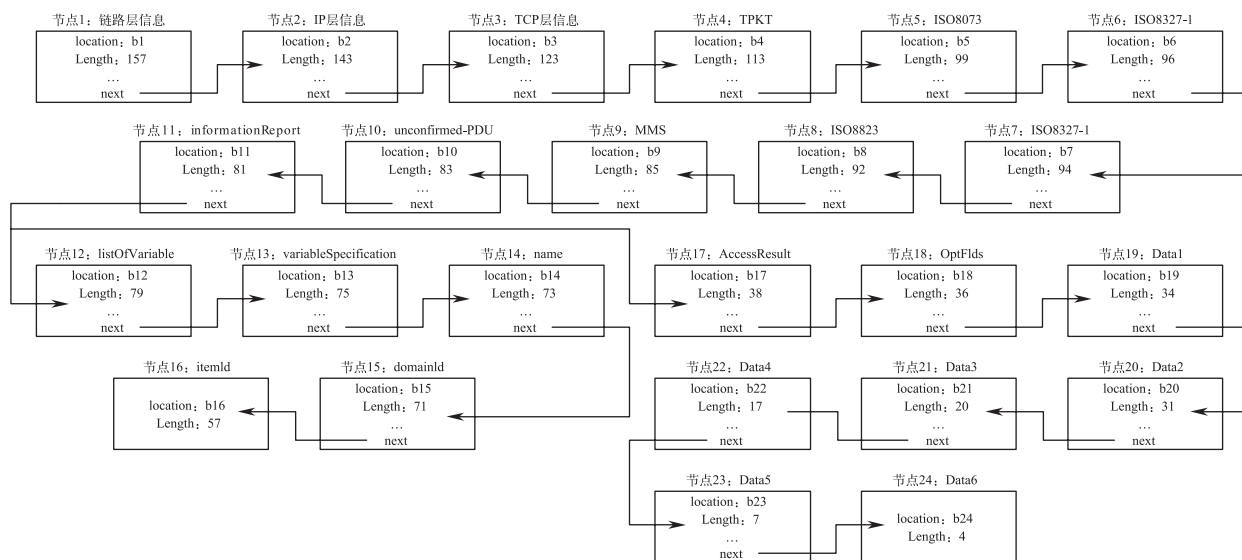


图4 节点链表图

Fig. 4 Link structure

2 MMS服务及帧格式

IEC 61850标准是由2004年国际电工委员会(IEC)TC57工作组指定的全球唯一的变电站自动化设备互操作的通信标准^[18]。IEC 61850在电力系统中的应用需要具有强壮的实时的底层通信协议的支持,并且能够传输复杂的自描述的可扩展的数据信息,目前ISO/IEC 9506制造报文规范(MMS)是唯一的有能力支持IEC 61850的国际标准^[19]。为保证ACSI的独立性以及适应未来的网络技术发展的变化,IEC 61850协议中并没有具体指定实现ACSI的方法,只提供特殊通信服务映射描述过程^[20],映射关系如图5所示。

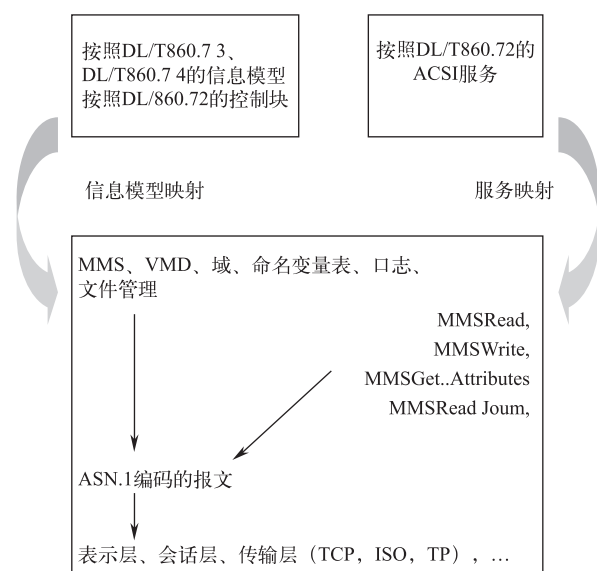


图5 映射到 MMS 示意图

Fig. 5 Map to MMS diagram

MMS采用ASN.1及其基本编码规则(BER)作为数据结构定义描述工具与传输语法^[21]。

利用BER编码得到的结果可以在任何支持字节流(Strings of Octets)的通信介质中传输。正如ASN.1是层次结构化的一样,BER也遵循这种层次嵌套结构。编码是按照类型(Type)、长度(Length)和值(Value)的顺序进行^[22],一般称为TLV结构。数据单元传送的重要信息包含在值(Value)中,它可以是递归的,支持TLV结构的嵌套,结构如图6所示。

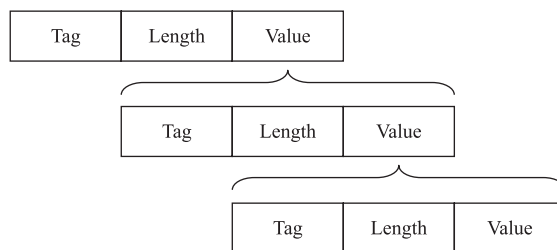


图6 TLV递归结构

Fig. 6 TLV recursion structure

3 设计方案及实现

Wireshark对MMS报文解析的主要问题体现在不能对MMS语义上的异常进行识别并输出告警信息。

要克服上述问题,要求对Wireshark的功能进行扩展,扩展的功能如下:增加从SCD文件中解析出MMS配置的功能;根据配置及异常判断逻辑进行判断并输出告警信息的功能。

依据Wireshark框架,新增模块在程序中的位置如图7所示。

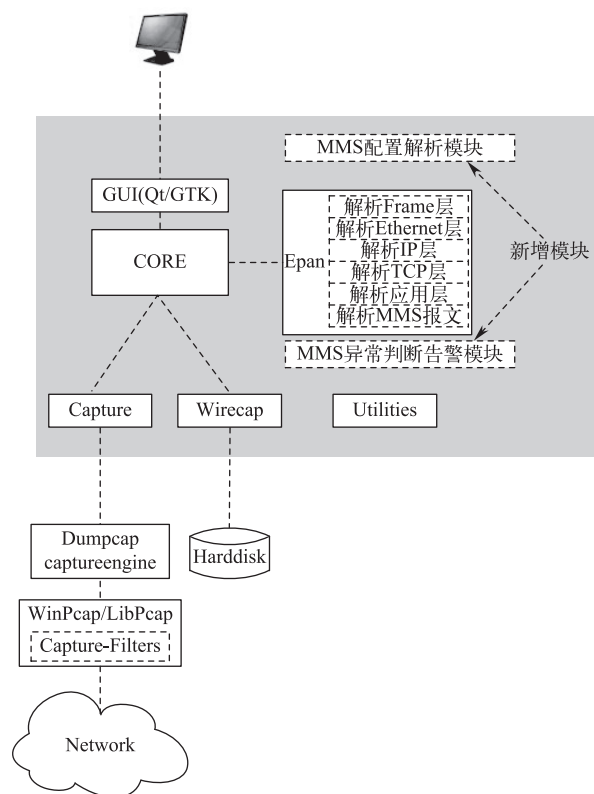


图7 新增模块示意图

Fig. 7 Schematic diagram of new module

3.1 MMS配置解析模块

智能变电站SCD包含了全站IED的实例配置和通信参数、IED间通信配置及变电站一次系统结构^[23]，在智能变电站工作中SCD文件的建模是由系统集成厂商完成的，SCD文件包含每个装置的CID信息^[24]。

MMS配置解析模块的功能就是从中解析出MMS控制块的相关信息，以供MMS异常判断及告警模块使用，具体获取信息见表1。

表1 MMS控制块信息

Tab. 1 MMS control block information

序号	名称	备注
1	所属网络	SCD 读取
2	IED name	SCD 读取
3	IED desc	SCD 读取
4	端口序号	SCD 读取
5	rptID	SCD 读取
6	Dataset1 ref	SCD 读取
7	TrgOps	SCD 读取
8	数据集成员 1 信息	成员 1 通道描述 SCD 读取
		成员 1ref SCD 读取
		成员 1 类型 SCD 读取
		⋮
<i>n</i>	数据集成员 <i>n</i> 信息	成员 <i>n</i> 通道描述 SCD 读取

SCD模型文件是标准的XML格式文件，有相关的XSD文件进行语法约束^[25]。若想从一个复杂的XML文件中提取信息，需要具备对SCD模型文件的快速解析能力。为了快速地解析SCD文件，选用了Qt提供的QtXml模块完成对SCD文件的解析。

3.2 异常判断及告警模块

Wireshark只是判断MMS报文的语法方面的错误，例如无效数据类型、MMS报文长度错误、类型错误和不符合TLV编码规则等，但并没有对MMS报文一些语义上的异常作出判断，见表2。

为实现以上异常判断，另定义异常识别模块。本模块在解析完成后从MMS规约tree结构中获取当前帧的各个层次或字段解析后的信息，包括DomainId、ItemId、ListOfData、

DataAccessError、ListOfAccessResult和WrRspItem等，tree的结构为：

```
typedef proto__node {
    proto__node *first__child; // 首子节点
    proto__node *last__child; // 尾子节点
    proto__node *next; // 下一个子节点
    proto__node *parent; // 父子节点
    field__info *finfo; // 字段信息
    tree__data_t *tree_data;
} proto__node;
```

表2 MMS异常

Tab. 2 Abnormal MMS

序号	名称
1	修改定值失败
2	修改定值组失败
3	初始化 BufTm 异常
4	初始化 ConfRev 异常
5	初始化 EntryID 异常
6	初始化 IntgPd 异常
7	初始化 OptFlds 异常
8	初始化 TrgOps 异常
9	遥控失败

程序首先创造树根，随后进行逐层解析，在层层解析中逐次创建首字节节点、尾字节节点及下一个节点等，最终形成树形结构。

为了不破坏原解析模块，本开发新增全局变量g_tMMSInfo，数据成员为：

```
typedef struct Dissector_Info
{
    TimeInterval tTimestamp; // 时间戳
    Report tReportData;
    TagDatSet DatSet;
    GPtrArray *pDomainIds;
    GPtrArray *pItemIds;
    GPtrArray *pListOfData;
    GPtrArray *pDataAccessErrors;
    GArray *pFailures;
    GArray *pListOfAccessResults;
    GArray *pWrRspItems;
    int nPortId; // 端口号
```

```
int      nMMSpdu; // pdu类型
.....

unsigned short    nSrcPort;
unsigned short    nDstPort;
unsigned char    cSrcMac[6];
unsigned char    cDstMac[6];
unsigned char    cSrcIP[4];
unsigned char    cDstIP[4];
} Dissector_Info_t;
```

增加获取信息模块，MMS报文解析结束后将树形结构中获取MMS相关信息填入增加获取信息模块。

增加异常判断及告警模块，在获取信息后对异常进行判断，当异常发生时发出告警。

程序总流程图及新增模块位置如图8所示。

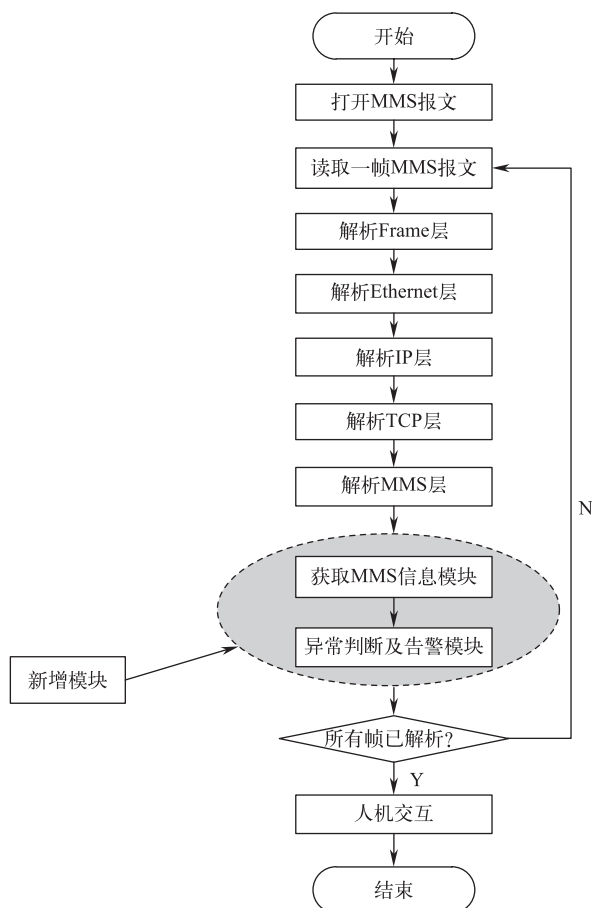


图8 总流程图及新增模块位置
Fig. 8 Flow chart and new module location

4 结果展示

MMS异常分析结果如图9~图17所示，包括修改定值失败、修改定值组失败、BufTm初始化异常、ConfRev初始化异常、EntryID初始化异常、IntgPd初始化异常、optFlds初始化异常和遥控失败。

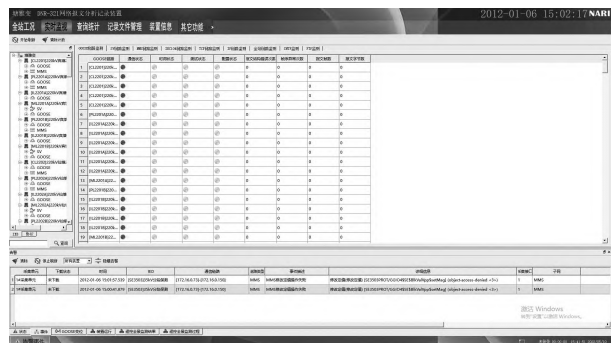


图9 修改定值失败
Fig. 9 Modified setting value failed

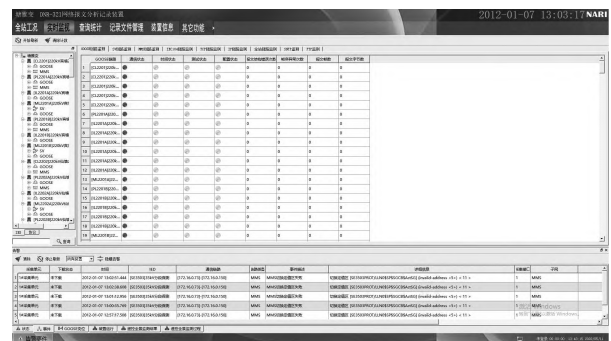


图10 修改定值组失败
Fig. 10 Modified setting value group failed

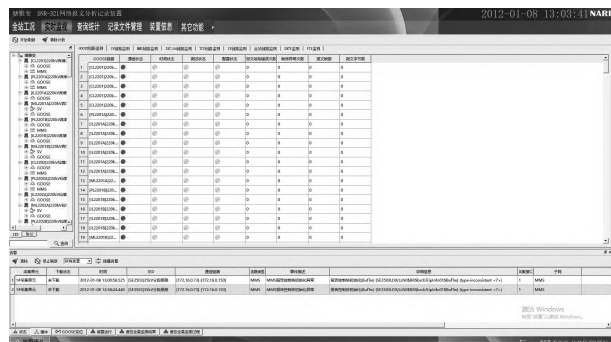


图11 BufTm 初始化异常
Fig. 11 BufTm abnormal initialization

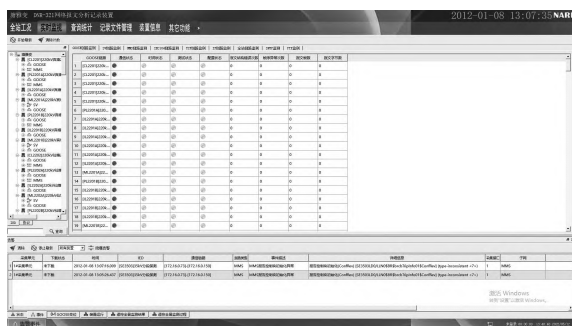


图 12 ConfRev 初始化异常

Fig. 12 ConfRev abnormal initialization

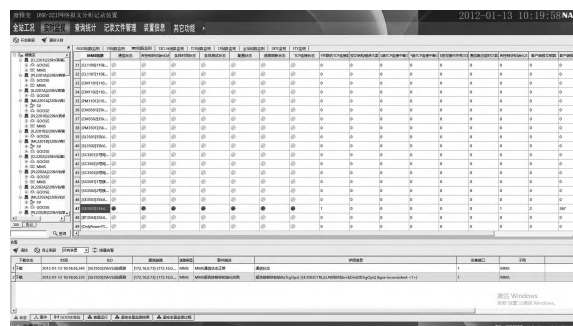


图 16 TrgOps 初始化异常

Fig. 16 TrgOps abnormal initialization

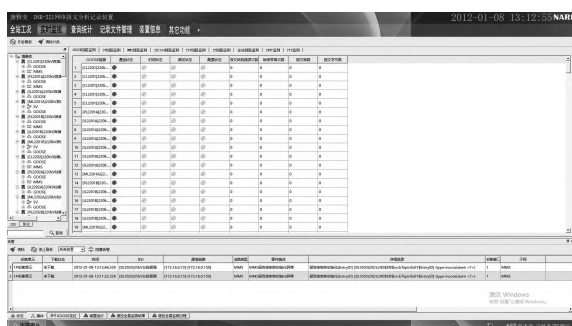


图 13 EntryID 初始化异常

Fig. 13 EntryID abnormal initialization

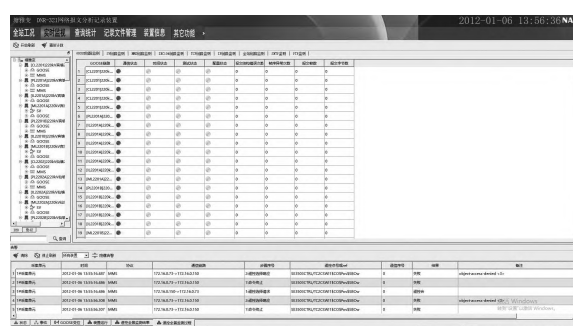


图 17 遥控失败

Fig. 17 Remote control failed

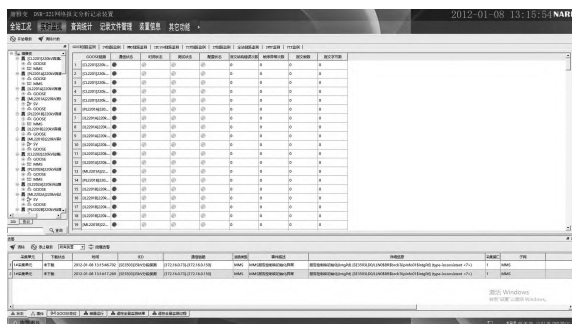


图 14 IntgPd 初始化异常

Fig. 14 IntgPd abnormal initialization

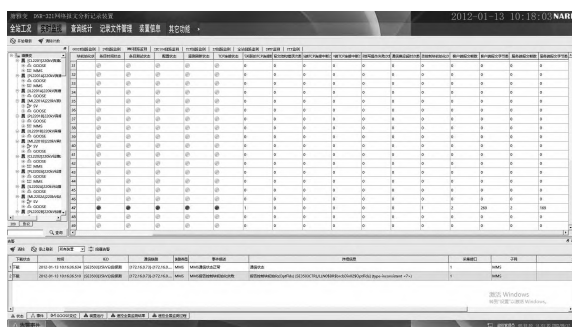


图 15 optFlds 初始化异常

Fig. 15 OptFlds abnormal initialization

5 结束语

基于Wireshark开发的MMS报文分析及告警程序能准确地分析MMS报文，并就各种异常情况作出判断。该软件已经在工程现场得到大量应用，并得到调试人员的肯定。本设计拓宽了在Wireshark基础上进行再次开发的思路，为Wireshark在电力系统中的应用提供了一种新方向。接下来，将利用设计思路完成国产化规约CMS（自主可控的新一代变电站通信规约）的解析及异常识别工作，为智能电网的建设提供有力支持。

参考文献

- [1] XIA Changliang, SONG Zhanfeng. Wind energy in China: current scenario and future perspectives[J]. Renewable and Sustainable Energy Reviews, 2009, 13(8): 1966-1974.
- [2] ZHANG S, TSENG King Jet, VILATHGAMUWA

- D M, et al. Design of a robust grid interface system for PMSG-based wind turbine generators[J]. IEEE Transactions on Industrial Electronics, 2011, 58(1): 316-328.
- [3] 胡书举, 李建林, 许洪华. 永磁直驱风电系统变流器拓扑分析[J]. 电力自动化设备, 2008, 28(4): 77-81.
- [4] 帅军庆. 创新发展建设智能电网——华东高级调度中心项目群建设的实践[J]. 中国电力企业管理, 2009(2): 19-21.
- [5] 刘峻, 何世恩. 建设坚强智能电网助推酒泉风电基地发展[J]. 电力系统保护与控制, 2010, 38(21): 19-23.
- [6] 张瑶, 王傲寒, 张宏. 中国智能电网发展综述[J]. 电力系统保护与控制, 2021, 49(5): 180-187.
- [7] 袁安富, 于海, 缪文贵, 等. 智能变电站MMS报文捕获分析的研究与实现[J]. 电测与仪表, 2013, 50(9): 74-78.
- [8] 李紫龙, 叶进, 吕燕石. 制造报文规范在变电站自动化系统中的研究与应用[J]. 低压电器, 2010(12): 21-23, 27.
- [9] 丁力, 王晓茹, 王林. IEC 61850标准中MMS映射分析及其编码/解码模块的设计[J]. 电力系统保护与控制, 2008, 36(12): 69-73.
- [10] 董科, 关彬, 王巍. IEC 61850与MMS的映射的研究[J]. 电力系统保护与控制, 2010, 38(10): 92-95.
- [11] 徐吉用, 廖晓春, 李福, 等. 智能变电站站控层在线监测技术的应用研究[J]. 电力信息与通信技术, 2019, 17(8): 50-56.
- [12] 李忠安, 王娇, 张惠刚, 等. IEC 61850过程层网络通信分析诊断工具设计[J]. 电力系统保护与控制, 2015(1): 93-97.
- [13] 栾庆武, 岳蔚, 周永华. 基于Wireshark的智能变电站SV报文分析工具设计及实现[J]. 电力系统保护与控制, 2019, 47(24): 169-177.
- [14] 罗青林, 徐克付, 臧文羽, 等. Wireshark环境下的网络协议解析与验证方法[J]. 计算机工程与设计, 2011, 32(3): 770-773.
- [15] 王娇, 张惠刚, 李广华, 等. IEC 61850新型网络冗余报文捕获解析工具开发[J]. 电力建设, 2014, 35(10): 84-88.
- [16] 刘隽, 李博. 利用Wireshark查找进程间网络通信问题[J]. 铁路计算机应用, 2015(9): 30-32.
- [17] 朱振乾, 张周晶, 马慧慧, 等. 基于Wireshark与Nmap的工业协议分析与工业漏洞挖掘的实现[J]. 通信技术, 2021, 54(3): 716-726.
- [18] 李江宝. 基于Wireshark开源代码移植的DDS通信应用数据解析实现[J]. 指挥控制与仿真, 2019, 41(5): 116-120.
- [19] 吕雪峰, 张春芳. Wireshark网络协议解析原理与新协议添加方法[J]. 软件导刊, 2011, 10(12): 105-107.
- [20] 孔凤颖, 侯思祖. 基于IEC 61850的MMS报文通信的研究[J]. 电力信息与通信技术, 2013, 11(9): 44-48.
- [21] 井立翠, 李秦伟, 董方. 基于IEC 61850标准的GOOSE信息模型的构建研究[J]. 自动化与仪器仪表, 2012(6): 5-8.
- [22] 林知明, 扬丰萍, 余瑛. IEC 61850到MMS映射分析及实现[J]. 继电器, 2007, 35(2): 64-67.
- [23] 黄文华, 虞善德. IEC 61850标准中ACSI映射实现研究[J]. 现代电子技术, 2011, 34(15): 63-66.
- [24] 王德文, 朱永利, 邸剑, 等. 面向电力系统实时通信的MMS协议[J]. 电力自动化设备, 2009, 29(7): 101-104.
- [25] 范立众, 赵明生. ASN. 1编解码器的JAVA实现[J]. 计算机工程与应用, 2002, 38(10): 175-177.

作者简介

王宇 (1976—), 男, 硕士, 高级工程师, 研究方向为电力系统继电保护和智能变电站。

(收稿日期: 2022-10-11)