(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107547540 B
(45)授权公告日 2020.06.26

(21)申请号 201710760832.7

(22)申请日 2017.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 107547540 A

(43)申请公布日 2018.01.05

(73)专利权人 上海许继电气有限公司
地址 200122 上海市浦东新区浦电路489号由由燕乔大厦11楼
专利权人 许继集团有限公司
国家电网有限公司

(72)发明人 袁同浩 王力 陈浩 黄保莉 高玉宝 沈永良 赵德基 陈鹏 狄军峰 黄小倩 刘裕桦 邬军军 张漪

(74)专利代理机构 上海智信专利代理有限公司 31002
代理人 王洁 郑暄

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

(56)对比文件
CN 101072147 A,2007.11.14,
CN 101572440 A,2009.11.04,
CN 105577705 A,2016.05.11,
US 2016112323 A1,2016.04.21,
CN 106093627 A,2016.11.09,
CN 105656720 A,2016.06.08,

审查员 刘金鑫

权利要求书3页 说明书8页 附图3页

(54)发明名称

IEC-60870-5-104协议报文监控方法

(57)摘要

本发明涉及一种IEC-60870-5-104协议报文监控方法,包括初始化变量、创建报文解析线程、创建决策线程,能够简单方便的对104链路状态进行判断,对实时报文结构进行分析,对遥控和遥信过程进行监控,立即报告严重错误,定期上送统计信息,实现了104协议的全方位监控,提高了通信可靠性。

CN 107547540 B

1.一种IEC-60870-5-104协议报文监控方法,其特征在于,所述的方法包括以下步骤:

(1)初始化变量;

(2)创建报文解析线程;

(3)创建决策线程;

所述的步骤(1)中的初始化为:

将相关变量初始化为零,并清空TCP连接映射表map_link和控制过程映射表map_ctl,其中,所述的相关变量包括报告周期定时器t_rpt、链路通信状态定时器t_commuState、遥测刷新状态定时器t_rfhState[n],其中n表示遥测点数量,主站关闭TCP连接次数n_masterclose、子站关闭TCP连接次数n_slaveclose、遥测数据无效次数n_teleMesInvalid、遥测数据溢出次数n_teleMesOv和遥信数据无效次数n_teleSigInvalid;

所述的步骤(2)中的创建报文解析线程为:

(2.1)读取报文,并取出报文中的链路层报文;

(2.2)在链路层对该链路层报文进行分析,获取网络层报文,并判断该网络层报文是否为IP报文,若是,则进入步骤(2.3),否则返回步骤(2.1);

(2.3)在网络层对该IP报文进行分析,获取传输层报文,并判断该传输层报文是否为TCP报文,若是,则进入步骤(2.4),否则返回步骤(2.1);

(2.4)在传输层对该TCP报文进行分析,获取应用层报文,并判断该应用层报文是否为IEC-60870-5-104报文,若是,则进入步骤(2.5),否则返回步骤(2.1);

(2.5)在应用层对该IEC-60870-5-104报文进行分析,并保存分析结果,返回步骤(2.1);

所述的步骤(2.4)中包括以下步骤:

(2.4.1)在传输层对该TCP报文进行分析,获取该TCP报文的TCP头信息,并判断是否存在TCP连接,若不存在,则新建TCP连接;

所述的TCP连接中包括以下在新建TCP连接时要进行初始化清零的相关变量:

客户端建立请求变量establish_req、服务端确认变量establish_ack、客户端确认变量establish_ackself、释放请求变量release_req、释放确认变量release_ ack、释放再次请求变量release_req2和释放再次确认变量release_ ack2、客户端端口号变量port_client、服务端端口号变量port_serv、连接关闭者变量closer;

新建TCP连接时进行初始化的变量还包括超时计时器t_timeout、客户端IP地址ip_client、服务端IP地址ip_serv,其中,对客户端IP地址ip_client和服务端IP地址ip_serv的初始化均为置空,对超时计时器t_timeout的初始化为将当前时间置为超时计时器t_timeout的初始值;

所述的客户端建立请求变量establish_req、服务端确认变量establish_ack、客户端确认变量establish_ackself、释放请求变量release_req、释放确认变量release_ ack、释放再次请求变量release_req2和释放再次确认变量release_ ack2的值与各变量对应的事件是否发生相关,若各变量对应的事件发生,则置1,否则置0,其中,

客户端建立请求变量establish_req对应TCP连接中发生客户端建立请求这一事件;

服务端确认变量establish_ack对应TCP连接中发生服务端确认这一事件;

客户端确认变量establish_ackself对应TCP连接中发生客户端确认这一事件;

释放请求变量release_req对应TCP连接中发生释放请求这一事件；

释放确认变量release_ ack对应TCP连接中发生释放确认这一事件；

释放再次请求变量release_req2对应TCP连接中发生连续两次释放请求时发生第二次释放请求这一事件；

释放再次确认变量release_ ack2对应TCP连接中发生连续两次释放请求时发生第二释放确认这一事件；

所述的连接关闭者变量closer的值与该TCP连接的连接情况相关，若该TCP连接正常，置0；若该TCP连接由客户端关闭，置1；若该TCP连接由服务端关闭，置2；

所述的步骤(2.5)为：

(2.5.1)判断连接关闭者变量closer的值，若为0，进入步骤(2.5.2)；若为1，子站关闭TCP连接次数n_slaveclose加1，并返回步骤(2.1)，若为2，则主站关闭TCP连接次数n_masterclose加1，返回步骤(2.1)；

(2.5.2)检查IEC-60870-5-104报文的应用服务数据单元ASDU类型标识符，若为遥测报文，则进入步骤(2.5.3)，否则进入步骤(2.5.5)；

(2.5.3)更新遥测点刷新时间t_rfhState[n]，其中n表示第n个遥测点，判断数据遥测数据是否为无效，若是，则令遥测数据无效次数n_teleMesInvalid加1；否则进入步骤(2.5.4)；

(2.5.4)判断遥测数据是否溢出，若是，则令遥测数据溢出次数n_teleMesOv加1；否则进入步骤(2.5.5)；

(2.5.5)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥信报文，则进入步骤(2.5.6)，否则进入步骤(2.5.7)；

(2.5.6)判断遥信数据是否无效，若是，则令遥信数据无效次数n_teleSigInvalid加1，否则进入步骤(2.5.7)；

(2.5.7)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥控报文，则进入步骤(2.5.9)，否则进入步骤(2.5.8)；

(2.5.8)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥调报文，则进入步骤(2.5.9)，否则进入步骤(2.5.11)；

(2.5.9)根据IP报文的IP地址判断是否存在控制过程，若存在，则进入(2.5.10)，否则在新建控制过程后进入(2.5.10)；所述的控制过程中包含主站选择命令变量select_req、子站选择确认命令变量select_ack、主站撤销命令变量cancel_req、子站取消确认变量cancel_ack、主站执行命令变量act_req和子站执行响应变量act_ack，分别代表遥控过程中的实际执行步骤和遥调过程中的实际执行步骤，相应步骤未执行时变量置0，否则置1，控制过程中还包含响应超时计时器t_response和过程超时计时器t_process，新建控制过程时，响应超时计时器t_response和过程超时计时器t_process均设置为当前时间，且该控制过程中的其他变量在新建时均设置为0；

(2.5.10)更新响应超时计时器t_response和过程超时计时器t_process为当前时间，将相应步骤标识变量置1；

(2.5.11)将该IEC-60870-5-104报文与标准报文格式进行对比，若该IEC-60870-5-104报文的报文格式有错，则报文格式错误计数器加1；

所述的步骤(3)的创建决策线程为：

(3.1)判断配置的TCP链路是否都存在，若有配置的TCP链路不存在，立即报告链路中断事件，并进入步骤(3.2)；否则进入步骤(3.2)；

(3.2)检查已存在的所有TCP链路的链路通信状态定时器t_commuState与当前时间之差是否超过预定的第一阈值，若是，则报告通信中断事件，并进入步骤(3.3)，否则进入步骤(3.3)；

(3.3)对于循环配置的遥测点，检查遥测点刷新时间t_rfhState[n]与当前时间之差是否超过预定的第二阈值，若是，则报告遥测点未刷新事件，并进入步骤(3.4)，否则进入步骤(3.4)，且遥测点刷新时间t_rfhState[n]中的n表示第n个遥测点；

(3.4)对于所有遥控过程和遥调过程，判断响应超时计时器t_response和当前时间之差是否超过预设的第三阈值，若是，则报告遥控过程或遥调过程失败，并进入步骤(3.5)，否则进入步骤(3.5)；

(3.5)对于所有遥控过程和遥调过程，判断过程超时计时器t_process和当前时间之差是否超过预设的第四阈值，若是，则报告遥控过程或遥调过程失败，并进入步骤(3.6)；否则进入步骤(3.6)；

(3.6)判断周期报告计时器是否到期，若是，则进入步骤(3.7)并将周期报告计时器清零，重新计时，否则返回步骤(3.1)；

(3.7)计算所有的TCP连接数量并报告；

(3.8)报告报文格式错误计数器示数、主站关闭TCP连接次数n_masterclose、子站关闭TCP连接次数n_slaveclose、遥测数据无效次数n_teleMesInvalid、遥信数据无效次数n_teleSigInvalid和遥测数据溢出次数n_teleMesOv，并在报告后进行清零处理，返回步骤(3.1)。

2.根据权利要求1所述的IEC-60870-5-104协议报文监控方法，其特征在于，所述的步骤(2.3)包含以下步骤：

(2.3.1)在网络层对该IP报文进行网络层分析，获取该IP报文的源IP地址和目的IP地址，并获取传输层报文；

(2.3.2)解析出该传输层报文的传输层协议类型。

3.根据权利要求1所述的IEC-60870-5-104协议报文监控方法，其特征在于，所述的步骤(2.4.1)后还包括以下步骤：

(2.4.2)将超时计时器t_timeout更新为当前时间，并根据获取的TCP头信息，判断当前报文是否为TCP连接建立或释放时的特殊报文，若是，则将TCP连接中的相应变量置1后进入步骤(2.4.3)，否则直接进入步骤(2.4.3)；

(2.4.3)判断当前TCP连接中的释放再次确认变量release_ack2是否被置1，若是，则进入步骤(2.4.4)，否则进入步骤(2.4.5)；

(2.4.4)判断当前报文源端口号是否等于客户端端口号变量port_client，若是，则将连接关闭者变量closer置1，否则将连接关闭者变量closer置2；

(2.4.5)根据TCP头信息判断该应用层报文是否为IEC-60870-5-104报文，若是，则进入步骤(2.5)，否则返回步骤(2.1)。

IEC-60870-5-104协议报文监控方法

技术领域

[0001] 本发明涉及智能变电站网络报文分析领域，尤其涉及通信协议的报文分析技术领域，具体是指一种IEC-60870-5-104协议报文监控方法。

背景技术

[0002] 智能变电站是智能电网的关键环节，通信平台网络化是其重要特征，传统变电站的电缆直连通信方式由交换机和网线替代。站内二次设备之间通过网络报文的方式进行数据交换。随着站内智能设备和设备产生的数据越来越多，二次设备调试和维护越来越困难，智能变电站网络报文分析系统通过镜像抓取并在线分析站内网络报文，实现了对二次设备的实时监控，有效提高了变电站运行效率。

[0003] 智能变电站内设备类型较多，对通信实时性要求不同，导致站内设备间通过多种协议进行通信。传统网络报文分析仪基本覆盖了站内常见的通信协议，如IEC61850标准中使用的SV-9-2、GOOSE、MMS等。但是，目前对变电站与调度系统之间的通信协议监控的较少。

[0004] 变电站与调度系统之间一般通过IEC60870-5-104(简称104)协议进行通信，104以TCP/IP系列协议为底层通信协议，技术成熟，使用方便。但是，由于TCP/IP协议延迟不固定等问题，在具体实现上除了控制网络流量之外，还需要对104协议的报文进行监控。

[0005] 现有技术中，一类通过定时发送测试报文判断链路连接状态，无法对实时报文结构错误进行判断；一类利用端口镜像方法抓取实时报文，对报文结构进行仔细的检查，但是通过报文长度判断报文类型，容易出错，且该方法只能分析报文结构，对于涉及到多条报文的控制过程无法监控；其他方法通过镜像抓取全站报文，对报文结构和各种命令进行了多维的统计，但是计算太过复杂，实现难度较大，实用性较差。

发明内容

[0006] 为解决以上问题，本发明提供了一种可大大提高通信可靠性的IEC-60870-5-104协议报文监控方法。

[0007] 为了实现上述目的，本发明的IEC-60870-5-104协议报文监控方法如下：

[0008] 该IEC-60870-5-104协议报文监控方法，其主要特点是，所述的方法包括以下步骤：

[0009] (1)初始化变量；

[0010] (2)创建报文解析线程；

[0011] (3)创建决策线程。

[0012] 较佳地，所述的步骤(1)中的初始化为：

[0013] 将相关变量初始化为零，并清空TCP连接映射表map_link和控制过程映射表map_ctl，其中，所述的相关变量包括报告周期定时器t_rpt、链路通信状态定时器t_commuState、遥测刷新状态定时器t_rfhState[n]，其中n表示遥测点数量，主站关闭TCP连接次数n_masterclose、子站关闭TCP连接次数n_slaveclose、遥测数据无效次数n_

teleMesInvalid、遥测数据溢出次数n_teleMesOv和遥信数据无效次数n_teleSigInvalid。

[0014] 更佳地，所述的步骤(2)中的创建报文解析线程为：

[0015] (2.1)读取报文，并取出报文中的链路层报文；

[0016] (2.2)在链路层对该链路层报文进行分析，获取网络层报文，并判断该网络层报文是否为IP报文，若是，则进入步骤(2.3)，否则返回步骤(2.1)；

[0017] (2.3)在网络层对该IP报文进行分析，获取传输层报文，并判断该传输层报文是否为TCP报文，若是，则进入步骤(2.4)，否则返回步骤(2.1)；

[0018] (2.4)在传输层对该TCP报文进行分析，获取应用层报文，并判断该应用层报文是否为IEC-60870-5-104报文，若是，则进入步骤(2.5)，否则返回步骤(2.1)；

[0019] (2.5)在应用层对该IEC-60870-5-104报文进行分析，并保存分析结果，返回步骤(2.1)。

[0020] 尤佳地，所述的步骤(2.3)包含以下步骤：

[0021] (2.3.1)在网络层对该IP报文进行网络层分析，获取该IP报文的源IP地址和目的IP地址，并解析IP报文获取传输层报文；

[0022] (2.3.2)解析出该传输层报文的传输层协议类型，并根据传输层协议类型进一步判断其是否为TCP报文。

[0023] 尤佳地，所述的步骤(2.4)中包括以下步骤：

[0024] (2.4.1)在传输层对该TCP报文进行分析，获取该TCP报文的TCP头信息，并判断是否存在TCP连接，若不存在，则新建TCP连接。

[0025] 甚佳地，所述的TCP连接中包括以下在新建TCP连接时要进行初始化清零的相关变量：

[0026] 客户端建立请求变量establish_req、服务端确认变量establish_ack、客户端确认变量establish_ackself、释放请求变量release_req、释放确认变量release_ack、释放再次请求变量release_req2和释放再次确认变量release_ack2、客户端端口号变量port_client、服务端端口号变量port_serv、连接关闭者变量closer；

[0027] 新建TCP连接时进行初始化的变量还包括超时计时器t_timeout、客户端IP地址ip_client、服务端IP地址ip_serv，其中，对客户端IP地址ip_client和服务端IP地址ip_serv的初始化均为置空，对超时计时器t_timeout的初始化为将当前时间置为超时计时器t_timeout的初始值。

[0028] 极佳地，所述的客户端建立请求变量establish_req、服务端确认变量establish_ack、客户端确认变量establish_ackself、释放请求变量release_req、释放确认变量release_ack、释放再次请求变量release_req2和释放再次确认变量release_ack2的值与各变量对应的事件是否发生相关，若各变量对应的事件发生，则置1，否则置0，其中，

[0029] 客户端建立请求变量establish_req对应TCP连接中发生客户端建立请求这一事件；

[0030] 服务端确认变量establish_ack对应TCP连接中发生服务端确认这一事件；

[0031] 客户端确认变量establish_ackself对应TCP连接中发生客户端确认这一事件；

[0032] 释放请求变量release_req对应TCP连接中发生释放请求这一事件；

[0033] 释放确认变量release_ack对应TCP连接中发生释放确认这一事件；

[0034] 释放再次请求变量release_req2对应TCP连接中发生连续两次释放请求时发生第二次释放请求这一事件；

[0035] 释放再次确认变量release_ack2对应TCP连接中发生连续两次释放请求时发生第二释放确认这一事件；

[0036] 所述的连接关闭者变量closer的值与该TCP连接的连接情况相关，若该TCP连接正常，置0；若该TCP连接由客户端关闭，置1；若该TCP连接由服务端关闭，置2。

[0037] 绝佳地，所述的步骤(2.4.1)后还包括以下步骤：

[0038] (2.4.2)将超时计时器t_timeout更新为当前时间，并根据获取的TCP头信息，判断当前报文是否为TCP连接建立或释放时的特殊报文，若是，则将TCP连接中的相应变量置1后进入步骤(2.4.3)，否则直接进入步骤(2.4.3)；

[0039] (2.4.3)判断当前TCP连接中的释放再次确认变量release_ack2是否被置1，若是，则进入步骤(2.4.4)，否则进入步骤(2.4.5)；

[0040] (2.4.4)判断当前报文源端口号是否等于客户端端口号变量port_client，若是，则将连接关闭者变量closer置1，否则将连接关闭者变量closer置2；

[0041] (2.4.5)根据TCP头信息判断该应用层报文是否为IEC-60870-5-104报文，若是，则进入步骤(2.5)，否则返回步骤(2.1)。

[0042] 绝佳地，所述的步骤(2.5)为：

[0043] (2.5.1)判断连接关闭者变量closer的值，若为0，进入步骤(2.5.2)；若为1，子站关闭TCP连接次数n_slaveclose加1，并返回步骤(2.1)，若为2，则主站关闭TCP连接次数n_masterclose加1，返回步骤(2.1)；

[0044] (2.5.2)检查IEC-60870-5-104报文的应用服务数据单元ASDU类型标识符，若为遥测报文，则进入步骤(2.5.3)，否则进入步骤(2.5.5)；

[0045] (2.5.3)更新遥测点刷新时间t_rfhState[n]，其中n表示第n个遥测点，判断数据遥测数据是否为无效，若是，则令遥测数据无效次数n_teleMesInvalid加1；否则进入步骤(2.5.4)；

[0046] (2.5.4)判断遥测数据是否溢出，若是，则令遥测数据溢出次数n_teleMesOv加1；否则进入步骤(2.5.5)；

[0047] (2.5.5)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥信报文，则进入步骤(2.5.6)，否则进入步骤(2.5.7)；

[0048] (2.5.6)判断遥信数据是否无效，若是，则令遥信数据无效次数n_teleSigInvalid加1，否则进入步骤(2.5.7)；

[0049] (2.5.7)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥控报文，则进入步骤(2.5.9)，否则进入步骤(2.5.8)；

[0050] (2.5.8)检查IEC-60870-5-104报文应用服务数据单元ASDU类型标识符，若为遥调报文，则进入步骤(2.5.9)，否则进入步骤(2.5.11)；

[0051] (2.5.9)根据IP报文的IP地址判断是否存在控制过程，若存在，则进入(2.5.10)，否则在新建控制过程后进入(2.5.10)；所述的控制过程中包含主站选择命令变量select_req、子站选择确认命令变量select_ack、主站撤销命令变量cancel_req、子站取消确认变量cancel_ack、主站执行命令变量act_req和子站执行响应变量act_ack，分别代表遥控过

程中的实际执行步骤和遥调过程中的实际执行步骤，相应步骤未执行时变量置0，否则置1，控制过程中还包含响应超时计时器t_response和过程超时计时器t_process，新建控制过程时，响应超时计时器t_response和过程超时计时器t_process均设置为当前时间，且该控制过程中的其他变量在新建时均设置为0；

[0052] (2.5.10)更新响应超时计时器t_response和过程超时计时器t_process为当前时间，将相应步骤标识变量置1；

[0053] (2.5.11)将该IEC-60870-5-104报文与标准报文格式进行对比，若该IEC-60870-5-104报文的报文格式有错，则报文格式错误计数器加1。

[0054] 超佳地，所述的步骤(3)的创建决策线程为：

[0055] (3.1)判断配置的TCP链路是否都存在，若有配置的TCP链路不存在，立即报告链路中断事件，并进入步骤(3.2)；否则进入步骤(3.2)；

[0056] (3.2)检查已存在的所有TCP链路的链路通信状态定时器t_commuState与当前时间之差是否超过预定的第一阈值，若是，则报告通信中断事件，并进入步骤(3.3)，否则进入步骤(3.3)；

[0057] (3.3)对于循环配置的遥测点，检查遥测点刷新时间t_rfhState[n]与当前时间之差是否超过预定的第二阈值，若是，则报告遥测点未刷新事件，并进入步骤(3.4)，否则进入步骤(3.4)，且遥测点刷新时间t_rfhState[n]中的n表示第n个遥测点；

[0058] (3.4)对于所有遥控过程和遥调过程，判断响应超时计时器t_response和当前时间之差是否超过预设的第三阈值，若是，则报告遥控过程或遥调过程失败，并进入步骤(3.5)，否则进入步骤(3.5)；

[0059] (3.5)对于所有遥控过程和遥调过程，判断过程超时计时器t_process和当前时间之差是否超过预设的第四阈值，若是，则报告遥控过程或遥调过程失败，并进入步骤(3.6)；否则进入步骤(3.6)；

[0060] (3.6)判断周期报告计时器是否到期，若是，则进入步骤(3.7)并将周期报告计时器清零，重新计时，否则返回步骤(3.1)；

[0061] (3.7)计算所有的TCP连接数量并报告；

[0062] (3.8)报告报文格式错误计数器示数、主站关闭TCP连接次数n_masterclose、子站关闭TCP连接次数n_slaveclose、遥测数据无效次数n_teleMesInvalid、遥信数据无效次数n_teleSigInvalid和遥测数据溢出次数n_teleMesOv，并在报告后进行清零处理，返回步骤(3.1)。

[0063] 采用本发明的IEC-60870-5-104协议报文监控方法，可在网络报文分析仪中实现，在不影响原链路的情况下，简单方便的对基于IEC-60870-5-104协议的链路状态进行判断，对实时报文结构进行分析，对遥控和遥信过程进行监控，对严重错误立即报告，定期上送统计信息，实现了IEC-60870-5-104协议的全方位监控，提高了通信可靠性。

附图说明

[0064] 图1为根据本发明的IEC-60870-5-104协议报文监控方法实施的系统流程图。

[0065] 图2为根据本发明的IEC-60870-5-104协议报文监控方法实施的报文解析线程。

[0066] 图3为根据本发明的IEC-60870-5-104协议报文监控方法实施的决策线程。

具体实施方式

[0067] 为了能够更清楚地描述本发明的技术内容，下面结合具体实施例来进行进一步的描述。

[0068] 请参阅图1，在一种具体实施例中，该IEC-60870-5-104协议报文监控方法具有以下步骤：

[0069] (1)将相应变量初始化为零，清空TCP连接映射表map_link和控制过程映射表map_ctl，相应变量包括报告周期定时器t_rpt、链路通信状态定时器t_commuState、遥测刷新状态定时器t_rfhState[n]，其中n表示遥测点数量，主站关闭TCP连接次数n_masterclose、子站关闭TCP连接次数n_slaveclose、遥测数据无效次数n_teleMesInvalid、遥测数据溢出次数n_teleMesOv和遥信数据无效次数n_teleSigInvalid；

[0070] (2)创建报文解析线程；

[0071] (3)创建决策线程。

[0072] 请参阅图2，第(2)步创建报文解析线程包含以下步骤：

[0073] (2.1)读取报文并取出链路层报文；

[0074] (2.2)在链路层对链路层报文进行分析，获取网络层报文，并判断网络层报文是否为IP报文，若是，则进入步骤(2.3)，否则返回步骤(2.1)进入下一轮；

[0075] (2.3)在网络层对该IP报文进行分析，获取传输层报文，并判断该传输层报文是否为TCP报文，若是，则进入步骤(2.4)，否则返回步骤(2.1)进入下一轮；

[0076] (2.4)进行传输层分析，获取应用层报文，并判断应用层报文是否为104报文，若是，则进入步骤(2.5)，否则返回步骤(2.1)进入下一轮；

[0077] (2.5)进行应用层分析，保存分析结果，返回步骤(2.1)进入下一轮。

[0078] 其中第(2.3)步包含以下步骤：

[0079] (2.3.1)在网络层对该IP报文进行网络层分析，获取该IP报文的源IP地址和目的IP地址，并解析IP报文获取传输层报文；

[0080] (2.3.2)解析出该传输层报文的传输层协议类型，并根据传输层协议类型进一步判断其是否为TCP报文。

[0081] 实际上，后续对报文类型的判断，都是基于对该层协议类型的判断，对报文的首部进行解析，获取相应的层级协议类型。

[0082] 其中第(2.4)步包含以下步骤：

[0083] (2.4.1)解析出TCP报文的TCP头信息，判断TCP连接是否已经存在，若是，则进入(2.4.2)，否则先新建一个TCP连接再进入(2.4.2)，每条TCP连接包括客户端建立请求变量establish_req，服务端确认变量establish_ack，客户端确认变量establish_ackself，释放请求变量release_req，释放确认变量release_ack，释放再次请求变量release_req2，释放再次确认变量release_ack2，上述7个变量分别代表TCP连接建立和释放时的实际步骤，取值为0表示该步骤未完成，取值为1表示该步骤已完成，新建时上述7个变量均为0，每条TCP连接还包含超时计时器t_timeout，在新建TCP连接时被初始化为当前时间，客户端IP地址ip_client，初始化为空，服务端IP地址ip_serv，初始化为空，客户端端口号变量port_client，初始为0，服务端端口号变量port_serv，初始为0，以及连接关闭者closer，取0表示连接正常没有关闭，取1表示由客户端关闭，取2表示由服务端关闭；

[0084] (2.4.2)将超时计时器t_timeout更新为当前时间,并根据获取的TCP头信息,判断当前报文是否为TCP连接建立或释放时的特殊报文,若是,则将TCP连接中的相应变量置1后进入步骤(2.4.3),该种特殊报文对应的相应变量包括客户端建立请求变量establish_req和释放请求变量release_req等;否则直接进入步骤(2.4.3);

[0085] (2.4.3)若当前TCP连接中的释放再次确认变量release_ack2被置1,进入(2.4.4),否则进入(2.4.5);

[0086] (2.4.4)若当前报文源端口号等于客户端端口号变量port_client,将连接关闭者变量closer置1,否则将连接关闭者变量closer置2;

[0087] (2.4.5)根据TCP头信息判断应用层报文是否为104报文,若是则继续,否则返回步骤(2.1)进入下一轮。

[0088] 所述的步骤(2.5)包含以下步骤:

[0089] (2.5.1)根据传输层分析结果,若连接关闭者变量closer为0,进入(2.5.2),若连接关闭者变量closer为1,子站关闭TCP连接次数n_slaveclose加1,返回步骤(2.1)进入下一轮,若连接关闭者变量closer为2,主站关闭TCP连接次数n_masterclose加1,返回步骤(2.1)进入下一轮;

[0090] (2.5.2)检查104报文应用服务数据单元ASDU类型标识符,若为遥测报文进入(2.5.3),否则继进入(2.5.5);

[0091] (2.5.3)更新遥测点刷新时间t_rfhState[n],其中n表示第n个遥测点,判断数据遥测数据是否为无效,若是,则令遥测数据无效次数n_teleMesInvalid加1,否则继续(2.5.4);

[0092] (2.5.4)判断遥测数据是否溢出,是则令遥测数据溢出次数n_teleMesOv加1,否则继续(2.5.5);

[0093] (2.5.5)检查104报文应用服务数据单元ASDU类型标识符,若为遥信报文,则进入(2.5.6),否则进入(2.5.7);

[0094] (2.5.6)判断遥信数据是否无效,是则令遥信数据无效次数n_teleSigInvalid加1,否则继续下一步;

[0095] (2.5.7)检查104报文应用服务数据单元ASDU类型标识符,若为遥控报文,则进入(2.5.9),否则继续(2.5.8);

[0096] (2.5.8)检查104报文应用服务数据单元ASDU类型标识符,若为遥调报文,则进入(2.5.9),否则进入(2.5.11);

[0097] (2.5.9)根据IP地址判断控制过程是否存在,是则进入(2.5.10),否则新建控制过程后进入(2.5.10),控制过程包含主站选择命令变量select_req,子站选择确认命令变量select_ack,主站撤销命令变量cancel_req,子站取消确认变量cancel_ack,主站执行命令变量act_req,子站执行响应变量act_ack,上述变量分别代表遥控和遥调命令实际执行步骤,且

[0098] 其中主站选择命令变量select_req对应遥控和遥调命令实际执行步骤中的主站选择命令事件,子站选择确认命令变量select_ack对应遥控和遥调命令实际执行步骤中的子站选择确认命令事件;主站撤销命令变量cancel_req对应遥控和遥调命令实际执行步骤中的主站撤销命令事件;子站取消确认变量cancel_ack对应遥控和遥调命令实际执行步骤

中的子站取消确认事件;主站执行命令变量act_req对应遥控和遥调命令实际执行步骤中的主站执行命令事件;子站执行响应变量act_ack对应遥控和遥调命令实际执行步骤中的子站执行响应事件;上述变量取值为0表示相应步骤未执行,取值为1表示相应步骤已执行,控制过程还包含响应超时计时器t_response和过程超时计时器t_process,新建时,上述两个计时器设置为当前时间,其他变量均为0;

[0099] (2.5.10)更新响应超时计时器t_response和过程超时计时器t_process为当前时间,将相应步骤标识变量置1;

[0100] (2.5.11)与标准报文格式进行对比,若该104报文的报文格式有错,则报文格式错误计数器加1。

[0101] 第(3)步包含以下步骤:

[0102] (3.1)观察系统保存的TCP链路,判断配置的TCP链路是否都存在,若有配置的链路不存在,立即报告链路中断事件,并进入下一步;否则继续进入下一步;

[0103] (3.2)对于已存在的所有TCP链路,检查链路通信状态定时器t_commuState与当前时间之差是否超过预定的阈值,是则立即报告通信中断事件,并进入下一步,否则继续进入下一步;

[0104] (3.3)循环配置的遥测点,检查遥测点刷新时间t_rfhState[n](其中n表示第n个遥测点)与当前时间之差是否超过预定的阈值,是则立即报告遥测点未刷新事件,并进入下一步,否则继续进入下一步;

[0105] (3.4)对于所有遥控和遥调过程,判断响应超时计时器t_response和当前时间之差是否超过阈值,是则立即报告遥控过程或遥调过程失败,并进入下一步,否则进入(3.5);

[0106] (3.5)对于所有遥控和遥调过程,判断过程超时计时器t_process和当前时间之差是否超过阈值,是则立即报告遥控过程或遥调过程失败,并进入下一步,否则进入(3.6);

[0107] (3.6)判断周期报告计时器t_rpt是否到期,是则进入下一步并将计时器清零重新计时,否则返回步骤(3.1)进入下一轮;

[0108] (3.7)计算所有的TCP连接数量并报告;

[0109] 在一种具体的实施例中,该方法中各种数据的上报具有一定顺序,请参阅图3,在该具体实施例中,各种数据以以下顺序进行上报:

[0110] (3.8)报告报文结构错误次数,并清零次数;

[0111] (3.9)报告主站关闭TCP连接次数,并清零次数;

[0112] (3.10)报告子站关闭TCP连接次数,并清零次数;

[0113] (3.11)报告遥测数据无效次数,并清零次数;

[0114] (3.12)报告遥信数据无效次数,并清零次数;

[0115] (3.13)报告遥测数据溢出次数,并清零次数;

[0116] (3.14)返回步骤(3.1)进入下一轮。

[0117] 采用本发明的IEC-60870-5-104协议报文监控方法,可在网络报文分析仪中实现,在不影响原链路的情况下,简单方便的对基于IEC-60870-5-104协议的链路状态进行判断,对实时报文结构进行分析,对遥控和遥信过程进行监控,对严重错误立即报告,定期上送统计信息,实现了IEC-60870-5-104协议的全方位监控,提高了通信可靠性。

[0118] 在说明书中,本发明已参照其特定的实施例作了描述。但是,很显然仍可以作出各

种修改和变换而不背离本发明的精神和范围。因此，说明书和附图应被认为是说明性的而非限制性的。

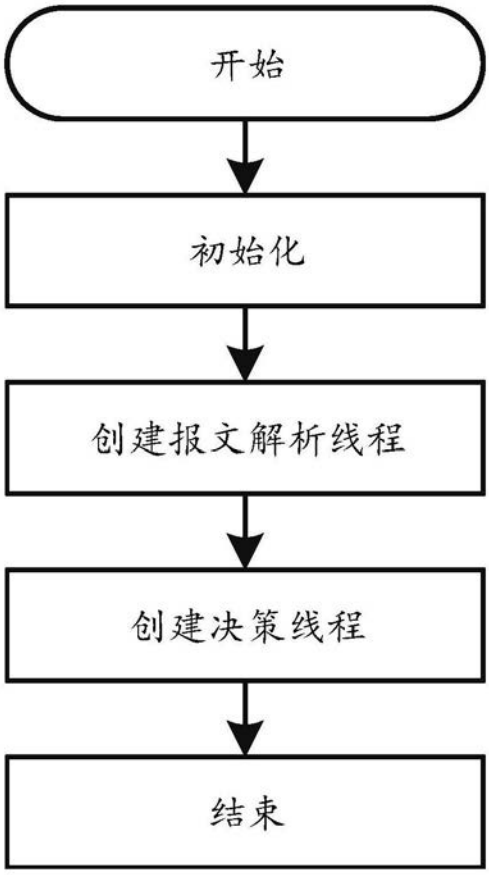

图1

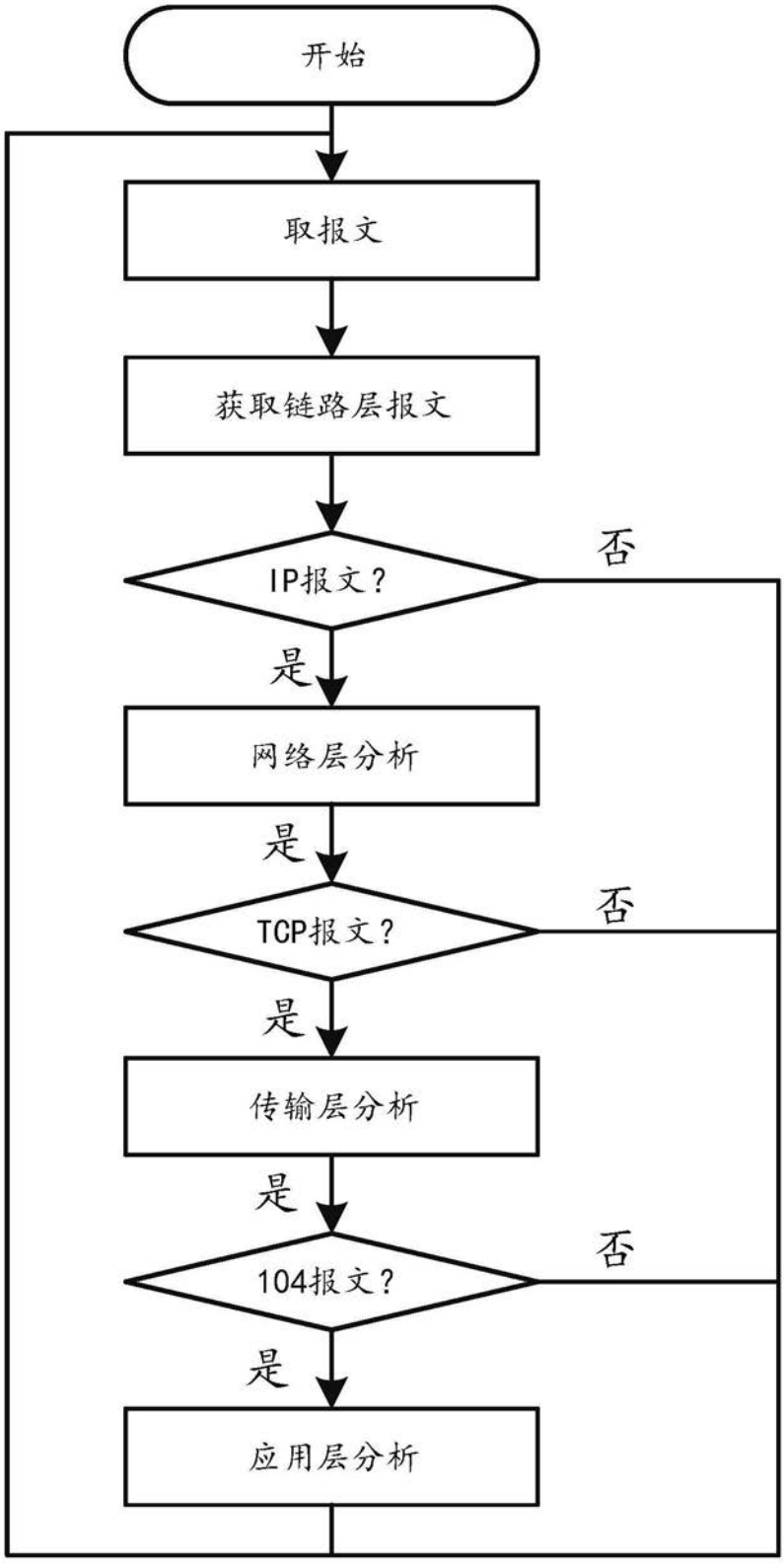

图2

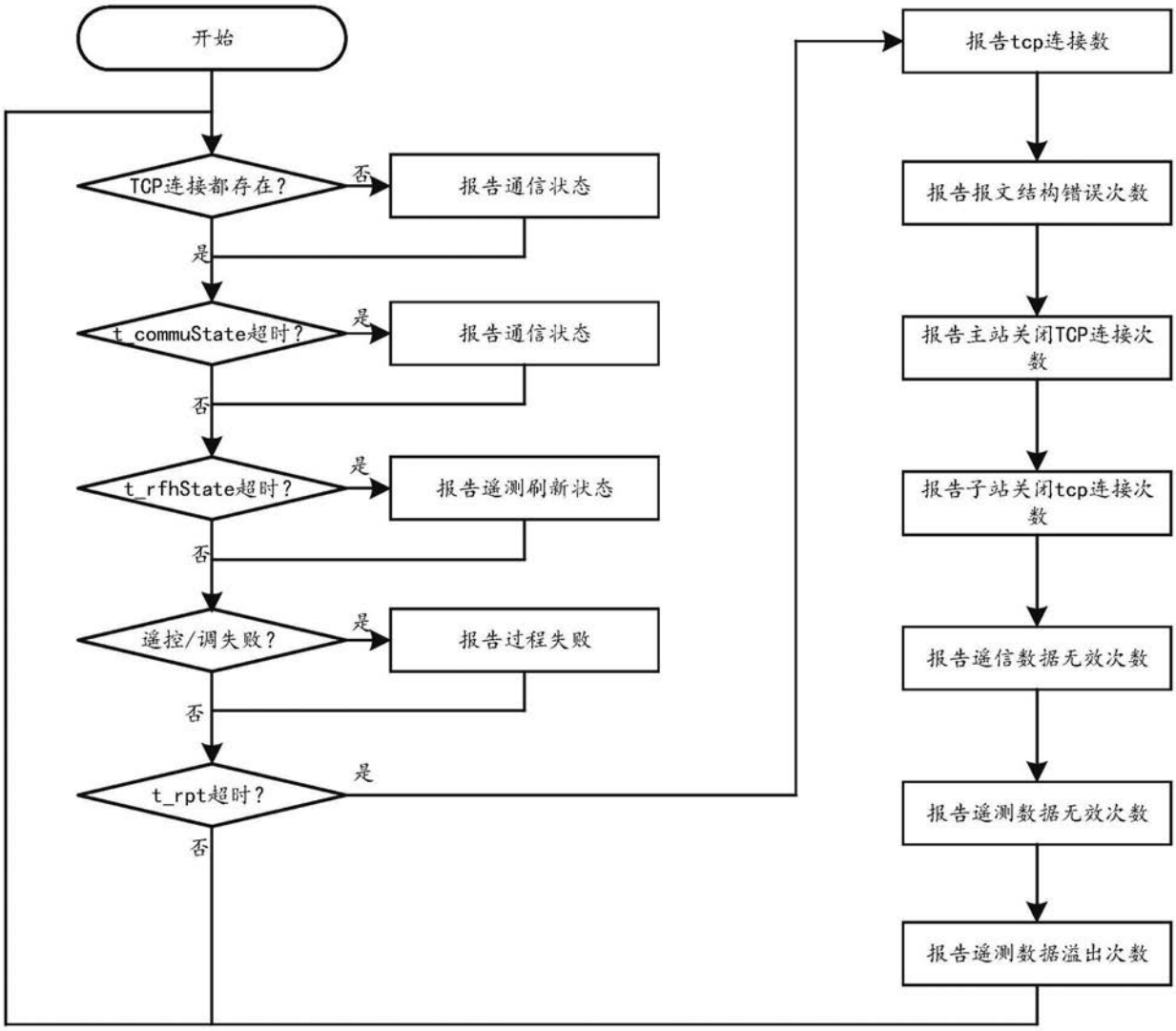
开始
TCP连接都存在？
否
报告通信状态
是
t_commuState超时？
是
报告通信状态
否
t_rfhState超时？
是
报告遥测刷新状态
否
遥控/调失败？
是
报告过程失败
否
t_rpt超时？
是
否
报告tcp连接数
报告报文结构错误次数
报告主站关闭TCP连接次数
报告子站关闭tcp连接次数
报告遥信数据无效次数
报告遥测数据无效次数
报告遥测数据溢出次数

图3