(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114825607 A
(43)申请公布日 2022.07.29

(21)申请号 202111675512.4

(22)申请日 2021.12.31

(71)申请人 湖南大学
地址 410082 湖南省长沙市岳麓区麓山南路2号

(72)发明人 刘绚 王文博 张博 宋宇飞 于宗超

(74)专利代理机构 长沙正奇专利事务所有限责任公司 43113
专利代理师 王娟 马强

(51)Int.Cl.
H02J 13/00(2006.01)
H04L 9/40(2022.01)

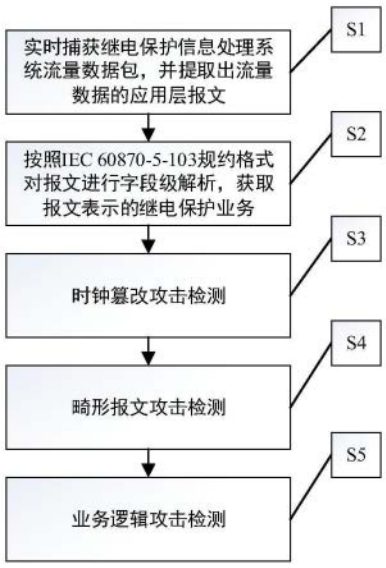
权利要求书3页 说明书13页 附图5页

(54)发明名称

继电保护信息处理系统攻击行为监测方法及装置

(57)摘要

本发明公开了一种继电保护信息处理系统攻击行为监测方法及装置,对实时捕获的继电保护信息处理系统的流量数据进行应用层报文提取,并按照IEC 60870-5-103规约解析。其次对报文进行时钟篡改攻击检测。然后根据规约要求针对报文格式进行畸形报文攻击检测。最后建立各类系统业务的正常行为模型,依据正常行为模型对系统流量数据进行应用层的攻击行为检测。本发明克服了现有继电保护信息处理系统攻击行为检测方法侧重于继电保护装置测量点的数据分析,缺乏针对流量数据应用层报文进行攻击行为检测的不足,提升了继电保护信息处理系统攻击行为检测的精准性。



CN 114825607 A

1.一种继电保护信息处理系统攻击行为监测方法,其特征在于,包括以下步骤:

S1、实时捕获继电保护信息处理系统流量数据包,并提取出当前帧流量数据的应用层报文;

S2、对所述应用层报文进行字段级解析;

S3、对解析后的报文进行时钟篡改攻击检测,若报文的时钟范围、时钟逻辑、时钟同步、时钟延时不符合正常时钟特征,则判定存在时钟篡改攻击,否则进入步骤S4;

S4、对解析后的报文进行畸形报文攻击检测,若报文的长度字段、类型标识、传送原因、信息序号值与规约要求不符,则判定存在畸形报文攻击,否则进入步骤S5;

S5、按照解析后的报文所属的业务系统,对解析后的报文进行攻击检测,若解析后的报文不符合正常业务模型,则判定存在业务逻辑攻击,否则将当前帧流量数据判定为正常流量。

2.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法,其特征在于,步骤S3中,对解析后的报文进行时钟篡改攻击检测的具体实现过程包括:

1)判断公式$Y_t \in [1970,2069]$是否成立,若否,则判定为时钟篡改攻击,否则,进入步骤2);其中,$Y_t = \begin{cases} y_t + 2000, y_t < 70 \\ y_t + 1900, y_t \geq 70 \end{cases}$,$Y_t$表示时标年份,$y_t$表示时标的年份标识字节数值;

2)判断公式$\forall P \in P_{DS} \Rightarrow A_g(P) = \mathrm{FFH}$是否成立,若否,则判定为时钟篡改攻击,否则,进入步骤3);其中,∀表示全称量词“任意”,P为步骤S2解析后的应用层报文,P_{DS}表示IEC 60870-5-103对时报文,$A_g(P)$表示报文ASDU地址高8位的值,F表示16进制的15,H表示数值为16进制;

3)判断公式$\forall P \in P_{DZ} \Rightarrow T_{js}(P) - T_{sj}(P) > 0$是否成立,若否,则判定为时钟篡改攻击,否则,进入步骤4);其中,P_{DZ}表示IEC 60870-5-103告警、遥信变位、动作事件数据上送报文中的一种,$T_{js}(P)$表示事件子站接收时间,$T_{sj}(P)$表示事件实际发生时间;

4)检测子站上送历史故障信息时间段与主站召唤故障历史信息时间段是否一致,若两者时间不一致,则判定为时钟篡改攻击,否则进入步骤5);

5)判断公式$\forall P \in P_{XC} \Rightarrow T_{cs}(P) < T_{max}$是否成立,若否,则判定为时钟篡改攻击,否则,进入步骤S4;其中,$T_{max} = \begin{cases} 0.5, P = P_1 \text{或} P_2 \text{或} P_3 \\ 6, \ P = P_4 \end{cases}$;$P_{XC}$表示IEC60870-5-103主-子站信息传送报文,$T_{cs}(P)$表示信息传送时间,T_{max}表示最大延迟时间,P_1表示继电保护装置动作信息传送报文,P_2表示继电保护装置模拟量测量值传送报文,P_3表示继电保护装置运行状态传送报文,P_4表示继电保护装置定值传送报文。

3.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法,其特征在于,对解析后的报文进行畸形报文攻击检测的具体实现过程包括:

I)判断公式$\forall P \in P_{IEC103} \Rightarrow F_l(P) = L_s(P)$是否成立,若否,则判定为畸形报文攻击,否则进入步骤II);其中,P_{IEC103}表示IEC 60870-5-103报文,$F_l(P)$表示报文理论长度,$L_s(P)$表示报文实际长度;

II)判断公式$\forall P \in P_{IEC103} \Rightarrow L_s(P) \leq 2048$是否成立,若否,则判定为畸形报文攻击,否则

进入步骤III)；

III)判断公式$\forall P \in P_{IEC103} \Rightarrow F_t(P) \in [1,31]$是否成立，若否，判定为畸形报文攻击，否则进入步骤IV)；其中，$F_t(P)$表示报文类型标识字段值；

IV)判断公式$\forall P \in P_{IEC103} \Rightarrow F_c(P) \in [1,63]$是否成立，若否，判定为畸形报文攻击，否则进入步骤V)；其中，$F_c(P)$表示报文传送原因字段值；

V)判断公式$\forall P \in P_{IEC103} \Rightarrow F_i(P) \in \{[0,159],[240,255]\}$是否成立，若否，判定为畸形报文攻击，否则进入步骤S5；$F_i(P)$表示报文信息序号字段值。

4.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法，其特征在于，步骤S5中，当报文为读取子站配置业务时，对解析后的报文进行攻击检测的具体实现过程包括：

判断公式$\forall P \in P_{BT} \Rightarrow B_n(P) == B_s$是否成立，若否，则判定存在配置数据恶意拦截攻击，否则，判断公式$\forall P \in P_{BT} \Rightarrow \forall B_{zh}(P) == C_{zh}$是否成立，若否，则判定存在数据篡改攻击，否则将当前帧流量数据判定为正常流量；其中，P_{BT}表示继电保护信息处理系统中读取子站配置业务报文，$B_n(P)$表示子站上送标题数目，B_s表示子站配置的所有标题数目，$B_{zh}(P)$表示同一组标题信息的各个条目的组号，C_{zh}表示当前组标题信息的组号。

5.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法，其特征在于，步骤S5中，当报文为保护事件上送业务，对解析后的报文进行攻击检测的具体实现过程包括：

A)判断公式$\forall P \in P_{BH} \Rightarrow D_{pi}(P) \in \{0,1,2,3\}$是否成立，若否，则判定存在双点信息恶意篡改攻击，否则，进入步骤B)；其中，P_{BH}表示继电保护信息处理系统中保护事件上送报文，$D_{pi}(P)$表示双点信息数值；

B)检测开关量变位、动作信号、压板状态前后帧报文逻辑是否正确，若开关量变位前一帧为开/合，后一帧仍为开/合；动作信号前一帧为复归/动作，后一帧仍为复归/动作；压板状态前一帧为未投入/投入，后一帧仍为未投入/投入，则判定存在恶意开合攻击，否则进入步骤C)；

C)判断公式$\forall P \in P_{BH} \Rightarrow L_{bh}(P) = \begin{cases} 1, P = P_5 \\ 2, P = P_6 \end{cases}$是否成立，若否，则判定存在动作事件非法上送攻击，否则将当前帧流量数据判定为正常流量；其中，$L_{bh}(P)$表示保护事件报文类型标识，P_5表示告警或开关量变位事件报文，P_6表示动作事件报文。

6.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法，其特征在于，步骤S5中，当报文为录波简报上送业务时对解析后的报文进行攻击检测的具体实现过程包括：

i)判断公式$\forall P \in P_{LB} \Rightarrow G_{xb}(P) == Z_{xb}(P)$是否成立，若否，则判定存在跳闸相别恶意篡改攻击，否则进入步骤ii)；其中，P_{LB}表示继电保护信息处理系统中录波简报业务报文，$G_{xb}(P)$表示故障相别，$Z_{xb}(P)$表示跳闸相别；

ii)判断公式$\forall P \in P_{LB} \Rightarrow D_3 = \begin{cases} 1, & D_0 = 1 \wedge D_1 = 1 \wedge D_2 = 1 \\ 0或1, & D_0 = 0 \vee D_1 = 0 \vee D_2 = 0 \end{cases}$是否成立，若否，则判定存在接地故障标志位数据篡改攻击，否则进入步骤iii)；其中，D_3表示报文短路接地故障标志位数值，D_0表示报文A相短路故障标志位数值，D_1表示报文B相故短路障标志位数值，D_2表示报文C相短路故障标志位数值；

iii)检测录波简报中的重合闸是否异常,若故障发生后有重合闸,但重合闸时间为0,或者没有重合闸,但重合闸时间不为0,则判定存在重合闸时间篡改攻击,否则将当前帧流量数据判定为正常流量。

7.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法,其特征在于,步骤S5中,当报文为定值操作业务时,对解析后的报文进行攻击检测的具体实现过程包括:

判断逻辑$X_{g1}\rightarrow X_{g2}\rightarrow X_{g3}\rightarrow X_{g4}\rightarrow X_{g5}\rightarrow X_{g6}\rightarrow X_{g7}\rightarrow X_{g8}$是否成立,若否,则判定存在继电保护装置整定值恶意篡改攻击,否则将当前帧流量数据判定为正常流量;其中,X_{g1}表示召唤装置当前运行定值区号报文,X_{g2}表示子站上传装置当前运行定值区号报文,X_{g3}表示主站召唤装置定值报文,X_{g4}表示子站上传装置定值报文,X_{g5}表示向子站下装定值报文,X_{g6}表示响应子站下装定值报文,X_{g7}表示执行定值修改报文,X_{g8}子站响应定值修改报文。

8.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法,其特征在于,步骤S5中,当报文为总召唤业务时,对解析后的报文进行攻击检测的具体实现过程包括:

判断逻辑$Z_{h1}\rightarrow Z_{h2}\rightarrow Z_{h3}$是否成立,若否,则判定存在非法总召攻击,否则判断公式$\forall P\in P_{ZH}\Rightarrow Z_{hn}=\begin{cases} Z_{hs}, & A_s=00\mathrm{H} \\ 1, & A_s\in[01\mathrm{H},\mathrm{FFH}] \end{cases}$是否成立,若否,则判定存在非法总召攻击,否则将当前帧流量数据判定为正常流量;其中,Z_{h1}表示主站启动总召唤报文,Z_{h2}表示子站上送信息报文,Z_{h3}表示总召唤结束报文,P_{ZH}表示继电保护信息处理系统总召唤业务,Z_{hn}表示子站上送信息数目,Z_{hs}表示子站装置数量,A_s表示报文ASDU地址,H表示数值为16进制。

9.根据权利要求1所述的继电保护信息处理系统攻击行为监测方法,其特征在于,步骤S5中,当报文为通用文件传输业务,对解析后的报文进行攻击检测的具体实现过程包括:

检测文件名称是否只包含目录名和通配符,若含有其他的非法字符,则判定存在非法文件上送攻击,否则判断公式$\forall P\in P_{WJ}\Rightarrow T_{lb}(P)\in[C_q,C_z]$是否成立,若否,则判定存在文件时钟篡改攻击,否则将当前帧流量数据判定为正常流量;

其中,P_{WJ}表示继电保护信息处理系统文件列表上传报文,$T_{lb}(P)$表示文件列表上传时间,C_q表示文件列表时查询起始时间,C_z表示文件列表时查询终止时间。

10.一种计算机装置,包括存储器、处理器及存储在存储器上的计算机程序;其特征在于,所述处理器执行所述计算机程序,以实现权利要求1～9之一所述方法的步骤。

继电保护信息处理系统攻击行为监测方法及装置

技术领域

[0001] 本发明涉及电力系统信息安全技术领域，特别是一种继电保护信息处理系统攻击行为监测方法及装置。

背景技术

[0002] 随着变电站自动化、调度自动化水平的不断提高，电力系统信息化、智能化程度逐步增强。由继电保护装置、安全自动装置和故障录波器组成的继电保护信息处理系统已经成为电力系统的重要组成部分。继电保护信息处理系统能够实时采集继电保护装置的动作信息和运行状态信息，并对保护装置的动作信息进行自动、深入的分析，协助电力调度人员快速判断保护动作行为、进行故障定位、做出决策、处理事故。因此，继电保护信息的可靠传输与正确处理对电力系统的安全稳定运行具有重要意义。

[0003] 继电保护信息处理系统采用IEC 60870-5-103规约进行信息的传输，由于规约的自身设计存在缺乏认证机制、缺乏授权机制、缺乏加密机制的脆弱性，面临着报文的窃取、拦截、篡改等网络攻击。但是现有的继电保护系统网络攻击检测方法侧重于继电保护装置测量点的数据分析，容易出现误报、漏报等问题，同时缺乏针对具体继电保护业务在报文层面进行攻击行为的检测。因此，亟需发明一种新的继电保护信息处理系统攻击行为监测方法，提升检测攻击行为的准确性，增强电力系统的网络安全防御能力。

发明内容

[0004] 本发明所要解决的技术问题是，针对现有技术不足，提供一种继电保护信息处理系统攻击行为监测方法及装置，有效解决现有检测方法不能针对继电保护系统业务在应用层进行攻击行为检测的局限性，提升继电保护信息处理系统的安全性和可靠性。

[0005] 为解决上述技术问题，本发明所采用的技术方案是：一种继电保护信息处理系统攻击行为监测方法，包括以下步骤：

[0006] S1、实时捕获继电保护信息处理系统流量数据包，并提取出当前帧流量数据的应用层报文；

[0007] S2、对所述应用层报文进行字段级解析；

[0008] S3、对解析后的报文进行时钟篡改攻击检测，若报文的时钟范围、时钟逻辑、时钟同步、时钟延时不符合正常时钟特征，则判定存在时钟篡改攻击，否则进入步骤S4；

[0009] S4、对解析后的报文进行畸形报文攻击检测，若报文的长度字段、类型标识、传送原因、信息序号值与规约要求不符，则判定存在畸形报文攻击，否则进入步骤S5；

[0010] S5、按照解析后的报文所属的业务系统，对解析后的报文进行攻击检测，若解析后的报文不符合正常业务模型，则判定存在业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0011] 本发明对继电保护信息处理系统流量数据的应用层报文进行解析(按照IEC60870-5-103规约解析报文)，并对解析后的报文进行时钟篡改攻击检测、畸形报文攻击

检测、业务逻辑攻击检测，有效解决了现有检测方法不能针对继电保护系统业务在应用层进行攻击行为检测的局限性，提升了继电保护信息处理系统的安全性和可靠性。

[0012] 步骤S3中，对解析后的报文进行时钟篡改攻击检测的具体实现过程包括：

[0013] 1)判断公式$Y_t \in [1970,2069]$是否成立，若否，则判定为时钟篡改攻击，否则，进入步骤2)；其中，$Y_t = \begin{cases} y_t + 2000, y_t < 70 \\ y_t + 1900, y_t \geq 70 \end{cases}$，$Y_t$表示时标年份，$y_t$表示时标的年份标识字节数值；

[0014] 2)判断公式$\forall P \in P_{DS} \Rightarrow A_g(P) = \mathrm{FFH}$是否成立，若否，则判定为时钟篡改攻击，否则，进入步骤3)；其中，$\forall$表示全称量词“任意”，P为步骤S2解析后的应用层报文，P_{DS}表示IEC 60870-5-103对时报文，$A_g(P)$表示报文ASDU地址高8位的值，F表示16进制的15，H表示数值为16进制；

[0015] 3)判断公式$\forall P \in P_{DZ} \Rightarrow T_{js}(P) - T_{sj}(P) > 0$是否成立，若否，则判定为时钟篡改攻击，否则，进入步骤4)；其中，P_{DZ}表示IEC 60870-5-103告警、遥信变位、动作事件数据上送报文中的一种，$T_{js}(P)$表示事件子站接收时间，$T_{sj}(P)$表示事件实际发生时间；

[0016] 4)检测子站上送历史故障信息时间段与主站召唤故障历史信息时间段是否一致，若两者时间不一致，则判定为时钟篡改攻击，否则进入步骤5)；

[0017] 5)判断公式$\forall P \in P_{XC} \Rightarrow T_{cs}(P) < T_{max}$是否成立，若否，则判定为时钟篡改攻击，否则，进入步骤S4；其中，$T_{max} = \begin{cases} 0.5, P = P_1 \text{或} P_2 \text{或} P_3 \\ 6, \ P = P_4 \end{cases}$；$P_{XC}$表示IEC 60870-5-103主-子站信息传送报文，$T_{cs}(P)$表示信息传送时间，T_{max}表示最大延迟时间，P_1表示继电保护装置动作信息传送报文，P_2表示继电保护装置模拟量测量值传送报文，P_3表示继电保护装置运行状态传送报文，P_4表示继电保护装置定值传送报文。

[0018] 本发明通过对继电保护信息处理系统流量数据进行时钟篡改攻击检测，能够识别出针对时钟范围、时钟逻辑、时钟同步、时钟延时等时钟特征的攻击行为，克服了现有检测方法侧重于时标的数值分析而不能针对时标逻辑等特征进行异常检测的不足。时钟篡改攻击检测有效避免了各类继电保护装置因时钟异常导致不能正常工作状况的发生，同时也能够防止攻击者恶意扩大信息上送的时间范围而非法获取系统信息，提升了继电保护信息处理系统应对非数值时标篡改攻击的能力。

[0019] 对解析后的报文进行畸形报文攻击检测的具体实现过程包括：

[0020] I)判断公式$\forall P \in P_{IEC103} \Rightarrow F_l(P) = L_s(P)$是否成立，若否，则判定为畸形报文攻击，否则进入步骤II)；其中，P_{IEC103}表示IEC 60870-5-103报文，$F_1(P)$表示报文理论长度，$L_s(P)$表示报文实际长度；

[0021] II)判断公式$\forall P \in P_{IEC103} \Rightarrow L_s(P) \leq 2048$是否成立，若否，则判定为畸形报文攻击，否则进入步骤III)；

[0022] III)判断公式$\forall P \in P_{IEC103} \Rightarrow F_t(P) \in [1.31]$是否成立，若否，判定为畸形报文攻击，否则进入步骤IV)；其中，$F_t(P)$表示报文类型标识字段值；

[0023] IV)判断公式$\forall P \in P_{IEC103} \Rightarrow F_c(P) \in [1,63]$是否成立，若否，判定为畸形报文攻击，否则进入步骤V)；其中，$F_c(P)$表示报文传送原因字段值；

[0024] V)判断公式$\forall P \in P_{IEC103} \Rightarrow F_i(P) \in \{[0,159],[240,255]\}$是否成立,若否,判定为畸形报文攻击,否则进入步骤S5;F_i(P)表示报文信息序号字段值。

[0025] 本发明畸形报文攻击检测过程能够在报文格式正确的情况下识别出畸形报文,包括报文长度畸形、报文字段阈值畸形等,克服了现有方法仅能针对报文格式进行合法性校验的局限性。同时,畸形报文攻击检测在报文所属具体业务未执行前发现其畸形之处,从而快速向调度中心反应,重新建立继电保护信息处理系统中该业务的通信过程,并发送正常的业务报文,避免畸形报文在执行后出现异常,进而影响正常业务的执行过程。

[0026] 步骤S5中,当报文为读取子站配置业务时,对解析后的报文进行攻击检测的具体实现过程包括:

[0027] 判断公式$\forall P \in P_{BT} \Rightarrow B_n(P) == B_s$是否成立,若否,则判定存在配置数据恶意拦截攻击,否则,判断公式$\forall P \in P_{BT} \Rightarrow \forall B_{zh}(P) == C_{zh}$是否成立,若否,则判定存在数据篡改攻击,否则将当前帧流量数据判定为正常流量;其中,P_{BT}表示继电保护信息处理系统中读取子站配置业务报文,B_n(P)表示子站上送标题数目,B_s表示子站配置的所有标题数目,B_{zh}(P)表示同一组标题信息的各个条目的组号,C_{zh}表示当前组标题信息的组号。

[0028] 本发明的读取子站配置业务逻辑攻击行为检测能够实现配置信息是否完整上送、配置信息的条目和组号是否一致的检测。配置信息的完整上送和条目、组号的一致性是保障继电保护装置正常运行的前提,该检测方法克服了现有继电保护信息处理系统攻击行为检测方法侧重于对继电保护装置测量点的数据分析,缺乏针对流量数据应用层报文的业务逻辑进行攻击行为检测的不足,有效避免了配置信息被拦截和篡改的风险。

[0029] 步骤S5中,当报文为保护事件上送业务,对解析后的报文进行攻击检测的具体实现过程包括:

[0030] A)判断公式$\forall P \in P_{BH} \Rightarrow D_{pi}(P) \in \{0,1,2,3\}$是否成立,若否,则判定存在双点信息恶意篡改攻击,否则,进入步骤B);其中,P_{BH}表示继电保护信息处理系统中保护事件上送报文,D_{pi}(P)表示双点信息数值;

[0031] B)检测开关量变位、动作信号、压板状态前后帧报文逻辑是否正确,若开关量变位前一帧为开/合,后一帧仍为开/合;动作信号前一帧为复归/动作,后一帧仍为复归/动作;压板状态前一帧为未投入/投入,后一帧仍为未投入/投入,则判定存在恶意开合攻击,否则进入步骤C);

[0032] C)判断公式$\forall P \in P_{BH} \Rightarrow L_{bh}(P) = \begin{cases} 1, P = P_5 \\ 2, P = P_6 \end{cases}$是否成立,若否,则判定存在动作事件非法上送攻击,否则将当前帧流量数据判定为正常流量;其中,L_{bh}(P)表示保护事件报文类型标识,P_5表示告警或开关量变位事件报文,P_6表示动作事件报文。

[0033] 本发明的保护事件上送业务逻辑攻击行为检测能够实现继电保护信息处理系统中各类保护事件的恶意篡改攻击检测、非法上送攻击检测。保护事件的业务逻辑攻击行为能够高度隐藏在正常的流量数据中,现有的方法仅通过对继电保护装置测量点的数据进行分析,难以检测到该类高能隐身攻击行为。本发明深入融合了流量数据应用层报文中保护事件的上送业务逻辑,从而提升了继电保护信息处理系统攻击行为的准确性。

[0034] 步骤S5中,当报文为录波简报上送业务时对解析后的报文进行攻击检测的具体实

现过程包括：

[0035] i)判断公式$\forall P \in P_{LB} \Rightarrow G_{xb}(P) == Z_{xb}(P)$是否成立，若否，则判定存在跳闸相别恶意篡改攻击，否则进入步骤ii)；其中，P_{LB}表示继电保护信息处理系统中录波简报业务报文，$G_{xb}(P)$表示故障相别，$Z_{xb}(P)$表示跳闸相别；

[0036] ii)判断公式$\forall P \in P_{LB} \Rightarrow D_3 = \begin{cases} 1\ , & D_0 = 1 \wedge D_1 = 1 \wedge D_2 = 1 \\ 0或1, & D_0 = 0 \vee D_1 = 0 \vee D_2 = 0 \end{cases}$是否成立，若否，则判定存在接地故障标志位数据篡改攻击，否则进入步骤iii)；其中，D_3表示报文短路接地故障标志位数值，D_0表示报文A相短路故障标志位数值，D_1表示报文B相故短路障标志位数值，D_2表示报文C相短路故障标志位数值；

[0037] iii)检测录波简报中的重合闸是否异常，若故障发生后有重合闸，但重合闸时间为0，或者没有重合闸，但重合闸时间不为0，则判定存在重合闸时间篡改攻击，否则将当前帧流量数据判定为正常流量。

[0038] 本发明的录波简报上送业务逻辑攻击行为检测能够判别跳闸相别恶意篡改攻击、接地故障标志位数据篡改攻击以及重合闸时间篡改攻击。跳闸相别、故障标志、重合闸时间等录波简报上送业务的信息须通过对继电保护信息系统流量数据应用层报文的字段级深度解析提取，仅通过报文的格式校验不能识别出该类攻击行为。本发明所提供的攻击行为检测方法克服了现有检测方法不能针对录波简报的时序和上下文逻辑进行检测的局限性，提升了对录波简报数据的完整性、准确性进行防护的能力。

[0039] 步骤S5中，当报文为定值操作业务时，对解析后的报文进行攻击检测的具体实现过程包括：

[0040] 判断逻辑$X_{g1} \rightarrow X_{g2} \rightarrow X_{g3} \rightarrow X_{g4} \rightarrow X_{g5} \rightarrow X_{g6} \rightarrow X_{g7} \rightarrow X_{g8}$是否成立，若否，则判定存在继电保护装置整定值恶意篡改攻击，否则将当前帧流量数据判定为正常流量；其中，X_{g1}表示召唤装置当前运行定值区号报文，X_{g2}表示子站上传装置当前运行定值区号报文，X_{g3}表示主站召唤装置定值报文，X_{g4}表示子站上传装置定值报文，X_{g5}表示向子站下装定值报文，X_{g6}表示响应子站下装定值报文，X_{g7}表示执行定值修改报文，X_{g8}子站响应定值修改报文。

[0041] 本发明的定值操作业务逻辑攻击行为检测根据正常的定值修改逻辑能够在定值修改过程中判别出继电保护装置整定值恶意篡改攻击，并对恶意篡改定值的攻击行为进行主动阻断。而现有的继电保护装置测量点数据分析方法只能在定值被篡改后进行检测，不能及时监测和阻断定值的修改。本发明提供的定值操作业务逻辑攻击行为检测方法深入到流量数据的应用层，能够有效防止继电保护装置的整定值被恶意篡改，对继电保护装置的正确动作具有重要意义。

[0042] 步骤S5中，当报文为总召唤业务时，对解析后的报文进行攻击检测的具体实现过程包括：

[0043] 判断逻辑$Z_{h1} \rightarrow Z_{h2} \rightarrow Z_{h3}$是否成立，若否，则判定存在非法总召攻击，否则判断公式$\forall P \in P_{ZH} \Rightarrow Z_{hn} = \begin{cases} Z_{hs}, & A_s = 00\mathrm{H} \\ 1, & A_s \in [01\mathrm{H}, \mathrm{FFH}] \end{cases}$是否成立，若否，则判定存在非法总召攻击，否则将当前帧流量数据判定为正常流量；其中，Z_{h1}表示主站启动总召唤报文，Z_{h2}表示子站上送信息报文，Z_{h3}表示总召唤结束报文，P_{ZH}表示继电保护信息处理系统总召唤业务，Z_{hn}表示子站

上送信息数目，Z_{hs}表示子站装置数量，A_s表示报文ASDU地址，H表示数值为16进制。

[0044] 本发明的总召唤业务逻辑攻击行为检测能够根据总召唤的正常业务逻辑判别出非法总召攻击。非法总召攻击能够将构造的总召唤业务报文通过篡改或注入的方式与正常的总召唤业务报文进行组合，从而进行数据的非法获取。这种攻击行为仅通过对报文字段的合法性检查以及遥测数据的一致性分析不能识别，必须深入到报文的业务逻辑层面进行攻击行为的识别。本发明提供的总召唤业务逻辑攻击行为检测通过对总召唤业务的逻辑、范围进行检测，可以有效识别出针对总召唤业务的攻击行为，防止信息的冗余上送以及残缺上送。

[0045] 步骤S5中，当报文为通用文件传输业务，对解析后的报文进行攻击检测的具体实现过程包括：检测文件名称是否只包含目录名和通配符，若含有其他的非法字符，则判定存在非法文件上送攻击，否则判断公式$\forall P \in P_{WJ} \Rightarrow T_{lb}(P) \in [C_q, C_z]$是否成立，若否，则判定存在文件时钟篡改攻击，否则将当前帧流量数据判定为正常流量；其中，P_{WJ}表示继电保护信息处理系统文件列表上传报文，$T_{lb}(P)$表示文件列表上传时间，C_q表示文件列表时查询起始时间，C_z表示文件列表时查询终止时间。

[0046] 本发明的通用文件传输业务逻辑攻击行为检测能够判别出非法文件上送攻击、文件时钟篡改攻击。包含有攻击代码的非法文件一旦上送到主站，会使主站失去控制权限；文件时钟篡改攻击通过对文件上传列表的时间进行篡改，从而非法窃取信息。本发明提供的通用文件传输业务逻辑攻击行为检测克服了现有方法侧重于网络层流量统计分析的局限性，能够有效防止攻击者通过上送恶意文件数据或篡改文件时间导致主站崩溃、文件被窃取情况的发生。

[0047] 一种计算机装置，包括存储器、处理器及存储在存储器上的计算机程序；所述处理器执行所述计算机程序，以实现本发明方法的步骤。

[0048] 与现有技术相比，本发明所具有的有益效果为：

[0049] (1)本发明针对继电保护信息处理系统面临的报文窃取、拦截、篡改等网络攻击风险，提出了流量数据应用层报文的攻击行为检测方法，克服了现有攻击检测方法侧重于继电保护装置测量点数据分析的局限性。

[0050] (2)本发明提出了针对继电保护信息处理系统流量数据应用层报文的时钟篡改攻击与畸形报文攻击检测，克服了IEC 60870-5-103规约缺乏认证机制、缺乏授权机制、缺乏加密机制的不足。

[0051] (3)本发明根据继电保护信息处理系统的业务特征建立电力业务正常行为模型，对流量数据的应用层报文进行攻击行为检测，实现了对继电保护信息处理系统流量数据在应用层的攻击行为主动防御，提升了业务系统信息传输的安全性。

附图说明

[0052] 图1是本发明实施例中的继电保护信息处理系统攻击行为监测方法的流程图。

[0053] 图2是本发明实施例中继电保护信息处理系统攻击行为监测系统的结构示意图。

[0054] 图3是本发明实施例中时钟篡改攻击检测模块的系统单元图。

[0055] 图4是本发明实施例中畸形报文攻击检测模块的系统单元图。

[0056] 图5是本发明实施例中业务逻辑攻击检测模块的系统单元图。

具体实施方式

[0057] 图1为本发明实施例提供的继电保护信息处理系统攻击行为监测方法的流程图，具体实施步骤如下：

[0058] 步骤S1：实时捕获继电保护信息处理系统流量数据包，并提取出当前帧流量数据的应用层报文；

[0059] 步骤S2：按照IEC 60870-5-103规约对报文进行字段级解析，获取报文长度字段、类型标识、传送原因、信息序号的具体数值以及时钟特征，并确定报文所属系统业务；

[0060] 步骤S3：对步骤S2解析后的报文进行时钟篡改攻击检测，如果报文的时钟范围、时钟逻辑、时钟同步、时钟延时不符合正常时钟特征，则判定存在时钟篡改攻击，否则进入步骤S4；

[0061] 步骤S4：对步骤S2解析后的报文进行畸形报文攻击检测，如果报文的长度字段、类型标识、传送原因、信息序号值与规约要求不符，则判定存在畸形报文攻击，否则进入步骤S5；

[0062] 步骤S5：按照报文所属系统业务建立正常行为模型，依据正常行为模型对报文进行攻击检测，如果报文不符合正常业务模型，则判定存在业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0063] 进一步的，步骤S3包括：

[0064] S3-1：检测报文时标年份是否在正常范围内，如果时标年份越限，即违反式(1)，则判定为时钟篡改攻击，否则进入步骤S3-2。

[0065] $Y_t \in [1970,2069]$ (1)

[0066] $$Y_t = \begin{cases} y_t + 2000, y_t < 70 \\ y_t + 1900, y_t \geq 70 \end{cases} \quad (2)$$

[0067] 其中，Y_t表示时标年份，y_t表示时标的年份标识字节数值。

[0068] S3-2：检测对时报文是否为广播对时。主站下发广播对时命令，是针对所有的装置进行对时，此时报文的应用服务数据单元公共地址(简称ASDU地址)高8位为FFH，表示对子站内所有装置广播，如果违反式(3)，则判定为时钟篡改攻击，否则进入步骤S3-3。

[0069] $$\forall P \in P_{DS} \Rightarrow A_g(P) = \mathrm{FFH} \quad (3)$$

[0070] 其中，∀表示全称量词“任意”，P为步骤S2解析后的应用层报文，P_{DS}表示IEC60870-5-103对时报文，$A_g(P)$表示报文ASDU地址高8位的值，F表示16进制的15，H表示数值为16进制。

[0071] S3-3：检测告警、遥信变位、动作事件的实际发生时间与子站接收时间逻辑是否正确。告警、遥信变位、动作事件发生后继电保护装置会记录事件实际发生时间，子站接收到故障信息会有一定的延迟，因此子站接收时间一定大于实际发生时间，如果违反式(4)，则判定为时钟篡改攻击，否则进入步骤S3-4。

[0072] $$\forall P \in P_{DZ} \Rightarrow T_{js}(P) - T_{sj}(P) > 0 \quad (4)$$

[0073] 其中，P_{DZ}表示IEC 60870-5-103告警、遥信变位、动作事件数据上送报文中的一种，$T_{js}(P)$表示事件子站接收时间，$T_{sj}(P)$表示事件实际发生时间。

[0074] S3-4：检测子站上送历史故障信息时间段与主站召唤故障历史信息时间段是否一

致，如果两者时间不一致，则判定为时钟篡改攻击，否则进入步骤S3-5。

[0075] S3-5：检测主-子站信息传送是否超时。如果信息传送时间超过规约所要求的最大延迟时间，即违反公式(5)，则判定为时钟篡改攻击，否则进入步骤S4。

[0076] $$\forall P \in P_{XC} \Rightarrow T_{cs}(P) < T_{max} \quad (5)$$

[0077] $$T_{max} = \begin{cases} 0.5, P = P_1 或 P_2 或 P_3 \\ 6, \ P = P_4 \end{cases} \quad (6)$$

[0078] 其中，P_{XC}表示IEC 60870-5-103主-子站信息传送报文，$T_{cs}(P)$表示信息传送时间，T_{max}表示最大延迟时间，P_1表示继电保护装置动作信息传送报文，P_2表示继电保护装置模拟量测量值传送报文，P_3表示继电保护装置运行状态传送报文，P_4表示继电保护装置定值传送报文。

[0079] 进一步的，步骤S4包括：

[0080] S4-1：针对步骤S2解析后的报文，检测由长度字段计算出的报文理论长度与实际长度是否相等，如果不相等，即违反公式(7)，则判定为畸形报文攻击，否则进入步骤S4-2。

[0081] $$\forall P \in P_{IEC103} \Rightarrow F_l(P) = L_s(P) \quad (7)$$

[0082] 其中，P_{IEC103}表示IEC 60870-5-103报文，$F_l(P)$表示报文理论长度，$L_s(P)$表示报文实际长度。

[0083] S4-2：检测报文实际长度是否大于2048字节，如果大于，即违反公式(8)，则判定为畸形报文攻击，否则进入步骤S4-3。

[0084] $$\forall P \in P_{IEC103} \Rightarrow L_s(P) \le 2048 \quad (8)$$

[0085] S4-3：检测报文的类型标识字段值是否有效，如果无效，即违反公式(9)则判定为畸形报文攻击，否则进入步骤S4-4。

[0086] $$\forall P \in P_{IEC103} \Rightarrow F_t(P) \in [1.31] \quad (9)$$

[0087] 其中，$F_t(P)$表示报文类型标识字段值。

[0088] S4-4：检测报文的传送原因字段值是否有效，如果无效，即违反公式(10)则判定为畸形报文攻击，否则进入步骤S4-5。

[0089] $$\forall P \in P_{IEC103} \Rightarrow F_c(P) \in [1,63] \quad (10)$$

[0090] 其中，$F_c(P)$表示报文传送原因字段值。

[0091] S4-5：检测报文的信息序号字段值是否有效，如果无效，即违反公式(11)则判定为畸形报文攻击，否则进入步骤S5。

[0092] $$\forall P \in P_{IEC103} \Rightarrow F_i(P) \in \{[0,159],[240,255]\} \quad (11)$$

[0093] 其中，$F_i(P)$表示报文信息序号字段值。

[0094] 进一步的，步骤S5包括：

[0095] S5-1：针对步骤S2得到的报文所属的业务进行攻击行为的分类检测，如果报文为读取子站配置业务，进入步骤S5-2；如果报文为保护事件上送业务，进入步骤S5-3；如果报文为录波简报上送业务，进入步骤S5-4；如果报文为定值操作业务，进入步骤S5-5；如果报文为总召唤业务，进入步骤S5-6；如果报文为通用文件传输业务，进入步骤S5-7；

[0096] S5-2：根据继电保护信息处理系统技术规范对读取子站配置业务的正常逻辑进行

分析，基于正常业务逻辑建立读取子站配置业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在读取子站配置业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0097] S5-3：根据继电保护信息处理系统技术规范对保护事件上送业务的正常逻辑进行分析，基于正常业务逻辑建立保护事件上送业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在保护事件上送业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0098] S5-4：根据继电保护信息处理系统技术规范对录波简报上送业务的正常逻辑进行分析，基于正常业务逻辑建立录波简报上送业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在录波简报上送业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0099] S5-5：根据继电保护信息处理系统技术规范对定值操作业务的正常逻辑进行分析，基于正常业务逻辑建立定值操作业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在定值操作业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0100] S5-6：根据继电保护信息处理系统技术规范对总召唤业务的正常逻辑进行分析，基于正常业务逻辑建立总召唤业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在总召唤业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0101] S5-7：根据继电保护信息处理系统技术规范对通用文件传输业务的正常逻辑进行分析，基于正常业务逻辑建立通用文件传输业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在通用文件传输业务逻辑攻击，否则将当前帧流量数据判定为正常流量。

[0102] 进一步的，步骤S5-2包括：

[0103] S5-2-1：检测继电保护信息处理系统读取子站配置的各组标题时子站上送标题数目是否完整，如果不完整，即违反公式(12)，则判定存在配置数据恶意拦截攻击，否则进入步骤S5-2-2。

[0104] $$\forall P \in P_{BT} \Rightarrow B_n(P) == B_s \qquad (12)$$

[0105] 其中，P_{BT}表示继电保护信息处理系统中读取子站配置业务报文，$B_n(P)$表示子站上送标题数目，B_s表示子站配置的所有标题数目。

[0106] S5-2-2：检测同一组标题信息所有条目的组号是否一致，如果不一致，即违反公式(13)，则判定存在数据篡改攻击，否则将当前帧流量数据判定为正常流量。

[0107] $$\forall P \in P_{BT} \Rightarrow \forall B_{zh}(P) == C_{zh} \qquad (13)$$

[0108] 其中，$B_{zh}(P)$表示同一组标题信息的各个条目的组号，C_{zh}表示当前组标题信息的组号。

[0109] 进一步的，步骤S5-3包括：

[0110] S5-3-1：检测保护事件双点信息上送是否异常，如果双点信息状态不在规定范围内，即违反公式(14)，则判定存在双点信息恶意篡改攻击，否则进入步骤S5-3-2。

[0111] $$\forall P \in P_{BH} \Rightarrow D_{pi}(P) \in \{0,1,2,3\} \quad (14)$$

[0112] 其中，P_{BH}表示继电保护信息处理系统中保护事件上送报文，$D_{pi}(P)$表示双点信息数值。

[0113] S5-3-2：检测开关量变位、动作信号、压板状态前后帧报文逻辑是否正确，如果开关量变位前一帧为开/合，后一帧仍为开/合；动作信号前一帧为复归/动作，后一帧仍为复归/动作；压板状态前一帧为未投入/投入，后一帧仍为未投入/投入，则判定存在恶意开合攻击，否则进入步骤S5-3-3。

[0114] S5-3-3：检测保护事件上送采用的类型标识是否正确，告警、开关量变位事件只能采用类型标识1上送，动作事件只能采用类型标识2上送，如果违反公式(15)，则判定存在动作事件非法上送攻击，否则将当前帧流量数据判定为正常流量。

[0115] $$\forall P \in P_{BH} \Rightarrow L_{bh}(P) = \begin{cases} 1, P = P_5 \\ 2, P = P_6 \end{cases} \quad (15)$$

[0116] 其中，$L_{bh}(P)$表示保护事件报文类型标识，P_5表示告警或开关量变位事件报文，P_6表示动作事件报文。

[0117] 进一步的，步骤S5-4包括：

[0118] S5-4-1：检测录波简报中的故障相别与跳闸相别是否一致，如果不一致，即违反公式(16)，则判定存在跳闸相别恶意篡改攻击，否则进入步骤S5-4-2。

[0119] $$\forall P \in P_{LB} \Rightarrow G_{xb}(P) == Z_{xb}(P) \quad (16)$$

[0120] 其中，P_{LB}表示继电保护信息处理系统中录波简报业务报文，$G_{xb}(P)$表示故障相别，$Z_{xb}(P)$表示跳闸相别。

[0121] S5-4-2：检测录波简报中的短路接地故障标志位是否正确，如果不正确，即违反公式(17)，则判定接地故障标志位数据篡改攻击，否则进入步骤S5-4-3。

[0122] $$\forall P \in P_{LB} \Rightarrow D_3 = \begin{cases} 1, & D_0 = 1 \wedge D_1 = 1 \wedge D_2 = 1 \\ 0\text{或}1, & D_0 = 0 \vee D_1 = 0 \vee D_2 = 0 \end{cases} \quad (17)$$

[0123] 其中，D_3表示报文短路接地故障标志位数值，D_0表示报文A相短路故障标志位数值，D_1表示报文B相故短路障标志位数值，D_2表示报文C相短路故障标志位数值。

[0124] S5-4-3：检测录波简报中的重合闸是否异常。如果故障发生后有重合闸，但重合闸时间为0或者没有重合闸，但重合闸时间不为0，则判定存在重合闸时间篡改攻击，否则将当前帧流量数据判定为正常流量。

[0125] 进一步的，步骤S5-5包括：

[0126] S5-5-1：检测继电保护装置定值修改逻辑是否正确，如果逻辑错误，即违反公式(18)，则判定存在继电保护装置整定值恶意篡改攻击，否则将当前帧流量数据判定为正常流量。

[0127] $$X_{g1} \rightarrow X_{g2} \rightarrow X_{g3} \rightarrow X_{g4} \rightarrow X_{g5} \rightarrow X_{g6} \rightarrow X_{g7} \rightarrow X_{g8} \quad (18)$$

[0128] 其中，X_{g1}表示召唤装置当前运行定值区号报文，X_{g2}表示子站上传装置当前运行定值区号报文，X_{g3}表示主站召唤装置定值报文，X_{g4}表示子站上传装置定值报文，X_{g5}表示向子站下装定值报文，X_{g6}表示响应子站下装定值报文，X_{g7}表示执行定值修改报文，X_{g8}子站响应定值修改报文。

[0129] 进一步的,步骤S5-6包括:

[0130] S5-6-1:检测总召唤的业务流程是否异常,如果实际总召唤业务流程与正常流程不符,即违反公式(19),则判定存在非法总召攻击,否则进入步骤S5-6-2。

[0131] $Z_{h1}\rightarrow Z_{h2}\rightarrow Z_{h3}$ (19)

[0132] 其中,Z_{h1}表示主站启动总召唤报文,Z_{h2}表示子站上送信息报文,Z_{h3}表示总召唤结束报文。

[0133] S5-6-2:检测子站上送信息的数目是否正确。子站收到主站的总召唤命令后根据报文中ASDU地址回复指定信息,当ASDU地址不等于零时回答特定装置的开关量信息;当ASDU地址等于零时回答子站各装置的通信状态以及各装置的运行状态。如果违反公式(20),则判定存在非法总召攻击,否则将当前帧流量数据判定为正常流量。

[0134] $$\forall P\in P_{ZH}\Rightarrow Z_{hn}=\begin{cases} Z_{hs}, & A_s=00\mathrm{H} \\ 1, & A_s\in[01\mathrm{H},\mathrm{FFH}] \end{cases} \quad (20)$$

[0135] 其中,P_{ZH}表示继电保护信息处理系统总召唤业务,Z_{hn}表示子站上送信息数目,Z_{hs}表示子站装置数量,A_s表示报文ASDU地址,H表示数值为16进制。

[0136] 进一步的,步骤S5-7包括:

[0137] S5-7-1:检测文件名称是否只包含目录名和通配符(*和?),如果含有其他的非法字符则判定存在非法文件上送攻击,否则进入步骤S5-7-2。

[0138] S5-7-2:检测文件列表上传是否在查询时间范围内。主站召唤文件列表时会给出查询起始时间和终止时间,子站上传的文件列表需要在该时间范围内,如果超出,即违反公式(21),则判定存在文件时钟篡改攻击,否则将当前帧流量数据判定为正常流量。

[0139] $$\forall P\in P_{WJ}\Rightarrow T_{lb}(P)\in[C_q,C_z] \quad (21)$$

[0140] 其中,P_{WJ}表示继电保护信息处理系统文件列表上传报文,$T_{lb}(P)$表示文件列表上传时间,C_q表示文件列表时查询起始时间,C_z表示文件列表时查询终止时间。

[0141] 本发明依托海量继电保护信息处理系统流量数据,通过提取流量数据的应用层报文并按照IEC 60870-5-103规约进行报文解析,获取报文特征字段的具体数值以及报文所属系统业务。其次根据报文特征字段的具体数值进行时钟篡改攻击检测与畸形报文攻击检测。最后根据报文所属具体系统业务建立正常业务模型,并依据正常业务模型进行业务逻辑攻击检测,实现了继电保护信息处理系统攻击行为的全面监测,确保电力系统的安全、可靠运行。

[0142] 图2为本发明实施例提供的继电保护信息处理系统攻击行为监测系统的结构示意图,该系统适用于执行本发明任意实施例提供的方法,包括:流量数据获取模块100,应用层报文解析模块200,时钟篡改攻击检测模块300,畸形报文攻击检测模块400,业务逻辑攻击检测模块500。

[0143] 所述的流量数据获取模块100,用于采集继电保护信息处理系统流量数据,并提取出应用层报文。

[0144] 所述的应用层报文解析模块200,用于按照IEC 60870-5-103规约对应用层报文进行字段级解析,获取报文表示的具体继电保护业务。

[0145] 所述的时钟篡改攻击检测模块300,用于对报文的时钟范围、时钟逻辑、时钟同步、

时钟延时进行检测，判定是否存在时钟篡改攻击。

[0146] 所述的畸形报文攻击检测模块400，用于按照规约要求对报文格式进行校验，判定是否存在畸形报文攻击。

[0147] 所述的业务逻辑攻击检测模块500，用于对报文所属系统业务建立正常行为模型，并依据正常行为模型进行检测，判定是否存在业务逻辑攻击。

[0148] 所述流量数据获取模块100输出端与所述应用层报文解析模块200输入端相连，用于输入所提取的应用层报文。

[0149] 所述应用层报文解析模块200输出端与时钟篡改攻击检测模块300输入端相连，用于输入应用层报文及其解析结果。

[0150] 所述时钟篡改攻击检测模块300的输出端与所述的畸形报文攻击检测模块400输入端相连，用于输入应用层报文及其解析结果。

[0151] 所述畸形报文攻击检测模块400的输出端与所述的业务逻辑攻击检测模块500输入端相连，用于输入应用层报文及其解析结果。

[0152] 如图3，进一步的，时钟篡改攻击检测模块300包括：数据获取单元301，第一检测单元302，第二检测单元303，第三检测单元304，第四检测单元305，第五检测单元306。

[0153] 所述数据获取单元301的输出端与所述第一检测单元302输入端相连，用于输入应用层报文及其解析结果。

[0154] 所述第一检测单元302的输出端与第二检测单元303的输入端相连，所述第二检测单元303的输出端与第三检测单元304的输入端相连，所述第三检测单元304的输出端与第四检测单元305的输入端相连，所述第四检测单元305的输出端与第五检测单元306的输入端相连。

[0155] 在一个实施例中，数据获取单元301，读取流量数据的应用层报文及其解析结果，该单元将所读取信息传递给第一检测单元302、第二检测单元303、第三检测单元304、第四检测单元305，第五检测单元306。

[0156] 所述第一检测单元302，用于检测报文时标年份是否在正常范围内，如果时标年份越限，则判定为时钟篡改攻击。

[0157] 所述第二检测单元303，用于检测对时报文是否为广播对时，若否，则判定为时钟篡改攻击。

[0158] 所述第三检测单元304，用于检测告警、遥信变位、动作事件数据上送实际发生时间与子站接收时间逻辑是否正确，若否，则判定为时钟篡改攻击。

[0159] 所述第四检测单元305，用于检测子站上送历史故障信息时间段与主站召唤故障历史信息时间段是否一致，若否，则判定为时钟篡改攻击。

[0160] 所述第五检测单元306，用于主-子站信息传送是否超时，若是，则判定为时钟篡改攻击。

[0161] 如图4，进一步的，所述畸形报文攻击检测模块400包括：数据获取单元401，报文长度字段检测单元402，报文长度阈值检测单元403，类型标识字段检测单元404，传送原因字段检测单元405，信息序号字段检测单元406。

[0162] 所述数据获取单元401的输出端与所述报文长度字段检测单元402输入端相连，用于输入应用层报文及其解析结果。

[0163] 所述报文长度字段检测单元402的输出端与报文长度阈值检测单元403的输入端相连，所述报文长度阈值检测单元403的输出端与类型标识字段检测单元404的输入端相连，所述类型标识字段检测单元404的输出端与传送原因字段检测单元405的输入端相连，所述传送原因字段检测单元405的输出端与信息序号字段检测单元406的输入端相连。

[0164] 在一个实施例中，数据获取单元401，读取流量数据应用层报文及其解析结果，该单元将所读取信息传递给报文长度字段检测单元402、报文长度阈值检测单元403、类型标识字段检测单元404、传送原因字段检测单元405，信息序号字段检测单元406。

[0165] 所述报文长度字段检测单元402，用于检测由长度字段计算出的报文理论长度与实际长度是否相等，如果不相等，则判定为畸形报文攻击。

[0166] 所述报文长度阈值检测单元403，用于检测报文实际长度是否大于2048字节，如果大于，则判定为畸形报文攻击。

[0167] 所述类型标识字段检测单元404，用于检测报文的类型标识字段值是否有效，如果无效，则判定为畸形报文攻击。

[0168] 所述传送原因字段检测单元405，用于检测报文的传送原因字段值是否有效，如果无效，则判定为畸形报文攻击。

[0169] 所述信息序号字段检测单元406，用于检测报文的信息序号字段值是否有效，如果无效，则判定为畸形报文攻击。

[0170] 如图5，进一步的，所述业务逻辑攻击检测模块500包括：数据获取单元501，读取子站配置业务检测单元502，保护事件上送业务检测单元503，录波简报上送业务检测单元504，定制操作业务检测单元505，总召唤业务检测单元506，通用文件传输业务检测单元507。

[0171] 所述数据获取单元501的输出端与所述读取子站配置业务检测单元502输入端相连，用于输入报文所属继电保护业务。

[0172] 所述读取子站配置业务检测单元502的输出端与保护事件上送业务检测单元503的输入端相连，所述保护事件上送业务检测单元503的输出端与录波简报上送业务检测单元504的输入端相连，所述录波简报上送业务检测单元504的输出端与定制操作业务检测单元505的输入端相连，所述定制操作业务检测单元505的输出端与总召唤业务检测单元506的输入端相连，所述总召唤业务检测单元506的输出端与通用文件传输业务检测单元507的输入端相连。

[0173] 在一个实施例中，数据获取单元501，获取报文所属具体继电保护业务，该单元将读取信息传递给读取子站配置业务检测单元502、保护事件上送业务检测单元503、录波简报上送业务检测单元504、定制操作业务检测单元505、总召唤业务检测单元506、通用文件传输业务检测单元507。

[0174] 所述读取子站配置业务检测单元502，用于检测继电保护信息处理系统中读取子站配置业务中是否存在攻击行为。

[0175] 在一个实施例中，建立读取子站配置业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在读取子站配置业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

[0176] 所述保护事件上送业务检测单元503，用于检测保护事件上送业务中是否存在攻击行为。

[0177] 在一个实施例中，建立保护事件上送业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在保护事件上送业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

[0178] 所述录波简报上送业务检测单元504，用于检测录波简报上送业务中是否存在攻击行为。

[0179] 在一个实施例中，建立录波简报上送业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在录波简报上送业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

[0180] 所述定制操作业务检测单元505，用于检测定值操作业务中是否存在攻击行为。

[0181] 在一个实施例中，建立定值操作业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在定制操作业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

[0182] 所述总召唤业务检测单元506，用于检测总召唤业务中是否存在攻击行为。

[0183] 在一个实施例中，建立总召唤业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在总召唤业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

[0184] 所述通用文件传输业务检测单元507，用于检测通用文件传输业务中是否存在攻击行为。

[0185] 在一个实施例中，建立通用文件传输业务的正常行为模型，依据正常行为模型对继电保护信息处理系统中该业务的流量数据进行攻击行为检测，如果报文不符合正常行为模型，则判定存在通用文件传输业务逻辑攻击，该单元将检测结果作为业务逻辑攻击检测模块500的输出端。

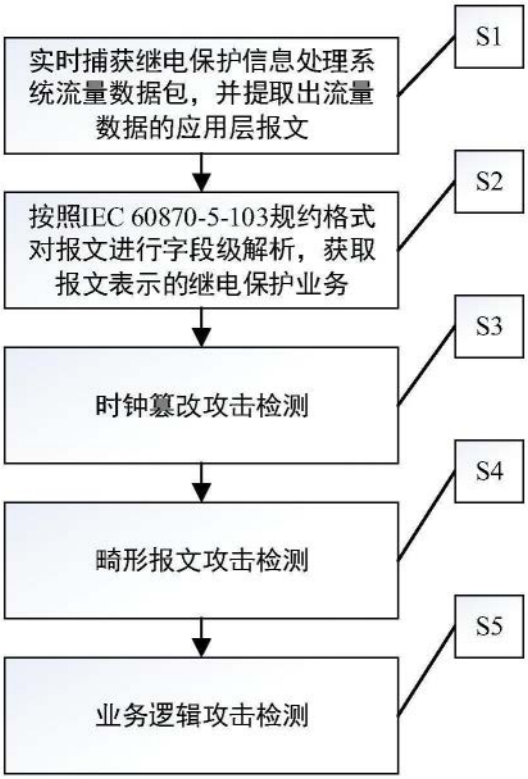

实时捕获继电保护信息处理系统流量数据包，并提取出流量数据的应用层报文
S1
按照IEC 60870-5-103规约格式对报文进行字段级解析，获取报文表示的继电保护业务
S2
时钟篡改攻击检测
S3
畸形报文攻击检测
S4
业务逻辑攻击检测
S5

图1

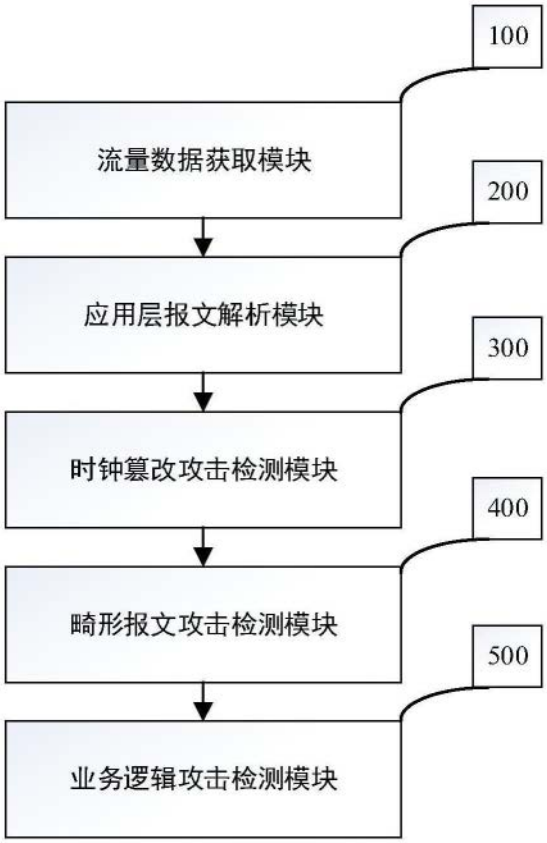

100
流量数据获取模块
200
应用层报文解析模块
300
时钟篡改攻击检测模块
400
畸形报文攻击检测模块
500
业务逻辑攻击检测模块

图2

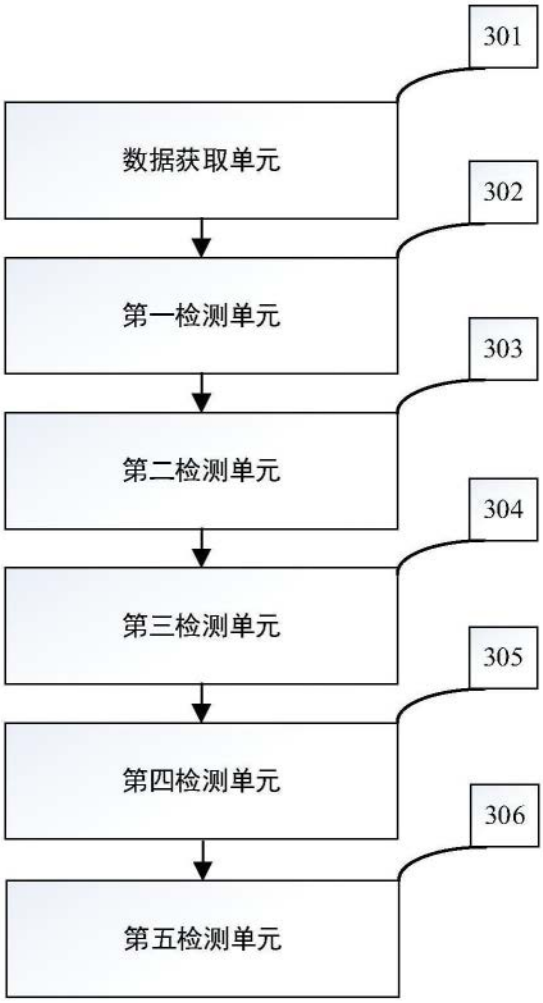

301
数据获取单元
302
第一检测单元
303
第二检测单元
304
第三检测单元
305
第四检测单元
306
第五检测单元

图3

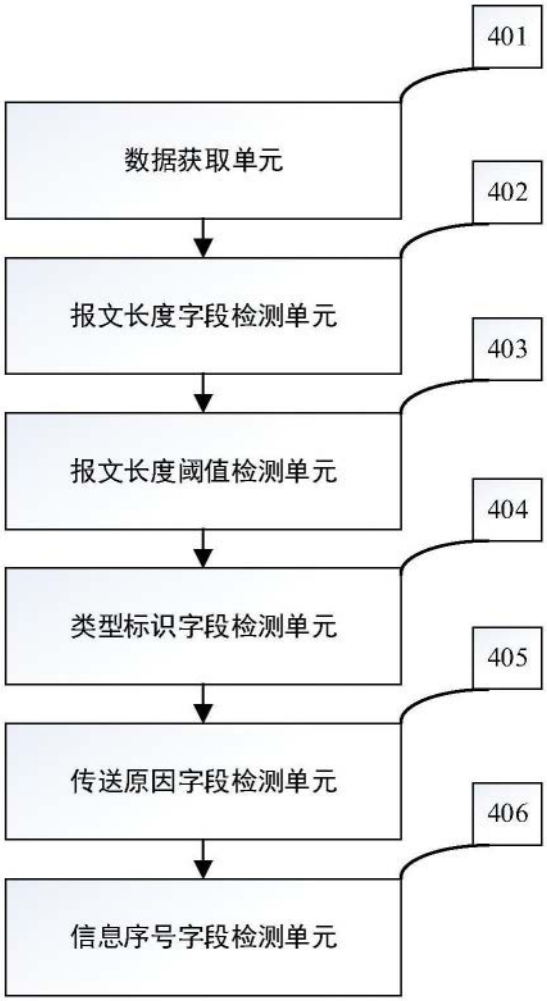

401
数据获取单元
402
报文长度字段检测单元
403
报文长度阈值检测单元
404
类型标识字段检测单元
405
传送原因字段检测单元
406
信息序号字段检测单元

图4

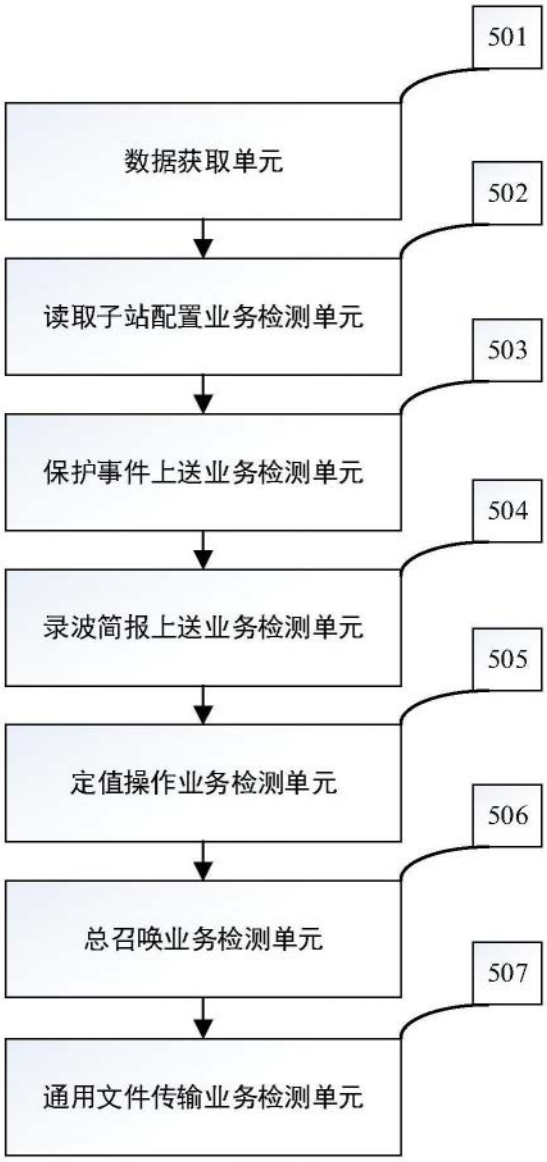

501
数据获取单元
502
读取子站配置业务检测单元
503
保护事件上送业务检测单元
504
录波简报上送业务检测单元
505
定值操作业务检测单元
506
总召唤业务检测单元
507
通用文件传输业务检测单元

图5