(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 111556083 B
(45)授权公告日 2021.01.19

(21)申请号 202010474625.7
(22)申请日 2020.05.29
(65)同一申请的已公布的文献号
申请公布号 CN 111556083 A
(43)申请公布日 2020.08.18
(73)专利权人 武汉大学
地址 430072 湖北省武汉市武昌区八一路299号
(72)发明人 王宇 李俊娥 陈洋荣 梁佳琦
(74)专利代理机构 湖北武汉永嘉专利代理有限公司 42102
代理人 唐万荣
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)

审查员 肖敬伟

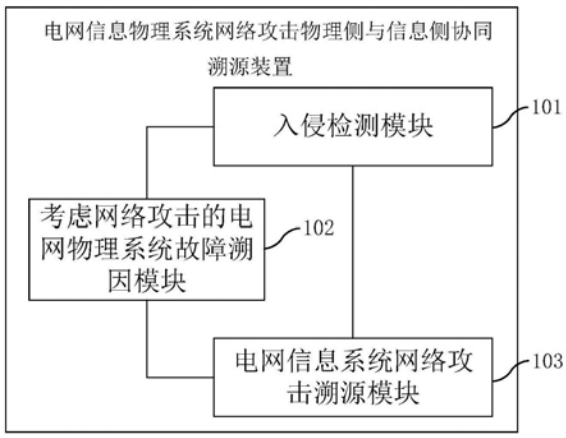
权利要求书2页 说明书7页 附图3页

(54)发明名称

电网信息物理系统网络攻击物理侧与信息侧协同溯源装置

(57)摘要

本发明公开了一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置，包括：入侵检测模块，用于输出各类攻击异常信息、业务威胁度、流量统计数据异常度及终端异常度；考虑网络攻击的电网物理系统故障溯因模块，用于确定故障物理元件及故障类型，并根据所述故障物理元件及所述故障类型，确定误动或拒动的信息系统故障节点和关联节点，并结合信息系统故障节点和关联节点的业务威胁度、流量统计数据异常度和终端异常度，确定故障原因；电网信息系统网络攻击溯源模块，用于若故障原因为网络攻击，则根据所述信息系统故障节点和关联节点的异常信息，确定攻击源与攻击路径。该装置能够准确定位故障原因，有利于进行攻击源和攻击路径的追溯。



CN 111556083 B

1.一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,其特征在于,包括:

入侵检测模块,包括报文攻击检测子模块、泛洪攻击检测子模块和恶意代码攻击检测子模块;

所述报文攻击检测子模块,用于对网络流量数据进行检测,并输出业务威胁度,若检测到报文攻击,输出报文攻击异常信息,所述报文攻击异常信息包括:原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间、受攻击终端的MAC地址;

所述泛洪攻击检测子模块,用于对网络流量统计数据进行检测,并输出流量统计数据异常度,若检测到泛洪攻击时输出泛洪攻击异常信息,所述泛洪攻击异常信息包括:原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间和受攻击终端的MAC地址;

所述恶意代码攻击检测子模块,用于对终端文件进行检测,并输出终端异常度,若检测到存在泛洪攻击,输出恶意代码攻击异常信息,所述恶意代码攻击异常信息包括:恶意代码文件、受攻击终端的MAC地址;

考虑网络攻击的电网物理系统故障溯因模块,用于确定故障物理元件及故障类型,并根据所述故障物理元件及所述故障类型,确定误动或拒动的信息系统故障节点和关联节点,并结合所述信息系统故障节点和关联节点的业务威胁度、流量统计数据异常度和终端异常度,确定故障原因;

电网信息系统网络攻击溯源模块,用于若故障原因为网络攻击,则根据所述信息系统故障节点和关联节点的攻击异常信息,确定攻击源与攻击路径。

2.根据权利要求1所述的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,其特征在于,所述考虑网络攻击的电网物理系统故障溯因模块,包括:

电网物理系统故障感知子模块,用于在物理系统发生故障后,确定故障的发生及故障级别;

电网物理系统故障定位子模块,用于在确定物理系统发生故障后,确定故障物理区段,以及物理元件,并确定元件故障类型;

电网信息系统故障节点及关联节点确定子模块,用于根据故障发生的物理区段与物理元件,确定误动或拒动的信息系统故障节点及关联节点;

信息收集子模块,用于获取故障物理区段、故障物理元件、误动或拒动的信息系统故障节点及关联节点的相关信息;

故障溯因子模块,根据信息收集子模块获取的相关信息,基于预设的故障溯因树,确定故障原因,若故障原因为网络攻击时,确定网络攻击类型,并从入侵检测模块获取攻击异常信息。

3.根据权利要求1所述的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,其特征在于,所述电网信息系统网络攻击溯源模块,包括:

溯源方法调度子模块,用于判断若故障原因为网络攻击,且为恶意代码攻击源时,直接输出攻击源,否则,通过溯源子模块进一步对攻击源进行追溯;

溯源子模块,用于根据信息系统故障节点和关联节点的攻击异常信息,确定攻击源与攻击路径。

4.根据权利要求1所述的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,其特征在于,所述故障原因包括:系统内部原因与网络攻击;

其中，所述系统内部原因包括，物理线路损坏、通信链路故障和软件错误；所述网络攻击包括，恶意代码攻击、泛洪攻击与报文攻击。

5.根据权利要求2所述的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置，其特征在于，所述相关信息包括：

故障物理区段及故障物理元件的状态信息；

信息系统故障节点及关联节点的告警信息、业务威胁度、流量统计数据异常度和设备异常度；所述告警信息包括设备自检告警信息、通信链路状态告警信息和采样值异常告警信息。

电网信息物理系统网络攻击物理侧与信息侧协同溯源装置

技术领域

[0001] 本发明属于智能电网安全技术领域,具体涉及一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置。

背景技术

[0002] 网络攻击溯源可以帮助电网信息物理系统(Grid Cyber-Physical Systems,GCPS)采取合适的防御策略,从源头处阻断攻击,最大程度上使电网信息物理系统摆脱攻击的威胁。目前,缺乏针对电网信息物理系统的网络攻击溯源模型的相关研究。由于传统的网络攻击溯源模型都是以入侵检测系统发现攻击为触发条件,利用已知的攻击相关信息定位攻击源所在位置,无法对电网物理系统发生故障的原因进行追溯,也无法对一些入侵检测系统未发现但已造成电网物理系统发生故障的攻击进行追溯。

发明内容

[0003] 本发明的目的在于提供一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,可以发现一部分已造成物理系统故障但未被入侵检测系统检测出的网络攻击,实现电网物理系统故障溯因与电网信息系统网络攻击溯源。

[0004] 本发明解决其技术问题所采用的技术方案是:

[0005] 一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,包括:

[0006] 入侵检测模块,包括报文攻击检测子模块、泛洪攻击检测子模块和恶意代码攻击检测子模块;

[0007] 所述报文攻击检测子模块,用于对网络流量数据进行检测,并输出业务威胁度,若检测到报文攻击时输出报文攻击异常信息,所述报文攻击异常信息包括:原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间、受攻击终端的MAC地址;

[0008] 所述泛洪攻击检测子模块,用于对网络流量统计数据进行检测,并输出流量统计数据异常度,若检测到泛洪攻击时输出泛洪攻击异常信息,所述泛洪攻击异常信息包括:原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间和受攻击终端的MAC地址;

[0009] 所述恶意代码攻击检测子模块,用于对终端文件进行检测,并输出终端异常度,若检测到存在泛洪攻击时,输出恶意代码攻击异常信息,所述恶意代码攻击异常信息包括:恶意代码文件、受攻击终端的MAC地址;

[0010] 考虑网络攻击的电网物理系统故障溯因模块,用于确定故障物理元件及故障类型,并根据所述故障物理元件及所述故障类型,确定误动或拒动的信息系统故障节点和关联节点,并结合所述信息系统故障节点和关联节点的业务威胁度、流量统计数据异常度和终端异常度,确定故障原因;

[0011] 电网信息系统网络攻击溯源模块,用于若故障原因为网络攻击,则根据所述信息系统故障节点和关联节点的攻击异常信息,确定攻击源与攻击路径。

[0012] 进一步地，所述考虑网络攻击的电网物理系统故障溯因模块，包括：

[0013] 电网物理系统故障感知子模块，用于在物理系统发生故障后，确定故障的发生及故障级别；

[0014] 电网物理系统故障定位子模块，用于在确定物理系统发生故障后，确定故障物理区段，以及物理元件，并确定元件故障类型；

[0015] 电网信息系统故障节点及关联节点确定子模块，用于根据故障发生的物理区段与物理元件，确定误动或拒动的信息系统故障节点及关联节点；

[0016] 信息收集子模块，用于获取故障物理区段、故障物理元件、误动或拒动的信息系统故障节点及关联节点的相关信息；

[0017] 故障溯因子模块，根据信息收集子模块获取的相关信息，基于预设的故障溯因树，确定故障原因，若故障原因为网络攻击时，确定网络攻击类型，并从入侵检测模块获取攻击异常信息。

[0018] 进一步地，所述电网信息系统网络攻击溯源模块，包括：

[0019] 溯源方法调度子模块，用于判断若故障原因为网络攻击，且为恶意代码攻击源时，直接输出攻击源，否则，通过溯源子模块进一步对攻击源进行追溯；

[0020] 溯源子模块，用于根据信息系统故障节点和关联节点的攻击异常信息，确定攻击源与攻击路径。

[0021] 进一步地，所述故障原因包括：系统内部原因与网络攻击；其中，所述系统内部原因包括，物理线路损坏、通信链路故障和软件错误；所述网络攻击包括，恶意代码攻击、泛洪攻击与报文攻击。

[0022] 进一步地，所述相关信息包括：故障物理区段及故障物理元件的状态信息；信息系统故障节点及关联节点的告警信息、业务威胁度、流量统计数据异常度和设备异常度；所述告警信息包括设备自检告警信息、通信链路状态告警信息和采样值异常告警信息。

[0023] 本发明的有益效果是：

[0024] 通过入侵检测模块获取各业务威胁度、流量统计数据异常度和终端异常度，实现了网络攻击的全面检测。通过考虑网络攻击的电网物理系统故障溯因模块，确定电网信息系统故障节点，再结合物理故障元件和各类攻击异常信息，能够准确定位故障原因是系统的物理故障还是网络攻击导致的故障，以及确定网络攻击的类型，有利于进行攻击源和攻击路径的追溯。可以帮助电网信息物理系统采取合适的防御策略，从源头处阻断攻击，最大程度上使电网信息物理系统摆脱攻击的威胁。

附图说明

[0025] 下面将结合附图及实施方式对本发明作进一步说明，附图中：

[0026] 图1为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置结构示意图；

[0027] 图2为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置应用场景图；

[0028] 图3为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置应用流程图。

具体实施方式

[0029] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例。应若理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0030] 图1为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置结构示意图，如图1所示，本发明实施例提供一种电网信息物理系统网络攻击物理侧与信息侧协同溯源装置，包括：

[0031] 入侵检测模块101，包括报文攻击检测子模块、泛洪攻击检测子模块和恶意代码攻击检测子模块。

[0032] 所述报文攻击检测子模块，用于对网络流量数据进行检测，并输出业务威胁度，若检测到报文攻击时输出报文攻击异常信息，所述报文攻击异常信息包括：原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间、受攻击终端的MAC地址。

[0033] 可设置多个阈值来对业务威胁度分级，检测到攻击时，业务威胁度高于最大阈值，确定为攻击。业务威胁度(以及流量统计数据异常度和终端异常度)可由入侵检测系统(intrusion detection system，简称IDS)对网络流量的报文进行评估计算得到。

[0034] 所述泛洪攻击检测子模块，用于对网络流量统计数据进行检测，并输出流量统计数据异常度，若检测到泛洪攻击时输出泛洪攻击异常信息，所述泛洪攻击异常信息包括：原始攻击报文、攻击报文的捕获点位置的MAC地址、攻击报文的捕获时间和受攻击终端的MAC地址。流量统计数据异常度为流量统计数据(每秒包的数量等)与制定的阈值的比值。

[0035] 所述恶意代码攻击检测子模块，用于对终端文件进行检测，并输出终端异常度，若检测到存在泛洪攻击时输出恶意代码攻击异常信息，所述恶意代码攻击异常信息包括：恶意代码文件、受攻击终端的MAC地址。计算设备的终端异常度，为计算设备的关键文件是恶意代码文件的概率，由现有的恶意代码检测方法给出，若某计算设备中存在多个关键文件时，计算设备异常度取所有概率中的最大值。

[0036] 进一步的，业务威胁度、流量统计数据异常度和终端异常度的转化方法包括：分别为

[0037] 将业务威胁度定义为R，若$X_{threat3}>R\geq 0$时，此时为事件1：业务无风险；若$X_{threat2}>R\geq X_{threat3}$时，此时为事件2：业务中风险；若$1>R\geq X_{threat2}$时，此时为事件3：业务高风险。$X_{threat3}$、$X_{threat2}$为业务威胁度告警阈值。

[0038] 将流量统计数据异常度定义为S，若$X_{flow2}>S\geq 0$时，此时为事件4：流量无风险；若$X_{flow1}>S\geq X_{flow2}$时，此时为事件5：流量中风险；若$S\geq X_{flow1}$时，此时为事件6：流量高风险。$X_{flow1}$、$X_{flow2}$为流量统计数据异常度告警阈值。

[0039] 将终端异常度定义为T，若$X_{equip3}>T\geq 0$时，此时为事件7：终端无风险；若$X_{equip2}>T\geq X_{equip3}$时，此时为事件8：终端中风险；若$1>T\geq X_{equip2}$时，此时为事件9：终端高风险。$X_{equip3}$、$X_{equip2}$为终端异常度告警阈值。

[0040] 考虑网络攻击的电网物理系统故障溯因模块102，用于确定故障物理元件及故障类型，并根据所述故障物理元件及所述故障类型，确定误动或拒动的信息系统故障节点和

关联节点;以及结合信息系统故障节点和关联节点的业务威胁度、流量统计数据异常度和终端异常度,确定故障原因。

[0041] 在确定了故障的信息系统故障节点后(误动或拒动的节点以及其关联节点),可以基于目前的故障溯因树来实现故障原因的分析。例如,根据不同故障节点和关联节点的业务威胁度、流量统计数据异常度及终端异常度,或者转换为相应的事件类型,如上述业务威胁度、流量统计数据异常度和终端异常度的转化方法,并结合各种告警日志,从预设的故障溯因树进行查找,确定故障原因,若故障原因为网络攻击时,确定网络攻击类型,包括恶意代码攻击、泛洪攻击与报文攻击。若不是网络攻击,则为系统内部原因导致,确定系统内部的具体故障原因。。其中,所述各种告警日志包括:线路巡检系统获取告警日志,监控系统或调度中心获取的信息系统故障节点及关联节点的告警日志。告警日志中的信息包括:终端自检告警、通信链路状态告警和采样值异常告警。

[0042] 作为可选实施例,故障原因包括,系统内部原因与网络攻击;其中,系统内部原因包括,物理线路损坏、通信链路故障和软件错误;网络攻击包括,恶意代码攻击、泛洪攻击与报文攻击。电网信息系统故障节点指直接控制物理故障元件的信息系统终端,由于故障节点为与物理设备直接关联的终端,按照控制业务流向划分,应为最下游节点;关联节点指与故障节点存在业务关联的终端,为故障节点的上游节点。

[0043] 电网信息系统网络攻击溯源模块103,用于若故障原因为网络攻击,则根据所述信息系统故障节点和关联节点的攻击异常信息,确定攻击源与攻击路径。在确定了关键的信息系统节点后,结合攻击异常信息,便可实现攻击的溯源,采用目前的适用于电网信息系统的网络攻击溯源方法便可实现。例如,包标记的溯源方法,包标记与包日志结合的混合溯源方法等。

[0044] 本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置,通过入侵检测模块获取各业务威胁度、流量统计数据异常度和终端异常度,实现了网络攻击的全面检测。通过考虑网络攻击的电网物理系统故障溯因模块,确定电网信息系统故障节点,再结合物理故障元件和各类攻击异常信息,能够准确定位故障原因是系统的物理故障还是网络攻击导致的故障,以及确定网络攻击的类型,有利于进行攻击源和攻击路径的追溯。可以帮助电网信息物理系统采取合适的防御策略,从源头处阻断攻击,而如果仅从被攻击对象处隔离攻击,攻击源可以转而攻击其它设备,攻击依旧会威胁GCPS,从而该方法能够最大程度上使电网信息物理系统摆脱攻击的威胁。

[0045] 基于上述实施例的内容,作为一种可选实施例,所述考虑网络攻击的电网物理系统故障溯因模块102,包括:

[0046] 电网物理系统故障感知子模块,用于在物理系统发生故障后,确定故障的发生及故障级别。在物理系统发生故障后,基于数据采集与监控系统SCADA或能量管理系统EMS提供的故障告警信息迅速感知到故障的发生及故障级别。

[0047] 电网物理系统故障定位子模块,用于在确定物理系统发生故障后,确定故障物理区段,以及物理元件,并确定元件故障类型。在感知到物理系统发生故障后,采用故障区段定位法、故障测距法等故障定位法,确定故障发生区段,给出相关物理元件,并根据调度中心的诊断方法确定元件故障类型。

[0048] 电网信息系统故障节点及关联节点确定子模块,用于根据故障发生的物理区段与

物理元件，确定误动或拒动的信息系统故障节点及关联节点。在确定故障发生的物理区段与物理元件后，通过业务拓扑进一步确定信息系统故障节点及关联节点，并根据调度中心的诊断方法确定是否存在某个节点发生误动或拒动。其中，电网信息系统故障节点指直接控制该故障节点的信息系统终端，由于故障节点为与物理设备直接关联的终端，按照控制业务流向划分，应为最下游节点；关联节点指与故障节点存在业务关联的终端，为故障节点的上游节点。

[0049] 信息收集子模块，用于获取故障物理区段、故障物理元件、误动或拒动的信息系统故障节点及关联节点的相关信息。例如，从线路巡检系统获取告警日志；从监控系统或调度中心获取信息系统故障节点及关联节点的相关告警日志，包括终端自检告警、通信链路状态告警和采样值异常告警等。

[0050] 故障溯因子模块，根据信息收集子模块获取的相关信息，基于预设的故障溯因树，确定故障原因，若故障原因为网络攻击时，确定网络攻击类型，并从入侵检测模块获取攻击异常信息，用于提供给防御系统使用，或者后期分析使用，属于溯源结果。例如，基于目前的溯因树实现，如考虑网络攻击的故障溯因树。根据不同故障节点和关联节点的业务威胁度、流量统计数据异常度及终端异常度，并结合各种告警日志，确定网络攻击的类型，若不是网络攻击，则为系统内部原因，确定系统内部的具体故障原因。其中，所述各种告警日志包括：线路巡检系统获取告警日志，监控系统或调度中心获取的信息系统故障节点及关联节点的告警日志。告警日志中的信息包括：终端自检告警、通信链路状态告警和采样值异常告警。

[0051] 基于上述实施例的内容，作为可选实施例，所述电网信息系统网络攻击溯源模块103，包括：溯源方法调度子模块和溯源子模块。

[0052] 溯源方法调度子模块，用于判断若故障原因为网络攻击，且为恶意代码攻击源时，直接输出攻击源，否则，通过溯源子模块进一步对攻击源进行追溯；

[0053] 溯源子模块，用于根据信息系统故障节点和关联节点的攻击异常信息，确定攻击源与攻击路径。在确定了关键的异常信息系统节点后，结合攻击异常信息，便可实现攻击的溯源，采用目前的适用于电网信息系统的网络攻击溯源方法便可实现。

[0054] 基于上述实施例的内容，作为一种可选实施例，上述相关信息包括：故障物理区段及故障物理元件的状态信息；信息系统故障节点及关联节点的告警信息、业务威胁度、流量统计数据异常度和设备异常度；所述告警信息包括设备自检告警信息、通信链路状态告警信息和采样值异常告警信息。

[0055] 从线路巡检系统获取故障物理区段及故障物理元件的状态信息，线路巡检系统会将存在问题的线路或元件记录在告警日志中，因此，仅需要获取线路巡检系统的告警日志即可，如果告警日志中没有故障物理区段及故障物理元件的相关信息，则认为故障物理区段及故障物理元件若前状态正常。从监控系统或调度中心获取信息系统故障节点及关联节点的相关告警日志，包括计算设备自检告警、通信链路状态告警和采样值异常告警等。从入侵检测模块处获取相关信息，包括业务威胁度、流量统计数据异常度和计算设备异常度。

[0056] 图2为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置应用场景图，表示了一种针对电网嵌入式终端可能遭受的网络攻击场景。如图2所示，“断路器1”、“断路器2”、“断路器3”和“断路器4”的初始状态都为闭合状态，设攻击者已经利用社会工程学方法将恶意代码植入运维人员设备上；之后，若运维人员使用该设备对“测控

终端6”进行运维时，该设备向其植入恶意代码；最后，攻击者将自己装有攻击程序的设备接入“主站交换机1”未使用的3号端口上，并将该设备的IP地址伪造成“站控主机1”的IP地址，以每秒钟1000个报文的速度向“测控终端1”发送ICMP泛洪报文，造成该终端拒绝服务，无法响应“站控主机2”下发的正常控制指令，使“站控主机2”失去对“断路器1”、“断路器2”和“断路器3”的控制能力，同时，该攻击设备通知“测控装置6”上植入的恶意代码开始工作，该恶意代码先发送伪造的恶意GOOSE报文PG_2控制“智能终端1”对“断路器2”执行开操作，再发送伪造的恶意GOOSE报文PG_3控制“智能终端1”对“断路器3”执行开操作，致使物理系统发生停电事故。图3为本发明实施例提供的电网信息物理系统网络攻击物理侧与信息侧协同溯源装置应用流程图。

[0057] 在电网信息物理系统遭受网络攻击时，具体实施方式如下：

[0058] 1)部署在子站站控层网络中的入侵检测模块中泛洪攻击检测模块会利用“子站交换机2”处获取的流量统计信息，发现流向“测控终端1”的ICMP报文超过合法阈值，判定“测控终端1”遭受ICMP Flood攻击；

[0059] 2)电网信息系统网络攻击溯源模块中溯源方法调度子模块根据入侵检测模块提供的攻击相关信息，判断需要进一步进行攻击源追溯；溯源子模块利用攻击相关信息，采用适用于电网信息系统的网络攻击溯源方法对攻击源进行追溯，输出ICMP Flood攻击的攻击路径与攻击源相关信息。

[0060] 3)考虑网络攻击的电网物理系统故障溯因模块，在感知到物理系统发生故障后开始工作，具体步骤如下：

[0061] 3.1)电网物理系统故障感知子模块，在物理系统发生故障后，基于数据采集与监控系统SCADA提供的故障告警信息迅速感知到故障的发生，并根据故障影响范围判断该故障级别为警戒；

[0062] 3.2)电网物理系统故障定位子模块，在感知到物理系统发生故障后，采用故障定位法，确定故障元件为“断路器2”与“断路器3”，并根据调度中心的诊断方法确定元件故障类型为元件误动；

[0063] 3.3)电网信息系统故障节点及关联节点确定，在确定故障发生的物理元件后，根据SCD文件，进一步确定信息系统故障节点及关联节点为“站控主机2”、“测控终端1”与“智能终端1”，并根据调度中心的诊断方法确定“测控终端1”发生拒动，“智能终端1”发生误动；

[0064] 3.4)信息收集子模块，获取“断路器2”、“断路器3”、“测控终端1”与“智能终端1”相关信息；

[0065] 3.5)故障溯因子模块，根据收集的相关信息及电网物理系统元件误动故障溯因树，判断“断路器2”与“断路器3”发生误动的原因都为“智能终端1”发生误动；然后，将“智能终端1”与“测控终端1”的业务威胁度、流量统计数据异常度和终端异常度信息转换为确定性的事件，作为电网信息系统终端误动溯因树的输入，此时，“智能终端1”的业务威胁度转换为事件3，“智能终端1”的流量统计数据异常度转换为事件4，“智能终端1”的终端异常度转换为事件7，“测控终端1”的业务威胁度转换为事件1，“测控终端1”的流量统计数据异常度转换为事件6，“测控终端1”的终端异常度转换为事件7；根据电网信息系统终端误动故障溯因树，判断“智能终端1”误动的产生原因为由若前终端控制业务发生事件3，即“智能终端1”接收了攻击者发送的恶意控制命令报文，致使其错误执行控制动作。

[0066] 4)电网信息系统网络攻击溯源模块中溯源方法调度子模块根据考虑网络攻击的电网物理系统故障溯因模块提供的攻击相关信息,判断需要进一步进行攻击源追溯;溯源子模块利用攻击相关信息,采用适用于电网信息系统的网络攻击溯源方法对攻击源进行追溯,输出恶意GOOSE报文攻击的攻击路径与攻击源相关信息。

[0067] 已经通过参考少量实施方式描述了本发明。然而,本领域技术人员所公知的,正如附带的专利权利要求所限定的,除了本发明以上公开的其他的实施例等同地落在本发明的范围内。

[0068] 通常地,在权利要求中使用的所有术语都根据他们在技术领域的通常含义被解释,除非在其中被另外明确地定义。所有的参考“一个/所述/该[装置、组件等]”都被开放地解释为所述装置、组件等中的至少一个实例,除非另外明确地说明。这里公开的任何方法的步骤都没必要以公开的准确的顺序运行,除非明确地说明。

[0069] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0070] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0071] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0072] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0073] 最后应若说明的是:以上实施例仅用以说明本发明的技术方案而非对其限制,尽管参照上述实施例对本发明进行了详细的说明,所属领域的普通技术人员应若理解:依然可以对本发明的具体实施方式进行修改或者等同替换,而未脱离本发明精神和范围的任何修改或者等同替换,其均应涵盖在本发明的权利要求保护范围之内。

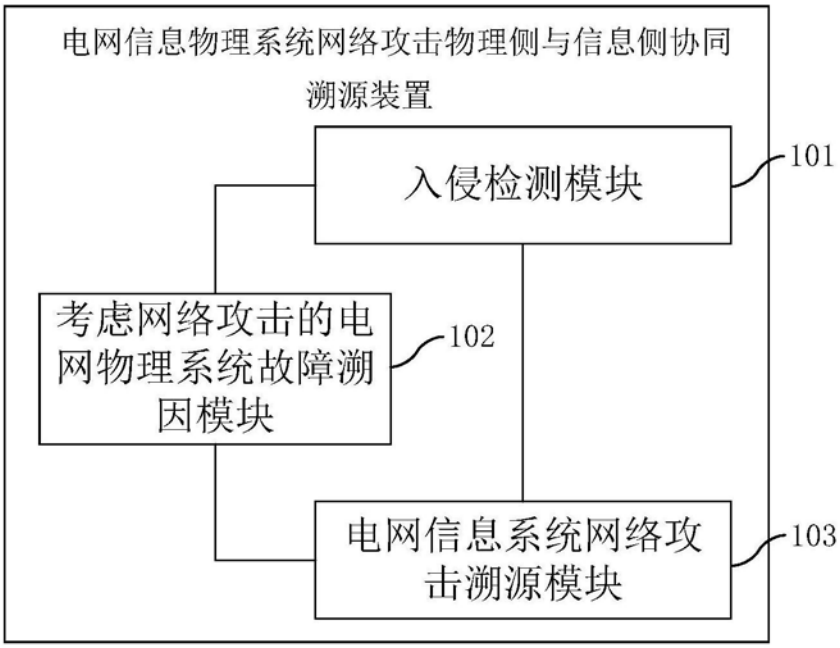

电网信息物理系统网络攻击物理侧与信息侧协同溯源装置
入侵检测模块
101
考虑网络攻击的电网物理系统故障溯因模块
102
电网信息系统网络攻击溯源模块
103

图1

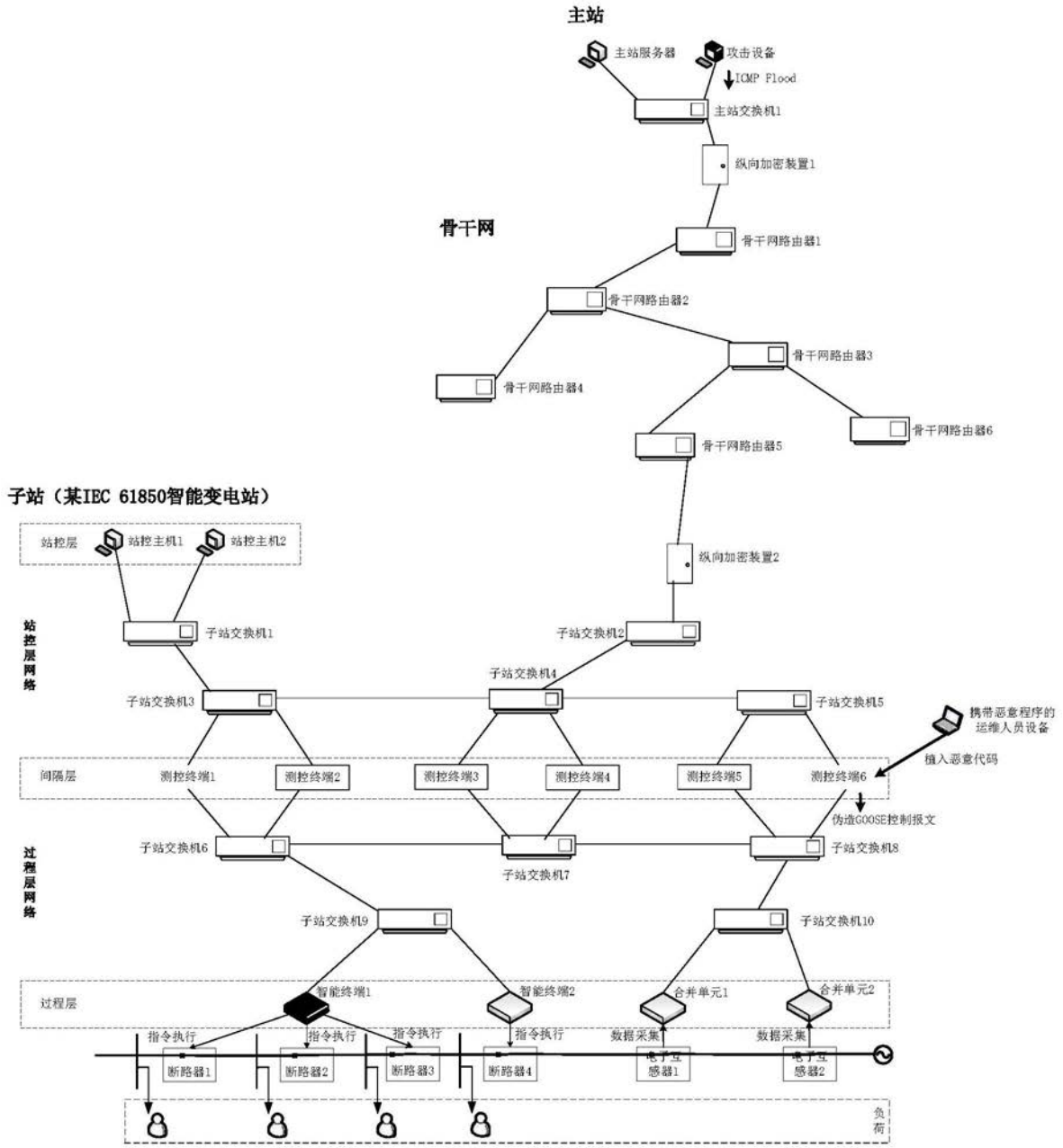

主站
主站服务器
攻击设备
ICMP Flood
主站交换机1
纵向加密装置1
骨干网
骨干网路由器1
骨干网路由器2
骨干网路由器3
骨干网路由器4
骨干网路由器5
骨干网路由器6
子站（某IEC 61850智能变电站）
站控层
站控主机1
站控主机2
纵向加密装置2
站控层网络
子站交换机1
子站交换机2
子站交换机3
子站交换机4
子站交换机5
携带恶意程序的运维人员设备
植入恶意代码
间隔层
测控终端1
测控终端2
测控终端3
测控终端4
测控终端5
测控终端6
伪造GOOSE控制报文
过程层网络
子站交换机6
子站交换机7
子站交换机8
子站交换机9
子站交换机10
过程层
智能终端1
智能终端2
合并单元1
合并单元2
指令执行
指令执行
指令执行
指令执行
数据采集
数据采集
断路器1
断路器2
断路器3
断路器4
电子互感器1
电子互感器2
负荷

图2

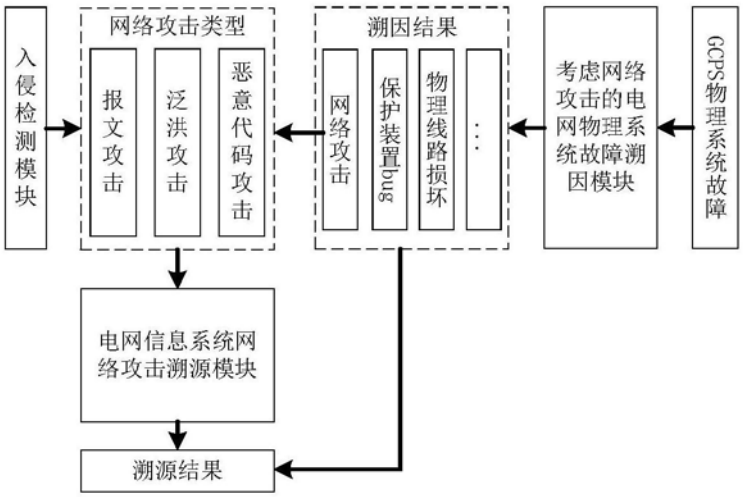

入侵检测模块
网络攻击类型
报文攻击
泛洪攻击
恶意代码攻击
溯因结果
网络攻击
保护装置bug
物理线路损坏
：
考虑网络攻击的电网物理系统故障溯因模块
GCPS物理系统故障
电网信息系统网络攻击溯源模块
溯源结果

图3