(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108055228 A
(43)申请公布日 2018.05.18

(21)申请号 201710929390.4

(22)申请日 2017.10.09

(71)申请人 全球能源互联网研究院有限公司
地址 102209 北京市昌平区未来科技城滨河大道18号
申请人 国家电网公司

(72)发明人 张涛 费稼轩 周诚 马媛媛 邵志鹏 石聪聪 范杰 黄秀丽 汪晨 陈牧 陈璐 戴造建 李尼格

(74)专利代理机构 北京三聚阳光知识产权代理有限公司 11250
代理人 李博洋

(51)Int.Cl.
H04L 29/06(2006.01)
G06K 9/62(2006.01)
G06N 3/04(2006.01)

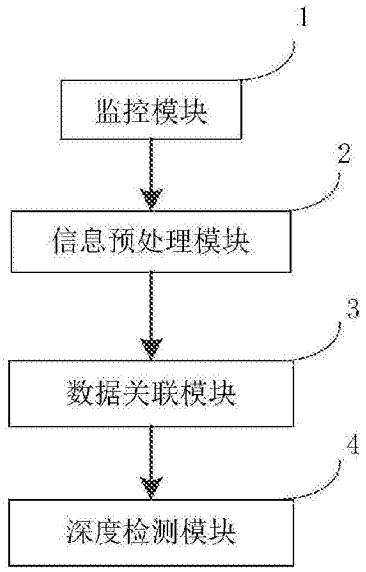
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种智能电网入侵检测系统及方法

(57)摘要

本发明公开了一种智能电网入侵检测系统及方法，其中系统包括：监控模块，用于获取智能电网中电力设备的数据；信息预处理模块，用于对电力设备中的数据进行预处理生成电网信息数据；数据关联模块，用于将电网信息数据进行集中和融合形成融合数据；深度检测模块，用于分析智能电网的融合数据识别入侵攻击的类型。本发明提供的智能电网入侵检测系统及方法可以全面地获取信息系统中的运行数据，从而有效识别恶意攻击行为，在提高了智能电网的入侵检测精度的同时增强了入侵检测的可扩展性，降低智能电网的入侵攻击误报率和漏报率。



CN 108055228 A

1.一种智能电网入侵检测系统，其特征在于，包括：

监控模块，用于获取所述智能电网中电力设备的数据；

信息预处理模块，用于对所述电力设备中的数据进行预处理生成电网信息数据；

数据关联模块，用于将所述电网信息数据进行集中和融合，形成融合数据；

深度检测模块，用于分析所述智能电网的融合数据，识别入侵攻击的类型。

2.根据权利要求1所述的智能电网入侵检测系统，其特征在于，

所述电力设备的数据包括：所述电力设备的报文及一次线路中电力设备的量测量；

所述监控模块，包括：网络单元及智能设备，其中：

所述网络单元收集所述电力设备的报文；

所述智能设备采集所述一次线路中电力设备的量测量。

3.根据权利要求2所述的智能电网入侵检测系统，其特征在于，所述信息预处理模块包括：报文特征提取单元、量测量检测单元以及设备状态估计单元，其中：

所述报文特征提取单元分析所述报文，获取所述报文的基本信息及特征信息；

所述设备状态估计单元获取所述量测量，通过最小二乘法计算出设备状态估计向量；

所述量测量检测单元根据所述量测量及所述设备状态估计向量计算生成量测量异常度向量。

4.根据权利要求3所述的智能电网入侵检测系统，其特征在于，所述数据关联模块具体用于：

根据预设的映射关系表将时间信息、所述报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。

5.根据权利要求4所述的智能电网入侵检测系统，其特征在于，所述深度检测模块包括：快速建模单元，所述快速建模单元通过聚类算法，根据所述融合数据识别入侵攻击的类型。

6.根据权利要求5所述的智能电网入侵检测系统，其特征在于，所述深度检测模块还包括：扩展单元，所述扩展单元通过增量式GHSOM算法分析所述快速建模单元无法识别的入侵攻击，输出分析结果。

7.一种智能电网入侵检测方法，其特征在于，包括如下步骤：

获取智能电网中电力设备的数据；

对所述电力设备的数据进行预处理生成电网信息数据；

将所述电网信息数据进行集中和融合，形成融合数据；

分析所述智能电网的融合数据，识别入侵攻击的类型。

8.根据权利要求7所述的智能电网入侵检测方法，其特征在于，所述电力设备的数据包括：所述电力设备的报文及一次线路中电力设备的量测量。

9.根据权利要求8所述的智能电网入侵检测方法，其特征在于，所述对所述电力设备的数据进行预处理生成电网信息数据，包括：

分析所述报文，获取所述报文的基本信息及特征信息；

获取所述量测量，利用最小二乘法计算得出设备状态估计向量；

根据所述量测量及所述设备状态估计向量计算生成量测量异常度向量。

10.根据权利要求9所述的智能电网入侵检测方法，其特征在于，所述将所述电网信息

数据进行集中和融合，形成融合数据，包括：

根据预设的映射关系表将时间信息、所述报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。

11.根据权利要求10所述的智能电网入侵检测方法，其特征在于，所述分析所述智能电网的融合数据，识别入侵攻击的类型，包括：

通过聚类算法，根据所述融合数据识别入侵攻击的类型；

通过增量式GHSOM算法分析聚类算法无法识别的入侵攻击，输出分析结果。

12.一种智能电网入侵检测设备，其特征在于，包括：至少一个处理器；以及与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器执行权利要求7-11中任一项所述的方法的步骤。

13.一种非暂态计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现权利要求7-11中任一项所述的方法的步骤。

一种智能电网入侵检测系统及方法

技术领域

[0001] 本发明涉及信息技术安全领域，具体涉及一种智能电网入侵检测系统及方法。

背景技术

[0002] 随着智能电网的兴起，智能电网中不良数据注入、篡改设备状态等攻击方式，针对智能电网中由信息技术引入地安全威胁，许多研究者提出利用信息网络中的入侵检测方法来保护智能电网。入侵检测是通过计算机系统或网络中的若干关键点收集和分析审计记录、安全日志、用户行为以及网络数据包等信息，检查网络或系统中当前是否存在违反安全策略的入侵行为和被攻击的迹象。然而当前大部分入侵检测系统的构建都是基于某种规则的设计，不仅存在误报率较高的问题，而且难以察觉其他未知攻击。

[0003] 针对智能电网当中可能存在的各种攻击手段，当前大多数检测系统的检测精度普遍不理想，大量误报和漏报现象使得检测系统的可用性遭到了质疑，其原因在于不能充分发掘智能电网海量数据的潜在信息。除此之外，检测规则一旦确定便无法修改。这将导致系统无法准确识别未知攻击，严重制约系统的可扩展性。然而随着传输边界的不断扩张，智能电网面对的攻击手段变得纷繁复杂，因此如何及时有效地检测攻击，提高检测的可用性和可扩展性，是保障智能电网安全亟待解决的问题。

发明内容

[0004] 因此，本发明为了克服现有技术中智能电网入侵检测不能有效检测攻击可扩展性差的原因，从而提供一种智能电网入侵检测系统及方法，降低智能电网的入侵攻击误报率和漏报率，提高入侵检测的精度，增强了攻击检测的可扩展性，强化了智能电网的主动防御能力。

[0005] 本发明提供的一种智能电网入侵检测系统，包括：监控模块，用于获取所述智能电网中电力设备的数据；信息预处理模块，用于对所述电力设备中的数据进行预处理生成电网信息数据；数据关联模块，用于将所述电网信息数据进行集中和融合，形成融合数据；深度检测模块，用于分析所述智能电网的融合数据，识别入侵攻击的类型。

[0006] 优选地，所述电力设备的数据包括：所述电力设备的报文及一次线路中电力设备的量测量；所述监控模块，包括：网络单元及智能设备，其中：所述网络单元收集所述电力设备的报文；所述智能设备采集所述一次线路中电力设备的量测量。

[0007] 优选地，所述信息预处理模块包括：报文特征提取单元、量测量检测单元以及设备状态估计单元，其中：所述报文特征提取单元分析所述报文，获取所述报文的基本信息及特征信息；所述设备状态估计单元获取所述量测量，通过最小二乘法计算出设备状态估计向量；所述量测量检测单元根据所述量测量及所述设备状态估计向量计算生成量测量异常度向量。

[0008] 优选地，所述数据关联模块具体用于：根据预设的映射关系表将时间信息、所述报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。

[0009] 优选地，所述深度检测模块包括：快速建模单元，所述快速建模单元通过聚类算法，根据所述融合数据识别入侵攻击的类型。

[0010] 优选地，所述深度检测模块还包括：扩展单元，所述扩展单元通过增量式GHSOM算法分析所述快速建模单元无法识别的入侵攻击，输出分析结果。

[0011] 本发明提供的一种智能电网入侵检测方法，包括如下步骤：获取智能电网中电力设备的数据；对所述电力设备的数据进行预处理生成电网信息数据；将所述电网信息数据进行集中和融合，形成融合数据；分析所述智能电网的融合数据，识别入侵攻击的类型。

[0012] 优选地，所述电力设备的数据包括：所述电力设备的报文及一次线路中电力设备的量测量。

[0013] 优选地，所述对所述电力设备的数据进行预处理生成电网信息数据，包括：分析所述报文，获取所述报文的基本信息及特征信息；获取所述量测量，利用最小二乘法计算得出设备状态估计向量；根据所述量测量及所述设备状态估计向量计算生成量测量异常度向量。

[0014] 优选地，所述将所述电网信息数据进行集中和融合，形成融合数据，包括：根据预设的映射关系表将时间信息、所述报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。

[0015] 优选地，所述分析所述智能电网的融合数据，识别入侵攻击的类型，包括：通过聚类算法，根据所述融合数据识别入侵攻击的类型；通过增量式GHSOM算法分析聚类算法无法识别的入侵攻击，输出分析结果。

[0016] 本发明提供的一种智能电网入侵检测设备，包括：至少一个处理器；以及与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器执行上述方法的步骤。

[0017] 本发明提供的一种非暂态计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现上述方法的步骤。

[0018] 本发明技术方案，具有如下优点：

[0019] 1.本发明提供的智能电网入侵检测系统，用于检测智能电网当中潜在的入侵攻击行为，可以全面地获取信息系统中上下行报文特征、物理系统中设备量测信息和运行状态，从而有效识别、定位、评估各类恶意攻击行为并及时做出调整，提高了智能电网的入侵检测精度，同时增强了入侵检测的可扩展性。

[0020] 2.本发明提供的智能电网入侵检测方法，可以降低智能电网的入侵攻击误报率和漏报率，提高入侵检测的精度，增强了攻击检测的可扩展性，强化了智能电网的主动防御能力。

附图说明

[0021] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0022] 图1为本发明实施例1中一种智能电网入侵检测系统的一个具体示例的原理框图；

[0023] 图2为本发明实施例1中一种智能电网入侵检测系统的另一个具体示例的原理框图；

[0024] 图3为本发明实施例2中一种智能电网入侵检测方法的一个具体示例的流程图；

[0025] 图4为本发明实施例3中一种智能电网入侵检测设备的一个具体示例的原理框图。

具体实施方式

[0026] 下面将结合附图对本发明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一部分实施例，而不是全部的实施例。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。

[0027] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，还可以是两个元件内部的连通，可以是无线连接，也可以是有线连接。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

[0028] 此外，下面所描述的本发明不同实施方式中所涉及的技术特征只要彼此之间未构成冲突就可以相互结合。

[0029] 实施例1

[0030] 本发明实施例提供一种智能电网入侵检测系统，如图1所示，包括：监控模块1、信息预处理模块2、数据关联模块3、深度检测模块4，其中：

[0031] 如图2所示，监控模块1，用于获取智能电网中电力设备的数据，在一实施例中，该电力设备的数据主要包括：电力设备的报文及一次线路中电力设备的量测量。具体地，该监控模块1包括网络单元11和智能设备12，其中：网络单元11收集电力设备的报文；智能设备12采集一次线路中电力设备的量测量。

[0032] 本发明实施例将监控模块1分布式地部署在智能电网当中同时收集信息系统和电力系统中的有用信息，每一个监控模块1包含网络单元11与智能设备12两块核心部件。网络单元11负责将监控模块1连接在统一的信息系统当中，每一块网络单元11拥有唯一的电网内IP地址，各监控模块1通过网络单元11进行互相间的通信与协作控制。智能设备12负责将监控模块1部署在物理系统当中，每一块智能设备12在逻辑上连接了一次线路当中的若干电力设备，负责这些设备的配置、检测以及控制工作。

[0033] 在一实施例中，设在智能设备12二次线路中总共部署了n个监控模块1($M_1,M_2,\cdots,M_n$)，这n个监控模块1包含了n个智能设备12($T_1,T_2,\cdots,T_n$)以及n个网络单元11($W_1,W_2,\cdots,W_n$)。管理员在启动监控模块1后，首先为各网络单元11分配IP地址($IP_1,IP_2,\cdots,IP_n$)并完成通信相关的初始化操作，然后为各智能设备12分配目标电力设备群组。假定第i个监控模块1的智能设备12负责配置、检测、控制一次线路中的m个目标电力设备，这些目标电力设备构成一个目标电力设备群组。设获取了目标电力设备群组的1个量测量$P_i=(p_{i,1},p_{i,2},\cdots,p_{i,1})$，则$T_i$将$P_i$发送给信息预处理模块2。同时$M_i$的网络单元11$M_i$将收集的所有上行下行报文镜像给信息预处理模块2。监控模块1不仅为智能电网的入侵检测分析提供全方位的数据支撑，还能够凭借入侵检测的反馈机制以及装置间的配合协作实现电网的自适应调整

[0034] 信息预处理模块2，用于对电力设备中的数据进行预处理生成电网信息数据。具体

地，该信息预处理模块2包括：报文特征提取单元21、量测量检测单元22以及设备状态估计单元23，其中：报文特征提取单元21分析报文，获取报文的基本信息及特征信息；设备状态估计单元22获取量测量，通过最小二乘法计算出设备状态估计向量；量测量检测单元23根据量测量及设备状态估计向量计算生成量测量异常度向量。

[0035] 在本发明实施例中，报文特征提取单元21按照如下表1所示的特征向量解析镜像得到的所有上行或下行报文：

[0036] 表1

[0037]

报文编号	协议类型	源Ip	目的Ip	报文内容	异常类型	报警时间

[0038] 如特征向量所示，该单元会为所有报文给予单独的编号，并将报文与特征库进行匹配最终获取电网协议类型、源IP、目的IP，报文内容即为解析后得到的明文。随后报文特征提取单元21采用一种基于状态转移分析的误用检测方法，通过对报文产生事件序列进行分析并赋予报文相应的异常类型。每个报文的异常类型将用一个有限长度的二进制序列表示，表示形式如下表2所示：

[0039] 表2

[0040]

normal	********000
unknown	********001
flood	********010

[0041]

teardrop	********011
backdoor	********100
smurf	********101
buffoverflow	********110
…	…

[0042] 如表2中所示，被标识为normal的报文为正常报文；被标识为unknown的报文为经过特征提取后无法归类为已知类型的报文；flood、teardrop、backdoor、smurf、buffoverflow等标识均为当前系统已知的各类网络攻击手段。对于异常类型标识为正常(normal)的报文，特征向量中的报警时间则为保留字段。若报文经解析后被标识为其他异常类型，那么报文特征提取单元21将在其特征信息中记录报警时间。

[0043] 当T_i将目标电力设备群组G_i的l个量测量$P_i=(p_{i,1},p_{i,2},\cdots,p_{i,l})$发送给信息预处理模块2，其中的设备状态估计单元23采用最小二乘法计算得出各电力设备的状态估计矩阵$S_i=(s_{i,1},s_{i,2},\cdots,s_{i,m})$。与此同时，量测量检测单元22利用目标函数评价各量测量，给出所有量测量的异常度向量$E_i=(e_{i,1},e_{i,2},\cdots,e_{i,l})$。最终，信息预处理模块2完成了智能电网

的信息系统和电力系统所有有关数据的分析、提取、结构化预处理工作。

[0044] 数据关联模块3，用于将电网信息数据进行集中和融合，形成融合数据，具体地，该数据关联模块3用于根据预设的映射关系表将时间信息、报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。

[0045] 本发明实施例中，可根据一预设的关联规则生成该融合数据，基于该关联规则在系统中设置了数据关联模块3，用以增强局部地区的数据关联性。假设某监控模块$1M_j$的网络单元$11W_j$为其在信息系统中配备了一个IP地址，设该地址为IP_j。同时为该装置的智能设备$12T_j$分配了目标电力设备群组$G_j=(g_{j,1},g_{j,2},\cdots,g_{j,m})$，群组中包含了m台一次线路电力设备，$T_j$获取的l个量测量为$P_j=(p_{j,1},p_{j,2},\cdots,p_{j,l})$。在本发明实施例中采用了一种映射表进行数据的关联操作，该映射表为：

[0046] <时间片段，状态估计，量测量异常度，源地址报文集合，目的报文集合>

[0047] 设数据收集的起止时间为t_0和t_1，时间片段为(t_0,t_1)。以IP_j为源地址的报文集合为$C_j=\{m|from\ IP_j\}$，以IP_j为目的地址的报文集合为$D_j=\{m|to\ IP_j\}$。目标电力设备群组的设备状态估计为$S_j=(s_{j,1},s_{j,2},\cdots,s_{j,m})$，量测量异常度向量为$E_j=(e_{j,1},e_{j,2},\cdots,e_{j,l})$。那么，在该时间片段内关于监控模块$1M_j$的融合数据为$<(t_0,t_1),S_j,E_j,C_j,D_j>$。融合后的数据将交由深度检测模块4执行入侵检测操作。

[0048] 深度检测模块4，用于分析智能电网的融合数据，识别入侵攻击的类型。具体地，该深度检测模块4包括：快速建模单元41，快速建模单元41通过聚类算法，根据融合数据识别入侵攻击的类型；扩展单元42，扩展单元42通过增量式GHSOM算法分析快速建模单元41无法识别的入侵攻击，输出分析结果。攻击检测日志记录下所有分析结果，并将结果反馈给监控装置1用以调整电网系统。

[0049] 本发明实施例的深度检测模块4是基于集成分类器思想，快速建模单元41的核心算法为基于主方向分裂划分层次聚类算法，该算法对于初始值和融合数据的输入顺序不敏感，对于已知入侵攻击，不仅检测率高而且检测速度快，适用于入侵检测的快速建模。但对于未知的变种入侵攻击，其识别效果不甚理想。扩展单元42基于增量式GHSOM算法构建，该算法是一种具备较强适应性的神经网络算法，适用于进一步检测未知的入侵攻击，因此有助于构建对扩展性有一定要求的攻击检测模型。

[0050] 深度检测模块4采用串行条件结构连接快速建模单元41和扩展单元42，快速建模单元41作为基分类器，扩展单元42作为下一分类器，根据基分类器的分类结果确定是否需要继续使用下一分类器。

[0051] 深度检测模4首先将融合数据矩阵输入快速建模单元41进行聚类分析，所有融合数据将被划分为正常、已知入侵攻击以及未知三大类，其中已知入侵攻击被细分为各类入侵攻击。对于被划分为已知入侵攻击的融合数据实例，快速建模单元41会输出详细的评估信息；对于被划分为未知的融合数据，快速建模单元41将启动扩展单元42，并将被划分为未知的融合数据发送给扩展单元42。经过扩展单元42的检测识别，被划分为未知的融合数据又进一步被划分为正常、入侵攻击两大类，其中入侵攻击类型随着检测系统的使用将会不断细分为各类入侵攻击。对于被划分为入侵攻击的融合数据实例，扩展单元42最终将输出详细的相关评估信息。深度检测模4输出的入侵攻击评估信息包含发动时间t，目标设备群组G，设备状态向量S，目标量测量向量P，威胁评估R等关键信息，即输出信息的元组为：<t，

G,S,P,R>。基于串行条件结构，深度检测模4首先把易分类的已知入侵攻击过滤掉，少数难分的实例将保留下来让扩展单元42继续进行分类，调整好快速建模单41的阈值参数，在控制好其错分率的前提下就能提高最终的识别精度。

[0052] 实施例2

[0053] 本发明实施例提供一种智能电网入侵检测方法，如图3所示，包括如下步骤：

[0054] 步骤S1：获取智能电网中电力设备的数据。在一实施例中，该电力设备的数据包括：电力设备的报文及一次线路中电力设备的量测量。

[0055] 在一实施例中，设在智能电网二次线路中总共部署了n个监控模块($M_1,M_2,\cdots,M_n$)，这n个监控模块包含了n个智能设备($T_1,T_2,\cdots,T_n$)以及n个网络单元($W_1,W_2,\cdots,W_n$)。管理员在启动监控模块后，首先为各网络单元分配IP地址($IP_1,IP_2,\cdots,IP_n$)并完成通信相关的初始化操作，然后为各智能设备分配目标电力设备群组。假定第i个监控模块M_i的智能设备T_i负责配置、检测、控制一次线路中的m个目标电力设备，这些目标电力设备构成一个目标电力设备群组G_i。设T_i获取了目标电力设备群组G_i的l个量测量$P_i=(p_{i,1},p_{i,2},\cdots,p_{i,l})$，同时$M_i$的网络单元$W_i$将收集的所有上行下行报文。至此完成了智能电网中电力设备的数据。

[0056] 步骤S2：对电力设备的数据进行预处理生成电网信息数据。预处理生成电网信息数据的步骤，具体包括：分析步骤S1获取的电力设备报文，获取报文的基本信息及特征信息；获取量测量，利用最小二乘法计算得出设备状态估计向量；根据量测量及设备状态估计向量计算生成量测量异常度向量。

[0057] 本发明实施例按照如表1所示的特征向量解析镜像得到的所有上行或下行报文。

[0058] 如特征向量所示，该单元会为所有报文给予单独的编号，并将报文与特征库进行匹配最终获取电网协议类型、源IP、目的IP，报文内容即为解析后得到的明文。随后采用一种基于状态转移分析的误用检测方法，通过对报文产生事件序列进行分析并赋予报文相应的异常类型。每个报文的异常类型将用一个有限长度的二进制序列表示，表示形式如表2所示。

[0059] 如表2中所示，被标识为normal的报文为正常报文；被标识为unknown的报文为经过特征提取后无法归类为已知类型的报文；flood、teardrop、backdoor、smurf、buffoverflow等标识均为当前系统已知的各类网络攻击手段。对于异常类型标识为正常(normal)的报文，特征向量中的报警时间则为保留字段。若报文经解析后被标识为其他异常类型，那么在其特征信息中记录报警时间。当接收到T_i将目标电力设备群组G_i的l个量测量$P_i=(p_{i,1},p_{i,2},\cdots,p_{i,l})$时采用最小二乘法计算得出各电力设备的状态估计矩阵$S_i=(s_{i,1},s_{i,2},\cdots,s_{i,m})$。与此同时利用目标函数评价各量测量，给出所有量测量的异常度向量$E_i=(e_{i,1},e_{i,2},\cdots,e_{i,l})$。最终完成了智能电网的信息系统和物理系统所有有关数据的分析、提取、结构化预处理工作。

[0060] 步骤S3：将电网信息数据进行集中和融合，形成融合数据。具体来说是根据预设的映射关系表将时间信息、报文的基本信息、设备状态估计向量、量测量异常度向量进行关联，生成所述融合数据。本发明实施例中，可根据一预设的关联规则生成该融合数据，基于该关联规则用以增强局部地区的数据关联性。假设某监控模块M_j的网络单元W_j为其在信息系统中配备了一个IP地址，设该地址为IP_j。同时为智能设备T_j分配了目标电力设备群组$G_j=(g_{j,1},g_{j,2},\cdots,g_{j,m})$，群组中包含了m台一次线路电力设备，$T_j$获取的l个量测量为$P_j=$

$(p_{j,1},p_{j,2},\cdots,p_{j,l})$。在本发明中采用了一种映射表进行数据的关联操作，该映射表为：

[0061] <时间片段，状态估计，量测量异常度，源地址报文集合，目的报文集合>

[0062] 设数据收集的起止时间为t_0和t_1，时间片段为(t_0,t_1)。以IP_j为源地址的报文集合为$C_j=\{m|from\ IP_j\}$，以IP_j为目的地址的报文集合为$D_j=\{m|to\ IP_j\}$。目标电力设备群组的设备状态估计为$S_j=(s_{j,1},s_{j,2},\cdots,s_{j,m})$，量测量异常度向量为$E_j=(e_{j,1},e_{j,2},\cdots,e_{j,l})$。那么，在该时间片段内关于监控模块$M_j$的融合数据为$<(t_0,t_1),S_j,E_j,C_j,D_j>$。

[0063] 步骤S4：分析智能电网的融合数据，识别入侵攻击的类型。具体来说是通过聚类算法，根据所述融合数据识别入侵攻击的类型；通过增量式GHSOM算法分析聚类算法无法识别的入侵攻击，输出分析结果。

[0064] 本发明实施例采用串行条件结构连接基分类器和下一分类器，首先将融合数据矩阵输入基分类器进行聚类分析，所有融合数据将被划分为正常、已知入侵攻击以及未知三大类，其中已知入侵攻击被细分为各类入侵攻击。对于被划分为已知入侵攻击的融合数据实例输出详细的评估信息；对于被划分为未知的融合数据又进一步被下一分类器划分为正常、入侵攻击两大类，其中入侵攻击类型随着检测系统的使用将会不断细分为各类入侵攻击。对于被划分为入侵攻击的融合数据实例最终将输出详细的相关评估信息。输出的入侵攻击评估信息包含发动时间t，目标设备群组G，设备状态向量S，目标量测量向量P，威胁评估R等关键信息，即输出信息的元组为：<t,G,S,P,R>。基于串行条件结构，首先把易分类的已知入侵攻击过滤掉，少数难分的实例将保留下来继续进行分类。调整好基分类器的阈值参数，在控制好其错分率的前提下就能提高最终的识别精度。

[0065] 上述智能电网入侵检测方法，实现对潜在入侵攻击行为的即时发现、准确识别、深度分析、详细评估，保证智能电网构建有效的安全防护，提高其主动防御能力，进而促进整个电力系统安全的保障升级。

[0066] 实施例3

[0067] 本发明实施例提供一种智能电网入侵检测设备，如图4所示，包括：至少一个处理器210，例如CPU(Central Processing Unit，中央处理器)，以及与至少一个处理器通信连接的存储器220；图4中以一个处理器210为例。该系统还可以包括：输入单元230。

[0068] 处理器210、存储器220、输入单元230可以通过总线200或者其他方式连接，图3中以通过总线200连接为例。

[0069] 其中，存储器220存储有可被处理器210执行的指令，处理器210通过运行存储在存储器220中的非暂态软件程序、指令以及模块，从而执行服务器的各种功能应用以及数据处理，即实现实施例2中的方法。

[0070] 输入单元230可接收输入的数字或字符信息，以及产生与列表项操作的处理装置的用户设置以及功能控制有关的键信号输入。

[0071] 一个或者多个模块存储在存储器220中，当被一个或者多个处理器210执行时，执行如图3所示的方法。

[0072] 上述产品可执行本发明实施例2所提供的方法，具备执行方法相应的功能模块和有益效果。未在本发明实施例中详尽描述的技术细节，具体可参见如图2所示的实施例中的相关描述。

[0073] 本发明实施例还提供了一种非暂态计算机存储介质，其上存储有计算机存储介质

存储有计算机可执行指令，该计算机可执行指令可执行实施例2中的智能电网入侵检测方法。其中，存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)、随机存储记忆体(Random Access Memory，RAM)、快闪存储器(Flash Memory)、硬盘(Hard Disk Drive，缩写：HDD)或固态硬盘(Solid-State Drive，SSD)等；存储介质还可以包括上述种类的存储器的组合。

[0074] 显然，上述实施例仅仅是为清楚地说明所作的举例，而并非对实施方式的限定。对于所属领域的普通技术人员来说，在上述说明的基础上还可以做出其它不同形式的变化或变动。这里无需也无法对所有的实施方式予以穷举。而由此所引伸出的显而易见的变化或变动仍处于本发明创造的保护范围之中。

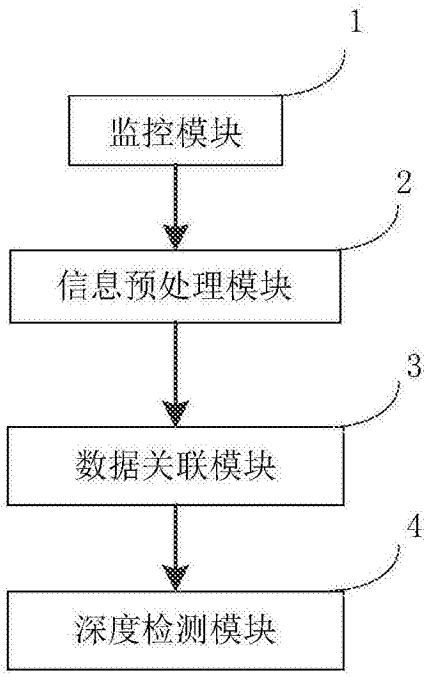


图1

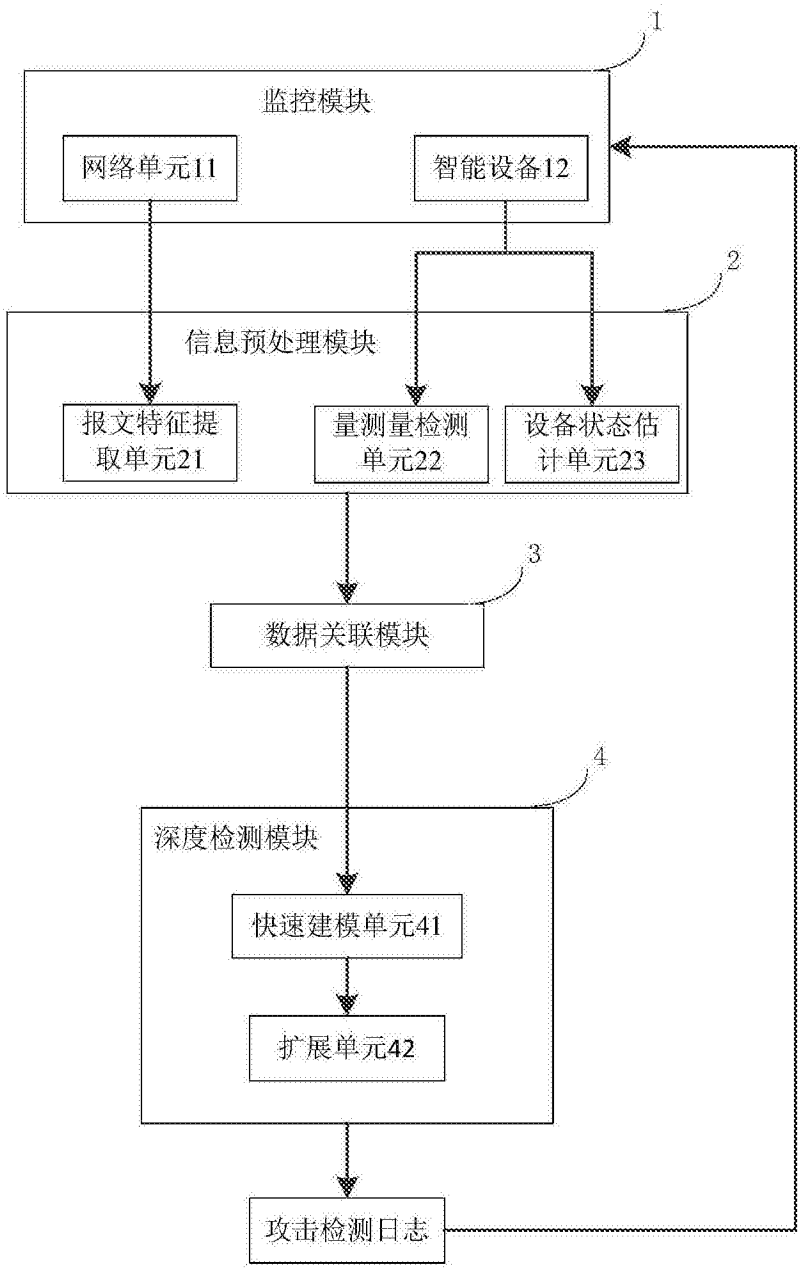

1
监控模块
网络单元11
智能设备12
2
信息预处理模块
报文特征提取单元21
量测量检测单元22
设备状态估计单元23
3
数据关联模块
4
深度检测模块
快速建模单元41
扩展单元42
攻击检测日志

图2

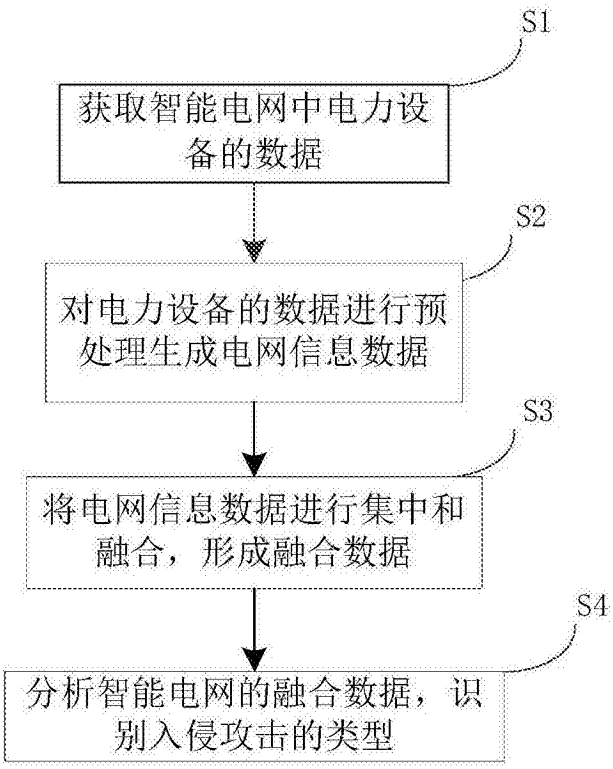

S1
获取智能电网中电力设备的数据
S2
对电力设备的数据进行预处理生成电网信息数据
S3
将电网信息数据进行集中和融合，形成融合数据
S4
分析智能电网的融合数据，识别入侵攻击的类型

图3

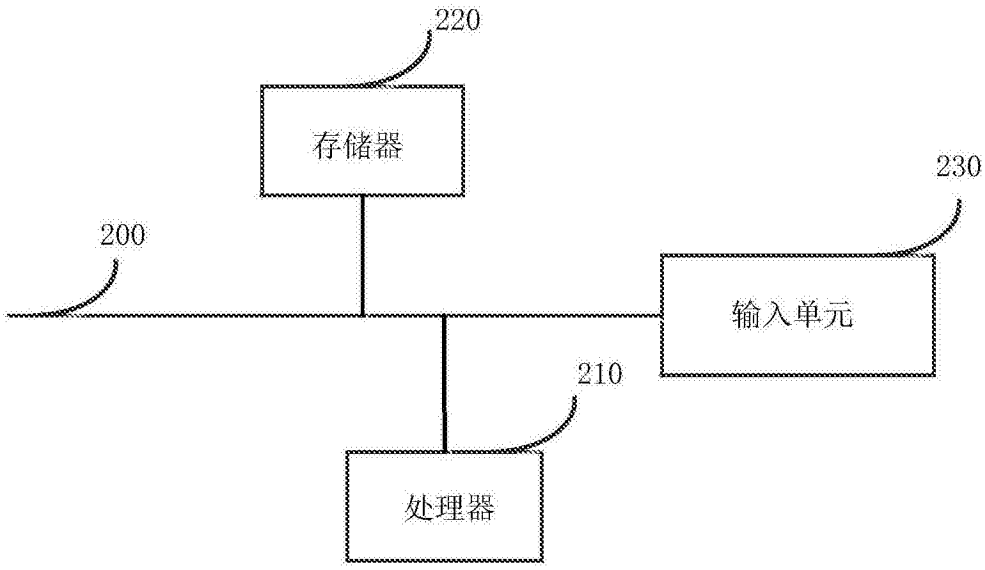

220
存储器
230
200
输入单元
210
处理器

图4