(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 113259380 B
(45)授权公告日 2021.09.17

(21)申请号 202110658158.8
(22)申请日 2021.06.15
(65)同一申请的已公布的文献号
申请公布号 CN 113259380 A
(43)申请公布日 2021.08.13
(73)专利权人 广东电网有限责任公司湛江供电局
地址 524005 广东省湛江市霞山区海滨大道南50号
(72)发明人 孙洁 叶鹏运 胡浩莹 罗宗杰 林鸿昊 许超尧 喻凌立 廖颖欢 陈臻
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 刘晓娟
(51)Int.Cl.
H04L 29/06(2006.01)
G06K 9/62(2006.01)
审查员 于兰

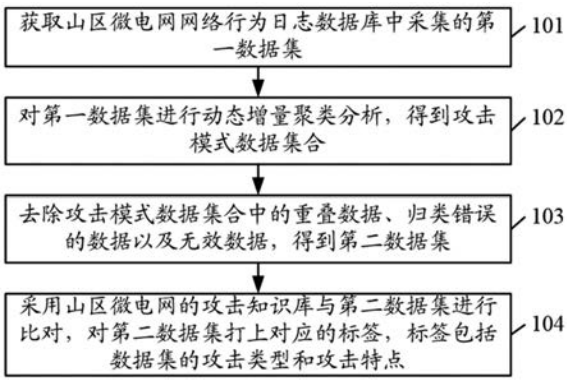
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种山区微电网网络攻击检测方法及装置

(57)摘要

本申请公开了一种山区微电网网络攻击检测方法及装置，包括：获取山区微电网网络行为日志数据库中采集的第一数据集；对第一数据集进行动态增量聚类分析，得到攻击模式数据集合；去除攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；采用山区微电网的攻击知识库与第二数据集进行比对，对第二数据集打上对应的标签，标签包括数据集的攻击类型和攻击特点。本申请提高攻击模式识别的准确率，降低网络安全系统中人为因素的影响。



CN 113259380 B

1.一种山区微电网网络攻击检测方法,其特征在于,包括:

获取山区微电网网络行为日志数据库中采集的第一数据集;

对所述第一数据集进行动态增量聚类分析,得到攻击模式数据集合,包括:

采用马氏距离法对所述第一数据集中的数据进行相似度分析,包括:

采用马氏距离函数对所述第一数据集对应的矩阵A进行计算,得到模糊等价关系矩阵M,$M=\left[m_{0j}\right]_{n\times n}$,$j=1,2,\cdots,n$,$m_{0j}$表示样本$a_0$和样本$a_j$间的相似系数,样本$a_0$和$a_j$是矩阵A中的数据;

根据设定的聚类划分准则,选择预设的阀值r对矩阵M进行划分,完成对所述第一数据集的分类,包括:

当$m_{0j}\geq r$时,将对应的a_j划为一类;其中,最优r值的选取公式为:

$$r_0=\frac{r_{i-1}-r_i}{n_i-n_{i-1}}$$

式中:i≥2,表示r从高到低排列的聚类次数;r_0表示最优r值;n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数;r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值;若存在$r_0=\max_j\left(r_j\right)$,$r_j$表示第j个选择的预设的阈值,j=1,2...,n,$\max_j\left(r_j\right)$表示选择的预设的阈值中的最大值,则第i次聚类的置信水平r_i为最佳阀值;

去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据,得到第二数据集;

采用山区微电网的攻击知识库与所述第二数据集进行比对,对所述第二数据集打上对应的标签,所述标签包括数据集的攻击类型和攻击特点。

2.根据权利要求1所述的山区微电网网络攻击检测方法,其特征在于,在所述对所述第一数据集进行动态增量聚类分析,得到攻击模式数据集合,之前还包括:

对所述第一数据集中的数据进行标准化处理。

3.根据权利要求2所述的山区微电网网络攻击检测方法,其特征在于,所述对所述第一数据集中的数据进行标准化处理,包括:

将所述第一数据集中的数据进行数据清洗、数据规约和数据集成,将所述第一数据集转化成具有统一格式的数据。

4.根据权利要求1所述的山区微电网网络攻击检测方法,其特征在于,所述去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据,得到第二数据集,包括:

若所述攻击模式数据集合中存在重叠数据,则将有重叠数据的数据集合并成一个数据集;

若所述攻击模式数据集合中不存在重叠数据,则去除数据集中归类错误的数据以及无效数据;

得到第二数据集。

5.一种山区微电网网络攻击检测装置,其特征在于,包括:

获取单元,用于获取山区微电网网络行为日志数据库中采集的第一数据集;

聚类分析单元，用于对所述第一数据集进行动态增量聚类分析，得到攻击模式数据集合；具体包括：

相似度分析单元，用于采用马氏距离法对所述第一数据集中的数据进行相似度分析，包括：

采用马氏距离函数对所述第一数据集对应的矩阵A进行计算，得到模糊等价关系矩阵M，$\mathrm{M}=\left[\mathrm{m}_{0\mathrm{j}}\right]_{\mathrm{n}\times\mathrm{n}}$，$\mathrm{j}=1,2,\cdots,\mathrm{n}$，$\mathrm{m}_{0\mathrm{j}}$表示样本$a_0$和样本$a_j$间的相似系数，样本$a_0$和$a_j$是矩阵A中的数据；

动态聚类分析单元，用于根据设定的聚类划分准则，选择预设的阀值r对矩阵M进行划分，完成对所述第一数据集的分类，包括：

当$\mathrm{m}_{0\mathrm{j}}\geqslant r$时，将对应的$a_j$划为一类；其中，最优$r$值的选取公式为：

$$r_0=\frac{r_{i-1}-r_i}{n_i-n_{i-1}}$$

式中：i≥2，表示r从高到低排列的聚类次数；r_0表示最优r值；n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数；r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值；若存在$r_0=\max_j\left(r_j\right)$，$\mathrm{r}_j$表示第j个选择的预设的阈值，j=1,2...,n，$\max_j\left(r_j\right)$表示选择的预设的阈值中的最大值，则第i次聚类的置信水平r_i为最佳阀值；

数据去除单元，用于去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；

标注单元，用于采用山区微电网的攻击知识库与所述第二数据集进行比对，对所述第二数据集打上对应的标签，所述标签包括数据集的攻击类型和攻击特点。

6.根据权利要求5所述的山区微电网网络攻击检测装置，其特征在于，还包括标准化单元，用于对所述第一数据集中的数据进行标准化处理。

7.根据权利要求6所述的山区微电网网络攻击检测装置，其特征在于，所述标准化单元具体用于将所述第一数据集中的数据进行数据清洗、数据规约和数据集成，将所述第一数据集转化成具有统一格式的数据。

一种山区微电网网络攻击检测方法及装置

技术领域

[0001] 本申请涉及网络安全技术领域，尤其涉及一种山区微电网网络攻击检测方法及装置。

背景技术

[0002] 山区微电网并入具有容量小、低压、分散等特点，随着山区微电网的快速发展，大规模新能源并网调控，网络运行日志也将更趋于海量化、异构化和低质化。面临的网络安全威胁主要表现在两个方面：一方面是电力终端设备本身的安全缺陷所引入的不可控风险；另一方面是承载终端设备控制信息流与数据流的微电网通信网络遭受入侵的风险。

发明内容

[0003] 本申请实施例提供了一种山区微电网网络攻击检测方法，采用基于SDN的山区微电网通信网攻击架构和基于动态增量聚类分析的网络攻击算法，通过基于虚拟映射的山区微网多业务通信、安全性能需求模型。提升攻击模式识别的准确率，降低网络安全系统中人为因素的影响，提高其可靠性和稳定性。

[0004] 有鉴于此，本申请第一方面提供了一种山区微电网网络攻击检测方法，所述方法包括：

[0005] 获取山区微电网网络行为日志数据库中采集的第一数据集；

[0006] 对所述第一数据集进行动态增量聚类分析，得到攻击模式数据集合；

[0007] 去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；

[0008] 采用山区微电网的攻击知识库与所述第二数据集进行比对，对所述第二数据集打上对应的标签，所述标签包括数据集的攻击类型和攻击特点。

[0009] 可选的，在所述对所述第一数据集进行动态增量聚类分析，得到攻击模式数据集合，之前还包括：

[0010] 对所述第一数据集中的数据进行标准化处理。

[0011] 可选的，所述对所述第一数据集中的数据进行标准化处理，包括：

[0012] 将所述第一数据集中得数据进行数据清洗、数据规约和数据集成，将所述第一数据集转化成具有统一格式的数据。

[0013] 可选的，所述对所述第一数据集进行动态增量聚类分析，得到攻击模式数据集合，包括：

[0014] 采用马氏距离法对所述第一数据集中的数据进行相似度分析，包括：

[0015] 采用马氏距离函数对所述第一数据集对应的矩阵A进行计算，得到模糊等价关系矩阵M，$M=\left[m_{0j}\right]_{n\times n}$，$j=1,2,\cdots,n$，$m_{0j}$表示样本$a_0$和样本$a_j$间的相似系数，样本$a_0$和$a_j$是矩阵A中的数据；

[0016] 根据设定的聚类划分准则，选择预设的阀值r对矩阵M进行划分，完成对所述第一

数据集的分类，包括：

[0017] 当$m_{0j} \geq r$时，将对应的a_j划为一类；其中，最优r值的选取公式为：

[0018] $$r_0 = \frac{r_{i-1} - r_i}{n_i - n_{i-1}}$$

[0019] 式中：i≥2，表示r从高到低排列的聚类次数；r_0表示最优r值；n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数；r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值；若存在$r_0 = \max_j(r_j)$，r_j表示第j个选择的预设的阈值，j=1,2...,n，$\max_j(r_j)$表示选择的预设的阈值中的最大值，则第i次聚类的置信水平r_i为最佳阀值；

[0020] 可选的，所述去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集，包括：

[0021] 若所述攻击模式数据集合中存在重叠数据，则将有重叠数据的数据集合并成一个数据集；

[0022] 若所述攻击模式数据集合中不存在重叠数据，则去除数据集中归类错误的数据以及无效数据；

[0023] 得到第二数据集。

[0024] 本申请第二方面提供一种山区微电网网络攻击检测装置，所述装置包括：

[0025] 获取单元，用于获取山区微电网网络行为日志数据库中采集的第一数据集；

[0026] 聚类分析单元，用于对所述第一数据集进行动态增量聚类分析，得到攻击模式数据集合；

[0027] 数据去除单元，用于去除所述攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；

[0028] 标注单元，用于采用山区微电网的攻击知识库与所述第二数据集进行比对，对所述第二数据集打上对应的标签，所述标签包括数据集的攻击类型和攻击特点。

[0029] 可选的，还包括标准化单元，用于对所述第一数据集中的数据进行标准化处理。

[0030] 可选的，所述标准化单元具体用于将所述第一数据集中得数据进行数据清洗、数据规约和数据集成，将所述第一数据集转化成具有统一格式的数据。

[0031] 可选的，所述聚类分析单元具体包括：

[0032] 相似度分析单元，用于采用马氏距离法对所述第一数据集中的数据进行相似度分析，包括：

[0033] 采用马氏距离函数对所述第一数据集对应的矩阵A进行计算，得到模糊等价关系矩阵M，$M = [m_{0j}]_{n \times n}$，$j = 1,2,\cdots,n$，$m_{0j}$表示样本$a_0$和样本$a_j$间的相似系数，样本$a_0$和$a_j$是矩阵A中的数据；

[0034] 动态聚类分析单元，用于根据设定的聚类划分准则，选择预设的阀值r对矩阵M进行划分，完成对所述第一数据集的分类，包括：

[0035] 当$m_{0j} \geq r$时，将对应的a_j划为一类；其中，最优r值的选取公式为：

[0036] $$r_0 = \frac{r_{i-1} - r_i}{n_i - n_{i-1}}$$

[0037] 式中：i≥2，表示r从高到低排列的聚类次数；r_0表示最优r值；n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数；r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值；若存在$r_0 = \max_j(r_j)$，r_j表示第j个选择的预设的阈值，j=1,2...,n，$\max_j(r_j)$表示选择的预设的阈值中的最大值，则第i次聚类的置信水平r_i为最佳阀值；

[0038] 本申请第三方面提供一种山区微电网网络，包括：SDN架构的山区微电网网络，所述SDN架构的山区微电网网络包括：

[0039] 转发平面，由山区微电网的具体通信设备组成，通信设备包括电力线通信网络、光纤网络、微功无线以及微波红外网络设备，用于向集中控制平面上传采集到的数据；

[0040] 所述集中控制平面采用适配基于动态增量聚类分析的网络攻击模式识别算法，通过南向接口与光纤网络、微功无线网络和电力线以及微波红外网络设备进行通信；收集配电通信网络的各项统计信息，分析所述统计信息实现配电通信网络的攻击检测和拓扑辨识、路由管理、流量监测、安全防控的功能；通过北向接口上传所述统计信息并接收配网应用平面下发的控制逻辑信号；

[0041] 所述配网应用平面用于面向维持微电网上传的所述统计信息进行攻击检测、攻击识别和攻击拦截；并根据预置的业务逻辑向所述集中控制平面下发控制逻辑信号。

[0042] 从以上技术方案可以看出，本申请具有以下优点：

[0043] 本申请提供了一种山区微电网网络攻击检测方法，包括：获取山区微电网网络行为日志数据库中采集的第一数据集；对第一数据集进行动态增量聚类分析，得到攻击模式数据集合；去除攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；采用山区微电网的攻击知识库与第二数据集进行比对，对第二数据集打上对应的标签，标签包括数据集的攻击类型和攻击特点。

[0044] 本申请提出基于SDN的山区微电网通信网攻击架构和基于动态增量聚类分析的网络攻击算法，通过基于虚拟映射的山区微网多业务通信、安全性能需求模型。提升攻击模式识别的准确率，降低网络安全系统中人为因素的影响，提高其可靠性和稳定性。

附图说明

[0045] 图1为本申请一种山区微电网网络攻击检测方法的一个实施例的方法流程图；

[0046] 图2为本申请一种山区微电网网络攻击检测装置的实施例中的装置结构图；

[0047] 图3为本申请一种山区微电网网络的实施例中网络架构示意图；

[0048] 图4为本申请一种山区微电网网络攻击检测方法的一个具体实施方式的方法流程图。

具体实施方式

[0049] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

[0050] 图1为本申请一种山区微电网网络攻击检测方法的一个实施例的方法流程图，如图1所示，图1中包括：

[0051] 101、获取山区微电网网络行为日志数据库中采集的第一数据集；

[0052] 需要说明的是，本申请可以获取山区微电网网络行为日志数据库，从数据库中获取需要进行聚类算法的数据。本申请采集的数据将生产厂家、设备编号、运行设备所在地址、用电性质等基础档案分别录入数据库。假设体现客户用电情况的电流、电压、有功功率、功率因数等电能量数据的集合为$A=\{a_1,a_2,\cdots,a_i,\cdots,a_n\}(i=1,2,\cdots,n)$，每个元素$a_i$具有$m$个特征，可用$a_i=\left(a_{i1},a_{i2},\cdots,a_{ij},\cdots,a_{im}\right)$表示，$a_{ij}$表示第$i$个样本的第$j$项特性指标，$j=1,2,\cdots,m$，则电能量数据集合$A$的特性指标矩阵形式为：

[0053] $$A=\begin{pmatrix} a_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & a_{22}, & \cdots, & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1}, & a_{n1}, & \cdots, & a_{nm} \end{pmatrix}。$$

[0054] 102、对第一数据集进行动态增量聚类分析，得到攻击模式数据集合；

[0055] 需要说明的是，针对电力系统监测量的特点，采用马氏距离法对数据集中的各元素进聚类相似度分析。

[0056] 具体的，假设经马氏距离函数计算后得到矩阵A的模糊等价关系矩阵M为：

[0057] $\mathrm{M}=\left[\mathrm{m}_{0\mathrm{j}}\right]_{\mathrm{n}\times\mathrm{n}}$，$\mathrm{j}=1,2,\cdots,\mathrm{n}$，假设$\mathrm{m}_{0\mathrm{j}}$表示样本$a_0$和样本$a_j$间的相似系数。当$\mathrm{m}_{0\mathrm{j}}$的绝对值越接近1，则表明$a_0$和$a_j$越相似。反之，两者关系越疏远。根据设定的聚类划分准则，选择适当的阀值r对矩阵M进行截割，就可得到该样本集A的分类。可以规定$\mathrm{m}_{0\mathrm{j}}\geq r$时，满足此条件的$a_j$划为一类。因为阀值$r$不同，样本集分类结果也将不同。$r$从1逐渐变化到0，分类数目从粗糙到精细不断变化，可形成对样本集的一个动态聚类过程，最优r值的选取，可以通过下式逐渐调整以求得最优解。

[0058] $$r_0=\frac{r_{i-1}-r_i}{n_i-n_{i-1}}$$

[0059] 式中：i≥2，表示r从高到低排列的聚类次数；r_0表示最优r值；n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数；r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值；若存在$r_0=\max_j\left(r_j\right)$，$r_j$表示第j个选择的预设的阈值，j=1,2...,n，$\max_j\left(r_j\right)$表示选择的预设的阈值中的最大值，则第i次聚类的置信水平r_0为最佳阀值；

[0060] 103、去除攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集；

[0061] 需要说明的是，针对获取的攻击模式数据集合进行后处理，若攻击模式数据集合中存在数据重叠的数据集，则将具有重叠数据的数据集合并为一个新的数据集。针对全部的攻击模式数据集合重复此合并过程，直到不再存在数据重叠的组。若不存在数据重叠(部

分集合之间可能会存在重叠的数据)的攻击模式数据集合,则进一步从攻击特征、攻击频率和经验知识等方面出发对数据集中的数据做进一步的筛选,去除归类错误的数据和无效类数据,形成第二数据集。

[0062] 104、采用山区微电网的攻击知识库与第二数据集进行比对,对第二数据集打上对应的标签,标签包括数据集的攻击类型和攻击特点。

[0063] 需要说明的是,对于第二数据集数据集,运用山区微电网通信网络积累的攻击知识库和专家系统对第二数据集进行标签化操作,对第二数据集的攻击的类型和攻击的特点打上标签,生成完整的攻击模式分类数据集,动态增量聚类分析负责对数据根据特征进行面向攻击模式的归类。

[0064] 本申请提出基于动态增量聚类分析的网络攻击算法,通过基于虚拟映射的山区微网多业务通信、安全性能需求模型。提升攻击模式识别的准确率,降低网络安全系统中人为因素的影响,提高其可靠性和稳定性。

[0065] 在一种具体的实施方式中,本申请还提供了一种山区微电网网络攻击检测方法的一个具体的实施方式,如图4所示,图4中在对第一数据集进行动态增量聚类分析,得到攻击模式数据集合,之前还包括:

[0066] 对第一数据集中的数据进行标准化处理。

[0067] 需要说明的是,可以将山区微电网中的安全设施(包括交换机、IPS防御设备、防火墙等)得到的第一数据集中的数据进行数据清洗、数据规约和数据集成,将第一数据集转化成具有统一格式的数据。

[0068] 本申请还提供了一种山区微电网网络攻击检测装置的实施例,如图2所示,图2中包括:

[0069] 获取单元201,用于获取山区微电网网络行为日志数据库中采集的第一数据集;

[0070] 聚类分析单元202,用于对第一数据集进行动态增量聚类分析,得到攻击模式数据集合;

[0071] 数据去除单元203,用于去除攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据,得到第二数据集;

[0072] 标注单元204,用于采用山区微电网的攻击知识库与第二数据集进行比对,对第二数据集打上对应的标签,标签包括数据集的攻击类型和攻击特点。

[0073] 还包括标准化单元,用于对第一数据集中的数据进行标准化处理。

[0074] 聚类分析单元202具体包括:

[0075] 相似度分析单元,用于采用马氏距离法对第一数据集中的数据进行相似度分析,包括:

[0076] 采用马氏距离函数对第一数据集对应的矩阵A进行计算,得到模糊等价关系矩阵M,$M=\left[m_{0j}\right]_{n\times n}$,$j=1,2,\cdots,n$,$m_{0j}$表示样本$a_0$和样本$a_j$间的相似系数,样本$a_0$和$a_j$是矩阵A中的数据;

[0077] 动态聚类分析单元,用于根据设定的聚类划分准则,选择预设的阀值r对矩阵M进行划分,完成对所述第一数据集的分类,包括:

[0078] 当$m_{0j}\geq r$时,将对应的a_j划为一类;其中,最优r值的选取公式为:

[0079] $$r_0=\frac{r_{i-1}-r_i}{n_i-n_{i-1}}$$

[0080] 式中：i≥2，表示r从高到低排列的聚类次数；r_0表示最优r值；n_i和n_{i-1}分别为第i次和第i-1次聚类的元素个数；r_i和r_{i-1}分别为第i次和第i-1次聚类的阀值；若存在$r_0=\max_j(r_j)$，r_j表示第j个选择的预设的阈值，j=1,2...,n，$\max_j(r_j)$表示选择的预设的阈值中的最大值，则第i次聚类的置信水平r_i为最佳阀值；

[0081] 本申请还提供了一种山区微电网网络的一个实施例的系统结构图，如图3所示，图3中包括SDN架构的山区微电网网络，SDN架构的山区微电网网络包括：

[0082] 转发平面，由山区微电网的具体通信设备组成，通信设备包括电力线通信网络、光纤网络、微功无线以及微波红外网络设备，用于向集中控制平面上传采集到的数据；

[0083] 集中控制平面采用适配基于动态增量聚类分析的网络攻击模式识别算法，通过南向接口与光纤网络、微功无线网络和电力线以及微波红外网络设备进行通信；收集配电通信网络的各项统计信息，分析统计信息实现配电通信网络的攻击检测和拓扑辨识、路由管理、流量监测、安全防控的功能；通过北向接口上传统计信息并接收配网应用平面下发的控制逻辑信号；

[0084] 配网应用平面用于面向维持微电网上传的统计信息进行攻击检测、攻击识别和攻击拦截；并根据预置的业务逻辑向集中控制平面下发控制逻辑信号。

[0085] 需要说明的是，采用SDN架构融入到配电通信网体系中，能够在全局视角上对网络架构和功能进行调整，从而大大降低网络管理的难度。根据SDN网络架构体系，将山区微电网通信网网络架构划分为三层：配网应用平面、集中控制平面和转发平面。

[0086] 其中配网应用平面用于面向维持微电网正常运行的各种服务，运行网络管理人员根据入侵检测需求定制不同的应用，主要包攻击检测、攻击识别、攻击拦截等，不同应用可以负责完全独立的山区微电网配电业务管理逻辑，并行通过北向接口将逻辑下发。

[0087] 集中控制平面是采用适配基于动态增量聚类分析的网络攻击模式识别算法，通过南向接口与光纤网络、微功无线网络和电力线以及微波红外等进行通信，收集配电通信网络的各项统计信息，汇总分析这些统计信息实现配电通信网络的攻击检测和拓扑辨识、路由管理、流量监测、安全防控等基础功能。通过北向接口上传网络统计信息并接收配网应用平面下发的控制逻辑，保障应用平面对山区微电网通信网络资源的集中、灵活管理，同时准确检测和识别攻击行为。

[0088] 转发平面用于转发平面由山区微电网具体通信设备组成，电力线通信网络、光纤网络、微功无线以及微波、红外等网络和中的转发设备仅保留数据转发功能，其逻辑转发功能被上移到配网应用平面集中管理，简化了通信终端结构。

[0089] 本申请提出基于SDN的山区微电网通信网攻击架构和基于动态增量聚类分析的网络攻击算法，通过基于虚拟映射的山区微网多业务通信、安全性能需求模型。提升攻击模式识别的准确率，降低网络安全系统中人为因素的影响，提高其可靠性和稳定性。

[0090] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0091] 本申请的说明书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等是用于区

别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0092] 应当理解，在本申请中，“至少一个(项)”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，用于描述关联对象的关联关系，表示可以存在三种关系，例如，“A和/或B”可以表示：只存在A，只存在B以及同时存在A和B三种情况，其中A，B可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a，b或c中的至少一项(个)，可以表示：a，b，c，“a和b”，“a和c”，“b和c”，或“a和b和c”，其中a，b，c可以是单个，也可以是多个。

[0093] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0094] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0095] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0096] 以上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

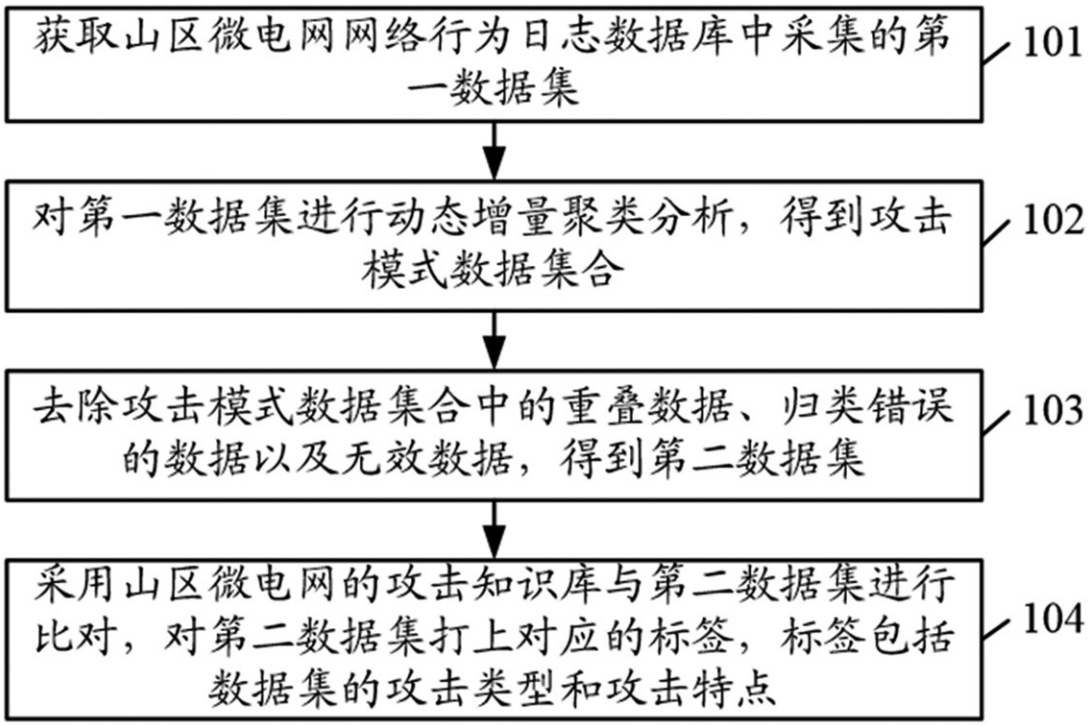

获取山区微电网网络行为日志数据库中采集的第一数据集
101
对第一数据集进行动态增量聚类分析，得到攻击模式数据集合
102
去除攻击模式数据集合中的重叠数据、归类错误的数据以及无效数据，得到第二数据集
103
采用山区微电网的攻击知识库与第二数据集进行比对，对第二数据集打上对应的标签，标签包括数据集的攻击类型和攻击特点
104

图 1

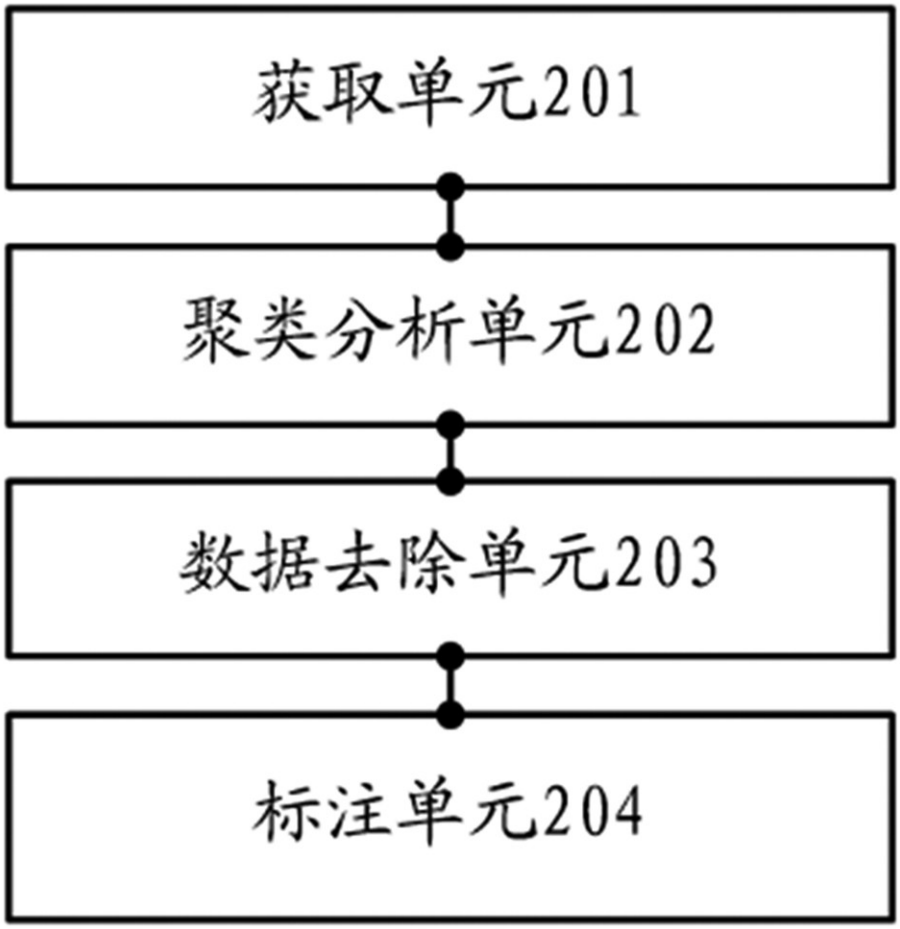


图 2

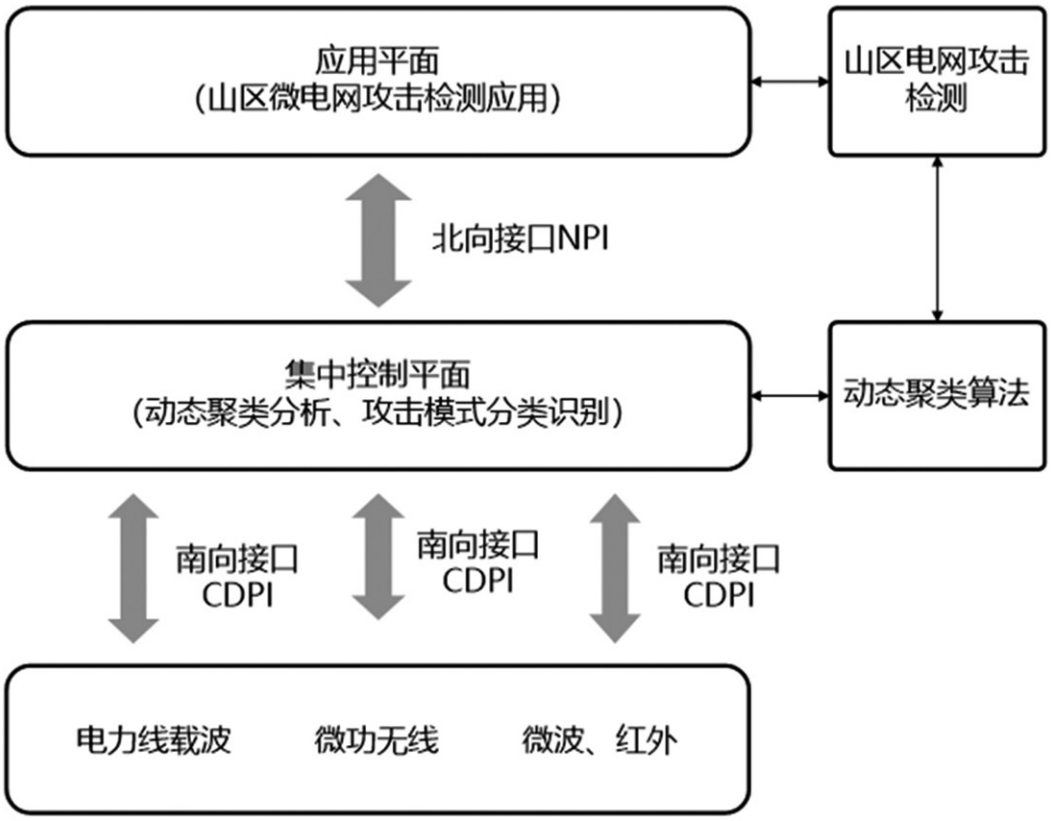

应用平面
(山区微电网攻击检测应用)
山区电网攻击检测
北向接口NPI
集中控制平面
(动态聚类分析、攻击模式分类识别)
动态聚类算法
南向接口CDPI
南向接口CDPI
南向接口CDPI
电力线载波
微功无线
微波、红外

图 3

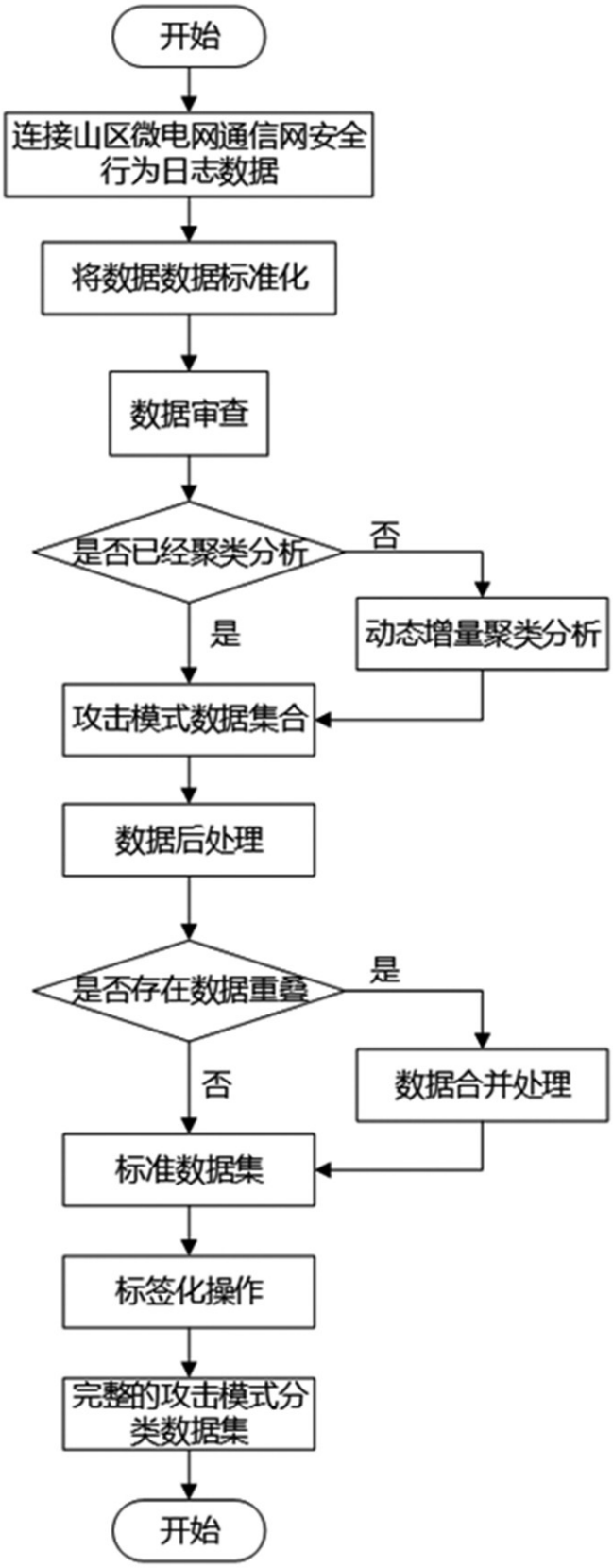

开始
连接山区微电网通信网安全行为日志数据
将数据数据标准化
数据审查
是否已经聚类分析
否
是
动态增量聚类分析
攻击模式数据集合
数据后处理
是否存在数据重叠
是
否
数据合并处理
标准数据集
标签化操作
完整的攻击模式分类数据集
开始

图 4