(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112464295 B
(45)授权公告日 2023.06.30

(21)申请号 202011465272.0
(22)申请日 2020.12.14
(65)同一申请的已公布的文献号
申请公布号 CN 112464295 A
(43)申请公布日 2021.03.09
(73)专利权人 国网辽宁省电力有限公司抚顺供电公司
地址 113008 辽宁省抚顺市新抚区西一路13号
专利权人 国家电网有限公司 东北大学
(72)发明人 张海 刘鑫蕊 丁以心 孙秋野 张瑶瑶 樊志诚 湛树广 王震 张祥 陈杰辉
(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
专利代理师 梁焱
(51)Int.Cl.
G06F 21/72(2013.01)
G06F 18/24(2023.01)
G06F 18/214(2023.01)
G06N 20/00(2019.01)
(56)对比文件
US 2020287914 A1,2020.09.10
US 2004261116 A1,2004.12.23
CN 110602041 A,2019.12.20
US 2019319977 A1,2019.10.17
US 2014123269 A1,2014.05.01
审查员 章鹏

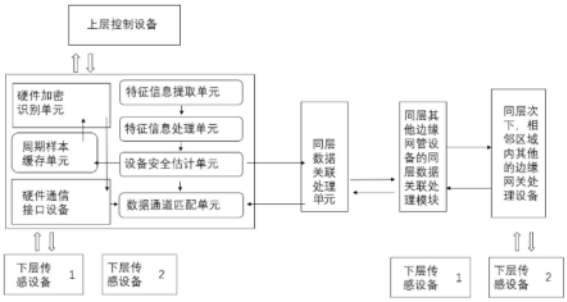
权利要求书3页 说明书9页 附图2页

(54)发明名称

基于电力边缘网关设备的维护通信安全装置

(57)摘要

本发明提供一种基于电力边缘网关设备的维护通信安全装置，涉及电气设备技术领域。该装置包括硬件部分和软件部分；硬件部分包括加密识别单元及其通信接口设备，用于对下层设备传入的通信数据进行信息读取、白名单资格比对和预分类，与软件端口之间有数据连接；软件部分包括基础判别模块、周期白名单设备检查模块、信息检测及故障判别模块。本发明在机器学习的算法与硬件加密特征编码信息的基础上，实现对于底层传感设备的唯一识别及安全评估，并安排周期性的白名单更新，达到对于整个设备数据传输过程安保的要求。并在此基础上设计了在同层次边缘网关内实现多网关矩阵式辅助安全评估的功能，达到提高判断准确率的目的。



CN 112464295 B

1.一种基于电力边缘网关设备的维护通信安全装置,其特征在于:包括硬件部分和软件部分;

硬件部分包括加密识别单元及其通信接口设备,用于对下层设备传入的通信数据进行信息读取、白名单资格比对和预分类,与软件端口之间有数据连接;

加密识别单元,用于通过对于软件部分的基础判别模块生成的周期性的单个设备的设备特征信息编号进行基于RAS加密算法的加密,以达到对白名单信息的物理加密的目的;

通信接口部分用于在设定好通讯协议的情况下匹配下层设备,并读取设备的特征信息编号,通过固定的解码方法,达到设备基础信息预读的目的;

软件部分包括基础判别模块、周期白名单设备检查模块、信息检测及故障判别模块;

基础判别模块,包括依次连接的特征信息提取单元、特征信息处理单元、设备安全估计单元和数据通道匹配单元,用于通过对于下层设备的上载请求及内容信息的特征值进行提取,并通过KNN构架下的算法构建一个具有辨识性的唯一的设备特征信息编号,并生成相对应的安全评估,依据评估结果对设备进行操作权限的赋予;

所述特征信息提取单元,用于对非白名单设备的上行数据的一些基于其工作特点和设备特点的特征数据进行提取,并将提取的特征数据进行数字化以方便之后的计算运行;还用于对白名单设备进行抽样式的特征提取,用以之后进行周期性的状态检测;

所述特征信息处理单元,用于将提取上来的传感器设备的特征信息进行处理学习,构建基于相关设备的运行机制的“识别指纹”,生成一个具有相关分类判断能力的训练模型,同时对相关数据的处理结果进行分类并进行比对,进行异常比对的参数在初始阶段可以通过预先设置进行设定,用以区分是否可以将此类设备放入白名单;还用于通过判断数据的连接申请命令及调度命令是否存在异常状态,给设备信息赋予安全状态;在遇到非安全状态反馈以后,通过获取同层数据关联处理单元的数据反馈后,对安全状态进行二次评估或更新;在数据量较多的情况下优先处理非白名单设备,从而达到计算能力自适应匹配的效果;

所述设备安全估计单元,在一般数据通过处理判断后,如果在白名单内,且判断为安全状态,则只需通过简单的命令匹配后,进入边缘网关的核心处理模块进行数据的处理运算;如果被判断为非安全状态,则连接同层数据关联处理单元将信息返回多个设备的特征信息处理单元和设备安全估计单元进行联合判比之后,将结果反馈至数据通道匹配单元进行处理;

所述数据通道匹配单元,根据设备安全估计单元将设备特征信息处理结束以后反馈的处理结果,对设备数据分类赋予权限,权限包括只允许设备信息上行、只允许设备信息下行、同时允许设备数据双向传递和暂时断开设备连接;

周期白名单设备检查模块,包括与设备安全估计单元连接的周期样本缓存单元,用于通过设置人为时间作为阈值或通过白名单增长的数量作为阈值,来进行对于已经判别为安全的白名单设备进行周期性二次安全风险评估;

所述周期样本缓存单元,用于对硬件模块反馈的活跃性比较高的设备类型,以及部分新加入白名单的设备的特征值处理结果进行储存;并以一定周期或白名单设备增长数量作为触发阈值,不定向的从特征信息处理单元中抽取并保存已在白名单中的各类型设备的信息特征,并在之后的运行中按照一定周期频率与该类型设备的新进数据进行比对,确保其

传输通道稳定或按照一定规律变化，如不满足该条件，则重新审查其白名单资格；同时检查存储部分是否存在重复存储现象；通过以上操作，达到更新白名单的目的；

信息检测及故障判别模块，包括与设备安全估计单元连接的同层数据关联处理单元，用于在设备安全估计单元判定为非安全设备的数量到达一定阈值或处理优先级到达阈值时，通过将数据完整打包发送给其他同层状态下的边缘网关进行辅助判断，即少数服从多数的概率判断。

2.根据权利要求1所述的基于电力边缘网关设备的维护通信安全装置，其特征在于：所述加密识别单元及其通信接口设备，具有链路识别维护、数据加密、信息指纹比对、设备特征信息提取的功能，用于通过基础判别模块生成的单个设备的设备特征信息编号进行基于RAS加密算法的加密，并根据去加密算法的数学性质，周期性的更新加密算子，以达到对于白名单信息的物理加密的目的；还用于接受多种链路信号，并通过机器学习的方法对于设定的特征进行提取和分析，并将其与储存在白名单上的数据进行对比，得出粗略的结果，以达到设备基础数据预读取的目的；

其具体功能实现过程如下：

步骤1.1：检测接入设备是否符合通信标准，不为无效信息；如为判定符合标准，则确认设备的特征信息编号是否已经被安全估计单元判断为安全可接入白名单设备；

步骤1.2：在通信接口设备对传入并读取到的设备特征信息编号赋予一个现场生成的包含有此时处于匹配状态的设备的一部分预读信息的身份编号数列，该编号数列是用于识别具体对应的设备，编号与设备具有唯一性，该编号数列的长度不超过16位；

步骤1.3：在运行中依据RAS加密算法原理产生一个基于500位计算值以内的RAS明码和加密暗码，其加密暗码部分及上一步获得的设备身份编号数列保存在白名单中作为鉴别，明码部分用于对身份编号加密；

步骤1.4：将上一步中加密后的对应单独设备的身份编号数列以一种数据标签的方式添加；为保证识别效率和防止被替代，加密后的身份编号将插入设备特征信息编号，作为新的设备特征信息的一部分，但并不直接单独赋予这个设备；

步骤1.5：当设备再次申请连接时，特征信息编号中的身份编号部分被提出，对身份编号进行解码，并将解码部分与白名单库中保存的设备身份编号进行对比，确定其合法性，并读取编码中的信息段，获取其应用方向，完成第一道效验部分。

3.根据权利要求1所述的基于电力边缘网关设备的维护通信安全装置，其特征在于：所述基础判别模块，引入具有KNN架构下的机器学习算法的特征信息提取单元与设备安全评估单元，所述算法的应用基础是：

(1)对于目前的大部分设备具有很好的适应性和拓展性；

(2)在同厂家生产的大部分设备为了接口的一致性，都具有基于功能性的较相似的数据排列特征；所述算法通过对接收下层设备的数据的提取分析，构建具有相关分类判断能力的训练模型；

其具体实现过程如下：

步骤2.1：在模型训练阶段，向基础判别模块输入作为参考和训练的数据，包括输入的数据所对应的具体类别及其安全情况；作为参考和训练的数据依据边缘网关所处的范围区域内设备种类不同而加以调整；再通过已知的边缘网关需要的数据特征，对于训练的数据

进行数字化特征提取和分析;通过提取的特征和数据集合,完成下层传输设备输入信息的分类判断;在下层传输设备输入信息之前需要通过硬件部分通信方式的认证对数据的有效性进行分析,排除非安全信息因素;

步骤2.2:采用将数据特征分层的方式,通过数据的复杂性将下层设备传输数据的分类过程分为两层,第一层通过提取数字长度较短的特征信息,来对样本数据进行初步的分类判断,根据K-邻近算法,通过计算相同特征数据的欧式距离将数字化后的这些特征信息进行总距离计算,并选取距离最短的K个数据点,然后将此样本数据归为K个数据中出现频率最高的两到三类数据,并进入通过传输数据的具体内容进行分类;如果样本数据与训练数据在这些特征上总和的最短距离超过某一阈值L时认为其类别不在训练的白名单上,让其以新的类别形式加入白名单中;

步骤2.3:在第一层完成了对数据类型的初步判断后,获得几个与样本可能为一类的训练数据,在第二层次的计算中通过获得的这几个训练数据中的具体传输数据和表示终端运行的状态数据来确定输入样品数据的安全等级并将驶入样品数据放入对应类型的白名单中;需要注意的是,要根据不同的传输层数据类型进行不同的划分,然后才能计算样本数据与白名单数据之间的相似度,计算完成后仍然利用上一层的K-邻近算法,算出与样品数据相似度最近的K个值,并且得出某个类别的某一级安全性在这K个值中所占的频数最大,就可以将由下层设备传输的样品数据进行归类,并进行安全评估。

4.根据权利要求1所述的基于电力边缘网关设备的维护通信安全装置,其特征在于:所述同层数据关联处理单元,将多个边缘网关的处理范围进行重叠用以进行辅助判断,由一个主处理网关和一个或多个副处理网关构成,其中主处理网关负责构建多个网关之间的数据通道,并作为一个发送节点,对数据命令进行双向的传输,副边缘网关则不涉及通道构建,而只作为安全状态辅助评估;

其具体实施步骤如下:

步骤3.1:多个边缘网关相互连接,各自在处理所属区域内设备请求的时候,按照一定规律周期性的将一部分判断为不合格的申请数据在保留主要控制权限的基础上,分享给同层的其他边缘网关进行安全判断;

步骤3.2:当出现异常信息判断时,将同层内多个边缘网关互相的链接作为一张矩阵网并划分区域,将边缘网关作为节点;从上层设备收集到的边缘网关反馈信息中,通过步进的方式,锁定发出警报的区域网关节点所工作的范围,进而通过类似于麦克风阵列锁定声源发出方向的计算思想,以一个警报节点作为参考,计算各个节点发出警报信息的时间差,进而锁定原始警报发出节点,并获得异常下层设备的具体型号和IP地址。

基于电力边缘网关设备的维护通信安全装置

技术领域

[0001] 本发明涉及电气设备技术领域，尤其涉及一种基于电力边缘网关设备的维护通信安全装置。

背景技术

[0002] 在通讯速度日益增快的前提下，处理设备越来越倾向于智能化、便携化，由此带来了物联网技术的快速发展。智能设备的互相连接，也推动着智能电网相关设备的快速发展，但随之而来的，是愈加庞大的数据量和更多种类形式的通信要求。在这个前提下，边缘计算与承载技术的边缘网关设备，一种具有更好的信息提取能力和更快的数据处理反馈速度的处理器布设方式开始兴起，但这也随之带来了对于信息安全的一定威胁。

[0003] 传统电网的信息传递过程大多使用的暗网的形式，即使用区域内网进行信息传输，这样的传输方式虽然较保守，但通过固定的密钥数量及访问权限可以做到更为安全的传输。相对的，新型边缘网关设备因为要保持对于多传感器的数据采集，不再适宜使用传统的区域网技术，大多采用云端进行数据处理，由此带来了数据在无线网络传输过程中的安全隐患。

[0004] 其安全隐患主要存在于数据传输和信息保存两个方面。对于数据传输：1.在数据上行通道方面，对于大量的传感器设备数据，信息可能出现被恶意替换或者恶意屏蔽的情况，造成在数据判断方面的缺失遗漏。2.在数据下行方面，可能出现针对设备的大量非正常指令，使下一层设备进入短暂的失控状态，干扰正常的运行。对于信息保存：由于大量数据被临时保存在边缘网关设备中，容易遭到恶意读取，导致部分客户信息泄露。

[0005] 现行的方法比较常用的是对于设备通信信息的加密和设置设备白名单。目前的处理方法中：1.大多通过计算加密的方式实现传感器及边缘网关的相互认证与信息加密，但这类方法一般复杂度比较高，对于处理设备的计算能力有一定要求，对于边缘网关设备来说不是十分适宜。2.也有通过区块链技术实现的安全加密，通过对于链上相关区块的加密，实现该区块信息的有效保护，但这类方法对于已信任设备的误判信息的处理效果不是很好，且运行数据的判断较为独立，没有形成整体判断。3.还有部分通过硬件设备进行加密，但是对于需要处理大量传感器的边缘网关设备，在每个传感器上都安装相应的安全硬件对于成本又有所限制。并且在白名单机制上面，无法对白名单成员进行动态的筛选。

发明内容

[0006] 本发明要解决的技术问题是针对上述现有技术的不足，提供一种基于电力边缘网关设备的维护通信安全装置，通过硬件部分和软件部分相配合的方式，通过实现以安全算法为核心的边缘计算技术以及通过对于同层次多网关的数据共同处理，实现边缘网关节点与上下层设备的通信安全且高效，具有在同层范围内多设备连接共享以实现对于误判数据的尽可能减少，防止误判信息导致的长时间通道断开，同时实现对于出错点的预先位置估计，并根据算法学习生成一个基于数据类型白名单，通过数量反馈帮助统计时段内通信请

求密度。

[0007] 为解决上述技术问题，本发明所采取的技术方案是：

[0008] 一种基于电力边缘网关设备的维护通信安全装置，包括硬件部分和软件部分；

[0009] 硬件部分包括加密识别单元及其通信接口设备，用于对下层设备传入的通信数据进行信息读取、白名单资格比对和预分类，与软件端口之间有数据连接；

[0010] 加密识别单元，用于通过对于软件部分的基础判别模块生成的周期性的单个设备的设备特征信息编号进行基于RAS加密算法的加密，以达到对白名单信息的物理加密的目的；

[0011] 通信接口部分用于在设定好通讯协议的情况下匹配下层设备，并读取设备的特征信息编号，通过固定的解码方法，达到设备基础信息预读的目的；

[0012] 软件部分包括基础判别模块、周期白名单设备检查模块、信息检测及故障判别模块；

[0013] 基础判别模块，包括依次连接的特征信息提取单元、特征信息处理单元、设备安全估计单元和数据通道匹配单元，用于通过对于下层设备的上载请求及内容信息的特征值进行提取，并通过KNN构架下的算法构建一个具有辨识性的唯一的设备特征信息编号，并生成相对应的安全评估，依据评估结果对设备进行操作权限的赋予；

[0014] 所述特征信息提取单元，用于对非白名单设备的上行数据的一些基于其工作特点和设备特点的特征数据进行提取，并将提取的特征数据进行数字化以方便之后的计算运行；还用于对白名单设备进行抽样式的特征提取，用以之后进行周期性的状态检测；

[0015] 所述特征信息处理单元，用于将提取上来的传感器设备的特征信息进行处理学习，构建基于相关设备的运行机制的“识别指纹”，生成一个具有相关分类判断能力的训练模型，同时对相关数据的处理结果进行分类并进行比对，进行异常比对的参数在初始阶段可以通过预先设置进行设定，用以区分是否可以将此类设备放入白名单；还用于通过判断数据的连接申请命令及调度命令是否存在异常状态，给设备信息赋予安全状态；在遇到非安全状态反馈以后，通过获取同层数据关联处理单元的数据反馈后，对安全状态进行二次评估或更新；在数据量较多的情况下优先处理非白名单设备，从而达到计算能力自适应匹配的效果；

[0016] 所述设备安全估计单元，在一般数据通过处理判断后，如果在白名单内，且判断为安全状态，则只需通过简单的命令匹配后，进入边缘网关的核心处理模块进行数据的处理运算；如果被判断为非安全状态，则连接同层数据关联处理单元将信息返回多个设备的特征信息处理单元和设备安全估计单元进行联合判比之后，将结果反馈至数据通道匹配单元进行处理；

[0017] 所述数据通道匹配单元，根据设备安全估计单元将设备特征信息处理结束以后反馈的处理结果，对设备数据分类赋予权限，权限包括只允许设备信息上行、只允许设备信息下行、同时允许设备数据双向传递和暂时断开设备连接；

[0018] 周期白名单设备检查模块，包括与设备安全估计单元连接的周期样本缓存单元，用于通过设置人为时间作为阈值或通过白名单增长的数量作为阈值，来进行对于已经判别为安全的白名单设备进行周期性二次安全风险评估；

[0019] 所述周期样本缓存单元，用于对硬件模块反馈的活跃性比较高的设备类型，以及

部分新加入白名单的设备的特征值处理结果进行储存;并以一定周期或白名单设备增长数量作为触发阈值,不定向的从特征信息处理单元中抽取并保存已在白名单中的各类型设备的信息特征,并在之后的运行中按照一定周期频率与该类型设备的新进数据进行比对,确保其传输通道稳定或按照一定规律变化,如不满足该条件,则重新审查其白名单资格;同时检查存储部分是否存在重复存储现象;通过以上操作,达到更新白名单的目的;

[0020] 信息检测及故障判别模块,包括与设备安全估计单元连接的同层数据关联处理单元,用于在设备安全估计单元判定为非安全设备的数量到达一定阈值或处理优先级到达阈值时,通过将数据完整打包发送给其他同层状态下的边缘网关进行辅助判断,即少数服从多数的概率判断。

[0021] 进一步地,所述加密识别单元及其通信接口设备,具有链路识别维护、数据加密、信息指纹比对、设备特征信息提取的功能,用于通过基础判别模块生成的单个设备的设备特征信息编号进行基于RAS加密算法的加密,并根据去加密算法的数学性质,周期性的更新加密算子,以达到对于白名单信息的物理加密的目的;还用于接受多种链路信号,并通过机器学习的方法对于设定的特征进行提取和分析,并将其与储存在白名单上的数据进行对比,得出粗略的结果,以达到设备基础数据预读取的目的;

[0022] 其具体功能实现过程如下:

[0023] 步骤1.1:检测接入设备是否符合通信标准,不为无效信息;如为判定符合标准,则确认设备的特征信息编号是否已经被安全估计单元判断为安全可接入白名单设备;

[0024] 步骤1.2:在通信接口设备对传入并读取到的设备特征信息编号赋予一个现场生成的包含有此时处于匹配状态的设备的一部分预读信息的身份编号数列,该编号数列是用于识别具体对应的设备,编号与设备具有唯一性,该编号数列的长度不超过16位;

[0025] 步骤1.3:在运行中依据RAS加密算法原理产生一个基于500位计算值以内的RAS明码和加密暗码,其加密暗码部分及上一步获得的设备身份编号数列保存在白名单中作为鉴别,明码部分用于对身份编号加密;

[0026] 步骤1.4:将上一步中加密后的对应单独设备的身份编号数列以一种数据标签的方式添加;为保证识别效率和防止被替代,加密后的身份编号将插入设备特征信息编号,作为新的设备特征信息的一部分,但并不直接单独赋予这个设备;

[0027] 步骤1.5:当设备再次申请连接时,特征信息编号中的身份编号部分被提出,对身份编号进行解码,并将解码部分与白名单库中保存的设备身份编号进行对比,确定其合法性,并读取编码中的信息段,获取其应用方向,完成第一道效验部分。

[0028] 进一步地,所述基础判别模块,引入具有KNN架构下的机器学习算法的特征信息提取单元与设备安全评估单元,所述算法的应用基础是:

[0029] (1)对于目前的大部分设备具有很好的适应性和拓展性;

[0030] (2)在同厂家生产的大部分设备为了接口的一致性,都具有基于功能性的较相似的数据排列特征;所述算法通过对接收下层设备的数据的提取分析,构建具有相关分类判断能力的训练模型;

[0031] 其具体实现过程如下:

[0032] 步骤2.1:在模型训练阶段,向基础判别模块输入作为参考和训练的数据,包括输入的数据所对应的具体类别及其安全情况;作为参考和训练的数据依据边缘网关所处的范

围区域内设备种类不同而加以调整;再通过已知的边缘网关需要的数据特征,对于训练的数据进行数字化特征提取和分析;通过提取的特征和数据集合,完成下层传输设备输入信息的分类判断;在下层传输设备输入信息之前需要通过硬件部分通信方式的认证对数据的有效性进行分析,排除非安全信息因素;

[0033] 步骤2.2:采用将数据特征分层的方式,通过数据的复杂性将下层设备传输数据的分类过程分为两层,第一层通过提取数字长度较短的特征信息,来对样本数据进行初步的分类判断,根据K-邻近算法,通过计算相同特征数据的欧式距离将数字化后的这些特征信息进行总距离计算,并选取距离最短的K个数据点,然后将此样本数据归为K个数据中出现频率最高的两到三类数据,并进入通过传输数据的具体内容进行分类;如果样本数据与训练数据在这些特征上总和的最短距离超过某一阈值L时认为其类别不在训练的白名单上,让其以新的类别形式加入白名单中;

[0034] 步骤2.3:在第一层完成了对数据类型的初步判断后,获得几个与样本可能为一类的训练数据,在第二层次的计算中通过获得的这几个训练数据中的具体传输数据和表示终端运行的状态数据来确定输入样品数据的安全等级并将驶入样品数据放入对应类型的白名单中;需要注意的是,要根据不同的传输层数据类型进行不同的划分,然后才能计算样本数据与白名单数据之间的相似度,计算完成后仍然利用上一层的K-邻近算法,算出与样品数据相似度最近的K个值,并且得出某个类别的某一级安全性在这K个值中所占的频数最大,就可以将由下层设备传输的样品数据进行归类,并进行安全评估。

[0035] 进一步地,所述同层数据关联处理单元,将多个边缘网关的处理范围进行重叠用以进行辅助判断,由一个主处理网关和一个或多个副处理网关构成,其中主处理网关负责构建多个网关之间的数据通道,并作为一个发送节点,对数据命令进行双向的传输,副边缘网关则不涉及通道构建,而只作为安全状态辅助评估;

[0036] 其具体实施步骤如下:

[0037] 步骤3.1:多个边缘网关相互连接,各自在处理所属区域内设备请求的时候,按照一定规律周期性的将一部分判断为不合格的申请数据在保留主要控制权限的基础上,分享给同层的其他边缘网关进行安全判断;

[0038] 步骤3.2:当出现异常信息判断时,将同层内多个边缘网关互相的链接作为一张矩阵网并划分区域,将边缘网关作为节点;从上层设备收集到的边缘网关反馈信息中,通过步进的方式,锁定发出警报的区域网关节点所工作的范围,进而通过类似于麦克风阵列锁定声源发出方向的计算思想,以一个警报节点作为参考,计算各个节点发出警报信息的时间差,进而锁定原始警报发出节点,并获得异常下层设备的具体型号和IP地址。

[0039] 采用上述技术方案所产生的有益效果在于:本发明提供的基于电力边缘网关设备的维护通信安全装置,相比于目前经常运用的边缘网关的数据传输方式,有以下改进效果:

[0040] (1)本发明采用特征提取方法实现具有唯一性的安全识别性质的设备特征信息编号:通过对于设备传输数据特征信息的提取,利用机器学习算法在KNN构架下对设备数据进行学习评估,并生成相关的分类模型。进而通过与白名单内已有的设备信息指纹进行对比,并用数据异常估算的方式决定是否将申请设备纳入白名单。如果为陌生设备,则要求进行安全状态估计,用以判断是否有资格进行数据通道的建立,实现了设备安全性的准确判别。同时基于这种方法,生成了具有针对性的分类模型,避免了对每个申请连接的设备都进行

全流程的安全性识别,使判断速度加快。

[0041] (2)本发明采用动态更新白名单的方式提高异常识别能力:通过将部分设备的特征信息储存在周期样本缓存单元,并周期性的将其和现有相关类型设备的数据进行对比,动态的进行白名单的更新,确保白名单设备的安全性,提高加密识别的准确率。

[0042] (3)本发明采用同层数据关联方式实现对于误判率的降低以及对于异常设备的粗定位:通过将多个边缘网关的处理范围进行交叉,实现对于同一异常设备多次单独处理判断,完善了对于异常信息的甄别,降低了基于特征训练模型参数差等问题所带来的误判风险;同时,通过范围部分重叠,在无法识别异常信号具体来源设备时,可以通过对于同层内边缘网关矩阵的异常信息反馈交叉比对,相比于传统方法下的逐个比对,可以更快速的确定异常设备所处区域。

附图说明

[0043] 图1为本发明实施例提供的基于电力边缘网关设备的维护通信安全装置各单元数据连接关系示意图;

[0044] 图2为本发明实施例提供的软件算法运行过程示意图。

具体实施方式

[0045] 下面结合附图和实施例,对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明,但不用来限制本发明的范围。

[0046] 需要说明的是,下述所提及的连接是构建数据通道产生信息交换之意,其多为算法部分,与实际模块结构无关。需要说明的是,本发明所改进功能主要由算法代码实现,其具体执行函数方便调节,故在此处只以其作用简单分类后的相关单元作为代替。

[0047] 边缘网关作为边缘计算的实际应用载体,应用广泛但也存在数据安全问题。本发明通过硬件部分和软件部分相配合的方式,在机器学习的算法与硬件加密特征编码信息的基础上,实现对于底层传感设备的唯一识别及安全评估,并安排周期性的白名单更新,达到对于整个设备数据传输过程安保的要求。并在此基础上设计了在同层次边缘网关内实现多网关矩阵式辅助安全评估的功能,达到提高判断准确率的目的。

[0048] 如图1所示,本实施例的基于电力边缘网关设备的维护通信安全装置包括硬件部分和软件部分。

[0049] 硬件部分包括加密识别单元及其通信接口设备,用于对下层设备传入的通信数据进行信息读取、白名单资格比对和预分类,与软件端口之间有数据连接;具有链路识别维护、数据加密、信息指纹比对、设备特征信息提取的功能,用于通过基础判别模块生成的单个设备的设备特征信息编号进行基于RAS加密算法的加密,并根据去加密算法的数学性质,周期性的更新加密算子,以达到对于白名单信息的物理加密的目的;还用于接受多种链路信号,并通过机器学习的方法对于设定的特征进行提取和分析,并将其与储存在白名单上的数据进行对比,得出粗略的结果,以达到设备基础数据预读取的目的。

[0050] 硬件部分具体功能实现过程如下:

[0051] 步骤1.1:检测接入设备是否符合通信标准,不为无效信息;如为判定符合标准,则确认设备的特征信息编号即设备特征信息指纹是否已经被安全估计单元判断为安全可接

入白名单设备；

[0052] 步骤1.2：在通信接口设备对传入并读取到的设备特征信息编号赋予一个现场生成的包含有此时处于匹配状态的设备的一部分预读信息的身份编号数列，该编号数列是用于识别具体对应的设备，编号与设备具有唯一性，该编号数列的长度不超过16位；

[0053] 步骤1.3：在运行中依据RAS加密算法原理产生一个基于500位计算值以内的RAS明码和加密暗码，其加密暗码部分及上一步获得的设备身份编号数列保存在白名单中作为鉴别，明码部分用于对身份编号加密；500位计算值，保证在算力有限的情况下达到安全效果，在使用中根据硬件支持提升这一数值；

[0054] 步骤1.4：将上一步中加密后的对应单独设备的身份编号数列以一种数据标签的方式添加；为保证识别效率和防止被替代，加密后的身份编号将插入设备特征信息编号，作为新的设备特征信息的一部分，但并不直接单独赋予这个设备(在该情况下当出现攻击方试图顶替该设备发送指令信息时，会生成不同的指纹而无法匹配)；

[0055] 步骤1.5：当设备再次申请连接时，特征信息编号中的身份编号部分被提出，对身份编号进行解码，并将解码部分与白名单库中保存的设备身份编号进行对比，确定其合法性，并读取编码中的信息段，获取其应用方向，完成第一道效验部分。

[0056] 软件部分包括基础判别模块、周期白名单设备检查模块、信息检测及故障判别模块。其算法运行过程如图2所示。

[0057] 基础判别模块，包括依次连接的特征信息提取单元、特征信息处理单元、设备安全估计单元和数据通道匹配单元，用于通过对于下层设备的上载请求及内容信息的特征值进行提取，并通过KNN构架下的算法构建一个具有辨识性的唯一的设备特征信息编号，并生成相对应的安全评估，依据评估结果对设备进行操作权限的赋予。

[0058] 特征信息提取单元，用于对非白名单设备的上行数据的一些基于其工作特点和设备特点的特征数据进行提取，并将提取的特征数据进行数字化以方便之后的计算运行；还用于对白名单设备进行抽样式的特征提取，用以之后进行周期性的状态检测。

[0059] 特征信息处理单元，用于将提取上来的传感器设备的特征信息进行处理学习，构建基于相关设备的运行机制的“识别指纹”，生成一个具有相关分类判断能力的训练模型，同时对相关数据的处理结果进行分类并进行比对，进行异常比对的参数在初始阶段可以通过预先设置进行设定，用以区分是否可以将此类设备放入白名单；还用于通过判断数据的连接申请命令及调度命令是否存在异常状态，给设备信息赋予安全状态；在遇到非安全状态反馈以后，通过获取同层数据关联处理单元的数据反馈后，对安全状态进行二次评估或更新；在数据量较多的情况下优先处理非白名单设备，从而达到计算能力自适应匹配的效果。

[0060] 设备安全估计单元，在一般数据通过处理判断后，如果在白名单内，且判断为安全状态，则只需通过简单的命令匹配后，进入边缘网关的核心处理模块进行数据的处理运算。如果被判断为非安全状态，则连接同层数据关联处理单元将信息返回多个设备的信息处理和安全估计单元进行联合判比之后，将结果反馈至数据通道匹配单元进行处理。

[0061] 数据通道匹配单元，根据设备安全估计单元将设备特征信息处理结束以后反馈的处理结果，对设备数据分类赋予权限，权限包括只允许设备信息上行、只允许设备信息下行、同时允许设备数据双向传递和暂时断开设备连接。

[0062] 基础判别模块引入具有KNN架构下的机器学习算法的特征信息提取单元与设备安全评估单元，所述算法的应用基础是：

[0063] (1)对于目前的大部分设备具有很好的适应性和拓展性；

[0064] (2)在同厂家生产的大部分设备为了接口的一致性，都具有基于功能性的较相似的数据排列特征；所述算法通过对接收下层设备的数据的提取分析，可以构建具有相关分类判断能力的训练模型。

[0065] 基础判别模块具体实现过程如下：

[0066] 步骤2.1：在模型训练阶段，向基础判别模块输入作为参考和训练的数据，包括输入的数据所对应的具体类别及其安全情况；作为参考和训练的数据依据边缘网关所处的范围区域内设备种类不同而加以调整；再通过已知的边缘网关需要的数据特征，对于训练的数据进行数字化特征提取和分析；边缘网关需要提取的特征主要为链路数据，数据长度，发送频率及其发送端所处的IP地址及电网的状态传输信息等，通过提取的特征和数据集合，完成下层传输设备输入信息的分类判断；在下层传输设备输入信息之前需要通过硬件部分通信方式的认证对数据的有效性进行分析，排除非安全信息因素；

[0067] 步骤2.2：考虑到这些信息的类别较多且特征相对复杂，直接采用机器学习的方法会导致电力边缘网关设备学习和计算分类的速度缓慢。所以本发明采用将数据特征分层的方式，通过数据的复杂性将下层设备传输数据的分类过程分为两层，第一层通过提取链路数据、发送频率、IP地址等数字长度较短的特征信息，来对样本数据进行一个初步的分类判断，根据K-邻近算法，通过计算相同特征数据的欧式距离将数字化后的这些特征信息进行总距离计算，并选取距离最短的K个数据点，然后将此样本数据归为K个数据中出现频率最高的两到三类数据，并进入通过传输数据的具体内容进行分类。但如果样本数据与训练数据在这些特征上总和的最短距离超过某一阈值L时就可以认为其类别不在训练的白名单上，就可以让其以新的类别的形式加入白名单中，以此来增加边缘网关的识别数据类型的自适应度；

[0068] 步骤2.3：在第一层完成了对数据类型的初步判断后，获得几个与样本可能为一类的训练数据，在第二层次的计算中通过获得的这几个训练数据中的具体传输数据和表示终端运行的状态数据，比如电网的运行的频率、电压变化等，来确定输入样品数据的安全等级并将输入样品数据放入对应类型的白名单中。因为在第二层计算中电力边缘网关只需从几个训练数据的白名单中选出一个结果即可，不需要对全部的白名单类型进行计算，节约了边缘网关所需要的计算量。因为具体的传输数据的大小和数据量可能会很大，也有可能一次性传输了多种测量结果的数据比如电压、电流、幅值等随时间变化的情况等。所以要根据不同的传输层数据类型进行不同的划分，然后才能计算样本数据与白名单数据之间的相似度，计算完成后仍然利用上一层的K-邻近算法，算出与样品数据相似度最近的K个值，并且得出某个类别的某一级安全性在这K个值中所占的频数最大，就可以将由下层设备传输的样品数据进行归类，并进行安全评估。

[0069] 周期白名单设备检查模块，是提高防护效率的辅助单元，包括与设备安全估计单元连接的周期样本缓存单元，用于通过设置人为时间作为阈值或通过白名单增长的数量作为阈值，来进行对于已经判别为安全的白名单设备进行周期性二次安全风险评估，可以防止一些在白名单内的设备在运行期间出现问题而无法发现；

[0070] 具体对应周期样本缓存单元使用，用于对硬件模块反馈的活跃性比较高的设备类型，以及部分新加入白名单的设备的特征值处理结果进行储存；并以一定周期或白名单设备增长数量作为触发阈值，不定向的从特征信息处理单元中抽取并保存已在白名单中的各类型设备的信息特征，并在之后的运行中按照一定周期频率与该类型设备的新进数据进行比对，确保其传输通道稳定或按照一定规律变化，如不满足该条件，则重新审查其白名单资格；同时检查存储部分是否存在重复存储现象。通过以上操作，达到更新白名单的目的。

[0071] 周期白名单设备检查模块运行的过程是：

[0072] 步骤4.1：通过人为设置一定周期或白名单设备增长数目(确保不会一次性处理太多数据)作为阈值，将部分特征信息处理单元处理分类设置为白名单的设备的结果以及其在特征提取阶段的特征值保存在周期样本缓存单元，记录其对应的特征结果。

[0073] 步骤4.2：按照一定周期或白名单设备增长数目作为阈值，通过将白名单设备的存储数据与其先行数据申请重新在设备安全估计单元进行对比，判断其是否出现异常的数据形式或连接方式出现较大变化，完成对于白名单设备的周期性检查与更新。

[0074] 信息检测及故障判别模块，包括与设备安全估计单元连接的同层数据关联处理单元，主要通过连接同层多个设备，通过对于多个网关交叉处理的结果进行加权评估，实现对于误判率的降低。用于在设备安全估计单元判定为非安全设备的数量到达一定阈值或处理优先级到达阈值时，通过将数据完整打包发送给其他同层状态下的边缘网关进行辅助判断，即少数服从多数的概率判断，避免因单个网关收到的区域设备类型单一导致的算法训练过拟合，同时产生判断误差。

[0075] 同层数据关联处理单元，将多个边缘网关的处理范围进行重叠用以进行辅助判断，由一个主处理网关和一个或多个副处理网关构成，其中主处理网关负责构建多个网关之间的数据通道，并作为一个发送节点，对数据命令进行双向的传输，副边缘网关则不涉及通道构建，而只作为安全状态辅助评估；其优点有：

[0076] (1)基于KNN所训练出来的模型，可能会由于处理数据具有一定的偏向性导致训练出来的模型在固定类型数据的条件下能达到完美的效果，但在处理一些个别数据的时候出现误判。同层数据关联单元可以通过交叉处理辅助判断的方式，减小这种误判情况的发生；进一步的，可以通过相互关联数据的判断，保持对于白名单的周期性更新时的正确率。

[0077] (2)在突然遇到紧急信号或者异常信号时，可以通过多边缘网关组成的二维阵列网络，通过对于不同区域内边缘网关交叉部分的预警情况比对，快速确定故障设备所处范围。

[0078] 信息检测及故障判别模块具体实施步骤如下：

[0079] 步骤3.1：多个边缘网关相互连接，各自在处理所属区域内设备请求的时候，按照一定规律周期性的将一部分判断为不合格的申请数据在保留主要控制权限的基础上，分享给同层的其他边缘网关进行安全判断；其得到的效果是，面对同一设备的申请和数据，可能有多个边缘网关在进行相互独立的识别判断，通过加权的方式生成一个总的处理结果，二次判断其是否为异常信息，并将其反馈回数据通道匹配单元；

[0080] 步骤3.2：当出现异常信息判断时，将同层内多个边缘网关互相的链接作为一张矩阵网并划分区域，将边缘网关作为节点；从上层设备收集到的边缘网关反馈信息中，通过步进的方式，锁定发出警报的区域网关节点所工作的范围，进而通过类似于麦克风阵列锁定

声源发出方向的计算思想，以一个警报节点作为参考，计算各个节点发出警报信息的时间差，进而锁定原始警报发出节点，并获得异常下层设备的具体型号和IP地址。该方法代替了传统的数据比对寻找一场节点的做法，极大的加快了锁定时间。

[0081] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述实施例所记载的技术方案进行修改，或者对其中部分或者全部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发明权利要求所限定的范围。

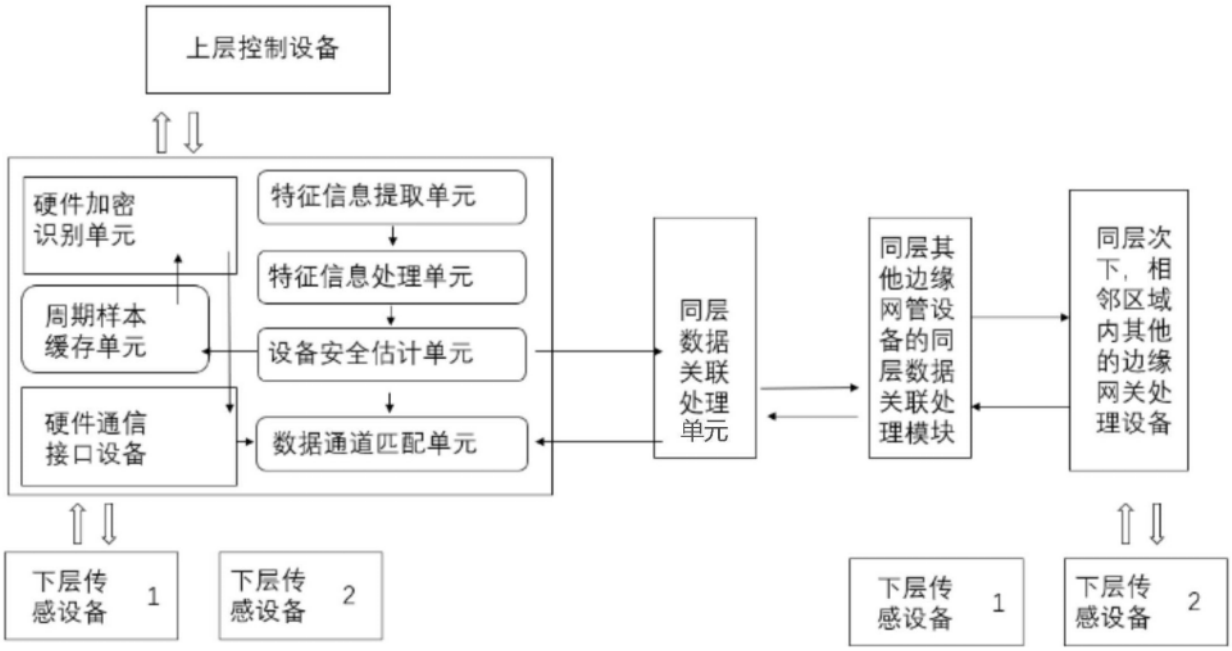

上层控制设备
硬件加密识别单元
特征信息提取单元
特征信息处理单元
周期样本缓存单元
设备安全估计单元
硬件通信接口设备
数据通道匹配单元
同层数据关联处理单元
同层其他边缘网管设备的同层数据关联处理模块
同层次下，相邻区域内其他的边缘网关处理设备
下层传感设备 1
下层传感设备 2
下层传感设备 1
下层传感设备 2

图1

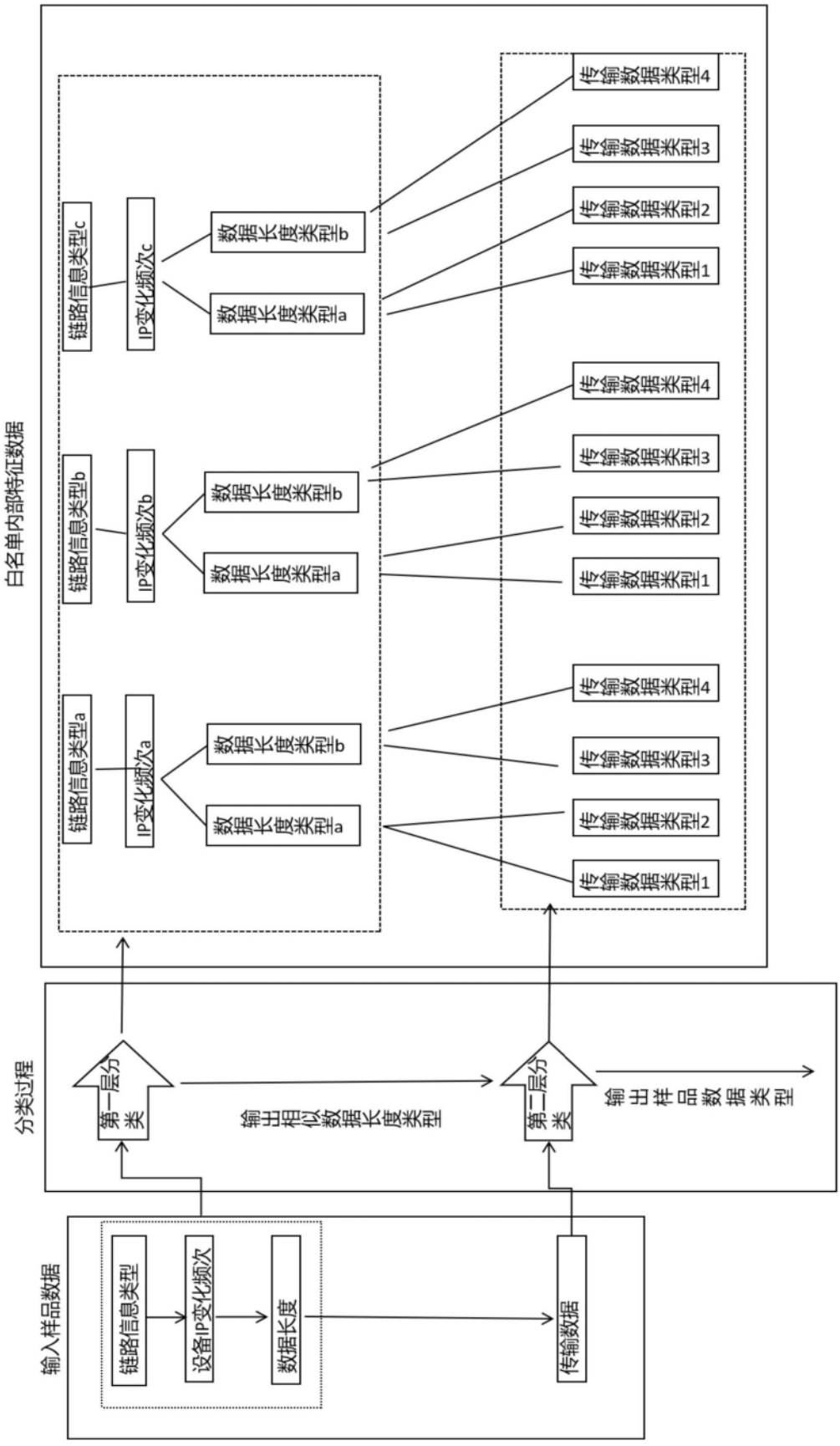

输入样品数据
链路信息类型
设备IP变化频次
数据长度
传输数据
分类过程
第一层分类
输出相似数据长度类型
第二层分类
输出样品数据类型
白名单内部特征数据
链路信息类型a
链路信息类型b
链路信息类型c
IP变化频次a
IP变化频次b
IP变化频次c
数据长度类型a
数据长度类型b
传输数据类型1
传输数据类型2
传输数据类型3
传输数据类型4

图2