(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118170662 A
(43)申请公布日 2024.06.11

(21)申请号 202410329348.9

(22)申请日 2024.03.21

(71)申请人 贵州电网有限责任公司信息中心
地址 550003 贵州省贵阳市瑞金南路38号贵州电网信息中心
申请人 南方电网科学研究院有限责任公司

(72)发明人 陶佳冶 梁志宏 付鋆 洪超 班秋成 杨祎巍 魏力鹏 李攀登 周泽元 张宇南 刘俊荣 蒋屹新 严彬元 徐文倩 张猛

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
专利代理师 霍文娟

(51)Int.Cl.
G06F 11/36(2006.01)
G06N 3/0464(2023.01)
G06N 3/08(2023.01)

权利要求书4页 说明书21页 附图3页

(54)发明名称

电力协议的模糊测试方法、装置和电力协议测试系统

(57)摘要

本申请提供了一种电力协议的模糊测试方法、装置和电力协议测试系统,该方法包括:对目标电力协议和目标系统进行梳理得到第一目标数据,根据第一目标数据确定状态迁移图;获取第一数据集,对第一数据集进行标记得到第二数据集,根据第二数据集确定第一目标神经网络;将第二数据集输入第一目标神经网络得到第三数据集并对第三数据集进行处理得到第四数据集;将第四数据集分为第五数据集和第六数据集,根据第五数据集对神经网络进行训练并根据第六数据集进行测试得到第二目标神经网络;根据第四数据集确定目标模糊测试集,根据目标模糊测试集对目标系统进行模糊测试。该方法解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。

CN 118170662 A

1.一种电力协议的模糊测试方法,其特征在于,包括:

对目标电力协议和目标系统进行梳理得到第一目标数据,根据所述第一目标数据确定状态迁移图,所述目标系统为所述目标电力协议部署的电力系统,所述第一目标数据至少包括所述目标电力协议的类型、格式和结构以及在所述目标系统的运行原理,所述状态迁移图用于表征所述目标系统的系统状态之间的转移关系;

监测所述目标系统的运行数据得到第一数据集,对所述第一数据集进行标记得到第二数据集,根据所述第二数据集确定至少一个第一目标神经网络,不同所述第一目标神经网络用于提取不同类型的特征数据;

将所述第二数据集输入所述第一目标神经网络得到第三数据集并对所述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集;

将所述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据所述第五数据集对神经网络进行训练并根据所述第六数据集进行测试,在所述神经网络的损失函数小于阈值的情况下将所述神经网络确定为第二目标神经网络,所述神经网络用于基于所述目标系统的运行数据生成模糊测试集;

将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集,根据所述目标模糊测试集对所述目标系统进行模糊测试,根据所述目标系统的响应确定模糊测试结果,所述模糊测试结果包括所述目标系统的异常状态和异常行为。

2.根据权利要求1所述的方法,其特征在于,对所述目标电力协议和所述目标系统进行梳理得到第一目标数据,包括:

对所述目标系统进行分析,确定所述目标电力协议的协议类型,所述协议类型包括DNP3、Modbus和IEC 61850中的一个或多个;

对所述目标电力协议进行分析,确定所述目标电力协议的协议作用,所述协议作用至少包括监测所述目标系统中电力设备状态、执行控制命令和传输告警信息中的一个或多个;

对所述目标电力协议进行分析,确定所述目标电力协议的格式信息,所述格式信息包括消息头、消息体和校验和中的至少一个;

对所述目标电力协议进行分析,确定所述目标电力协议的消息内容,所述消息内容包括设备标识符、命令类型、控制参数和设备地址中的至少一个;

对所述目标电力协议进行分析,确定所述目标电力协议的安全机制,所述安全机制包括加密通信、身份验证和完整性验证中的至少一个;

对所述目标电力协议进行分析,确定所述目标电力协议的风险类型,所述风险类型包括中间人攻击和数据注入中的至少一个;

根据所述协议类型、所述协议作用、所述格式信息、所述消息内容、所述安全机制和所述风险类型构建所述第一目标数据。

3.根据权利要求1所述的方法,其特征在于,根据所述第一目标数据确定状态迁移图,包括:

将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备允许进行数据发送和接收,且允许对所述目标系统进行监控操作和控制操作的状态确定为连接建立状态;

将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备周期性进行所述

监控操作并发送监控数据或周期性接收其他设备的指令并执行所述控制操作的状态确定为正常监控状态；

将所述目标系统在所述目标电力协议控制下，所述目标系统中的设备产生报警信息并执行安全措施的状态确定为异常告警状态；

将所述目标系统在所述目标电力协议控制下，所述目标系统中的设备不允许发送数据的状态确定为断开连接状态；

基于所述第一目标数据确定所述目标系统处于所述连接建立状态、所述正常监控状态、所述异常告警状态或所述断开连接状态的情况下，分别对应的可以触发的目标事件，并根据对应的所述目标事件确定触发后的所述目标系统的所述系统状态，绘制所述状态迁移图。

4.根据权利要求3所述的方法，其特征在于，监测所述目标系统的运行数据得到第一数据集，对所述第一数据集进行标记得到第二数据集，包括：

监测所述目标系统处于所述正常监控状态下的Modbus通信数据得到第一运行数据；

监测所述目标系统中的设备之间的查询数据、响应数据和所述监控数据得到第二运行数据；

监测所述目标系统中的设备的异常输入数据得到第三运行数据；

监测所述目标系统中的设备的异常响应数据得到第四运行数据；

根据所述第一运行数据、所述第二运行数据、所述第三运行数据和所述第四运行数据构建所述第一数据集，对所述第一数据集中所述第一运行数据和所述第二运行数据添加第一标识信息，对所述第三运行数据和所述第四运行数据添加第二标识信息得到所述第二数据集，所述第一标识信息用于表征数据为正常数据，所述第二标识信息用于表征数据为异常数据。

5.根据权利要求1所述的方法，其特征在于，根据所述第二数据集确定至少一个第一目标神经网络，包括：

在所述第二数据集中包括消息序列的情况下，确定所述第一目标神经网络为循环神经网络和卷积神经网络，所述循环神经网络用于提取所述第二数据集中的数据的时序特征，所述卷积神经网络用于提取所述第二数据集中的数据的结构信息；

在所述第二数据集中不包括所述消息序列的情况下，确定所述第一目标神经网络为所述卷积神经网络。

6.根据权利要求5所述的方法，其特征在于，将所述第二数据集输入所述第一目标神经网络得到第三数据集，并对所述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集，包括：

在所述第一目标神经网络为所述卷积神经网络的情况下，提取所述第二数据集中数据的数据结构特征，所述数据结构特征包括消息头、功能码、寄存器地址和内容数据对应的数值或编码表示；

提取所述第二数据集中数据的数据长度特征，所述数据长度特征包括不同类型数据的长度；

提取所述第二数据集中数据的预设匹配特征，所述预设匹配特征包括与所述卷积神经网络中预设关键字匹配的文本转换得到的数值或编码表示；

在所述第一目标神经网络为所述循环神经网络的情况下,提取所述第二数据集中数据的数据时序特征,所述数据时序特征包括所述第二数据集中各数据的顺序关系;

根据所述数据结构特征、所述数据长度特征、所述预设匹配特征和所述数据时序特征构建所述第三数据集;

将所述第三数据集中类别型数据转换为数值型数据、将所述第三数据集中数据按照所述数据时序特征构建消息序列、将所述第三数据集中的数值型数据进行归一化映射到预设数值范围、对所述第三数据集中的数值型数据进行数据填充得到第七数据集,将所述第五数据集转换为向量组合形式进行表示得到第八数据集;

根据所述第七数据集和所述第八数据集构建所述第四数据集。

7.根据权利要求6所述的方法,其特征在于,将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集,包括:

在所述第四数据集的数据中引入随机噪声;和/或

对所述第四数据集的数据进行随机变更;和/或

根据第一预设字段对所述第四数据集的数据中第二预设字段进行替换;和/或

根据所述第四数据集的数据对应的数据类型在所述第四数据集中添加对应不同数据类型的边界数值型数据;和/或

根据所述第四数据集的数据对应的数据类型在所述第四数据集中添加对应不同数据类型的错误数据;和/或

变更所述第四数据集中的所述消息序列的时序进行变更,得到所述目标模糊测试集。

8.一种电力协议的模糊测试装置,其特征在于,所述装置包括:

第一获取单元,用于对目标电力协议和目标系统进行梳理得到第一目标数据,根据所述第一目标数据确定状态迁移图,所述目标系统为所述目标电力协议部署的电力系统,所述第一目标数据至少包括所述目标电力协议的类型、格式和结构以及在所述目标系统的运行原理,所述状态迁移图用于表征所述目标系统的系统状态之间的转移关系;

第二获取单元,用于监测所述目标系统的运行数据得到第一数据集,对所述第一数据集进行标记得到第二数据集,根据所述第二数据集确定至少一个第一目标神经网络,不同所述第一目标神经网络用于提取不同类型的特征数据;

第一输入单元,用于将所述第二数据集输入所述第一目标神经网络得到第三数据集并对所述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集;

训练单元,用于将所述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据所述第五数据集对神经网络进行训练并根据所述第六数据集进行测试,在所述神经网络的损失函数小于阈值的情况下将所述神经网络确定为第二目标神经网络,所述神经网络用于基于所述目标系统的运行数据生成模糊测试集;

第二输入单元,用于将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集,根据所述目标模糊测试集对所述目标系统进行模糊测试,根据所述目标系统的响应确定模糊测试结果,所述模糊测试结果包括所述目标系统的异常状态和异常行为。

9.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质包括存储的程序,其中,在所述程序运行时控制所述计算机可读存储介质所在设备执行权利要求1至7中任意一项所述的方法。

10.一种电力协议测试系统,其特征在于,包括:一个或多个处理器,存储器,以及一个或多个程序,其中,所述一个或多个程序被存储在所述存储器中,并且被配置为由所述一个或多个处理器执行,所述一个或多个程序包括用于执行权利要求1至7中任意一项所述的方法。

电力协议的模糊测试方法、装置和电力协议测试系统

技术领域

[0001]　本发明涉及工业控制系统技术领域,具体而言,涉及一种电力协议的模糊测试方法、装置、计算机可读存储介质和电力协议测试系统。

背景技术

[0002]　工业控制系统中的电力协议是指用于监控、管理和控制电力系统的通信协议。电力系统是一个庞大而复杂的系统,包括电力生产、传输和分配等多个环节。为了实现对电力系统各个组件的监测和控制,需要使用特定的通信协议来确保设备之间能够有效地交换信息。然而,随着网络技术的不断发展,电力系统也面临着新的安全挑战,例如网络攻击、恶意软件等。

[0003]　目前,电力系统中常用的电力协议有IEC61850、Modbus、DNP3等等,这些协议或多或少存在着一些漏洞,例如缓冲区溢出、未经身份验证的访问、明文通信、协议解析问题等等。这些漏洞可能会被黑客或攻击者利用,从而导致电力系统的安全风险。

[0004]　因此,对电力协议进行安全评估和对电力的监控就变得至关重要,以确保电力系统的稳健性,防范潜在的威胁。在这方面,安全专业人员必须采用一些手段,定期审查和更新协议,以适应不断演变的网络安全威胁。在现有协议测试方法中,对电力协议的评估多依赖于专业人员的经验进行。

发明内容

[0005]　本申请的主要目的在于提供一种电力协议的模糊测试方法、装置、计算机可读存储介质和电力协议测试系统,以至少解决现有技术中需要人工进行电力协议分析,准确性较低的问题。

[0006]　为了实现上述目的,根据本申请的一个方面,提供了一种电力协议的模糊测试方法,包括:对目标电力协议和目标系统进行梳理得到第一目标数据,根据所述第一目标数据确定状态迁移图,所述目标系统为所述目标电力协议部署的电力系统,所述第一目标数据至少包括所述目标电力协议的类型、格式和结构以及在所述目标系统的运行原理,所述状态迁移图用于表征所述目标系统的系统状态之间的转移关系;监测所述目标系统的运行数据得到第一数据集,对所述第一数据集进行标记得到第二数据集,根据所述第二数据集确定至少一个第一目标神经网络,不同所述第一目标神经网络用于提取不同类型的特征数据;将所述第二数据集输入所述第一目标神经网络得到第三数据集并对所述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集;将所述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据所述第五数据集对神经网络进行训练并根据所述第六数据集进行测试,在所述神经网络的损失函数小于阈值的情况下将所述神经网络确定为第二目标神经网络,所述神经网络用于基于所述目标系统的运行数据生成模糊测试集;将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集,根据所述目标模糊测试集对所述目标系统进行模糊测试,根据所述目标系统的响应确定模糊测试

结果,所述模糊测试结果包括所述目标系统的异常状态和异常行为。

[0007] 可选地,对所述目标电力协议和所述目标系统进行梳理得到第一目标数据,包括:对所述目标系统进行分析,确定所述目标电力协议的协议类型,所述协议类型包括DNP3、Modbus和IEC 61850中的一个或多个;对所述目标电力协议进行分析,确定所述目标电力协议的协议作用,所述协议作用至少包括监测所述目标系统中电力设备状态、执行控制命令和传输告警信息中的一个或多个;对所述目标电力协议进行分析,确定所述目标电力协议的格式信息,所述格式信息包括消息头、消息体和校验和中的至少一个;对所述目标电力协议进行分析,确定所述目标电力协议的消息内容,所述消息内容包括设备标识符、命令类型、控制参数和设备地址中的至少一个;对所述目标电力协议进行分析,确定所述目标电力协议的安全机制,所述安全机制包括加密通信、身份验证和完整性验证中的至少一个;对所述目标电力协议进行分析,确定所述目标电力协议的风险类型,所述风险类型包括中间人攻击和数据注入中的至少一个;根据所述协议类型、所述协议作用、所述格式信息、所述消息内容、所述安全机制和所述风险类型构建所述第一目标数据。

[0008] 可选地,根据所述第一目标数据确定状态迁移图,包括:将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备允许进行数据发送和接收,且允许对所述目标系统进行监控操作和控制操作的状态确定为连接建立状态;将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备周期性进行所述监控操作并发送监控数据或周期性接收其他设备的指令并执行所述控制操作的状态确定为正常监控状态;将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备产生报警信息并执行安全措施的状态确定为异常告警状态;将所述目标系统在所述目标电力协议控制下,所述目标系统中的设备不允许发送数据的状态确定为断开连接状态;基于所述第一目标数据确定所述目标系统处于所述连接建立状态、所述正常监控状态、所述异常告警状态或所述断开连接状态的情况下,分别对应的可以触发的目标事件,并根据对应的所述目标事件确定触发后的所述目标系统的所述系统状态,绘制所述状态迁移图。

[0009] 可选地,监测所述目标系统的运行数据得到第一数据集,对所述第一数据集进行标记得到第二数据集,包括:监测所述目标系统处于所述正常监控状态下的Modbus通信数据得到第一运行数据;监测所述目标系统中的设备之间的查询数据、响应数据和所述监控数据得到第二运行数据;监测所述目标系统中的设备的异常输入数据得到第三运行数据;监测所述目标系统中的设备的异常响应数据得到第四运行数据;根据所述第一运行数据、所述第二运行数据、所述第三运行数据和所述第四运行数据构建所述第一数据集,对所述第一数据集中所述第一运行数据和所述第二运行数据添加第一标识信息,对所述第三运行数据和所述第四运行数据添加第二标识信息得到所述第二数据集,所述第一标识信息用于表征数据为正常数据,所述第二标识信息用于表征数据为异常数据。

[0010] 可选地,根据所述第二数据集确定至少一个第一目标神经网络,包括:在所述第二数据集中包括消息序列的情况下,确定所述第一目标神经网络为循环神经网络和卷积神经网络,所述循环神经网络用于提取所述第二数据集中的数据的时序特征,所述卷积神经网络用于提取所述第二数据集中的数据的结构信息;在所述第二数据集中不包括所述消息序列的情况下,确定所述第一目标神经网络为所述卷积神经网络。

[0011] 可选地,将所述第二数据集输入所述第一目标神经网络得到第三数据集,并对所

述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集，包括：在所述第一目标神经网络为所述卷积神经网络的情况下，提取所述第二数据集中数据的数据结构特征，所述数据结构特征包括消息头、功能码、寄存器地址和内容数据对应的数值或编码表示；提取所述第二数据集中数据的数据长度特征，所述数据长度特征包括不同类型数据的长度；提取所述第二数据集中数据的预设匹配特征，所述预设匹配特征包括与所述卷积神经网络中预设关键字匹配的文本转换得到的数值或编码表示；在所述第一目标神经网络为所述循环神经网络的情况下，提取所述第二数据集中数据的数据时序特征，所述数据时序特征包括所述第二数据集中各数据的顺序关系；根据所述数据结构特征、所述数据长度特征、所述预设匹配特征和所述数据时序特征构建所述第三数据集；将所述第三数据集中类别型数据转换为数值型数据、将所述第三数据集中数据按照所述数据时序特征构建消息序列、将所述第三数据集中的数值型数据进行归一化映射到预设数值范围、对所述第三数据集中的数值型数据进行数据填充得到第七数据集，将所述第五数据集转换为向量组合形式进行表示得到第八数据集；根据所述第七数据集和所述第八数据集构建所述第四数据集。

[0012] 可选地，将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集，包括：在所述第四数据集的数据中引入随机噪声；和/或对所述第四数据集的数据进行随机变更；和/或根据第一预设字段对所述第四数据集的数据中第二预设字段进行替换；和/或根据所述第四数据集的数据对应的数据类型在所述第四数据集中添加对应不同数据类型的边界数值型数据；和/或根据所述第四数据集的数据对应的数据类型在所述第四数据集中添加对应不同数据类型的错误数据；和/或变更所述第四数据集中的所述消息序列的时序进行变更，得到所述目标模糊测试集。

[0013] 根据本申请的另一方面，提供了一种电力协议的模糊测试装置，所述装置包括：第一获取单元，用于对目标电力协议和目标系统进行梳理得到第一目标数据，根据所述第一目标数据确定状态迁移图，所述目标系统为所述目标电力协议部署的电力系统，所述第一目标数据至少包括所述目标电力协议的类型、格式和结构以及在所述目标系统的运行原理，所述状态迁移图用于表征所述目标系统的系统状态之间的转移关系；第二获取单元，用于监测所述目标系统的运行数据得到第一数据集，对所述第一数据集进行标记得到第二数据集，根据所述第二数据集确定至少一个第一目标神经网络，不同所述第一目标神经网络用于提取不同类型的特征数据；第一输入单元，用于将所述第二数据集输入所述第一目标神经网络得到第三数据集并对所述第三数据集进行处理将所述第三数据集中的数据转换为预设格式得到第四数据集；训练单元，用于将所述第四数据集分为训练集和测试集得到第五数据集和第六数据集，根据所述第五数据集对神经网络进行训练并根据所述第六数据集进行测试，在所述神经网络的损失函数小于阈值的情况下将所述神经网络确定为第二目标神经网络，所述神经网络用于基于所述目标系统的运行数据生成模糊测试集；第二输入单元，用于将所述第四数据集输入所述第二目标神经网络得到目标模糊测试集，根据所述目标模糊测试集对所述目标系统进行模糊测试，根据所述目标系统的响应确定模糊测试结果，所述模糊测试结果包括所述目标系统的异常状态和异常行为。

[0014] 根据本申请的再一方面，提供了一种计算机可读存储介质，所述计算机可读存储介质包括存储的程序，其中，在所述程序运行时控制所述计算机可读存储介质所在设备执

行任意一种所述的方法。

[0015] 根据本申请的又一方面,提供了一种电力协议测试系统,包括:一个或多个处理器,存储器,以及一个或多个程序,其中,所述一个或多个程序被存储在所述存储器中,并且被配置为由所述一个或多个处理器执行,所述一个或多个程序包括用于执行任意一种所述的方法。

[0016] 应用本申请的技术方案,在上述电力协议的模糊测试方法中,首先,对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;然后,监测上述目标系统的运行数据得到第一数据集,对上述第一数据集进行标记得到第二数据集,根据上述第二数据集确定至少一个第一目标神经网络,不同上述第一目标神经网络用于提取不同类型的特征数据;之后,将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集;之后,将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试,在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络,上述神经网络用于基于上述目标系统的运行数据生成模糊测试集;最后,将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集,根据上述目标模糊测试集对上述目标系统进行模糊测试,根据上述目标系统的响应确定模糊测试结果,上述模糊测试结果包括上述目标系统的异常状态和异常行为。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。

附图说明

[0017] 图1示出了根据本申请的实施例中提供的一种电力协议的模糊测试方法的移动终端的硬件结构框图;

[0018] 图2示出了根据本申请的实施例提供的一种电力协议的模糊测试方法的流程示意图;

[0019] 图3示出了根据本申请的实施例提供的一种电力协议的模糊测试方法装置的结构框图。

[0020] 其中,上述附图包括以下附图标记:

[0021] 102、处理器;104、存储器;106、传输设备;108、输入输出设备。

具体实施方式

[0022] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0023] 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,所描述的实施例仅仅是本申请一部分的实施例,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,都应当属于本申请保护的范围。

[0024] 需要说明的是,本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”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。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。

[0025] 正如背景技术中所介绍的,现有技术中现有协议测试方法中,对电力协议的评估多依赖于专业人员的经验进行,为解决现有技术中需要人工进行电力协议分析,准确性较低的问题,本申请的实施例提供了一种电力协议的模糊测试方法、装置、计算机可读存储介质和电力协议测试系统。

[0026] 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。

[0027] 本申请实施例中所提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。以运行在移动终端上为例,图1是本发明实施例的一种电力协议的模糊测试方法的移动终端的硬件结构框图。如图1所示,移动终端可以包括一个或多个(图1中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)和用于存储数据的存储器104,其中,上述移动终端还可以包括用于通信功能的传输设备106以及输入输出设备108。本领域普通技术人员可以理解,图1所示的结构仅为示意,其并不对上述移动终端的结构造成限定。例如,移动终端还可包括比图1中所示更多或者更少的组件,或者具有与图1所示不同的配置。

[0028] 存储器104可用于存储计算机程序,例如,应用软件的软件程序以及模块,如本发明实施例中的设备信息的显示方法对应的计算机程序,处理器102通过运行存储在存储器104内的计算机程序,从而执行各种功能应用以及数据处理,即实现上述的方法。存储器104可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器104可进一步包括相对于处理器102远程设置的存储器,这些远程存储器可以通过网络连接至移动终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。传输设备106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括移动终端的通信供应商提供的无线网络。在一个实例中,传输设备106包括一个网络适配器(Network Interface Controller,简称为NIC),其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中,传输设备106可以为射频(Radio Frequency,简称为RF)模块,其用于通过无线方式与互联网

进行通讯。

[0029] 在本实施例中提供了一种运行于移动终端、计算机终端或者类似的运算装置的电力协议的模糊测试方法,需要说明的是,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0030] 图2是根据本申请实施例的电力协议的模糊测试方法的流程图。如图2所示,该方法包括以下步骤:

[0031] 步骤S201,对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;

[0032] 具体地,根据计划进行测试的电力协议进行分析,得到电力协议在相关系统的基本工作原理,得到上述第一目标数据,进而根究工作原理,确定电力协议的状态迁移图,用于表征各种可能的状态与状态之间的转移。

[0033] 步骤S202,监测上述目标系统的运行数据得到第一数据集,对上述第一数据集进行标记得到第二数据集,根据上述第二数据集确定至少一个第一目标神经网络,不同上述第一目标神经网络用于提取不同类型的特征数据;

[0034] 具体地,收集相关系统中与电力协议相关的数据,包括有效的协议消息和一场输入得到上述第一数据集。进而对第一数据集中的数据进行标记,区分为正常数据和异常数据,以便于神经网络进行学习,提取相关特征,得到上述第二数据集。根据相关协议消息中的有用特征选择合适的神经网络模型得到上述第一目标神经网络。

[0035] 步骤S203,将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集;

[0036] 具体地,将上述第二数据集输入上述第一目标神经网络进行特征提取得到特征数据集集,即上述第三数据集。进而对上述第三数据集进行数据处理将第三数据集中的数据转换为适合神经网络进行处理的数据格式得到上述第四数据集。

[0037] 步骤S204,将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试,在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络,上述神经网络用于基于上述目标系统的运行数据生成模糊测试集;

[0038] 具体地,对上述第四数据集进行划分,得到训练集和测试集,即上述第五数据集和上述第六数据集。进而根据训练集对模型进行训练,根据测试集评估模型的性能。在上述神经网络的损失函数小于阈值的情况下确定模型的性能满足要求,将之确定为第二目标神经网络。

[0039] 步骤S205,将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集,根据上述目标模糊测试集对上述目标系统进行模糊测试,根据上述目标系统的响应确定模糊测试结果,上述模糊测试结果包括上述目标系统的异常状态和异常行为。

[0040] 具体地,将格式转换之后的特征数据集,输入上述第二目标神经网络,生成模糊测试集,进而基于模糊测试集对电力系统进行模糊测试,监控系统的响应,收集系统的异常行

为和错误状态,根据测试结果确定电力协议的漏洞和风险。

[0041] 通过本实施例,首先,对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;然后,监测上述目标系统的运行数据得到第一数据集,对上述第一数据集进行标记得到第二数据集,根据上述第二数据集确定至少一个第一目标神经网络,不同上述第一目标神经网络用于提取不同类型的特征数据;之后,将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集;之后,将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试,在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络,上述神经网络用于基于上述目标系统的运行数据生成模糊测试集;最后,将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集,根据上述目标模糊测试集对上述目标系统进行模糊测试,根据上述目标系统的响应确定模糊测试结果,上述模糊测试结果包括上述目标系统的异常状态和异常行为。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。

[0042] 为了得到上述第一目标数据,在一种可选的实施方式中,上述步骤S201包括:

[0043] 步骤S20101,对上述目标系统进行分析,确定上述目标电力协议的协议类型,上述协议类型包括DNP3、Modbus和IEC 61850中的一个或多个;

[0044] 具体地,对电力协议进行梳理包括:确定电力系统通信协议的类型,包括DNP3、Modbus、IEC 61850等。

[0045] 步骤S20102,对上述目标电力协议进行分析,确定上述目标电力协议的协议作用,上述协议作用至少包括监测上述目标系统中电力设备状态、执行控制命令和传输告警信息中的一个或多个;

[0046] 具体地,对电力协议进行梳理包括:确定该电力协议配置于电力系统的主要目的,包括实时监测电力设备状态,执行控制命令,传递告警信息等。

[0047] 步骤S20103,对上述目标电力协议进行分析,确定上述目标电力协议的格式信息,上述格式信息包括消息头、消息体和校验和中的至少一个;

[0048] 具体地,对电力协议进行梳理包括:确定电力协议中消息的格式、字段、结构,包括消息体、消息头和校验码等。

[0049] 步骤S20104,对上述目标电力协议进行分析,确定上述目标电力协议的消息内容,

上述消息内容包括设备标识符、命令类型、控制参数和设备地址中的至少一个；
[0050] 具体地，对电力协议进行梳理包括：确定在该电力协议中设备之间消息包含的内容，例如设备标识符、命令类型、参数、设备地址等。
[0051] 步骤S20105，对上述目标电力协议进行分析，确定上述目标电力协议的安全机制，上述安全机制包括加密通信、身份验证和完整性验证中的至少一个；
[0052] 具体地，对电力协议进行梳理包括：确定电力协议中使用的安全机制，包括加密、身份验证、和完整性验证等。
[0053] 步骤S20106，对上述目标电力协议进行分析，确定上述目标电力协议的风险类型，上述风险类型包括中间人攻击和数据注入中的至少一个；
[0054] 具体地，对电力协议进行梳理包括：确定该电力协议的通信过程中村存在的风险，包括中间人攻击和恶意数据注入等。
[0055] 步骤S20107，根据上述协议类型、上述协议作用、上述格式信息、上述消息内容、上述安全机制和上述风险类型构建上述第一目标数据。
[0056] 具体地，对上述数据以预设格式进行整合得到上述第一目标数据。
[0057] 为了得到上述状态迁移图，在一种可选的实施方式中，上述步骤S201还包括：
[0058] 步骤S20108，将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备允许进行数据发送和接收，且允许对上述目标系统进行监控操作和控制操作的状态确定为连接建立状态；
[0059] 具体地，绘制状态迁移图，首先梳理电力协议中可能存在的状态，在一种实施例中，将系统分为正常工作状态和异常状态，进一步确定每个状态的含义以及预期行为，将状态进一步细化，包括将设备可以发送和接收数据，进行正常的监控和控制操作的状态确定为连接建立状态。
[0060] 步骤S20109，将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备周期性进行上述监控操作并发送监控数据或周期性接收其他设备的指令并执行上述控制操作的状态确定为正常监控状态；
[0061] 具体地，将设备周期性地发送监测数据，接收其他设备的指令，并根据需要执行相应的控制操作的状态确定为正常监控状态。
[0062] 步骤S20110，将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备产生报警信息并执行安全措施的状态确定为异常告警状态；
[0063] 具体地，将设备可能会发送报警消息，通知其他系统组件发生了问题，并可能采取预定的应急措施，如切断电源或改变工作模式的状态确定为异常告警状态。
[0064] 步骤S20111，将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备不允许发送数据的状态确定为断开连接状态；
[0065] 具体地，将设备停止发送数据，可能会提供断开连接的通知，等待重新连接或进行维护操作的状态确定为断开连接状态。
[0066] 步骤S20112，基于上述第一目标数据确定上述目标系统处于上述连接建立状态、上述正常监控状态、上述异常告警状态或上述断开连接状态的情况下，分别对应的可以触发的目标事件，并根据对应的上述目标事件确定触发后的上述目标系统的上述系统状态，绘制上述状态迁移图。

[0067]　具体地,除上述常规状态之外,系统最终还存在由特殊事件触发的状态,进而,基于各系统状态的状态迁移图,显示电力协议在不同状态之间的可能转移路径;标识触发状态转移的事件和条件,包括收到特定类型的消息,消息中包含指定的告警标识符,表示设备在远程位置检测到异常情况;超时事件,设备未在规定时间内收到来自关键设备的确认消息,触发超时事件,可能导致设备切换到断开连接状态;错误检测事件,接收到的消息在传输过程中发生错误,校验和验证失败,触发错误检测事件,可能导致设备切换到异常报警状态;用户命令事件,接收到用户命令的设备可能会根据命令内容进行状态转移,例如执行紧急停机或切换到备用模式;系统内部触发条件,设备检测到内部故障,触发系统内部保护机制,可能导致设备切换到异常报警状态并采取相应的应急措施;确认通信协议中对错误和异常情况的处理方式,包括错误代码,协议规定了一套错误代码,用于指示通信中可能发生的各种错误类型,包括消息格式错误、校验和错误;重试机制,在某些错误情况下,协议可能定义了重试机制,允许设备在一定时间内多次尝试发送消息;切换到安全状态,在一些严重错误情况下,协议可能规定了切换到安全状态的行为,以避免进一步损害系统;拒绝不良消息,协议可能规定了当设备收到无效或异常的消息时的处理方式,包括直接忽略、返回错误响应或断开连接;异常输入处理,协议可能定义了对异常输入的处理方式,以防范潜在的攻击和异常情况;考虑可能导致协议状态变化的边界条件包括消息大小超出限制,协议规定了每个消息的最大大小为1000字节;超时值异常,协议规定了正常情况下,设备等待响应的超时时间为5秒;异常状态持续时间,设备在异常状态下的最长持续时间为10分钟;频繁状态转移,协议规定了两次状态转移之间的最小时间间隔为1秒;无效参数范围,(协议规定了某个参数的有效范围为1到100。

[0068]　为了得到神经网络的训练数据,在一种可选的实施方式中,上述步骤S202包括:

[0069]　步骤S2021,监测上述目标系统处于上述正常监控状态下的Modbus通信数据得到第一运行数据;

[0070]　具体地,从实际的电力监控系统中捕获和记录正常工作状态下的Modbus通信消息得到上述第一运行网数据。

[0071]　步骤S2022,监测上述目标系统中的设备之间的查询数据、响应数据和上述监控数据得到第二运行数据;

[0072]　具体地,收集设备之间的查询和响应消息,以及周期性发送的监控数据得到上述第二运行数据。

[0073]　步骤S2023,监测上述目标系统中的设备的异常输入数据得到第三运行数据;

[0074]　具体地,收集异常输入,包括人为制造一些异常情况,包括发送格式错误的消息、无效的功能码或损坏的数据得到上述第三运行数据。

[0075]　步骤S2023,监测上述目标系统中的设备的异常响应数据得到第四运行数据;

[0076]　具体地,收集系统在接收到上述异常输入时候的异常响应数据,得到上述第四运行数据。

[0077]　步骤S2024,根据上述第一运行数据、上述第二运行数据、上述第三运行数据和上述第四运行数据构建上述第一数据集,对上述第一数据集中上述第一运行数据和上述第二运行数据添加第一标识信息,对上述第三运行数据和上述第四运行数据添加第二标识信息得到上述第二数据集,上述第一标识信息用于表征数据为正常数据,上述第二标识信息用

于表征数据为异常数据。

[0078] 具体地,将上述第一运行数据、上述第二运行数据、上述第三运行数据和上述第四运行数据以预设格式进行存储得到上述第一数据集,进而对上述第一运行数据和上述第二运行数据添加正常数据得到标识,对上述第三运行数据和上述第四运行数据添加异常数据的标识得到上述第二数据集。

[0079] 为了确定上述第一目标神经网络,在一种可选的实施方式中,上述步骤S202还包括:

[0080] 步骤S2025,在上述第二数据集中包括消息序列的情况下,确定上述第一目标神经网络为循环神经网络和卷积神经网络,上述循环神经网络用于提取上述第二数据集中的数据的时序特征,上述卷积神经网络用于提取上述第二数据集中的数据的结构信息;

[0081] 具体地,循环神经网络(RNN)可以用于捕获消息中的时序特征,包括消息的先后顺序和状态之间的转移;使用RNN对连续的协议消息序列进行建模,以捕获消息之间的时序关系;RNN可以帮助模型理解消息序列中状态之间的转移模式,有助于检测异常状态或行为;RNN的记忆性质使得模型能够考虑到过去的消息,有助于对当前消息的处理。

[0082] 步骤S2026,在上述第二数据集中不包括上述消息序列的情况下,确定上述第一目标神经网络为上述卷积神经网络。

[0083] 具体地,在电力协议的情境下,通过卷积操作来捕获消息可能包含有规律的结构,包括消息头、消息体;使用卷积层来提取消息中的结构信息,包括消息头、消息体的特征;卷积神经网络(CNN)能够捕获消息中不同部分之间的空间关系,有助于理解消息的整体结构;通过卷积核的学习,CNN可以自动捕获消息中的关键特征,提高模型对重要信息的敏感性。

[0084] 为了得到上述第四数据集,在一种可选的实施方式中,上述步骤S203包括:

[0085] 步骤S2031,在上述第一目标神经网络为上述卷积神经网络的情况下,提取上述第二数据集中数据的数据结构特征,上述数据结构特征包括消息头、功能码、寄存器地址和内容数据对应的数值或编码表示;

[0086] 具体地,消息结构特征提取包括:利用协议规范定义的字段,解析消息并提取各个字段的数值或编码表示,对于Modbus协议,消息包括消息头、功能码、寄存器地址、数据,通过提取这些字段,可以获得消息的结构特征。

[0087] 步骤S2032,提取上述第二数据集中数据的数据长度特征,上述数据长度特征包括不同类型数据的长度;

[0088] 具体地,消息长度特征包括:对于不同类型的消息,其长度可能会有所不同,消息长度可以作为一个重要的特征,将其作为神经网络的输入特征之一。

[0089] 步骤S2033,提取上述第二数据集中数据的预设匹配特征,上述预设匹配特征包括与上述卷积神经网络中预设关键字匹配的文本转换得到的数值或编码表示;

[0090] 具体地,关键字匹配特征包括:利用文本处理技术,检测消息中包含的关键词,并将其转换为对应的数值或编码,包括“查询”、“响应”等。

[0091] 步骤S2034,在上述第一目标神经网络为上述循环神经网络的情况下,提取上述第二数据集中数据的数据时序特征,上述数据时序特征包括上述第二数据集中各数据的顺序关系;

[0092] 具体地,消息的时序特征可以通过记录消息的发送时间戳、消息之间的时间间隔

等来获取。

[0093] 步骤S2035,根据上述数据结构特征、上述数据长度特征、上述预设匹配特征和上述数据时序特征构建上述第三数据集;

[0094] 具体地,将上述提取得到的数据存入数据集中得到上述第三数据集。

[0095] 步骤S2036,将上述第三数据集中类别型数据转换为数值型数据、将上述第三数据集中数据按照上述数据时序特征构建消息序列、将上述第三数据集中的数值型数据进行归一化映射到预设数值范围、对上述第三数据集中的数值型数据进行数据填充得到第七数据集,将上述第五数据集转换为向量组合形式进行表示得到第八数据集;

[0096] 具体地,将消息转换为适合神经网络处理的格式的方法包括数值化/编码(使用独热编码(one-hot encoding)等技术,将类别型数据转换为数值型,以便神经网络能够处理)、序列化(将提取的特征按时间戳排序,形成消息序列,以便RNN能够有效地捕捉时序信息)、标准化/归一化(使用标准差标准化或最小-最大归一化等方法,将特征值映射到合适的数值范围)、填充(在短序列后面添加特定值或进行截断,确保所有序列长度一致,以便形成固定长度的输入)、特征向量组合(将所有特征组合成一个向量,可以是嵌入向量或连接的特征向量,包括提取的结构特征、长度特征,以供CNN处理。

[0097] 步骤S2037,根据上述第七数据集和上述第八数据集构建上述第四数据集。

[0098] 具体地,将上述第七数据集和上述第八数据集按照预设顺序存储得到上述第四数据集。

[0099] 为了得到上述目标模糊测试集,在一种可选的实施方式中,上述步骤S205包括:

[0100] 步骤S2051,在上述第四数据集的数据中引入随机噪声;和/或

[0101] 步骤S2052,对上述第四数据集的数据进行随机变更;和/或

[0102] 步骤S2053,根据第一预设字段对上述第四数据集的数据中第二预设字段进行替换;和/或

[0103] 步骤S2054,根据上述第四数据集的数据对应的数据类型在上述第四数据集中添加对应不同数据类型的边界数值型数据;和/或

[0104] 步骤S2055,根据上述第四数据集的数据对应的数据类型在上述第四数据集中添加对应不同数据类型的错误数据;和/或

[0105] 步骤S2056,变更上述第四数据集中的上述消息序列的时序进行变更,得到上述目标模糊测试集。

[0106] 具体地,生成目标模糊测试集的方式包括,引入噪声,通过在正常消息中引入随机噪声,包括随机修改消息中的某些字节或添加额外的无意义信息;改变消息结构,在正常消息的基础上,随机改变消息结构,包括交换消息字段的位置、增加或删除某些字段;模拟异常条件,引入特定的异常条件,包括将消息中的校验和设置为无效值、模拟超时情况;机生成消息,根据协议规范随机生成符合规范但不常见的消息,包括使用非常见功能码、寄存器地址;错误参数注入,针对消息中的参数,包括寄存器地址、数据值,注入错误的数值或越界数值;时间序列扰动,对生成的消息序列引入时间上的扰动,包括随机改变消息的发送时间戳或时间间隔;生成攻击样本,利用神经网络的生成对抗网络生成具有误导性的消息,使其在正常情况下看起来合法但具有攻击性中的一个或多个。

[0107] 需要说明的是,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的

计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0108] 本申请实施例还提供了一种电力协议的模糊测试装置,需要说明的是,本申请实施例的电力协议的模糊测试装置可以用于执行本申请实施例所提供的用于电力协议的模糊测试方法。该装置用于实现上述实施例及优选实施方式,已经进行过说明的不再赘述。如以下所使用的,术语"模块"可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现,但是硬件,或者软件和硬件的组合的实现也是可能并被构想的。

[0109] 以下对本申请实施例提供的电力协议的模糊测试装置进行介绍。

[0110] 图3是根据本申请实施例的电力协议的模糊测试装置的结构框图。如图3所示,该装置包括:

[0111] 第一获取单元10,用于对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;

[0112] 具体地,根据计划进行测试的电力协议进行分析,得到电力协议在相关系统的基本工作原理,得到上述第一目标数据,进而根究工作原理,确定电力协议的状态迁移图,用于表征各种可能的状态与状态之间的转移。

[0113] 第二获取单元20,用于监测上述目标系统的运行数据得到第一数据集,对上述第一数据集进行标记得到第二数据集,根据上述第二数据集确定至少一个第一目标神经网络,不同上述第一目标神经网络用于提取不同类型的特征数据;

[0114] 具体地,收集相关系统中与电力协议相关的数据,包括有效的协议消息和一场输入得到上述第一数据集。进而对第一数据集中的数据进行标记,区分为正常数据和异常数据,以便于神经网络进行学习,提取相关特征,得到上述第二数据集。根据相关协议消息中的有用特征选择合适的神经网络模型得到上述第一目标神经网络。

[0115] 第一输入单元30,用于将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集;

[0116] 具体地,将上述第二数据集输入上述第一目标神经网络进行特征提取得到特征数据集集,即上述第三数据集。进而对上述第三数据集进行数据处理将第三数据集中的数据转换为适合神经网络进行处理的数据格式得到上述第四数据集。

[0117] 训练单元40,用于将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试,在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络,上述神经网络用于基于上述目标系统的运行数据生成模糊测试集;

[0118] 具体地,对上述第四数据集进行划分,得到训练集和测试集,即上述第五数据集和上述第六数据集。进而根据训练集对模型进行训练,根据测试集评估模型的性能。在上述神经网络的损失函数小于阈值的情况下确定模型的性能满足要求,将之确定为第二目标神经网络。

[0119]　第二输入单元50,用于将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集,根据上述目标模糊测试集对上述目标系统进行模糊测试,根据上述目标系统的响应确定模糊测试结果,上述模糊测试结果包括上述目标系统的异常状态和异常行为。

[0120]　具体地,将格式转换之后的特征数据集,输入上述第二目标神经网络,生成模糊测试集,进而基于模糊测试集对电力系统进行模糊测试,监控系统的响应,收集系统的异常行为和错误状态,根据测试结果确定电力协议的漏洞和风险。

[0121]　通过本实施例,第一获取单元对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;第二获取单元监测上述目标系统的运行数据得到第一数据集,对上述第一数据集进行标记得到第二数据集,根据上述第二数据集确定至少一个第一目标神经网络,不同上述第一目标神经网络用于提取不同类型的特征数据;第一输入单元将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集;训练单元将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集,根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试,在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络,上述神经网络用于基于上述目标系统的运行数据生成模糊测试集;第二输入单元将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集,根据上述目标模糊测试集对上述目标系统进行模糊测试,根据上述目标系统的响应确定模糊测试结果,上述模糊测试结果包括上述目标系统的异常状态和异常行为。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。本申请给予对电力设备的实际场景中的数据与神经网络进行结合,通过神经网络实现对数据中的特征进行分析,并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集,根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。

[0122]　为了得到上述第一目标数据,在一种可选的实施方式中,上述第一获取单元包括:

[0123]　第一确定模块,用于对上述目标系统进行分析,确定上述目标电力协议的协议类型,上述协议类型包括DNP3、Modbus和IEC 61850中的一个或多个;

[0124]　具体地,对电力协议进行梳理包括:确定电力系统通信协议的类型,包括DNP3、Modbus、IEC 61850等。

[0125]　第二确定模块,用于对上述目标电力协议进行分析,确定上述目标电力协议的协议作用,上述协议作用至少包括监测上述目标系统中电力设备状态、执行控制命令和传输告警信息中的一个或多个;

[0126]　具体地,对电力协议进行梳理包括:确定该电力协议配置于电力系统的主要目的,包括实时监测电力设备状态,执行控制命令,传递告警信息等。

[0127] 第三确定模块，用于对上述目标电力协议进行分析，确定上述目标电力协议的格式信息，上述格式信息包括消息头、消息体和校验和中的至少一个；

[0128] 具体地，对电力协议进行梳理包括：确定电力协议中消息的格式、字段、结构，包括消息体、消息头和校验码等。

[0129] 第四确定模块，用于对上述目标电力协议进行分析，确定上述目标电力协议的消息内容，上述消息内容包括设备标识符、命令类型、控制参数和设备地址中的至少一个；

[0130] 具体地，对电力协议进行梳理包括：确定在该电力协议中设备之间消息包含的内容，例如设备标识符、命令类型、参数、设备地址等。

[0131] 第五确定模块，用于对上述目标电力协议进行分析，确定上述目标电力协议的安全机制，上述安全机制包括加密通信、身份验证和完整性验证中的至少一个；

[0132] 具体地，对电力协议进行梳理包括：确定电力协议中使用的安全机制，包括加密、身份验证、和完整性验证等。

[0133] 第六确定模块，用于对上述目标电力协议进行分析，确定上述目标电力协议的风险类型，上述风险类型包括中间人攻击和数据注入中的至少一个；

[0134] 具体地，对电力协议进行梳理包括：确定该电力协议的通信过程中村存在的风险，包括中间人攻击和恶意数据注入等。

[0135] 第一构建模块，用于根据上述协议类型、上述协议作用、上述格式信息、上述消息内容、上述安全机制和上述风险类型构建上述第一目标数据。

[0136] 具体地，对上述数据以预设格式进行整合得到上述第一目标数据。

[0137] 为了得到上述状态迁移图，在一种可选的实施方式中，上述第一获取单元还包括：

[0138] 第七确定模块，用于将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备允许进行数据发送和接收，且允许对上述目标系统进行监控操作和控制操作的状态确定为连接建立状态；

[0139] 具体地，绘制状态迁移图，首先梳理电力协议中可能存在的状态，在一种实施例中，将系统分为正常工作状态和异常状态，进一步确定每个状态的含义以及预期行为，将状态进一步细化，包括将设备可以发送和接收数据，进行正常的监控和控制操作的状态确定为连接建立状态。

[0140] 第八确定模块，用于将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备周期性进行上述监控操作并发送监控数据或周期性接收其他设备的指令并执行上述控制操作的状态确定为正常监控状态；

[0141] 具体地，将设备周期性地发送监测数据，接收其他设备的指令，并根据需要执行相应的控制操作的状态确定为正常监控状态。

[0142] 第九确定模块，用于将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备产生报警信息并执行安全措施的状态确定为异常告警状态；

[0143] 具体地，将设备可能会发送报警消息，通知其他系统组件发生了问题，并可能采取预定的应急措施，如切断电源或改变工作模式的状态确定为异常告警状态。

[0144] 第十确定模块，用于将上述目标系统在上述目标电力协议控制下，上述目标系统中的设备不允许发送数据的状态确定为断开连接状态；

[0145] 具体地，将设备停止发送数据，可能会提供断开连接的通知，等待重新连接或进行

维护操作的状态确定为断开连接状态。

[0146]　第二构建模块,用于基于上述第一目标数据确定上述目标系统处于上述连接建立状态、上述正常监控状态、上述异常告警状态或上述断开连接状态的情况下,分别对应的可以触发的目标事件,并根据对应的上述目标事件确定触发后的上述目标系统的上述系统状态,绘制上述状态迁移图。

[0147]　具体地,除上述常规状态之外,系统最终还存在由特殊事件触发的状态,进而,基于各系统状态的状态迁移图,显示电力协议在不同状态之间的可能转移路径;标识触发状态转移的事件和条件,包括收到特定类型的消息,消息中包含指定的告警标识符,表示设备在远程位置检测到异常情况;超时事件,设备未在规定时间内收到来自关键设备的确认消息,触发超时事件,可能导致设备切换到断开连接状态;错误检测事件,接收到的消息在传输过程中发生错误,校验和验证失败,触发错误检测事件,可能导致设备切换到异常报警状态;用户命令事件,接收到用户命令的设备可能会根据命令内容进行状态转移,例如执行紧急停机或切换到备用模式;系统内部触发条件,设备检测到内部故障,触发系统内部保护机制,可能导致设备切换到异常报警状态并采取相应的应急措施;确认通信协议中对错误和异常情况的处理方式,包括错误代码,协议规定了一套错误代码,用于指示通信中可能发生的各种错误类型,包括消息格式错误、校验和错误;重试机制,在某些错误情况下,协议可能定义了重试机制,允许设备在一定时间内多次尝试发送消息;切换到安全状态,在一些严重错误情况下,协议可能规定了切换到安全状态的行为,以避免进一步损害系统;拒绝不良消息,协议可能规定了当设备收到无效或异常的消息时的处理方式,包括直接忽略、返回错误响应或断开连接;异常输入处理,协议可能定义了对异常输入的处理方式,以防范潜在的攻击和异常情况;考虑可能导致协议状态变化的边界条件包括消息大小超出限制,协议规定了每个消息的最大大小为1000字节;超时值异常,协议规定了正常情况下,设备等待响应的超时时间为5秒;异常状态持续时间,设备在异常状态下的最长持续时间为10分钟;频繁状态转移,协议规定了两次状态转移之间的最小时间间隔为1秒;无效参数范围,(协议规定了某个参数的有效范围为1到100。

[0148]　为了得到神经网络的训练数据,在一种可选的实施方式中,上述第二获取单元包括:

[0149]　第一获取模块,用于监测上述目标系统处于上述正常监控状态下的Modbus通信数据得到第一运行数据;

[0150]　具体地,从实际的电力监控系统中捕获和记录正常工作状态下的Modbus通信消息得到上述第一运行网数据。

[0151]　第二获取模块,用于监测上述目标系统中的设备之间的查询数据、响应数据和上述监控数据得到第二运行数据;

[0152]　具体地,收集设备之间的查询和响应消息,以及周期性发送的监控数据得到上述第二运行数据。

[0153]　第三获取模块,用于监测上述目标系统中的设备的异常输入数据得到第三运行数据;

[0154]　具体地,收集异常输入,包括人为制造一些异常情况,包括发送格式错误的消息、无效的功能码或损坏的数据得到上述第三运行数据。

[0155] 第四获取模块,用于监测上述目标系统中的设备的异常响应数据得到第四运行数据;

[0156] 具体地,收集系统在接收到上述异常输入时候的异常响应数据,得到上述第四运行数据。

[0157] 第三构建模块,用于根据上述第一运行数据、上述第二运行数据、上述第三运行数据和上述第四运行数据构建上述第一数据集,对上述第一数据集中上述第一运行数据和上述第二运行数据添加第一标识信息,对上述第三运行数据和上述第四运行数据添加第二标识信息得到上述第二数据集,上述第一标识信息用于表征数据为正常数据,上述第二标识信息用于表征数据为异常数据。

[0158] 具体地,将上述第一运行数据、上述第二运行数据、上述第三运行数据和上述第四运行数据以预设格式进行存储得到上述第一数据集,进而对上述第一运行数据和上述第二运行数据添加正常数据得到标识,对上述第三运行数据和上述第四运行数据添加异常数据的标识得到上述第二数据集。

[0159] 为了确定上述第一目标神经网络,在一种可选的实施方式中,上述第二获取单元还包括:

[0160] 第十一确定模块,用于在上述第二数据集中包括消息序列的情况下,确定上述第一目标神经网络为循环神经网络和卷积神经网络,上述循环神经网络用于提取上述第二数据集中的数据的时序特征,上述卷积神经网络用于提取上述第二数据集中的数据的结构信息;

[0161] 具体地,循环神经网络(RNN)可以用于捕获消息中的时序特征,包括消息的先后顺序和状态之间的转移;使用RNN对连续的协议消息序列进行建模,以捕获消息之间的时序关系;RNN可以帮助模型理解消息序列中状态之间的转移模式,有助于检测异常状态或行为;RNN的记忆性质使得模型能够考虑到过去的消息,有助于对当前消息的处理。

[0162] 第十二确定模块,用于在上述第二数据集中不包括上述消息序列的情况下,确定上述第一目标神经网络为上述卷积神经网络。

[0163] 具体地,在电力协议的情境下,通过卷积操作来捕获消息可能包含有规律的结构,包括消息头、消息体;使用卷积层来提取消息中的结构信息,包括消息头、消息体的特征;卷积神经网络(CNN)能够捕获消息中不同部分之间的空间关系,有助于理解消息的整体结构;通过卷积核的学习,CNN可以自动捕获消息中的关键特征,提高模型对重要信息的敏感性。

[0164] 为了得到上述第四数据集,在一种可选的实施方式中,上述第一输入单元包括:

[0165] 第五获取模块,用于在上述第一目标神经网络为上述卷积神经网络的情况下,提取上述第二数据集中数据的数据结构特征,上述数据结构特征包括消息头、功能码、寄存器地址和内容数据对应的数值或编码表示;

[0166] 具体地,消息结构特征提取包括:利用协议规范定义的字段,解析消息并提取各个字段的数值或编码表示,对于Modbus协议,消息包括消息头、功能码、寄存器地址、数据,通过提取这些字段,可以获得消息的结构特征。

[0167] 第六获取模块,用于提取上述第二数据集中数据的数据长度特征,上述数据长度特征包括不同类型数据的长度;

[0168] 具体地,消息长度特征包括:对于不同类型的消息,其长度可能会有所不同,消息

长度可以作为一个重要的特征,将其作为神经网络的输入特征之一。

[0169] 第七获取模块,用于提取上述第二数据集中数据的预设匹配特征,上述预设匹配特征包括与上述卷积神经网络中预设关键字匹配的文本转换得到的数值或编码表示;

[0170] 具体地,关键字匹配特征包括:利用文本处理技术,检测消息中包含的关键词,并将其转换为对应的数值或编码,包括"查询"、"响应"等。

[0171] 第八获取模块,用于在上述第一目标神经网络为上述循环神经网络的情况下,提取上述第二数据集中数据的数据时序特征,上述数据时序特征包括上述第二数据集中各数据的顺序关系;

[0172] 具体地,消息的时序特征可以通过记录消息的发送时间戳、消息之间的时间间隔等来获取。

[0173] 第四构建模块,用于第五获取模块,用于根据上述数据结构特征、上述数据长度特征、上述预设匹配特征和上述数据时序特征构建上述第三数据集;

[0174] 具体地,将上述提取得到的数据存入数据集中得到上述第三数据集。

[0175] 第五构建模块,用于将上述第三数据集中类别型数据转换为数值型数据、将上述第三数据集中数据按照上述数据时序特征构建消息序列、将上述第三数据集中的数值型数据进行归一化映射到预设数值范围、对上述第三数据集中的数值型数据进行数据填充得到第七数据集,将上述第五数据集转换为向量组合形式进行表示得到第八数据集;

[0176] 具体地,将消息转换为适合神经网络处理的格式的方法包括数值化/编码(使用独热编码(one-hot encoding)等技术,将类别型数据转换为数值型,以便神经网络能够处理)、序列化(将提取的特征按时间戳排序,形成消息序列,以便RNN能够有效地捕捉时序信息)、标准化/归一化(使用标准差标准化或最小-最大归一化等方法,将特征值映射到合适的数值范围)、填充(在短序列后面添加特定值或进行截断,确保所有序列长度一致,以便形成固定长度的输入)、特征向量组合(将所有特征组合成一个向量,可以是嵌入向量或连接的特征向量,包括提取的结构特征、长度特征,以供CNN处理。

[0177] 第六构建模块,用于根据上述第七数据集和上述第八数据集构建上述第四数据集。

[0178] 具体地,将上述第七数据集和上述第八数据集按照预设顺序存储得到上述第四数据集。

[0179] 为了得到上述目标模糊测试集,在一种可选的实施方式中,上述第二输入单元包括:

[0180] 第一处理模块,用于在上述第四数据集的数据中引入随机噪声;和/或

[0181] 第二处理模块,用于对上述第四数据集的数据进行随机变更;和/或

[0182] 第三处理模块,用于根据第一预设字段对上述第四数据集的数据中第二预设字段进行替换;和/或

[0183] 第四处理模块,用于根据上述第四数据集的数据对应的数据类型在上述第四数据集中添加对应不同数据类型的边界数值型数据;和/或

[0184] 第五处理模块,用于根据上述第四数据集的数据对应的数据类型在上述第四数据集中添加对应不同数据类型的错误数据;和/或

[0185] 第六处理模块,用于变更上述第四数据集中的上述消息序列的时序进行变更,得

到上述目标模糊测试集。

[0186] 具体地,生成目标模糊测试集的方式包括,引入噪声,通过在正常消息中引入随机噪声,包括随机修改消息中的某些字节或添加额外的无意义信息;改变消息结构,在正常消息的基础上,随机改变消息结构,包括交换消息字段的位置、增加或删除某些字段;模拟异常条件,引入特定的异常条件,包括将消息中的校验和设置为无效值、模拟超时情况;机生成消息,根据协议规范随机生成符合规范但不常见的消息,包括使用非常见功能码、寄存器地址;错误参数注入,针对消息中的参数,包括寄存器地址、数据值,注入错误的数值或越界数值;时间序列扰动,对生成的消息序列引入时间上的扰动,包括随机改变消息的发送时间戳或时间间隔;生成攻击样本,利用神经网络的生成对抗网络生成具有误导性的消息,使其在正常情况下看起来合法但具有攻击性中的一个或多个。

[0187] 上述电力协议的模糊测试装置包括处理器和存储器,上述第一获取单元、第二获取单元、第一输入单元、训练单元和第二输入单元等均作为程序单元存储在存储器中,由处理器执行存储在存储器中的上述程序单元来实现相应的功能。上述模块均位于同一处理器中;或者,上述各个模块以任意组合的形式分别位于不同的处理器中。

[0188] 处理器中包含内核,由内核去存储器中调取相应的程序单元。内核可以设置一个或以上,通过调整内核参数来提高电力协议测试的准确性。

[0189] 存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM),存储器包括至少一个存储芯片。

[0190] 本发明实施例提供了一种计算机可读存储介质,上述计算机可读存储介质包括存储的程序,其中,在上述程序运行时控制上述计算机可读存储介质所在设备执行上述电力协议的模糊测试方法。

[0191] 本发明实施例提供了一种处理器,上述处理器用于运行程序,其中,上述程序运行时执行上述电力协议的模糊测试方法。

[0192] 本发明实施例提供了一种通信系统,通信系统包括一级通信域、二级通信域处理器、存储器及存储在存储器上并可在处理器上运行的程序,处理器执行程序时实现至少上述电力协议的模糊测试方法的步骤。

[0193] 本申请还提供了一种计算机程序产品,当在数据处理设备上执行时,适于执行初始化有至少上述电力协议的模糊测试方法方法步骤的程序。

[0194] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0195] 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。
[0196] 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。
[0197] 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。
[0198] 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。
[0199] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。
[0200] 存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。
[0201] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带,磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。
[0202] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。
[0203] 从以上的描述中,可以看出,本申请上述的实施例实现了如下技术效果:
[0204] 1)、本申请的电力协议的模糊测试方法,首先,对目标电力协议和目标系统进行梳理得到第一目标数据,根据上述第一目标数据确定状态迁移图,上述目标系统为上述目标电力协议部署的电力系统,上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理,上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系;然后,监测上述目标系统的运行数据得到第一数据集,对上述第一数据集

进行标记得到第二数据集，根据上述第二数据集确定至少一个第一目标神经网络，不同上述第一目标神经网络用于提取不同类型的特征数据；之后，将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集；之后，将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集，根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试，在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络，上述神经网络用于基于上述目标系统的运行数据生成模糊测试集；最后，将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集，根据上述目标模糊测试集对上述目标系统进行模糊测试，根据上述目标系统的响应确定模糊测试结果，上述模糊测试结果包括上述目标系统的异常状态和异常行为。本申请给予对电力设备的实际场景中的数据与神经网络进行结合，通过神经网络实现对数据中的特征进行分析，并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集，根据模糊测试的数据集控制电力设备进行状态迁移模糊测试，以对电力协议中存在的风险等进行验证，解决了现有技术中需要人工进行电力协议分析，准确性较低的问题。本申请给予对电力设备的实际场景中的数据与神经网络进行结合，通过神经网络实现对数据中的特征进行分析，并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集，根据模糊测试的数据集控制电力设备进行状态迁移模糊测试，以对电力协议中存在的风险等进行验证，解决了现有技术中需要人工进行电力协议分析，准确性较低的问题。

[0205] 2)、本申请的电力协议的模糊测试装置，第一获取单元对目标电力协议和目标系统进行梳理得到第一目标数据，根据上述第一目标数据确定状态迁移图，上述目标系统为上述目标电力协议部署的电力系统，上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理，上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系；第二获取单元监测上述目标系统的运行数据得到第一数据集，对上述第一数据集进行标记得到第二数据集，根据上述第二数据集确定至少一个第一目标神经网络，不同上述第一目标神经网络用于提取不同类型的特征数据；第一输入单元将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集；训练单元将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集，根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试，在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络，上述神经网络用于基于上述目标系统的运行数据生成模糊测试集；第二输入单元将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集，根据上述目标模糊测试集对上述目标系统进行模糊测试，根据上述目标系统的响应确定模糊测试结果，上述模糊测试结果包括上述目标系统的异常状态和异常行为。本申请给予对电力设备的实际场景中的数据与神经网络进行结合，通过神经网络实现对数据中的特征进行分析，并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集，根据模糊测试的数据集控制电力设备进行状态迁移模糊测试，以对电力协议中存在的风险等进行验证，解决了现有技术中需要人工进行电力协议分析，准确性较低的问题。本申请给予对电力设备的实际场景中的数据与神经网络进行结合，通过神经网络实现对数据中的特征进行分析，并进一步通过神经网络基于实际数据进行处理得到模糊测试的数据集，

根据模糊测试的数据集控制电力设备进行状态迁移模糊测试,以对电力协议中存在的风险等进行验证,解决了现有技术中需要人工进行电力协议分析,准确性较低的问题。

[0206] 以上所述仅为本申请的优选实施例而已,并不用于限制本申请,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

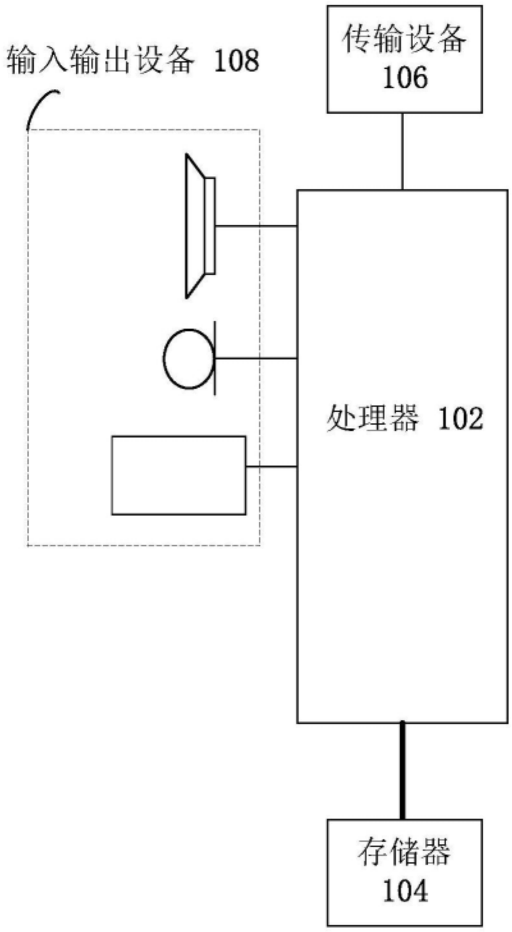

图1


对目标电力协议和目标系统进行梳理得到第一目标数据，根据上述第一目标数据确定状态迁移图，上述目标系统为上述目标电力协议部署的电力系统，上述第一目标数据至少包括上述目标电力协议的类型、格式和结构以及在上述目标系统的运行原理，上述状态迁移图用于表征上述目标系统的系统状态之间的转移关系；
S201
监测上述目标系统的运行数据得到第一数据集，对上述第一数据集进行标记得到第二数据集，根据上述第二数据集确定至少一个第一目标神经网络，不同上述第一目标神经网络用于提取不同类型的特征数据；
S202
将上述第二数据集输入上述第一目标神经网络得到第三数据集并对上述第三数据集进行处理将上述第三数据集中的数据转换为预设格式得到第四数据集；
S203
将上述第四数据集分为训练集和测试集得到第五数据集和第六数据集，根据上述第五数据集对神经网络进行训练并根据上述第六数据集进行测试，在上述神经网络的损失函数小于阈值的情况下将上述神经网络确定为第二目标神经网络，上述神经网络用于基于上述目标系统的运行数据生成模糊测试集；
S204
将上述第四数据集输入上述第二目标神经网络得到目标模糊测试集，根据上述目标模糊测试集对上述目标系统进行模糊测试，根据上述目标系统的响应确定模糊测试结果，上述模糊测试结果包括上述目标系统的异常状态和异常行为。
S205

图2

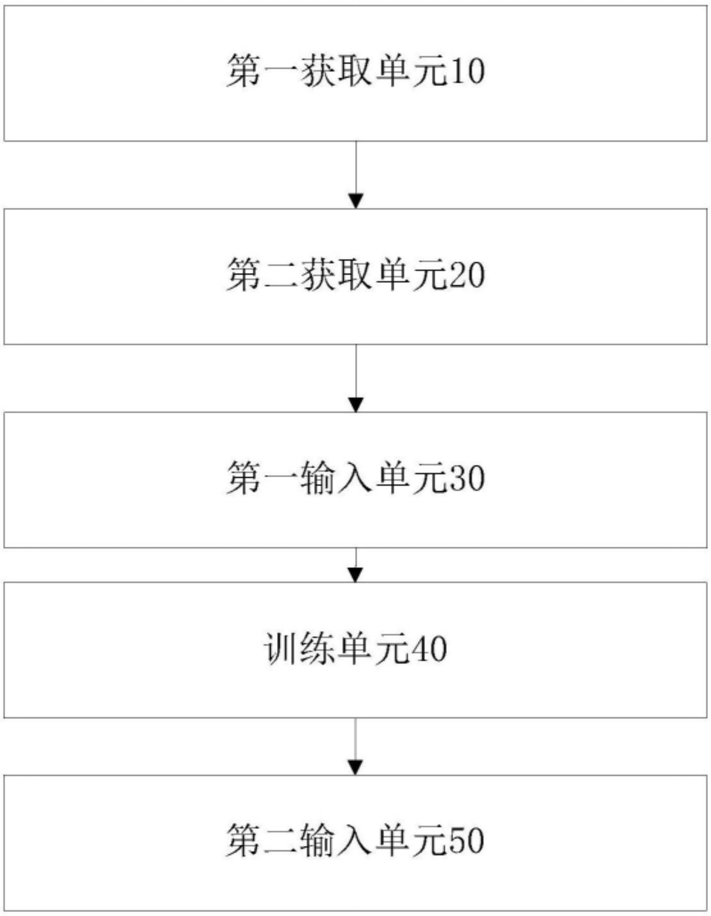

图3