(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112073375 B
(45)授权公告日 2023.09.26

(21)申请号 202010789502.2
(22)申请日 2020.08.07
(65)同一申请的已公布的文献号
申请公布号 CN 112073375 A
(43)申请公布日 2020.12.11
(73)专利权人 中国电力科学研究院有限公司
地址 100192 北京市海淀区清河小营东路15号
专利权人 国家电网有限公司
国网山西省电力公司营销服务中心
(72)发明人 梁晓兵 翟峰 岑炜 付义伦 曹永峰 刘鹰 李保丰 王晖南 徐萌 许斌 孔令达 冯云 冯占成
(74)专利代理机构 北京工信联合知识产权代理有限公司 11266
专利代理师 夏德政
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/12(2022.01)
H04L 69/22(2022.01)
H04L 69/08(2022.01)
G16Y 10/35(2020.01)
(56)对比文件
US 2020106686 A1,2020.04.02
US 2015150110 A1,2015.05.28
US 2017346631 A1,2017.11.30
CN 110493225 A,2019.11.22
CN 109889532 A,2019.06.14
CN 110472584 A,2019.11.19
CN 110210858 A,2019.09.06
CN 111447153 A,2020.07.24
CN 106991317 A,2017.07.28
CN 107276987 A,2017.10.20
CN 106250857 A,2016.12.21
CN 110933055 A,2020.03.27
CN 110855756 A,2020.02.28
CN 108965283 A,2018.12.07
CN 103905451 A,2014.07.02
US 2018337948 A1,2018.11.22
CN 105656883 A,2016.06.08
CN 106941494 A,2017.07.11
CN 109005189 A,2018.12.14
CN 109525606 A,2019.03.26 (续)
审查员 程慧

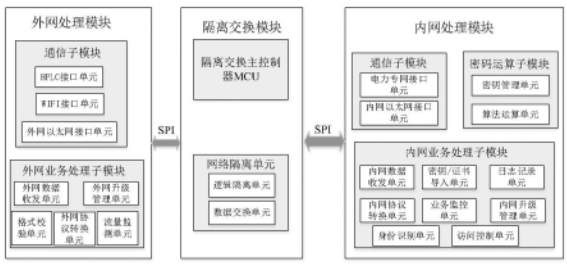
权利要求书4页 说明书11页 附图3页

(54)发明名称

一种适用于电力物联网客户侧的隔离装置及隔离方法

(57)摘要

本发明涉及一种适用于电力物联网客户侧的隔离装置及隔离方法，利用外网处理模块对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对关键信息进行协议格式转换处理，以获取第二数据报文；利用隔离交换模块控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验；并在所述第二数据报文通过格式校验后利用内网处理模块对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备，实现了开放的客户侧接入网络与电力物联网核心网络的安全隔离，能够有效防止核心业务系统被非法入侵。



CN 112073375 B

[转续页]

[接上页]

(56)对比文件

CN 104486336 A,2015.04.01
CN 109842585 A,2019.06.04
CN 104683332 A,2015.06.03
CN 103619020 A,2014.03.05
CN 110620791 A,2019.12.27
CN 207638693 U,2018.07.20
US 2020045023 A1,2020.02.06
WO 2015085809 A1,2015.06.18

1.一种适用于电力物联网客户侧的隔离装置,其特征在于,所述装置包括:

外网处理模块,用于对接收的外网设备发送的第一数据报文进行解析,以获取关键信息,并按照数据摆渡协议对所述关键信息进行协议格式转换处理,以获取第二数据报文并发送至隔离交换模块;

隔离交换模块,用于控制外网处理模块和内网处理模块处于物理隔离的状态,对所述第二数据报文进行格式校验,并在所述第二数据报文通过格式校验后,将所述第二数据报文发送至内网处理模块;

内网处理模块,用于对所述第二数据报文进行解密处理,并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理,以获取第三数据报文并发送至内网设备;

其中,所述装置还包括:

内网处理模块,用于对接收的内网设备发送的第四数据报文进行加密处理,并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理,以获取第五数据报文并发送至隔离交换模块;

隔离交换模块,用于控制外网处理模块和内网处理模块处于物理隔离的状态,对所述第五数据报文进行格式校验,并在所述第五数据报文通过格式校验后,将所述第五数据报文发送至外网处理模块;

外网处理模块,用于按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理,以获取第六数据报文并发送至外网设备;

其中,所述内网处理模块,还包括:

身份识别单元,用于根据解密后的第二数据报文,获取待接入的外网设备的身份信息,并根据待接入的外网设备的身份信息进行身份鉴别;其中,若身份鉴别成功,则允许所述待接入的外网设备接入电力物联网进行信息交互;若身份鉴别失败,则拒绝所述待接入的外网设备接入电力物联网进行信息交互;其中所述关键信息包括:外网设备的身份信息;

身份鉴别的过程包括:

(1)感知设备或用户电器设备将其MAC、IP、通信协议P_r、有效数据D_v、数据格式D_f设备参数信息发送给内网处理模块;内网处理模块分析其合法性和有效性,如果符合物联网环境准入要求,形成“设备指纹”D_{fp},并将验证结果反馈给感知设备或用户电器设备;

(2)感知设备或用户电器设备将能耗变化Ec、信号强度变化Sc、流量变化Fc环境参数信息,发送给内网处理模块;隔离装置生成“运行环境指纹”E_{fp},并将接收结果反馈给感知设备或用户电器设备;

(3)内网处理模块将采集到的指纹信息传输至后台集中管理平台中,建立感知设备准入白名单W_1;

(4)当待接入的设备通过WIFI、HPLC或以太网方式接入隔离装置时,内网处理模块将再次根据待接入的外网设备的身份信息按照预设的指纹生成策略,分别生成设备指纹和运行环境指纹,并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对,以进行身份鉴别;其中,所述身份信息包括:设备参数信息和运行环境参数信息;

其中,所述身份识别单元,根据待接入的外网设备的身份信息进行身份鉴别,包括:

根据待接入的外网设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；所述设备参数信息包括：外网设备的MAC地址、IP、通信协议、有效数据和数据格式；所述运行环境参数信息包括：外网设备的能耗变化、信号强度变化和流量变化；

其中，所述隔离交换模块，控制外网处理模块和内网处理模块处于物理隔离的状态，包括：

控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。

2.根据权利要求1所述的装置，其特征在于，所述外网处理模块，还包括：

格式校验单元，用于校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求；

流量监测单元，用于监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

3.根据权利要求1所述的装置，其特征在于，所述隔离交换模块，利用如下方式进行格式校验，包括：

校验待传输的数据报文的格式是否符合数据摆渡协议；其中，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

4.根据权利要求1所述的装置，其特征在于，所述内网处理模块，还包括：

访问控制单元，用于根据预设的访问控制策略对所述外网设备进行接入控制，确定所述外网设备访问权限；

业务监控单元，用于对所述内网处理模块中的进程进行监测，并在出现异常事件时，及时对所述异常事件进行处理，以维护所述内网处理模块能够正常服务；

日志记录单元，用于记录各类操作日志和通信日志；

密钥证书导入单元，用于与电力统一密码基础设施对接，以实现外网设备密钥的分发和数字证书的申请及下发。

5.一种适用于电力物联网客户侧的隔离方法，其特征在于，所述方法包括：

对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文；

控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验；

在所述第二数据报文通过格式校验后，对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备；

其中，所述方法还包括：

对接收的内网设备发送的第四数据报文进行加密处理，并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理，以获取第五数据报文；

控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第五数据报文进行格式校验；

在所述第五数据报文通过格式校验后，按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理，以获取第六数据报文并发送至外网设备；

其中，所述方法还包括：

根据解密后的第二数据报文，获取待接入的外网设备的身份信息，并根根据待接入的外网设备的身份信息进行身份鉴别；其中，若身份鉴别成功，则允许所述待接入的外网设备接入电力物联网进行信息交互；若身份鉴别失败，则拒绝所述待接入的外网设备接入电力物联网进行信息交互；其中所述关键信息包括：外网设备的身份信息；

身份鉴别的过程包括：

(1)感知设备或用户电器设备将其MAC、IP、通信协议P_r、有效数据D_v、数据格式D_f设备参数信息发送给内网处理模块；内网处理模块分析其合法性和有效性，如果符合物联网环境准入要求，形成“设备指纹”D_{fp}，并将验证结果反馈给感知设备或用户电器设备；

(2)感知设备或用户电器设备将能耗变化Ec、信号强度变化Sc、流量变化Fc环境参数信息，发送给内网处理模块；隔离装置生成“运行环境指纹”E_{fp}，并将接收结果反馈给感知设备或用户电器设备；

(3)内网处理模块将采集到的指纹信息传输至后台集中管理平台中，建立感知设备准入白名单W_1；

(4)当待接入的设备通过WIFI、HPLC或以太网方式接入隔离装置时，内网处理模块将再次根据待接入的外网设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；

其中，所述根据待接入的外网设备的身份信息进行身份鉴别，包括：

根据待接入的外网设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；所述设备参数信息包括：外网设备的MAC地址、IP、通信协议、有效数据和数据格式；所述运行环境参数信息包括：外网设备的能耗变化、信号强度变化和流量变化；

其中，所述控制外网处理模块和内网处理模块处于物理隔离的状态，包括：

控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。

6.根据权利要求5所述的方法，其特征在于，所述方法还包括：在对接收的外网设备发送的第一数据报文进行解析之前，校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述

外网设备的数据传输请求；

监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

7.根据权利要求5所述的方法，其特征在于，所述方法利用如下方式进行格式校验，包括：

校验待传输的数据报文的格式是否符合数据摆渡协议；其中，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

8.根据权利要求5所述的方法，其特征在于，所述方法还包括：

根据预设的访问控制策略对所述外网设备进行接入控制，确定所述外网设备访问权限；

对所述内网处理模块中的进程进行监测，并在出现异常事件时，及时对所述异常事件进行处理，以维护所述内网处理模块能够正常服务；

记录各类操作日志和通信日志；

与电力统一密码基础设施对接，以实现外网设备密钥的分发和数字证书的申请及下发。

一种适用于电力物联网客户侧的隔离装置及隔离方法

技术领域

[0001] 本发明涉及物联网技术领域，并且更具体地，涉及一种适用于电力物联网客户侧的隔离装置及隔离方法。

背景技术

[0002] 随着移动互联、人工智能等新技术的发展，电力用户与智能电网的双向交互越来越频繁，用户对电网的服务形式和服务质量要求也越来越高。为了满足电力用户的应用需求，增强电力用户对智能电网的感知度和参与度，电力物联网随之而产生。电力物联网具有运行状态全面感知、信息高效处理、应用便捷灵活等特征，将电力用户及其设备，各类企业及设备，以及人和物连接起来，产生共享数据，为用户、电网、电力企业、供应商和社会服务，并以电网为枢纽，发挥平台和共享作用，为全行业和更多市场主体提供更有价值的服务。

[0003] 为提升电力物联网与用户的互动性，需要在电力物联网客户侧接入充电桩、外部综合能源设备等海量安全不受控的非电网资产设备。这些设备可通过WIFI等便捷通信方式与各类电器设备连接，实现用电数据的采集与信息交互。这不可避免地使电力网络从封闭式服务方式转变为开放式，导致电力物联网与公共网络直接连接，在很大程度上增加了电力物联网遭受伪造终端接入、木马、病毒、恶意代码等网络攻击的风险，使恶意人员更容易通过感知层入侵到整个电力网络并进行攻击破坏。因此，需要隔离装置实现网络隔离和网络间数据的安全交互。然而，传统隔离设备或系统功能较为单一，设备体积和功耗较大，需要的计算资源相对较多，大多只适用于传统网络的边界隔离，不能满足低功耗、低成本、多分布需求的电力物联网感知层或边缘层的客户侧不受控设备信息安全交互需求。

[0004] 因此，急需研究物联网微隔离技术，研制能够部署于电力物联网感知层或边缘层的网络隔离装置，将开放给电力用户的接入网络与电力物联网核心网络进行安全隔离。

发明内容

[0005] 本发明提出一种适用于电力物联网客户侧的隔离装置及隔离方法，以解决如何将开放的物联网客户侧接入网络与电力物联网核心网络进行安全隔离的问题。

[0006] 为了解决上述问题，根据本发明的一个方面，提供了一种适用于电力物联网客户侧的隔离装置，所述装置包括：

[0007] 外网处理模块，用于对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文并发送至隔离交换模块；

[0008] 隔离交换模块，用于控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验，并在所述第二数据报文通过格式校验后，将所述第二数据报文发送至内网处理模块；

[0009] 内网处理模块，用于对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至

内网设备。

[0010] 优选地，其中所述装置还包括：

[0011] 内网处理模块，用于对接收的网内设备发送的第四数据报文进行加密处理，并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理，以获取第五数据报文并发送至隔离交换模块；

[0012] 隔离交换模块，用于控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第五数据报文进行格式校验，并在所述第五数据报文通过格式校验后，将所述第五数据报文发送至外网处理模块；

[0013] 外网处理模块，用于按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理，以获取第六数据报文并发送至外网设备。

[0014] 优选地，其中所述外网处理模块，还包括：

[0015] 格式校验单元，用于校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求；

[0016] 流量监测单元，用于监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

[0017] 优选地，其中所述隔离交换模块，控制外网处理模块和内网处理模块处于物理隔离的状态，包括：

[0018] 控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。

[0019] 优选地，其中所述隔离交换模块，利用如下方式进行格式校验，包括：

[0020] 校验待传输的数据报文的格式是否符合数据摆渡协议；其中，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

[0021] 优选地，其中所述内网处理模块，还包括：

[0022] 身份识别单元，用于根据解密后的第二数据报文，获取待接入的外网设备的身份信息，并根据待接入的外网设备的身份信息进行身份鉴别；其中，若身份鉴别成功，则允许所述待接入的网外设备接入电力物联网进行信息交互；若身份鉴别失败，则拒绝所述待接入的网外设备接入电力物联网进行信息交互；其中所述关键信息包括：外网设备的身份信息。

[0023] 优选地，其中所述身份识别单元，根据待接入的外网设备的身份信息进行身份鉴别，包括：

[0024] 根据待接入的网外设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；所述设备参数信息包括：外网设备的MAC地址、IP、通信协议、有效数据和数据格式；所述运行环境参数信息包括：外网设备的能耗变化、信号强度变化和流量变化。

[0025] 优选地，其中所述内网处理模块，还包括：

[0026] 访问控制单元，用于根据预设的访问控制策略对所述外网设备进行接入控制，确定所述网外设备访问权限；

[0027] 业务监控单元，用于对所述内网处理模块中的进程进行监测，并在出现异常事件时，及时对所述异常事件进行处理，以维护所述内网处理模块能够正常服务；

[0028] 日志记录单元，用于记录各类操作日志和通信日志；

[0029] 密钥证书导入单元，用于与电力统一密码基础设施对接，以实现外网设备密钥的分发和数字证书的申请及下发。

[0030] 根据本发明的另一个方面，提供了一种适用于电力物联网客户侧的隔离方法，所述方法包括：

[0031] 对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文；

[0032] 控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验；

[0033] 在所述第二数据报文通过格式校验后，对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备。

[0034] 优选地，其中所述方法还包括：

[0035] 对接收的网内设备发送的第四数据报文进行加密处理，并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理，以获取第五数据报文；

[0036] 控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第五数据报文进行格式校验；

[0037] 在所述第五数据报文通过格式校验后，按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理，以获取第六数据报文并发送至外网设备。

[0038] 优选地，其中所述方法还包括：

[0039] 在对接收的外网设备发送的第一数据报文进行解析之前，校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求；

[0040] 监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

[0041] 优选地，其中所述控制外网处理模块和内网处理模块处于物理隔离的状态，包括：

[0042] 控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。

[0043] 优选地，其中所述方法利用如下方式进行格式校验，包括：

[0044] 校验待传输的数据报文的格式是否符合数据摆渡协议；其中，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

[0045] 优选地，其中所述方法还包括：

[0046] 根据解密后的第二数据报文，获取待接入的外网设备的身份信息，并根据待接入的外网设备的身份信息进行身份鉴别；其中，若身份鉴别成功，则允许所述待接入的网外设备接入电力物联网进行信息交互；若身份鉴别失败，则拒绝所述待接入的网外设备接入电力物联网进行信息交互；其中所述关键信息包括：外网设备的身份信息。

[0047] 优选地，其中所述根据待接入的外网设备的身份信息进行身份鉴别，包括：

[0048] 根据待接入的网外设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；所述设备参数信息包括：外网设备的MAC地址、IP、通信协议、有效数据和数据格式；所述运行环境参数信息包括：外网设备的能耗变化、信号强度变化和流量变化。

[0049] 优选地，其中所述方法还包括：

[0050] 根据预设的访问控制策略对所述外网设备进行接入控制，确定所述网外设备访问权限；

[0051] 对所述内网处理模块中的进程进行监测，并在出现异常事件时，及时对所述异常事件进行处理，以维护所述内网处理模块能够正常服务；

[0052] 记录各类操作日志和通信日志；

[0053] 与电力统一密码基础设施对接，以实现外网设备密钥的分发和数字证书的申请及下发。

[0054] 本发明提供了一种适用于电力物联网客户侧的隔离装置及隔离方法，利用外网处理模块对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文；利用隔离交换模块控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验；并在所述第二数据报文通过格式校验后利用内网处理模块对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备，实现了开放的客户侧接入网络与电力物联网核心网络的安全隔离，能够有效防止核心业务系统被非法入侵。

附图说明

[0055] 通过参考下面的附图，可以更为完整地理解本发明的示例性实施方式：

[0056] 图1为根据本发明实施方式的适用于电力物联网客户侧的隔离装置100的结构示意图；

[0057] 图2为根据本发明实施方式的网络隔离装置的逻辑架构图；

[0058] 图3为根据本发明实施方式的身份鉴别的流程图；

[0059] 图4为根据本发明实施方式的隔离装置的读写逻辑图；

[0060] 图5为根据本发明实施方式的基于透明代理模式的应用层数据交换的原理图；

[0061] 图6为根据本发明实施方式的适用于电力物联网客户侧的隔离方法600的流程图。

具体实施方式

[0062] 现在参考附图介绍本发明的示例性实施方式，然而，本发明可以用许多不同的形式来实施，并且不局限于此处描述的实施例，提供这些实施例是为了详尽地且完全地公开本发明，并且向所属技术领域的技术人员充分传达本发明的范围。对于表示在附图中的示例性实施方式中的术语并不是对本发明的限定。在附图中，相同的单元/元件使用相同的附图标记。

[0063] 除非另有说明，此处使用的术语(包括科技术语)对所属技术领域的技术人员具有通常的理解含义。另外，可以理解的是，以通常使用的词典限定的术语，应当被理解为与其相关领域的语境具有一致的含义，而不应该被理解为理想化的或过于正式的意义。

[0064] 图1为根据本发明实施方式的适用于电力物联网客户侧的隔离装置100的结构示意图。如图1所示，本发明提供的适用于电力物联网客户侧的隔离装置实现了开放的客户侧接入网络与电力物联网核心网络的安全隔离，能够有效防止核心业务系统被非法入侵。本发明实施方式提供的适用于电力物联网客户侧的隔离装置100，包括：外网处理模块101、隔离交换模块102和内网处理摸103。

[0065] 优选地，所述外网处理模块101，用于对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文并发送至隔离交换模块。

[0066] 优选地，其中所述外网处理模块101，还包括：

[0067] 格式校验单元，用于校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求；

[0068] 流量监测单元，用于监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

[0069] 图2为根据本发明实施方式的微型网络隔离装置的逻辑架构图。如图2所示，在本发明的实施方式中，外网处理模块包括：外网通信子模块和外网业务处理子模块。

[0070] 其中，外网通信子模块包括：HPLC接口单元、WIFI接口单元和外网以太网接口单元；外网设备可通过WIFI、HPLC和以太网等方式实现网络接入。

[0071] 其中，外网业务处理子模块，主要包括外网数据收发单元、格式校验单元、流量监测单元、外网协议转换单元和外网升级管理单元。外网数据收发单元，用于接收外网设备发送的第一数据报文。格式校验单元用于校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求。流量监测单元，用于监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。外网协议转换单元，用于对所述第一数据报文进行解析，以获取关键信息，并对所述关键信息进行去传输层协议处理和按照数据摆渡协议对关键信息进行封装处理，以获取第二数据报文并发送至隔离交换模块。其中，所述关键信息包括：设备MAC信息、IP地址、设备发送的指令有效数据等信息。协议转换处理前的数据报文格式符合外网设备的通信协议，协议转换处理后的

数据符合数据摆渡协议。外网升级管理单元，主要负责对外网处理模块的软件进行升级维护。

[0072] 优选地，所述隔离交换模块102，用于控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验，并在所述第二数据报文通过格式校验后，将所述第二数据报文发送至内网处理模块。

[0073] 优选地，其中所述隔离交换模块102，控制外网处理模块和内网处理模块处于物理隔离的状态，包括：

[0074] 控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。

[0075] 优选地，其中所述隔离交换模块，利用如下方式进行格式校验，包括：

[0076] 校验待传输的数据报文的格式是否符合数据摆渡协议；其中，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

[0077] 如图2所示，在本发明的实施方式中，隔离交换模块，包括：隔离交换主控制器MCU和网络隔离子模块；网络隔离子模块包括：逻辑隔离单元和数据交换单元。

[0078] 其中，通过逻辑隔离单元控制外网处理模块和内网处理模块处理物理隔离的状态，并利用数据交换模块对第二数据报文进行格式校验和在所述第二数据报文通过格式校验后，将所述第二数据报文发送至内网处理模块的操作，完成数据传输。其中，利用隔离交换模块中的逻辑隔离单元控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态；其中，若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互，则所述逻辑隔离单元与另一个模块处于断开状态，待进行数据交互的一个模块完成数据交互且释放隔离控制信号后，另一个模块能够与所述逻辑隔离单元进行数据交互。在校验第二数据报文的格式是否符合数据摆渡协议时，若格式校验通过，则传输所述待传输的数据报文；若格式校验未通过，则拒绝所述待传输的数据报文。

[0079] 其中，隔离交换主控制器MCU包括至少3个CPU，其中两个CPU分别用于处理内网业务和外网业务，另一个CPU用于对系统配置和安全策略设置进行管理。

[0080] 优选地，所述内网处理模块103，用于对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备。

[0081] 优选地，其中所述内网处理模块，还包括：

[0082] 身份识别单元，用于根据解密后的第二数据报文，获取待接入的外网设备的身份信息，并根根据待接入的外网设备的身份信息进行身份鉴别；其中，若身份鉴别成功，则允许所述待接入的网外设备接入电力物联网进行信息交互；若身份鉴别失败，则拒绝所述待接入的网外设备接入电力物联网进行信息交互；其中所述关键信息包括：外网设备的身份信息。

[0083] 优选地，其中所述身份识别单元，根据待接入的外网设备的身份信息进行身份鉴别，包括：

[0084] 根据待接入的网外设备的身份信息按照预设的指纹生成策略，分别生成设备指纹

和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息；所述设备参数信息包括：外网设备的MAC地址、IP、通信协议、有效数据和数据格式；所述运行环境参数信息包括：外网设备的能耗变化、信号强度变化和流量变化。

[0085] 优选地，其中所述内网处理模块，还包括：

[0086] 访问控制单元，用于根据预设的访问控制策略对所述外网设备进行接入控制，确定所述网外设备访问权限；

[0087] 业务监控单元，用于对所述内网处理模块中的进程进行监测，并在出现异常事件时，及时对所述异常事件进行处理，以维护所述内网处理模块能够正常服务；

[0088] 日志记录单元，用于记录各类操作日志和通信日志；

[0089] 密钥证书导入单元，用于与电力统一密码基础设施对接，以实现外网设备密钥的分发和数字证书的申请及下发。

[0090] 如图2所示，在本发明的实施方式中，内网处理模块包括：内网通信子模块、密码运算子模块和内网业务处理子模块。其中，内网通信子模块，包括：电力专网接口单元和内网以太网接口单元。密码运算子模块，包括：密钥管理单元和算法运算单元。内网业务处理子模块，包括：内网数据收发单元、内网协议转换单元、身份识别单元、业务监控单元、访问就控制单元、密钥证书导入单元、日志记录单元和内网升级管理单元。

[0091] 在本发明的实施方式中，密钥管理单元，用于负责密钥全生命周期的安全管理。算法运算单元，用于进行国密SM1、SM2、SM3、SM4、SM7和SM9等密码算法的运算，对第二数据报文进行解密，以获取解密后的第二数据报文。内网处理模块在通过内网数据收发模块接收到隔离交换模块发送的第二报文数据后，通过算法运算模块对第二数据报文进行解密，利用内网协议转换单元按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文，并利用内网数据收发单元将协议转换和封装后的第三数据报文发送至内网设备。其中，协议转换处理前的数据报文格式符合符合数据摆渡协议；协议转换处理后的数据符合电力物联网专用通信协议。另外，内网处理模块还利用身份识别单元根据待接入的外网设备的身份信息进行身份鉴别；其中，若身份鉴别成功，则允许所述待计入的外网设备接入；若身份鉴别失败，则拒绝所述待接入的外网设备接入。具体地，身份鉴别的过程如图3所示，包括：

[0092] (1)感知设备或用户电器设备将其MAC、IP、通信协议P_r、有效数据D_v、数据格式D_f等设备参数信息发送给内网处理模块。内网处理模块分析其合法性和有效性，如果符合物联网环境准入要求，形成“设备指纹”D_{fp}，并将验证结果反馈给感知设备或用户电器设备。

[0093] (2)感知设备或用户电器设备将能耗变化Ec、信号强度变化Sc、流量变化Fc等环境参数信息，发送给内网处理模块。隔离装置生成“运行环境指纹”E_{fp}，并将接收结果反馈给感知设备或用户电器设备。

[0094] (3)内网处理模块将采集到的指纹信息传输至后台集中管理平台中，建立感知设备准入白名单W_1。

[0095] (4)当待接入的设备通过WIFI、HPLC或以太网方式接入隔离装置时，内网处理模块将再次根据待接入的网外设备的身份信息按照预设的指纹生成策略，分别生成设备指纹和运行环境指纹，并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹

和环境指纹进行比对，以进行身份鉴别；其中，所述身份信息包括：设备参数信息和运行环境参数信息。

[0096] 本发明实施方式的隔离装置主要通过双向身份认证、数据加密封装和数据完整性验证实现业务数据/指令加密保护。所述双向身份认证过程为：采用国密SM1、SM2和SM3等密码算法，基于挑战应答、数字证书签名验签等机制与主站业务应用系统进行双向身份认证。所述数据加密封装过程为：基于电力物联网专用安全通信协议实现对业务数据和控制指令的封装和数据加密。所述数据完整性验证过程为：通过消息鉴别码、数字签名及数据时效性验证保证业务数据和控制指令的完整性。

[0097] 在本发明的实施方式中，访问控制单元，用于根据预设的访问控制策略对所述外网设备进行接入控制，确定所述外网设备访问权限。内网升级管理单元，用于对内网处理模块的软件进行升级维护。密钥证书导入单元，负责与电力统一密码基础设施对接，实现外网设备密钥的分发和数字证书的申请及下发。日志记录单元，用于记录各类操作日志、通信日志等信息，供事后分析追溯。

[0098] 优选地，其中所述装置还包括：

[0099] 内网处理模块，用于对接收的网内设备发送的第四数据报文进行加密处理，并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理，以获取第五数据报文并发送至隔离交换模块；

[0100] 隔离交换模块，用于控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第五数据报文进行格式校验，并在所述第五数据报文通过格式校验后，将所述第五数据报文发送至外网处理模块；

[0101] 外网处理模块，用于按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理，以获取第六数据报文并发送至外网设备。

[0102] 在本发明的实施方式中，在从内网向外网传递数据时，内网处理模块，还用于利用算法运算单元对接收的网内设备发送的第四数据报文进行加密处理，并利用内网协议转换单元按照隔离交换模块的数据摆渡协议对加密后的第四数据进行协议格式转换处理，以获取第五数据报文，并利用内网数据收发单元发送至隔离交换模块。其中，协议转换处理前的数据报文符合电力物联网专用通信协议，协议转换处理后的数据报文符合隔离交换模块的数据摆渡协议。隔离交换模块，还用于控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第五数据报文进行格式校验，并在所述第五数据报文通过格式校验后，将所述第五数据报文发送至外网处理模块。外网处理模块，还用于利用外网协议转换单元按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理，以获取第六数据报文并利用外网数据收发单元发送至外网设备。其中，协议转换处理前的数据报文符合数据摆渡协议；协议转换处理后的数据报文符合外网设备的通信协议。

[0103] 图4为根据本发明实施方式的隔离装置的读写逻辑图。如图4所示，本发明实施方式的隔离装置主要采用内外网读写通道独立、信息摆渡机制实现内外网的安全隔离和信息安全交互。所述内外网处理模块之间交换的对象不是IP数据报文，而是经专用内部协议封装的应用层数据报文，任意原始IP数据报文不可能通过该通道。所示隔离装置能够在网络的物理层将两个网络或主机彻底断开，确保在同一时刻外网接口与内网接口物理切断的情况下，负责“摆渡”安全的网络数据。如果一端网络通过隔离装置交换数据，则隔离装置与另

一端网络是处于断开状态。等该端进行完数据交互并释放了隔离控制信号后，另一端才能与隔离装置进行信息交互。两端的数据都会存入隔离装置的缓冲区内，写缓冲区前查看状态，状态允许时将数据写入缓冲区，否则等待。读缓冲区前查看状态，状态允许时读取缓冲区中的数据，否则等待。数据具体读写过程为：内网处理模块和外网处理模块如果要从一端网络发送数据到另一端网络，数据会写到发送FIFO模块中，这时会关闭FIFO接收模块，只有写通道处于连通状态；如果要从另一个处理单元读取数据，数据会写到FIFO接收模块，这时会关闭FIFO发送模块，只有读通道处于连通状态。

[0104] 图5为根据本发明实施方式的基于透明代理模式的应用层数据交换的原理图。如图5所示，在本发明的实施方式中，隔离装置主要采用透明代理模式实现应用层数据交换。所述透明代理包括代理引擎和代理存根两部分，分别位于不同的网络处理单元上。所述代理存根主要用于网络连接请求检查。所述代理引擎主要用于调用传输接口，将外部网络返回的信息通过高速交换通道交换到网络处理单元。所述代理引擎和代理存根基于高速交换通道和专用协议进行对话和数据通信。

[0105] 本发明实施方式的隔离装置在数据机密性和完整性保护方面，隔离装置主要通过双向身份认证、数据加密封装和数据完整性验证实现业务数据/指令加密保护。所述双向身份认证过程为：采用国密SM1、SM2和SM3等密码算法，基于挑战应答、数字证书签名验签等机制与主站业务应用系统进行双向身份认证。所述数据加密封装过程为：基于电力物联网专用安全通信协议实现对业务数据和控制指令的封装和数据加密。所述数据完整性验证过程为：通过消息鉴别码、数字签名及数据时效性验证保证业务数据和控制指令的完整性。

[0106] 本发明实施方式的隔离装置实现了开放的客户侧接入网络与电力物联网核心网络的安全隔离，能够有效防止核心业务系统被非法入侵。

[0107] 图6为根据本发明实施方式的适用于电力物联网客户侧的隔离方法600的流程图。如图6所示，本发明实施方式提供的适用于电力物联网客户侧的隔离方法600，从步骤601处开始，在步骤601对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文。

[0108] 优选地，其中所述方法还包括：

[0109] 在对接收的外网设备发送的第一数据报文进行解析之前，校验所述第一数据报文的报文格式是否符合电力物联网准入要求；其中，若校验通过，则对所述第一数据报文进行解析；若校验不通过，则拒绝所述外网设备的数据传输请求；

[0110] 监测外网设备的数据流量是否符合电力物联网准入要求，是否存在异常数据流；其中，若存在异常数据流，则拒绝所述外网设备的数据传输请求；若不存在异常数据流，则允许所述外网设备的数据传输请求。

[0111] 在步骤602，控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验。

[0112] 在步骤603，在所述第二数据报文通过格式校验后，对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备。

[0113] 优选地，其中所述方法还包括：

[0114] 根据解密后的第二数据报文，获取待接入的外网设备的身份信息，并根据待接入

的外网设备的身份信息进行身份鉴别;其中,若身份鉴别成功,则允许所述待接入的网外设备接入电力物联网进行信息交互;若身份鉴别失败,则拒绝所述待接入的网外设备接入电力物联网进行信息交互;其中所述关键信息包括:外网设备的身份信息。

[0115] 优选地,其中所述根据待接入的外网设备的身份信息进行身份鉴别,包括:

[0116] 根据待接入的网外设备的身份信息按照预设的指纹生成策略,分别生成设备指纹和运行环境指纹,并将所述设备指纹和运行环境指纹和预设的设备准入白名单中的设备指纹和环境指纹进行比对,以进行身份鉴别;其中,所述身份信息包括:设备参数信息和运行环境参数信息;所述设备参数信息包括:外网设备的MAC地址、IP、通信协议、有效数据和数据格式;所述运行环境参数信息包括:外网设备的能耗变化、信号强度变化和流量变化。

[0117] 优选地,其中所述方法还包括:

[0118] 对接收的网内设备发送的第四数据报文进行加密处理,并按照数据摆渡协议对加密后的第四数据进行协议格式转换处理,以获取第五数据报文;

[0119] 控制外网处理模块和内网处理模块处于物理隔离的状态,对所述第五数据报文进行格式校验;

[0120] 在所述第五数据报文通过格式校验后,按照外网设备的通信协议对所述第五数据报文进行协议格式转换处理,以获取第六数据报文并发送至外网设备。

[0121] 优选地,其中所述控制外网处理模块和内网处理模块处于物理隔离的状态,包括:

[0122] 控制所述外网处理模块与内网处理模块在同一时刻下处于物理切断的状态;其中,若所述外网处理模块和内网处理模块中的一个模块正在与逻辑隔离单元进行数据交互,则所述逻辑隔离单元与另一个模块处于断开状态,待进行数据交互的一个模块完成数据交互且释放隔离控制信号后,另一个模块能够与所述逻辑隔离单元进行数据交互。

[0123] 优选地,其中所述方法利用如下方式进行格式校验,包括:

[0124] 校验待传输的数据报文的格式是否符合数据摆渡协议;其中,若格式校验通过,则传输所述待传输的数据报文;若格式校验未通过,则拒绝所述待传输的数据报文。

[0125] 优选地,其中所述方法还包括:

[0126] 根据预设的访问控制策略对所述外网设备进行接入控制,确定所述网外设备访问权限;

[0127] 对所述内网处理模块中的进程进行监测,并在出现异常事件时,及时对所述异常事件进行处理,以维护所述内网处理模块能够正常服务;

[0128] 记录各类操作日志和通信日志;

[0129] 与电力统一密码基础设施对接,以实现外网设备密钥的分发和数字证书的申请及下发。

[0130] 本发明的实施例的适用于电力物联网客户侧的隔离方法600与本发明的另一个实施例的适用于电力物联网客户侧的隔离装置100相对应,在此不再赘述。

[0131] 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,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。

[0132] 通常地,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。

[0133] 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。

[0134] 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。

[0135] 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。

[0136] 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。

[0137] 最后应当说明的是: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当理解: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保护范围之内。


100
外网处理模块101
隔离交换模块102
内网处理摸103

图1

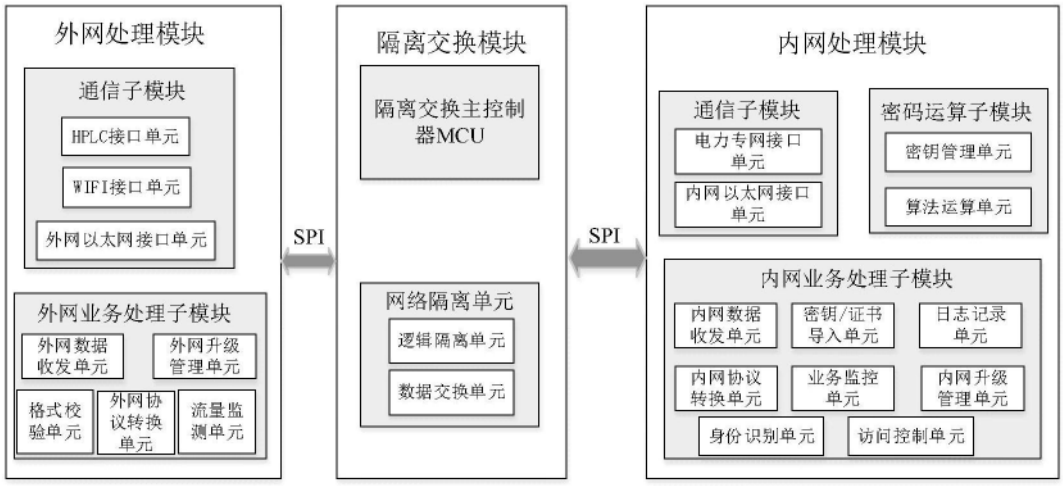

外网处理模块
通信子模块
HPLC接口单元
WIFI接口单元
外网以太网接口单元
外网业务处理子模块
外网数据收发单元
外网升级管理单元
格式校验单元
外网协议转换单元
流量监测单元
SPI
隔离交换模块
隔离交换主控制器MCU
网络隔离单元
逻辑隔离单元
数据交换单元
SPI
内网处理模块
通信子模块
电力专网接口单元
内网以太网接口单元
密码运算子模块
密钥管理单元
算法运算单元
内网业务处理子模块
内网数据收发单元
密钥/证书导入单元
日志记录单元
内网协议转换单元
业务监控单元
内网升级管理单元
身份识别单元
访问控制单元

图2

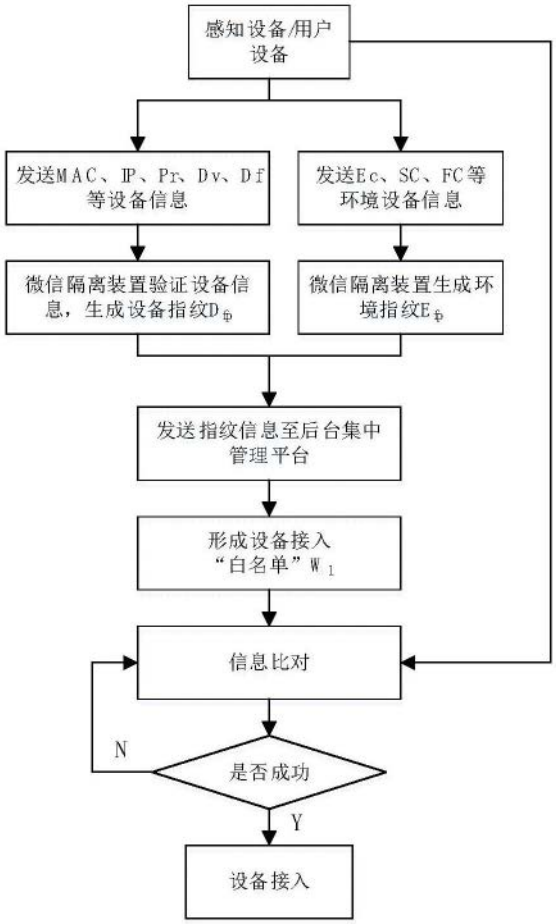

感知设备/用户设备
发送MAC、IP、Pr、Dv、Df等设备信息
发送Ec、SC、FC等环境设备信息
微信隔离装置验证设备信息，生成设备指纹D_{ip}
微信隔离装置生成环境指纹E_{ip}
发送指纹信息至后台集中管理平台
形成设备接入“白名单”W_1
信息比对
是否成功
N
Y
设备接入

图3

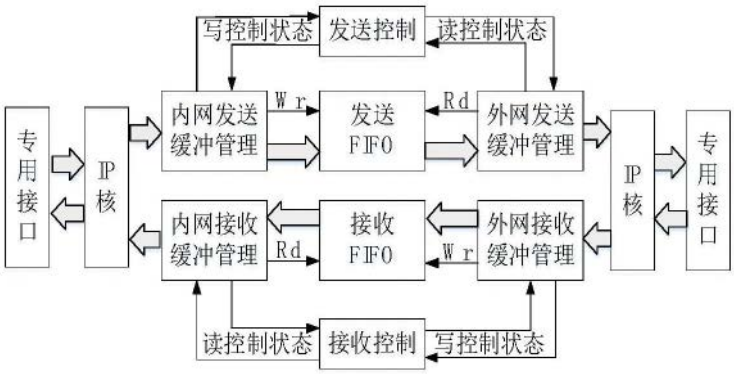

写控制状态
发送控制
读控制状态
专用接口
IP核
内网发送缓冲管理
Wr
发送FIFO
Rd
外网发送缓冲管理
IP核
专用接口
内网接收缓冲管理
Rd
接收FIFO
Wr
外网接收缓冲管理
读控制状态
接收控制
写控制状态

图4

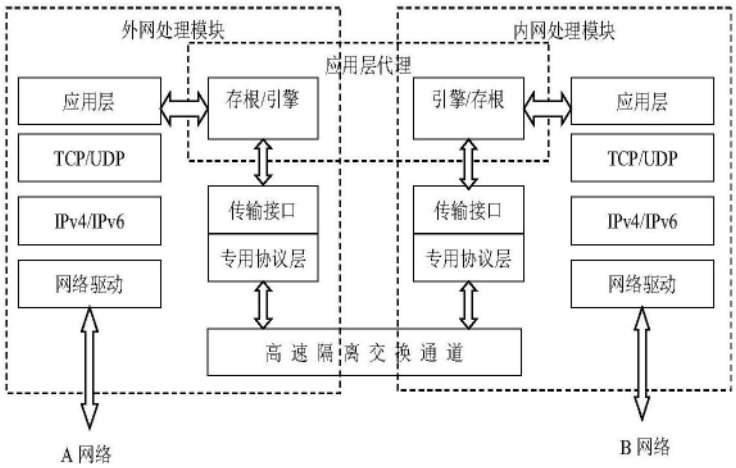

外网处理模块
内网处理模块
应用层代理
应用层
存根/引擎
引擎/存根
应用层
TCP/UDP
TCP/UDP
IPv4/IPv6
传输接口
传输接口
IPv4/IPv6
网络驱动
专用协议层
专用协议层
网络驱动
高速隔离交换通道
A网络
B网络

图5

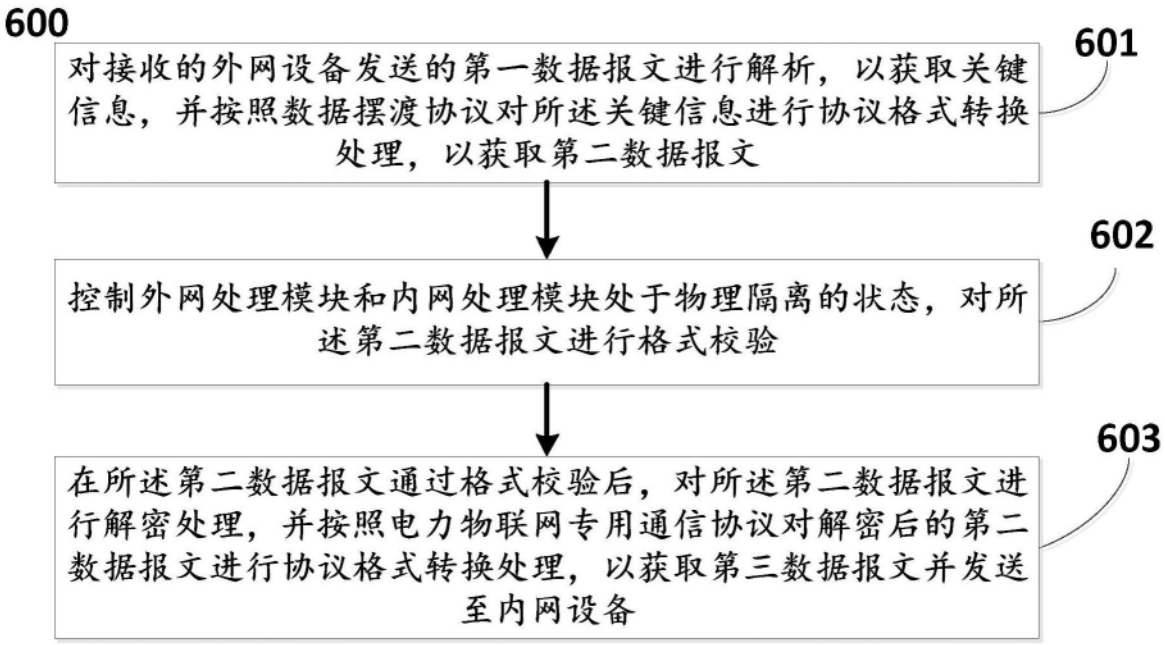

600
对接收的外网设备发送的第一数据报文进行解析，以获取关键信息，并按照数据摆渡协议对所述关键信息进行协议格式转换处理，以获取第二数据报文
601
控制外网处理模块和内网处理模块处于物理隔离的状态，对所述第二数据报文进行格式校验
602
在所述第二数据报文通过格式校验后，对所述第二数据报文进行解密处理，并按照电力物联网专用通信协议对解密后的第二数据报文进行协议格式转换处理，以获取第三数据报文并发送至内网设备
603

图6