(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112367664 B
(45)授权公告日 2024.03.01

(21)申请号 202011008057.8

(22)申请日 2020.09.23

(65)同一申请的已公布的文献号
申请公布号 CN 112367664 A

(43)申请公布日 2021.02.12

(73)专利权人 国家电网有限公司
地址 100031 北京市西城区西长安街86号
专利权人 中国电力科学研究院有限公司

(72)发明人 李保丰 杜新纲 徐英辉 翟峰 葛得辉 梁晓兵 周晖 许斌 彭楚宁 冯占成 王齐 付义伦 刘书勇 任博 韩文博 孔令达

(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.
H04W 12/06(2021.01)
H04W 12/122(2021.01)
H04W 12/106(2021.01)
H04W 12/0431(2021.01)
H04W 12/02(2009.01)
H04W 12/03(2021.01)
H04L 9/40(2022.01)

(56)对比文件
CN 101753312 A,2010.06.23
CN 103095696 A,2013.05.08
CN 104333547 A,2015.02.04
CN 107172008 A,2017.09.15
CN 109257327 A,2019.01.22
CN 109450854 A,2019.03.08
CN 110753344 A,2020.02.04
CN 110798309 A,2020.02.14
李保丰.《适用于智能电表双向互动系统的安全通信协议》.《电力系统自动化》.2016,全文.
翟峰.《电力采集系统安全防护和密码管理体系》.《网络空间安全》.2018,全文.

审查员 焦伟

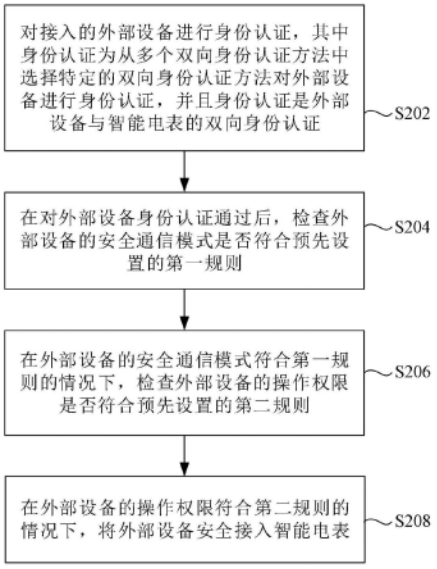
权利要求书3页 说明书14页 附图8页

(54)发明名称

一种外部设备安全接入智能电表的方法及装置

(57)摘要

本申请公开了一种外部设备安全接入智能电表的方法及装置,其中,该方法包括:对接入的外部设备进行身份认证,其中所述身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对所述外部设备进行身份认证,并且所述身份认证是所述外部设备与智能电表的双向身份认证;在对所述外部设备身份认证通过后,检查所述外部设备的安全通信模式是否符合预先设置的第一规则;在所述外部设备的安全通信模式符合所述第一规则的情况下,检查所述外部设备的操作权限是否符合预先设置的第二规则;以及在所述外部设备的操作权限符合第二规则的情况下,将所述外部设备安全接入智能电表。



CN 112367664 B

1.一种外部设备安全接入智能电表的方法,其特征在于,包括:

对接入的外部设备进行身份认证,其中所述身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对所述外部设备进行身份认证,并且所述身份认证是所述外部设备与智能电表的双向身份认证;

在对所述外部设备身份认证通过后,检查所述外部设备的安全通信模式是否符合预先设置的第一规则;

在所述外部设备的安全通信模式符合所述第一规则的情况下,检查所述外部设备的操作权限是否符合预先设置的第二规则;以及

在所述外部设备的操作权限符合第二规则的情况下,将所述外部设备安全接入智能电表;

对接入的外部设备进行身份认证,包括:

在所述外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对所述外部设备进行身份认证;或者

在所述外部设备为手机时,基于SM2非对称密码算法对所述外部设备进行身份认证;或者

在所述外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对所述外部设备进行身份认证;

在所述外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对所述外部设备进行身份认证,包括:

在所述外部设备发送会话密钥协商信息数据报文给智能电表后,组织命令发送到管理模组;

利用所述管理模组执行所述会话密钥协商信息数据报文,当执行成功后,将掌机返回信息组成应用连接请求的认证响应信息数据报文发送至所述外部设备,其中所述手机返回信息为将服务器随机数以及服务器签名信息;以及

利用外部设备对所述服务器随机数以及服务器签名信息进行校验;

在所述外部设备为手机时,基于SM2非对称密码算法对所述外部设备进行身份认证,包括:

利用管理模组接收所述外部设备发送的第一数据报文,验证所述第一数据报文中的手机证书的有效性,其中所述第一数据报文为将所述外部设备产生的手机随机数、手机证书和签名信息进行打包的报文;

在所述手机证书有效的情况下,利用所述管理模组的嵌入式控制模块通过所述手机证书验证所述第一数据报文中的签名信息是否有效;以及

在所述第一数据报文中的签名信息通过所述手机证书验证的情况下,利用所述管理模组的嵌入式控制模块将手机返回信息组成认证请求的响应信息第一数据报文发送给所述外部设备,其中所述手机返回信息为随机数密文、管理模组序列号、管理模组证书和签名信息;

在所述外部设备为手机时,基于SM2非对称密码算法对所述外部设备进行身份认证,还包括:

在所述外部设备获得所述认证请求的响应信息第一数据报文后,所述外部设备验证所

述管理模组证书的有效性;

在所述管理模组证书有效的情况下,所述外部设备利用所述管理模组证书验证所述第一数据报文中的签名信息;

在所述第一数据报文中的签名信息通过所述管理模组证书验证的情况下,确定会话密钥包和会话确认数据,并且所述外部设备将所述会话确认数据组成的认证确认信息第一数据报文发送给管理模组;以及

在所述管理模组获得所述认证确认信息第一数据报文后,验证所述会话确认数据;

在所述外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对所述外部设备进行身份认证,包括:

在所述外部设备发送第二数据报文给智能电表后,读取所述第二数据报文信息,其中所述第二数据报文信息为所述外部设备的序列号信息以及密钥版本信息;以及

根据所述第二数据报文信息,利用管理模组组织会话协商数据计算指令发送至嵌入式控制模块;

利用所述嵌入式控制模块判断所述外部设备的序列号是否在白名单中并进行计算,确定第一随机数,将第一红外认证请求组数据报文发送至所述外部设备,其中所述第一红外认证请求组数据报文是将所述第一数据报文进行封装得到;

在所述外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对所述外部设备进行身份认证,包括:

在所述外部设备获得所述第一红外认证请求组数据报文后,所述外部设备根据第一随机数,确定第一随机数密文以及第二随机数信息;

所述外部设备将红外认证请求的响应信息数据报文发送给管理模组,其中所述红外认证请求的响应信息数据报文是将所述第一随机数密文以及所述第二随机数信息组成;

利用管理模组对所述第一随机数密文进行校验,对第二随机数进行加密,确定第二随机数密文;

将第二红外认证请求组数据报文发送至所述外部设备,其中所述第二红外认证请求组数据报文是将所述第二随机数密文进行封装得到;

在所述外部设备获得第二红外认证请求组数据报文后,所述外部设备对所述第二随机数密文进行解密,确定帧数据报文;

外部设备与主站通信必须经过智能电表转发,智能电表与外部设备和主站采用不同的物理通信接口进行通信,实现外部设备与主站的通信接口硬隔离,外部设备与主站通信的报文必须经过电能表进行报文过滤以及转加密。

2.根据权利要求1所述的方法,其特征在于,所述第一规则包括智能电表的安全通信模式以及所述智能电表的数据项以及数据项对应的每项操作,并且所述智能电表的安全通信模式包括一级安全通信模式、二级安全通信模式、三级安全通信模式以及四级安全通信模式,所述一级安全通信模式为纯明文方式、所述二级安全通信模式为明文+消息鉴别码方式、所述三级安全通信模式为纯密文以及所述四级安全通信模式为密文加消息鉴别码方式;以及

所述第二规则为针对不同的外部设备选择不同的操作权项。

3.根据权利要求2所述的方法,其特征在于,检查所述外部设备的安全通信模式是否符

合预先设置的第一规则,包括:

在所述数据项为电表号时,以所述一级安全通信模式或者所述二级安全通信模式或者所述三级安全通信模式或者所述四级安全通信模式进行读取;

在所述数据项为电量时,以所述二级安全通信模式或者所述三级安全通信模式或者所述四级安全通信模式进行读取;以及

在所述数据项为跳闸时,以所述四级安全通信模式进行读取。

4.根据权利要求2所述的方法,其特征在于,检查所述外部设备的操作权限是否符合预先设置的第二规则,包括:

在所述外部设备为掌机时,对所述外部设备执行所有操作;或者

在所述外部设备为手机时,对所述外部设备执行读取和设置操作;以及

在所述外部设备为智能家居时,对所述外部设备中有限的数据项进行转发。

5.根据权利要求4所述的方法,其特征在于,检查所述外部设备的操作权限是否符合预先设置的第二规则,还包括:

当通信数据不符合操作权限时,将所述通信数据过滤掉,不转发给主站。

一种外部设备安全接入智能电表的方法及装置

技术领域

[0001] 本申请涉及智能电表领域,特别是涉及一种外部设备安全接入智能电表的方法及装置。

背景技术

[0002] 能源互联网是新一代能源系统和互联网技术的深度融合及发展,是智能电网发展的更高阶段。随着能源互联网建设的推进,智能电网逐渐由原来的封闭系统走向开放、共享,围绕电网将会产生非常多的新业务和新应用。新一代智能电能表作为能源互联网的末梢设备,未来将成为能源互联网与外部设备交互的入口节点,通信接口更加丰富,蓝牙等无线通信接口的引入,在方便业务的同时,也使得攻击者获取攻击电表的攻击途径更为容易。随着能源互联网的发展,未来将会有很多不是电网资产的非受控设备接入电表,通过电表与电网进行互动,实现“能源流、业务流、数据流”的交互。如何保证接入智能电能表的设备的身份合法性,避免攻击者伪造终端接入电能表,进而以电能表为跳板向电力系统主站发起攻击,引发大规模安全事故?如何保证智能电能表与接入设备之间数据传输的机密性、完整性,避免攻击者篡改两者之间的交互数据,诱使主站异常操作引发大规模断电等安全事故?如何避免攻击者以接入设备为跳板通过智能电能表向主站发动网络攻击,造成主站异常,影响正常电力系统业务开展等安全事故?这些安全风险都是智能电能表亟需解决的技术问题。

[0003] 针对上述的现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题,目前尚未提出有效的解决方案。

发明内容

[0004] 本公开的实施例提供了一种外部设备安全接入智能电表的方法及装置,以至少解决现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。

[0005] 根据本公开实施例的一个方面,提供了一种外部设备安全接入智能电表的方法,包括:对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0006] 根据本公开实施例的另一个方面,还提供了一种存储介质,存储介质包括存储的程序,其中,在程序运行时由处理器执行以上任意一项所述的方法。

[0007] 根据本公开实施例的另一个方面,还提供了一种外部设备安全接入智能电表的装置,包括:身份认证模块,用于对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;第一检查模块,用于在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;第二检查模块,用于在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及安全接入模块,用于在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0008] 根据本公开实施例的另一个方面,还提供了一种外部设备安全接入智能电表的装置,包括:处理器;以及存储器,与处理器连接,用于为处理器提供处理以下处理步骤的指令:对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0009] 在本公开实施例中,基于密码技术设计专用身份认证协议,实现智能表与外部接入设备的双向身份认证并同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护,同时针对外部接入设备与主站的报文交互,由智能电能表对外部接入设备向主站发送的数据报文进行报文过滤,对于不合符操作权限的报文及非法的报文进行阻断,同时通过将与外部接入设备的通信接口和与主站的通信接口进行物理隔离,从而避免外部接入设备直接向主站发动网络攻击。仅为解决了现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。

附图说明

[0010] 此处所说明的附图用来提供对本公开的进一步理解,构成本申请的一部分,本公开的示意性实施例及其说明用于解释本公开,并不构成对本公开的不当限定。在附图中:

[0011] 图1是用于实现根据本公开实施例1所述的方法的计算设备的硬件结构框图;

[0012] 图2是根据本公开实施例1的第一个方面所述的外部设备安全接入智能电表的方法的流程示意图;

[0013] 图3是根据本公开实施例1的第以个方面所述的与不同类型的外部设备进行连接的示意图;

[0014] 图4是根据本公开实施例1的第一个方面所述的智能电表与掌机进行双向身份认证的流程示意图;

[0015] 图5是根据本公开实施例1的第一个方面所述的智能电表与手机进行双向身份认证的流程示意图;

[0016] 图6是根据本公开实施例1的第一个方面所述的智能电表与智能家居进行双向身份认证的流程示意图;

[0017] 图7是根据本公开实施例1的第一个方面所述的智能电能表与外部接入设备报文加密保护的流程示意图；

[0018] 图8是根据本公开实施例1的第一个方面所述的智能电能表对外部设备发送主站报文过滤转发的流程示意图；

[0019] 图9是根据本公开实施例1的第一个方面所述的手机外部设备安全接入智能电表的的流程示意图；

[0020] 图10是根据本公开实施例2所述的外部设备安全接入智能电表的装置的示意图；以及

[0021] 图11是根据本公开实施例3所述的外部设备安全接入智能电表的装置的示意图。

具体实施方式

[0022] 为了使本技术领域的人员更好地理解本公开的技术方案，下面将结合本公开实施例中的附图，对本公开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公开一部分的实施例，而不是全部的实施例。基于本公开中的实施例，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，都应当属于本公开保护的范围。

[0023] 需要说明的是，本公开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，以便这里描述的本公开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。

[0024] 实施例1

[0025] 根据本实施例，还提供了一种外部设备安全接入智能电表的方法实施例，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。

[0026] 本实施例所提供的方法实施例可以在智能电表或者类似的计算设备中执行。图1示出了一种用于实现外部设备安全接入智能电表的方法的计算设备的硬件结构框图。如图1所示，计算设备可以包括一个或多个处理器(处理器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)、用于存储数据的存储器、以及用于通信功能的传输装置。除此以外，还可以包括：显示器、输入/输出接口(I/O接口)、通用串行总线(USB)端口(可以作为I/O接口的端口中的一个端口被包括)、网络接口、电源和/或相机。本领域普通技术人员可以理解，图1所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算设备还可包括比图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。

[0027] 应当注意到的是上述一个或多个处理器和/或其他数据处理电路在本文中通常可以被称为“数据处理电路”。该数据处理电路可以全部或部分的体现为软件、硬件、固件或其他任意组合。此外，数据处理电路可为单个独立的处理模块，或全部或部分的结合到计算设

备中的其他元件中的任意一个内。如本公开实施例中所涉及到的,该数据处理电路作为一种处理器控制(例如与接口连接的可变电阻终端路径的选择)。

[0028] 存储器可用于存储应用软件的软件程序以及模块,如本公开实施例中的外部设备安全接入智能电表的方法对应的程序指令/数据存储装置,处理器通过运行存储在存储器内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的应用程序的外部设备安全接入智能电表的方法。存储器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,存储器可进一步包括相对于处理器远程设置的存储器,这些远程存储器可以通过网络连接至计算设备。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。

[0029] 传输装置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计算设备的通信供应商提供的无线网络。在一个实例中,传输装置包括一个网络适配器(Network Interface Controller,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,传输装置可以为射频(Radio Frequency,RF)模块,其用于通过无线方式与互联网进行通讯。

[0030] 显示器可以例如触摸屏式的液晶显示器(LCD),该液晶显示器可使得用户能够与计算设备的用户界面进行交互。

[0031] 此处需要说明的是,在一些可选实施例中,上述图1所示的计算设备可以包括硬件元件(包括电路)、软件元件(包括存储在计算机可读介质上的计算机代码)、或硬件元件和软件元件两者的结合。应当指出的是,图1仅为特定具体实例的一个实例,并且旨在示出可存在于上述计算设备中的部件的类型。

[0032] 根据本实施例的第一个方面,提供了一种外部设备安全接入智能电表的方法。图2示出了该方法的流程示意图,参考图2所示,该方法包括:

[0033] S202:对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;

[0034] S204:在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;

[0035] S206:在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及

[0036] S208:在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0037] 具体地,在本实施例中,对接入的外部设备进行身份认证,对需要接入智能电能表的外部设备进行身份的真实性、合法性检查,身份合法且真实有效才允许接入电能表。检查外部身份真实性、合法性的方法是采用身份认证,针对不同的外部设备采用的身份认证方法也不尽相同。智能电表与外部设备进行连接,根据外部设备发送的协议报文中的设备类型,判断外部设备的类型。智能电能表上电启动完成后,收到外部设备发送的698协议中的应用连接建立请求,根据协议报文中的设备类型的不同,进入不同的安全接入认证处理流程。

[0038] 进一步地,参考图3所示,针对不同的外部设备采用的身份认证方法身是从从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证。同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护。身份认证主要分为三类:第一类是基于SM1对称密码算法实现,采用这种方式的外部设备主要有掌机、采集系统主站、检测软件等;第二类是基于SM2非对称密码算法实现的,采用这种方式的外部设备主要有用户手机;第三类是基于SM4对称密码算法实现的,采用这种方式的外部设备主要有智能家居、外置断路器、扩展模组等。

[0039] 进一步地,在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则。预先设置的规则为电能表的安全通信模式有以下几种:一是纯明文方式;二是明文+消息鉴别码方式;三是纯密文方式;四是密文+消息鉴别码方式,安全等级由低到高分别为一级、二级、三级、四级。外部设备实际安全通信模式的安全等级不能低于预置的安全通信模式,例如:若电量抄读的预置安全模式是二级即明文+消息鉴别码方式,则电能表可以允许外部设备以明文+消息鉴别码方式(二级)、纯密文方式(三级)、密文+消息鉴别码方式(四级)三种方式进行,但不能以纯明文方式(一级)进行。

[0040] 进一步地,在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则。外部设备的操作权限符合电能表内预置的规则才允许接入电能表。具体实现方式如下:电能表内预置的一个不同外部设备的操作权限表,例如主站和掌机的操作权限是可以对电能表进行所有操作;手机仅能对有限的数据项进行读取和设置;智能家居仅会对有限的数据项进行转发等。不符合操作权限的通信数据就会被电能表过滤掉,对于需要转发给主站的数据会被电表隔离起来,不会转发给主站。在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0041] 从而,基于密码技术设计专用身份认证协议,实现智能表与外部接入设备的双向身份认证并同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护,同时针对外部接入设备与主站的报文交互,由智能电能表对外部接入设备向主站发送的数据报文进行报文过滤,对于不合符操作权限的报文及非法的报文进行阻断,同时通过将与外部接入设备的通信接口和与主站的通信接口进行物理隔离,从而避免外部接入设备直接向主站发动网络攻击。仅为解决了现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。

[0042] 可选地,对接入的外部设备进行身份认证,包括:在外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对外部设备进行身份认证;或者在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证;或者在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证。

[0043] 可选地,第一规则包括智能电表的安全通信模式以及智能电表的数据项以及数据项对应的每项操作,并且智能电表的安全通信模式包括一级安全通信模式、二级安全通信模式、三级安全通信模式以及四级安全通信模式,一级安全通信模式为纯明文方式、二级安全通信模式为明文+消息鉴别码方式、三级安全通信模式为纯密文以及四级安全通信模式为密文加消息鉴别码方式;以及第二规则为针对不同的外部设备选择不同的操作权项。

[0044] 可选地,检查外部设备的安全通信模式是否符合预先设置的第一规则,包括:在数

据项为电表号时,以一级安全通信模式或者二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;在数据项为电量时,以二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;以及在数据项为跳闸时,以四级安全通信模式进行读取。

[0045] 具体地,参考图4所示,在外部设备为掌机的情况下,读取芯片序列号报文、当前计数器报文以及管理芯表号报文,其中芯片序列号报文、当前计数器报文以及管理芯表号报文都是嵌入式控制模块ESAM的报文,嵌入式控制模块安装在智能电表中;以及组织芯片序列号报文、当前计数器报文以及管理芯表号报文,并将组织好的芯片序列号报文、当前计数器报文以及管理芯表号报文发送至掌机。

[0046] 可选地,检查外部设备的操作权限是否符合预先设置的第二规则,包括:在外部设备为掌机或者主站时,对外部设备执行所有操作;或者在外部设备为手机时,对外部设备执行读取和设置操作;以及在外部设备为智能家居时,对外部设备中有限的数据项进行转发。

[0047] 可选地,检查外部设备的操作权限是否符合预先设置的第二规则,还包括:当通信数据不符合操作权限时,将通信数据过滤掉,不转发给主站。

[0048] 可选地,在外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对外部设备进行身份认证,包括:在外部设备发送会话密钥协商信息数据报文给智能电表后,组织命令发送到管理模组;利用管理模组执行会话密钥协商信息数据报文,当执行成功后,将掌机返回信息组成应用连接请求的认证响应信息数据报文发送至外部设备,其中手机返回信息为将服务器随机数以及服务器签名信息;以及利用外部设备对服务器随机数以及服务器签名信息进行校验。

[0049] 具体地,参考图4所示,基于SM1对称密码算法的身份认证流程如下:

[0050] 步骤a:外部设备下发会话密钥协商信息数据报文M1_DATA和MAC1给电能表;

[0051] 步骤b:电能表获得会话密钥协商信息数据报文M1_DATA和MAC1后,组织命令发送到管理模组ESAM中;

[0052] 步骤c:管理模组ESAM执行失败,返回错误码,跳转至步骤e);执行成功,则返回服务器随机数和服务器签名信息;电能表将返回信息组成应用连接请求的认证响应信息数据报文发送给客户端;

[0053] 步骤d:客户端对返回的服务器随机数和服务器签名信息进行校验。

[0054] 步骤e:流程结束。

[0055] 在外部设备将会话协商数据密文M1_DATA和第一消息认证码MAC1发送至智能电表后,检验第一消息认证码MAC1,解密会话协商数据密文M1_DATA,得到第二随机数R2,其中会话协商数据密文M1_DATA是将第一随机数R1进行签名得到;将第二随机数R2和第二消息验证码MAC2发送至掌机,利用密码机校验第二消息验证码MAC2,并利用掌机保存二随机数R2;以及确定掌机与智能电表之间的会话密钥。

[0056] 可选地,在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证,包括:利用管理模组接收外部设备发送的第一数据报文,验证第一数据报文中的手机证书的有效性,其中第一数据报文为将外部设备产生的手机随机数、手机证书和签名信息进行打包的报文;在手机证书有效的情况下,利用管理模组的嵌入式控制模块通过手机证书验证第一数据报文中的签名信息是否有效;以及在第一数据报文中的签名信息通过手机证

书验证的情况下,利用管理模组的嵌入式控制模块将手机返回信息组成认证请求的响应信息第一数据报文发送给外部设备,其中手机返回信息为随机数密文、管理模组序列号、管理模组证书和签名信息。

[0057] 可选地,在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证,还包括:在外部设备获得认证请求的响应信息第一数据报文后,外部设备验证管理模组证书的有效性;在管理模组证书有效的情况下,外部设备利用管理模组证书验证第一数据报文中的签名信息;在第一数据报文中的签名信息通过管理模组证书验证的情况下,确定会话密钥包和会话确认数据,并且外部设备将会话确认数据组成的认证确认信息第一数据报文发送给管理模组;以及在管理模组获得认证确认信息第一数据报文后,验证会话确认数据。

[0058] 可选地,在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证,包括:在外部设备发送第二数据报文给智能电表后,读取第二数据报文信息,其中第二数据报文信息为外部设备的序列号信息以及密钥版本信息;根据第二数据报文信息,利用管理模组组织会话协商数据计算指令发送至嵌入式控制模块;利用嵌入式控制模块判断外部设备的序列号是否在白名单中并进行计算,确定第一随机数,将第一红外认证请求组数据报文发送至外部设备,其中第一红外认证请求组数据报文是将第一报文进行封装得到。。

[0059] 具体地,参考图5所示,基于SM2非对称密码算法的身份认证流程如下所示:

[0060] 步骤a:手机产生随机数1、手机证书和签名信息1,组数据报文给管理模组;

[0061] 步骤b:管理模组获得认证请求数据报文后,验证手机证书的有效性,证书非法则跳转到i);证书合法,则继续;

[0062] 步骤c:管理模组使用手机证书验证数据报文中的签名信息1,返回错误码,跳转至步骤i);执行成功,则返回随机数密文、管理模组序列号、管理模组证书和签名信息2;

[0063] 步骤d:管理模组将返回信息组成认证请求的响应信息数据报文发送给手机;

[0064] 步骤e:手机获得认证请求响应数据报文后,验证管理模组证书的有效性,证书非法则跳转到i);证书合法,则继续;

[0065] 步骤f:手机使用管理模组证书验证数据报文中的签名信息2,返回错误码,跳转至步骤i);执行成功,则返回会话密钥包和会话确认数据;

[0066] 步骤g:手机将返回会话确认数据组成认证确认信息数据报文发送给管理模组;

[0067] 步骤h:管理模组获得认证确认数据报文后,验证会话确认数据,验证失败则跳转到i);验证成功,,则返回确认帧数据报文;

[0068] 步骤i:流程结束。

[0069] 可选地,在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证,包括:在外部设备获得第一红外认证请求组数据报文后,外部设备根据第一随机数,确定第一随机数密文以及第二随机数信息;外部设备将红外认证请求的响应信息数据报文发送给管理模组,其中红外认证请求的响应信息数据报文是将第一随机数密文以及第二随机数信息组成;利用管理模组对第一随机数密文进行校验,对第二随机数进行加密,确定第二随机数密文;将第二红外认证请求组数据报文发送至外部设备,其中第二红外认证请求组数据报文是将第二随机数密文进行封装得到;在外部设备获

得第二红外认证请求组数据报文后,外部设备对第二随机数密文进行解密,确定帧数据报文。

[0070] 具体地,参考图6所示,基于SM4对称密码算法的身份认证流程如下所示:

[0071] 步骤a:电能表组织抄读智能家居序列号、密钥版本信息等数据报文给智能家居;

[0072] 步骤b:智能家居根据需要抄读信息,根据返回信息组响应数据报文给管理模组;

[0073] 步骤c:管理模组根据智能家居序列号、密钥版本等信息组织会话协商数据计算指令,发送管理模组ESAM;

[0074] 步骤d:管理模组ESAM判断智能家居ESAM序列号是否在白名单中并进行计算,管理模组ESAM执行失败,返回错误码,跳转至步骤i);执行成功,则返回产生随机数1,参考DL/T 698红外认证请求组数据报文给智能家居;

[0075] 步骤e:智能家居获得红外认证请求数据报文后,则返回随机数1密文和随机数2信息,将返回信息组成红外认证请求的响应信息数据报文发送给管理模组;

[0076] 步骤f:管理模组对返回的随机数1密文进行校验并对随机数2进行加密,执行失败,返回错误码,跳转至步骤i);执行成功,则返回随机数2密文。

[0077] 步骤g:管理模组参考DL/T 698红外认证组数据报文给智能家居;

[0078] 步骤h:智能家居获得红外认证请求数据报文后,验证随机数2密文,失败,返回错误码,跳转至步骤9);执行成功,则返回确认帧数据报文;

[0079] 步骤i:流程结束。

[0080] 此外,参考图7、图8以及图9所示,电能表上电启动后,首先与主站建立应用连接完成双向身份认证及协商出会话密钥SK1。智能家居向电能表发起应用连接建立请求,电能表收到后报文后,通过698报文中的设备类型判断外部设备为智能家居,按照与智能家居的双向认证流程完成与智能家居的双向身份认证以及协商会话密钥SK2。智能家居向主站发送报文,使用于智能电能表协商的会话密钥SK2进行加密。电能表收到报文后,使用对应的会话密钥SK2进行解密,并对报文的类型、格式、校验值、操作类型能进行过滤和权限判断,判断报文为合法报文,则使用电能表与主站协商的会话密钥SK1进行加密,然后通过上行通信模块发送给主站。电能表收到主站回复报文,使用会话密钥SK1进行解密后,根据报文目的地址,判断报文是回复给智能家居的,使用会话密钥SK2进行加密后,通过与智能家居的通信接口发送给智能家居。

[0081] 本实施例是根据外部设备的重要等级、安全模块配置情况等选择不同的双向身份认证方法,以保证接入智能电能表的外部设备的合法身份,确保其安全接入。

[0082] 智能电能表与掌机配用安全芯片,支持SM1、2、3、4等国密算法,采用对称密码机制实现两者的双向身份认证。

[0083] 手机配用软算法模块,支持SM2、3、4等国密算法,基于电能表发行时申请的数字证书与手机中软件下载时同步申请的数字证书,采用数字证书机制实现两者的双向身份认证。

[0084] 智能家居要求配用安全芯片或软算法模块,支持SM2、3、4等国密算法,基于电能表发行时申请的数字证书与手机中软件下载时同步申请的数字证书,采用数字证书机制实现两者的双向身份认证。

[0085] 智能电能表与外部设备之间的通信报文采用会话密钥进行加密保护,防篡改和/

或防窃听。外部设备与主站通信必须经过电能表转发,电能表与外部设备和主站采用不同的物理通信接口进行通信,实现外部设备与主站的通信接口硬隔离。外部设备与主站通信的报文必须经过电能表进行报文过滤以及转加密。

[0086] 此外,参考图1所示,根据本实施例的第二个方面,提供了一种存储介质。存储介质包括存储的程序,其中,在程序运行时由处理器执行以上任意一项所述的方法。

[0087] 从而根据本实施例,基于密码技术设计专用身份认证协议,实现智能表与外部接入设备的双向身份认证并同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护,同时针对外部接入设备与主站的报文交互,由智能电能表对外部接入设备向主站发送的数据报文进行报文过滤,对于不合符操作权限的报文及非法的报文进行阻断,同时通过将与外部接入设备的通信接口和与主站的通信接口进行物理隔离,从而避免外部接入设备直接向主站发动网络攻击。仅为解决了现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。

[0088] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0089] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。

[0090] 实施例2

[0091] 图10示出了根据本实施例所述的一种外部设备安全接入智能电表的装置1000,该装置1000与根据实施例1的第一个方面所述的方法相对应。参考图10所示,该装置1000包括:身份认证模块1010,用于对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;第一检查模块1020,用于在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;第二检查模块1030,用于在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及安全接入模块1040,用于在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0092] 可选地,身份认证模块1010,包括:第一身份认证子模块,用于在外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对外部设备进行身份认证;或者第二身份认证子模块,用于在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证;或者第三身份认证子模块,用于在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证。

[0093] 可选地,第一规则包括智能电表的安全通信模式以及智能电表的数据项以及数据项对应的每项操作,并且智能电表的安全通信模式包括一级安全通信模式、二级安全通信模式、三级安全通信模式以及四级安全通信模式,一级安全通信模式为纯明文方式、二级安全通信模式为明文+消息鉴别码方式、三级安全通信模式为纯密文以及四级安全通信模式为密文加消息鉴别码方式;以及第二规则为针对不同的外部设备选择不同的操作权项。

[0094] 可选地,第一检查模块1020,包括:第一读取子模块,用于在数据项为电表号时,以一级安全通信模式或者二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;第二读取子模块,用于在数据项为电量时,以二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;以及第三读取子模块,用于在数据项为跳闸时,以四级安全通信模式进行读取。

[0095] 可选地,第二检查模块1030,包括:第一执行子模块,用于在外部设备为掌机或者主站时,对外部设备执行所有操作;或者第二执行子模块,用于在外部设备为手机时,对外部设备执行读取和设置操作;以及第三执行子模块,用于在外部设备为智能家居时,对外部设备中有限的数据项进行转发。

[0096] 可选地,第二检查模块1030,还包括:过滤子模块,用于当通信数据不符合操作权限时,将通信数据过滤掉,不转发给主站。

[0097] 可选地,第一身份认证子模块,包括:组织单元,用于在外部设备发送会话密钥协商信息数据报文给智能电表后,组织命令发送到管理模组;第一发送单元,用于利用管理模组执行会话密钥协商信息数据报文,当执行成功后,将掌机返回信息组成应用连接请求的认证响应信息数据报文发送至外部设备,其中手机返回信息为将服务器随机数以及服务器签名信息;以及第一校验单元,用于利用外部设备对服务器随机数以及服务器签名信息进行校验。

[0098] 可选地,第二身份认证子模块,包括:第一验证单元,用于利用管理模组接收外部设备发送的第一数据报文,验证第一数据报文中的手机证书的有效性,其中第一数据报文为将外部设备产生的手机随机数、手机证书和签名信息进行打包的报文;第二验证单元,用于在手机证书有效的情况下,利用管理模组的嵌入式控制模块通过手机证书验证第一数据报文中的签名信息是否有效;以及第二发送单元,用于在第一数据报文中的签名信息通过手机证书验证的情况下,利用管理模组的嵌入式控制模块将手机返回信息组成认证请求的响应信息第一数据报文发送给外部设备,其中手机返回信息为随机数密文、管理模组序列号、管理模组证书和签名信息。

[0099] 可选地,第二身份认证子模块,还包括:第一获得单元,用于在外部设备获得认证请求的响应信息第一数据报文后,外部设备验证管理模组证书的有效性;第三验证单元,用于在管理模组证书有效的情况下,外部设备利用管理模组证书验证第一数据报文中的签名信息;

[0100] 第三发送单元,用于在第一数据报文中的签名信息通过管理模组证书验证的情况下,确定会话密钥包和会话确认数据,并且外部设备将会话确认数据组成的认证确认信息第一数据报文发送给管理模组;以及第四验证单元,用于在管理模组获得认证确认信息第一数据报文后,验证会话确认数据。

[0101] 可选地,第三身份认证子模块,包括:读取单元,用于在外部设备发送第二数据报

文给智能电表后,读取第二数据报文信息,其中第二数据报文信息为外部设备的序列号信息以及密钥版本信息;第四发送单元,用于根据第二数据报文信息,利用管理模组组织会话协商数据计算指令发送至嵌入式控制模块;确定第一随机数单元,用于利用嵌入式控制模块判断外部设备的序列号是否在白名单中并进行计算,确定第一随机数,将第一红外认证请求组数据报文发送至外部设备,其中第一红外认证请求组数据报文是将第一报文进行封装得到。

[0102] 可选地,第三身份认证子模块,包括:确定随机数单元,用于在外部设备获得第一红外认证请求组数据报文后,外部设备根据第一随机数,确定第一随机数密文以及第二随机数信息;第五发送单元,用于外部设备将红外认证请求的响应信息数据报文发送给管理模组,其中红外认证请求的响应信息数据报文是将第一随机数密文以及第二随机数信息组成;加密单元,用于利用管理模组对第一随机数密文进行校验,对第二随机数进行加密,确定第二随机数密文;第六发送单元,用于将第二红外认证请求组数据报文发送至外部设备,其中第二红外认证请求组数据报文是将第二随机数密文进行封装得到;解密单元,用于在外部设备获得第二红外认证请求组数据报文后,外部设备对第二随机数密文进行解密,确定帧数据报文。

[0103] 从而根据本实施例,通过一种外部设备安全接入智能电表的装置1000,基于密码技术设计专用身份认证协议,实现智能表与外部接入设备的双向身份认证并同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护,同时针对外部接入设备与主站的报文交互,由智能电能表对外部接入设备向主站发送的数据报文进行报文过滤,对于不合符操作权限的报文及非法的报文进行阻断,同时通过将与外部接入设备的通信接口和与主站的通信接口进行物理隔离,从而避免外部接入设备直接向主站发动网络攻击。仅为解决了现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。

[0104] 实施例3

[0105] 图11示出了根据本实施例所述的一种外部设备安全接入智能电表的装置1100,该装置1100与根据实施例1的第一个方面所述的方法相对应。参考图11所示,该装置1100包括:处理器1110;以及存储器1120,与处理器1110连接,用于为处理器1110提供处理以下处理步骤的指令:对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及在外部设备的操作权限符合第二规则的情况下,将外部设备安全接入智能电表。

[0106] 可选地,对接入的外部设备进行身份认证,其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证,并且身份认证是外部设备与智能电表的双向身份认证;在对外部设备身份认证通过后,检查外部设备的安全通信模式是否符合预先设置的第一规则;在外部设备的安全通信模式符合第一规则的情况下,检查外部设备的操作权限是否符合预先设置的第二规则;以及在外部设备的操作权限符合第

二规则的情况下,将外部设备安全接入智能电表。

[0107] 可选地,第一规则包括智能电表的安全通信模式以及智能电表的数据项以及数据项对应的每项操作,并且智能电表的安全通信模式包括一级安全通信模式、二级安全通信模式、三级安全通信模式以及四级安全通信模式,一级安全通信模式为纯明文方式、二级安全通信模式为明文+消息鉴别码方式、三级安全通信模式为纯密文以及四级安全通信模式为密文加消息鉴别码方式;以及第二规则为针对不同的外部设备选择不同的操作权项。

[0108] 可选地,检查外部设备的安全通信模式是否符合预先设置的第一规则,包括:在数据项为电表号时,以一级安全通信模式或者二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;在数据项为电量时,以二级安全通信模式或者三级安全通信模式或者四级安全通信模式进行读取;以及在数据项为跳闸时,以四级安全通信模式进行读取。

[0109] 可选地,检查外部设备的操作权限是否符合预先设置的第二规则,包括:在外部设备为掌机或者主站时,对外部设备执行所有操作;或者在外部设备为手机时,对外部设备执行读取和设置操作;以及在外部设备为智能家居时,对外部设备中有限的数据项进行转发。

[0110] 可选地,检查外部设备的操作权限是否符合预先设置的第二规则,还包括:当通信数据不符合操作权限时,将通信数据过滤掉,不转发给主站。

[0111] 可选地,在外部设备为掌机、采集系统主站以及检测软件时,基于SM1对称密码算法对外部设备进行身份认证,包括:在外部设备发送会话密钥协商信息数据报文给智能电表后,组织命令发送到管理模组;利用管理模组执行会话密钥协商信息数据报文,当执行成功后,将掌机返回信息组成应用连接请求的认证响应信息数据报文发送至外部设备,其中手机返回信息为将服务器随机数以及服务器签名信息;以及利用外部设备对服务器随机数以及服务器签名信息进行校验。

[0112] 可选地,在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证,包括:利用管理模组接收外部设备发送的第一数据报文,验证第一数据报文中的手机证书的有效性,其中第一数据报文为将外部设备产生的手机随机数、手机证书和签名信息进行打包的报文;在手机证书有效的情况下,利用管理模组的嵌入式控制模块通过手机证书验证第一数据报文中的签名信息是否有效;以及在第一数据报文中的签名信息通过手机证书验证的情况下,利用管理模组的嵌入式控制模块将手机返回信息组成认证请求的响应信息第一数据报文发送给外部设备,其中手机返回信息为随机数密文、管理模组序列号、管理模组证书和签名信息。

[0113] 可选地,在外部设备为手机时,基于SM2非对称密码算法对外部设备进行身份认证,还包括:在外部设备获得认证请求的响应信息第一数据报文后,外部设备验证管理模组证书的有效性;在管理模组证书有效的情况下,外部设备利用管理模组证书验证第一数据报文中的签名信息;在第一数据报文中的签名信息通过管理模组证书验证的情况下,确定会话密钥包和会话确认数据,并且外部设备将会话确认数据组成的认证确认信息第一数据报文发送给管理模组;以及在管理模组获得认证确认信息第一数据报文后,验证会话确认数据。

[0114] 可选地,在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证,包括:在外部设备发送第二数据报文给智能电表后,读取第

二数据报文信息,其中第二数据报文信息为外部设备的序列号信息以及密钥版本信息;根据第二数据报文信息,利用管理模组组织会话协商数据计算指令发送至嵌入式控制模块;以及利用嵌入式控制模块判断外部设备的序列号是否在白名单中并进行计算,确定第一随机数,将第一红外认证请求组数据报文发送至外部设备,其中第一红外认证请求组数据报文是将第一报文进行封装得到。

[0115] 可选地,在外部设备为智能家居、外置断路器以及扩展模组时,基于SM4对称密码算法对外部设备进行身份认证,包括:在外部设备获得第一红外认证请求组数据报文后,外部设备根据第一随机数,确定第一随机数密文以及第二随机数信息;外部设备将红外认证请求的响应信息数据报文发送给管理模组,其中红外认证请求的响应信息数据报文是将第一随机数密文以及第二随机数信息组成;利用管理模组对第一随机数密文进行校验,对第二随机数进行加密,确定第二随机数密文;将第二红外认证请求组数据报文发送至外部设备,其中第二红外认证请求组数据报文是将第二随机数密文进行封装得到;在外部设备获得第二红外认证请求组数据报文后,外部设备对第二随机数密文进行解密,确定帧数据报文。

[0116] 从而根据本实施例,通过一种外部设备安全接入智能电表的装置1100,基于密码技术设计专用身份认证协议,实现智能表与外部接入设备的双向身份认证并同步协商两者之间的会话密钥,基于会话密钥对两者之间交互报文进行加密保护,同时针对外部接入设备与主站的报文交互,由智能电能表对外部接入设备向主站发送的数据报文进行报文过滤,对于不合符操作权限的报文及非法的报文进行阻断,同时通过将与外部接入设备的通信接口和与主站的通信接口进行物理隔离,从而避免外部接入设备直接向主站发动网络攻击。仅为解决了现有技术中存在的智能电能表与外部接入设备两者之间的双向身份认证问题、交互数据的完整性保护问题以及外部接入设备直接与主站交互对主站系统造成的安全风险的技术问题。。

[0117] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0118] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0119] 在本申请所提供的几个实施例中,应该理解到,所揭露的技术内容,可通过其它的方式实现。其中,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,单元或模块的间接耦合或通信连接,可以是电性或其它的形式。

[0120] 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。

[0121] 另外,在本发明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。

[0122] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0123] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

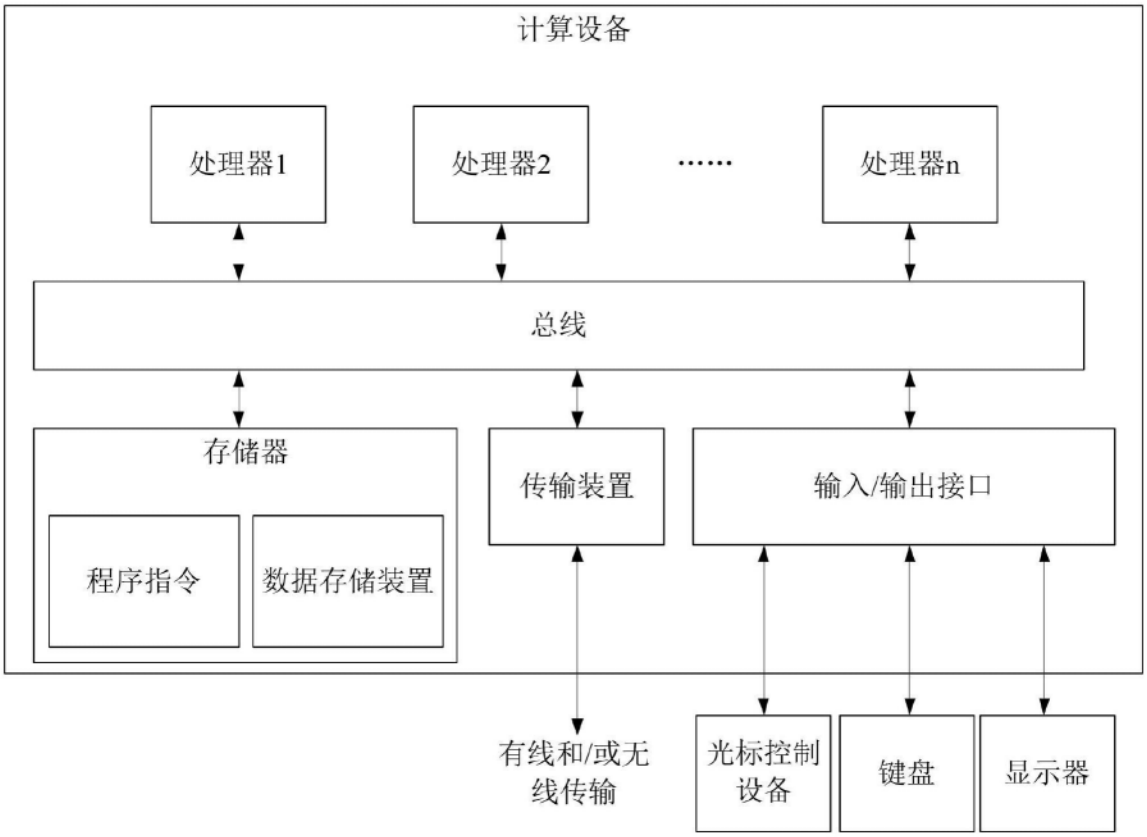

计算设备
处理器1
处理器2
……
处理器n
总线
存储器
程序指令
数据存储装置
传输装置
输入/输出接口
有线和/或无线传输
光标控制设备
键盘
显示器

图1

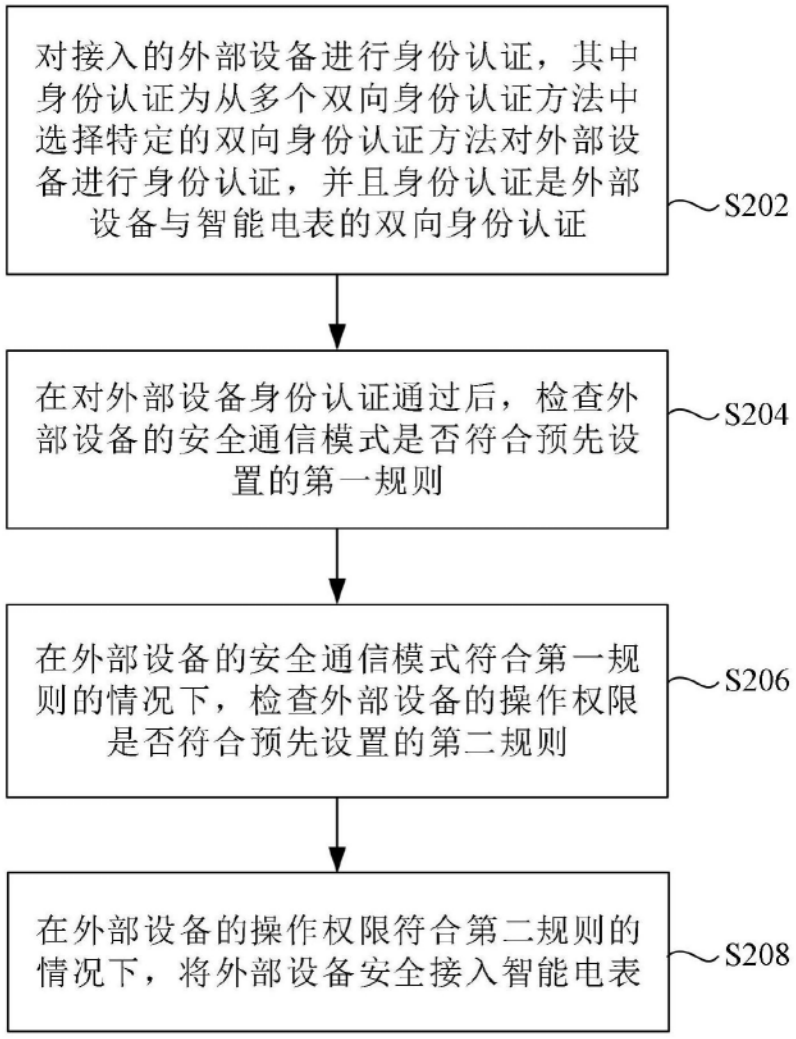

对接入的外部设备进行身份认证，其中身份认证为从多个双向身份认证方法中选择特定的双向身份认证方法对外部设备进行身份认证，并且身份认证是外部设备与智能电表的双向身份认证
S202
在对外部设备身份认证通过后，检查外部设备的安全通信模式是否符合预先设置的第一规则
S204
在外部设备的安全通信模式符合第一规则的情况下，检查外部设备的操作权限是否符合预先设置的第二规则
S206
在外部设备的操作权限符合第二规则的情况下，将外部设备安全接入智能电表
S208

图2

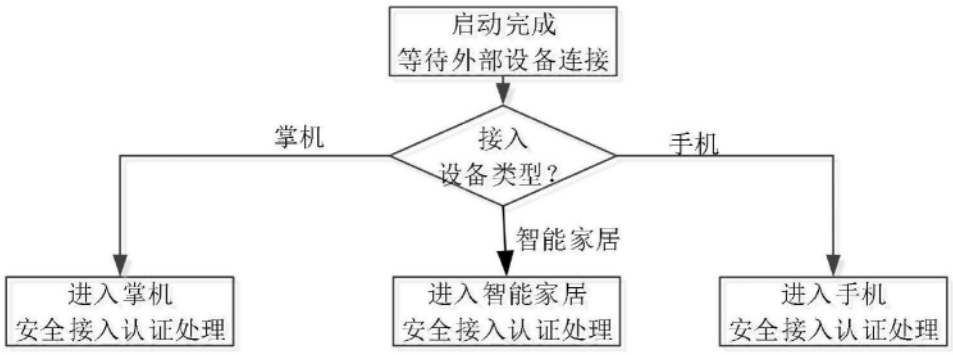

启动完成
等待外部设备连接
接入
设备类型？
掌机
手机
智能家居
进入掌机
安全接入认证处理
进入智能家居
安全接入认证处理
进入手机
安全接入认证处理

图3

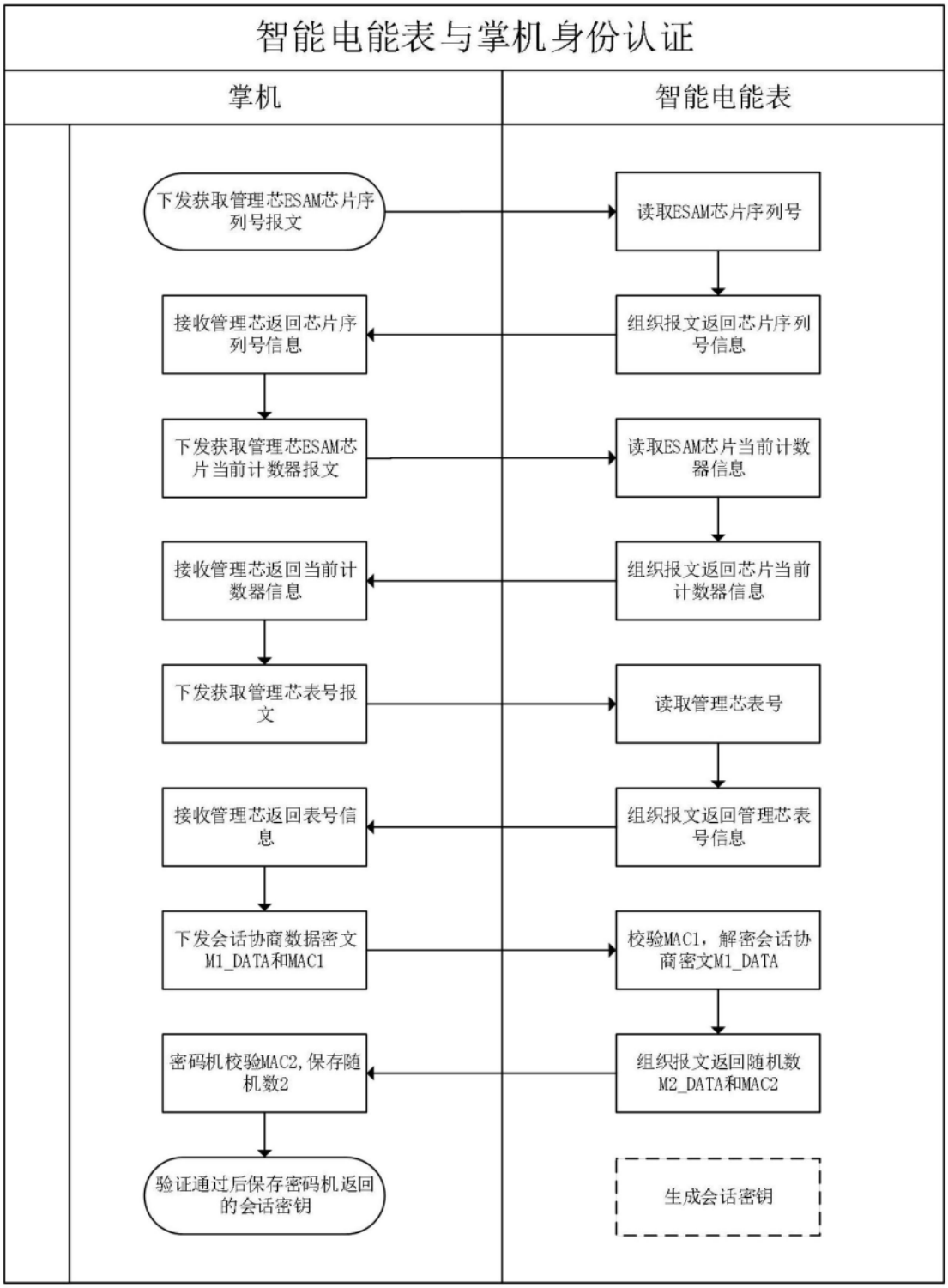

智能电能表与掌机身份认证
掌机
智能电能表
下发获取管理芯ESAM芯片序列号报文
读取ESAM芯片序列号
接收管理芯返回芯片序列号信息
组织报文返回芯片序列号信息
下发获取管理芯ESAM芯片当前计数器报文
读取ESAM芯片当前计数器信息
接收管理芯返回当前计数器信息
组织报文返回芯片当前计数器信息
下发获取管理芯表号报文
读取管理芯表号
接收管理芯返回表号信息
组织报文返回管理芯表号信息
下发会话协商数据密文M1_DATA和MAC1
校验MAC1，解密会话协商密文M1_DATA
密码机校验MAC2,保存随机数2
组织报文返回随机数M2_DATA和MAC2
验证通过后保存密码机返回的会话密钥
生成会话密钥

图4

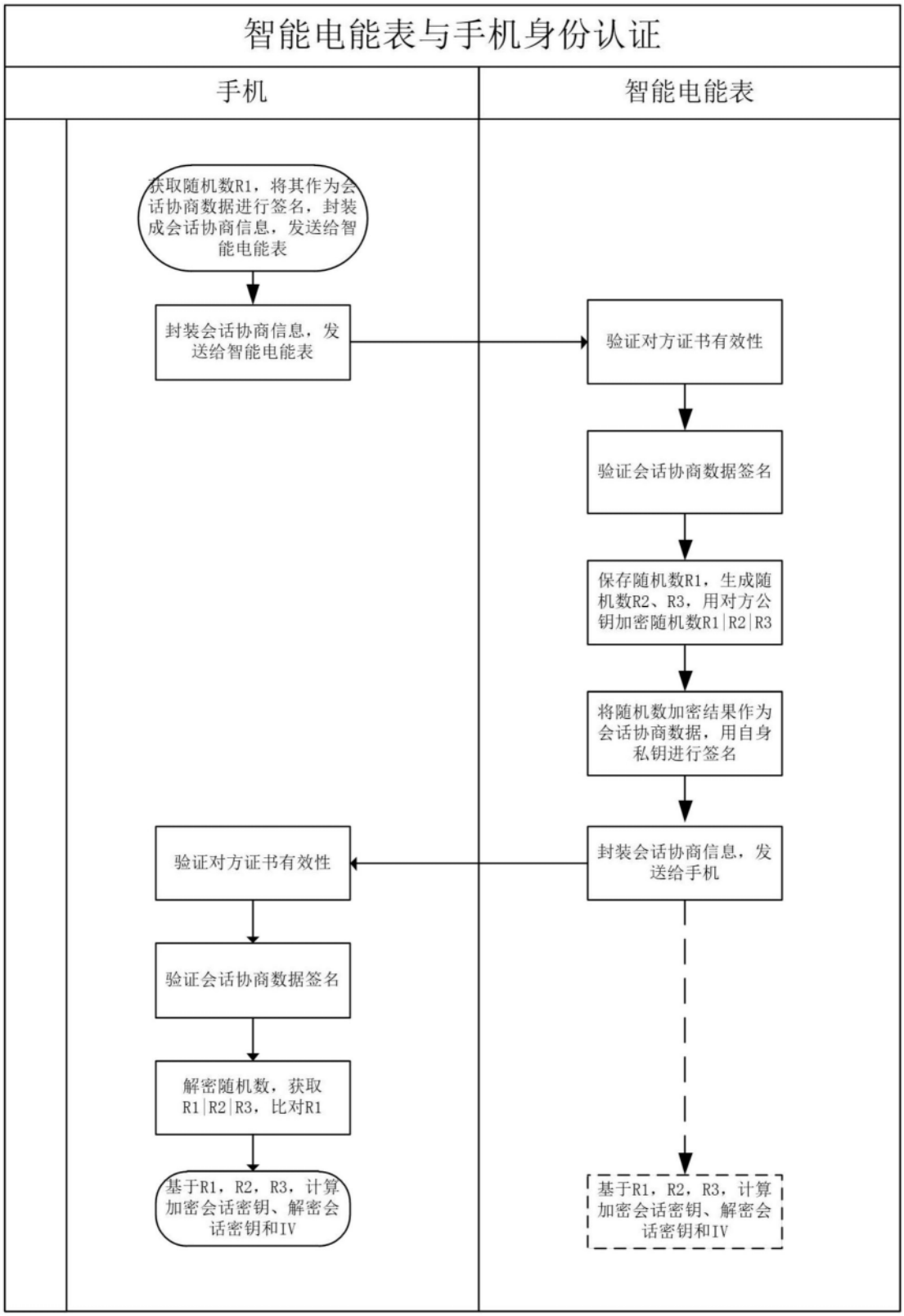

智能电能表与手机身份认证
手机
智能电能表
获取随机数R1，将其作为会话协商数据进行签名，封装成会话协商信息，发送给智能电能表
封装会话协商信息，发送给智能电能表
验证对方证书有效性
验证会话协商数据签名
保存随机数R1，生成随机数R2、R3，用对方公钥加密随机数R1|R2|R3
将随机数加密结果作为会话协商数据，用自身私钥进行签名
封装会话协商信息，发送给手机
验证对方证书有效性
验证会话协商数据签名
解密随机数，获取R1|R2|R3，比对R1
基于R1，R2，R3，计算加密会话密钥、解密会话密钥和IV
基于R1，R2，R3，计算加密会话密钥、解密会话密钥和IV

图5

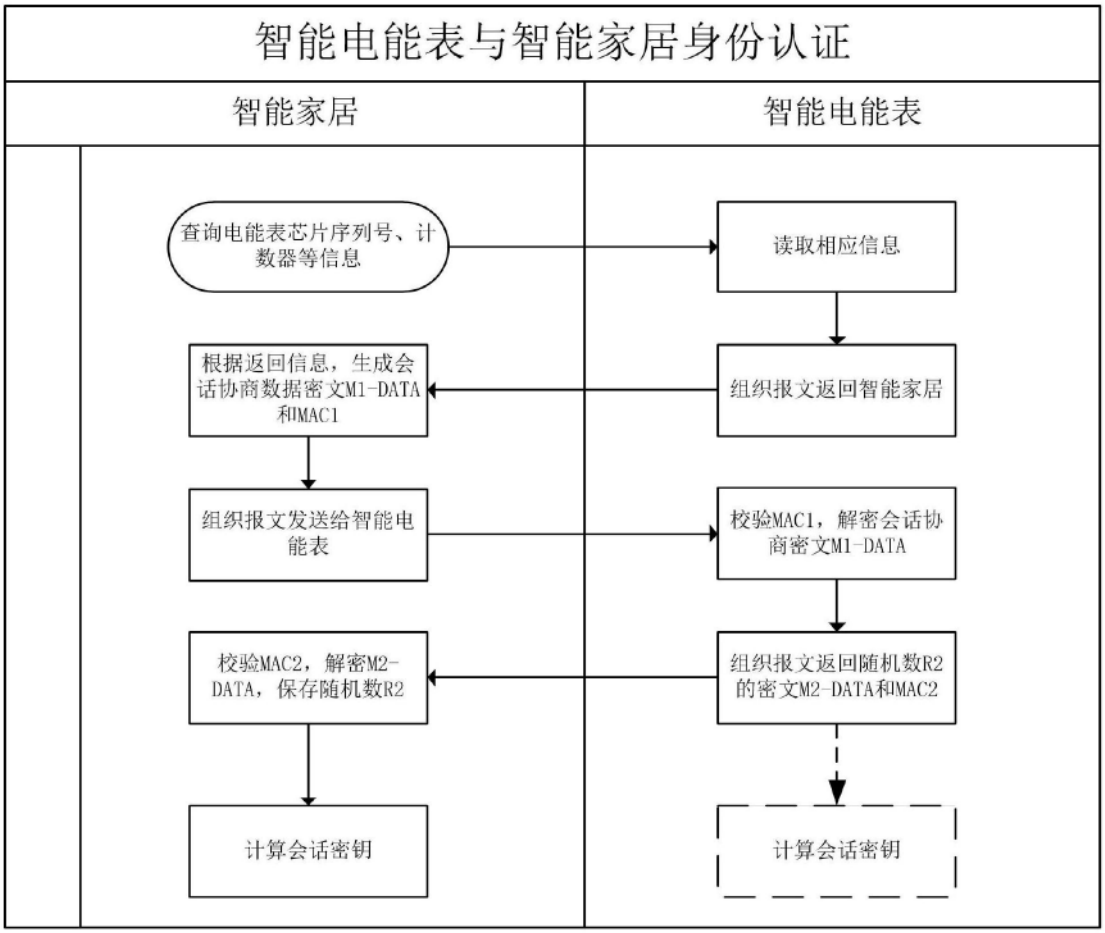

智能电能表与智能家居身份认证
智能家居
智能电能表
查询电能表芯片序列号、计数器等信息
读取相应信息
根据返回信息，生成会话协商数据密文M1-DATA和MAC1
组织报文返回智能家居
组织报文发送给智能电能表
校验MAC1，解密会话协商密文M1-DATA
校验MAC2，解密M2-DATA，保存随机数R2
组织报文返回随机数R2的密文M2-DATA和MAC2
计算会话密钥
计算会话密钥

图6

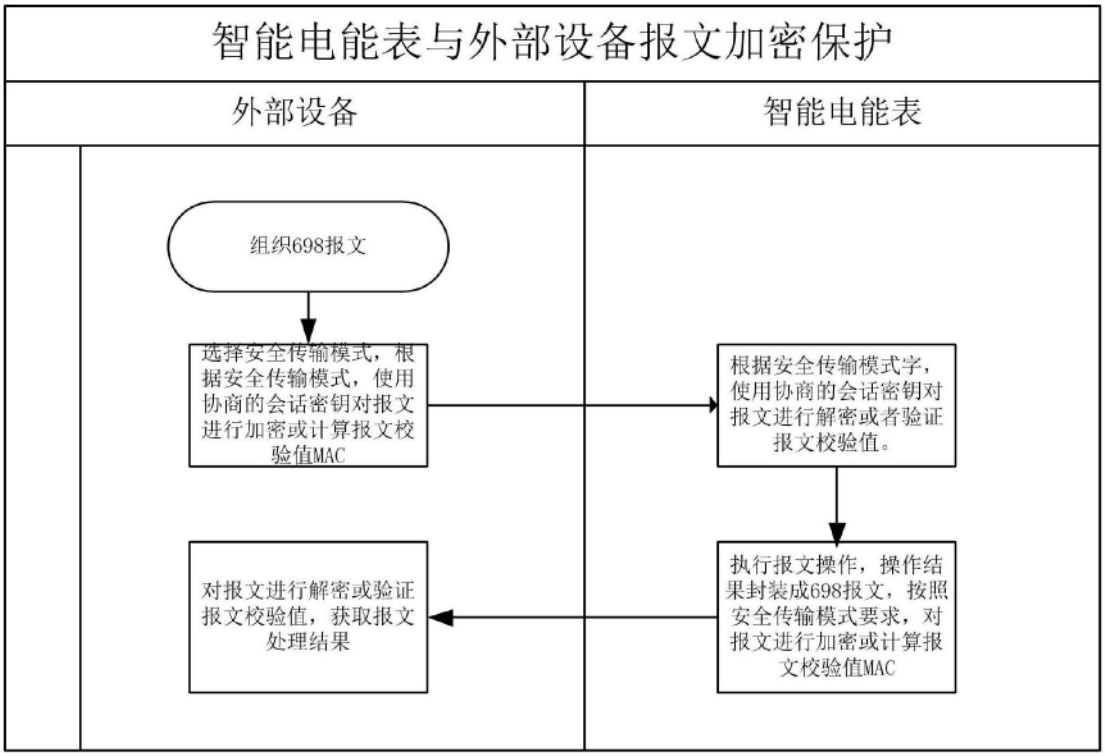

智能电能表与外部设备报文加密保护
外部设备
智能电能表
组织698报文
选择安全传输模式，根据安全传输模式，使用协商的会话密钥对报文进行加密或计算报文校验值MAC
根据安全传输模式字，使用协商的会话密钥对报文进行解密或者验证报文校验值。
执行报文操作，操作结果封装成698报文，按照安全传输模式要求，对报文进行加密或计算报文校验值MAC
对报文进行解密或验证报文校验值，获取报文处理结果

图7

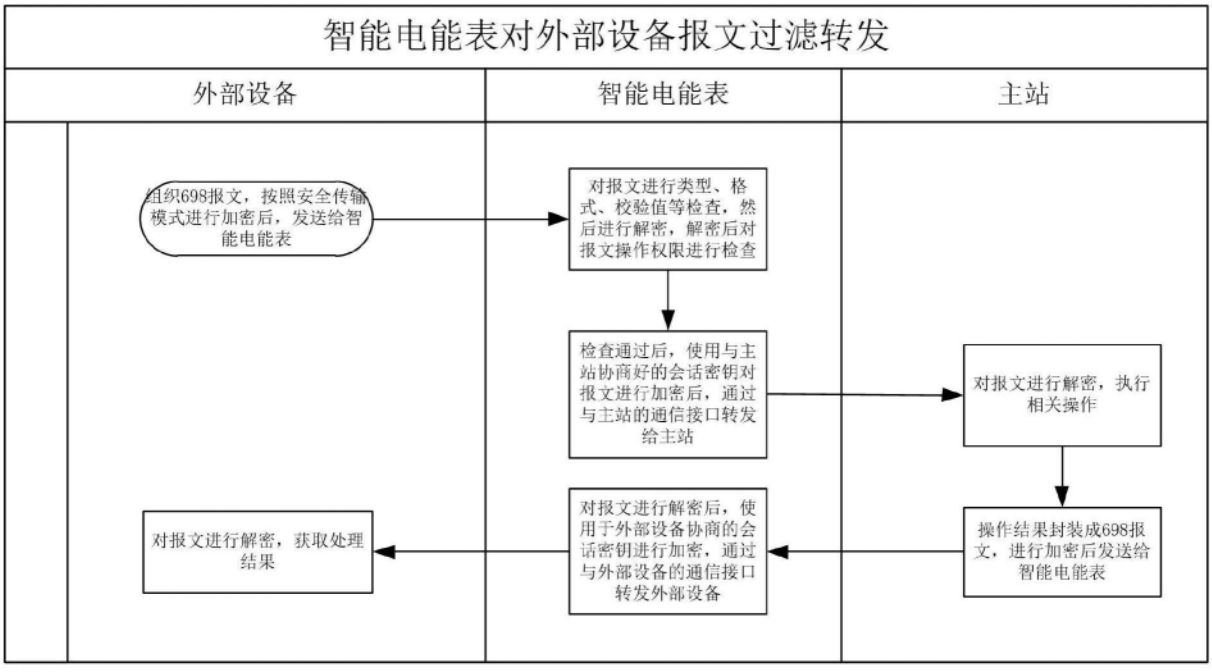

智能电能表对外部设备报文过滤转发
外部设备
智能电能表
主站
组织698报文，按照安全传输模式进行加密后，发送给智能电能表
对报文进行类型、格式、校验值等检查，然后进行解密，解密后对报文操作权限进行检查
检查通过后，使用与主站协商好的会话密钥对报文进行加密后，通过与主站的通信接口转发给主站
对报文进行解密，执行相关操作
操作结果封装成698报文，进行加密后发送给智能电能表
对报文进行解密后，使用于外部设备协商的会话密钥进行加密，通过与外部设备的通信接口转发外部设备
对报文进行解密，获取处理结果

图8

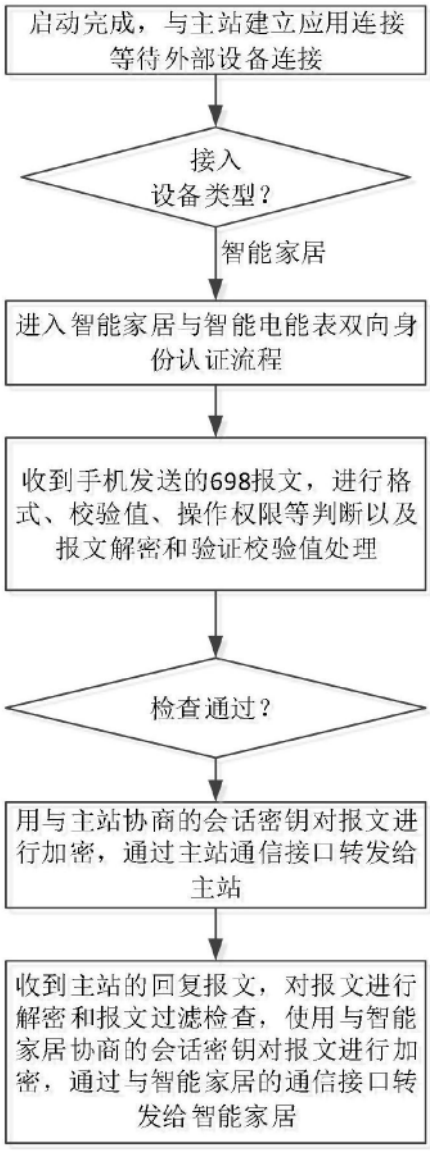

启动完成，与主站建立应用连接
等待外部设备连接
接入
设备类型？
智能家居
进入智能家居与智能电能表双向身份认证流程
收到手机发送的698报文，进行格式、校验值、操作权限等判断以及报文解密和验证校验值处理
检查通过？
用与主站协商的会话密钥对报文进行加密，通过主站通信接口转发给主站
收到主站的回复报文，对报文进行解密和报文过滤检查，使用与智能家居协商的会话密钥对报文进行加密，通过与智能家居的通信接口转发给智能家居

图9


身份认证模块 1010
第一检查模块 1020
第二检查模块 1030
安全接入模块 1040
1000

图10


处理器 1110
存储器 1120
1100

图11