(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114697022 A
(43)申请公布日 2022.07.01

(21)申请号 202210268396.2

(22)申请日 2022.03.18

(71)申请人 北京国泰网信科技有限公司
地址 100089 北京市海淀区昆明湖南路51号B座3层303号
申请人 成都国泰网信科技有限公司

(72)发明人 李欣 李元正 付晓晨

(74)专利代理机构 北京维正专利代理有限公司 11508
专利代理师 谢明晖

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/12(2022.01)
G06Q 50/06(2012.01)

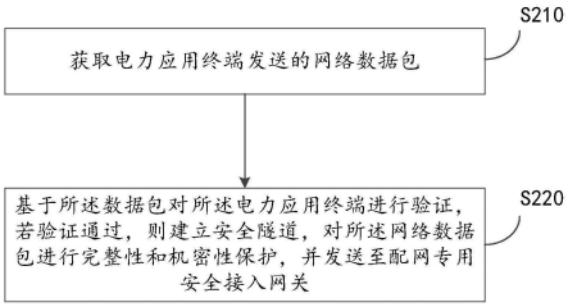
权利要求书1页 说明书6页 附图2页

(54)发明名称

应用于配电网系统的加密认证方法

(57)摘要

本申请的实施例提供了应用于配电网系统的加密认证方法、装置、设备和计算机可读存储介质。所述方法包括获取电力应用终端发送的网络数据包;基于所述数据包对所述电力应用终端进行验证,若验证通过,则建立安全隧道,对所述网络数据包进行完整性和机密性保护,并发送至配网专用安全接入网关。以此方式,确保了通信双方对的身份正确性同时也保障了在网传输数据不被窃取和篡改。



CN 114697022 A

1.一种应用于配电网系统的加密认证方法,其特征在于,包括:

获取电力应用终端发送的网络数据包;

基于所述数据包对所述电力应用终端进行验证,若验证通过,则建立安全隧道,对所述网络数据包进行完整性和机密性保护,并发送至配网专用安全接入网关。

2.根据权利要求1所述的方法,其特征在于,所述网络数据包包括IP、MAC地址。

3.根据权利要求2所述的方法,其特征在于,所述基于所述数据包对所述电力应用终端进行验证包括:

基于所述数据包,通过IP、MAC地址和/或身份鉴别认证的方式对所述电力应用终端进行验证。

4.根据权利要求3所述的方法,其特征在于,所述对所述网络数据包进行完整性和机密性保护包括:

利用SM2/3/4算法,对所述网络数据包进行完整性和机密性保护。

5.根据权利要求4所述的方法,其特征在于,还包括:

通过PKI机制下证书认证的方式,对电力应用终端进行验证。

6.根据权利要求5所述的方法,其特征在于,还包括:

采用标准化的IPSec协议和功能,进行互联通信。

7.一种应用于配电网系统的加密认证装置,其特征在于,包括:

获取模块,用于获取电力应用终端发送的网络数据包;

验证模块,基于所述数据包对所述电力应用终端进行验证,若验证通过,则建立安全隧道,对所述网络数据包进行完整性和机密性保护,并发送至配网专用安全接入网关。

8.根据权利要求7所述的装置,其特征在于,所述网络数据包包括IP、MAC地址。

9.一种电子设备,包括存储器和处理器,所述存储器上存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1～6中任一项所述的方法。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如权利要求1～6中任一项所述的方法。

应用于配电网系统的加密认证方法

技术领域

[0001] 本申请的实施例涉及配电网数据通信加密领域，尤其涉及应用于配电网系统的加密认证方法、装置、设备和计算机可读存储介质。

背景技术

[0002] 随着国家信息化的发展，关键基础设施的安全防护显得尤为重要，加强国家基础设施的安全防护，已成为各行各业的管理者及从业者重视的问题，特别是在国家电力行业，安全问题涉及到民生、经济发展等，对安全的防护及管理和技术创新提出了明确的要求，严格防护安全事故发生，保护好电网系统的安全生产。

[0003] 在国家电网安全方面。在国家电网作为国家基础设施，其信息安全问题不仅与电力生产安全和经济安全密不可分，而且已经关系到国计民生、社会稳定与公众利益。信息安全保障工作是电网安全稳定运行的重要基础，同时也是国家安全战略的重要组成部分。

[0004] 国家的配电网安全逐步在加强。近年来随着中低压配电网快速发展，有些不具备光纤通信条件的配电网采用了公网通信方式(GPRS/CDMA-SCDMA/230MHz等)传输控制指令，致使系统面临来公共网络攻击的风险，影响对用户的安全可靠供电，同时犯罪分子可能通过子站终端入侵主站，造成更大范围的安全威胁。为保障电网安全稳定运行，对配电网二次系统安全防护的相关方案势在必行。

发明内容

[0005] 根据本申请的实施例，提供了一种应用于配电网系统的加密认证方案。

[0006] 在本申请的第一方面，提供了一种应用于配电网系统的加密认证方法。该方法包括：

[0007] 获取电力应用终端发送的网络数据包；

[0008] 基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关。

[0009] 进一步地，所述网络数据包包括IP、MAC地址。

[0010] 进一步地，所述基于所述数据包对所述电力应用终端进行验证包括：

[0011] 基于所述数据包，通过IP、MAC地址和/或身份鉴别认证的方式对所述电力应用终端进行验证。

[0012] 进一步地，所述对所述网络数据包进行完整性和机密性保护包括：

[0013] 利用SM2/3/4算法，对所述网络数据包进行完整性和机密性保护。

[0014] 进一步地，还包括：

[0015] 通过PKI机制下证书认证的方式，对电力应用终端进行验证。

[0016] 进一步地，还包括：

[0017] 采用标准化的IPSec协议和功能，进行互联通信。

[0018] 在本申请的第二方面，提供了一种应用于配电网系统的加密认证装置。该装置包

括：

[0019] 获取模块，用于获取电力应用终端发送的网络数据包；

[0020] 验证模块，基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关。

[0021] 进一步地，所述网络数据包包括IP、MAC地址。。

[0022] 在本申请的第三方面，提供了一种电子设备。该电子设备包括：存储器和处理器，所述存储器上存储有计算机程序，所述处理器执行所述程序时实现如以上所述的方法。

[0023] 在本申请的第四方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现如根据本申请的第一方面的方法。

[0024] 本申请实施例提供的应用于配电网系统的加密认证方法，通过获取电力应用终端发送的网络数据包；基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关，确保了通信双方对的身份正确性同时也保障了在网传输数据不被窃取和篡改。

[0025] 应当理解，发明内容部分中所描述的内容并非旨在限定本申请的实施例的关键或重要特征，亦非用于限制本申请的范围。本申请的其它特征将通过以下的描述变得容易理解。

附图说明

[0026] 结合附图并参考以下详细说明，本申请各实施例的上述和其他特征、优点及方面将变得更加明显。在附图中，相同或相似的附图标记表示相同或相似的元素，其中：

[0027] 图1示出了本申请的实施例提供的方法所涉及的系统架构图。

[0028] 图2示出了根据本申请的实施例的应用于配电网系统的加密认证方法的流程图；

[0029] 图3示出了根据本申请的实施例的应用于配电网系统的加密认证装置的方框图；

[0030] 图4示出了适于用来实现本申请实施例的终端设备或服务器的结构示意图。

具体实施方式

[0031] 为使本公开实施例的目的、技术方案和优点更加清楚，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，所描述的实施例是本公开一部分实施例，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作出创造性劳动前提下所获得的全部其他实施例，都属于本公开保护的范围。

[0032] 另外，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0033] 图1示出了可以应用本申请的应用于配电网系统的加密认证方法或应用于配电网系统的加密认证装置的实施例的示例性系统架构100。

[0034] 如图1所示，系统架构100可以包括终端设备101、102、103，网络104和服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0035] 用户可以使用终端设备101、102、103通过网络104与服务器105交互，以接收或发

送消息等。终端设备101、102、103上可以安装有各种通讯客户端应用，例如模型训练类应用、视频识别类应用、网页浏览器应用、社交平台软件等。

[0036] 终端设备101、102、103可以是硬件，也可以是软件。当终端设备101、102、103为硬件时，可以是具有显示屏的各种电子设备，包括但不限于智能手机、平板电脑、电子书阅读器、MP3播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。当终端设备101、102、103为软件时，可以安装在上述所列举的电子设备中。其可以实现成多个软件或软件模块(例如用来提供分布式服务的多个软件或软件模块)，也可以实现成单个软件或软件模块。在此不做具体限定。

[0037] 当终端101、102、103为硬件时，其上还可以安装有视频采集设备。视频采集设备可以是各种能实现采集视频功能的设备，如摄像头、传感器等等。用户可以利用终端101、102、103上的视频采集设备来采集视频。

[0038] 服务器105可以是提供各种服务的服务器，例如对终端设备101、102、103上显示的数据处理的后台服务器。后台服务器可以对接收到的数据进行分析等处理，并可以将处理结果(例如识别结果)反馈给终端设备。

[0039] 需要说明的是，服务器可以是硬件，也可以是软件。当服务器为硬件时，可以实现成多个服务器组成的分布式服务器集群，也可以实现成单个服务器。当服务器为软件时，可以实现成多个软件或软件模块(例如用来提供分布式服务的多个软件或软件模块)，也可以实现成单个软件或软件模块。在此不做具体限定。

[0040] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。特别地，在目标数据不需要从远程获取的情况下，上述系统架构可以不包括网络，而只包括终端设备或服务器。

[0041] 如图2所示，是本申请实施例应用于配电网系统的加密认证方法的流程图。从图2中可以看出，本实施例的应用于配电网系统的加密认证方法，包括以下步骤：

[0042] S210，获取电力应用终端发送的网络数据包。

[0043] 在本实施例中，用于应用于配电网系统的加密认证方法的执行主体(例如图1所示的服务器)可以通过有线方式或者无线连接的方式获取网络数据包。

[0044] 其中，所述网络数据包包括IP、MAC地址等信息。

[0045] S220，基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关。

[0046] 在一些实施例中，基于所述数据包对所述电力应用终端进行验证前，需要导入设备证书。本公开采用双证书认证体系，包含加密密钥对和签名密钥对，其中，证书和秘钥格式均为DER格式。

[0047] 进一步地，证书导入完成后，创建唯一系统管理员，输入系统管理员名称和强口令(至少包含数字，大写字母，小写字母和特殊符号其中的三种且密钥长度不低于8位)，点击“确定”按钮。

[0048] 进一步地，可通过插入USBKey的方式，生成系统管理员身份Key。安全管理员的创建、删除和修改需要系统管理员登陆管理系统进入“人员管理”界面进行操作。

[0049] 创建安全管理员具体操作如下：

[0050] (1)点击“新增人员”按钮，弹出新增表单；

[0051] (2)选择角色：安全管理员(负责设备参数配置、策略配置、设备密钥的生成、导入、备份和恢复等操作)。

[0052] (3)输入安全管理员名、安全管理员说明、并输入两次口令，两次口令必须一致。

[0053] (4)插入USBKey，点击“保存”按钮，微型加密认证装置将生成安全管理员认证信息并导入USBKey，提示创建成功后创建完成。

[0054] 在一些实施例中，所述证书中可包括名称、组织、机构名、国家名、省和区县等信息。

[0055] 在一些实施例中，可采用WEB的操作方式，通过IE浏览器简单、快速的完成设备参数、IP、安全策略、日志审计等配置。

[0056] 在一些实施例中，采用标准化的IPSec协议和功能，进行互联通信。

[0057] 在一些实施例中，产品采用标准化的国家密码局的密码算法，实现了身份认证、加解密处理、安全通信等能力，即，利用SM2/3/4算法加强了设备连接的安全性和数据传输的完整性、机密性等能力。

[0058] 在一些实施例中，本公开的方法，支持符合《GM/T 0015基于SM2密码算法的数字证书格式规范》格式的证书、支持第三方CA，实现了证书下载、验证、使用的能力，提升了系统安全应用的扩展性和便利性。

[0059] 在一些实施例中，基于所述数据包，通过IP、MAC地址和/或身份鉴别认证的方式对所述电力应用终端进行验证；也可基于数字证书的PKI机制进行双向身份认证；认证通过后，建立安全隧道，对数据进行完整性、机密性保护。

[0060] 根据本公开的实施例，实现了以下技术效果：

[0061] 采用内外网隔离的方式，并结合网络内部的证书使用和加解密算法的应用，在数据上传和接收时的数据交换过程中实现安全防护，从而保证系统数据的非明文传输和应用。

[0062] 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，本申请并不受所描述的动作顺序的限制，因为依据本申请，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可选实施例，所涉及的动作和模块并不一定是本申请所必须的。

[0063] 以上是关于方法实施例的介绍，以下通过装置实施例，对本申请所述方案进行进一步说明。

[0064] 图3示出了根据本申请的实施例的应用于配电网系统的加密认证装置300的方框图，如图3所示，装置300包括：

[0065] 获取模块310，用于获取电力应用终端发送的网络数据包；

[0066] 验证模块320，基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关。

[0067] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，所述描述的模块

的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0068] 图4示出了适于用来实现本申请实施例的终端设备或服务器的结构示意图。

[0069] 如图4所示，终端设备或服务器400包括中央处理单元(CPU)401，其可以根据存储在只读存储器(ROM)402中的程序或者从存储部分408加载到随机访问存储器(RAM)403中的程序而执行各种适当的动作和处理。在RAM 403中，还存储有系统400操作所需的各种程序和数据。CPU 401、ROM 402以及RAM 403通过总线404彼此相连。输入/输出(I/O)接口405也连接至总线404。

[0070] 以下部件连接至I/O接口405：包括键盘、鼠标等的输入部分406；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分407；包括硬盘等的存储部分408；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分409。通信部分409经由诸如因特网的网络执行通信处理。驱动器410也根据需要连接至I/O接口405。可拆卸介质411，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器410上，以便于从其上读出的计算机程序根据需要被安装入存储部分408。

[0071] 特别地，根据本申请的实施例，上文方法流程步骤可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括承载在机器可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分409从网络上被下载和安装，和/或从可拆卸介质411被安装。在该计算机程序被中央处理单元(CPU)401执行时，执行本申请的系统中限定的上述功能。

[0072] 需要说明的是，本申请所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0073] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，前述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要

注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0074] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中。其中，这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0075] 作为另一方面，本申请还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中的。上述计算机可读存储介质存储有一个或者多个程序，当上述前述程序被一个或者一个以上的处理器用来执行描述于本申请的方法。

[0076] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的申请范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离前述申请构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中申请的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

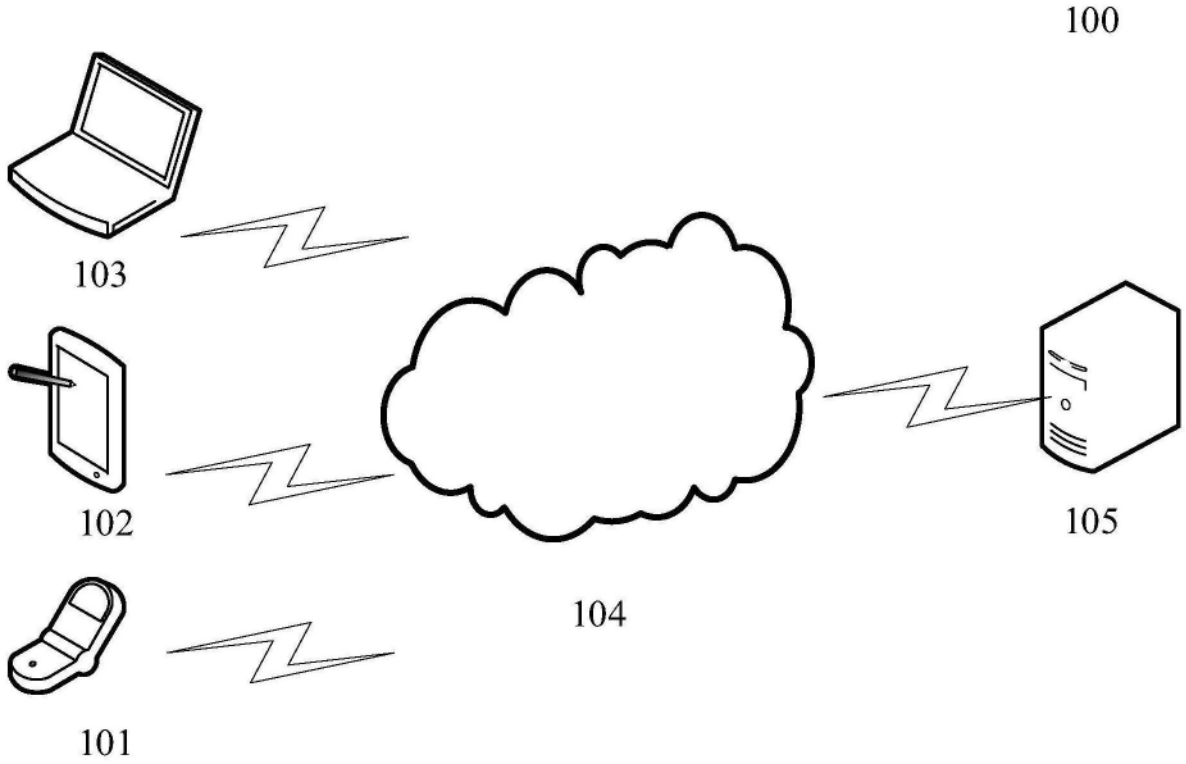

100
103
102
101
104
105

图1

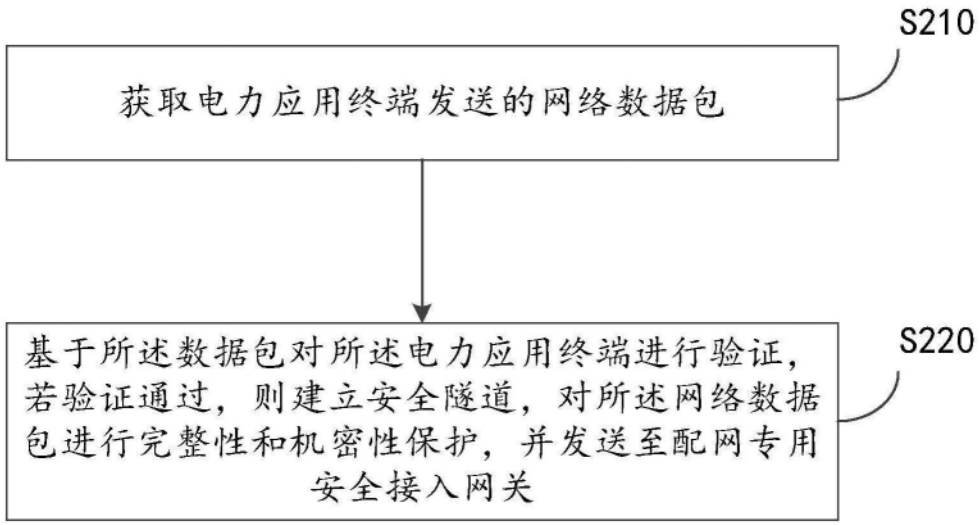

S210
获取电力应用终端发送的网络数据包
S220
基于所述数据包对所述电力应用终端进行验证，若验证通过，则建立安全隧道，对所述网络数据包进行完整性和机密性保护，并发送至配网专用安全接入网关

图2

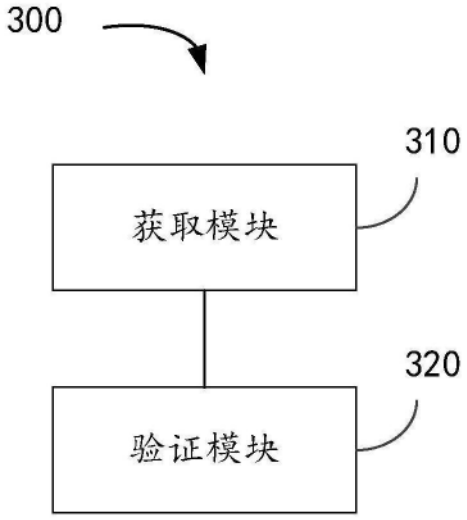

300
310
获取模块
320
验证模块

图3

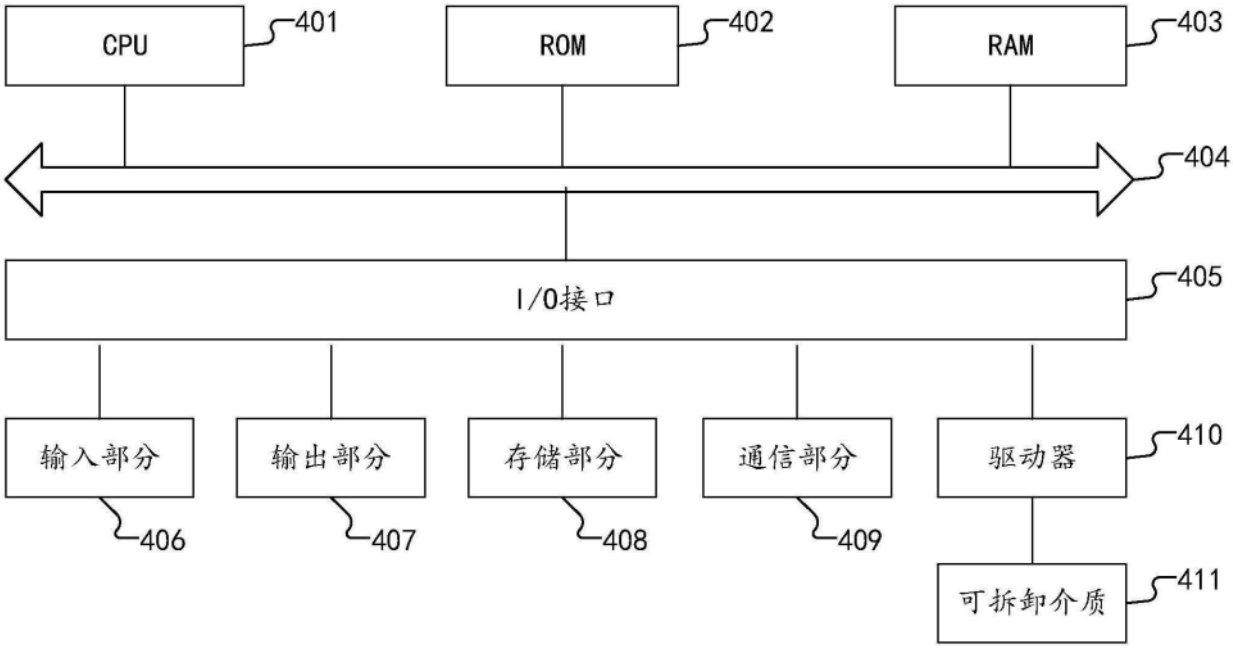

CPU
401
ROM
402
RAM
403
404
I/O接口
405
输入部分
406
输出部分
407
存储部分
408
通信部分
409
驱动器
410
可拆卸介质
411

图4