(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110035058 B
(45)授权公告日 2021.07.06

(21)申请号 201910152554.6

(22)申请日 2019.02.28

(65)同一申请的已公布的文献号
申请公布号 CN 110035058 A

(43)申请公布日 2019.07.19

(73)专利权人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 唐海

(74)专利代理机构 上海光栅知识产权代理有限公司 31340
代理人 马雯雯

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
ISO/IEC.ISO_IEC_30118-1_2018.《https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html》.2018,
OCF.OCF_Security_Specification_v2.0.1.《http://openconnectivity.org》.2019,

审查员 李瑞梅

权利要求书4页 说明书18页 附图9页

(54)发明名称

资源请求方法、设备及存储介质

(57)摘要

本申请实施例提供一种资源请求方法、设备及存储介质，应用于控制设备的方法包括：生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据，向资源集合设备发送资源集合请求消息。控制设备通过生成第一校验数据，并将第一校验数据携带在资源集合请求消息，使得远端服务设备根据第一校验数据判断资源请求的来源的可靠性，从而能够提高控制设备和远端服务节点之间传输的数据的安全性。

CN 110035058 B

1.一种资源请求方法,其特征在于,应用于控制设备,所述方法包括:

生成资源集合请求消息,所述资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据;

通过资源集合设备向所述至少一个远端服务节点中的每一个远端服务节点发送所述资源集合请求消息;

所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求进行加密得到的,用于向所述至少一个远端服务节点指示发送所述资源集合请求消息的控制设备。

2.根据权利要求1所述的方法,其特征在于,所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求中的第一信息进行加密得到的,所述第一信息用于标识对不同的远端服务节点的资源请求。

3.根据权利要求1或2所述的方法,其特征在于,所述加密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

4.根据权利要求3所述的方法,其特征在于,所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

5.根据权利要求3所述的方法,其特征在于,所述控制设备中保存有多个不同的共享密钥,所述多个共享密钥中的每个共享密钥对应一个远端服务节点。

6.根据权利要求1或2所述的方法,其特征在于,所述加密密钥为第一私钥。

7.根据权利要求1或2所述的方法,其特征在于,所述第一校验数据中还包括对应的远端服务节点的资源请求的标识,用于所述远端服务节点判断资源请求是否为重放请求。

8.根据权利要求1或2所述方法,其特征在于,所述方法还包括:

接收所述资源集合设备发送的所述资源集合请求消息对应的资源集合响应消息,所述资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据;

采用解密密钥对所述第二校验数据进行解密。

9.根据权利要求8所述的方法,其特征在于,所述解密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

10.根据权利要求9所述的方法,其特征在于,所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

11.根据权利要求9所述的方法,其特征在于,所述控制设备中保存有多个不同的共享密钥,所述多个共享密钥中的每个共享密钥对应一个远端服务节点。

12.根据权利要求8所述的方法,其特征在于,所述解密密钥包括第一私钥和第二公钥;

采用解密密钥对所述第二校验数据进行解密,包括:

采用所述第一私钥对所述第二校验数据进行第一次解密,得到所述远端服务节点的资源响应以及第一加密数据;

根据所述远端服务节点的标识,确定所述第二公钥;

采用所述第二公钥对所述第一加密数据进行第二次解密,得到所述远端服务节点的资源响应。

13.根据权利要求12所述的方法,其特征在于,所述方法还包括:

当第一次解密得到的所述远端服务节点的资源响应和第二次解密得到的远端服务节

点的资源响应相同时，确定所述远端服务节点的资源响应正确。

14.根据权利要求8所述的方法，其特征在于，所述解密密钥包括第二公钥，所述资源集合响应消息中还包括至少一个远端服务节点的资源响应；

采用解密密钥对所述第二校验数据进行解密，包括：

根据所述远端服务节点的标识，确定所述第二公钥；

采用所述第二公钥对所述第二校验数据进行解密，得到所述远端服务节点的资源响应。

15.根据权利要求14所述的方法，其特征在于，所述方法还包括：

当所述资源集合响应消息中包括的所述远端服务节点的资源响应和解密得到的所述远端服务节点的资源响应相同时，确定所述远端服务节点的资源响应正确。

16.根据权利要求8所述的方法，其特征在于，所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述资源响应的标识用于判断资源响应是否为重放消息。

17.一种资源请求方法，其特征在于，应用于远端服务节点，所述方法包括：

接收控制设备通过资源集合设备发送的资源请求消息，所述资源请求消息中包括对所述远端服务节点的资源请求及其对应的第一校验数据，所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求进行加密得到的，用于向所述远端服务节点指示发送所述资源集合请求消息的控制设备；

采用解密密钥对所述第一校验数据进行解密。

18.根据权利要求17所述的方法，其特征在于，所述解密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

19.根据权利要求18所述的方法，其特征在于，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

20.根据权利要求18所述的方法，其特征在于，所述共享密钥与其他远端服务节点对应的共享密钥不同。

21.根据权利要求17所述的方法，其特征在于，所述解密密钥为第一公钥。

22.根据权利要求17-21任一项所述方法，其特征在于，解密结果中包括对所述远端服务节点的资源请求或者对所述远端服务节点的资源请求中的第一信息，第一信息用于标识对不同远端服务节点的资源请求。

23.根据权利要求17-21任一项所述方法，其特征在于，所述第一校验数据中还包括所述远端服务节点的资源请求的标识，所述资源请求的标识用于判断资源请求是否为重放消息。

24.根据权利要求17-21任一项所述的方法，其特征在于，所述方法还包括：

生成资源响应消息，所述资源响应消息中包括所述远端服务节点的资源响应对应的第二校验数据；

向所述资源集合设备发送所述资源响应消息。

25.根据权利要求24所述的方法，其特征在于，所述第二校验数据由所述远端服务节点采用加密密钥对所述远端服务节点的资源响应加密得到。

26.根据权利要求25所述的方法，其特征在于，所述加密密钥为所述远端服务节点与所述控制设备之间的共享密钥。

27.根据权利要求26所述的方法，其特征在于，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

28.根据权利要求26所述的方法，其特征在于，所述共享密钥与其他远端服务节点对应的共享密钥不同。

29.根据权利要求25所述的方法，其特征在于，所述加密密钥为第二私钥。

30.根据权利要求25所述的方法，其特征在于，所述加密密钥为第二私钥和第一公钥，所述第二私钥用于对所述远端服务节点的资源响应进行加密得到第一加密数据，所述第一公钥用于对所述远端服务节点的资源响应和所述第一加密数据进行加密得到所述第二校验数据。

31.根据权利要求25所述的方法，其特征在于，所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述远端服务节点的资源响应的标识用于判断资源响应是否为重放消息。

32.一种控制设备，其特征在于，包括：

生成模块，用于生成资源集合请求消息，所述资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据；

发送模块，用于通过资源集合设备向所述至少一个远端服务节点中的每一个远端服务节点发送所述资源集合请求消息；

所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求进行加密得到的，用于向所述至少一个远端服务节点指示发送所述资源集合请求消息的控制设备。

33.根据权利要求32所述的设备，其特征在于，所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求中的第一信息进行加密得到的，所述第一信息用于标识对不同的远端服务节点的资源请求。

34.根据权利要求32或33所述的设备，其特征在于，所述第一校验数据中还包括对应的远端服务节点的资源请求的标识，用于所述远端服务节点判断资源请求是否为重放请求。

35.根据权利要求32或33所述设备，其特征在于，还包括：

接收模块，用于接收所述资源集合设备发送的所述资源集合请求消息对应的资源集合响应消息，所述资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据；

解密模块，用于采用解密密钥对所述第二校验数据进行解密。

36.根据权利要求35所述的设备，其特征在于，所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述资源响应的标识用于判断资源响应是否为重放消息。

37.一种远端服务节点，其特征在于，包括：

接收模块，用于接收控制设备通过资源集合设备发送的资源请求消息，所述资源请求消息中包括对所述远端服务节点的资源请求及其对应的第一校验数据，所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求进行加密得到的，用于向所述远端服务节点指示发送所述资源集合请求消息的控制设备；

解密模块，用于采用解密密钥对所述第一校验数据进行解密。

38.根据权利要求37所述的节点，其特征在于，解密结果中包括对所述远端服务节点的

资源请求或者对所述远端服务节点的资源请求中的第一信息，第一信息用于标识对不同的远端服务节点的资源请求。

39.根据权利要求37或38所述的节点，其特征在于，所述第一校验数据中还包括所述远端服务节点的资源请求的标识，所述资源请求的标识用于判断资源请求是否为重放消息。

40.根据权利要求37或38所述的节点，其特征在于，还包括：

生成模块，用于生成资源响应消息，所述资源响应消息中包括所述远端服务节点的资源响应对应的第二校验数据；

发送模块，用于向所述资源集合设备发送所述资源响应消息。

41.根据权利要求40所述的节点，其特征在于，所述第二校验数据由所述远端服务节点采用加密密钥对所述远端服务节点的资源响应加密得到。

42.根据权利要求41所述的节点，其特征在于，所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述远端服务节点的资源响应的标识用于判断资源响应是否为重放消息。

43.一种控制设备，其特征在于，包括：

处理器、存储器、与网络设备进行通信的接口；

所述存储器存储计算机执行指令；

所述处理器执行所述存储器存储的计算机执行指令，使得所述处理器执行如权利要求1至16任一项所述的资源请求方法。

44.一种远端服务节点，其特征在于，包括：

处理器、存储器、与终端设备进行通信的接口；

所述存储器存储计算机执行指令；

所述处理器执行所述存储器存储的计算机执行指令，使得所述处理器执行如权利要求17至31任一项所述的资源请求方法。

45.一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中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现如权利要求1至16任一项所述的资源请求方法。

46.一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中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现如权利要求17至31任一项所述的资源请求方法。

资源请求方法、设备及存储介质

技术领域

[0001] 本申请实施例涉及物联网技术，尤其涉及一种资源请求方法、设备及存储介质。

背景技术

[0002] 开放连接基金会(英文:Open Connectivity Foundation，简称:OCF)是物联网设备最大的工业连接和互操作性标准组织之一。OCF网络包括原客户端(英文:Original Client，简称:OC)、远端服务主机(英文:Remote Reference Host，简称:RRH)和组资源主机(英文:Collection Host，简称:CH)。

[0003] 其中，OC用于对RRH的资源进行操作，OC可以对多个RRH的资源进行操作，RRH的各种功能称为RRH的资源，OC和RRH通过CH进行连接和通信，CH用于对本地资源以及 RRH的资源进行统一管理。OC可以为智能手机、电脑等控制设备，CH可以为家庭网关等连接设备，RRH可以为提供各种服务的智能设备，例如智能台灯、智能音箱、智能空调等。当OC需要对RRH的资源进行操作时，OC向CH发送组(collection)资源请求，CH验证 OC是否具有访问RRH资源的权限，如有，则CH将collection资源请求分解为对每个RRH 的资源的请求，并向RRH发送资源请求，RRH向CH返回资源响应，CH将每个RRH的资源响应集成后，同一返回给OC。

[0004] 但是，现有的通信方案使得OC和RRH之间传输的数据的安全性低。

发明内容

[0005] 本申请实施例提供一种资源请求方法、设备及存储介质，提高了控制设备和远端服务节点之间传输的数据的安全性。

[0006] 第一方面，本申请实施例可提供一种资源请求方法，应用于控制设备，所述方法包括：

[0007] 生成资源集合请求消息，所述资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据；

[0008] 向资源集合设备发送所述资源集合请求消息。

[0009] 第二方面，本申请实施例可提供一种资源请求方法，应用于远端服务节点，所述方法包括：

[0010] 接收资源集合设备发送的资源请求消息，所述资源请求消息中包括所述远端服务节点的资源请求及其对应的第一校验数据；

[0011] 采用解密密钥对所述第一校验数据进行解密。

[0012] 第三方面，本申请实施例可提供一种资源请求方法，应用于资源集合设备，所述方法包括：

[0013] 接收控制设备发送的资源集合请求消息，所述资源集合请求消息中包括至少一个远端服务节点的资源请求及其对应的第一校验数据；

[0014] 将所述资源集合请求消息分解为对每个远端服务节点的资源请求消息，所述每个远端服务节点的资源请求消息中包括该远端服务节点的资源请求及其第一校验数据；

[0015] 向所述每个远端服务节点发送对应的资源请求消息。

[0016] 第四方面，本申请实施例可提供一种控制设备，包括：

[0017] 生成模块，用于生成资源集合请求消息，所述资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据；

[0018] 发送模块，用于向资源集合设备发送所述资源集合请求消息。

[0019] 第五方面，本申请实施例可提供一种远端服务节点，包括：

[0020] 接收模块，用于接收资源集合设备发送的资源请求消息，所述资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据；

[0021] 解密模块，用于采用解密密钥对所述第一校验数据进行解密。

[0022] 第六方面，本申请实施例可提供一种资源集合设备，包括：

[0023] 接收模块，用于接收控制设备发送的资源集合请求消息，所述资源集合请求消息中包括至少一个远端服务节点的资源请求及其对应的第一校验数据；

[0024] 分解模块，用于将所述资源集合请求消息分解为对每个远端服务节点的资源请求消息，所述每个远端服务节点的资源请求消息中包括该远端服务节点的资源请求及其第一校验数据；

[0025] 发送模块，用于向所述每个远端服务节点发送对应的资源请求消息。

[0026] 第七方面，本申请实施例可提供一种控制设备，包括：

[0027] 处理器、存储器、与网络设备进行通信的接口；

[0028] 所述存储器存储计算机执行指令；

[0029] 所述处理器执行所述存储器存储的计算机执行指令，使得所述处理器执行如第一方面所述的资源请求方法。

[0030] 第八方面，本申请实施例可提供一种远端服务节点，包括：

[0031] 处理器、存储器、与终端设备进行通信的接口；

[0032] 所述存储器存储计算机执行指令；

[0033] 所述处理器执行所述存储器存储的计算机执行指令，使得所述处理器执行如第二方面所述的资源请求方法。

[0034] 第九方面，本申请实施例可提供一种资源集合设备，包括：

[0035] 处理器、存储器、与终端设备进行通信的接口；

[0036] 所述存储器存储计算机执行指令；

[0037] 所述处理器执行所述存储器存储的计算机执行指令，使得所述处理器执行如第三方面所述的资源请求方法。

[0038] 第十方面，本申请实施例可提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现如第一方面所述的资源请求方法。

[0039] 第十一方面，本申请实施例可提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现如第二方面所述的资源请求方法。

[0040] 第十二方面，本申请实施例可提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现如第三

方面所述的资源请求方法。

[0041] 第十三方面，本申请实施例提供一种程序，当该程序被处理器执行时，用于执行如上第一方面所述的资源请求方法。

[0042] 第十四方面，本申请实施例还提供一种程序，当该程序被处理器执行时，用于执行如上第二方面所述的资源请求方法。

[0043] 第十五方面，本申请实施例还提供一种程序，当该程序被处理器执行时，用于执行如上第三方面所述的资源请求方法。

[0044] 可选地，上述处理器可以为芯片。

[0045] 第十六方面，本申请实施例提供一种计算机程序产品，包括程序指令，程序指令用于实现第一方面所述的资源请求方法。

[0046] 第十七方面，本申请实施例提供一种计算机程序产品，包括程序指令，程序指令用于实现第二方面所述的资源请求方法。

[0047] 第十八方面，本申请实施例提供一种计算机程序产品，包括程序指令，程序指令用于实现第三方面所述的资源请求方法。

[0048] 第十九方面，本申请实施例提供了一种芯片，包括：处理模块与通信接口，该处理模块能执行第一方面所述的资源请求方法。

[0049] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行第一方面所述的资源请求方法。

[0050] 第二十方面，本申请实施例提供了一种芯片，包括：处理模块与通信接口，该处理模块能执行第二方面所述的资源请求方法。

[0051] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行第二方面所述的资源请求方法。

[0052] 第二十一方面，本申请实施例提供了一种芯片，包括：处理模块与通信接口，该处理模块能执行第三方面所述的资源请求方法。

[0053] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行第三方面所述的资源请求方法。

[0054] 本申请实施例提供的资源请求方法、设备及存储介质，应用于控制设备的方法包括：生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据，向资源集合设备发送资源集合请求消息。控制设备通过生成第一校验数据，并将第一校验数据携带在资源集合请求消息，使得远端服务设备根据第一校验数据判断该资源请求的来源是否可靠，从而提高了控制设备和远端服务节点之间传输的数据的安全性。

附图说明

[0055] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图做一简单地介绍，显而易见地，下面描述中的附图是本申

请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0056] 图1为本申请实施例适用的一种网络架构的示意图；

[0057] 图2为OCF网络中各设备的应用层的示意图；

[0058] 图3为本申请实施例一提供的资源请求方法的一种流程示意图；

[0059] 图4为本申请实施例二提供的资源请求方法的又一种流程示意图；

[0060] 图5为本申请实施例三提供的资源请求方法的另一种流程示意图；

[0061] 图6为本申请实施例四提供的资源请求方法的再一种流程示意图；

[0062] 图7为本申请实施例五提供的资源请求方法的再一种信令流程示意图；

[0063] 图8为本申请实施例六提供的资源请求方法的再一种信令流程示意图；

[0064] 图9为本申请实施例七提供的资源请求方法的再一种信令流程示意图；

[0065] 图10为本申请实施例八提供的一种控制设备的结构示意图；

[0066] 图11为本申请实施例九提供的另一种控制设备的结构示意图；

[0067] 图12为本申请实施例十提供的一种远端服务节点的结构示意图；

[0068] 图13为本申请实施例十一提供的另一种远端服务节点的结构示意图；

[0069] 图14为本申请实施例十二提供的又一种控制设备的结构示意图；

[0070] 图15为本申请实施例十三提供的又一种远端服务节点的结构示意图。

具体实施方式

[0071] 为使本申请实施例的目的、技术方案和优点更加清楚，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，所描述的实施例是本申请一部分实施例，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，都属于本申请保护的范围。

[0072] 本申请实施例的说明书、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。

[0073] 图1为本申请实施例适用的一种网络架构的示意图。如图1所示，该网络架构中至少包括控制设备11、资源集合设备12和远端服务节点13。可以理解的是，在实际网络部署中，控制设备11、资源集合设备12和远端服务节点13均可以有一个或多个，该图1仅以一个作为示例。

[0074] 控制设备11和资源集合设备12之间可以通过有线或者无线方式进行连接通信，同样，资源集合设备12和远端服务节点13之间也可以通过有线或者无线方式进行连接通信。

[0075] 控制设备11通过资源集合设备12对远端服务节点13提供的资源进行访问和操作，每个远端服务节点13能够提供一种或多种资源，该资源可以是远端服务节点13 的功能。资源集合设备12用于对本地资源以及远端服务节点13提供的资源进行统一管理，为控制设备

11提供访问资源的接口。

[0076] 如图2所示，该网络架构可以为OCF网络，相应的，控制设备11为OC，资源集合设备为12为CH，远端服务节点13为RRH。可以理解是，该网络架构不限于OCF 网络，还可以为物联网环境下通过一个中间设备(功能类似于CH)控制作为客户端和服务端的智能设备。

[0077] 以OCF网络为例，OC可以为智能手机、个人电脑、平板电脑等，CH可以为家庭网关或者其他网关设备，RRH可以为智能家电设备，例如智能台灯、智能冰箱、智能音箱等。

[0078] 图2为OCF网络中各设备的应用层的示意图。如图2所示，CH上包括第一访问控制项(英文:Access Control Entry，简称:ACE)、第二ACE和组资源(collection resource)A。其中，第一ACE定义了允许OC访问的组资源A，组资源A为CH的本地资源，第二ACE定义了允许OC访问的组资源B，组资源B为RRH的资源。

[0079] 示例性的，第一ACE中包括组资源A的信息以及允许访问的OC的ID或者规则，第二ACE中包括组资源B的信息以及允许访问的OC的ID或者规则。

[0080] CH接收到OC发送的collection资源请求消息时，判断OC是否与第一ACE和第二ACE匹配。如果匹配，CH对collection资源请求消息进行分解、封装，得到RRH 的资源请求，将RRH的资源请求发送给RRH。

[0081] RRH上包括第三ACE，该第三ACE定义了允许CH访问组资源B，可选的，RRH 上还包括第四ACE，该ACE定义了允许OC访问的组资源B。当RRH收到CH发送的资源访问请求消息时，根据第三ACE判断是否执行该请求，并向CH返回响应。CH收集到所有响应后，统一打包发送给OC。

[0082] CH上包括一个或多个collection资源，每个collection资源包括一个或多个link资源，每个link资源为CH的本地资源或RRH的一种资源的地址或者索引。

[0083] 例如，一个Collection资源包含设备A(light)的开关资源的link，以及设备B(fan)的开关资源的link，形成了集中的资源组。OC可以通过访问Collection资源的oic.if.b接口同时请求多个资源，CH会把请求发送给links中的每一个资源，并收集每个资源返回的响应，集中后统一返回给OC。

[0084] 现有技术中，CH存在被非法控制的风险，从而导致RRH接收到的资源请求消息被篡改，或者，OC接收到的组资源响应消息被篡改。为了解决现有技术中的问题，本申请提供一种资源请求方法。

[0085] 图3为本申请实施例一提供的资源请求方法的一种流程示意图，本实施例从控制设备的角度描述该方法，如图3所示，本实施例提供的方法包括以下步骤：

[0086] S101、生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据。

[0087] 不同于现有技术，本实施例中在资源集合请求消息中携带了对远端服务节点的资源请求对应的第一校验数据，该第一校验数据用于远端服务节点验证资源请求的来源是否可靠，即远端服务节点根据第一校验数据验证资源请求是否由该控制设备发送，而不是由其他设备发送。该资源请求消息中还包括其他信息，例如，控制设备的标识。

[0088] 当本实施例的方法应用在OCF网络中时，该资源集合请求消息可以为collection资源请求消息。

[0089] 该第一校验数据可以为控制设备采用加密密钥对远端服务节点的资源请求进行

加密得到的。或者，该第一校验数据为控制设备采用加密密钥对远端服务节点的资源请求中的第一信息进行加密得到的，该第一信息用于标识对不同的远端服务节点的资源请求，该资源请求中除第一信息外的其他信息可以称为第二信息。可选的，第一信息可以是多个信息。

[0090] 该加密密钥可以是控制设备和远端服务节点预先协商确定的，也可以是其他管理设备为控制设备配置的，还可以是工作人员手动配置的。

[0091] 控制设备可以采用该加密密钥对远端服务节点的资源请求整体进行加密，也可以对远端服务节点的资源请求中的第一信息进行加密。本实施例不对该第一信息限定，只要该第一信息能够标识对不同的远端服务节点的资源请求即可，例如，该第一信息为资源的地址。

[0092] 本实施例中，控制设备和远端服务节点可以采用对称加密算法，也可以采用非对称加密算法。

[0093] 对称加密算法中使用的密钥为控制设备与远端服务节点之间的共享密钥，共享密钥指控制设备和远端服务节点使用同一个密钥，共享密钥用于对远端服务节点的资源请求进行加密得到第一校验数据，相应的，远端服务节点使用该共享密钥才能解密第一校验数据。

[0094] 可选的，该共享密钥为控制设备与多个远端服务节点共用的密钥。该方式中，多个不同的远端服务节点使用的密钥相同。

[0095] 或者，控制设备中保存有多个不同的共享密钥，该多个共享密钥中的每个共享密钥对应一个远端服务节点，即不同的远端服务节点的使用的密钥不同。

[0096] 非对称加密算法中控制设备和远端服务节点使用不同的密钥进行加密和解密。本实施例中，为控制设备和远端服务节点分别配置了一对公钥和私钥，使用私钥加密的数据，只能使用对应的公钥进行解密，同理，使用公钥加密的数据，只能使用对应的私钥进行解密。

[0097] 本申请的各实施例中，将为控制设备配置的公钥称为第一公钥，将为控制设备配置的私钥称为第一私钥，通过第一私钥加密的数据只能被第一公钥解密，通过第一公钥加密的数据只能被第一私钥解密。第一私钥存储在控制设备的安全区域，只能被控制设备调用。

[0098] 将为远端服务节点配置的公钥称为第二公钥，将为远端服务节点配置的私钥称为第二私钥，通过第二私钥加密的数据只能被第二公钥解密，通过第二公钥加密的数据只能被第二私钥解密。第二私钥存储在远端服务节点的安全区域，只能被远端服务节点调用。

[0099] 本实施例中，控制设备还存储有第二公钥，远端服务节点还存储有第一公钥。

[0100] 本实施例中，控制设备使用第一私钥对远端服务节点的资源请求或者资源请求中的第一信息进行加密得到第一校验数据，相应的，远端服务节点使用第一公钥才能解密第一校验数据。

[0101] 可选的，第一校验数据中还包括对远端服务节点的资源请求的标识，该资源请求的标识用于远端服务节点判断资源请求是否为重放请求。如果第一校验数据中包括对远端服务节点的资源请求的标识，则控制设备在生成第一校验数据时，使用加密密钥对远端服务节点的资源请求(或者资源请求中的第一信息)和资源请求的标识一起进行加密，得到第

一校验数据。

[0102] 资源集合设备会缓存对远端服务节点的资源请求，如果资源集合设备被非法控制了，资源集合设备可能会重复发送之前缓存的对远端服务节点的资源请求进行重放攻击。重放攻击也称为重播攻击或者回放攻击，重放攻击主要用于身份认证过程中，破坏认证的正确性。

[0103] 本实施例中，针对每个资源请求，控制设备生成了该资源请求的标识，该资源请求的标识用于唯一标示一个资源请求。通过将该资源请求的标识与对远端服务节点的资源请求(或者资源请求中的第一信息)一起被加密，从而保证了资源请求的标识不被篡改。

[0104] 远端服务节点通过解密得到资源请求的标识，并判断该资源请求的标识是否为新的标识，如果该资源请求的标识为新的标识，则确定该资源请求不是重放消息，如果该资源请求的标识不是新的标识，则确定该资源请求为重放消息。该资源请求的标识不是新的标识，说明该资源请求的标识已经被发送过，所以能够确定该资源请求为重放消息。远端服务节点根据判断结果进行处理。

[0105] 可选的，该资源请求的标识为序列号或者时间戳。该序列号可以按照预设的规则生成，例如，每次在前一次序列号的基础上加一，该序列号还可以随机生成。该时间戳可以为对远端服务节点的资源请求的生成时间或者资源集合请求消息的生成时间。

[0106] S102、向资源集合设备发送资源集合请求消息。

[0107] 控制设备将资源集合请求消息发送给资源集合设备，资源集合设备将资源集合请求消息分解为对每个远端服务节点的资源请求消息，对每个远端服务节点的资源请求消息中包括对该远端服务节点的资源请求及其第一校验数据，并向每个远端服务节点发送对应的资源请求消息，该资源请求中还包括控制设备的标识。

[0108] 资源集合设备对资源集合请求消息进行分解和重组得到对每个远端服务节点的资源请求消息。分解和重组方法参照现有已有技术，这里不再赘述。

[0109] 本实施例中，控制设备通过生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据，向资源集合设备发送资源集合请求消息。使得远端服务节点根据第一校验数据验证该资源请求的来源是否可靠，从而提高了数据传输的安全性。

[0110] 图4为本申请实施例二提供的资源请求方法的又一种流程示意图，在实施例一的基础上，远端服务节点可以对资源响应进行了加密，相应的，控制设备对资源响应进行解密操作，以验证资源响应的来源是否可靠。如图4所示，本实施例的方法，在实施例一的基础上，还包括以下步骤：

[0111] S103、接收资源集合设备发送的资源集合请求消息对应的资源集合响应消息，资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据。

[0112] 该资源集合响应消息是资源集合设备对该至少一个远端服务节点发送的资源响应消息进行组合得到的。当本实施例的方法应用在OCF网络中时，该资源集合响应消息可以为collection资源响应消息。

[0113] S104、采用解密密钥对第二校验数据进行解密。

[0114] 控制设备根据解密结果验证资源响应的来源是否可靠，示例性的，如果控制设备使用解密密钥能够成功解码第二校验数据，则确定资源响应的来源可靠，如果控制设备使

用解密密钥不能成功解密第二校验数据，则确定资源响应的来源不可靠。

[0115] 当采用对称加密算法时，该解密密钥为控制设备与远端服务节点之间的共享密钥。该共享密钥可以为控制设备与多个所述远端服务节点共用的密钥，或者，控制设备中保存有多个不同的共享密钥，多个共享密钥中的每个共享密钥对应一个远端服务节点，控制设备根据远端服务节点的标识查询对应的共享密钥，使用远端服务节点对应的共享密钥进行解密，远端服务节点的标识携带在资源集合请求消息中。

[0116] 可选的，采用对称加密算法时，该资源集合请求消息中还包括明文的资源响应。

[0117] 当采用非对称加密算法时，一种实现方式中，解密密钥包括第一私钥和第二公钥。

[0118] 相应的，控制设备采用如下方式进行解密：采用第一私钥对第二校验数据进行第一次解密，得到远端服务节点的资源响应以及第一加密数据。根据远端服务节点的标识确定第二公钥，采用第二公钥对第一加密数据进行第二次解密，得到远端服务节点的资源响应。由于控制设备上存储有多个远端服务节点的公钥，因此，需要根据远端服务节点的标识确定第二公钥。

[0119] 可选的，控制设备还比较第一次解密得到的远端服务节点的资源响应和第二次解密得到的远端服务节点的资源响应，当第一次解密得到的远端服务节点的资源响应和第二次解密得到的远端服务节点的资源响应相同时，确定远端服务节点的资源响应正确。

[0120] 该方式中，远端服务节点通过第一公钥对资源响应进行加密，使得网络中的其他节点无法获得资源响应。

[0121] 如果第一次解密得到的远端服务节点的资源响应和第二次解密得到的远端服务节点的资源响应不相同，则确定远端服务节点的资源响应不正确。

[0122] 当采用非对称加密算法时，另一种方式中，该解密密钥包括第二公钥，资源集合响应消息中还包括至少一个远端服务节点的资源响应。控制设备根据远端服务节点的标识确定第二公钥，采用第二公钥对第二校验数据进行解密，得到远端服务节点的资源响应。

[0123] 该方式中，资源集合响应消息中包括的远端服务节点的资源响应是明文数据，即远端服务节点只对资源响应进行了签名，控制设备通过签名同样能够确认消息的来源是否为该远端服务节点。但是，资源集合响应消息中携带的明文的资源响应可能被网络中其他节篡改。

[0124] 可选的，控制设备比较资源集合响应消息中包括的远端服务节点的资源响应和解密得到的远端服务节点的资源响应，当资源集合响应消息中包括的远端服务节点的资源响应和解密得到的远端服务节点的资源响应相同时，则确定远端服务节点的资源响应正确，如果资源集合响应消息中包括的远端服务节点的资源响应和解密得到的远端服务节点的资源响应不相同，则确定远端服务节点的资源响应不正确，被其他节点篡改了。

[0125] 可选的，第二校验数据中还包括远端服务节点的资源响应的标识，该资源响应的标识用于判断资源响应是否为重放消息。

[0126] 相应的，控制设备根据远端服务节点的资源响应的标识，判断远端服务节点的资源响应是否为重放消息，当远端服务节点的资源响应为重放消息时，结束流程；当远端服务节点的资源响应不为重放消息时，根据解密得到的数据验证远端服务节点的资源响应是否正确。

[0127] 其中，控制设备判断资源响应是否为重放消息的方式与远端服务节点判断资源请

求是否为重放消息的方式相同，这里不再赘述。

[0128] 可选的，该资源响应的标识为序列号或者时间戳。可以理解，该资源响应的标识可以与对应的资源请求的标识关联，也可以不关联。

[0129] 当该资源响应的标识可以与对应的资源请求的标识关联时，该资源响应的标识可以与对应的资源请求的标识相同。该资源响应的标识也可以是在资源请求的标识的基础上按照某种规则计算得到，例如，当资源请求的标识为序列号时，资源响应的标识可以是在资源请求消息中携带的序列号的基础上加N，N大于或等于1。当资源请求的标识为时间戳时，资源响应的标识可以是在资源请求消息中携带的时间戳的基础上加上预设时间得到。

[0130] 本实施例中，控制设备接收所述资源集合设备发送的所述资源集合请求消息对应的资源集合响应消息，资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据，使用解密密钥对第二校验数据进行解密，如果能够解密成功，则确定资源响应的来源可靠，从而提高了数据传输的安全性。

[0131] 图5为本申请实施例三提供的资源请求方法的另一种流程示意图，本实施例从远端服务节点的角度描述该方法，如图5所示，本实施例的方法包括以下步骤：

[0132] S201、接收资源集合设备发送的资源请求消息，资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据。

[0133] 该第一校验数据是控制设备采用加密密钥对远端服务节点的资源请求加密得到的，或者，该第一校验数据是控制设备对远端服务节点的资源请求中的第一信息进行加密得到的。

[0134] S202、采用解密密钥对第一校验数据进行解密。

[0135] 远端服务节点根据解密结果验证资源请求的来源是否可靠，如果远端服务节点使用解密密钥成功解密第一校验数据，则确定资源请求的来源可靠，如果远端服务节点使用解密密钥解密失败，则确定资源请求的来源不可靠。

[0136] 该解密结果中包括对远端服务节点的资源请求或者对远端服务节点的资源请求中的第一信息。

[0137] 可选的，如果解密结果中包括对远端服务节点的资源请求，远端服务节点可以将解密得到的资源请求与资源请求消息中包括的明文的资源请求进行比较，以验证该资源请求的可靠性。

[0138] 当采用对称加密算法时，该解密密钥为所控制设备与远端服务节点之间的共享密钥。可选的，该共享密钥为控制设备与多个所述远端服务节点共用的密钥，或者，该共享密钥与其他远端服务节点对应的共享密钥不同，即每个远端服务节点对应一个共享密钥，多个远端服务节点对应的多个共享密钥不同。

[0139] 当采用非对称加密算法时，第一校验数据采用第一私钥加密得到，相应的，该解密密钥为第一公钥。

[0140] 可选的，该第一校验数据中还包括远端服务节点的资源请求的标识，该资源请求的标识用于判断资源请求是否为重放消息。

[0141] 远端服务节点解密得到资源请求的标识，根据资源请求的标识判断该资源请求是否为重放消息，当该资源请求不为重放消息时，验证远端服务节点的资源请求是否正确。当该资源请求为重放消息时，结束流程，可选的，还可以向管理设备上报该重放事件。

[0142] 远端服务节点通过判断资源请求的标识是否为新的标识确定资源请求是否为重放消息。远端服务节点可以通过如下方式判断资源请求的标识是否为新的标识：

[0143] (1)当资源请求的标识为时间戳时，远端服务节点判断当前资源请求中携带的时间戳是否大于上一个资源请求中携带的时间戳，如果当前资源请求中携带的时间戳大于上一个资源请求中携带的时间戳，则确定当前资源请求的标识为新的标识。如果当前资源请求中携带的时间戳不大于(小于或等于)上一个资源请求中携带的时间戳，则确定当前资源请求的标识不是新的标识。

[0144] 远端服务节点每次接收到一个新的资源请求后，保存该资源请求中携带的时间戳，用于下一次的判断。

[0145] (2)当资源请求的标识为序列号时，如果控制设备生成的序列号按照某种规则增大，则远端服务节点判断当前资源请求携带的当前序列号是否为上一个资源请求携带的序列号增大后的值，如果是，则确定当前资源请求的标识是新的标识，否则，确定当前资源请求的标识不是新的标识。

[0146] 或者，远端服务节点判断当前资源请求携带的当前序列号是否与本地保存的已经接收到的资源请求携带的序列号相同，如果不相同，则确定当前资源请求的标识是新的标识，如果相同，则确定当前资源请求的标识不是新的标识。

[0147] 本实施例中，远端服务节点通过接收资源集合设备发送的资源请求消息，资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据，使用解密密钥解密第一校验数据，根据解密结果验证资源请求的来源是否可靠，从而提高了控制设备和远端服务节点之间传输的数据的安全性。

[0148] 图6为本申请实施例四提供的资源请求方法的再一种流程示意图，本实施例在实施例三的基础上，远端服务节点向控制设备发送了资源响应，并对资源响应进行了加密，如图6所示，本实施例的方法包括以下步骤：

[0149] S203、生成资源响应消息，资源响应消息中包括远端服务节点的资源响应对应的第二校验数据。

[0150] 远端服务节点验证资源请求的来源可靠之后，生成资源响应消息，不同于现有技术，该资源响应消息中携带了远端服务节点的资源响应对应的第二校验数据。

[0151] 该第二校验数据用于控制设备验证远端服务节点的资源响应的来源是否可靠。该第二校验数据由远端服务节点采用加密密钥对远端服务节点的资源响应加密得到。

[0152] 当采用对称加密算法进行加密时，该加密密钥为远端服务节点与控制设备之间的共享密钥。可选的，该共享密钥为控制设备与多个远端服务节点共用的密钥，或者，该共享密钥与其他远端服务节点使用的共享密钥不同。

[0153] 当采用非对称加密算法进行加密时，该加密密钥为第二私钥，或者，该加密密钥为第二私钥和第一公钥。

[0154] 当该加密密钥为远端服务节点上保存的第二私钥和第一公钥时，远端服务节点先用第二私钥对远端服务节点的资源响应进行加密得到第一加密数据，然后使用第一公钥对远端服务节点的资源响应和第一加密数据进行加密得到第二校验数据。该方式中，通过两次加密，使得资源集合设备无法获取到远端服务节点的资源响应。

[0155] 可选的，该第二校验数据中还包括远端服务节点的资源响应的标识，远端服务节

点的资源响应的标识用于判断资源响应是否为重放消息。其中，远端服务节点的资源请求的标识为序列号或者时间戳。

[0156] S204、向资源集合设备发送资源响应消息。

[0157] 本实施例中，远端服务节点通过在资源响应消息中携带远端服务节点的资源响应对应的第二校验数据，以使得控制设备根据该第二校验数据验证资源响应的来源是否可靠，从而提高了控制设备和远端服务节点之间传输的数据的安全性。

[0158] 基于上述方案，下面以OCF网络为例，说明OCF网络中资源请求方法的几种方式。

[0159] 图7为本申请实施例五提供的资源请求方法的再一种信令流程示意图，本实施例以OCF网络为例，且OC和RRH采用对称加密算法进行加密为例进行说明，如图7 所示，本实施例的方法包括以下步骤：

[0160] S301、为OC和RRH配置共享密钥。

[0161] 可选的，该共享密钥为OC与多个RRH共用的密钥，或者，多个RRH的共享密钥不同。

[0162] S302、OC生成collection请求消息，包括对RRH的资源请求及其对应的第一校验数据。

[0163] OC先生成RRH的资源请求和序列号，然后，使用共享密钥对RRH的资源请求和序列号进行加密，得到第一校验数据，将RRH的资源请求和第一校验数据携带在 collection请求消息中，collection请求消息中还可以包括其他信息，例如，OC的标识。

[0164] 例如，该RRH可以为灯1(light)，RRH的资源请求用于请求灯1的开关资源，该collection请求消息可以包括对多个RRH的资源请求。

[0165] S303、OC将collection请求消息发送给CH。

[0166] S304、CH检查OC对collection资源的访问权限。

[0167] CH根据本次保存的OC的ACE，判断OC是否对collection资源具有访问权限，如果OC有权限，则执行S305，如果OC没有权限，则向OC返回拒绝消息。

[0168] S305、CH将collection请求消息分解为RRH的资源请求消息。

[0169] 如果collection请求消息中包括多个RRH的资源请求，则将collection请求消息分解为多个RRH的资源请求消息，将OC的标识以及该RRH的资源请求及其对应的第一校验数据添加到RRH的资源请求消息中。

[0170] collection请求消息中包括明文的RRH的资源请求，即没有加密的RRH的资源请求，CH根据明文的RRH的资源请求对collection请求消息进行分解，得到各RRH的资源请求消息。

[0171] S306、CH将资源请求消息发送给RRH。

[0172] CH发送给RRH的资源请求消息中包括明文的RRH的资源请求和第一校验数据。

[0173] S307、RRH验证CH对资源的访问权限。

[0174] RRH接收到资源请求消息后，根据ACE验证CH对资源的访问权限，如果CH 对资源具有访问权限，则执行S308，如果CH对资源没有访问权限，则向CH返回拒绝消息，

[0175] S308、RRH共享密钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠。

[0176] RRH使用共享密钥对第一校验数据进行解密，得到资源请求和序列号，则确定资源请求的来源可靠。RRH判断解密得到的序列号是否为新的序列号，如果为新的序列号，则确

定该资源请求不是重放消息，执行步骤S309。

[0177] 可选的，还可以判断解密得到的资源请求与资源请求消息中携带的明文的资源请求是否相同，如果相同，则确定资源请求正确，在确定资源请求正确之后执行S309。如果解密得到的资源请求与资源请求消息中携带的明文的资源请求不相同，则确定资源请求不可靠，验证失败，RRH可以向CH返回请求失败消息。

[0178] 如果解密得到的序列号不是新的序列号，则确定资源请求消息为重放消息。RRH可以向CH返回请求失败消息，可选的，RRH还可以向其他设备上报发生重放攻击事件。

[0179] S309、执行RRH的资源请求对应的操作，得到执行结果。

[0180] 例如，如果RRH的资源请求对应的操作为关闭light1，则关闭light1。如果RRH 的资源请求对应的操作为开启light1，则开启light1。如果RRH的资源请求对应的操作为调整light1的颜色/亮度，则调整light1的颜色/亮度。

[0181] S310、RRH生成资源响应消息，该资源响应消息中包括RRH的资源响应对应的第二校验数据。

[0182] RRH的资源响应中包括S309中的执行结果，RRH使用共享密钥对RRH的资源响应和序列号进行加密得到第二校验数据，第二校验数据中的序列号可以与第一校验数据中携带的序列号相同，也可以不同。

[0183] 可选的，该资源响应消息中还可以包括明文的资源响应。

[0184] S311、RRH将资源响应消息发送给CH。

[0185] S312、CH向OC发送collection响应消息。

[0186] 如果collection请求消息中包括多个RRH的资源请求，则CH等待接收到所有RRH的资源响应消息后，统一打包发送给OC。

[0187] S313、OC使用共享密钥对第二校验数据进行解密，根据解密结果判断资源响应的来源是否可靠。

[0188] 如果解密得到RRH的资源响应和序列号，则确定资源响应的来源可靠。OC根据序列号判断RRH的资源响应是否为重放消息，如果不是重放消息。如果OC根据序列号判断RRH的资源响应为重放消息，则执行对应的操作，例如，向上层设备上报重放攻击事件，或者，统计重放消息的个数，本实施例不对此进行限制。

[0189] 图8为本申请实施例六提供的资源请求方法的再一种信令流程示意图，本实施例以OCF网络为例，且OC和RRH采用非对称加密算法进行加密为例进行说明，如图 8所示，本实施例的方法包括以下步骤：

[0190] S401、为OC配置第一私钥、第一公钥以及第二公钥，为RRH配置第二私钥、第二公钥和第一公钥。

[0191] S402、OC使用第一私钥对RRH的资源请求和序列号进行加密，得到第一校验数据。

[0192] OC将明文的资源请求和第一校验数据携带在collection请求消息中，collection请求消息中还包括OC的标识。

[0193] S403、OC将collection请求消息发送给CH。

[0194] S404、CH检查OC对collection资源的访问权限。

[0195] CH根据本次保存的OC的ACE，判断OC是否对collection资源具有访问权限，如果OC有权限，则执行S405，如果OC没有权限，则向OC返回拒绝消息。

[0196] S405、CH将collection请求消息分解为RRH的资源请求消息。

[0197] 如果collection请求消息中包括多个RRH的资源请求，CH根据collection请求消息中包括的多个明文的RRH的资源请求，将collection请求消息分解为多个RRH的资源请求消息，将OC的标识以及明文的RRH的资源请求及其对应的第一校验数据添加到RRH的资源请求消息中。

[0198] S406、CH将资源请求消息发送给RRH。

[0199] S407、RRH验证CH对资源的访问权限。

[0200] RRH接收到资源请求消息后，根据ACE验证CH对资源的访问权限，如果CH 对资源具有访问权限，则执行S308，如果CH对资源没有访问权限，则向CH返回拒绝消息，

[0201] S408、RRH使用第一公钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠。

[0202] RRH根据OC的ID查询得到第一公钥，使用第一公钥对第一校验数据进行解密，如果解密得到RRH的资源请求和序列号，则确定资源请求的来源可靠。RRH还可以判断解密得到的序列号是否为新的序列号，如果为新的序列号，则确定RRH的资源请求不是重放消息，如果解密得到的序列号不是新的序列号，则确定资源请求消息为重放消息。

[0203] 可选的，当判断RRH的资源请求不是重放消息时，可以进一步判断解密得到的 RRH的资源请求与资源请求消息中携带的明文的资源请求是否相同，如果相同，则确定RRH的资源请求正确，继续执行S409。如果解密得到的RRH的资源请求与资源请求消息中携带的明文的资源请求不相同，则确定RRH的资源请求不正确，RRH可以向CH返回请求失败消息。

[0204] 当确定RRH的资源请求为重放消息时，RRH可以向CH返回请求失败消息，可选的，RRH还可以向其他设备上报发生重放攻击事件。

[0205] S409、RRH执行资源请求对应的操作，得到执行结果。

[0206] S410、RRH使用第二私钥对RRH的资源响应进行加密，得到第一加密数据，使用第一公钥对RRH的资源响应、序列号和第一加密数据进行加密，得到第二校验数据。

[0207] RRH通过使用第一公钥对RRH的资源响应、序列号和第一加密数据进行加密，使得网络中的其他设备无法获取到RRH的资源响应。

[0208] 第二校验数据中的序列号可以与第一校验数据中携带的序列号相同，也可以不同。

[0209] S411、RRH将资源响应消息发送给CH。

[0210] 资源响应消息中包括RRH的资源响应及其对应的第二校验数据。

[0211] S412、CH向OC发送collection响应消息。

[0212] 如果collection请求消息中包括多个RRH的资源请求，则CH等待接收到所有RRH的资源响应消息后，统一打包发送给OC。

[0213] S413、OC使用第一私钥对第二校验数据进行解密，得到RRH的资源响应、序列号和第一加密数据。

[0214] S414、若OC验证序列号正确，则使用第二公钥对第一加密数据进行解密，根据解密结果判断RRH的资源响应的来源是否可靠。

[0215] 如果OC使用第二公钥成功解密第一加密数据，则确定RRH的资源响应的来源可靠。可选的，OC判断第二次解密得到的RRH的资源响应与第一次解密得到的RRH 的资源响应是

否相同，如果相同，则确定RRH的资源响应正确，如果第二次解密得到的RRH的资源响应与第一次解密得到的RRH的资源响应不相同，则确定RRH的资源响应不正确。

[0216] 需要说明的是，本实施例中以OC使用第一私钥对RRH的资源请求进行加密得到第一校验数据为例，可以理解的是，在本申请的其他实施例中，OC可以使用第一私钥对RRH的资源请求中的第一信息进行加密得到第一校验数据。另外，本实施例中序列号可以替换为时间戳。

[0217] 图9为本申请实施例七提供的资源请求方法的再一种信令流程示意图，本实施例与实施例六的区别为：本实施例中RRH仅对资源响应进行了签名，没有加密，如图9 所示，本实施例的方法包括以下步骤：

[0218] S501、为OC配置第一私钥、第一公钥以及第二公钥，为RRH配置第二私钥、第二公钥和第一公钥。

[0219] S502、OC使用第一私钥对RRH的资源请求和序列号进行加密，得到第一校验数据。

[0220] OC将明文的资源请求和第一校验数据携带在collection请求消息中，collection请求消息中还包括OC的标识。

[0221] S503、OC将collection请求消息发送给CH。

[0222] S504、CH检查OC对collection资源的访问权限。

[0223] S505、CH将collection请求消息分解为RRH的资源请求消息。

[0224] S506、CH将资源请求消息发送给RRH。

[0225] S507、RRH验证CH对资源的访问权限。

[0226] S508、RRH使用第一公钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠。

[0227] S509、执行RRH的资源请求对应的操作，得到执行结果。

[0228] S501-S509的步骤与实施例六中S401-S409相同，这里不再赘述。

[0229] S510、RRH使用第二私钥对RRH的资源响应和序列号进行加密，得到第二校验数据。

[0230] 不同于实施例四，本实施例中，RRH仅使用第二私钥对RRH的资源响应和序列号进行了签名。

[0231] S511、RRH将资源响应消息发送给CH。

[0232] 该资源响应消息中包括明文的RRH的资源响应、第二校验数据以及RRH的标识。

[0233] S512、CH向OC发送collection响应消息。

[0234] CH对多个RRH发送的资源响应消息进行打包后得到collection响应消息。

[0235] S513、OC使用第二公钥对第二校验数据进行解密。

[0236] S514、OC根据解密结果判断RRH的资源响应的来源是否可靠。

[0237] 如果OC使用第二公钥正确解密得到资源响应和序列号，则确定资源响应的来源可靠。OC根据解密得到的序列号判断RRH的资源响应是否为重放消息，如果不是重放消息，则判断解密得到的RRH的资源响应与collection响应消息中包括的RRH的资源响应是否相同，如果相同，则确定RRH的资源响应正确，如果不相同，则确定 RRH的资源响应不正确。

[0238] 图10为本申请实施例八提供的一种控制设备的结构示意图，如图10所示，该控制设备100包括：

[0239] 生成模块111，用于生成资源集合请求消息，所述资源集合请求消息中包括对至少

一个远端服务节点的资源请求及其对应的第一校验数据；

[0240] 发送模块112，用于向资源集合设备发送所述资源集合请求消息。

[0241] 可选的，所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求进行加密得到的。或者，所述第一校验数据为所述控制设备采用加密密钥对所述远端服务节点的资源请求中的第一信息进行加密得到的，所述第一信息用于标识对不同的远端服务节点的资源请求。

[0242] 可选的，所述加密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

[0243] 其中，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

[0244] 或者，所述控制设备中保存有多个不同的共享密钥，所述多个共享密钥中的每个共享密钥对应一个远端服务节点。

[0245] 可选的，所述加密密钥为第一私钥。

[0246] 可选的，所述第一校验数据中还包括对应的远端服务节点的资源请求的标识，用于所述远端服务节点判断资源请求是否为重放请求。

[0247] 可选的，所述远端服务节点的资源请求的标识为序列号或者时间戳。

[0248] 图11为本申请实施例九提供的另一种控制设备的结构示意图，如图11所示，该控制设备100在图10所示设备的基础上，还包括：

[0249] 接收模块113，用于接收所述资源集合设备发送的所述资源集合请求消息对应的资源集合响应消息，所述资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据；

[0250] 解密模块114，用于采用解密密钥对所述第二校验数据进行解密。

[0251] 可选的，所述解密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

[0252] 其中，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

[0253] 或者，所述控制设备中保存有多个不同的共享密钥，所述多个共享密钥中的每个共享密钥对应一个远端服务节点。

[0254] 可选的，所述解密密钥包括第一私钥和第二公钥，相应的，所述解密模块114具体用于：

[0255] 采用所述第一私钥对所述第二校验数据进行第一次解密，得到所述远端服务节点的资源响应以及第一加密数据；

[0256] 根据所述远端服务节点的标识，确定所述第二公钥；

[0257] 采用所述第二公钥对所述第一加密数据进行第二次解密，得到所述远端服务节点的资源响应。

[0258] 可选的，还包括：验证模块，用于当第一次解密得到的所述远端服务节点的资源响应和第二次解密得到的远端服务节点的资源响应相同时，确定所述远端服务节点的资源响应正确。

[0259] 可选的，所述解密密钥包括第二公钥，所述资源集合响应消息中还包括至少一个远端服务节点的资源响应。相应的，所述解密模块114具体用于：

[0260] 根据所述远端服务节点的标识，确定所述第二公钥；

[0261] 采用所述第二公钥对所述第二校验数据进行解密，得到所述远端服务节点的资源响应。

[0262] 可选的，还包括：验证模块，用于当所述资源集合响应消息中包括的所述远端服务节点的资源响应和解密得到的所述远端服务节点的资源响应相同时，确定所述远端服务节点的资源响应正确。

[0263] 可选的，所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述资源响应标识用于判断资源响应是否为重放消息。

[0264] 上述任一实现方式提供的控制设备，用于执行前述任一方法实施例中控制设备执行的技术方案，其实现原理和技术效果类似，在此不再赘述。

[0265] 图12为本申请实施例十提供的一种远端服务节点的结构示意图，如图12所示，该远端服务节点200包括：

[0266] 接收模块211，用于接收资源集合设备发送的资源请求消息，所述资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据；

[0267] 解密模块212，用于采用解密密钥对所述第一校验数据进行解密。

[0268] 解密结果中包括对所述远端服务节点的资源请求或者对所述远端服务节点的资源请求中的第一信息，第一信息用于标识对不同的远端服务节点的资源请求。

[0269] 可选的，所述解密密钥为所述控制设备与所述远端服务节点之间的共享密钥。

[0270] 其中，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

[0271] 其中，所述共享密钥与其他远端服务节点对应的共享密钥不同。

[0272] 可选的，所述解密密钥为第一公钥。

[0273] 可选的，所述第一校验数据中还包括所述远端服务节点的资源请求的标识，所述资源请求的标识用于判断资源请求是否为重放消息。

[0274] 可选的，所述远端服务节点的资源请求的标识为序列号或者时间戳。

[0275] 图13为本申请实施例十一提供的另一种远端服务节点的结构示意图，如图13所示，该远端服务节点200在图12所示设备的基础上，还包括：

[0276] 生成模块213，用于生成资源响应消息，所述资源响应消息中包括所述远端服务节点的资源响应对应的第二校验数据；

[0277] 发送模块214，用于向所述资源集合设备发送所述资源响应消息。

[0278] 可选的，所述第二校验数据由所述远端服务节点采用加密密钥对所述远端服务节点的资源响应加密得到。

[0279] 可选的，所述加密密钥为所述远端服务节点与所述控制设备之间的共享密钥。

[0280] 其的，所述共享密钥为所述控制设备与多个所述远端服务节点共用的密钥。

[0281] 或者，所述共享密钥与其他远端服务节点对应的共享密钥不同。

[0282] 可选的，所述加密密钥为第二私钥。

[0283] 可选的，所述加密密钥为第二私钥和第一公钥，所述第二私钥用于对所述远端服务节点的资源响应进行加密得到第一加密数据，所述第一公钥用于对所述远端服务节点的资源响应和所述第一加密数据进行加密得到所述第二校验数据。

[0284] 可选的所述第二校验数据中还包括所述远端服务节点的资源响应的标识，所述远端服务节点的资源响应的标识用于判断资源响应是否为重放消息。

[0285] 可选的所述远端服务节点的资源请求的标识为序列号或者时间戳。

[0286] 上述任一实现方式提供的远端服务节点，用于执行前述任一方法实施例中远端服

务节点执行的技术方案，其实现原理和技术效果类似，在此不再赘述。

[0287] 图14为本申请实施例十二提供的又一种控制设备的结构示意图，如图14所示，该控制设备400包括：

[0288] 处理器411、存储器412、与资源集合设备进行通信的接口413；

[0289] 所述存储器412存储计算机执行指令；

[0290] 所述处理器411执行所述存储器存储的计算机执行指令，使得所述处理器411执行前述任一方法实施例中控制设备执行的技术方案。

[0291] 图14为控制设备的一种简单设计，本申请实施例不限制控制设备中处理器和存储器的个数，图14仅以个数为1作为示例说明。

[0292] 图15为本申请实施例十三提供的又一种远端服务节点的结构示意图，如图15所示，该远端服务节点500包括：

[0293] 处理器511、存储器512、与资源集合设备进行通信的接口513；

[0294] 所述存储器512存储计算机执行指令；

[0295] 所述处理器511执行所述存储器512存储的计算机执行指令，使得所述处理器511执行前述任一方法实施例中远端服务节点执行的技术方案。

[0296] 图15为远端服务节点的一种简单设计，本申请实施例不限制远端服务节点中处理器和存储器的个数，图15仅以个数为1作为示例说明。

[0297] 在上述图14所示的控制设备或图15所述的远端服务节点的一种具体实现中，存储器、处理器以及接口之间可以通过总线连接，可选的，存储器可以集成在处理器内部。

[0298] 本申请实施例还提供一种计算机可读存储介质所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现前述任一方法实施例中控制设备执行的技术方案。

[0299] 本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现前述任一方法实施例中远端服务节点执行的技术方案。

[0300] 本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当所述计算机执行指令被处理器执行时用于实现前述任一方法实施例中资源集合设备执行的技术方案。

[0301] 本申请实施例还提供一种程序，当该程序被处理器执行时，用于执行前述任一方法实施例中控制设备执行的技术方案。

[0302] 本申请实施例还提供一种程序，当该程序被处理器执行时，用于执行前述任一方法实施例中远端服务节点执行的技术方案。

[0303] 本申请实施例还提供一种程序，当该程序被处理器执行时，用于执行前述任一方法实施例中资源集合设备执行的技术方案。

[0304] 可选地，上述处理器可以为芯片。

[0305] 本申请实施例还提供一种计算机程序产品，包括程序指令，程序指令用于实现前述任一方法实施例中控制设备执行的技术方案。

[0306] 本申请实施例还提供一种计算机程序产品，包括程序指令，程序指令用于实现前述任一方法实施例中远端服务节点执行的技术方案。

[0307] 本申请实施例还提供一种计算机程序产品，包括程序指令，程序指令用于实现前述任一方法实施例中资源集合设备执行的技术方案。

[0308] 本申请实施例还提供一种芯片，包括：处理模块与通信接口，该处理模块能执行前述任一方法实施例中控制设备执行的技术方案。

[0309] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行前述任一方法实施例中控制设备执行的技术方案。

[0310] 本申请实施例还提供一种芯片，包括：处理模块与通信接口，该处理模块能执行前述任一方法实施例中远端服务节点执行的技术方案。

[0311] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行前述任一方法实施例中远端服务节点执行的技术方案。

[0312] 本申请实施例还提供一种芯片，包括：处理模块与通信接口，该处理模块能执行前述任一方法实施例中资源集合设备执行的技术方案。

[0313] 进一步地，该芯片还包括存储模块(如，存储器)，存储模块用于存储指令，处理模块用于执行存储模块存储的指令，并且对存储模块中存储的指令的执行使得处理模块执行前述任一方法实施例中资源集合设备执行的技术方案。

[0314] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述模块的划分，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，例如多个模块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，模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0315] 在上述终端设备和网络设备的具体实现中，应理解，处理器可以是中央处理单元(英文：Central Processing Unit，简称：CPU)，还可以是其他通用处理器、数字信号处理器(英文：Digital Signal Processor，简称：DSP)、专用集成电路(英文：Application Specific Integrated Circuit，简称：ASIC)等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0316] 实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一可读取存储器中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储器(存储介质)包括：只读存储器(英文：read-only memory，简称：ROM)、RAM、快闪存储器、硬盘、固态硬盘、磁带(英文：magnetic tape)、软盘(英文：floppy disk)、光盘(英文：optical disc)及其任意组合。

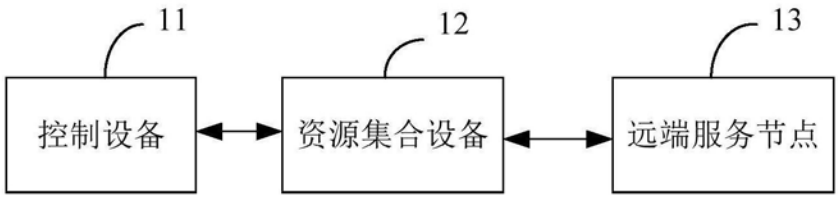
11
12
13
控制设备
资源集合设备
远端服务节点

图1

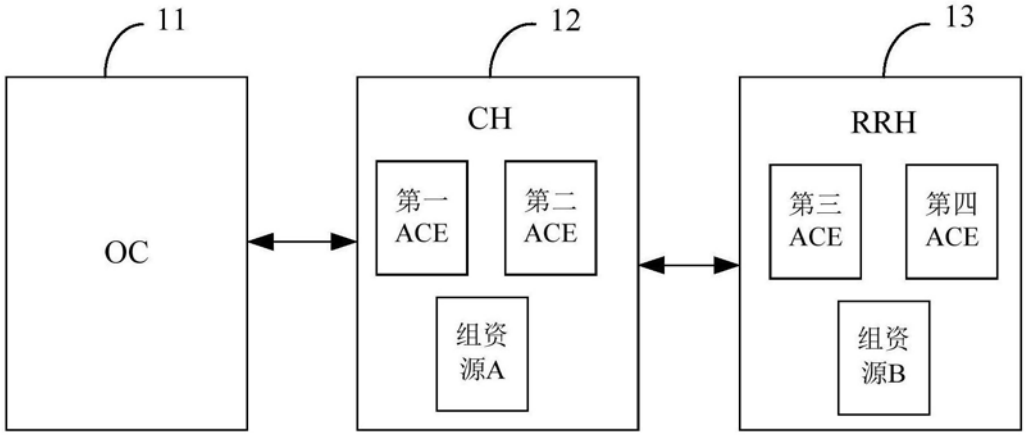
11
12
13
OC
CH
第一 ACE
第二 ACE
组资源A
RRH
第三 ACE
第四 ACE
组资源B

图2


生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据
S101
向资源集合设备发送资源集合请求消息
S102

图3

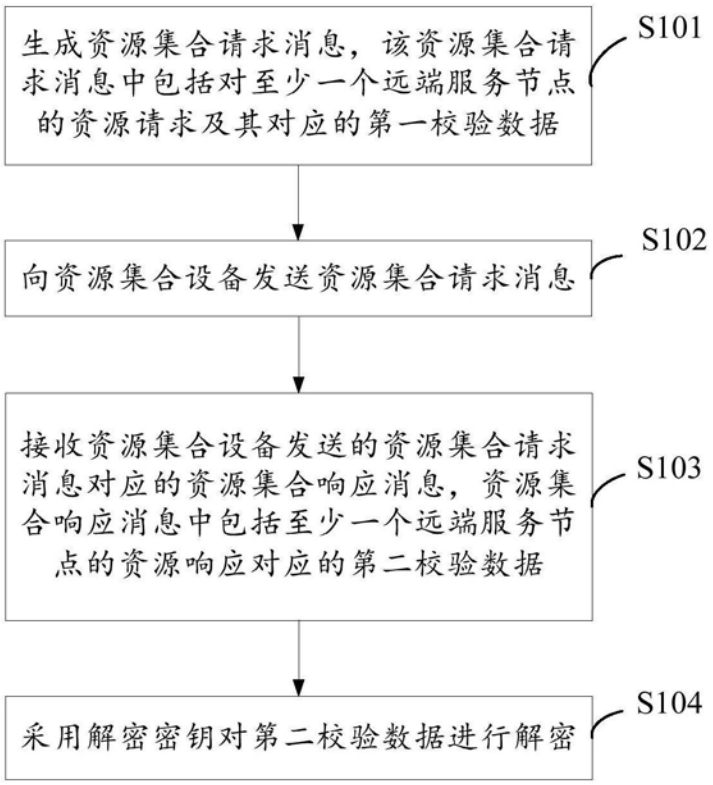
生成资源集合请求消息，该资源集合请求消息中包括对至少一个远端服务节点的资源请求及其对应的第一校验数据
S101
向资源集合设备发送资源集合请求消息
S102
接收资源集合设备发送的资源集合请求消息对应的资源集合响应消息，资源集合响应消息中包括至少一个远端服务节点的资源响应对应的第二校验数据
S103
采用解密密钥对第二校验数据进行解密
S104

图4

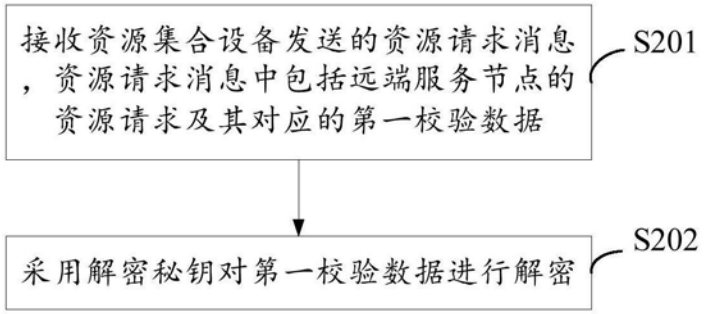
接收资源集合设备发送的资源请求消息，资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据
S201
采用解密秘钥对第一校验数据进行解密
S202

图5

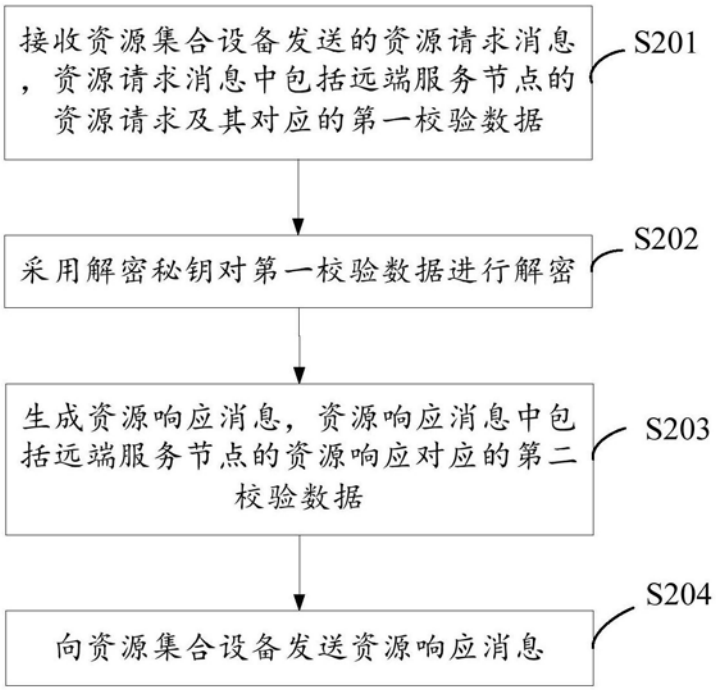
接收资源集合设备发送的资源请求消息，资源请求消息中包括远端服务节点的资源请求及其对应的第一校验数据
S201
采用解密秘钥对第一校验数据进行解密
S202
生成资源响应消息，资源响应消息中包括远端服务节点的资源响应对应的第二校验数据
S203
向资源集合设备发送资源响应消息
S204

图6

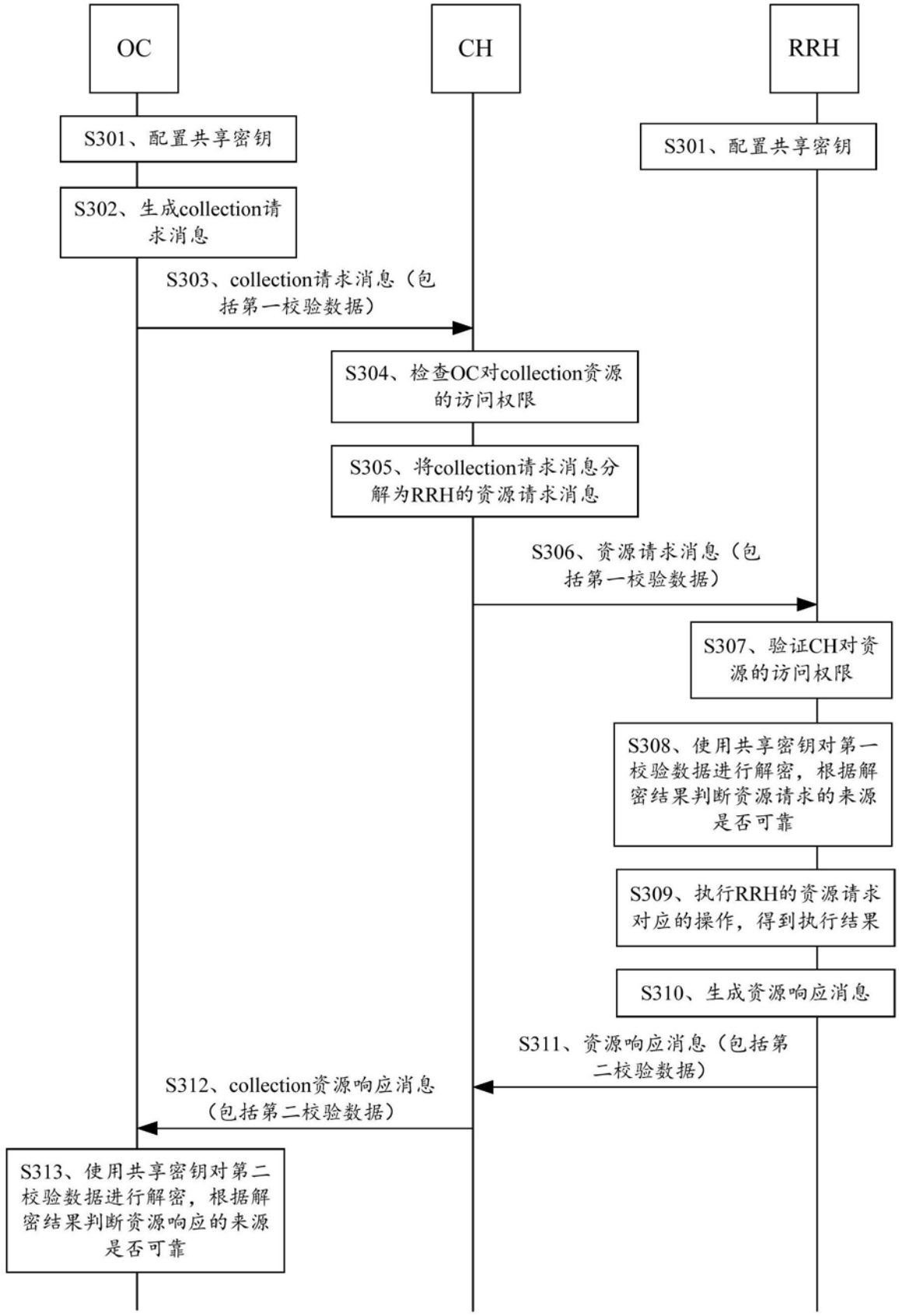
OC
CH
RRH
S301、配置共享密钥
S301、配置共享密钥
S302、生成collection请求消息
S303、collection请求消息（包括第一校验数据）
S304、检查OC对collection资源的访问权限
S305、将collection请求消息分解为RRH的资源请求消息
S306、资源请求消息（包括第一校验数据）
S307、验证CH对资源的访问权限
S308、使用共享密钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠
S309、执行RRH的资源请求对应的操作，得到执行结果
S310、生成资源响应消息
S311、资源响应消息（包括第二校验数据）
S312、collection资源响应消息（包括第二校验数据）
S313、使用共享密钥对第二校验数据进行解密，根据解密结果判断资源响应的来源是否可靠

图7

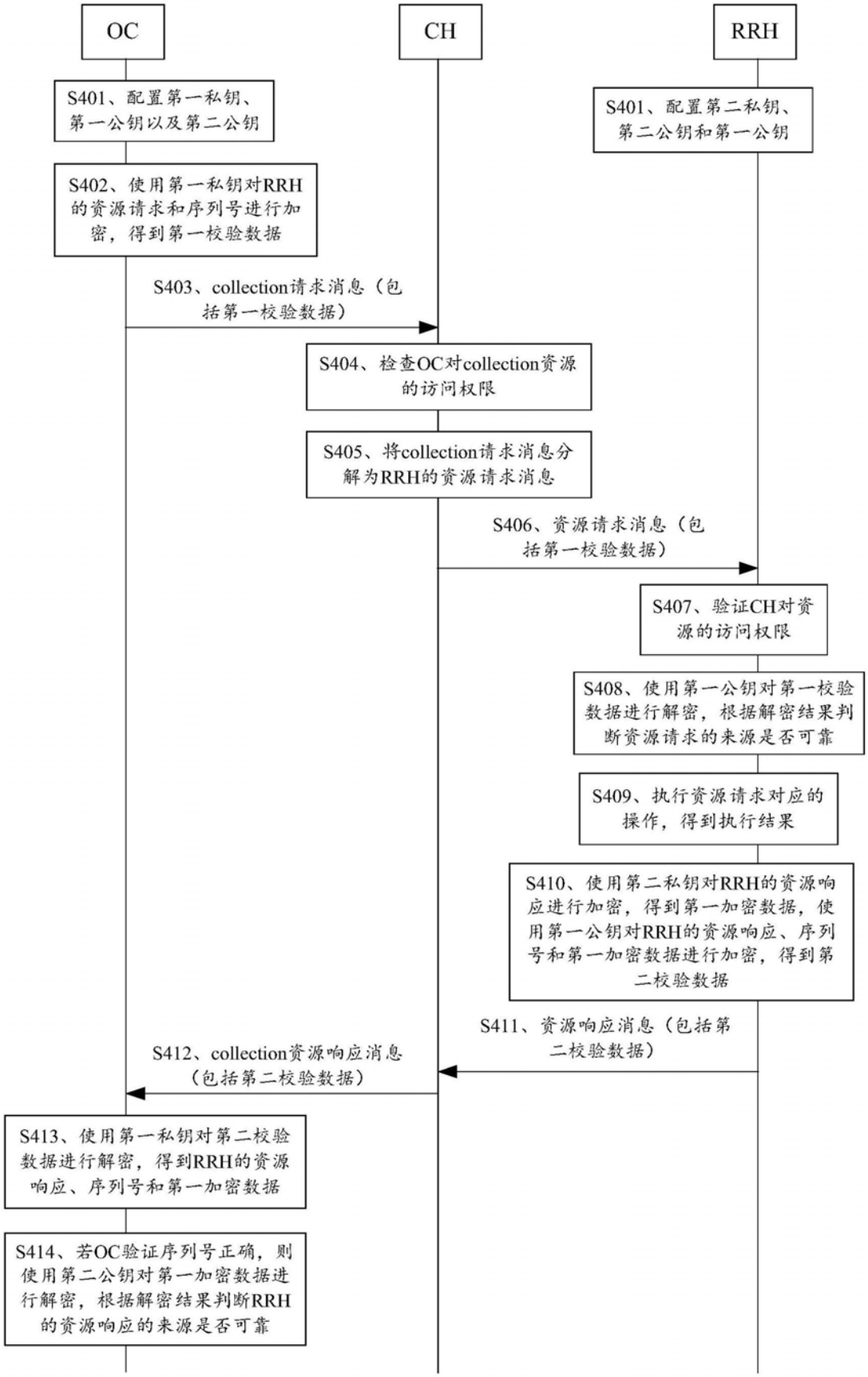
OC
CH
RRH
S401、配置第一私钥、第一公钥以及第二公钥
S401、配置第二私钥、第二公钥和第一公钥
S402、使用第一私钥对RRH的资源请求和序列号进行加密，得到第一校验数据
S403、collection请求消息（包括第一校验数据）
S404、检查OC对collection资源的访问权限
S405、将collection请求消息分解为RRH的资源请求消息
S406、资源请求消息（包括第一校验数据）
S407、验证CH对资源的访问权限
S408、使用第一公钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠
S409、执行资源请求对应的操作，得到执行结果
S410、使用第二私钥对RRH的资源响应进行加密，得到第一加密数据，使用第一公钥对RRH的资源响应、序列号和第一加密数据进行加密，得到第二校验数据
S411、资源响应消息（包括第二校验数据）
S412、collection资源响应消息（包括第二校验数据）
S413、使用第一私钥对第二校验数据进行解密，得到RRH的资源响应、序列号和第一加密数据
S414、若OC验证序列号正确，则使用第二公钥对第一加密数据进行解密，根据解密结果判断RRH的资源响应的来源是否可靠

图8

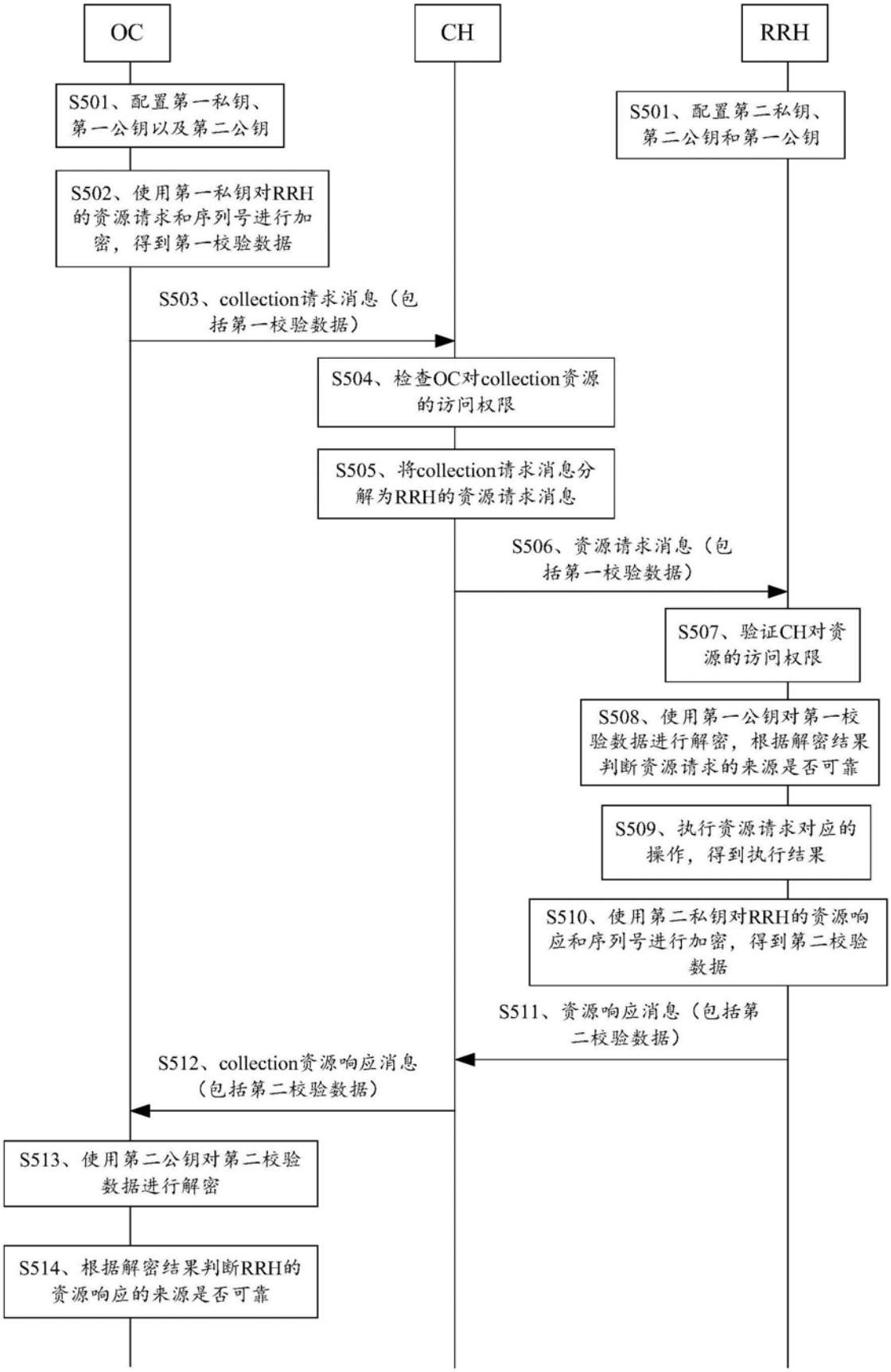
OC
CH
RRH
S501、配置第一私钥、第一公钥以及第二公钥
S501、配置第二私钥、第二公钥和第一公钥
S502、使用第一私钥对RRH的资源请求和序列号进行加密，得到第一校验数据
S503、collection请求消息（包括第一校验数据）
S504、检查OC对collection资源的访问权限
S505、将collection请求消息分解为RRH的资源请求消息
S506、资源请求消息（包括第一校验数据）
S507、验证CH对资源的访问权限
S508、使用第一公钥对第一校验数据进行解密，根据解密结果判断资源请求的来源是否可靠
S509、执行资源请求对应的操作，得到执行结果
S510、使用第二私钥对RRH的资源响应和序列号进行加密，得到第二校验数据
S511、资源响应消息（包括第二校验数据）
S512、collection资源响应消息（包括第二校验数据）
S513、使用第二公钥对第二校验数据进行解密
S514、根据解密结果判断RRH的资源响应的来源是否可靠

图9

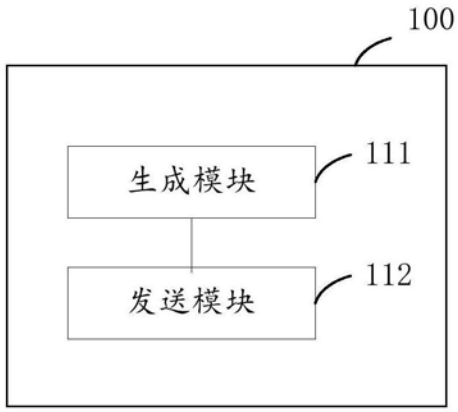

图10

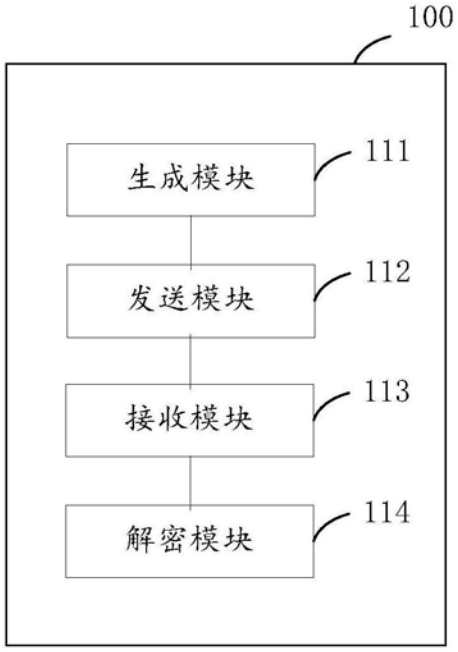

图11

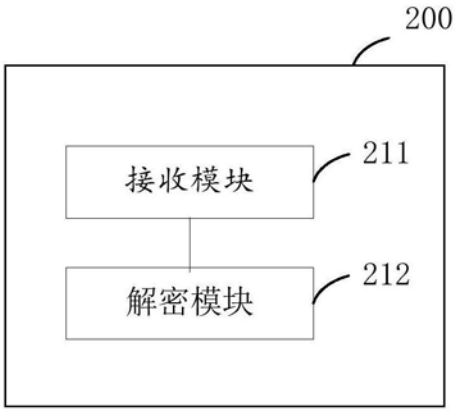

图12

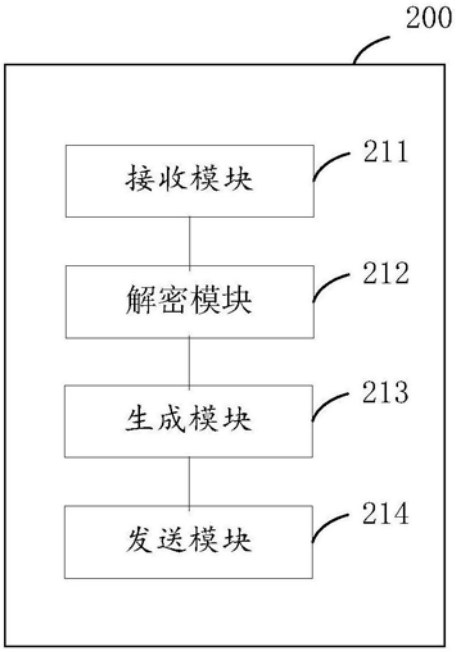

图13

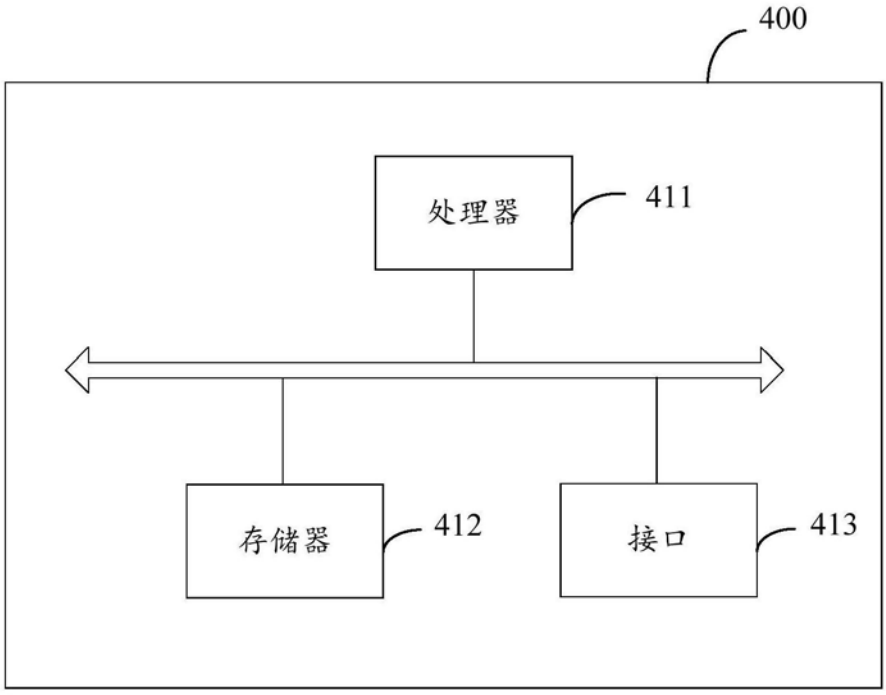

图14

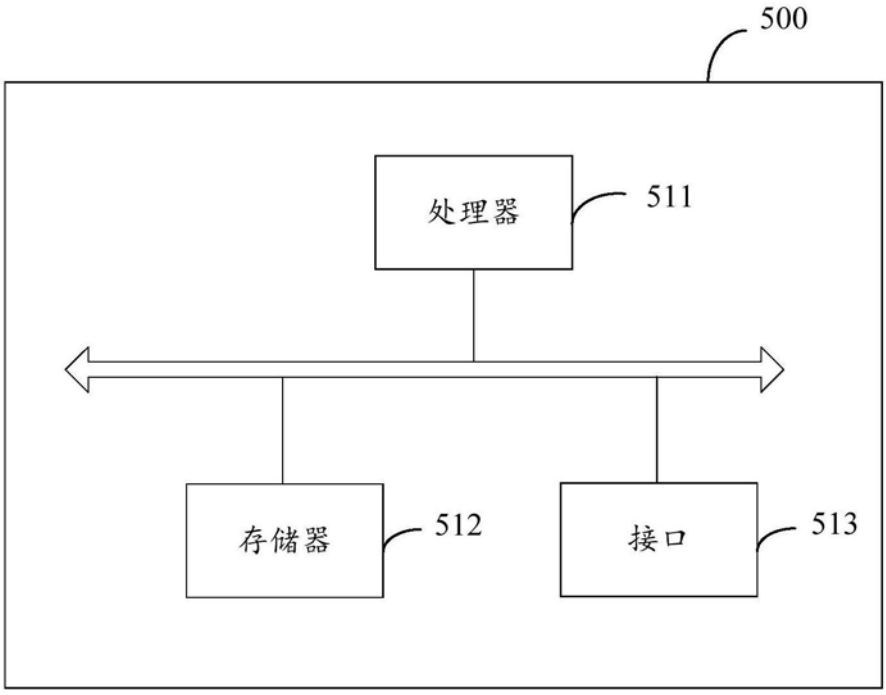

图15