



# (12)发明专利申请

(10)申请公布号 CN 108462681 A

(43)申请公布日 2018.08.28

(21)申请号 201710097425.2

(22)申请日 2017.02.22

(71)申请人 中国移动通信集团公司  
地址 100032 北京市西城区金融大街29号  
申请人 中移物联网有限公司

(72)发明人 刘愿 何渝君 龚国成 雷希  
吴松伟 吴露露 雷洪

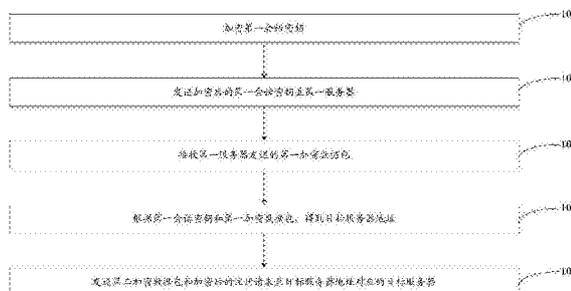
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270  
代理人 张颖玲 王花丽

(51)Int.Cl.  
H04L 29/06(2006.01)  
H04L 29/08(2006.01)

权利要求书3页 说明书14页 附图9页

(54)发明名称  
一种异构网络的通信方法、设备及系统

(57)摘要  
本发明实施例提供一种异构网络的通信方法,包括:加密用于第一服务器生成第一加密数据包的第一会话密钥,并将加密后的第一会话密钥发送至第一服务器;接收第一服务器发送的用于确定第二服务器中目标服务器的第一加密数据包;根据第一会话密钥和第一加密数据包,得到目标服务器地址;发送用于注册的第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器。本发明实施例同时还提供一种异构网络的通信设备及系统。



1. 一种异构网络的通信方法,其特征在于,所述方法包括:  
加密第一会话密钥;其中,所述第一会话密钥用于第一服务器生成第一加密数据包;  
发送加密后的第一会话密钥至所述第一服务器;  
接收所述第一服务器发送的第一加密数据包;其中,所述第一加密数据包用于确定目标服务器,所述目标服务器为第二服务器中的服务器;  
根据所述第一会话密钥和所述第一加密数据包,得到目标服务器地址;  
发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器;  
其中,所述第二加密数据包和所述加密后的注册请求用于所述目标服务器完成物联网设备的注册。

2. 根据权利要求1所述的方法,其特征在于,所述第一加密数据包中包括采用所述第一会话密钥加密的第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址;  
所述第二加密数据包中包括采用预设算法加密的访问令牌和第二会话密钥;  
所述加密后的注册请求为采用第二会话密钥加密的注册请求。

3. 根据权利要求2所述的方法,其特征在于,所述根据所述第一会话密钥和所述第一加密数据包,得到目标服务器地址,包括:

采用所述第一会话密钥解密所述第一加密数据包,得到所述第二加密数据包、所述第二会话密钥和所述通过预设方式处理的目标服务器地址;

根据所述通过预设方式处理的目标服务器地址得到所述目标服务器地址;

所述发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器,包括:

采用所述第二会话密钥加密注册请求;

发送所述第二加密数据包和加密后的注册请求至所述目标服务器地址对应的所述目标服务器。

4. 根据权利要求3所述的方法,其特征在于,所述方法还包括:

接收所述目标服务器发送的加密后的鉴权码;其中,所述加密后的鉴权码为采用第二会话密钥加密的鉴权码;

采用所述第二会话密钥解密所述加密后的鉴权码,得到所述鉴权码;

通过预设方式处理待传输数据,并采用所述第二会话密钥加密处理后的所述待传输数据,生成第三加密数据包;

发送所述第三加密数据包和所述鉴权码至所述目标服务器。

5. 根据权利要求2-4任一所述的方法,其特征在于,所述预设方式为数据序列化系统AVRO方式。

6. 一种异构网络的通信方法,其特征在于,所述方法包括:

接收物联网设备发送的加密后的第一会话密钥;

对所述加密后的第一会话密钥进行解密得到第一会话密钥;

采用所述第一会话密钥加密生成第一加密数据包;其中,所述第一加密数据包用于所述物联网设备确定目标服务器,所述目标服务器为第二服务器中的服务器;

发送所述第一加密数据包至所述物联网设备。

7. 根据权利要求6所述的方法,其特征在于,所述采用所述第一会话密钥加密生成第一

加密数据包,包括:

生成第二会话密钥和访问令牌;

采用预设算法加密所述访问令牌和所述第二会话密钥,生成第二加密数据包;

获取目标服务器地址;

通过预设方式处理所述目标服务器地址;

采用所述第一会话密钥加密所述第二加密数据包、所述第二会话密钥和处理后的所述目标服务器地址,生成所述第一加密数据包。

8. 根据权利要求7所述的方法,其特征在于,所述获取目标服务器地址,包括:

通过第三服务器获取第二服务器的负载;

将所述第二服务器的负载小于预设阈值的第二服务器的地址,作为所述目标服务器地址。

9. 一种异构网络的通信方法,其特征在于,所述方法包括:

接收物联网设备发送的第二加密数据包和加密后的注册请求;

解密所述第二加密数据包;

根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功。

10. 根据权利要求9所述的方法,其特征在于,所述根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功,包括:

若能够成功解密所述第二加密数据包且得到访问令牌和第二会话密钥;采用所述第二会话密钥解密所述加密后的注册请求得到注册请求;

获取所述注册请求中的注册码;

判断所述注册码是否合法;

若所述注册码合法,确定物联网设备注册成功。

11. 根据权利要求10所述的方法,其特征在于,所述方法还包括:

为所述物联网设备分配鉴权码;

采用所述第二会话密钥加密所述鉴权码;

发送加密后的所述鉴权码至所述物联网设备。

12. 根据权利要求11所述的方法,其特征在于,所述方法还包括:

接收所述物联网设备发送的第三加密数据包和鉴权码;

判断所述鉴权码是否正确;

若所述鉴权码正确,采用所述第二会话密钥解密所述第三加密数据包,得到所述待传输数据。

13. 一种物联网设备,其特征在于,所述物理网设备包括:

第一加密模块,用于加密第一会话密钥;其中,所述第一会话密钥用于第一服务器生成第一加密数据包;

第一发送模块,用于发送加密后的第一会话密钥至第一服务器;

第一接收模块,用于接收所述第一服务器发送的第一加密数据包;其中,所述第一加密数据包用于确定目标服务器,所述目标服务器为第二服务器中的服务器;

第一解密模块,用于根据所述第一会话密钥和所述第一加密数据包,得到目标服务器

地址；

所述第一发送模块，还用于发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器；其中，所述第二加密数据包和所述加密后的注册请求用于所述目标服务器完成物联网设备的注册。

14. 根据权利要求13所述的物联网设备，其特征在于，

所述第一接收模块，还用于接收所述目标服务器发送的加密后的鉴权码；其中，所述加密后的鉴权码为采用第二会话密钥加密的鉴权码；

所述第一解密模块，还用于采用所述第二会话密钥解密所述加密后的鉴权码，得到所述鉴权码；

所述第一加密模块，还用于通过预设方式处理待传输数据，并采用所述第二会话密钥加密处理后的所述待传输数据，生成第三加密数据包；

所述第一发送模块，还用于发送所述第三加密数据包和所述鉴权码至所述目标服务器。

15. 一种第一服务器，其特征在于，所述第一服务器包括：

第二接收模块，用于接收物联网设备发送的加密后的第一会话密钥；

第二解密模块，用于对所述加密后的第一会话密钥进行解密得到第一会话密钥；

第二加密模块，用于采用所述第一会话密钥加密生成第一加密数据包；其中，所述第一加密数据包用于所述物联网设备确定目标服务器，所述目标服务器为第二服务器中的服务器；

第二发送模块，用于发送所述第一加密数据包至所述物联网设备。

16. 一种目标服务器，其特征在于，所述目标服务器包括：

第三接收模块，用于接收物联网设备发送的第二加密数据包和加密后的注册请求；

第三解密模块，用于解密所述第二加密数据包；

处理模块，用于根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功。

17. 根据权利要求16所述的目标服务器，其特征在于，

所述第三接收模块，还用于接收所述物联网设备发送的第三加密数据包和鉴权码；

所述处理模块，还用于判断所述鉴权码是否正确；若所述鉴权码正确，采用所述第二会话密钥解密所述第三加密数据包，得到所述待传输数据。

18. 一种异构网络的通信系统，其特征在于，所述系统包括如权利要求13或14所述的物联网设备、如权利要求15所述的第一服务器、如权利要求16或17所述的目标服务器，以及第三服务器；

其中，所述第三服务器，用于获取第二服务器的负载，所述第二服务器的负载用于所述物联网设备确定所述目标服务器。

## 一种异构网络的通信方法、设备及系统

### 技术领域

[0001] 本发明涉及物联网技术领域,尤其涉及一种异构网络的通信方法、设备及系统。

### 背景技术

[0002] 异构网络是一种特殊类型的网络,其是由不同制造商生产的服务器和物联网设备组成的,运行在不同的协议上支持不同的功能或应用。在现有的异构网络中,物联网设备首先运行某服务,然后通过该服务获取设备ID并动态获得服务器域名和端口号以与服务器建立通信连接,或者首先预设身份标识和服务器地址,然后向目标服务器地址发送身份标识,待验证通过后与服务器建立通信连接。

[0003] 然而,随着物联网产业的快速发展,物联网设备的数量激增,现有的异构网络的通信方法,服务器一方面需要对物联网设备的高并发注册请求进行处理(即完成建立通信连接的过程),另一方面又要在注册成功后接收并处理物联网设备上传的数据,会加大负载,从而造成注册请求的处理时间延长,影响物联网设备的注册。

### 发明内容

[0004] 有鉴于此,本发明实施例期望提供一种异构网络的通信方法、设备及系统,能够有效平衡服务器负载,保证物联网设备的注册请求能够及时地得到处理。

[0005] 本发明实施例的技术方案是这样实现的:

[0006] 一种异构网络的通信方法,包括:

[0007] 加密第一会话密钥;其中,所述第一会话密钥用于第一服务器生成第一加密数据包;

[0008] 发送加密后的第一会话密钥至所述第一服务器;

[0009] 接收所述第一服务器发送的第一加密数据包;其中,所述第一加密数据包用于确定目标服务器,所述目标服务器为第二服务器中的服务器;

[0010] 根据所述第一会话密钥和所述第一加密数据包,得到目标服务器地址;

[0011] 发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器;其中,所述第二加密数据包和所述加密后的注册请求用于所述目标服务器完成物联网设备的注册。

[0012] 如上所述的方法,所述第一加密数据包中包括采用所述第一会话密钥加密的第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址;

[0013] 所述第二加密数据包中包括采用预设算法加密的访问令牌和第二会话密钥;

[0014] 所述加密后的注册请求为采用第二会话密钥加密的注册请求。

[0015] 如上所述的方法,所述根据所述第一会话密钥和所述第一加密数据包,得到目标服务器地址,包括:

[0016] 采用所述第一会话密钥解密所述第一加密数据包,得到所述第二加密数据包、所述第二会话密钥和所述通过预设方式处理的目标服务器地址;

- [0017] 根据所述通过预设方式处理的目标服务器地址得到所述目标服务器地址；
- [0018] 所述发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器,包括:
- [0019] 采用所述第二会话密钥加密注册请求;
- [0020] 发送所述第二加密数据包和加密后的注册请求至所述目标服务器地址对应的所述目标服务器。
- [0021] 如上所述的方法,还包括:
- [0022] 接收所述目标服务器发送的加密后的鉴权码;其中,所述加密后的鉴权码为采用第二会话密钥加密的鉴权码;
- [0023] 采用所述第二会话密钥解密所述加密后的鉴权码,得到所述鉴权码;
- [0024] 通过预设方式处理待传输数据,并采用所述第二会话密钥加密处理后的所述待传输数据,生成第三加密数据包;
- [0025] 发送所述第三加密数据包和所述鉴权码至所述目标服务器。
- [0026] 如上所述的方法,所述预设方式为数据序列化系统AVRO方式。
- [0027] 一种异构网络的通信方法,包括:
- [0028] 接收物联网设备发送的加密后的第一会话密钥;
- [0029] 对所述加密后的第一会话密钥进行解密得到第一会话密钥;
- [0030] 采用所述第一会话密钥加密生成第一加密数据包;其中,所述第一加密数据包用于所述物联网设备确定目标服务器,所述目标服务器为第二服务器中的服务器;
- [0031] 发送所述第一加密数据包至所述物联网设备。
- [0032] 如上所述的方法,所述采用所述第一会话密钥加密生成第一加密数据包,包括:
- [0033] 生成第二会话密钥和访问令牌;
- [0034] 采用预设算法加密所述访问令牌和所述第二会话密钥,生成第二加密数据包;
- [0035] 获取目标服务器地址;
- [0036] 通过预设方式处理所述目标服务器地址;
- [0037] 采用所述第一会话密钥加密所述第二加密数据包、所述第二会话密钥和处理后的所述目标服务器地址,生成所述第一加密数据包。
- [0038] 如上所述的方法,所述获取目标服务器地址,包括:
- [0039] 通过第三服务器获取第二服务器的负载;
- [0040] 将所述第二服务器的负载小于预设阈值的第二服务器的地址,作为所述目标服务器地址。
- [0041] 一种异构网络的通信方法,包括:
- [0042] 接收物联网设备发送的第二加密数据包和加密后的注册请求;
- [0043] 解密所述第二加密数据包;
- [0044] 根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功。
- [0045] 如上所述的方法,所述根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功,包括:
- [0046] 若能够成功解密所述第二加密数据包且得到访问令牌和第二会话密钥;采用所述

第二会话密钥解密所述加密后的注册请求得到注册请求；

[0047] 获取所述注册请求中的注册码；

[0048] 判断所述注册码是否合法；

[0049] 若所述注册码合法,确定物联网设备注册成功。

[0050] 如上所述的方法,还包括:

[0051] 为所述物联网设备分配鉴权码;

[0052] 采用所述第二会话密钥加密所述鉴权码;

[0053] 发送加密后的所述鉴权码至所述物联网设备。

[0054] 如上所述的方法,还包括:

[0055] 接收所述物联网设备发送的第三加密数据包和鉴权码;

[0056] 判断所述鉴权码是否正确;

[0057] 若所述鉴权码正确,采用所述第二会话密钥解密所述第三加密数据包,得到所述待传输数据。

[0058] 一种物联网设备,包括:

[0059] 第一加密模块,用于加密第一会话密钥;其中,所述第一会话密钥用于第一服务器生成第一加密数据包;

[0060] 第一发送模块,用于发送加密后的第一会话密钥至第一服务器;

[0061] 第一接收模块,用于接收所述第一服务器发送的第一加密数据包;其中,所述第一加密数据包用于确定目标服务器,所述目标服务器为第二服务器中的服务器;

[0062] 第一解密模块,用于根据所述第一会话密钥和所述第一加密数据包,得到目标服务器地址;

[0063] 所述第一发送模块,还用于发送第二加密数据包和加密后的注册请求至所述目标服务器地址对应的目标服务器;其中,所述第二加密数据包和所述加密后的注册请求用于所述目标服务器完成物联网设备的注册。

[0064] 如上所述的物联网设备,所述第一接收模块,还用于接收所述目标服务器发送的加密后的鉴权码;其中,所述加密后的鉴权码为采用第二会话密钥加密的鉴权码;

[0065] 所述第一解密模块,还用于采用所述第二会话密钥解密所述加密后的鉴权码,得到所述鉴权码;

[0066] 所述第一加密模块,还用于通过预设方式处理待传输数据,并采用所述第二会话密钥加密处理后的所述待传输数据,生成第三加密数据包;

[0067] 所述第一发送模块,还用于发送所述第三加密数据包和所述鉴权码至所述目标服务器。

[0068] 一种第一服务器,包括:

[0069] 第二接收模块,用于接收物联网设备发送的加密后的第一会话密钥;

[0070] 第二解密模块,用于对所述加密后的第一会话密钥进行解密得到第一会话密钥;

[0071] 第二加密模块,用于采用所述第一会话密钥加密生成第一加密数据包;其中,所述第一加密数据包用于所述物联网设备确定目标服务器,所述目标服务器为第二服务器中的服务器;

[0072] 第二发送模块,用于发送所述第一加密数据包至所述物联网设备。

- [0073] 一种目标服务器,包括:
- [0074] 第三接收模块,用于接收物联网设备发送的第二加密数据包和加密后的注册请求;
- [0075] 第三解密模块,用于解密所述第二加密数据包;
- [0076] 处理模块,用于根据解密所述第二加密数据包得到的结果和所述加密后的注册请求确定所述物联网设备是否注册成功。
- [0077] 如上所述的目标服务器,所述第三接收模块,还用于接收所述物联网设备发送的第三加密数据包和鉴权码;
- [0078] 所述处理模块,还用于判断所述鉴权码是否正确;若所述鉴权码正确,采用所述第二会话密钥解密所述第三加密数据包,得到所述待传输数据。
- [0079] 一种异构网络的通信系统,包括如上所述的任一种物联网设备、如上所述的任一种第一服务器、如上所述的任一种目标服务器,以及第三服务器;
- [0080] 其中,所述第三服务器,用于获取第二服务器的负载,所述第二服务器的负载用于所述物联网设备确定所述目标服务器。
- [0081] 本发明实施例所提供的异构网络的通信方法、设备及系统,物联网设备加密第一会话密钥,并将加密后的第一会话密钥发送至第一服务器;其中,第一会话密钥用于第一服务器生成第一加密数据包;接收第一服务器发送的第一加密数据包;其中,第一加密数据包用于确定目标服务器,目标服务器为第二服务器中的服务器;根据第一会话密钥和第一加密数据包,得到目标服务器地址;发送第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器;其中,第二加密数据包和加密后的注册请求用于目标服务器完成物联网设备的注册;这样物联网设备给第一服务器确定的负载较小的目标服务器发送注册请求,能够有效平衡服务器负载,并保证物联网设备的注册请求能够及时地得到处理;同时,通过加密解密的方式完成交互过程有效地防止了恶意设备的接入。

## 附图说明

- [0082] 图1为本发明实施例提供的一种异构网络的通信方法的流程示意图;
- [0083] 图2为本发明实施例提供了物联网设备与第一服务器的通信示意图;
- [0084] 图3为本发明实施例提供的另一种异构网络的通信方法的流程示意图;
- [0085] 图4为本发明实施例提供的又一种异构网络的通信方法的流程示意图;
- [0086] 图5为本发明实施例提供的又一种异构网络的通信方法的流程示意图;
- [0087] 图6为本发明实施例提供的又一种异构网络的通信方法的流程示意图;
- [0088] 图7为本发明实施例提供的一种物联网设备的结构示意图;
- [0089] 图8为本发明实施例提供的另一种物联网设备的结构示意图;
- [0090] 图9为本发明实施例提供的一种第一服务器的结构示意图;
- [0091] 图10为本发明实施例提供的另一种第一服务器的结构示意图;
- [0092] 图11为本发明实施例提供的一种目标服务器的结构示意图;
- [0093] 图12为本发明实施例提供的另一种目标服务器的结构示意图;
- [0094] 图13为本发明实施例提供的又一种目标服务器的结构示意图;
- [0095] 图14为本发明实施例提供的一种异构网络的通信系统的结构示意图。

## 具体实施方式

[0096] 在对本发明实施例中的技术方案进行描述前,首先提供两篇专利以说明现有技术,其中,一篇是专利申请号为201310324359.X的《一种保障物联网数据传输安全的方法》,另一篇是专利申请号为201310655393.5的《身份认证方法及设备、服务器》。

[0097] 《一种保障物联网数据传输安全的方法》公开了一种保障物联网数据传输安全的方法,并具体包括以下的步骤:感知终端发送数据时,采用对称算法密钥对数据进行加密,生成加密数据;感知终端采用其对应的服务器的公钥将对称算法密钥进行非对称算法的加密,生成加密后的密钥;感知终端将加密数据和加密后的密钥同时发送给感知终端对应的服务器;服务器先采用其私钥将加密后的密钥进行解密,得到对称算法密钥,然后采用对称算法密钥对加密数据进行解密,得到数据。

[0098] 《身份认证方法及设备、服务器》公开了一种身份认证方法及设备、服务器,并具体包括以下的步骤:认证端利用私钥对获取的令牌进行加密,以获得签名;认证端向服务器发送令牌、签名和根据与私钥对应的公钥生成的第一身份标识;服务器根据令牌和签名,获得第二身份标识,根据第一身份标识和第二身份标识,进行身份认证。

[0099] 第一篇专利和第二篇专利公开的技术方案中均存在以下主要存在的问题:

[0100] 1、物联网设备上传数据过程中不进行加密传输,数据传输安全性差;

[0101] 2、服务器既要处理大批量物联网设备的连接请求,又要对成功接入的物联网设备上传的数据进行及时处理,因此,负载急剧增大,从而无法满足物联网设备的高并发注册请求。

[0102] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述。

[0103] 本发明实施例提供了一种异构网络的通信方法,如图1所示,该方法包括以下步骤:

[0104] 步骤101、加密第一会话密钥。

[0105] 需要说明的是,第一会话密钥用于第一服务器生成第一加密数据包。

[0106] 具体的,步骤101加密第一会话密钥可以是由物联网设备来实现的。第一会话密钥可以是物联网设备采用对称加密算法生成的,加密第一会话密钥所用的密钥可以是公私钥对中的公钥,其中,公私钥对由第一服务器采用非对称加密算法生成,第一服务器将公私钥对中的公钥公开,将公私钥对中的私钥保留。

[0107] 步骤102、发送加密后的第一会话密钥至第一服务器。

[0108] 具体的,步骤102发送加密后的第一会话密钥至第一服务器可以是由物联网设备来实现的。物联网设备中会预先配置一个或多个第一服务器地址。第一服务器地址与公钥具有对应关系,即用哪个第一服务器的公钥加密第一会话密钥,就要将加密后的第一会话密钥发送至该第一服务器。将加密后的第一会话密钥发送至第一服务器指的是根据预先配置的一个第一服务器的地址将加密后的第一会话密钥发送至第一服务器,若该第一服务器无法接收导致发送失败,物联网设备根据预先配置的另一个第一服务器的地址将加密后的第一会话密钥发送至第一服务器,只不过此时加密后的第一会话密钥指的是采用新选择的第一服务器地址对应的公钥进行加密的。若根据多个第一服务器地址都发送失败后,由用

户决定是否继续进行物联网设备的注册。

[0109] 具体的,物联网设备只能根据自身预先配置的第一服务器地址与相应的第一服务器通信。本发明实施例提供了物联网设备与第一服务器的通信示意图,假设物联网设备有两个,一个是物联网设备1,一个是物联网设备2,第一服务器有三个,分别是第一服务器1、第一服务器2和第一服务器3,假设物联网设备1上预先配置了第一服务器1、第一服务器2和第一服务器3的地址,物联网设备2上预先配置了第一服务器2和第一服务器3的地址,如图2所示,物联网设备2只能与第一服务器2和第一服务器3通信。

[0110] 具体的,若加密第一会话密钥所用的密钥是第一服务器生成的公私钥对中的公钥,那么第一服务器在接收到加密后的第一会话密钥后,就可以用自己生成的公私钥对中予以保留的私钥进行解密,从而得到第一会话密钥。

[0111] 步骤103、接收第一服务器发送的第一加密数据包。

[0112] 需要说明的是,第一加密数据包用于确定目标服务器,目标服务器为第二服务器中的服务器。

[0113] 具体的,步骤103接收第一服务器发送的第一加密数据包可以是由物联网设备来实现的。第一加密数据包中可以包括采用第一会话密钥加密的第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址;第二加密数据包中可以包括采用预设算法加密的访问令牌和第二会话密钥;加密后的注册请求为采用第二会话密钥加密的注册请求。

[0114] 步骤104、根据第一会话密钥和第一加密数据包,得到目标服务器地址。

[0115] 需要说明的是,第一加密数据包中的“第一”是为了标识用于目标服务器的加密数据包,以区别于其他用途的加密数据包;第二加密数据包中的“第二”是为了标识解密第一加密数据包所得到的加密数据包,以区别于所得到的其他加密数据包。

[0116] 步骤105、发送第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器。

[0117] 需要说明的是,第二加密数据包和加密后的注册请求用于目标服务器完成物联网设备的注册。

[0118] 本发明的实施例提供的异构网络的通信方法,物联网设备加密用于第一服务器生成第一加密数据包的第一会话密钥,并发送加密后的第一会话密钥至第一服务器;接收第一服务器发送的用于确定第二服务器中目标服务器的第一加密数据包;根据第一会话密钥和第一加密数据包,得到目标服务器地址;发送用于注册的第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器;这样物联网设备给第一服务器确定的负载较小的目标服务器发送注册请求,能够有效平衡服务器的负载,并保证了注册请求能够及时地得到处理;同时,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入。

[0119] 本发明实施例提供了另一种异构网络的通信方法,如图3所示,该方法包括以下步骤:

[0120] 步骤201、接收物联网设备发送的加密后的第一会话密钥。

[0121] 具体的,步骤201接收物联网设备发送的加密后的第一会话密钥可以是由第一服务器来实现的。

[0122] 需要说明的是,第一服务器中的“第一”是为了标识对物联网设备进行注册引导的服务器,以区别于第二服务器和第三服务器。第一服务器的数量可以是一个服务器,也可以

是多个服务器,本发明对此不作限制。

[0123] 步骤202、对加密后的第一会话密钥进行解密得到第一会话密钥。

[0124] 具体的,步骤202对加密后的第一会话密钥进行解密得到第一会话密钥可以是由第一服务器来实现的。若物联网设备在加密第一会话密钥时所用的密钥是第一服务器生成的公私钥对中的公钥,那么第一服务器在接收到加密后的第一会话密钥后,就可以用自己生成的公私钥对中予以保留的私钥进行解密,从而得到第一会话密钥。

[0125] 步骤203、采用第一会话密钥加密生成第一加密数据包。

[0126] 需要说明的是,第一加密数据包用于物联网设备确定目标服务器,目标服务器为第二服务器中的服务器。

[0127] 具体的,步骤203采用第一会话密钥加密生成第一加密数据包可以是由第一服务器来实现的。

[0128] 步骤204、发送第一加密数据包至物联网设备。

[0129] 具体的,步骤204发送第一加密数据包至物联网设备可以是由第一服务器来实现的。

[0130] 本发明的实施例提供的异构网络的通信方法,第一服务器接收物联网设备发送的加密后的第一会话密钥,并对加密后的第一会话密钥进行解密得到第一会话密钥;采用第一会话密钥生成用于物联网设备确定目标服务器的第一加密数据包并发送至物联网设备;这样物联网设备能够根据第一加密数据包获得第一服务器选择的负载较小的目标服务器,从而向这些目标服务器发送注册请求,因此避免了物联网设备向繁忙服务器发送注册请求造成繁忙服务器负载更大的问题,有效地平衡了服务器的负载,又保证了物联网设备的注册请求能够及时地得到处理;并且,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入。

[0131] 本发明实施例提供了又一种异构网络的通信方法,如图4所示,该方法包括以下步骤:

[0132] 步骤301、接收物联网设备发送的第二加密数据包和加密后的注册请求。

[0133] 具体的,步骤301接收物联网设备发送的第二加密数据包和加密后的注册请求可以是由目标服务器来实现的。

[0134] 步骤302、解密第二加密数据包。

[0135] 具体的,步骤302解密第二加密数据包可以是由目标服务器来实现的。由于第二加密数据包是由预设算法加密的,因此目标服务器利用预设算法解密第二加密数据包。

[0136] 步骤303、根据解密第二加密数据包得到的结果和加密后的注册请求确定物联网设备是否注册成功。

[0137] 具体的,步骤303根据解密第二加密数据包得到的结果和加密后的注册请求确定物联网设备是否注册成功可以是由目标服务器来实现的。

[0138] 本发明的实施例提供的异构网络的通信方法,目标服务器接收物联网设备发送的第二加密数据包和加密后的注册请求;解密第二加密数据包;根据解密第二加密数据包得到的结果和加密后的注册请求确定物联网设备是否注册成功;这样,由于目标服务器是第一服务器选择的负载较小的服务器,因此目标服务器在接收到物联网设备的注册请求后,可以及时地处理这些请求,从而有效地平衡了服务器的负载,保证了注册请求能够及时地

得到处理;同时,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入。

[0139] 下面提供一个完整的实施例说明本发明异构网络的通信方法,如图5所示,该方法包括:

[0140] 步骤401、物联网设备加密第一会话密钥。

[0141] 步骤402、物联网设备发送加密后的第一会话密钥至第一服务器。

[0142] 步骤403、第一服务器接收物联网设备发送的加密后的第一会话密钥。

[0143] 步骤404、第一服务器对加密后的第一会话密钥进行解密,得到第一会话密钥。

[0144] 步骤405、第一服务器生成第二会话密钥和访问令牌。

[0145] 具体的,第二会话密钥可以是第一服务器采用对称加密算法生成的。

[0146] 步骤406、第一服务器采用预设算法加密访问令牌和第二会话密钥,生成第二加密数据包。

[0147] 需要说明的是,预设算法是服务器之间的一种内部约定算法,采用该算法可以进行加密和解密。

[0148] 步骤407、第一服务器获取目标服务器地址。

[0149] 具体的,步骤407第一服务器获取目标服务器地址可以通过以下方式来实现:

[0150] 步骤407a、通过第三服务器获取第二服务器的负载。

[0151] 需要说明的是,第二服务器中的“第二”是标识对物联网设备进行注册以及后续接收物联网设备所上传数据的服务器,以区别与第一服务器和第三服务器;第三服务器中的“第三”是标识供第一服务器获取第二服务器负载的服务器,以区别于第一服务器和第二服务器。

[0152] 具体的,第一服务器通过第三服务器获取第二服务器的负载可以通过发送请求并接收回复的方式获取,即第一服务器向第三服务器发送获取第二服务器负载的请求,接收第三服务器发送的包含第二服务器负载情况的信息。由于第一服务器要通过第三服务器获取第二服务器的负载,那么第三服务器要首先获取到第二服务器的负载,第三服务器获取第二服务器的负载可以通过被动的方式获取,还可以通过主动的方式获取,其中,被动的方式是指第三服务器在接收到第一服务器发送的获取第二服务器负载的请求后,再向第二服务器发送负载情况的查询信息;主动的方式是指第三服务器每隔一定的时间就向第二服务器发送负载情况的查询信息,由第二服务器返回负载情况信息后进行存储。

[0153] 步骤407b、将第二服务器的负载小于预设阈值的第二服务器的地址,作为目标服务器地址。

[0154] 具体的,预设阈值可以是设定的负载率,假设为40%,那么第一服务器将负载率小于40%的第二服务器的地址,作为目标服务器地址。

[0155] 步骤408、第一服务器通过预设方式处理目标服务器地址。

[0156] 需要说明的是,由于获取的目标服务器地址可能会比较庞大,因此第一服务器需要通过预设方式进行预先处理,从而生成轻量化的数据包,再采用第一会话密钥加密第二加密数据包、第二会话密钥和处理后的目标服务器地址,生成第一加密数据包。

[0157] 具体的,预设方式是数据序列化系统AVRO方式。在本发明的各个实施例中,预设方式都是AVRO方式。采用JSON方式格式化数据后生成的数据包较大,从而耗费数据流量,而采用AVRO方式格式化数据后生成的数据包较小,从而降低数据流量消耗。

[0158] 步骤409、第一服务器采用第一会话密钥加密第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址,生成第一加密数据包。

[0159] 具体的,第一加密数据包中包括采用所述第一会话密钥加密的第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址;第二加密数据包中包括采用预设算法加密的访问令牌和第二会话密钥。

[0160] 步骤410、第一服务器发送第一加密数据包至物联网设备。

[0161] 步骤411、物联网设备接收第一服务器发送的第一加密数据包。

[0162] 步骤412、物联网设备采用第一会话密钥解密第一加密数据包,得到第二加密数据包、第二会话密钥和通过预设方式处理后的目标服务器地址。

[0163] 具体的,由于第一加密数据包是由第一服务器采用第一会话密钥加密第二加密数据包、第二会话密钥和通过预设方式处理后的目标服务器地址而生成的,因此,物联网设备采用第一会话密钥便可解密第二加密数据包。

[0164] 步骤413、物联网设备根据通过预设方式处理后的目标服务器地址得到目标服务器地址。

[0165] 步骤414、物联网设备采用第二会话密钥加密注册请求。

[0166] 步骤415、物联网设备发送第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器。

[0167] 需要说明的是,物联网设备与第一服务器通信过程中,数据上传时采用非对称加密算法加密数据,约为256字节数,消息下发时采用对称加密算法加密数据,约为 $16*n$ 字节数,其中 $n < 16$ ,减少了数据传输的字节数,进一步降低数据流量消耗。

[0168] 步骤416、目标服务器接收物联网设备发送的第二加密数据包和加密后的注册请求。

[0169] 具体的,加密后的注册请求为采用第二会话密钥加密的注册请求。

[0170] 步骤417、目标服务器解密第二加密数据包。

[0171] 具体的,目标服务器采用预设算法(服务器之间的一种内部约定算法)即可解密第二加密数据包。

[0172] 步骤418、若能够成功解密第二加密数据包且得到访问令牌和第二会话密钥,目标服务器采用第二会话密钥解密加密后的注册请求得到注册请求。

[0173] 需要说明的是,加密后的注册请求是物联网设备采用第二会话密钥加密的注册请求,若能够成功解密第二加密数据包且得到访问令牌和第二会话密钥,就能采用第二会话密钥就可解密加密后的注册请求,得到注册请求。

[0174] 步骤419、目标服务器获取注册请求中的注册码。

[0175] 需要说明的是,注册码包含在注册请求中。

[0176] 步骤420、目标服务器判断注册码是否合法。

[0177] 步骤421、若注册码合法,目标服务器确定物联网设备注册成功。

[0178] 具体的,物联网设备注册成功也就是指物联网设备接入成功。

[0179] 本发明的实施例提供的异构网络的通信方法,第一服务器确定负载较小的第二服务器作为目标服务器,并将目标服务器地址发送给物联网设备,物联网设备根据目标服务器地址向对应的目标服务器发送注册请求,目标服务器及时响应并确定注册是否成功,一

方面有效地平衡了服务器的负载,另一方面保证了物联网设备的注册请求能够及时地得到处理;同时,物联网设备、第一服务器和目标服务器之间采用加密解密的方式完成交互过程,还有效地防止了恶意设备的接入。

[0180] 在上述图5对应的实施例的基础上,本发明实施例提供了又一种异构网络的通信方法,如图6所示,该方法还包括:

[0181] 步骤422、目标服务器为物联网设备分配鉴权码。

[0182] 需要说明的是,目标服务器在确定物联网设备注册成功后会为物联网设备分配鉴权码。

[0183] 具体的,若物联网设备与目标服务器的连接断开,则需要重新进行注册的所有过程,待目标服务器确认物联网设备注册成功后,为物联网设备分配新的鉴权码。

[0184] 步骤423、目标服务器采用第二会话密钥加密鉴权码。

[0185] 步骤424、目标服务器发送加密后的鉴权码至物联网设备。

[0186] 步骤425、物联网设备接收目标服务器发送的加密后的鉴权码。

[0187] 需要说明的是,加密后的鉴权码为采用第二会话密钥加密的鉴权码。

[0188] 步骤426、物联网设备采用第二会话密钥解密加密后的鉴权码,得到鉴权码。

[0189] 步骤427、物联网设备通过预设方式处理待传输数据,并采用第二会话密钥加密处理后的待传输数据,生成第三加密数据包。

[0190] 具体的,由于待传输数据可能会比较庞大,因此物联网设备需要通过预设方式进行预先处理,从而生成轻量化的数据包,再采用第二会话密钥加密后生成第三加密数据包。

[0191] 步骤428、物联网设备发送第三加密数据包和鉴权码至目标服务器。

[0192] 需要说明的是,鉴权码用于向目标服务器表明自己是成功注册的物联网设备,在后续每一次待传输数据的发送过程中,物联网设备都需要携带鉴权码。

[0193] 步骤429、目标服务器接收物联网设备发送的第三加密数据包和鉴权码。

[0194] 步骤430、目标服务器判断鉴权码是否正确。

[0195] 需要说明的是,判断鉴权码的正确性是为了判断物联网设备是否成功注册了物联网设备。

[0196] 步骤431、若鉴权码正确,目标服务器采用第二会话密钥解密第三加密数据包,得到待传输数据。

[0197] 需要说明的是,第三加密数据包是物联网设备采用第二会话密钥加密的数据包,因此,采用第二会话密钥就能解密第三加密数据包,得到采用预设方式处理后的待传输数据,进而得到待传输数据。

[0198] 本发明的实施例提供的异构网络的通信方法,第一服务器确定负载较小的第二服务器作为目标服务器,并将目标服务器地址发送给物联网设备,物联网设备根据目标服务器地址向对应的目标服务器发送注册请求,目标服务器及时响应并确定注册是否成功,因此,一方面有效地平衡了服务器的负载,另一方面保证了物联网设备的注册请求能够及时地得到处理;同时,物联网设备、第一服务器和目标服务器之间采用加密解密的方式完成交互过程,还有效地防止了恶意设备的接入;并且在注册成功后,物联网设备对将要发送目标服务器的待传输数据进行加密,还保证了数据的安全性。

[0199] 本发明实施例提供了一种物联网设备,如图7所示,该物联网设备5包括:

[0200] 第一加密模块51,用于加密第一会话密钥;其中,第一会话密钥用于第一服务器生成第一加密数据包。

[0201] 第一发送模块52,用于将加密后的第一会话密钥发送至第一服务器。

[0202] 第一接收模块53,用于接收第一服务器发送的第一加密数据包;其中,第一加密数据包用于确定目标服务器,目标服务器为第二服务器中的服务器。

[0203] 第一解密模块54,用于根据第一会话密钥和第一加密数据包,得到目标服务器地址。

[0204] 第一发送模块52,还用于发送第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器;其中,第二加密数据包和加密后的注册请求用于目标服务器完成物联网设备的注册。

[0205] 进一步,第一加密数据包中包括采用第一会话密钥加密的第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址;第二加密数据包中包括采用预设算法加密的访问令牌和第二会话密钥;加密后的注册请求为采用第二会话密钥加密的注册请求。

[0206] 进一步,在图7对应的实施例的基础上,本发明实施例提供了另一种物联网设备,如图8所示,第一解密模块54包括:

[0207] 第一解密单元541,用于采用第一会话密钥解密第一加密数据包,得到第二加密数据包、第二会话密钥和通过预设方式处理的目标服务器地址。

[0208] 第一处理单元542,用于根据通过预设方式处理的目标服务器地址得到目标服务器地址。

[0209] 第一发送模块52包括:

[0210] 第一加密单元521,用于采用第二会话密钥加密注册请求。

[0211] 发送单元522,用于发送第二加密数据包和加密后的注册请求至目标服务器地址对应的目标服务器。

[0212] 进一步,第一接收模块53,还用于接收目标服务器发送的加密后的鉴权码;其中,加密后的鉴权码为采用第二会话密钥加密的鉴权码。

[0213] 第一解密模块54,还用于采用第二会话密钥解密加密后的鉴权码,得到鉴权码。

[0214] 第一加密模块51,还用于通过预设方式处理待传输数据,并采用第二会话密钥加密处理后的待传输数据,生成第三加密数据包;

[0215] 第一发送模块52,还用于发送第三加密数据包和鉴权码至目标服务器。

[0216] 进一步,预设方式为AVRO方式。

[0217] 本发明实施例提供的物联网设备,向第一服务器确定的负载较小的目标服务器发送注册请求,能够有效地平衡服务器的负载,并保证了注册请求能够及时地得到处理;同时,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入;并且,在成功注册目标服务器后,对将要发送目标服务器的待传输数据加密,保证了数据的安全性。

[0218] 在实际应用中,所述第一加密模块51、第一发送模块52、第一加密单元521、发送单元522、第一接收模块53、第一解密模块54、第一解密单元541、第一处理单元542可由位于物联网设备的中央处理器(Central Processing Unit,CPU)、微处理器(Micro Processor Unit,MPU)、数字信号处理器(Digital Signal Processor,DSP)或现场可编程门阵列(Field Programmable Gate Array,FPGA)等实现。

- [0219] 本发明实施例提供了一种第一服务器,如图9所示,该第一服务器6包括:
- [0220] 第二接收模块61,用于接收物联网设备发送的加密后的第一会话密钥。
- [0221] 第二解密模块62,用于对加密后的第一会话密钥进行解密得到第一会话密钥。
- [0222] 第二加密模块63,用于采用第一会话密钥加密生成第一加密数据包;其中,第一加密数据包用于物联网设备确定目标服务器,目标服务器为第二服务器中的服务器。
- [0223] 第二发送模块64,用于发送第一加密数据包至物联网设备。
- [0224] 进一步,在图9对应的实施例的基础上,本发明实施例提供了另一种第一服务器,如图10所示,第二加密模块63包括:
- [0225] 第二处理单元631,用于生成第二会话密钥和访问令牌;通过预设方式处理目标服务器地址。
- [0226] 第二加密单元632,用于采用预设算法加密访问令牌和第二会话密钥,生成第二加密数据包;采用第一会话密钥加密第二加密数据包、第二会话密钥和处理后的目标服务器地址,生成第一加密数据包。
- [0227] 第一获取单元633,用于获取目标服务器地址。
- [0228] 进一步,第一获取单元633,具体用于通过第三服务器获取第二服务器的负载;将第二服务器的负载小于预设阈值的第二服务器的地址,作为目标服务器地址。
- [0229] 本发明的实施例提供的第一服务器,接收物联网设备发送的加密后的第一会话密钥,并对加密后的第一会话密钥进行解密得到第一会话密钥;采用第一会话密钥生成用于物联网设备确定目标服务器的第一加密数据包并发送至物联网设备;这样物联网设备能够根据第一加密数据包获得第一服务器选择的负载较小的目标服务器,从而向这些目标服务器发送注册请求,因此避免了物联网设备向繁忙服务器发送注册请求造成繁忙服务器负载更大的问题,有效地平衡了服务器的负载,又保证了物联网设备的注册请求能够及时地得到处理;并且,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入。
- [0230] 在实际应用中,所述第二接收模块61、第二解密模块62、第二加密模块63、第二处理单元631、第二加密单元632、第一获取单元633、第二发送模块64均可由位于第一服务器中的CPU、MPU、DSP或FPGA等实现。
- [0231] 本发明实施例提供了一种目标服务器,如图11所示,该目标服务器7包括:
- [0232] 第三接收模块71,用于接收物联网设备发送的第二加密数据包和加密后的注册请求。
- [0233] 第三解密模块72,用于解密第二加密数据包。
- [0234] 处理模块73,用于根据解密第二加密数据包得到的结果和加密后的注册请求确定物联网设备是否注册成功。
- [0235] 进一步,在图11对应的实施例的基础上,本发明实施例提供了另一种目标服务器,如图12所示,处理模块73包括:
- [0236] 第二解密单元731,用于若能够成功解密所述第二加密数据包且得到访问令牌和第二会话密钥;采用所述第二会话密钥解密所述加密后的注册请求得到注册请求。
- [0237] 第二获取单元732,用于获取注册请求中的注册码。
- [0238] 判断单元733,用于判断注册码是否合法。
- [0239] 第三处理单元734,用于若注册码正确,确定物联网设备注册成功。

[0240] 进一步,在图12对应的实施例的基础上,本发明实施例提供了又一种目标服务器,如图13所示,该目标服务器7还包括:

[0241] 分配模块74,用于为物联网设备分配鉴权码。

[0242] 第三加密模块75,用于采用第二会话密钥加密鉴权码。

[0243] 第三发送模块76,用于将加密后的鉴权码发送至物联网设备。

[0244] 进一步,第三接收模块71,还用于接收物联网设备发送的第三加密数据包和鉴权码。

[0245] 处理模块73,还用于判断鉴权码是否正确;若鉴权码正确,采用第二会话密钥解密第三加密数据包,得到待传输数据。

[0246] 本发明的实施例提供的目标服务器,接收物联网设备发送的第二加密数据包和加密后的注册请求;解密第二加密数据包;根据解密第二加密数据包得到的结果和加密后的注册请求确定物联网设备是否注册成功;这样,由于目标服务器是第一服务器选择的负载较小的服务器,因此目标服务器在接收到物联网设备的注册请求后,可以及时地处理这些请求,从而有效地平衡了服务器的负载,保证了注册请求能够及时地得到处理;同时,通过加密解密的方式完成交互过程还有效地防止了恶意设备的接入;并且在注册成功后,接收物联网设备加密的待传输数据,还保证了数据的安全性。

[0247] 在实际应用中,所述第三接收模块71、第三解密模块72、处理模块73、第二解密单元731、第二获取单元732、判断单元733、第三处理单元734、分配模块74、第三加密模块75、第三发送模块76均可由位于目标服务器中的CPU、MPU、DSP或FPGA等实现。

[0248] 本发明实施例提供了一种异构网络的通信系统,如图14所示,异构网络的通信系统8包括如图7~8对应的实施例提供的物联网设备81、图9~10的实施例提供的实施例提供的第一服务器82、图11~13对应的实施例提供的目标服务器83以及第三服务器84,其中,第三服务器84,用于获取第二服务器的负载,第二服务器的负载用于物联网设备确定目标服务器。

[0249] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明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和光学存储器等)上实施的计算机程序产品的形式。

[0250] 本发明是参照根据本发明实施例的方法、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。

[0251] 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。

[0252] 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

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。

[0253] 以上所述,仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。

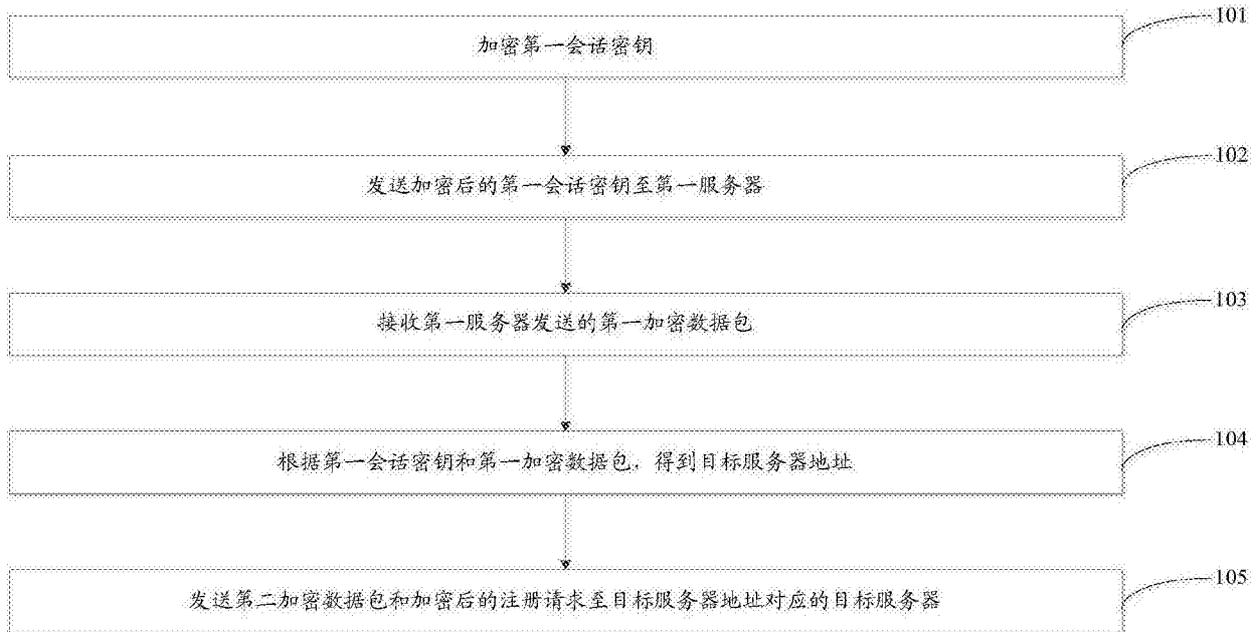


图1

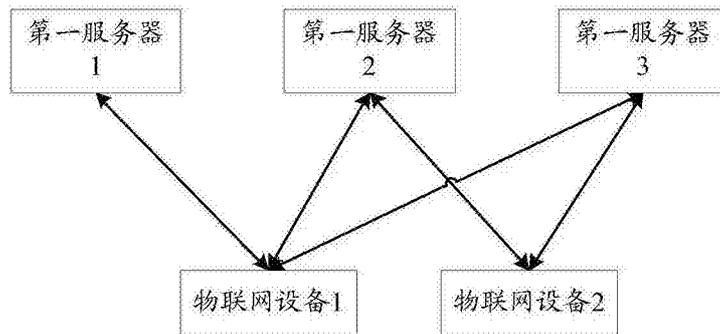


图2

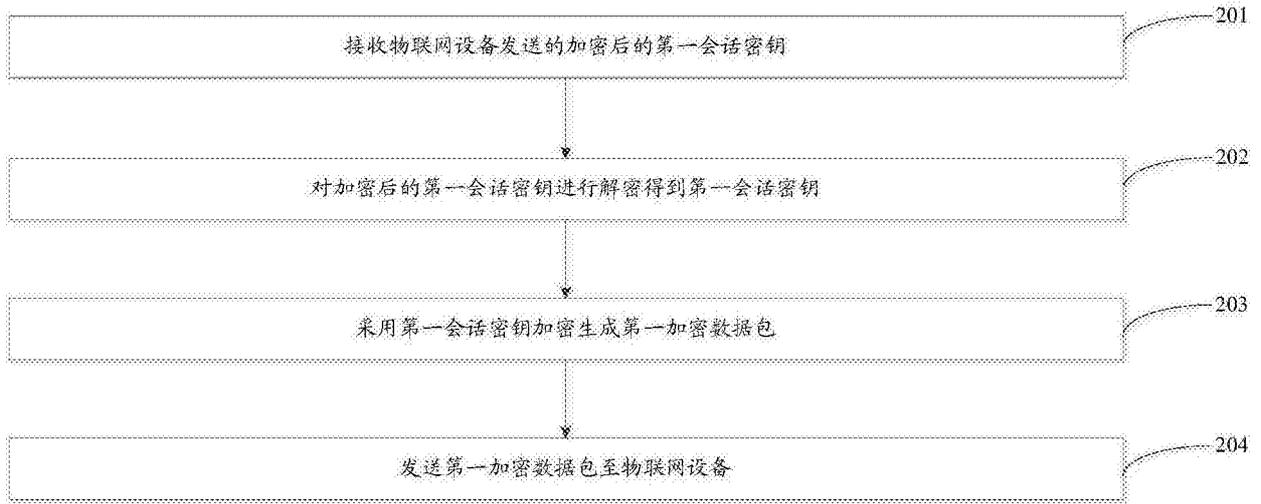


图3

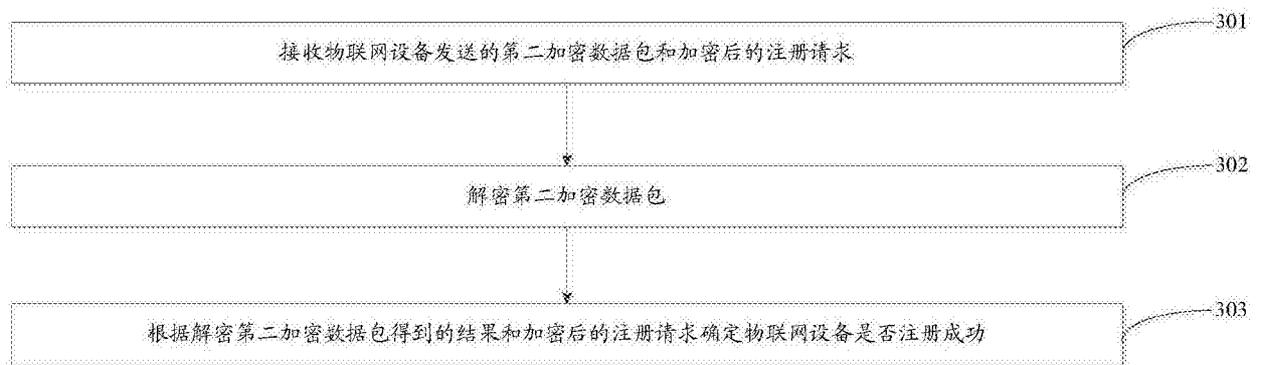


图4

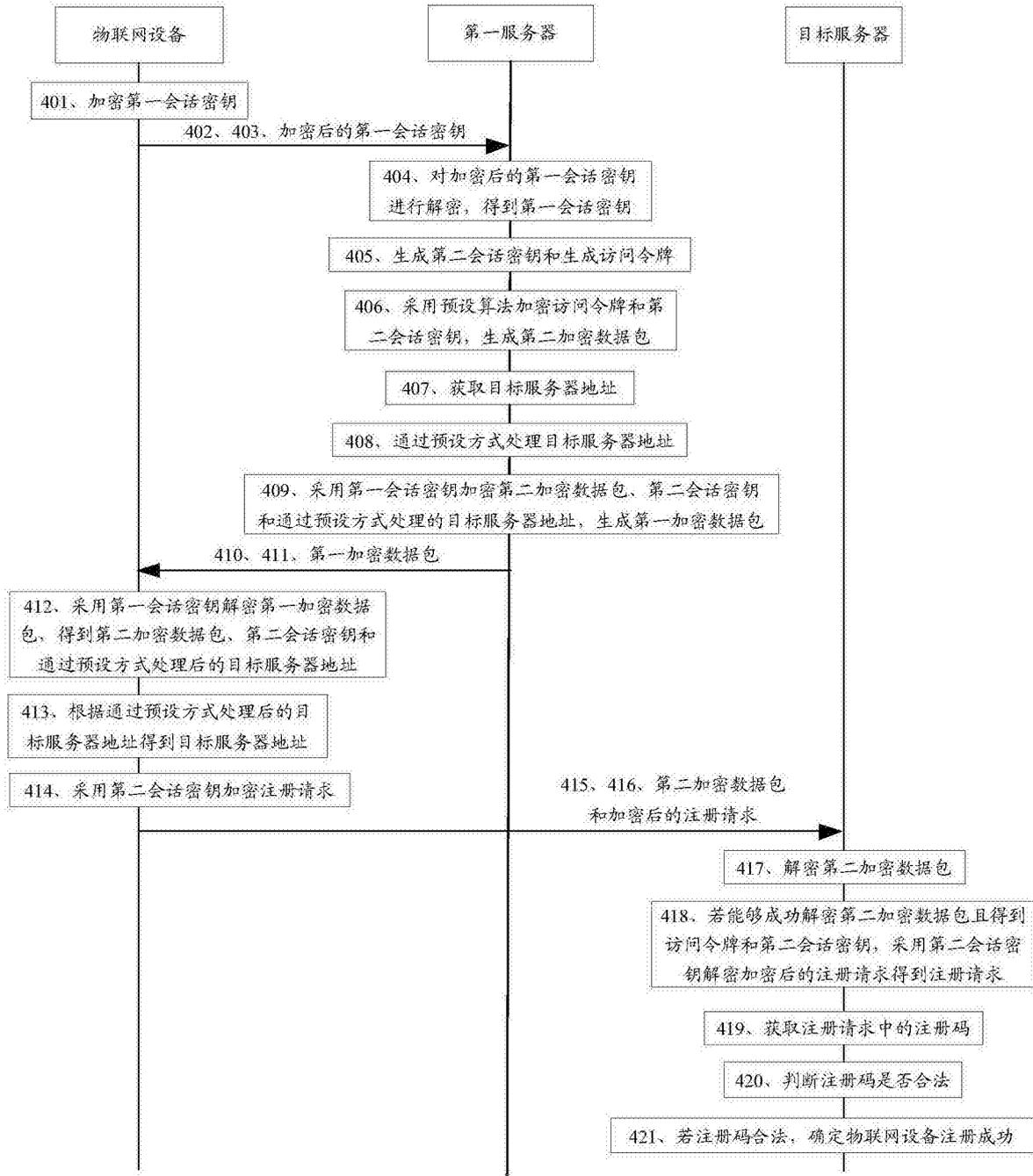


图5

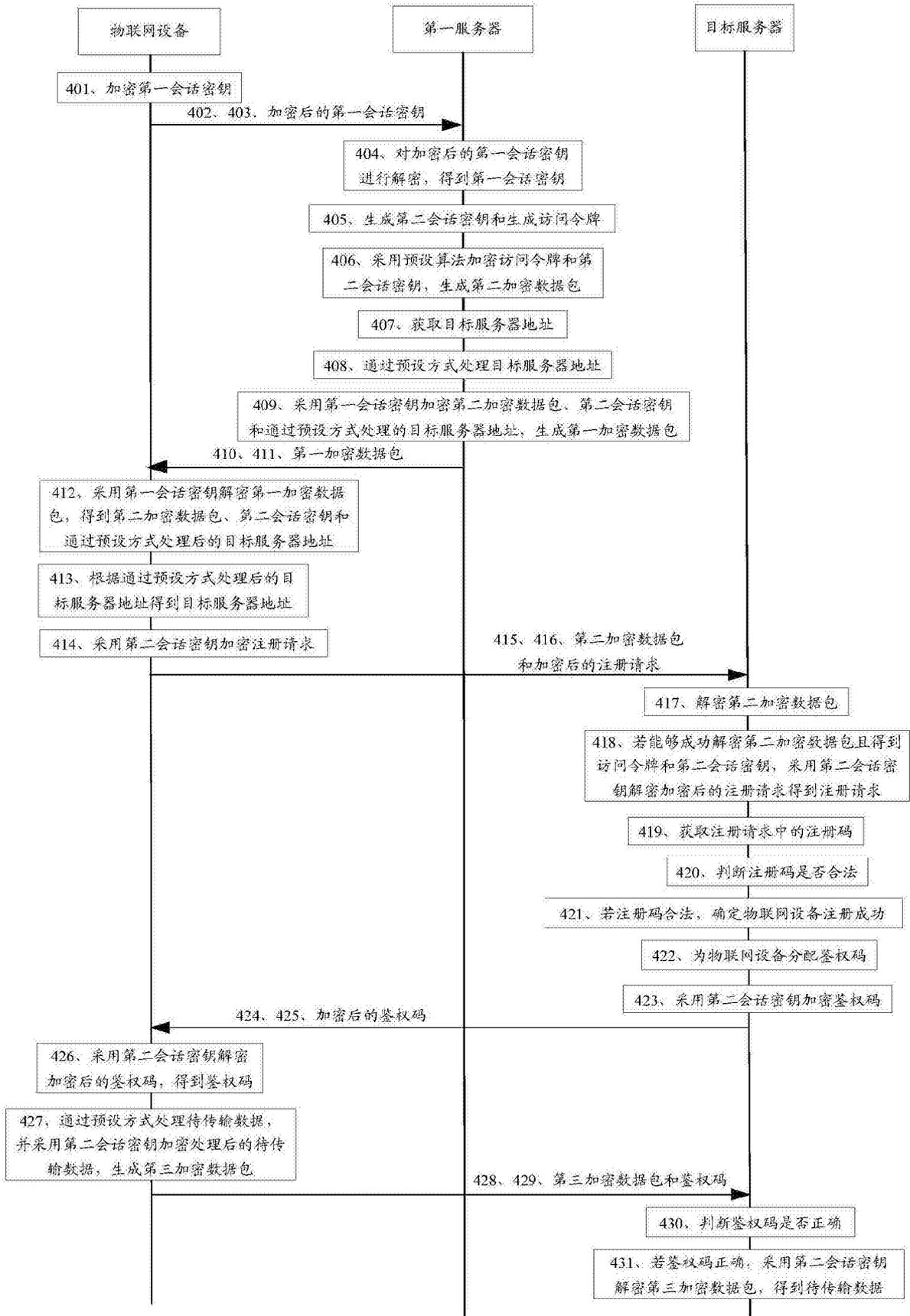


图6

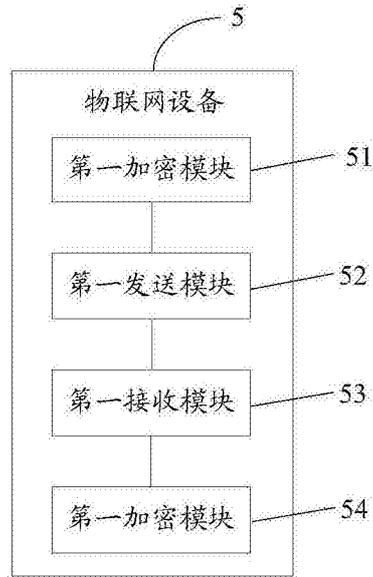


图7

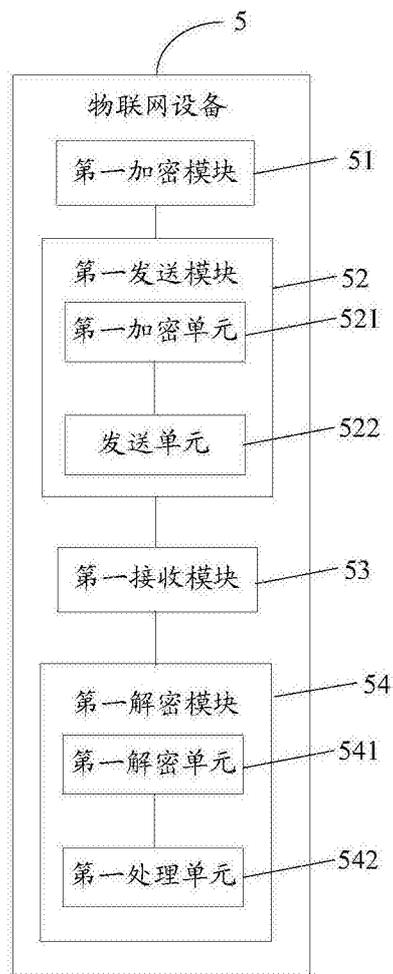


图8

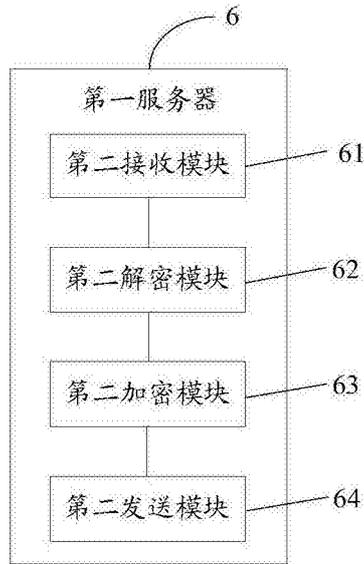


图9

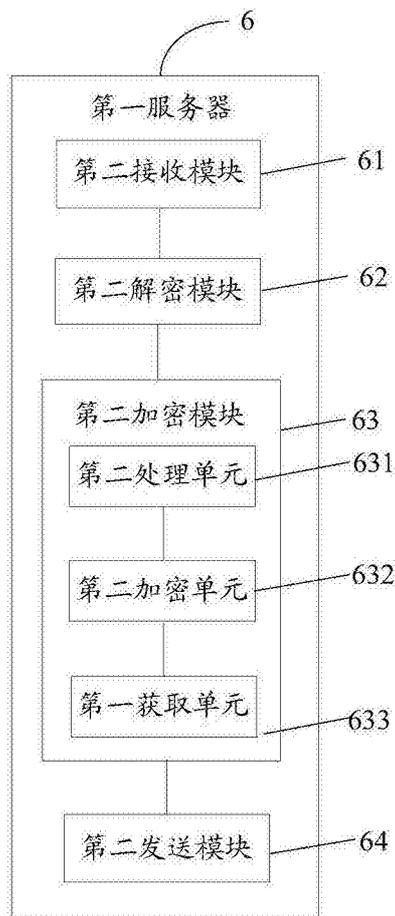


图10

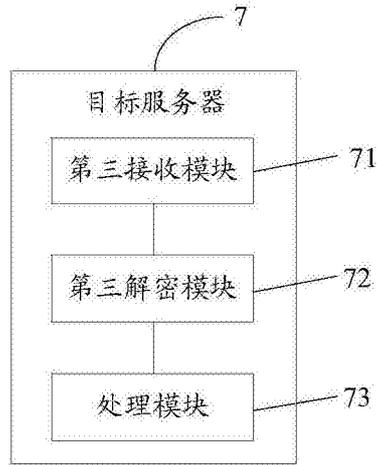


图11

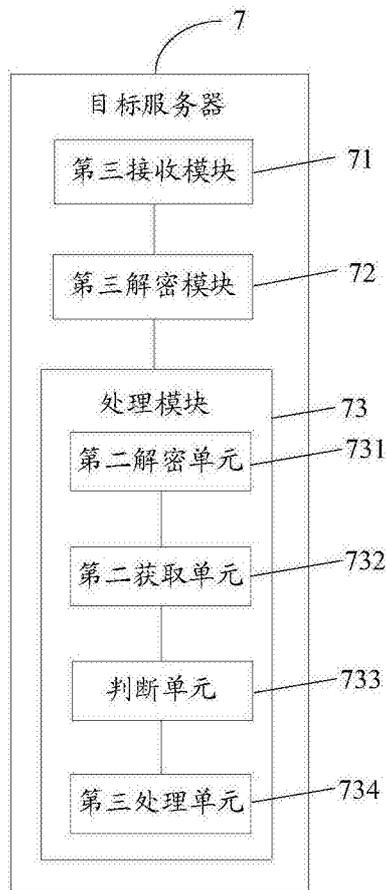


图12

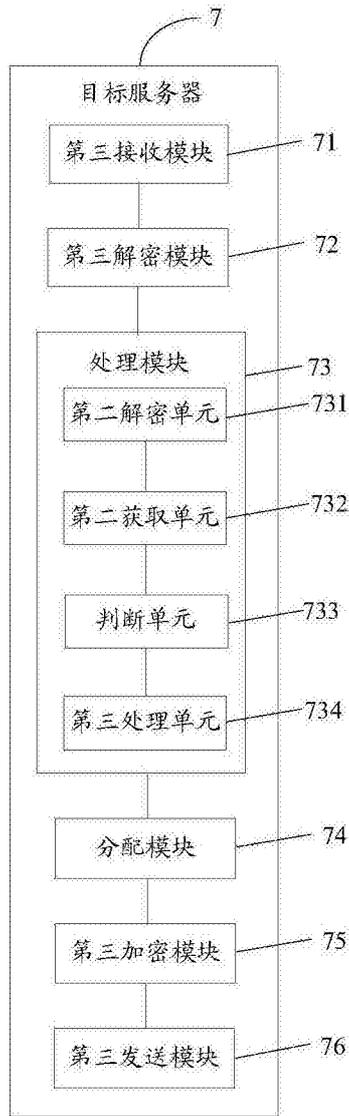


图13

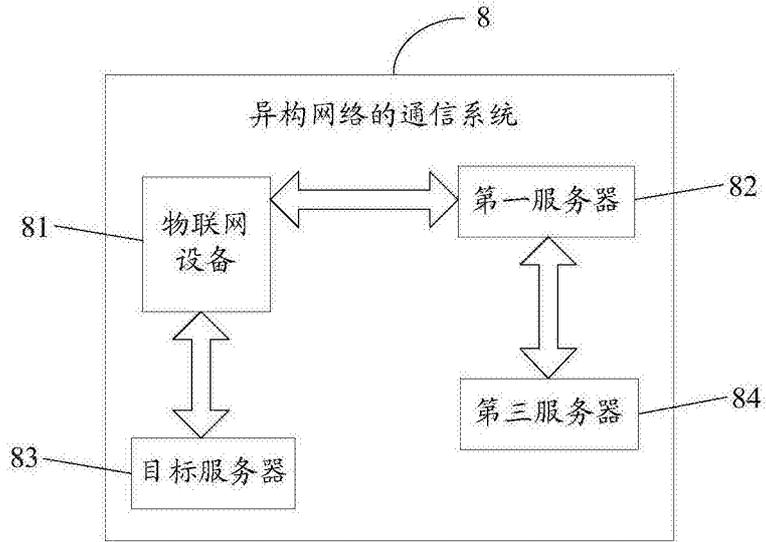


图14