(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 108667601 B
(45)授权公告日 2020.12.01

(21)申请号 201710210007.X
(22)申请日 2017.03.31
(65)同一申请的已公布的文献号
申请公布号 CN 108667601 A
(43)申请公布日 2018.10.16
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 肖杨 刘艳
(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 罗振安
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101345761 A,2009.01.14
CN 102594563 A,2012.07.18
CN 101989984 A,2011.03.23
CN 101931536 A,2010.12.29

审查员 代悦宁

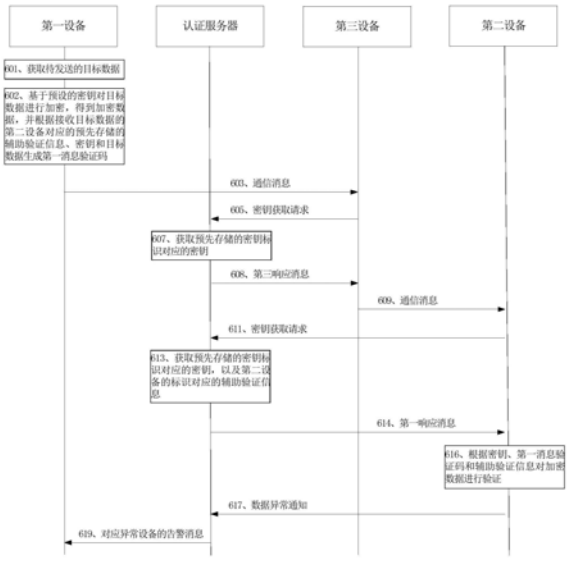
权利要求书4页 说明书18页 附图6页

(54)发明名称

一种传输数据的方法、装置和设备

(57)摘要

本公开提供了一种传输数据的方法、装置和设备，属于通信技术领域。所述方法包括：接收第一设备的通信消息，所述通信消息中携带有密钥标识、加密数据和第一消息验证码，其中，所述加密数据是通过所述密钥标识对应的密钥对待发送的目标数据加密得到的数据，所述第一消息验证码是根据所述密钥、所述目标数据和预设的辅助验证信息生成的验证码；获取所述密钥标识对应的密钥和所述辅助验证信息；根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证。本公开可以提高传输数据的可靠性。



CN 108667601 B

1.一种传输数据的方法,其特征在于,所述方法包括:

接收第一设备的通信消息,所述通信消息中携带有密钥标识、加密数据和第一消息验证码,其中,所述加密数据是通过所述密钥标识对应的密钥对待发送的目标数据加密得到的数据,所述第一消息验证码是根据所述密钥、所述目标数据和预设的辅助验证信息生成的验证码;

向认证服务器发送密钥获取请求,所述密钥获取请求中携带有所述密钥标识和本地的标识;

接收所述认证服务器发送的第一响应消息,所述第一响应消息中携带有所述密钥标识对应的密钥和所述辅助验证信息;

根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证。

2.根据权利要求1所述的方法,其特征在于,所述根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证,包括:

基于所述密钥对所述加密数据进行解密;

根据所述密钥、所述辅助验证信息和解密得到的数据生成第二消息验证码,如果所述第一消息验证码与所述第二消息验证码不匹配,则所述加密数据验证未通过。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

如果验证未通过,则向所述认证服务器发送数据异常通知。

4.根据权利要求1所述的方法,其特征在于,所述接收第一设备发送的通信消息之前,还包括:

向所述第一设备发送数据获取请求,以使所述第一设备发送所述通信消息。

5.根据权利要求1所述的方法,其特征在于,所述接收第一设备的通信消息,包括:

接收第三设备转发的第一设备的通信消息,所述第三设备是接收所述目标数据的传输路中的其他接收方。

6.一种传输数据的方法,其特征在于,所述方法包括:

接收第二设备发送的密钥获取请求,所述密钥获取请求中携带有密钥标识和所述第二设备的标识;

获取预先存储的所述密钥标识对应的密钥,以及所述第二设备的标识对应的辅助验证信息;

向所述第二设备发送第一响应消息,所述第一响应消息中携带有所述密钥和所述辅助验证信息,以使所述第二设备根据所述密钥和所述辅助验证信息对接收到的加密数据进行验证。

7.根据权利要求6所述的方法,其特征在于,所述方法还包括:

接收第一设备发送的密钥注册请求,所述密钥注册请求中携带有目标数据的接收方的标识和所述第一设备的标识;

根据所述第一设备的标识和所述接收方的标识,获取各接收方对应的传输路径;

如果所述各接收方中的所述第二设备对应的传输路径中,存在所述目标数据的其他接收方,则生成所述第二设备对应的辅助验证信息;

向所述第一设备发送第二响应消息,所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

8.根据权利要求7所述的方法，其特征在于，所述根据所述第一设备的标识和所述目标数据的接收方的标识，获取各接收方对应的传输路径，包括：

根据所述第一设备的标识和所述目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径；或者，

根据所述第一设备的标识和所述目标数据的接收方的标识，生成各接收方对应的传输路径。

9.根据权利要求6-8任一所述的方法，其特征在于，所述方法还包括：

接收所述第二设备发送的数据异常通知；

根据所述第二设备对应的传输路径，以及所述传输路径中的其他接收方，确定所述传输路径中的异常设备，向所述第一设备发送对应所述异常设备的告警消息。

10.一种传输数据的方法，其特征在于，所述方法包括：

向认证服务器发送密钥注册请求，所述密钥注册请求中携带有目标数据的接收方的标识和本地的标识；

接收所述认证服务器发送的第二响应消息，所述第二响应消息中携带有第二设备对应的辅助验证信息；

获取待发送的目标数据；

基于预设的密钥对所述目标数据进行加密，得到加密数据，并根据接收所述目标数据的所述第二设备对应的辅助验证信息、所述密钥和所述目标数据生成第一消息验证码，其中，所述第二设备对应的传输路径中存在所述目标数据的其他接收方；

向所述第二设备发送通信消息，所述通信消息中携带有所述密钥的密钥标识、所述加密数据和所述第一消息验证码。

11.根据权利要求10所述的方法，其特征在于，所述获取待发送的目标数据之前，还包括：

当接收到所述第二设备发送的数据获取请求时，执行获取待发送的目标数据的步骤。

12.根据权利要求10所述的方法，其特征在于，所述向所述第二设备发送通信消息，包括：

向第三设备发送所述通信消息，以使所述第三设备将所述通信消息转发给所述第二设备，所述第三设备是所述第二设备对应的传输路径中的其他接收方。

13.一种传输数据的装置，其特征在于，所述装置包括：

收发单元，用于接收第一设备的通信消息，所述通信消息中携带有密钥标识、加密数据和第一消息验证码，其中，所述加密数据是通过所述密钥标识对应的密钥对待发送的目标数据加密得到的数据，所述第一消息验证码是根据所述密钥、所述目标数据和预设的辅助验证信息生成的验证码；

获取单元，用于向认证服务器发送密钥获取请求，所述密钥获取请求中携带有所述密钥标识和本地的标识；接收所述认证服务器发送的第一响应消息，所述第一响应消息中携带有所述密钥标识对应的密钥和所述辅助验证信息；

处理单元，用于根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证。

14.根据权利要求13所述的装置，其特征在于，所述处理单元，还用于：

基于所述密钥对所述加密数据进行解密；

根据所述密钥、所述辅助验证信息和解密得到的数据生成第二消息验证码，如果所述第一消息验证码与所述第二消息验证码不匹配，则所述加密数据验证未通过。

15.根据权利要求13所述的装置，其特征在于，所述处理单元，还用于：

如果验证未通过，则控制所述收发单元向所述认证服务器发送数据异常通知。

16.根据权利要求13所述的装置，其特征在于，所述收发单元，还用于：

向所述第一设备发送数据获取请求，以使所述第一设备发送所述通信消息。

17.根据权利要求13所述的装置，其特征在于，所述收发单元，还用于：

接收第三设备转发的第一设备的通信消息，所述第三设备是接收所述目标数据的传输路中的其他接收方。

18.一种传输数据的装置，其特征在于，所述装置包括：

收发单元，用于接收第二设备发送的密钥获取请求，所述密钥获取请求中携带有密钥标识和所述第二设备的标识；

获取单元，用于获取预先存储的所述密钥标识对应的密钥，以及所述第二设备的标识对应的辅助验证信息；

所述收发单元，还用于向所述第二设备发送第一响应消息，所述第一响应消息中携带有所述密钥和所述辅助验证信息，以使所述第二设备根据所述密钥和所述辅助验证信息对接收到的加密数据进行验证。

19.根据权利要求18所述的装置，其特征在于，所述装置还包括：

所述收发单元，还用于接收第一设备发送的密钥注册请求，所述密钥注册请求中携带有目标数据的接收方的标识和所述第一设备的标识；

所述获取单元，还用于根据所述第一设备的标识和所述接收方的标识，获取各接收方对应的传输路径；

处理单元，用于如果所述各接收方中的所述第二设备对应的传输路径中，存在所述目标数据的其他接收方，则生成所述第二设备对应的辅助验证信息；

所述收发单元，还用于向所述第一设备发送第二响应消息，所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

20.根据权利要求19所述的装置，其特征在于，所述获取单元，还用于：

根据所述第一设备的标识和所述目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径；或者，

根据所述第一设备的标识和所述目标数据的接收方的标识，生成各接收方对应的传输路径。

21.根据权利要求18-20任一所述的装置，其特征在于，所述收发单元，还用于：

接收所述第二设备发送的数据异常通知；

根据所述第二设备对应的传输路径，以及所述传输路径中的其他接收方，确定所述传输路径中的异常设备，向所述第一设备发送对应所述异常设备的告警消息。

22.一种传输数据的装置，其特征在于，所述装置包括：

收发单元，用于：

向认证服务器发送密钥注册请求，所述密钥注册请求中携带有目标数据的接收方的标

识和本地的标识；

接收所述认证服务器发送的第二响应消息，所述第二响应消息中携带有第二设备对应的辅助验证信息；

获取单元，用于获取待发送的目标数据；

处理单元，用于基于预设的密钥对所述目标数据进行加密，得到加密数据，并根据接收所述目标数据的第二设备对应的辅助验证信息、所述密钥和所述目标数据生成第一消息验证码，其中，所述第二设备对应的传输路径中存在所述目标数据的其他接收方；

所述收发单元，还用于向所述第二设备发送通信消息，所述通信消息中携带有所述密钥的密钥标识、所述加密数据和所述第一消息验证码。

23.根据权利要求22所述的装置，其特征在于，所述收发单元，还用于：

当接收到所述第二设备发送的数据获取请求时，控制所述获取单元执行获取待发送的目标数据的步骤。

24.根据权利要求22所述的装置，其特征在于，所述收发单元，还用于：

向第三设备发送所述通信消息，以使所述第三设备将所述通信消息转发给所述第二设备，所述第三设备是所述第二设备对应的传输路径中的其他接收方。

25.一种计算机可读存储介质，其特征在于，所述计算机存储介质中存储有计算机程序，所述计算机程序由处理器加载并执行以实现如权利要求1-13任一项所述的方法。

一种传输数据的方法、装置和设备

技术领域

[0001] 本公开涉及通信技术领域，特别涉及一种传输数据的方法、装置和设备。

背景技术

[0002] 目前，通信网络的应用越来越广泛，人们可以通过通信网络实现信息化和远程管理控制。通信网络中两个设备跨越多个节点传输数据的多跳传输是常见的传输方式。在多跳传输的过程中，各设备将数据发送给与其相邻的设备，相邻设备根据某种方式(例如IP路由算法，或其他方式)将数据转发给自身相邻的设备，再由该设备进行转发，直到转发至接收方为止。例如，物联网通信网络可以包括业务服务器、平台服务器、网关和家庭中安装的摄像头，摄像头向业务服务器发送数据的传输路径为摄像头、网关、平台服务器、业务服务器。

[0003] 为了提高传输数据的安全性，可以对待发送的数据进行加密传输，其中一种常见的处理过程可以为：发送设备在认证服务器中注册密钥并获得密钥标识，用该密钥对待发送的数据进行加密，然后向接收设备发送通信消息，该通信消息中携带加密后的数据和密钥标识等。接收设备接收到该通信消息后，可以根据密钥标识从认证服务器中获取相应的密钥，对加密后的数据进行解密，从而获取到数据原文。

[0004] 在实际中，经常会出现数据被多个设备所需要的情况。例如，在家的用户通过访问本地的网关获取监控数据，外出的用户可以通过访问业务服务器获取监控数据，此时网关和业务服务器均需要获得监控数据。或者，一个人的健康数据(例如血糖，血压，体重等等)需要发送给远程诊断中心或者健身房中心，以获取日常注意指导或健身指导。为了确保安全，发送给网关和业务服务器的监控数据，或者发送给远程诊断中心或健身房中心的健康数据，均可采用上述方式进行加密传输。但这种情况下，若某一接收设备的传输路径中包含其他可以拥有密钥的接收设备(称中间设备)，则会带来安全隐患，例如，若中间设备被入侵，则入侵者可以通过该密钥解密得到数据原文，对数据原文进行篡改，然后再用该密钥进行加密，将加密后的数据发送给该接收设备，而该接收设备无法获知该数据已被篡改，导致传输数据的可靠性降低。

发明内容

[0005] 为了解决现有技术的问题，本公开实施例提供了一种传输数据的方法、装置和设备。所述技术方案如下：

[0006] 第一方面，提供了一种传输数据的方法，所述方法包括：

[0007] 接收第一设备的通信消息，所述通信消息中携带有密钥标识、加密数据和第一消息验证码，其中，所述加密数据是通过所述密钥标识对应的密钥对待发送的目标数据加密得到的数据，所述第一消息验证码是根据所述密钥、所述目标数据和预设的辅助验证信息生成的验证码；

[0008] 获取所述密钥标识对应的密钥和所述辅助验证信息；

[0009] 根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证。

[0010] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0011] 在一种可能的实现方式中，所述获取所述密钥标识对应的密钥和所述辅助验证信息，包括：

[0012] 向认证服务器发送密钥获取请求，所述密钥获取请求中携带有所述密钥标识和本地的标识；

[0013] 接收所述认证服务器发送的第一响应消息，所述第一响应消息中携带有所述密钥标识对应的密钥和所述辅助验证信息。

[0014] 这样，提供了一种获取密钥和辅助验证信息的实现方式。

[0015] 在另一种可能的实现方式中，所述根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证，包括：

[0016] 基于所述密钥对所述加密数据进行解密；

[0017] 根据所述密钥、所述辅助验证信息和解密得到的数据生成第二消息验证码，如果所述第一消息验证码与所述第二消息验证码不匹配，则所述加密数据验证未通过。

[0018] 这样，提供了一种对加密数据进行验证的实现方式。

[0019] 在另一种可能的实现方式中，所述方法还包括：

[0020] 如果验证未通过，则向所述认证服务器发送数据异常通知。

[0021] 这样，可以通知认证服务器数据出现异常，以便认证服务器按照预设的安全策略进行处理，提高数据的安全性。

[0022] 在另一种可能的实现方式中，所述接收第一设备发送的通信消息之前，还包括：

[0023] 向所述第一设备发送数据获取请求，以使所述第一设备发送所述通信消息。

[0024] 这样，第二设备可以主动获取第一设备的数据。

[0025] 在另一种可能的实现方式中，所述接收第一设备的通信消息，包括：

[0026] 接收第三设备转发的第一设备的通信消息，所述第三设备是接收所述目标数据的传输路中的其他接收方。

[0027] 第二方面，提供了一种传输数据的方法，所述方法包括：

[0028] 接收第二设备发送的密钥获取请求，所述密钥获取请求中携带有密钥标识和所述第二设备的标识；

[0029] 获取预先存储的所述密钥标识对应的密钥，以及所述第二设备的标识对应的辅助验证信息；

[0030] 向所述第二设备发送第一响应消息，所述第一响应消息中携带有所述密钥和所述辅助验证信息，以使所述第二设备对接收到的加密数据进行验证。

[0031] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数

据是否篡改，提高了传输数据的可靠性。

[0032] 在一种可能的实现方式中，所述方法还包括：

[0033] 接收第一设备发送的密钥注册请求，所述密钥注册请求中携带有所述目标数据的接收方的标识和所述第一设备的标识；

[0034] 根据所述第一设备的标识和所述接收方的标识，获取各接收方对应的传输路径；

[0035] 如果所述接收方中的所述第二设备对应的传输路径中，存在所述目标数据的其他接收方，则生成所述第二设备对应的辅助验证信息；

[0036] 向所述第一设备发送第二响应消息，所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

[0037] 这样，提供了注册密钥以及生成辅助验证信息的实现方式。

[0038] 在另一种可能的实现方式中，所述根据所述第一设备的标识和所述目标数据的接收方的标识，获取各接收方对应的传输路径，包括：

[0039] 根据所述第一设备的标识和所述目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径；或者，

[0040] 根据所述第一设备的标识和所述目标数据的接收方的标识，生成各接收方对应的传输路径。

[0041] 这样，提供了获取传输路径的实现方式。

[0042] 在另一种可能的实现方式中，所述方法还包括：

[0043] 接收所述第二设备发送的数据异常通知；

[0044] 根据所述第二设备对应的传输路径，以及所述传输路径中的其他接收方，确定所述传输路径中的异常设备，向所述第一设备发送对应所述异常设备的告警消息。

[0045] 这样，可以确定发生异常的设备，并可以通知第一设备，第一设备可以停止向异常设备发送通信消息，以防止数据被篡改。

[0046] 第三方面，提供了一种传输数据的方法，所述方法包括：

[0047] 获取待发送的目标数据；

[0048] 基于预设的密钥对所述目标数据进行加密，得到加密数据，并根据接收所述目标数据的第二设备对应的预先存储的辅助验证信息、所述密钥和所述目标数据生成第一消息验证码，其中，所述第二设备对应的传输路径中存在所述目标数据的其他接收方；

[0049] 向所述第二设备发送通信消息，所述通信消息中携带有所述密钥的密钥标识、所述加密数据和所述第一消息验证码。

[0050] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0051] 在一种可能的实现方式中，所述方法还包括：

[0052] 向认证服务器发送密钥注册请求，所述密钥注册请求中携带有所述目标数据的接收方的标识和本地的标识；

[0053] 接收所述认证服务器发送的第二响应消息，所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

[0054] 这样，提供了注册密钥以及生成辅助验证信息的实现方式。

[0055] 在另一种可能的实现方式中，所述获取待发送的目标数据之前，还包括：

[0056] 当接收到所述第二设备发送的数据获取请求时，执行获取待发送的目标数据的步骤。

[0057] 这样，第二设备可以主动获取第一设备的数据。

[0058] 在另一种可能的实现方式中，所述向所述第二设备发送通信消息，包括：

[0059] 向第三设备发送所述通信消息，以使所述第三设备将所述通信消息转发给所述第二设备，所述第三设备是所述第二设备对应的传输路径中的其他接收方。

[0060] 第四方面，提供了一种第二设备，该第二设备包括：第一处理器、第一网络接口、第一存储器、第一发射器和第一接收器，第一存储器与第一网络接口分别与第一处理器相连；第一处理器被配置为执行第一存储器中存储的指令；第一处理器通过执行指令来实现上述第一方面或第一方面中任意一种可能的实现方式所提供的传输数据的方法。

[0061] 第五方面，本发明实施例提供了一种传输数据的装置，该传输数据的装置包括至少一个单元，该至少一个单元用于实现上述第一方面或第一方面中任意一种可能的实现方式所提供的传输数据的方法。

[0062] 第六方面，提供了一种认证服务器，该认证服务器包括：第二处理器、第二网络接口、第二存储器、第二接收器和第二发射器，第二存储器与第二网络接口分别与第二处理器相连；第二处理器被配置为执行第二存储器中存储的指令；第二处理器通过执行指令来实现上述第二方面或第二方面中任意一种可能的实现方式所提供的传输数据的方法。

[0063] 第七方面，本发明实施例提供了一种传输数据的装置，该传输数据的装置包括至少一个单元，该至少一个单元用于实现上述第二方面或第二方面中任意一种可能的实现方式所提供的传输数据的方法。

[0064] 第八方面，提供了一种第一设备，该第一设备包括：第三处理器、第三网络接口、第三存储器、第三接收器和第三发射器，第三存储器与第三网络接口分别与第三处理器相连；第三处理器被配置为执行第三存储器中存储的指令；第三处理器通过执行指令来实现上述第三方面或第三方面中任意一种可能的实现方式所提供的传输数据的方法。

[0065] 第九方面，本发明实施例提供了一种传输数据的装置，该传输数据的装置包括至少一个单元，该至少一个单元用于实现上述第三方面或第三方面中任意一种可能的实现方式所提供的传输数据的方法。

[0066] 第十方面，本发明实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面至第三方面任意一种可能的实现方式所提供的传输数据的方法。

[0067] 本公开实施例提供的技术方案带来的有益效果是：

[0068] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

附图说明

[0069] 图1是本公开实施例提供的系统框架图；

[0070] 图2是本公开实施例提供的第二设备的结构示意图；

[0071] 图3是本公开实施例提供的认证服务器的结构示意图；

[0072] 图4是本公开实施例提供的第一设备的结构示意图；

[0073] 图5是本公开实施例提供的传输数据的方法流程图；

[0074] 图6是本公开实施例提供的传输数据的方法流程图；

[0075] 图7是本公开实施例提供的传输数据的方法流程图；

[0076] 图8是本公开实施例提供的传输数据的装置结构示意图；

[0077] 图9是本公开实施例提供的传输数据的装置结构示意图；

[0078] 图10是本公开实施例提供的传输数据的装置结构示意图。

具体实施方式

[0079] 为使本公开的目的、技术方案和优点更加清楚，下面将结合附图对本公开实施方式作进一步地详细描述。

[0080] 上述所有可选技术方案，可以采用任意结合形成本公开的可选实施例，在此不再一一赘述。

[0081] 随着通信网络的发展，设备之间的通讯方式越来越多样化。在机器通信(Machine-to-Machine Communications，M2M)系统中，通常会包含多层设备，例如，在智能监控的场景中，可以包括业务服务器、网关和家庭中安装的摄像头这三层设备。其中，层次相邻的设备，可称为相邻的设备。在多跳传输的过程中，各设备将数据发送给与其相邻的设备，相邻设备根据某种方式(例如IP路由算法，或其他方式)将数据转发给，直到转发至接收方为止。本发明实施例中，M2M系统可以包含应用服务节点(Application Service Node，ASN)、中间节点(Middle Node，MN)、基础设施节点(Infrastructure Node，IN)、M2M认证功能(M2M Authentication Function，MAF)设备和业务服务器。其中，ASN可以为终端设备，比如智能摄像头或智能空调等，ASN可以包含一个公共服务实体(Common Service Entity，CSE)和至少一个应用实体(Application Entity，AE)；MN可以为M2M系统中的网关设备，比如家庭网关，MN可以包含一个CSE，以及任意数目个AE；IN可以包含一个CSE，以及任意数目个AE；MAF可以是M2M系统在运行过程中为各设备注册和发放密钥的设备，可称为认证服务器；业务服务器可以是M2M系统中某业务的后台服务器，可以包含一个AE，比如某智能摄像头的后台服务器。如图1所示，为本实施提供的系统框架图，其中包括MAF001、AE002(即业务服务器)、IN003、MN004和ASN005。其中，MAF001可以与IN003、AE002建立数据连接，还可以与至少一个MN 004和ASN005建立数据连接。该数据连接可以是传输层安全(Transport Layer Security，TLS)协议连接，或数据包传输层安全性(Datagram Transport Layer Security，DTLS)协议连接。

[0082] 需要说明的是，上述设备可以是一个单独的设备或服务器，也可以是某设备或某服务器中的一个功能模块。在传输数据时，可以是终端设备向上级设备(即网关设备或业务服务器)发送数据，也可以是上级设备向终端设备发送数据。为了便于描述，本实施例中发送方可称为第一设备，接收方可称为第二设备，第一设备与第二设备的传输路径中，可以存

在至少一个中间设备，中间设备中可以存在至少一个待传输数据(即下文中的目标数据)的其他接收方。

[0083] 参见图2，其示出了本发明示例性实施例提供的用于接收通信消息的第二设备，该第二设备10包括第一收发器1011和第一存储器1012，该第二设备还可以包括第一处理器1013和第一网络接口1014。其中，第一存储器1012和第一网络接口1014分别与第一处理器1013连接；第一存储器1012用于存储程序代码，程序代码包括计算机操作指令，第一处理器1013和第一收发器1011用于执行第一存储器1012中存储的程序代码，用于实现传输数据的相关处理，并可以通过第一网络接口1014与第一设备和认证服务器进行交互。

[0084] 其中，第一存储器1012与第一网络接口1014分别与第一处理器1013和第一收发器1011相连，第一收发器1011可以包括第一发射器和第一接收器。

[0085] 第一存储器1012可用于存储软件程序以及单元。具体的，第一存储器1012可存储第一操作系统10121、至少一个功能所需的第一应用程序单元10122。第一操作系统10121可以是实时操作系统(Real Time eXecutive，RTX)、LINUX、UNIX、WINDOWS或OS X之类的操作系统。

[0086] 第一处理器1013包括一个或者一个以上处理核心。第一处理器1013通过运行软件程序以及单元，从而执行以下传输数据的操作的指令：

[0087] 接收第一设备的通信消息，所述通信消息中携带有密钥标识、加密数据和第一消息验证码，其中，所述加密数据是通过所述密钥标识对应的密钥对待发送的目标数据加密得到的数据，所述第一消息验证码是根据所述密钥、所述目标数据和预设的辅助验证信息生成的验证码；

[0088] 获取所述密钥标识对应的密钥和所述辅助验证信息；

[0089] 根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证。

[0090] 在一种可能的实现方式中，所述获取所述密钥标识对应的密钥和所述辅助验证信息，包括：

[0091] 向认证服务器发送密钥获取请求，所述密钥获取请求中携带有所述密钥标识和本地的标识；

[0092] 接收所述认证服务器发送的第一响应消息，所述第一响应消息中携带有所述密钥标识对应的密钥和所述辅助验证信息。

[0093] 在一种可能的实现方式中，所述根据所述密钥、所述第一消息验证码和所述辅助验证信息对所述加密数据进行验证，包括：

[0094] 基于所述密钥对所述加密数据进行解密；

[0095] 根据所述密钥、所述辅助验证信息和解密得到的数据生成第二消息验证码，如果所述第一消息验证码与所述第二消息验证码不匹配，则所述加密数据验证未通过。

[0096] 在一种可能的实现方式中，所述方法还包括：

[0097] 如果验证未通过，则向所述认证服务器发送数据异常通知。

[0098] 在一种可能的实现方式中，所述接收第一设备发送的通信消息之前，还包括：

[0099] 向所述第一设备发送数据获取请求，以使所述第一设备发送所述通信消息。

[0100] 在一种可能的实现方式中，所述接收第一设备的通信消息，包括：

[0101] 接收第三设备转发的第一设备的通信消息，所述第三设备是接收所述目标数据的传输路中的其他接收方。

[0102] 参见图3，其示出了本发明示例性实施例提供的一种认证服务器，该认证服务器20包括第二收发器2011和第二存储器2012，该认证服务器还可以包括第二处理器2013和第二网络接口2014。其中，第二存储器2012和第二网络接口2014分别与第二处理器2013连接；第二存储器2012用于存储程序代码，程序代码包括计算机操作指令，第二处理器2013和第二收发器2011用于执行第二存储器2012中存储的程序代码，用于实现传输数据的相关处理，并可以通过第二网络接口2014与网络设备进行交互。

[0103] 其中，第二存储器2012与第二网络接口2014分别与第二处理器2013和第二收发器2011相连，第二收发器2011可以包括第二发射器和第二接收器。

[0104] 第二存储器2012可用于存储软件程序以及单元。具体的，第二存储器2012可存储第二操作系统20121、至少一个功能所需的第二应用程序单元20122。第二操作系统20121可以是实时操作系统(Real Time eXecutive，RTX)、LINUX、UNIX、WINDOWS或OS X之类的操作系统。

[0105] 第二处理器2013包括一个或者一个以上处理核心。第二处理器2013通过运行软件程序以及单元，从而执行以下传输数据的操作的指令：

[0106] 接收第二设备发送的密钥获取请求，所述密钥获取请求中携带有密钥标识和所述第二设备的标识；

[0107] 获取预先存储的所述密钥标识对应的密钥，以及所述第二设备的标识对应的辅助验证信息；

[0108] 向所述第二设备发送第一响应消息，所述第一响应消息中携带有所述密钥和所述辅助验证信息，以使所述第二设备对接收到的加密数据进行验证。

[0109] 在一种可能的实现方式中，所述方法还包括：

[0110] 接收第一设备发送的密钥注册请求，所述密钥注册请求中携带有所述目标数据的接收方的标识和所述第一设备的标识；

[0111] 根据所述第一设备的标识和所述接收方的标识，获取各接收方对应的传输路径；

[0112] 如果所述各接收方中的所述第二设备对应的传输路径中，存在所述目标数据的其他接收方，则生成所述第二设备对应的辅助验证信息；

[0113] 向所述第一设备发送第二响应消息，所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

[0114] 在一种可能的实现方式中，所述根据所述第一设备的标识和所述目标数据的接收方的标识，获取各接收方对应的传输路径，包括：

[0115] 根据所述第一设备的标识和所述目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径；或者，

[0116] 根据所述第一设备的标识和所述目标数据的接收方的标识，生成各接收方对应的传输路径。

[0117] 在一种可能的实现方式中，所述方法还包括：

[0118] 接收所述第二设备发送的数据异常通知；

[0119] 根据所述第二设备对应的传输路径，以及所述传输路径中的其他接收方，确定所

述传输路径中的异常设备，向所述第一设备发送对应所述异常设备的告警消息。

[0120] 参见图4，其示出了本发明示例性实施例提供的一种用于发送通信消息的第一设备，该第一设备30包括第三收发器3011和第三存储器3012，该第一设备还可以包括第三处理器3013和第三网络接口3014。其中，第三存储器3012和第三网络接口3014分别与第三处理器3013连接；第三存储器3012用于存储程序代码，程序代码包括计算机操作指令，第三处理器3013和第三收发器3011用于执行第三存储器3012中存储的程序代码，用于实现传输数据的相关处理，并可以通过第三网络接口3014与第一设备和认证服务进行交互。

[0121] 其中，第三存储器3012与第三网络接口3014分别与第三处理器3013和第三收发器3011相连，第三收发器3011可以包括第三发射器和第三接收器。

[0122] 第三存储器3012可用于存储软件程序以及单元。具体的，第三存储器3012可存储第三操作系统30121、至少一个功能所需的第三应用程序单元30122。第三操作系统30121可以是实时操作系统(Real Time eXecutive，RTX)、LINUX、UNIX、WINDOWS或OS X之类的操作系统。

[0123] 第三处理器3013包括一个或者一个以上处理核心。第三处理器3013通过运行软件程序以及单元，从而执行以下传输数据的操作的指令：

[0124] 获取待发送的目标数据；

[0125] 基于预设的密钥对所述目标数据进行加密，得到加密数据，并根据接收所述目标数据的第二设备对应的预先存储的辅助验证信息、所述密钥和所述目标数据生成第一消息验证码，其中，所述第二设备对应的传输路径中存在所述目标数据的其他接收方；

[0126] 向所述第二设备发送通信消息，所述通信消息中携带有所述密钥的密钥标识、所述加密数据和所述第一消息验证码。

[0127] 在一种可能的实现方式中，所述方法还包括：

[0128] 向认证服务器发送密钥注册请求，所述密钥注册请求中携带有所述目标数据的接收方的标识和本地的标识；

[0129] 接收所述认证服务器发送的第二响应消息，所述第二响应消息中携带有所述第二设备对应的辅助验证信息。

[0130] 在一种可能的实现方式中，所述获取待发送的目标数据之前，还包括：

[0131] 当接收到所述第二设备发送的数据获取请求时，执行获取待发送的目标数据的步骤。

[0132] 在一种可能的实现方式中，所述向所述第二设备发送通信消息，包括：

[0133] 向第三设备发送所述通信消息，以使所述第三设备将所述通信消息转发给所述第二设备，所述第三设备是所述第二设备对应的传输路径中的其他接收方。

[0134] 为了提高传输数据的安全性和可靠性，本实施例提供了一种传输数据的方法，该方法可以由上述图2中的第二设备、上述图3中的认证服务器和上述图4中的第一设备共同实现。

[0135] 首先，在传输数据之前，第一设备需要先在认证服务器中进行密钥注册，认证服务器则会进行执行密钥创建操作并向第一设备返回密钥标识，以便在后续传输数据的过程中为各设备(比如数据接收方)发放该发送方的密钥。如图5所示，密钥注册的处理流程可以包括以下几个步骤：

[0136] 步骤501,第一设备向认证服务器发送密钥注册请求。

[0137] 实施中,当第一设备需要注册密钥时,第一设备可以获取预先存储的接收方的标识和本地的标识,进而向认证服务器发送密钥注册请求,密钥注册请求中可以携带有目标数据的接收方的标识和本地的标识。目标数据的接收方可以由技术人员预先配置,也可以是第一设备根据业务需要确定。对于接收方为多个的情况,接收方的标识可以以接收方列表的形式携带在密钥注册请求中。不同的目标数据对应的接收方可以是相同的,也可以是不同的。另外,第一设备可以达到预设周期时,向认证服务器发送密钥注册请求;也可以在接收到密钥注册指令后,向认证服务器发送密钥注册请求。

[0138] 传输数据的过程中所使用的密钥还可以由第一设备生成,相应的,密钥注册请求中还可以携带第一设备生成的密钥,该密钥可以是对称密钥。另外,密钥注册请求中还可以携带有密钥使用方式的标识。例如,该密钥注册请求可以如下:

[0139] POST http://m2m.maf.com/tef0001HTTP/1.1

[0140] X-M2M-Origin:http://m2m.things.com/cse001/ae001

[0141] Content-type:application/onem2m-resource+json

[0142] {“ResourceType”:“symmKeyReg”,

[0143] “symmKeyReg.targetIDs”:“/cse002,/cse000/ae002”,

[0144] “symmKeyReg.SUID”:“34”,

[0145] “symmKeyReg.keyValue”:“CDExedSGEdXGj142”}

[0146] 其中,http://m2m.maf.com/tef0001表示MAF(即认证服务器)的统一资源定位器(Uniform Resoure Locator,URL),也就是密钥想要注册的父节点,其中tef001为MAF的身份标识号码(Identity,ID);http://m2m.things.com/cse001/ae001表示ASN-AE(即发送方)的URL,其中/cse001为ASN-CSE的ID,/cse001/ae001为ASN-AE的ID;“ResourceType”:“symmKeyReg”,表示要在tef001下创建一个symmKeyReg资源,“symmKeyReg.targetIDs”:“/cse002,/cse000/ae002”为接收方列表,接收方列表中包含接收该发送方的数据的设备的标识,这些设备可以获取该发送方的密钥,本示例中,密钥可以被标识为/cse002和/cse000/ae002的设备获取,其中/cse002为MN-CSE(即网关设备)的ID,/cse000/ae002为IN-AE的ID(即业务服务器的标识);“symmKeyReg.SUID”:“34”表示密钥使用方式,当值为34时,表示该密钥可以用于多跳传输的数据加密;“symmKeyReg.keyValue”:“CDExedSGEdXGj142”表示需要注册的密钥的值为“CDExedSGEdXGj142”。

[0147] 或者,数据加密传输的过程中所使用的密钥也可以由认证服务器来生成,相应的,密钥注册请求则不需要携带密钥。例如,第一设备可以通知认证服务器生成密钥,认证服务器则可以使用TLS Key Export(IETF RFC 5705)算法生成密钥,并可以将该密钥发送给第一设备,以便第一设备基于该密钥,对目标数据进行加密处理。

[0148] 步骤502,认证服务器接收第一设备发送的密钥注册请求,密钥注册请求中携带有目标数据的接收方的标识和第一设备的标识。

[0149] 步骤503,认证服务器根据第一设备的标识和接收方的标识,获取各接收方对应的传输路径。

[0150] 在实施中,认证服务器接收到密钥注册请求后,可以创建该密钥注册请求对应的symmKeyReg资源,并为该symmKeyReg资源分配资源ID,比如skr001;认证服务器还可以为该

密钥分配密钥标识，即KcID，将该密钥注册请求中的密钥和接收方列表，与该密钥标识进行对应的存储，建立密钥标识与密钥的对应关系，以及密钥标识与接收方列表的对应关系。认证服务器可以根据接收方列表和密钥使用方式，判定该密钥是用于多数据接收方的多跳数据传输。认证服务器还可以根据第一设备的标识和接收方的标识，获取各接收方对应的传输路径，获取方式可以多样化，本实施例提供了两种可行的处理方式：

[0151] 方式一、认证服务器根据第一设备的标识和目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径。

[0152] 在实施中，技术人员可以预先配置各设备之间的传输路径，每个传输路径可以包括该传输路中的发送方的标识、需要经过的中间设备的标识和接收方的标识。例如，网络系统中可以包括业务服务器003、网关设备002和家庭中安装的摄像头001，摄像头向业务服务器发送数据的传输路径为001,002,003；摄像头向网关设备发送数据的传输路径为001,002。认证服务器可以根据第一设备的标识，以及各接收方的标识，在预设的传输路径中分别查询各接收方对应的传输路径。上述传输路径可以存储在认证服务器中，由认证服务器进行查询；或者，上述传输路径可以存储在基础设施节点中，向基础设施节点进行查询，然后将查询到的结果发送给认证服务器。对于从基础设施节点查询各接收方对应的传输路径的情况，具体的处理过程可以包括以下几个步骤：

[0153] 步骤1，认证服务器向基础设施节点发送传输路径查询请求。

[0154] 在实施中，传输路径查询请求中可以携带有第一设备的标识和接收方列表，还需携带有传输路径请求指示。例如，传输路径查询请求可以如下：

[0155] GET http://m2m.things.com/cse000/dataTransPath HTTP/1.1

[0156] X-M2M-Origin:http://m2m.maf.com/tef001

[0157] Content-type:application/onem2m-resource+json

[0158] {“symmKeyReg.resourceID”:“skr001”；

[0159] “sourceID”:“/cse001/ae001”,

[0160] “targetIDs”:“/cse002,/cse000/ae002”,

[0161] “dataTransPathIndicator”:“1”}

[0162] 其中，http://m2m.in.com/cse000/dataTransPath表示传输路径查询请求的虚资源URL，cse000为IN-CSE的ID(即基础设施节点的ID)，对于该虚资源的访问，会触发基础设施节点执行数据传输路径检索；“symmKeyReg.resourceID”:“skr001”表示该传输路径查询请求是针对skr001资源中注册Kc；“sourceIDs”:“/cse001/ae001”表示该传输路径的发送方为ASN-AE，“targetIDs”:“/cse002,/cse000/ae002”表示数据传输路径的接收方为MN-CSE和IN-AE，“dataTransPathIndicator”:“1”为传输路径请求指示。

[0163] 步骤2，基础设施节点根据第一设备的标识和目标数据的接收方的标识，在预设的传输路径中查询各接收方对应的传输路径。

[0164] 在实施中，基础设施节点中可以预先存储各设备之间的传输路径，基础设施节点接收到传输路径查询请求后，可以对该传输路径查询请求进行解析，获取第一设备的标识，以及各接收方的标识，然后根据第一设备的标识(可称为第一标识)，以及各接收方的标识(可称为第二标识)，在预设的传输路径中查询以发送方的标识为第一标识，且接收方的标识为第二标识的传输路，从而得到各接收方对应的传输路径。

[0165] 步骤3,基础设施节点将各接收方对应的传输路径发送给认证服务器。

[0166] 在实施中,基础设施节点查询到各接收方对应的传输路径后,可以将各接收方对应的传输路径分别发送给认证服务器,也可以将各接收方对应的传输路径携带在一个响应消息(可称为成功响应)中,发送给认证服务器。例如,该成功响应可以如下:

[0167] HTTP/1.1 200OK

[0168] Content-type:application/onem2m-resource+json

[0169] {“symmKeyReg.resourceID”:“skr001”;

[0170] “dataTransPathList”:{

[0171] “dataTransPath”:“/cse001/ae001,/cse001,/cse002”

[0172] “dataTransPath”:“/cse001/ae001,/cse001,/cse002,/cse000,/cse000/ae002”}}

[0173] 其中,“symmKeyReg.resourceID”:“skr001”;表示数据传输路径主要是针对skr001资源对应的注册Kc,“dataTransPath”:“/cse001/ae001,/cse001,/cse002”表示ASN-AE到MN-CSE的传输路径,“dataTransPath”:“/cse001/ae001,/cse001,/cse002,/cse000,/cse000/ae002”表示ASN-AE到IN-AE的传输路径。

[0174] 步骤4,认证服务器接收基础设施节点发送的各接收方对应的传输路径。

[0175] 方式二、认证服务器根据第一设备的标识和目标数据的接收方的标识,生成各接收方对应的传输路径。

[0176] 在实施中,认证服务器也可以在接收到密钥注册请求后,根据预设的传输路径生成算法、第一设备的标识和目标数据的各接收方的标识,分别生成各接收方对应的传输路径。该传输路径生成算法可以存储在认证服务器中,由认证服务器生成传输路径;或者,该传输路径生成算法也可以存储在基础设施节点中,由基础设施节点生成传输路径,然后将生成的传输路径发送给认证服务器。

[0177] 步骤504,如果接收方中的第二设备对应的传输路径中,存在目标数据的其他接收方,则认证服务器生成第二设备对应的辅助验证信息。

[0178] 在实施中,对于任一接收方,认证服务器根据获取到的传输路径,判断该传输路径所包含的中间设备的标识中,是否包含上述接收方列表中的标识,如果包含,则判定该接收方对应的传输路径中,存在目标数据的其他接收方,然后可以生成该接收方(即第二设备)对应的辅助验证信息(即ExtAuthenData);如果不包含,则判定该接收方对应的传输路径中,不存在目标数据的其他接收方,不生成辅助验证信息。例如,IN-AE的数据传输路径中“/cse001/ae001,/cse001,/cse002,/cse000,/cse000/ae002”包含拥有密钥的接收方MN-CSE(/cse002),则认证服务器可以为IN-AE分配附加认证数据ExtAuthenData:CHMEGKSjMX23J。

[0179] 其中,第二设备的数目可以是一个,也可以是多个。如果存在多个第二设备的情况,认证服务器可以分别生成每个第二设备对应的辅助验证信息,然后将设备的标识与对应的辅助验证信息进行存储,建立设备的标识和辅助验证信息的对应关系。

[0180] 步骤505,认证服务器向第一设备发送第二响应消息。

[0181] 在实施中,认证服务器生成第二设备对应的辅助验证信息后,可以向第一设备发送第二响应消息,第二响应消息中可以携带有每个第二设备对应的辅助验证信息,还可以携带有密钥标识和资源ID和接收方列表等信息。例如,第二响应消息可以如下:

[0182] HTTP/1.1 200OK

[0183] Content-type:application/onem2m-resource+json

[0184] {“symmKeyReg.kcIdentity”:“kc001”;

[0185] “symmKeyReg.targetIDs”:“/cse002,/cse000/ae002”,

[0186] “symmKeyReg.extAuthenDataList”:“/cse000/ae002,CHMEGKSjMX23J”}

[0187] 其中,“symmKeyReg.kcIdentity”:“kc001”表示KcID为kc001,“symmKeyReg.extAuthenDataList”:“/cse000/ae002,CHMEGKSjMX23J”是表示分配给IN-AE的辅助验证信息为CHMEGKSjMX23J的映射对,对于第二设备为多个的情况,那么“symmKeyReg.extAuthenDataList”可以赋值为多个映射对。

[0188] 步骤506,第一设备接收认证服务器发送的第二响应消息。

[0189] 在实施中,第一设备可以接收认证服务器发送的第二响应消息,然后对第二响应消息进行解析,获取第二设备对应的辅助验证信息,然后可以将第二设备的标识与该辅助验证信息进行对应的存储,建立设备的标识和辅助验证信息的对应关系,以便在向第二设备发送通信消息时,基于该辅助验证信息,生成第二设备对应的消息验证码(即第一消息验证码)。

[0190] 第一设备在认证服务器中成功注册密钥后,可以向接收方发送需要传输的目标数据,本实施例以第一设备通过第三设备将通信消息转发给第二设备,且第三设备被非法入侵为例,对上述传输数据方法进行说明,其中,第二设备和第三设备均是目标数据的接收方,均可以获得第一设备的密钥,第三设备设是第二设备对应的传输路径中的任一中间设备。如图6所示,该处理流程可以如下:

[0191] 步骤601,第一设备获取待发送的目标数据。

[0192] 在实施中,目标数据可以是第一设备检测到的数据,可以是其他设备向第一设备发送的数据,还可以是第一设备中预先存储的数据。相应的,第一设备获取目标数据的方式可以为,第一设备获取检测到的目标数据,或者,第一设备接收其他设备发送的目标数据,或者,第一设备获取预先存储的目标数据。例如,第一设备可以为智能摄像头,智能摄像头可以实时进行图像检测,将检测到的图像数据作为待发送的目标数据。

[0193] 步骤602,第一设备使用已注册的密钥对目标数据进行加密,得到加密数据,并根据接收目标数据的第二设备对应的由认证服务器分配的辅助验证信息、密钥和目标数据生成第一消息验证码。

[0194] 其中,第二设备对应的传输路径中可以存在目标数据的其他接收方。

[0195] 在实施中,第一设备在向接收方发送目标数据时,可以使用已注册的密钥和加密算法对目标数据(可称为Data)进行加密,得到加密数据(可称为Data-Encry),第一设备还可以判断本地存储的设备的标识和辅助验证信息的对应关系中,是否存在该接收方的标识。如果存在,则可以获取该接收方(即第二设备)的标识对应的辅助验证信息,然后可以在目标数据的后面添加该辅助验证信息(可称为Data’),然后根据Data’、密钥和预设的加密算法生成第一消息验证码。该加密算法可以是任意加密算法,例如,可以基于消息完整性编码(Message Integrity Code,MIC)进行加密,该加密算法是基于密钥、Hash函数和Data’来计算消息验证码的。第一设备可以根据加密数据和第一消息验证码,生成第二设备对应的通信消息,该通信消息中还可以携带有第一设备的密钥的密钥标识、加密算法的标识以及

第二设备的标识。其中，生成加密数据的加密算法，与生成消息验证码的加密算法可以是不同的。

[0196] 如果第一设备判定设备的标识和辅助验证信息的对应关系中，不存在该接收方的标识，则可以不执行生成消息验证码的处理。第一设备可以根据加密数据生成该接收方对应的通信消息，该通信消息中还可以携带有第一设备的密钥的密钥标识和加密算法的标识。对于不同的接收方，第一设备可以分别生成每个接收方对应的通信消息，然后分别发送给每个接收方，下文中的通信消息均指代第一设备发送给第二设备的通信消息。

[0197] 其中，上述通信消息的形式可以是多种多样的，例如，该通信消息可以是只用于发送上述数据的通信消息；或者，上述数据也可以携带其他通信消息中(比如Create/Update/Notify或响应消息等)，直接作为该消息中的某个资源的属性赋值，或者包含在某个oneM2M的参数中进行发送。

[0198] 步骤603，第一设备向第三设备发送通信消息。

[0199] 其中，该通信消息中可以携带有该密钥的密钥标识、加密数据和第一消息验证码，且该通信消息的目的地址为第二设备的地址。

[0200] 在实施中，第一设备生成第二设备对应的通信消息后，可以基于预设的传输策略，确定转发该通信消息的中间设备(即第三设备)，然后向第三设备发送该通信消息，以使第三设备将该通信消息转发给第二设备。

[0201] 步骤604，第三设备接收第一设备的通信消息。

[0202] 其中，该通信消息中可以携带有密钥标识、加密数据和第一消息验证码，该加密数据是通过密钥标识对应的密钥对待发送的目标数据加密得到的数据，该第一消息验证码是根据密钥、目标数据和预设的辅助验证信息生成的验证码。

[0203] 步骤605，第三设备向认证服务器发送密钥获取请求。

[0204] 在实施中，第三设备可以对第一设备发送给自身的通信消息进行解析，获取第一设备对应的密钥标识，或者，也可以对该通信消息进行解析，获取第一设备对应的密钥标识。第三设备可以根据该密钥标识，获取本地预先存储的密钥，或者，第三设备也可以向认证服务器发送密钥获取请求，以获取该密钥。密钥获取请求中可以携带有密钥标识和第三设备的标识。该密钥获取请求可以如下所示：

[0205] GET http://m2m.maf.com/tef001/kc001/keyValue HTTP/1.1

[0206] X-M2M-Origin:http://m2m.things.com/cse002

[0207] Content-type:application/onem2m-resource+json

[0208] 其中，http://m2m.maf.com/tef001/kc001/keyValue表示要请求的密钥标识为kc001。http://m2m.things.com/cse002表示该密钥获取请求的发送方为MN(即第三设备)的标识为cse002。

[0209] 步骤606，认证服务器接收第三设备发送的密钥获取请求。

[0210] 步骤607，认证服务器获取预先存储的密钥标识对应的密钥。

[0211] 在实施中，认证服务器接收第三设备发送的密钥获取请求后，可以对该密钥获取请求进行解析，获取其中携带的密钥标识和第三设备的标识，然后可以根据预先存储的密钥标识与接收方列表的对应关系，以及接收到的密钥标识，确定对应的接收方列表，然后判断该接收方列表中是否包含第三设备的标识，如果包含，则说明第三设备可以获取该密钥，

认证服务器可以根据预先存储的密钥标识与密钥的对应关系，确定接收到的密钥标识对应的密钥；如果不包含，则可以不进行处理，并可以向第三设备反馈请求失败的响应消息。例如，MAF根据密钥的标识kc001查找到其对应的接收方列表“/cse002,/cse000/ae002”，可以判断第三设备MN-CSE的标识/cse002在该接收方列表中，即MN-CSE具有获得Kc的权限。

[0212] 步骤608，认证服务器向第三设备发送第三响应消息。

[0213] 在实施中，第三响应消息中可以携带有该密钥标识对应的密钥，该第三响应消息可以如下所示：

[0214] HTTP/1.1 200OK

[0215] Content-type:application/onem2m-resource+json

[0216] {“symmKeyReg.kcIdentity”:“kc001”；

[0217] “symmKeyReg.keyValue”:“CDExedSGEdXGj142”}

[0218] 其中，“CDExedSGEdXGj142”为密钥的值，“kc001”为密钥标识。

[0219] 步骤609，第三设备将通信消息发送给第二设备。

[0220] 在实施中，第三设备在正常的状态下，不会对该通信消息进行解析，而是在接收到该通信消息后，根据该通信消息中的目的地址，将该通信消息直接转发给第二设备。第三设备被入侵后，不法分子可以通过第三设备，基于接收到的密钥和预设的加密算法，对通信消息中的加密数据进行解析，得到目标数据的数据原文，然后对该数据原文(Data)进行篡改(篡改后的数据可称为Data”)，通过该加密算法和密钥对Data”进行加密，将该加密数据携带在该通信消息中，将该通信消息转发给第二设备。

[0221] 步骤610，第二设备接收第三设备转发的通信消息。

[0222] 其中，该通信消息中可以携带有密钥标识、加密数据和第一消息验证码，还可以携带有加密算法的标识以及第二设备的标识，且该通信消息的目的地址为第二设备的地址。

[0223] 步骤611，第二设备向认证服务器发送密钥获取请求。

[0224] 在实施中，该密钥获取请求中携带有第二设备解析得到的密钥标识，以及第二设备的标识，该密钥获取请求可以参照上述605中的示例，不再赘述。

[0225] 步骤612，认证服务器接收第二设备发送的密钥获取请求。

[0226] 步骤613，认证服务器获取预先存储的密钥标识对应的密钥，以及第二设备的标识对应的辅助验证信息。

[0227] 在实施中，认证服务器接收第二设备发送的密钥获取请求后，可以对该密钥获取请求进行解析，获取其中携带的密钥标识和第二设备的标识，然后可以根据预先存储的密钥标识与接收方列表的对应关系，以及接收到的密钥标识，确定对应的接收方列表，然后判断该接收方列表中是否包含第二设备的标识，如果包含，则说明第二设备可以获取该密钥，认证服务器可以根据预先存储的密钥标识与密钥的对应关系，确定接收到的密钥标识对应的密钥；如果不包含，则可以不进行处理，并可以向第二设备反馈请求失败的响应消息。另外，认证服务器还可以根据预先存储的设备的标识和辅助验证信息的对应关系，以及第二设备的标识，获取第二设备对应的辅助验证信息。例如，MAF根据kc001对应symmKeyReg查找到其存储的targetIDs为“/cse002,/cse000/ae002”，可以判定第二设备IN-AE(/cse000/ae002)具有获得Kc的权限，并且该IN-AE被分配了辅助验证信息ExtAuthenData。

[0228] 步骤614，认证服务器向第二设备发送第一响应消息。

[0229] 在实施中，第一响应消息中可以携带有密钥和辅助验证信息，该第一响应消息可以如下所示：

[0230] HTTP/1.1 200OK

[0231] Content-type:application/onem2m-resource+json

[0232] {“symmKeyReg.kcIdentity”:“kc001”，

[0233] “symmKeyReg.keyValue”:“CDExedSGEdXGj142”，

[0234] “symmKeyReg.extAuthenDataList”:“/cse000/ae002,CHMEGKSjMX23J”}

[0235] 其中，“CDExedSGEdXGj142”为密钥的值，“kc001”为密钥标识。“CHMEGKSjMX23J”为第二设备对应的辅助验证信息。

[0236] 步骤615，第二设备接收认证服务器发送的第一响应消息。

[0237] 在实施中，第二设备接收到第一响应消息后，可以对第一响应消息进行解析，获取第一响应消息中的密钥和辅助验证信息。

[0238] 步骤616，第二设备根据密钥、第一消息验证码和辅助验证信息对加密数据进行验证。

[0239] 在实施中，第二设备可以根据该密钥对加密数据进行解密，得到解密后的数据，然后可以解密后的数据、辅助验证信息、该密钥和预设的加密算法，生成消息验证码(即第二消息验证码)，然后可以判定第二消息验证码是否与第一消息验证码匹配(比如是否相同)，如果第二消息验证码与第一消息匹配，则可以判定验证通过，该加密数据未被篡改；如果第二消息验证码与第一消息不匹配，则可以判定验证未通过，该加密数据异常，可能被篡改，然后可以执行步骤616。

[0240] 步骤617，第二设备向认证服务器发送数据异常通知。

[0241] 在实施中，如果验证未通过，则第二设备可以向认证服务器发送数据异常通知，该数据异常通知中可以携带有密钥标识和第二设备的标识，以便认证服务器可以根据该密钥标识对应的接收方列表，确定可能被篡改的接收方。该数据异常通知可以如下所示：

[0242] POST http://m2m.maf.com/tef001/HTTP/1.1

[0243] X-M2M-Origin:http://m2m.things.com/cse000/ae002

[0244] Content-type:application/onem2m-resource+json

[0245] {“symmKeyReg.kcIdentity”:“kc001”，

[0246] “kcAbnormalIndicator”:“1”}

[0247] 其中“symmKeyReg.kcIdentity”:“kc001”表示该数据异常通知是针对密钥标识为kc001的密钥，“kcAbnormalIndicator”:“1”表示该密钥出现异常现象。

[0248] 步骤618，认证服务器接收第二设备发送的数据异常通知。

[0249] 步骤619，认证服务器根据第二设备对应的传输路径，以及传输路径中的其他接收方，确定传输路径中的异常设备，向第一设备发送对应异常设备的告警消息。

[0250] 在实施中，认证服务器可以对该数据异常通知进行解析，获取其中的密钥标识和第二设备的标识，认证服务器可以根据预先获取到的第二设备对应的传输路径，判断第二设备的传输路径中存在其他能够获得该密钥标识对应的密钥的中间设备，说明可能是由于该中间设备受到攻击，导致数据发生异常，该密钥就可能被不法分子获得。认证服务器可以注销该密钥，并删除该密钥对应的symmKeyReg资源。认证服务器还可以获取该中间设备(即

异常设备)的标识,然后向第一设备发送对应异常设备的告警消息,该告警消息中可以携带有该异常设备的标识、密钥标识和密钥注销指示,该告警消息可以如下所示:

[0251] POST http://m2m.things.com/cse001/ae001/HTTP/1.1

[0252] X-M2M-Origin:http://m2m.maf.com/tef001

[0253] Content-type:application/onem2m-resource+json

[0254] {“symmKeyReg.kcIdentity”:“kc001”,

[0255] “symmKeyReg.targetAbnormalId”:“/cse002”,

[0256] “kcDeRegistIndicator”:“1”}

[0257] 其中“symmKeyReg.kcIdentity”:“kc001”表示该告警消息针对密钥标识为kc001的密钥,“symmKeyReg.targetAbnormalId”:“/cse002”表示第三设备MN-CSE存在异常的可能,“kcDeRegistIndicator”:“1”表示该密钥已被注销。

[0258] 如图7所示,本实施例还提供了一种传输数据的方法,该方法中,第二设备可以主动获取第一设备的目标数据。第二设备可以直接向第一设备请求目标数据,第一设备在接收到数据获取请求后,生成第二设备对应的通信消息,将该通信消息发送给第二设备。或者,第一设备也可以预先生成各接收方对应的通信消息,然后将该通信消息存储在其他设备(可称为第四设备)中,第二设备从第四设备中获取通信消息。本实施例以第二设备直接向第一设备请求目标数据为例进行说明,具体的处理流程可以如下:

[0259] 步骤701,第二设备向第一设备发送数据获取请求。

[0260] 步骤702,第一设备接收第二设备发送的数据获取请求。

[0261] 步骤703,第一设备获取待发送的目标数据。

[0262] 本步骤的具体处理过程可以参照上述步骤601中的相关说明。

[0263] 步骤704,第一设备基于预设的密钥对目标数据进行加密,得到加密数据,并根据接收目标数据的第二设备对应的预先存储的辅助验证信息、密钥和目标数据生成第一消息验证码。

[0264] 本步骤的具体处理过程可以参照上述步骤602中的相关说明。

[0265] 步骤705,第一设备向第三设备发送通信消息。

[0266] 本步骤的具体处理过程可以参照上述步骤603中的相关说明。

[0267] 步骤706,第三设备接收第一设备的通信消息。

[0268] 本步骤的具体处理过程可以参照上述步骤604中的相关说明。

[0269] 步骤707,第三设备向认证服务器发送密钥获取请求。

[0270] 本步骤的具体处理过程可以参照上述步骤605中的相关说明。

[0271] 步骤708,认证服务器接收第三设备发送的密钥获取请求。

[0272] 本步骤的具体处理过程可以参照上述步骤606中的相关说明。

[0273] 步骤709,认证服务器获取预先存储的密钥标识对应的密钥。

[0274] 本步骤的具体处理过程可以参照上述步骤607中的相关说明。

[0275] 步骤710,认证服务器向第三设备发送第三响应消息。

[0276] 本步骤的具体处理过程可以参照上述步骤608中的相关说明。

[0277] 步骤711,第三设备对将通信消息发送给第二设备。

[0278] 本步骤的具体处理过程可以参照上述步骤609中的相关说明。

[0279] 步骤712，第二设备接收第一设备的通信消息。

[0280] 本步骤的具体处理过程可以参照上述步骤610中的相关说明。

[0281] 步骤713，第二设备向认证服务器发送密钥获取请求。

[0282] 本步骤的具体处理过程可以参照上述步骤611中的相关说明。

[0283] 步骤714，认证服务器接收第二设备发送的密钥获取请求。

[0284] 本步骤的具体处理过程可以参照上述步骤612中的相关说明。

[0285] 步骤715，认证服务器获取预先存储的密钥标识对应的密钥，以及第二设备的标识对应的辅助验证信息。

[0286] 本步骤的具体处理过程可以参照上述步骤613中的相关说明。

[0287] 步骤716，认证服务器向第二设备发送第一响应消息。

[0288] 本步骤的具体处理过程可以参照上述步骤614中的相关说明。

[0289] 步骤717，第二设备接收认证服务器发送的第一响应消息。

[0290] 本步骤的具体处理过程可以参照上述步骤615中的相关说明。

[0291] 步骤718，第二设备根据密钥、第一消息验证码和辅助验证信息对加密数据进行验证。

[0292] 本步骤的具体处理过程可以参照上述步骤616中的相关说明。

[0293] 步骤719，第二设备向认证服务器发送数据异常通知。

[0294] 本步骤的具体处理过程可以参照上述步骤617中的相关说明。

[0295] 步骤720，认证服务器接收第二设备发送的数据异常通知。

[0296] 本步骤的具体处理过程可以参照上述步骤618中的相关说明。

[0297] 步骤721，认证服务器根据第二设备对应的传输路径，以及传输路径中的其他接收方，确定传输路径中的异常设备，向第一设备发送对应异常设备的告警消息。

[0298] 本步骤的具体处理过程可以参照上述步骤619中的相关说明。

[0299] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0300] 图8是本发明实施例提供的一种传输数据的装置的结构方框图，该装置可以通过软件、硬件或者两者的结合实现成为第二设备的部分或者全部。

[0301] 该装置包括：收发单元810、获取单元820和处理单元830。

[0302] 收发单元810用于执行上述实施例中的步骤610、步骤617、步骤701、步骤721和步骤719及其可选方案。

[0303] 获取单元820用于执行上述实施例中的步骤611、步骤617、步骤713和、步骤717及其可选方案。

[0304] 处理单元830用于执行上述实施例中的步骤616和步骤718及其可选方案。

[0305] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0306] 图9是本发明实施例提供的一种传输数据的装置的结构方框图，该装置可以通过软件、硬件或者两者的结合实现成为认证服务器的部分或者全部。

[0307] 该装置包括：收发单元910和获取单元920。

[0308] 收发单元910用于执行上述实施例中的步骤502、步骤505、步骤606、步骤608、步骤612、步骤614、步骤618、步骤619、步骤708、步骤710、步骤714、步骤716、步骤720和步骤721及其可选方案。

[0309] 获取单元920用于执行上述实施例中的步骤607及其可选方案。

[0310] 该装置还可以包括处理单元，处理单元用于执行上述实施例中的步骤504及其可选方案。

[0311] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0312] 图10是本发明实施例提供的一种传输数据的装置的结构方框图，该装置可以通过软件、硬件或者两者的结合实现成为第一设备的部分或者全部。

[0313] 该装置包括：获取单元1010、处理单元1020和收发单元1030。

[0314] 获取单元1010用于执行上述实施例中的步骤601和步骤703及其可选方案。

[0315] 处理单元1020用于执行上述实施例中的步骤602和步骤704及其可选方案。

[0316] 收发单元1030用于执行上述实施例中的步骤501、步骤506、步骤603、步骤702和步骤705及其可选方案。

[0317] 本公开实施例中，接收方接收第一设备发送的通信消息，该通信消息中携带有密钥标识、加密数据和第一消息验证码，接收方可以获取该密钥标识对应的密钥和辅助验证信息，根据该密钥、第一消息验证码和辅助验证信息对加密数据进行验证，从而判断加密数据是否篡改，提高了传输数据的可靠性。

[0318] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0319] 以上所述仅为本公开的可选实施例，并不用以限制本公开，凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

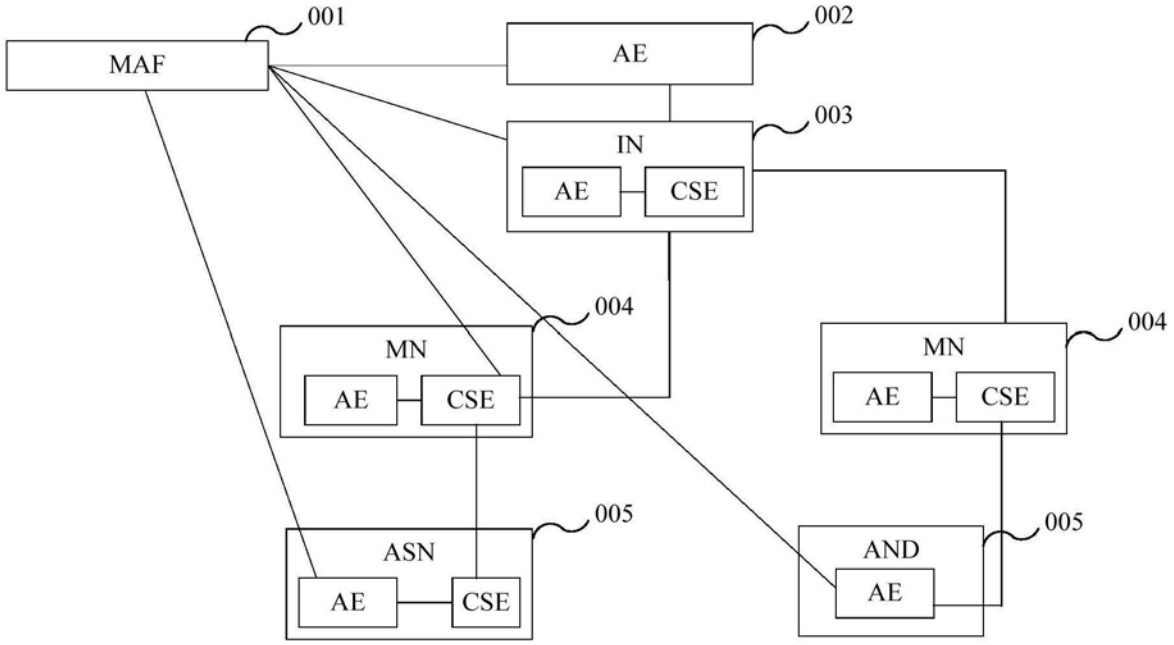

001
MAF
002
AE
003
IN
AE
CSE
004
MN
AE
CSE
004
MN
AE
CSE
005
ASN
AE
CSE
005
AND
AE

图1

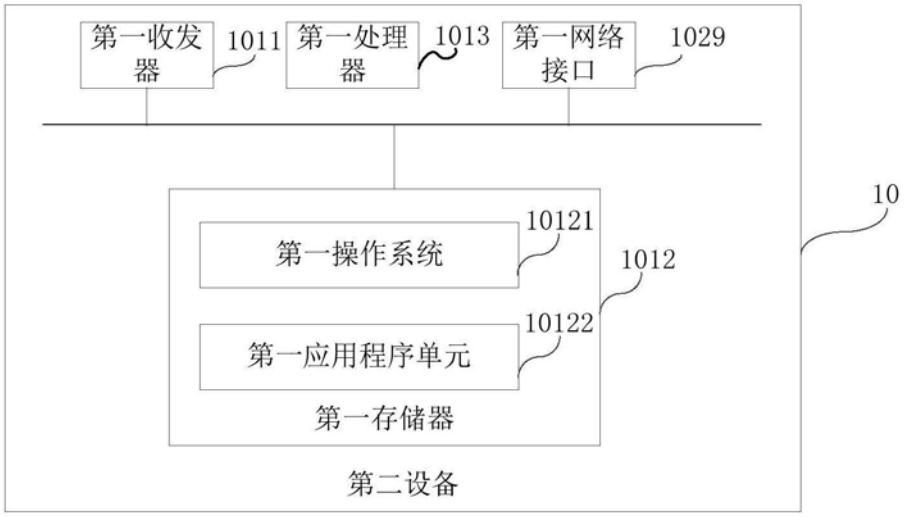

第一收发器
1011
第一处理器
1013
第一网络接口
1029
10
10121
第一操作系统
1012
10122
第一应用程序单元
第一存储器
第二设备

图2

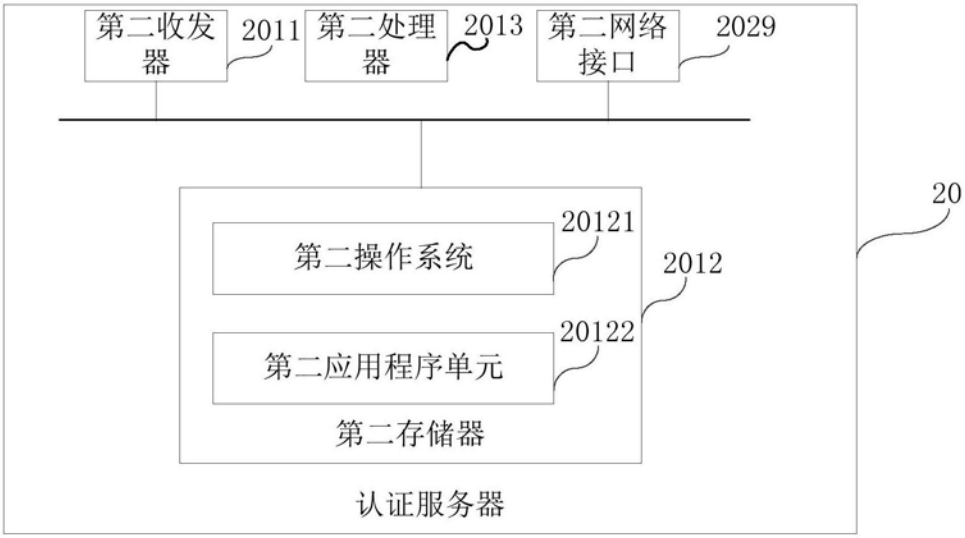

第二收发器
2011
第二处理器
2013
第二网络接口
2029
20
20121
第二操作系统
2012
20122
第二应用程序单元
第二存储器
认证服务器

图3

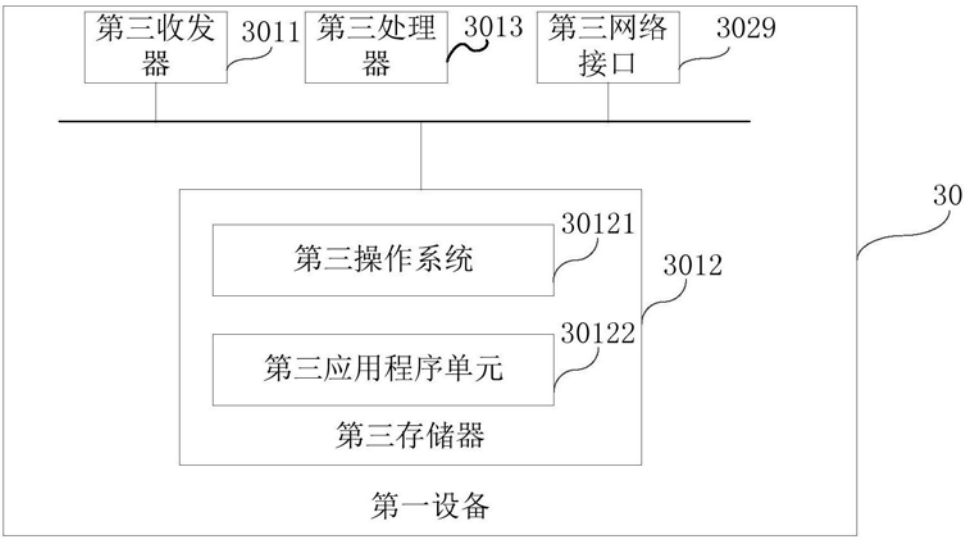

第三收发器
3011
第三处理器
3013
第三网络接口
3029
30
30121
第三操作系统
3012
30122
第三应用程序单元
第三存储器
第一设备

图4

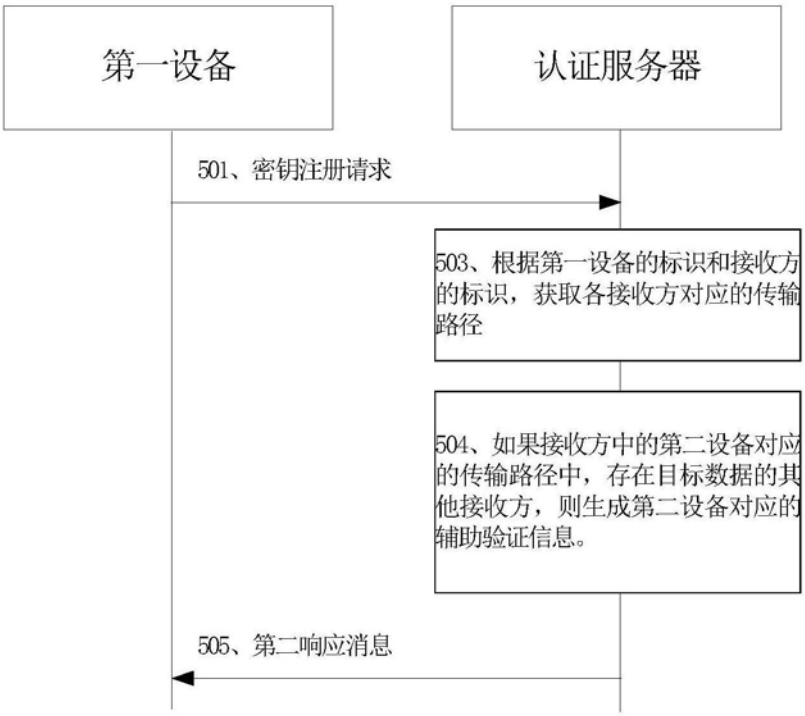

第一设备
认证服务器
501、密钥注册请求
503、根据第一设备的标识和接收方的标识，获取各接收方对应的传输路径
504、如果接收方中的第二设备对应的传输路径中，存在目标数据的其他接收方，则生成第二设备对应的辅助验证信息。
505、第二响应消息

图5

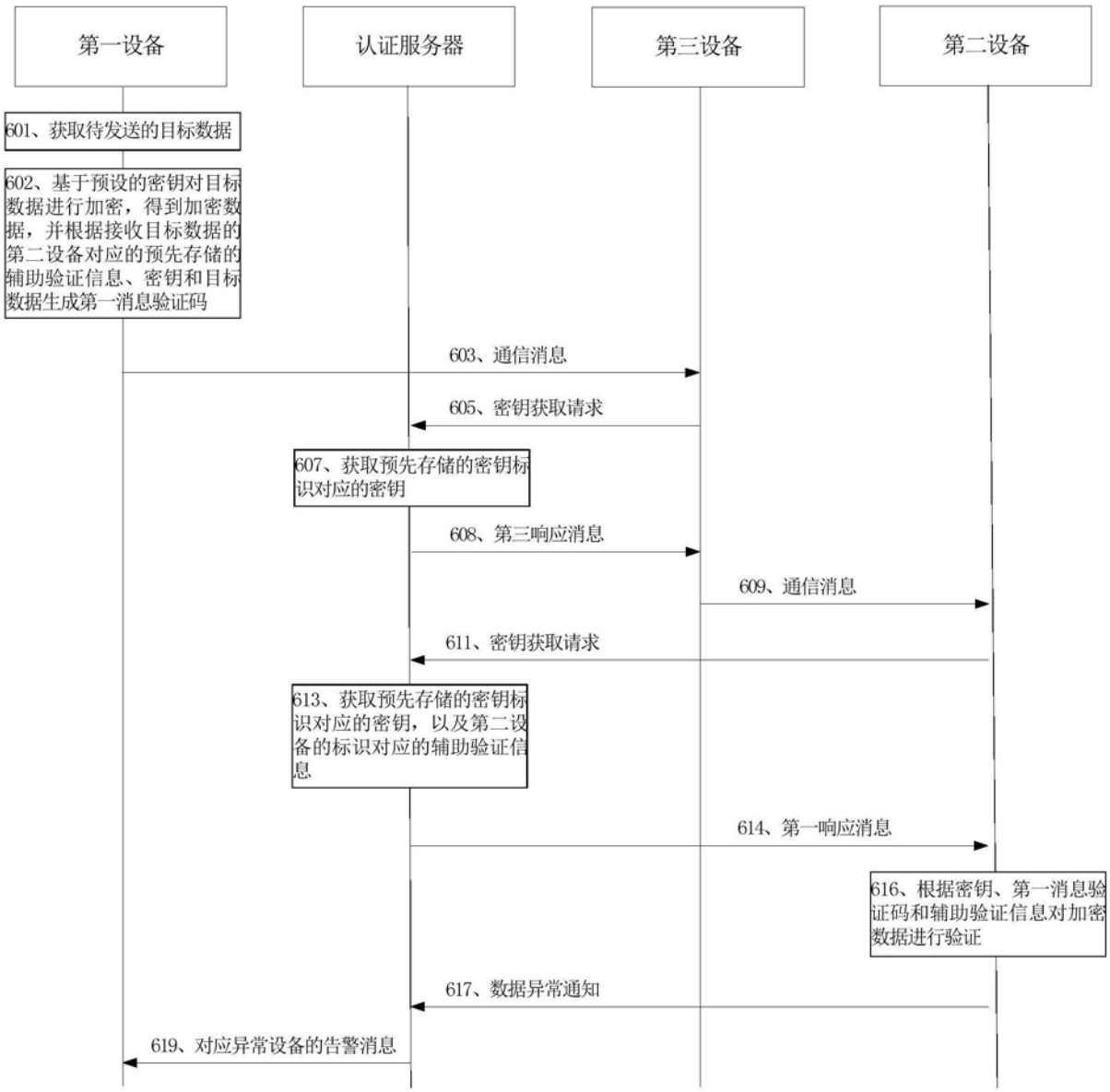

第一设备
认证服务器
第三设备
第二设备
601、获取待发送的目标数据
602、基于预设的密钥对目标数据进行加密，得到加密数据，并根据接收目标数据的第二设备对应的预先存储的辅助验证信息、密钥和目标数据生成第一消息验证码
603、通信消息
605、密钥获取请求
607、获取预先存储的密钥标识对应的密钥
608、第三响应消息
609、通信消息
611、密钥获取请求
613、获取预先存储的密钥标识对应的密钥，以及第二设备的标识对应的辅助验证信息
614、第一响应消息
616、根据密钥、第一消息验证码和辅助验证信息对加密数据进行验证
617、数据异常通知
619、对应异常设备的告警消息

图6

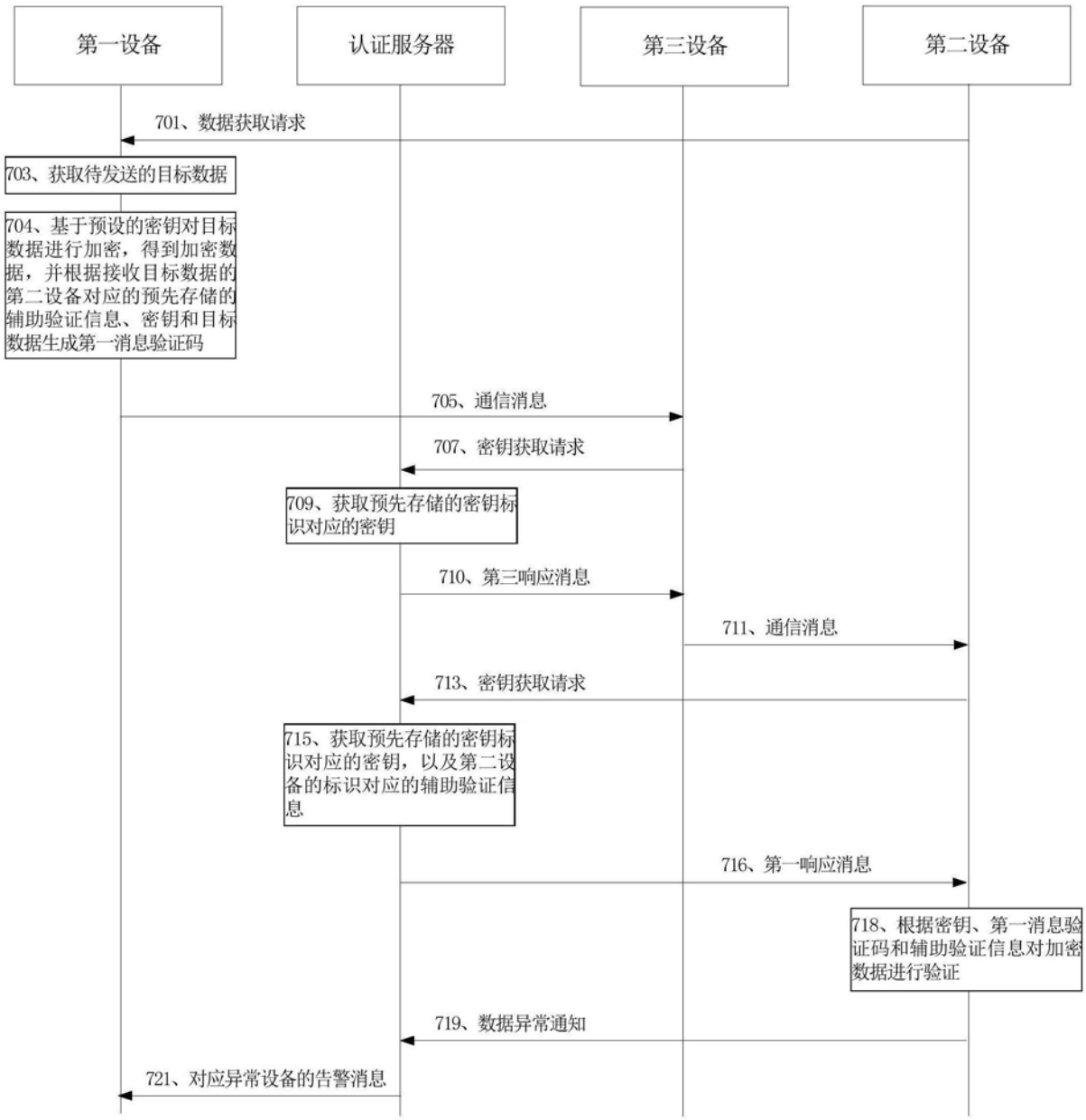

第一设备
认证服务器
第三设备
第二设备
701、数据获取请求
703、获取待发送的目标数据
704、基于预设的密钥对目标数据进行加密，得到加密数据，并根据接收目标数据的第二设备对应的预先存储的辅助验证信息、密钥和目标数据生成第一消息验证码
705、通信消息
707、密钥获取请求
709、获取预先存储的密钥标识对应的密钥
710、第三响应消息
711、通信消息
713、密钥获取请求
715、获取预先存储的密钥标识对应的密钥，以及第二设备的标识对应的辅助验证信息
716、第一响应消息
718、根据密钥、第一消息验证码和辅助验证信息对加密数据进行验证
719、数据异常通知
721、对应异常设备的告警消息

图7

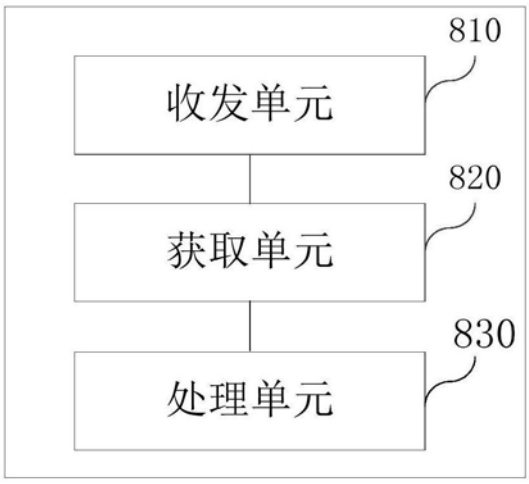

810
收发单元
820
获取单元
830
处理单元

图8


910
收发单元
920
获取单元

图9

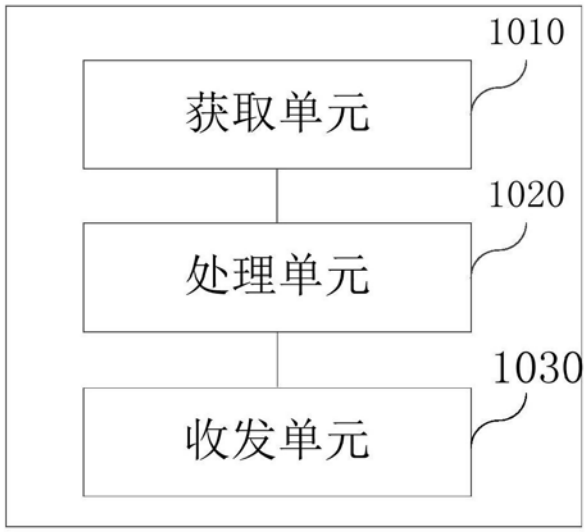

1010
获取单元
1020
处理单元
1030
收发单元

图10