(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 110896390 B
(45)授权公告日 2021.05.11

(21)申请号 201811063947.1
(22)申请日 2018.09.12
(65)同一申请的已公布的文献号
申请公布号 CN 110896390 A
(43)申请公布日 2020.03.20
(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 张裕海 杨艳江 王改良
(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 肖庆武
(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 107077557 A,2017.08.18
CN 106101068 A,2016.11.09
CN 108111467 A,2018.06.01
CN 105931052 A,2016.09.07
CN 106650496 A,2017.05.10
CN 106559211 A,2017.04.05
CN 107579817 A,2018.01.12
US 2017366516 A1,2017.12.21
US 2017033932 A1,2017.02.02
EP 3282775 A1,2018.02.14
CN 105187376 A,2015.12.23
CN 101729248 A,2010.06.09
EP 1912376 B1,2009.04.22
KR 20150024117 A,2015.03.06

审查员 李晴晴

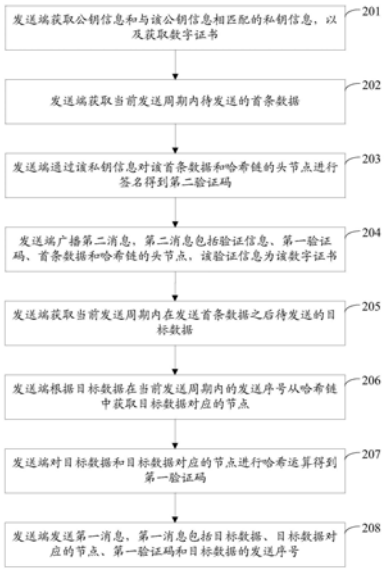
权利要求书6页 说明书24页 附图9页

(54)发明名称

一种发送消息的方法、验证消息的方法、装置及通信系统

(57)摘要

本申请公开了一种发送信息的方法、验证信息的方法、装置及通信系统，属于通信领域，可以应用在智能化的车辆(例如V2X网联汽车)上用于获取车外环境数据。所述方法包括：发送端获取待发送的目标数据，所述目标数据是当前发送周期内在发送首条数据之后待发送的数据；所述发送端根据所述目标数据在当前发送周期内的发送序号从哈希链中获取所述目标数据对应的节点，所述哈希链包括的节点数目等于当前发送周期内允许发送的数据数目；所述发送端对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一验证码，所述第一验证码用于接收端验证所述目标数据；所述发送端发送第一消息，所述第一消息包括所述目标数据、所述目标数据对应的节点、所述第一验证码和所述目标数据的发送序号。本申请能够提高传输消息的效率。



CN 110896390 B

1.一种发送消息的方法,其特征在于,所述方法包括:

发送端获取待发送的目标数据,所述目标数据是当前发送周期内在发送首条数据之后待发送的数据;

所述发送端根据所述目标数据在当前发送周期内的发送序号从哈希链中获取所述目标数据对应的节点,所述哈希链包括的节点数目等于当前发送周期内允许发送的数据数目;

所述发送端对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一验证码,所述第一验证码用于接收端验证所述目标数据;

所述发送端发送第一消息,所述第一消息包括所述目标数据、所述目标数据对应的节点、所述第一验证码和所述目标数据的发送序号。

2.如权利要求1所述的方法,其特征在于,所述根据所述目标数据在当前发送周期内的发送序号从哈希链中获取所述目标数据对应的节点之前,还包括:

随机生成所述哈希链的尾节点;

对所述哈希链中的节点h_{i-1}进行哈希运算得到所述哈希链中的节点h_i,i=1、2、……、N,N+1为当前发送周期内允许发送的数据数目,节点h_0为所述尾节点,节点h_N为所述哈希链的头节点。

3.如权利要求1所述的方法,其特征在于,所述根据所述目标数据在当前发送周期内的发送序号从哈希链中获取所述目标数据对应的节点,包括:

在根据所述目标数据的发送序号确定所述目标数据是当前发送周期内待发送的第二条数据时,获取所述哈希链的头节点作为所述目标数据对应的节点;

在根据所述目标数据的发送序号确定所述目标数据是位于所述第二条数据之后待发送的数据时,获取所述哈希链中位于第三节点之后且与所述第三节点相邻的第四节点作为所述目标数据对应的节点,所述第三节点是最近上一次发送的所述哈希链中的节点。

4.如权利要求1至3任一项所述的方法,其特征在于,所述第一消息还包括发送所述目标数据的第一时间戳。

5.如权利要求1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:

通过私钥信息对所述首条数据和所述哈希链的头节点进行签名得到第二验证码,所述第二验证码用于所述接收端对所述首条数据进行验证;

发送第二消息,所述第二消息包括验证信息、所述首条数据、所述第二验证码和所述首条数据对应的节点,所述验证信息包括与所述私钥信息相匹配的公钥信息。

6.如权利要求5所述的方法,其特征在于,所述通过私钥信息对所述首条数据和所述哈希链的头节点进行签名得到第二验证码,包括:

根据所述首条数据和所述哈希链的头节点生成第一摘要信息;

使用私钥信息对所述第一摘要信息进行签名得到第二验证码。

7.如权利要求5所述的方法,其特征在于,所述第二消息还包括发送所述目标数据的第二时间戳。

8.如权利要求5至7任一项所述的方法,其特征在于,所述验证信息为数字证书,所述数字证书包括所述公钥信息;或者,所述验证信息为所述公钥信息,所述公钥信息为所述发送端的身份标识信息。

9.一种验证消息的方法,其特征在于,所述方法包括:

接收端接收第一消息,所述第一消息包括目标数据、所述目标数据对应的哈希链中的一个节点、第一验证码和所述目标数据在目标发送周期中的发送序号,所述目标数据是所述目标发送周期内在发送首条数据之后发送的数据,所述哈希链包括的节点数目等于所述目标发送周期内允许发送的数据数目;

所述接收端根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。

10.如权利要求9所述的方法,其特征在于,所述根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证,包括:

根据所述目标数据的发送序号确定已接收的第一数据对应的节点,所述第一数据是发送端在发送所述目标数据之前最近发送的数据;

根据所述第一数据对应的节点对所述目标数据对应的节点进行验证;

在验证所述目标数据对应的节点通过时,对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一哈希结果;

在所述第一哈希结果与所述第一验证码匹配时,对所述目标数据验证通过。

11.如权利要求10所述的方法,其特征在于,所述第一数据为所述首条数据,所述首条数据对应的节点为所述哈希链的头节点,所述根据所述第一数据对应的节点对所述目标数据对应的节点进行验证,包括:

当所述目标数据对应的节点与所述首条数据对应的头节点相等时,对所述目标数据对应的节点验证通过。

12.如权利要求10所述的方法,其特征在于,所述第一数据为所述目标发送周期内在发送所述首条数据之后发送的数据,所述根据所述第一数据对应的节点对所述目标数据对应的节点进行验证,包括:

对所述目标数据对应的节点进行哈希运算得到第二哈希结果;

在所述第二哈希结果与所述第一数据对应的节点相等时,对所述目标数据对应的节点验证通过。

13.如权利要求9至12任一项所述的方法,其特征在于,所述第一消息还包括发送所述目标数据的第一时间戳;

所述根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证,包括:

获取所述第一时间戳和接收所述目标数据的第三时间戳之间的第一差值;

在所述第一差值不超过第一阈值时,根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。

14.如权利要求9所述的方法,其特征在于,所述接收第一消息之前,还包括:

接收第二消息,所述第二消息包括所述首条数据、所述首条数据对应的所述哈希链的头节点、第二验证码和验证信息,所述验证信息包括公钥信息;

根据所述第二验证码和所述公钥信息对所述首条数据进行验证。

15.如权利要求14所述的方法,其特征在于,所述根据所述第二验证码和所述公钥信息对所述首条数据进行验证,包括:

使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息；

根据所述首条数据和所述首条数据对应的头节点生成第二摘要信息；

在所述第一摘要信息与所述第二摘要信息匹配时，对所述首条数据验证通过。

16.如权利要求15所述的方法，其特征在于，所述验证信息为数字证书，所述数字证书包括所述公钥信息，

所述使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息，包括：

使用所述数字证书的颁发者公钥信息验证所述数字证书；

在验证所述数字证书通过后，使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息。

17.如权利要求16所述的方法，其特征在于，所述使用所述数字证书的颁发者公钥信息验证所述数字证书，包括：

将所述第二消息缓存在消息缓存区中；

在接收消息的时间长度达到第二阈值时，对接收到的Z个消息中的数字证书进行验证，所述Z个消息是所述消息缓存区中缓存的包括数字证书的消息，Z为大于0的整数；

在对所述Z个消息中的数字证书进行验证未通过时，使用所述数字证书的颁发者公钥信息验证所述数字证书。

18.如权利要求17所述的方法，其特征在于，所述对接收到的Z个消息中的数字证书进行验证，包括：

对Z个消息中的数字证书进行哈希运算，得到所述Z个消息中的数字证书的哈希值；

计算所述Z个消息中的数字证书的哈希值的乘积得到第一数值；

计算所述Z个消息中的数字证书中的数字签名的乘积得到第二数值；

在所述第二数值的e次方等于所述第一数值时，对所述Z个消息中的数字证书进行验证通过。

19.如权利要求14所述的方法，其特征在于，所述第二消息还包括发送所述首条数据的第二时间戳；

所述根据所述第二验证码和所述公钥信息对所述首条数据进行验证，包括：

获取所述第二时间戳和接收所述首条数据的第四时间戳之间的第二差值；

在所述第二差值不超过第一阈值时，根据所述第二验证码和所述公钥信息对所述首条数据进行验证。

20.如权利要求14至19任一项所述的方法，其特征在于，所述根据所述第二验证码和所述公钥信息对所述首条数据进行验证，包括：

将所述第二消息缓存在消息缓存区中；

在接收消息的时间长度达到第二阈值时，同时对接收到的Z个第二消息进行验证，所述Z个第二消息是所述消息缓存区中缓存的第二消息；

在同时对所述Z个第二消息验证不通过时，根据所述第二验证码和所述公钥信息对所述首条数据进行验证。

21.一种发送消息的装置，其特征在于，所述装置包括：

处理单元，用于获取待发送的目标数据，所述目标数据是当前发送周期内在发送首条数据之后待发送的数据；根据所述目标数据在当前发送周期内的发送序号从哈希链中获取

所述目标数据对应的节点，所述哈希链包括的节点数目等于当前发送周期内允许发送的数据数目；对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一验证码，所述第一验证码用于接收端验证所述目标数据；

发送单元，用于发送第一消息，所述第一消息包括所述目标数据、所述目标数据对应的节点、所述第一验证码和所述目标数据的发送序号。

22.如权利要求21所述的装置，其特征在于，所述处理单元，还用于：

随机生成所述哈希链的尾节点；

对所述哈希链中的节点h_{i-1}进行哈希运算得到所述哈希链中的节点h_i，i＝1、2、……、N，N+1为当前发送周期内允许发送的数据数目，节点h_0为所述尾节点，节点h_N为所述哈希链的头节点。

23.如权利要求21所述的装置，其特征在于，所述处理单元，用于：

在根据所述目标数据的发送序号确定所述目标数据是当前发送周期内待发送的第二条数据时，获取所述哈希链的头节点作为所述目标数据对应的节点；

在根据所述目标数据的发送序号确定所述目标数据是位于所述第二条数据之后待发送的数据时，获取所述哈希链中位于第三节点之后且与所述第三节点相邻的第四节点作为所述目标数据对应的节点，所述第三节点是最近上一次发送的所述哈希链中的节点。

24.如权利要求21至23任一项所述的装置，其特征在于，所述第一消息还包括发送所述目标数据的第一时间戳。

25.如权利要求21所述的装置，其特征在于，

所述处理单元，还用于通过私钥信息对所述首条数据和所述哈希链的头节点进行签名得到第二验证码，所述第二验证码用于所述接收端对所述首条数据进行验证；

所述发送单元，还用于发送第二消息，所述第二消息包括验证信息、所述首条数据、所述第二验证码和所述首条数据对应的节点，所述验证信息包括与所述私钥信息相匹配的公钥信息。

26.如权利要求25所述的装置，其特征在于，所述处理单元，用于：

根据所述首条数据和所述哈希链的头节点生成第一摘要信息；

使用私钥信息对所述第一摘要信息进行签名得到第二验证码。

27.如权利要求25所述的装置，其特征在于，所述第二消息还包括发送所述目标数据的第二时间戳。

28.如权利要求25至27任一项所述的装置，其特征在于，所述验证信息为数字证书，所述数字证书包括所述公钥信息；或者，所述验证信息为所述公钥信息，所述公钥信息为所述装置的身份标识信息。

29.一种验证消息的装置，其特征在于，所述装置包括：

接收单元，用于接收第一消息，所述第一消息包括目标数据、所述目标数据对应的哈希链中的一个节点、第一验证码和所述目标数据在目标发送周期中的发送序号，所述目标数据是所述目标发送周期内在发送首条数据之后发送的数据，所述哈希链包括的节点数目等于所述目标发送周期内允许发送的数据数目；

处理单元，用于根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。

30.如权利要求29所述的装置,其特征在于,所述处理单元,用于:

根据所述目标数据的发送序号确定已接收的第一数据对应的节点,所述第一数据是发送端在发送所述目标数据之前最近发送的数据;

根据所述第一数据对应的节点对所述目标数据对应的节点进行验证;

在验证所述目标数据对应的节点通过时,对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一哈希结果;

在所述第一哈希结果与所述第一验证码匹配时,对所述目标数据验证通过。

31.如权利要求30所述的装置,其特征在于,所述第一数据为所述首条数据,所述首条数据对应的节点为所述哈希链的头节点,所述处理单元,用于当所述目标数据对应的节点与所述首条数据对应的头节点相等时,对所述目标数据对应的节点验证通过。

32.如权利要求30所述的装置,其特征在于,所述第一数据为所述目标发送周期内在发送所述首条数据之后发送的数据,所述处理单元,用于:

对所述目标数据对应的节点进行哈希运算得到第二哈希结果;

在所述第二哈希结果与所述第一数据对应的节点相等时,对所述目标数据对应的节点验证通过。

33.如权利要求29至32任一项所述的装置,其特征在于,所述第一消息还包括发送所述目标数据的第一时间戳;

所述处理单元,用于:

获取所述第一时间戳和接收所述目标数据的第三时间戳之间的第一差值;

在所述第一差值不超过第一阈值时,根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。

34.如权利要求29所述的装置,其特征在于,

所述接收单元,还用于接收第二消息,所述第二消息包括所述首条数据、所述首条数据对应的所述哈希链的头节点、第二验证码和验证信息,所述验证信息包括公钥信息;

所述处理单元,还用于根据所述第二验证码和所述公钥信息对所述首条数据进行验证。

35.如权利要求34所述的装置,其特征在于,所述处理单元,用于:

使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息;

根据所述首条数据和所述首条数据对应的头节点生成第二摘要信息;

在所述第一摘要信息与所述第二摘要信息匹配时,对所述首条数据验证通过。

36.如权利要求35所述的装置,其特征在于,所述验证信息为数字证书,所述数字证书包括所述公钥信息,

所述处理单元,用于:

使用所述数字证书的颁发者公钥信息验证所述数字证书;

在验证所述数字证书通过后,使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息。

37.如权利要求36所述的装置,其特征在于,所述处理单元,用于:

将所述第二消息缓存在消息缓存区中;

在接收消息的时间长度达到第二阈值时,对接收到的Z个消息中的数字证书进行验证,

所述Z个消息是所述消息缓存区中缓存的包括数字证书的消息，Z为大于0的整数；

在对所述Z个消息中的数字证书进行验证未通过时，使用所述数字证书的颁发者公钥信息验证所述数字证书。

38.如权利要求37所述的装置，其特征在于，所述处理单元，用于：

对Z个消息中的数字证书进行哈希运算，得到所述Z个消息中的数字证书的哈希值；

计算所述Z个消息中的数字证书的哈希值的乘积得到第一数值；

计算所述Z个消息中的数字证书中的数字签名的乘积得到第二数值；

在所述第二数值的e次方等于所述第一数值时，对所述Z个消息中的数字证书进行验证通过。

39.如权利要求34至38任一项所述的装置，其特征在于，所述第二消息还包括发送所述首条数据的第二时间戳；

所述处理单元，用于：

获取所述第二时间戳和接收所述首条数据的第四时间戳之间的第二差值；

在所述第二差值不超过第一阈值时，根据所述第二验证码和所述公钥信息对所述首条数据进行验证。

40.如权利要求29所述的装置，其特征在于，所述处理单元，用于：

将第二消息缓存在消息缓存区中；

在接收消息的时间长度达到第二阈值时，同时对接收到的Z个第二消息进行验证，所述Z个第二消息是所述消息缓存区中缓存的第二消息；

在同时对所述Z个第二消息验证不通过时，根据第二验证码和公钥信息对所述首条数据进行验证。

41.一种通信系统，其特征在于，所述通信系统包括：如权利要求21至28任一项权利要求所述的装置和如权利要求29至40任一项权利要求所述的装置。

一种发送消息的方法、验证消息的方法、装置及通信系统

技术领域

[0001] 本申请涉及通信领域，特别涉及一种发送信息的方法、验证信息的方法、装置及通信系统。

背景技术

[0002] 随着信息技术的不断发展，诸如智能手机、智能电视、智能音箱、智能冰箱等智能化设备不断涌入人们的生活，人们越来越多的感受到智能化所带来的便利。与此同时，车辆的智能化，越来越被人们所关注，研究车外情景智能化离不开对车外环境数据的获取。

[0003] 对于任一车辆，该车辆可以获取其他车辆共享的车外环境数据，在实现时，各车辆在采集到车外环境数据时，可以将该车外环境数据发送给中央服务器。中央服务器接收该车外环境数据，可以绘制一个地图，该地图包括接收各车辆发送的车外环境数据。这样对于各车辆，该车辆可以从中央服务器中下载该地图，从而获取到各车辆共享的车外环境数据。

[0004] 在实现本申请的过程中，发明人发现现有技术至少存在以下问题：

[0005] 目前共享车外环境数据依赖中央服务器，车辆从中央服务器中获取数据的过程受到网络状态的影响，存在一定的网络延时。

发明内容

[0006] 为了提高传输消息的效率，本申请实施例提供了一种发送消息的方法、验证消息的方法、装置及通信系统。所述技术方案如下：

[0007] 第一方面，本申请提供了一种发送消息的方法，在所述方法中发送端获取待发送的目标数据，所述目标数据是当前发送周期内在发送首条数据之后待发送的数据；根据所述目标数据在当前发送周期内的发送序号从哈希链中获取所述目标数据对应的节点，所述哈希链包括的节点数目等于当前发送周期内允许发送的数据数目；对所述目标数据和所述目标数据对应的节点进行哈希运算得到第一验证码，所述第一验证码用于接收端验证所述目标数据；发送第一消息，所述第一消息包括所述目标数据、所述目标数据对应的节点、所述第一验证码和所述目标数据的发送序号。由于发送端可以直接向接收端发送第一消息，这样第一消息可以不经过服务器转发，减小了第一消息传输的延时，提高消息发送的效率。另外，由于发送端对目标数据和目标数据对应的节点进行哈希运算，哈希运算所需要的计算资源少，降低发送消息的成本，又由于第一消息还包括目标数据对应的节点，使得接收端可以通过验证目标数据对应的节点，提高消息传输的安全性，验证节点的速度较快，提高接收端验证的速率。

[0008] 在第一方面的一种可能实现方式中，随机生成所述哈希链的尾节点；对所述哈希链中的节点h_{i-1}进行哈希运算得到所述哈希链中的节点h_i，i＝1、2、……、N，N+1为当前发送周期内允许发送的数据数目，节点h_0为所述尾节点，节点h_N为所述哈希链的头节点。由于对所述哈希链中的节点h_{i-1}进行哈希运算得到所述哈希链中的节点h_i，这样使得哈希链具有单向映射的特性。

[0009] 在第一方面的一种可能实现方式中，在根据所述目标数据的发送序号确定所述目标数据是当前发送周期内待发送的第二条数据时，获取所述哈希链的头节点作为所述目标数据对应的节点；在根据所述目标数据的发送序号确定所述目标数据是位于所述第二条数据之后待发送的数据时，获取所述哈希链中位于第三节点之后且与所述第三节点相邻的第四节点作为所述目标数据对应的节点，所述第三节点是最近上一次发送的所述哈希链中的节点。这样可以使发送端在发送首条数据之后发送的各数据对应的节点都是连续的节点，接收端可以根据各数据对应的节点验证数据连续性，来保证数据传输的安全性。

[0010] 在第一方面的一种可能实现方式中，所述第一消息还包括发送所述目标数据的第一时间戳。这样可以使接收端通过第一时间戳验证接收的消息的时效性，以进一步提高消息传输的安全性。

[0011] 在第一方面的一种可能实现方式中，通过私钥信息对所述首条数据和所述哈希链的头节点进行签名得到第二验证码，所述第二验证码用于所述接收端对所述首条数据进行验证；发送第二消息，所述第二消息包括验证信息、所述首条数据、所述第二验证码和所述首条数据对应的节点，所述验证信息包括与所述私钥信息相匹配的公钥信息。由于发送端使用私钥信息对首条数据和哈希链的头节点进行签名得到第二验证码，这样提高消息传输的安全性。

[0012] 在第一方面的一种可能实现方式中，先根据所述首条数据和所述哈希链的头节点生成第一摘要信息；然后使用私钥信息对所述第一摘要信息进行签名得到第二验证码。对第一摘要信息进行签名，可以减小签名所需要的计算量。

[0013] 在第一方面的一种可能实现方式中，所述第二消息还包括发送所述目标数据的第二时间戳。这样可以使接收端通过第二时间戳验证接收的消息的时效性，以进一步提高消息传输的安全性。

[0014] 在第一方面的一种可能实现方式中，所述验证信息为数字证书，所述数字证书包括所述公钥信息；或者，所述验证信息为所述公钥信息，所述公钥信息为所述发送端的身份标识信息。

[0015] 第二方面，本申请提供了一种验证消息的方法，在所述方法中接收端接收第一消息，所述第一消息包括目标数据、所述目标数据对应的哈希链中的一个节点、第一验证码和所述目标数据在目标发送周期中的发送序号，所述目标数据是所述目标发送周期内在发送首条数据之后发送的数据，所述哈希链包括的节点数目等于所述目标发送周期内允许发送的数据数目；根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。由于接收端可以直接接收发送端发送的消息，这样该消息可以不经过服务器转发，减小了该消息传输的延时，提高消息发送的效率。另外，该消息包括目标数据对应的哈希链中的节点，这样接收端通过对该节点进行验证可以保障该消息传输的安全性。

[0016] 在第二方面的一种可能实现方式中，根据所述目标数据的发送序号确定已接收的第一数据对应的节点，所述第一数据是发送端在发送所述目标数据之前最近发送的数据；由于根据所述第一数据对应的节点对所述目标数据对应的节点进行验证，这样接收端通过验证目标数据对应的节点来保证消息传输的安全性，对节点的验证速度较快，又提高了验证的效率。在验证所述目标数据对应的节点通过时，由于对所述目标数据和所述目标数据

对应的节点进行哈希运算得到第一哈希结果;在所述第一哈希结果与所述第一验证码匹配时,对所述目标数据验证通过,这样接收端只需要对目标数据和目标数据对应的节点进行哈希运算,哈希运算所需要的计算资源少,减小了验证成本。

[0017] 在第二方面的一种可能实现方式中,所述第一数据为所述首条数据,当所述目标数据对应的节点与所述首条数据对应的头节点相等时,对所述目标数据对应的节点验证通过。这样在目标数据为第二条数据时,只需验证目标数据的节点和首条数据对应的头节点是否相等,验证操作简单,所需要的计算资源少,验证的速度快。

[0018] 在第二方面的一种可能实现方式中,所述第一数据为所述目标发送周期内在发送所述首条数据之后发送的数据,由于对所述目标数据对应的节点进行哈希运算得到第二哈希结果;在所述第二哈希结果与所述第一数据对应的节点相等时,对所述目标数据对应的节点验证通过,哈希运算所需要计算量较少,这样使得验证操作简单,所需要的计算资源少,验证的速度快。

[0019] 在第二方面的一种可能实现方式中,所述第一消息还包括发送所述目标数据的第一时间戳;获取所述第一时间戳和接收所述目标数据的第三时间戳之间的第一差值;在所述第一差值不超过第一阈值时,根据所述目标数据对应的节点、所述目标数据对应的发送序号和所述第一验证码对所述目标数据进行验证。这样接收端可以通过第一时间戳和第三时间戳验证接收的消息的时效性,以进一步提高消息传输的安全性。

[0020] 在第二方面的一种可能实现方式中,接收第二消息,所述第二消息包括所述首条数据、所述首条数据对应的所述哈希链的头节点、第二验证码和验证信息,所述验证信息包括公钥信息;根据所述第二验证码和所述公钥信息对所述首条数据进行验证。由于根据所述第二验证码和所述公钥信息对所述首条数据进行验证,这样发送端可以使私钥信息对首条数据进行签名,提高首条数据传输的安全性。

[0021] 在第二方面的一种可能实现方式中,使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息;根据所述首条数据和所述首条数据对应的头节点生成第二摘要信息;在所述第一摘要信息与所述第二摘要信息匹配时,对所述首条数据验证通过。由于接收端使用公钥信息对第二验证码进行解密,这样发送端在发送首条数据时就可以采用私钥信息加密,从而提高了消息安全性。

[0022] 在第二方面的一种可能实现方式中,所述验证信息为数字证书,所述数字证书包括所述公钥信息,使用所述数字证书的颁发者公钥信息验证所述数字证书;在验证所述数字证书通过后,使用所述公钥信息对所述第二验证码进行解密得到第一摘要信息。由于数字证书中包括公钥信息,对数字证书进行验证,在验证数字证书安全时,使用数字证书中的公钥信息解密,可以进一步提高安全性。

[0023] 在第二方面的一种可能实现方式中,将所述第二消息缓存在消息缓存区中;在接收消息的时间长度达到第二阈值时,对接收到的Z个消息中的数字证书进行验证,所述Z个消息是所述消息缓存区中缓存的包括数字证书的消息,Z为大于0的整数;在对所述Z个消息中的数字证书进行验证未通过时,使用所述数字证书的颁发者公钥信息验证所述数字证书。这样可以实现对多个数字证书批量验证,提高验证效率,另外对每个数字证书一一验证所需要的计算资源也较多,多于批量验证所需的计算资源,所以又可以减小计算资源的占用。

[0024] 在第二方面的一种可能实现方式中，对Z个消息中的数字证书进行哈希运算，得到所述Z个消息中的数字证书的哈希值；计算所述Z个消息中的数字证书的哈希值的乘积得到第一数值；计算所述Z个消息中的数字证书中的数字签名的乘积得到第二数值；在所述第二数值的e次方等于所述第一数值时，对所述Z个消息中的数字证书进行验证通过，从而实现了对M个数字证书进行批量验证。

[0025] 在第二方面的一种可能实现方式中，所述第二消息还包括发送所述首条数据的第二时间戳；获取所述第二时间戳和接收所述首条数据的第四时间戳之间的第二差值；在所述第二差值不超过第一阈值时，根据所述第二验证码和所述公钥信息对所述首条数据进行验证。这样接收端可以通过第二时间戳和第四时间戳验证接收的消息的时效性，以进一步提高消息传输的安全性。

[0026] 在第二方面的一种可能实现方式中，将所述第二消息缓存在消息缓存区中；在接收消息的时间长度达到第二阈值时，同时对接收到的Z个第二消息进行验证，所述Z个第二消息是所述消息缓存区中缓存的第二消息；在同时对所述Z个第二消息验证不通过时，根据所述第二验证码和所述公钥信息对所述首条数据进行验证。这样可以实现对多个消息批量验证，提高验证效率。

[0027] 第三方面，本申请实施例提供了一种发送消息的装置，用于执行第一方面或第一方面的任意一种可能实现方式中的方法。具体地，所述装置包括用于执行第一方面或第一方面的任意一种可能实现方式的方法的单元。

[0028] 第四方面，本申请实施例提供了一种验证消息的装置，用于执行第二方面或第二方面的任意一种可能实现方式中的方法。具体地，所述装置包括用于执行第二方面或第二方面的任意一种可能实现方式的方法的单元。

[0029] 第五方面，本申请实施例提供了一种发送消息的装置，所述装置包括：收发器、处理器和存储器。其中，所述收发器、所述处理器以及所述存储器之间可以通过总线系统相连。所述存储器用于存储程序、指令或代码，所述处理器用于执行所述存储器中的程序、指令或代码，完成第一方面或第一方面的任意可能实现方式中的方法。

[0030] 第六方面，本申请实施例提供了一种验证消息的装置，所述装置包括：收发器、处理器和存储器。其中，所述收发器、所述处理器以及所述存储器之间可以通过总线系统相连。所述存储器用于存储程序、指令或代码，所述处理器用于执行所述存储器中的程序、指令或代码，完成第二方面或第二方面的任意可能实现方式中的方法。

[0031] 第七方面，本申请实施例提供了一种计算机程序产品，所述计算机程序产品包括在计算机可读存储介质中存储的计算机程序，并且所述计算程序通过处理器进行加载来实现上述第一方面、第二方面、第一方面的任意可能实现方式或第二方面的任意可能实现方式的方法。

[0032] 第八方面，本申请实施例提供了一种非易失性计算机可读存储介质，用于存储计算机程序，所述计算机程序通过处理器进行加载来执行上述第一方面、第二方面、第一方面的任意可能实现方式或第二方面的任意可能实现方式的指令。

[0033] 第九方面，本申请实施例提供了一种芯片，所述芯片包括可编程逻辑电路和/或程序指令，当所述芯片运行时用于实现上述第一方面、第二方面、第一方面的任意可能实现方式或第二方面的任意可能实现方式的方法。

[0034] 第十方面，本申请实施例提供了一种通信系统，包括第三方面或第五方面所述的装置和第四方面或第六方面所述的装置。

附图说明

[0035] 图1-1是本申请实施例提供的一种通信系统的结构示意图；

[0036] 图1-2是本申请实施例提供的另一种通信系统的结构示意图；

[0037] 图2-1是本申请实施例提供的一种发送消息的方法流程图；

[0038] 图2-2是本申请实施例提供的一种数字证书的结构示意图；

[0039] 图2-3是本申请实施例提供的一种身份标识信息的结构示意图；

[0040] 图2-4是本申请实施例提供的一种设备类型信息的结构示意图；

[0041] 图2-5是本申请实施例提供的一种设备标识信息的结构示意图；

[0042] 图3是本申请实施例提供的一种验证消息的方法流程图；

[0043] 图4是本申请实施例提供的另一种发送消息的方法流程图；

[0044] 图5是本申请实施例提供的另一种验证消息的方法流程图；

[0045] 图6是本申请实施例提供的一种发送消息的装置结构示意图；

[0046] 图7是本申请实施例提供的一种验证消息的装置结构示意图；

[0047] 图8是本申请实施例提供的另一种发送消息的装置结构示意图；

[0048] 图9是本申请实施例提供的另一种验证消息的装置结构示意图；

[0049] 图10是本申请实施例提供的另一种通信系统的结构示意图。

具体实施方式

[0050] 下面将结合附图对本申请实施方式作进一步地详细描述。

[0051] 参见图1-1，本申请实施例提供了一种通信系统，该通信系统包括：

[0052] 发送端和接收端，发送端和接收端可以建立有通信连接；

[0053] 发送端可以获取待发送的数据，为了提高发送数据的效率，发送端可以直接向接收端广播该数据，这样该数据不需要经过位于网络侧的中央服务器转发给接收端，减小该数据传输的时延，提高该数据的发送效率。

[0054] 发送端采用直接向接收端广播该数据的方式时，发送端定义了发送周期，该发送周期周期性循环。在该数据为当前发送周期内待发送的首条数据时，发送端通过私钥信息对该首条数据和哈希链的头节点进行签名得到第二验证码；然后发送端广播第二消息，第二消息包括验证消息、第二验证码、该首条数据和该哈希链的头节点，该验证消息包括与该私钥信息相匹配的公钥信息。或者，在该数据为当前发送周期内除该首条数据以外的其他待发送的目标数据时，发送端从哈希链中获取目标数据对应的节点，对目标数据和目标数据对应的节点进行哈希运算得到第一验证码，广播第一消息，第一消息包括第一验证码、目标数据、目标数据对应的节点和目标数据的发送序号。

[0055] 这样接收端可以接收发送端广播的消息(该消息可以为第一消息或第二消息)，在该消息为第二消息时，根据该验证消息和第二验证码对首条数据进行验证。在该消息为第一消息时，根据目标数据对应的节点、第一验证码和目标数据对应的发送序号，对目标数据进行验证。

[0056] 哈希链中包括的节点数目等于一个发送周期内允许发送的数据数目。哈希链中任意相邻的两个节点，为了便于说明称该任意相邻的两个节点分别为第一节点和第二节点，第一节点靠近哈希链的头节点，第一节点是基于第二节点推算出来的。

[0057] 可选的，一个发送周期可以对应一个哈希链，这样发送端可以在每个发送周期发送首条数据之前生成哈希链；或者，m个发送周期可以对应一个哈希链，m为大于1的整数，这样发送端在一个发送周期内发送首条数据之前生成哈希链，在生成哈希链后接下来的连续m-1个发送周期内不用再生成哈希链，直至在第m+1个发送周期内在发送首条数据之前生成哈希链。

[0058] 上述通信系统可以应用在智能交通系统，在智能交通系统中发送端和接收端可以均为交通工具。可选的，发送端或接收端可以为安装或集成在交通工具中的车载终端等。

[0059] 假设，交通工具为汽车时，汽车在道路上可以获取数据，该数据可以是车外环境数据等，车外环境数据可以是路况信息等，车外环境数据可以是汽车的司机输入到汽车中的数据，例如，用户输入一段数据为“前方路口发生交通事故”，该一段数据就是车外环境数据。该汽车可以按上述方式向其他汽车广播数据，以将该数据共享给其他汽车，例如汽车可以将获取的路况信息广播到其他汽车，以实现将其获取的路况数据共享给其他汽车。

[0060] 可选的，交通工具除了是汽车外，还可以是自行车、平衡车或无人机等。上述发送端或接收端除了是交通工具，还可以是可穿戴设备、智能家居设备或移动终端等。例如，当发送端或接收端为可穿戴设备时，发送端或接收端可以为手环、手表、耳机或眼镜等。当发送端或接收端为智能家居设备时，发送端或接收端可以为音箱、电视、冰箱、彩电、洗衣机、马桶、路由器、灯具或空调等。当发送端或接收端为移动终端时，发送端或接收端可以为手机、平板电脑或笔记本电脑等。

[0061] 可选的，参见图1-2，该通信系统还可以包括服务器，发送端和接收端可以分别与服务器建立有通信连接，发送端和/或接收端可以从服务器获取数字证书颁发者的公钥信息和私钥信息等内容，发送端可以利用获取的内容发送消息，接收端可以利用获取的内容接收该消息，详细描述过程可以参见如下实施例中的相关内容，在此先不描述。

[0062] 参见图2-1，本申请实施例提供了一种发送消息的方法，该方法可以应用于图1-1所示的通信系统，该方法的执行主体为该通信系统的发送端，包括：

[0063] 步骤201：发送端获取公钥信息和与该公钥信息相匹配的私钥信息，以及获取数字证书。

[0064] 发送端可以采用公钥基础设施体系(public key infrastructure，PKI)机制获取公钥信息和与该公钥信息相匹配的私钥信息。可选的，在实现时获取公钥信息和私钥信息的过程可以为：发送端随机生成一串信息并将该信息作为公钥信息，然后生成与该公钥信息相匹配的私钥信息。

[0065] 数字证书包括数字签名和除该数字签名以外的其他部分内容，该其他部分内容可以包括该公钥信息和发送端的身份标识信息等内容。

[0066] 参见图2-2，数字证书包括多个字段，数字签名、该公钥信息和发送端的身份标识信息可以通过数字证书中的不同字段来携带。例如，在图2-2所示的数字证书中，CA数字签名(CA Digital Signature)字段携带该数字签名，主公钥信息(Subject Public Key Info)字段携带该公钥信息，主体唯一标识(Subject Unique ID)携带发送端的身份标识信

息。

[0067] 数字证书还可以包括其他字段，例如参见图2-2，还可以包括版本(Version)字段、序列号(Serial Number)字段、签名算法标识(Signature Algorithm ID)字段、发布者(CA)X500名字(Issuer(CA)X500Name)、有效周期(Validity Period)字段、主体X500名字(Subject X500 Name)字段、算法标识(Algorithm ID)字段、公钥值(Public Key Value)字段、发布者唯一标识(Issuer Unique ID)字段和扩展部分(Extension)字段。

[0068] 发送端可以先生成数字证书中除数字签名以外的其他部分，对该其他部分进行哈希运算得到哈希值，使用数字证书颁发者的私钥信息对该哈希值进行加密得到数字签名，将该数字签名和该其他部分组成数字证书。

[0069] 可选的，发送端可以事先从服务器中获取证书颁发者的私钥信息，然后在本地保存证书颁发者的私钥信息，所以发送端可以直接使用本地保存的证书颁发者的私钥信息对该哈希值进行加密。或者，发送端可以从服务器中获取证书颁发者的私钥信息，使用证书颁发者的私钥信息对该哈希值进行加密。

[0070] 可选的，发送端的身份标识信息可以包括发送端的设备类型信息和用于唯一标识发送端的设备标识信息。

[0071] 可选的，发送端的设备类型信息可以包括发送端属于的设备类别和发送端属于该设备类别包括的某个子类别。

[0072] 其中，可以定义多个设备类别，以及定义每个设备类别包括多个子类别。例如，参见下表1，下表1中的设备类别包括交通工具、可穿戴设备、智能家居和移动终端等。交通工具包括多个子类别，分别为汽车、自行车和平衡车等；可穿戴设备包括多个子类别，分别为手环、手表、耳机和眼镜等；智能家居包括多个子类别，分别为音箱、电视、冰箱、彩电、洗衣机、马桶、路由器、灯具和空调等；移动终端包括多个子类别，分别为手机、平板电脑和笔记本电脑等。

[0073] 表1

[0074]

设备类别	子类别
交通工具	汽车
	自行车
	平衡车
	无人机
	……
可穿戴设备	手环
	手表
	耳机
	眼镜
	……
智能家居	音箱
	电视
	冰箱
	彩电
	洗衣机
	马桶
	路由器
	灯具
	空调
	……
移动终端	手机
	平板电脑
	笔记本电脑
	……

[0075] 可选的，设备标识信息可以包括发送端的设备生产商标识信息、设备生产日期和生产序号等。

[0076] 可选的，发送端的身份标识信息可以包括第一部分和第二部分，第一部分包括至少一个字节，第一部分为发送端的设备类型信息，第一部分又可以分成两个子部分，其中一子部分包括多个比特且该子部分为发送端属于的设备类别，另一子部分包括多个比特且该另一部分为发送端属于的子类别。第二部分包括至少一个字节，第二部分为发送端的设备标识信息，第二部分又可以分成第一子部分、第二子部分和第三子部分，第一子部分包括至少一个字节且第一子部分为发送端的设备生产商标识信息，第二子部分包括至少一个字节且第二子部分为发送端的设备生产日期，第三子部分包括至少一个字节且第三子部分为发送端的生产序号。

[0077] 例如，如图2-3所示，假设身份标识信息可以包括12字节，第一部分包括前三个节字，即前三个字节可以为发送端的设备类型信息，第二部分包括后九个字节，即后九个字节

可以为设备标识信息。第一部分包括两个子部分，参见图2-4，在该例子中，假设其中一个子部分包括第一部分的前十二个比特，即该前十二个比特可以为发送端所属于的设备类别，另一个子部分包括第一部分的后十二个比特，即该后十二个比特可以为发送端属于该设备类别中的子类别。以及，参见图2-5，第二部分包括第一子部分、第二子部分和第三子部分，假设第一子部分包括第二部分的前三个字节，即该前三个字节可以为发送端的设备生产商标识信息，第二子部分包括第二部分的中间三个字节，即该中间三个字节可以为发送端的生产日期，第三子部分包括第二部分的后三个字节，即该后三个子节可以为发送端的生产序号，从而由该十二个字节组成了发送端的身份标识信息。

[0078] 步骤202：发送端获取当前发送周期内待发送的首条数据。

[0079] 可选的，首条数据可以是用户输入到发送端的数据，所以发送端可以接收用户输入的首条数据。

[0080] 在发送端中发送周期周期性循环。可选的，发送端可以定义一个周期长度，可以使用计时器来实现该发送周期。例如，发送端可以启动一个计时器，设置该计时器从零开始计时，表示一个发送周期开始；当该计时器计时的时间达到该周期长度时，重新设置该计时器从零开始计时，表示该一个发送周期结束且另一个发送周期开始，如此循环往复，实现发送周期周期性循环。

[0081] 对于每个发送周期，发送端可以记录在该发送周期内已发送的数据的发送序号。所以在当前发送周期内，当发送端接收到用户输入的数据时，发送端检测到本地有没有保存在当前发送周期内已发送的数据的发送序号，如果检测结果是没有保存，则确定该数据是当前发送周期的首条数据，如果检测结果是有保存，则确定该数据不是当前发送周期内的首条数据。

[0082] 步骤203：发送端通过该私钥信息对该首条数据和哈希链的头节点进行签名得到第二验证码。

[0083] 可选的，发送端还可以获取当前的第二时间戳，第二时间戳实质是发送端发送首条数据的时间戳，可以通过该私钥信息对第二时间戳、该首条数据和哈希链的头节点进行签名得到第二验证码。

[0084] 可选的，哈希链包括的节点数目等于一个发送周期内允许发送的数据数目。哈希链中任意相邻的两个节点，为了便于说明称该任意相邻的两个节点分别为第一节点和第二节点，第一节点靠近哈希链的头节点，第一节点是基于第二节点推算出来的。

[0085] 可选的，一个发送周期可以对应一个哈希链，或者，m个发送周期可以对应一个哈希链，m为大于1的整数。

[0086] 当一个发送周期对应一个哈希链时，发送端在对该首条数据和哈希链的头节点进行签名之前，还生成哈希链。

[0087] 当m个发送周期对应一个哈希链时，如果最近上次生成哈希链的时间所在的发送周期和当前发送周期间隔m-1个发送周期，则发送端在对该首条数据和哈希链的头节点进行签名之前，还生成哈希链；如果最近上次生成哈希链的时间所在的发送周期和当前发送周期间隔少于m-1个发送周期，发送端在对该首条数据和哈希链的头节点进行签名之前，获取最近上一次生成的哈希链。

[0088] 发送端生成哈希链的操作可以为：假设N+1为发送周期内允许发送的数据数目，发

送端随机生成一个随机值，将该随机值作为哈希链的尾节点，为了便于说明用h_0表示该尾节点；对于该哈希链的其他节点，为了便于说明用h_i表示其他节点，i＝1、2、……、N，对节点h_{i-1}进行哈希运算得到节点h_i，即$h_i=H(h_{i-1})$，H()为预设第一哈希函数，h_N为该哈希链的头节点。

[0089] 可选的，预设第一哈希函数可以为消息摘要算法第五版(message digest algorithm 5，MD5)算法等。

[0090] 在本步骤中，发送端可以根据该首条数据和哈希链的头节点生成第一摘要消息，使用该私钥信息对第一摘要消息进行加密得到第二验证码。

[0091] 可选的，发送端可以根据该首条数据和哈希链的头节点，通过MD5算法生成第一摘要消息。

[0092] 接下来举一个详细的例子，假设N＝3，即在当前发送周期内允许发送四条数据，假设当前发送周期存在四条数据，分别为m_0、m_1、m_2和m_3，m_0、m_1、m_2和m_3分别为当前发送周期内待发送的首条数据、第二条数据、第三条数据和第四条数据。发送端生成的哈希链包括头节点h_3，第二个节点h_2，第三个节点h_1和尾节点h_0，其中，尾节点h_0是一个随机值，第三个节点$h_1=H(h_0)$，第二个节点$h_2=H(h_1)$，头节点$h_3=H(h_2)$。

[0093] 发送端在获取到当前发送周期内的首条数据m_0时，可以根据首条数据m_0、当前的第二时间戳t_0和头节点h_3，生成第一摘要消息为MD_0，使用该私钥信息对第一摘要消息MD_0进行加密得到第二验证码e_0。

[0094] 其中，需要说明的是：使用私钥信息对第一摘要消息进行加密得到第二验证码所需要的计算资源较高，所以发送端在发送首条数据所需要的计算成本较高。

[0095] 步骤204：发送端广播第二消息，第二消息包括验证信息、第一验证码、首条数据和哈希链的头节点，该验证信息为该数字证书。

[0096] 可选的，发送端可以广播第二消息。

[0097] 可选的，第二消息还可以包括第二时间戳和首条数据在当前发送周期内的发送序号。

[0098] 可选的，发送端可以保存首条数据的发送序号。

[0099] 假设该数字证书为cert，则发送端广播的第二消息可以包括数字证书cert、第一验证码e_0、首条数据m_0、哈希链的头节点h_3、第二时间戳t_0、首条数据m_0在当前发送周期内的发送序号0，第二消息可以表示为$(cert、e_0、m_0、h_3、t_0、0)$。

[0100] 可选的，发送完首条数据后，发送端可以按如下流程发送当前发送周期内除首条数据以外的待发送的目标数据，该流程可以为。

[0101] 步骤205：发送端获取当前发送周期内在发送首条数据之后待发送的目标数据。

[0102] 由于发送端保存有最近上一次发送的当前发送周期内的数据的发送序号，所以发送端在获取到目标数据时，根据保存的最近上一次发送的当前发送周期内的数据的发送序号，可以确定该目标数据是当前发送周期的待发送的哪条数据，以及确定目标数据在当前发送周期内的发送序号。

[0103] 步骤206：发送端根据目标数据在当前发送周期内的发送序号从哈希链中获取目标数据对应的节点。

[0104] 当根据目标数据的发送序号确定目标数据是当前发送周期内待发送的第二条数

据时，发送端获取哈希链的头节点作为目标数据对应的节点；当根据目标数据的发送序号确定目标数据是位于该第二条数据之后待发送的数据时，发送端获取哈希链中位于第三节点之后且与第三节点相邻的第四节点作为目标数据对应的节点，第三节点是最近上一次发送的哈希链中的节点。

[0105] 例如，假设目标数据为当前发送期内待发送的第二条数据m_1，发送端获取哈希链中的头节点h_3作为第二条数据m_1对应的节点。

[0106] 步骤207：发送端对目标数据和目标数据对应的节点进行哈希运算得到第一验证码。

[0107] 可选的，发送端通过预设第二哈希函数对目标和目标数据对应的节点进行哈希运算。

[0108] 可选的，发送端还可以获取当前的第一时间戳，第一时间戳为发送目标数据的时间戳。发送端可以对目标数据、目标数据对应的节点和第一时间戳进行哈希运算得到第一验证码。

[0109] 例如，假设，目标数据为当前发送期内待发送的第二条数据m_1，发送端获取当前的第一时间戳t_1作为发送第二条数据m_1的时间戳。所以发送端对第二条数据m_1、第一时间戳t_1和第二条数据m_1对应的节点h_3进行哈希运算得到的第一验证码$e_1=MAC(m_1,t_1,h_3)$。MAC()为预设第二哈希函数，预设第二哈希函数可以为MD5算法等。

[0110] 步骤208：发送端发送第一消息，第一消息包括目标数据、目标数据对应的节点、第一验证码和目标数据的发送序号。

[0111] 可选的，发送端可以广播第一消息。

[0112] 可选的，第一消息还可以包括第一时间戳和/或发送端的身份标识信息。

[0113] 例如，发送端的身份标识信息可以用ID表示，发送端广播的第一消息可以包括第二条数据m_1、第二条数据m_1对应的节点h_3、第一验证码e_1、第二条数据m_1的发送序号1、第一时间戳为t_1和发送端的身份标识信息ID，第一消息可以表示为(m_1、h_3、e_1、1、t_1、ID)。

[0114] 接下来发送端开始发送第三条数据m_2，发送端获取当前的第一时间戳为t_2，最近上一次发送的哈希链中的节点为头节点h_3，获取与头节点h_3相邻且位于头节点h_3之后的第二个节点h_2，将第二个节点h_2作为第三条数据m_2对应的节点，所以发送端对第一时间戳t_2、第三条数据m_2和第三条数据m_2对应的节点h_2进行哈希运算得到的第一验证码$e_2=MAC(m_2,t_2,h_2)$，广播第一消息，第一消息可以表示为(m_2、h_2、e_2、2、t_2、ID)，其中2为第三条数据m_2的发送序号。

[0115] 再接下来发送端开始发送第四条数据m_3，发送端获取当前的第一时间戳为t_3，最近上一次发送的哈希链中的节点为第二个节点h_2，获取与第二个节点h_2相邻且位于第二个节点h_2之后的第三个节点h_1，将第三个节点h_1作为第四条数据m_3对应的节点，所以发送端对第一时间戳t_3、第四条数据m_3和第四条数据m_3对应的节点h_1进行哈希运算得到的第一验证码$e_3=MAC(m_3,t_3,h_1)$，广播第一消息，第一消息可以表示为(m_3、h_1、e_3、3、t_3、ID)，其中3为第四条数据m_3的发送序号。

[0116] 其中，哈希运算的操作所需要计算资源少于使用私钥加密的操作所需要的计算资源，所以发送端对目标数据和目标数据对应的节点进行哈希运算得到第一验证码所需要的计算资源较少，这样发送端在发送除首条数据以外的目标数据所需要的计算成本较低，但

数据的安全性不如使用私钥加密的方式，为了保证目标数据的安全性，发送端还发送目标数据对应的节点，以使接收端对该节点进行验证，增加目标数据传输的安全性。

[0117] 在本申请实施例中，发送端可以直接向接收端广播第一消息或第二消息，这样第一消息和第二消息可以不经过服务器转发，减小了第一消息和第二消息传输的延时，提高消息发送的效率。另外，发送端所使用到的数字证书颁发者的私钥信息可以事先从服务器中获取并保存在本地，因此发送端即使在离线场景或网络环境较差的情况下也可以完成消息的广播。由于发送端发送的第一消息中包括目标数据对应哈希链中的节点，哈希链中的节点为单向映射关系，即哈希链中的节点$h_i=H(h_{i-1})$，只能由节点h_{i-1}推算出节点h_i，不能由节点h_i推算出节点h_{i-1}。目标数据对应的节点是根据目标数据的发送序号确定的，这样发送端在当前发送周期内连续发送多条第一消息时，可以使接收端根据每条第一消息中节点验证每条第一消息的连续性，提高消息传输的安全性。

[0118] 参见图3，本申请实施例提供了一种验证消息的方法，该方法可以应用于图1-1所示的通信系统，其执行主体可以为接收端，用于接收图2-1所示的实施例发送的消息，该方法包括：

[0119] 步骤301：接收端接收消息，确定该消息为第二消息，第二消息包括首条数据、该首条数据对应的哈希链中的头节点、第二验证码和验证信息，该验证信息为数字证书，该数字证书包括公钥信息。

[0120] 可选的，第二消息还可以包括发送首条数据的第二时间戳和首条数据在目标发送周期中的发送序号。

[0121] 可选的，发送端广播的消息可能是包括首条数据的第二消息，也可能是包括除首条数据以外的其他目标数据的第一消息。接收端在接收到该消息，根据该消息中的发送序号确定接收的消息是第二消息或为第一消息。

[0122] 例如，接收端接收消息，假设该消息为(cert、e_0、m_0、h_3、t_0、0)，根据该消息中的发送序号0，确定该消息为第二消息。其中，在第二消息中cert为数字证书，e_0为第二验证码，m_0为首条数据，h_3为哈希链的头节点，t_0为第二时间戳，首条数据的发送序号为0。

[0123] 步骤302：接收端使用数字证书颁发者的公钥信息验证该数字证书，在验证数字证书通过时，执行步骤303。

[0124] 可选的，接收端验证数字证书的过程可以为：接收端从该数字证书中获取数字签名，使用数字证书颁发者的公钥信息对该数字签名进行解密得到第三哈希值；对该数字证书中除该数字签名以外的其他部分进行哈希运算得到第四哈希值，如果第三哈希值等于第四哈希值，则对该数字证书验证通过，如果第三哈希值不等于第四哈希值，则对该数字证书验证不通过。

[0125] 可选的，接收端可以事先从服务器中获取证书颁发者的公钥信息，然后在本地保存证书颁发者的公钥信息，所以接收端可以直接使用本地保存的证书颁发者的公钥信息对数字签名进行解密。或者，接收端可以从服务器中获取证书颁发者的公钥信息，使用证书颁发者的公钥信息对该数字签名进行解密。

[0126] 可选的，接收端中包括消息缓存区，接收端在接收到消息时，可以不立即执行步骤302的操作，而是将该消息缓存在消息缓存区中；在接收消息的时间长度达到第二阈值时，对接收到的Z个消息中的数字证书进行验证，该Z个消息是该消息缓存区中缓存的包括数字

证书的消息，在对该Z个消息中的数字证书进行验证通过时，执行对该Z个消息中的每个消息执行后续步骤303的操作，在对该Z个消息中的数字证书进行验证不通过时，执行对该Z个消息中的每个消息分别执行上述步骤302的操作，Z为大于0的整数，这样实现对该Z个消息中的数字证书进行批量验证，提高了验证效率。

[0127] 可选的，第二阈值可以等于目标发送周期的周期长度。

[0128] 可选的，接收端对接收到的Z个消息中的数字证书进行验证的操作，可以为：

[0129] 对该Z个消息中的数字证书进行哈希运算，得到该Z个消息中的数字证书的哈希值，计算该Z个消息中的数字证书的哈希值的乘积得到第一数值；计算该Z个消息中的数字证书中的数字签名的乘积得到第二数值；在第二数值的e次方等于第一数值时，对Z个消息中的数字证书进行验证通过，e为预设常数。

[0130] 其中，对于每个消息中的数字证书，该消息中的数字证书和该数字证书中的数字签名满足第一关系式：$h(cert)=\sigma^e$，h()为预设的哈希函数，cert为该数字证书，σ为该数字证书中的数字签名。

[0131] 在本步骤中，接收端获取的Z个消息中的数字证书，分别为$cert_1$、$cert_2$、……、$cert_Z$，从数字证书$cert_1$、$cert_2$、……、$cert_Z$中获取Z个数字签名，分别为σ_1、σ_2、……、σ_Z，如果该Z个数字证书和该Z个数字签名满足如下第二关系式，则对该Z个消息中的数字证书验证通过，如果该Z个数字证书和该Z个数字签名不满足如下第二关系式，则对该Z个消息中的数字证书验证不通过。

[0132] 第二关系式为：$h(cert_1)*h(cert_2)\cdots h(cert_Z)=(\sigma_1*\sigma_2\cdots\sigma_Z)^e$，*为乘法运算。

[0133] 可选的，对于该消息缓存区中不包括数字证书的每条消息，分别执行如下步骤303和304的操作。

[0134] 可选的，接收端在执行本步骤之前，还可以获取接收第二消息的第四时间戳，获取第二时间戳与第四时间戳之间的第二差值，在第二差值不超过第一阈值时，执行本步骤的操作。

[0135] 可选的，接收端可以将当前的时间戳作为接收第二消息的第四时间戳。

[0136] 发送端发送完第二消息后，接收端很快就可以接收到第二消息，发送第二消息的第二时间戳和接收第二消息的第四时间戳之间的差值较小，通常小于第一阈值。

[0137] 如果发送端发送第二消息后，第二消息被除接收端以外的其他设备截获，该其他设备可能重复地向接收端发送第二消息，这样接收端重复地处理第二消息，以实现攻击接收端。因此为了避免其他设备不断地攻击接收端，接收端判断第二时间戳与第四时间戳之间的差值是否超过第一阈值，在超过第一阈值时，丢弃第二消息，避免重复处理第二消息，以避免被其他设备不断地攻击；在未超过第一阈值时，执行本步骤的操作。第一阈值可以为1秒或2秒等数值。

[0138] 步骤303：接收端根据该数字证书中的公钥信息对第二验证码进行解密得到第一摘要信息，根据首条数据和首条数据对应的头节点生成第二摘要信息。

[0139] 可选的，接收端可以对首条数据和首条数据对应的头节点进行哈希运算得到第二摘要信息。

[0140] 可选的，接收端可以通过MD5算法对首条数据和首条数据对应的头节点进行哈希运算得到第二摘要信息。

[0141] 可选的，在第二消息中包括第二时间戳时，接收端可以对第二时间戳、首条数据和首条数据对应的头节点进行哈希运算得到第二摘要信息。

[0142] 例如，接收端接收的第二消息为(cert、e_0、m_0、h_3、t_0、0)，假设对数字证书cert验证通过，接收端使用数字证书cert中的公钥信息对应第二验证码e_0进行解密得到第一摘要消息为MD_0。使用MD5算法对首条数据m_0、第二时间戳t_0、首条数据对应的头节点h_3进行哈希运算得到第二摘要信息MD_1。

[0143] 步骤304：在第一摘要信息和第二摘要信息相等时，对首条数据验证通过。

[0144] 例如，在MD_0＝MD_1时，对首条数据m_0验证通过。

[0145] 可选的，在对首条数据验证通过后，接收端还可以保存首条数据对应的头节点。

[0146] 可选的，接收端接收到第二消息后，还继续接收发送端在目标发送周期内发送的各第一消息，详细实现过程为：

[0147] 步骤305：接收端接收消息，确定该消息为第一消息，第一消息包括目标数据、目标数据对应的哈希链中的节点、目标数据在目标发送周期中的发送序号和第一验证码，目标数据是目标发送周期内在发送首条数据之后发送的数据。

[0148] 可选的，第一消息还可以包括发送目标数据的第一时间戳和/或发送端的身份标识信息等。

[0149] 可选的，发送端广播的消息可能是包括首条数据的第二消息，也可能是包括除首条数据以外的其他目标数据的第一消息。接收端在接收到该消息，根据该消息中的发送序号确定接收的消息是第二消息或为第一消息。

[0150] 例如，接收端接收消息，假设该消息为(m_1、h_3、e_1、1、t_1、ID)，根据该消息中的发送序号1，确定该消息为第一消息。其中，在第一消息中m_1为目标发送周期内的第二条数据，t_1为发送第二条数据的第一时间戳，e_1为第一验证码，第二条数据的发送序号为1，h_3为第二条数据对应的节点、ID为发送端的身份标识信息。

[0151] 再例如，假设接收端接收的消息为(m_2、h_2、e_2、2、t_2、ID)，根据该消息中的发送序号2，确定该消息为第一消息。其中，在第一消息中m_2为目标发送周期内的第三条数据，t_2为发送第三条数据的第一时间戳，e_2为第一验证码，第三条数据的发送序号为2，h_2为第三条数据对应的节点。

[0152] 还例如，假设接收端接收的消息为(m_3、h_1、e_3、3、t_3、ID)，根据该消息中的发送序号3，确定该消息为第一消息。在第一消息中m_3为目标发送周期内的第四条数据，t_3为发送第四条数据的第一时间戳，e_3为第一验证码，第四条数据的发送序号为3，h_1为第四条数据对应的节点。

[0153] 步骤306：接收端根据目标数据的发送序号确定已接收的第一数据对应的节点，第一数据是发送端在发送目标数据之前最近发送的数据。

[0154] 可选的，当目标数据为目标发送周期内的第二条数据时，第一数据为目标发送周期内的首条数据。当目标数据为目标发送周期内的发送第二条数据之后的数据时，第一数据为目标发送周期内的发送首条数据之后的数据。

[0155] 例如，假设接收的第一消息为(m_1、h_3、e_1、1、t_1、ID)，根据目标数据m_1对应的发送序号1确定第一数据为首条数据m_0，以及确定第一数据对应的节点为头节点h_3。

[0156] 再例如，假设接收的第一消息为(m_2、h_2、e_2、2、t_2、ID)，根据目标数据m_2对应的发送

序号2确定第一数据为目标发送周期内的第二条数据m_1，以及确定第一数据对应的节点为头节点h_3。

[0157] 还例如，假设接收的第一消息为(m_3、h_1、e_3、3、t_3、ID)，根据目标数据m_3对应的发送序号3确定第一数据为目标发送周期内的第三条数据m_2，以及确定第一数据对应的节点为哈希链的第二个节点h_2。

[0158] 步骤307：接收端根据第一数据对应的节点对目标数据对应的节点进行验证。

[0159] 可选的，在第一数据为首条数据时，当目标数据对应的节点与首条数据对应的节点相等时，对目标数据对应的节点验证通过。

[0160] 例如，在第一数据为首条数据m_0时，目标数据为m_1，其中目标数据m_1对应的节点h_3与首条数据对应的头节点h_3相等，所以对目标数据m_1对应的节点h_3验证通过。

[0161] 可选的，在第一数据为目标发送周期内发送首条数据之后发送的数据时，对目标数据对应的节点进行哈希运算得到第二哈希结果，当第二哈希结果与第一数据对应的节点相等时，对目标数据对应的节点验证通过。

[0162] 例如，在第一数据为目标发送周期内的第二条数据m_1时，目标数据为m_2，对目标数据m_2对应的节点h_2进行哈希运算得到的第二哈希结果$H(h_2)$，且第二哈希结果$H(h_2)$等于第二条数据m_1对应的节点h_3相等，所以对目标数据m_2对应的节点h_2验证通过。

[0163] 再例如，在第一数据为目标发送周期内的第三条数据m_2时，目标数据为m_3，对目标数据m_3对应的节点h_1进行哈希运算得到的第二哈希结果$H(h_1)$，且第二哈希结果$H(h_1)$等于第三条数据m_3对应的节点h_2相等，所以对目标数据m_3对应的节点h_1验证通过。

[0164] 由于接收端接收的消息中包括目标数据对应哈希链的节点，哈希链中的节点为单向映射关系，即哈希链中的节点$h_i=H(h_{i-1})$，只能由节点h_{i-1}推算出节点h_i，不能由节点h_i推算出节点h_{i-1}。接收端利用最近上一次接收收的哈希链中的节点验证目标数据对应的节点，这样可以验证出接收端连续接收的消息是否连续，从而提高安全性。

[0165] 步骤308：在对目标数据对应的节点验证通过时，接收端对目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果。

[0166] 接收端可以采用预设第二哈希函数对目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果。

[0167] 可选的，在第一消息中包括第一时间戳时，接收端可以对第一时间戳、目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果。

[0168] 步骤309：在第一哈希结果等于第一验证码时，对目标数据验证通过。

[0169] 其中，通过对目标数据对应的节点进行验证可以保证消息传输的安全性，接收端对目标数据对应的节点进行验证的速度较快且所需要的计算资源较少，哈希运算得到第一哈希结果所需要的计算资源少于解密所需要的计算资源，且哈希运算的速度快于解密的速度，所以不仅保证了消息传输的安全性，还提高验证的速度。

[0170] 例如，假设接收的第一消息为(m_1、h_3、e_1、1、t_1、ID)，目标数据为目标发送周期内的第二条数据m_1，接收端对第一时间戳t_1、第二条数据m_1和第二条数据对应的节点h_3进行哈希运算得到第一哈希结果$f1=MAC(t_1,m_1,h_3)$，在第一哈希结果f1与第一验证码e_1相同时，对第二条数据m_1验证通过。

[0171] 再例如，假设接收的第一消息为(m_2、h_2、e_2、2、t_2、ID)，目标数据为目标发送周期内

的第三条数据m_2，接收端对第一时间戳t_2、第三条数据m_2和第三条数据对应的节点h_2进行哈希运算得到第一哈希结果f2＝MAC(t_2,m_2,h_2)，在第一哈希结果f2与第一验证码e_2相同时，对第三条数据m_2验证通过。

[0172] 还例如，假设接收的第一消息为(m_3、h_1、e_3、3、t_3、ID)，目标数据为目标发送周期内的第四条数据m_3，接收端对第一时间戳t_3、第四条数据m_3和第四条数据对应的节点h_1进行哈希运算得到第一哈希结果f3＝MAC(t_3,m_3,h_1)，在第一哈希结果f3与第一验证码e_3相同时，对第四条数据m_3验证通过。

[0173] 可选的，接收端对首条数据验证通过后可以处理首条数据，对目标数据验证通过后，可以处理目标数据。

[0174] 接收端处理首条数据或目标数据的方式可以为播放首条数据或目标数据，或者显示首条数据或目标数据等。

[0175] 可选的，由于第二消息中的数字证书中也包括发送端的身份标识信息，以及第一消息中包括发送端的身份标识信息，发送端的身份标识信息包括发送端的设备类型、设备生产商标识信息、设备生产日期和生产序号等信息，接收端可以直接从发送端的身份标识信息中提取这些信息，可以显示或播放这些信息，这样接收端不需要从网络中查询这些信息。

[0176] 在本申请实施例中，接收端可以直接接收发送端广播的消息，这样该消息可以不经过服务器转发，减小了该消息传输的延时，提高消息发送的效率。另外，接收端所使用到的数字证书颁发者的公钥信息可以事先从服务器中获取并保存在本地，因此接收端即使在离线场景或网络环境较差的情况下也可以完成消息的解析。由于发送端发送的消息中包括目标数据对应哈希链中的节点，哈希链中的节点为单向映射关系，即哈希链中的节点h_i＝H(h_{i-1})，只能由节点h_{i-1}推算出节点h_i，不能由节点h_i推算出节点h_{i-1}。目标数据对应的节点是根据目标数据的发送序号确定的，这样发送端在当前发送周期内连续发送多条消息时，接收端根据每条消息中节点验证每条消息的连续性，提高了消息传输的安全性。

[0177] 参见图4，本申请实施例提供了一种发送消息的方法，该方法可以应用于图1-1所示的通信系统，该方法的执行主体为该通信系统的发送端，包括：

[0178] 步骤401：发送端将其身份标识信息确定为公钥信息，并生成与该公钥信息相匹配的私钥信息。

[0179] 在本步骤中，发送端可以采用基于身份的签名机制(identity-based signature，IBS)方式获取公钥信息和私钥信息。IBS的方式为：发送端获取其自身的身份标识信息，将该身份标识信息作为公钥信息，基于该身份标识信息生成私钥信息。

[0180] 可选的，发送端采用IBS方式生成私钥信息的实现方式有多种，在本步骤中列举了如下一种实现方式。通过该实现方式生成的私钥信息包括第一私钥和第二私钥。该实现方式可以为：

[0181] 发送端可以事先接收服务器广播的乘法群的生成元g、乘法群的素数q和第一随机数x，然后保存在本地。这样在生成私钥信息时，可以生成小于该素数q的第二随机数r；根据该生成元g和第二随机数r获取第一私钥R，其中第一私钥R＝g^r；根据发送端的身份标识信息ID、第一私钥R、第一随机值x、第二随机值r，生成第二私钥Q，其中，第二私钥Q＝r+x*h1(ID,R)，其中h1()为预设的第三哈希函数。所以生成的私钥信息可以表示为(第一私钥R，

第二私钥Q)。

[0182] 服务器中事先预设一个乘法群,服务器可以获取该乘法群的生成元g和素数q,素数q为该乘法群中包括的元素数目,生成小于该素数q的第一随机数x;然后服务器广播该生成元g、该素数q和第一随机数x,发送端可以接收并保存该生成元g、该素数q和第一随机数x。这样发送端在生成私钥信息时可以获取本地保存的该生成元g、该素数q和第一随机数x,然后再生成私钥信息。或者,在生成私钥信息时,发送端也可以临时从服务器中获取该生成元g、该素数q和第一随机数x,然后再生成私钥信息。

[0183] 发送端的身份标识信息可以在发送端出厂时设置在发送端中。所以发送端可以从其本地获取其身份标识信息。

[0184] 关于发送端的身份标识信息的结构可以参见见图2-1所示实施例的步骤201中的相关内容,在此不再详细说明。

[0185] 步骤402:发送端获取当前发送周期内待发送的首条数据。

[0186] 可选的,首条数据可以是用户输入到发送端的数据,所以发送端可以接收用户输入的首条数据。

[0187] 在发送端中发送周期周期性循环。可选的,发送端可以定义一个周期长度,可以使用计时器来实现该发送周期。例如,发送端可以启动一个计时器,设置该计时器从零开始计时,表示一个发送周期开始;当该计时器计时的时间达到该周期长度时,重新设置该计时器从零开始计时,表示该一个发送周期结束且另一个发送周期开始,如此循环往复,实现发送周期周期性循环。

[0188] 对于每个发送周期,发送端可以记录在该发送周期内已发送的数据的发送序号。所以在当前发送周期内,当发送端接收到用户输入的数据时,发送端检测到本地有没有保存在当前发送周期内已发送的数据的发送序号,如果检测结果是没有保存,则确定该数据是当前发送周期的首条数据,如果检测结果是有保存,则确定该数据不是当前发送周期内的首条数据。

[0189] 步骤403发送端通过该私钥信息对该首条数据和哈希链的头节点进行签名得到第二验证码。

[0190] 可选的,发送端还可以获取当前的第二时间戳,第二时间戳实质是发送端发送首条数据的时间戳,可以通过该私钥信息对第二时间戳、该首条数据和哈希链的头节点进行签名得到第二验证码。

[0191] 可选的,哈希链包括的节点数目等于一个发送周期内允许发送的数据数目。哈希链中任意相邻的两个节点,为了便于说明称该任意相邻的两个节点分别为第一节点和第二节点,第一节点靠近哈希链的头节点,第一节点是基于第二节点推算出来的。

[0192] 可选的,一个发送周期可以对应一个哈希链,或者,m个发送周期可以对应一个哈希链,m为大于1的整数。

[0193] 当一个发送周期对应一个哈希链时,发送端在对首条数据和哈希链的头节点进行签名之前,还生成哈希链。

[0194] 当m个发送周期对应一个哈希链时,如果最近上次生成哈希链的时间所在的发送周期和当前发送周期间隔m-1个发送周期,则发送端在对首条数据和哈希链的头节点进行签名之前,还生成哈希链;如果最近上次生成哈希链的时间所在的发送周期和当前发送周

期间隔少于m-1个发送周期，发送端在对首条数据和哈希链的头节点进行签名之前，获取最近上一次生成的哈希链。

[0195] 在本步骤中，发送端可以根据该首条数据和哈希链的头节点生成第一摘要消息，使用该私钥信息对第一摘要消息进行加密得到第二验证码，第二验证码包括第一签名、第二签名和第一私钥。

[0196] 可选的，在对第一摘要消息进行加密时，发送端生成小于该元素数目q的第三随机数t，根据该生成元g和第三随机数t获取第一签名T，其中第一签名$T=g^t$；根据第一摘要信息MD、第一私钥R、第二私钥Q、第三随机值t和第一签名T，生成第二签名S，其中，第二签名S＝t+Q*h2(MD,T,R)，其中h2()为预设的第四哈希函数。所以生成的第二验证码可以表示为(第一签名T,第二签名S,第一私钥R)。

[0197] 步骤404：发送端发送第二消息，第二消息包括该公钥信息、第二验证码、该首条数据和哈希链的头节点。

[0198] 可选的，发送端可以广播第二消息。

[0199] 可选的，第二消息还可以包括第二时间戳和首条数据在当前发送周期内的发送序号。

[0200] 可选的，发送端在发送当前发送周期内除首条数据以外的其他待发送的目标数据时，发送端发送过程如下：

[0201] 步骤405-步骤408：分别步骤205至208相同，在此不再详细说明。

[0202] 在本申请实施例中，发送端可以直接向接收端广播第一消息或第二消息，这样第一消息和第二消息可以不经过服务器转发，减小了第一消息和第二消息传输的延时，提高消息发送的效率。另外，由于发送端发送的第一消息中包括目标数据对应哈希链中的节点，哈希链中的节点为单向映射关系，目标数据对应的节点是根据目标数据的发送序号确定的，这样发送端在当前发送周期内连续发送多条第一消息时，可以使接收端根据每条第一消息中节点验证每条第一消息的连续性，对于不连续的第一消息可能是其他设备伪造发送端的消息，使接收端及时验证出伪造的第一消息，提高了消息传输的安全性。

[0203] 参见图5，本申请实施例提供了一种验证消息的方法，该方法可以应用于图1-1所示的通信系统，其执行主体可以为接收端，用于接收图4所示的实施例发送的消息，该方法包括：

[0204] 步骤501：接收端接收消息，确定该消息为第二消息，第二消息包括首条数据、该首条数据对应的哈希链中的头节点、第二验证码和公钥信息。

[0205] 该公钥信息可以为发送端的身份标识信息。

[0206] 可选的，第二消息还可以包括发送首条数据的第二时间戳和首条数据在目标发送周期中的发送序号。

[0207] 可选的，发送端发送的消息可能是包括首条数据的第二消息，也可能是包括除首条数据以外的其他目标数据的第一消息。接收端在接收到该消息，根据该消息中的发送序号确定接收的消息是第二消息或为第一消息。

[0208] 可选的，接收端中包括消息缓存区，接收端在接收到消息时，该消息无论是第一消息，还是第二消息，可以先将该消息缓存在消息缓存区中；在接收消息的时间长度达到第一阈值时，同时对接收到的Z个第二消息进行验证，该Z个消息是消息缓存区中缓存的第二消

息，在同时对该Z个第二消息验证通过时，可以直接处理该Z个第二消息中的首条数据，在没有同时对该Z个第二消息验证通过时，对该Z个第二消息中的每个第二消息执行后续步骤502的操作，Z为大于0的整数，这样实现对该Z个第二消息中的第二验证码进行批量验证，提高了验证效率。

[0209] 可选的，接收端同时对接收到的Z个第二消息进行验证的操作，可以包括如下521至523的操作，分别为：

[0210] 521：接收端根据预设乘法群的生成元和该Z个第二消息中的第二验证码获取该Z个第二消息的第三数值。

[0211] 该乘法群的生成元可以预设在服务器或预设在接收端中。接收端可以事先接收服务器广播的乘法群的生成元g和第一随机数x，还可以根据该生成元g和第一随机数x生成主公钥值y，主公钥值$y=g^{x}$。

[0212] 这样在执行本步骤的操作时，对于该Z个第二消息中的每个第二消息，该第二消息的第二验证码可以表示为(第一签名T、第二签名S和第一私钥R)，根据该第二签名S和该生成元g获取该第二消息对应的第三数值A，第三数值为$A=g^{S}$；按上述方式获取每个第二消息对应的第三数值，分别为w_1、w_2、……、w_Z。

[0213] 522：接收端根据每个第二消息和每个第二消息中的第二验证码获取每个第二消息的第四数值。

[0214] 对于每个第二消息，对该第二消息包括的发送端的身份标识信息ID和该第一私钥R进行哈希运算得到该第二消息的第一哈希值w，w＝H1(ID,R)；对该第二消息、该第二消息包括的发送端的身份标识信息ID、该第一签名T和第一私钥R进行哈希运算得到该第二消息的第二哈希值v，v＝H2(Message,T,R,ID)，H1()和H2()为两个哈希函数，Message为该第二消息；根据该第一签名T、第一私钥R、主公钥值y、第一哈希值w和第二哈希值v获取该第二消息对应的第四数值B，第四数值$B=T*R^{w}*y^{w*v}$。按上述方式获取每个第二消息对应的第四数值，分别为v_1、v_2、……、v_Z。

[0215] 523：在该Z个第二消息对应的第三数值的乘积等于该Z个第二消息对应的第四数值的乘积时，对接收到的Z个第二消息验证通过，即$w_1*w_2*……*w_Z=v_1*v_2*……*v_Z$时，对接收到的Z个第二消息同时验证通过。

[0216] 步骤502：接收端根据该公钥信息对第二验证码进行解密得到第一摘要信息，根据该首条数据和该首条数据对应的头节点生成第二摘要信息。

[0217] 可选的，接收端在执行本步骤之前，还可以获取接收第二消息的第四时间戳，获取第二消息中的第二时间戳与第四时间戳之间的第二差值，在第二差值不超过第一阈值时，执行本步骤的操作。

[0218] 可选的，接收端可以将当前的时间戳作为接收第二消息的第四时间戳。

[0219] 发送端发送完第二消息后，接收端很快就可以接收到第二消息，发送第二消息的第二时间戳和接收第二消息的第四时间戳之间差值较小，通常小于第一阈值。

[0220] 如果发送端发送第二消息后，第二消息被除接收端以外的其他设备截获，该其他设备可能重复地向接收端发送第二消息，这样接收端重复地处理第二消息，以实现攻击接收端。因此为了避免其他设备不断攻击接收端，接收端判断第二时间戳与第四时间戳之间的第二差值是否超过第一阈值，在超过第一阈值时，丢弃第二消息，避免重复处理第二消

息,以避免被其他设备不断攻击;在未超过第一阈值时,执行本步骤的操作。

[0221] 步骤503:在第一摘要信息和第二摘要信息相等时,对第二消息中的首条数据验证通过。

[0222] 可选的,接收端接收到第二消息后,还继续接收发送端在目标发送周期内发送的各第一消息,详细实现过程为:

[0223] 步骤504-步骤508:分别与步骤305-步骤309相同,在此不再详细说明。

[0224] 在本申请实施例中,接收端可以直接接收发送端广播的消息,这样该消息可以不经过服务器转发,减小了该消息传输的延时,提高消息发送的效率。另外,由于发送端发送的消息中包括目标数据对应哈希链中的节点,哈希链中的节点为单向映射关系,目标数据对应的节点是根据目标数据的发送序号确定的,这样发送端在当前发送周期内连续发送多条消息时,接收端根据每条消息中节点验证每条消息的连续性,提高了消息传输的安全性。

[0225] 参见图6,本申请实施例提供了一种发送消息的装置600,所述装置600可以是上述任一实施例的发送端或发送端中的部分,包括:

[0226] 处理单元601,用于获取待发送的目标数据,目标数据是当前发送周期内在发送首条数据之后待发送的数据;根据目标数据在当前发送周期内的发送序号从哈希链中获取目标数据对应的节点,哈希链包括的节点数目等于当前发送周期内允许发送的数据数目;对目标数据和目标数据对应的节点进行哈希运算得到第一验证码,第一验证码用于接收端验证目标数据;

[0227] 发送单元602,用于发送第一消息,第一消息包括目标数据、目标数据对应的节点、第一验证码和目标数据的发送序号。

[0228] 可选的,处理单元601,还用于:

[0229] 随机生成哈希链的尾节点;

[0230] 对哈希链中的节点h_{i-1}进行哈希运算得到哈希链中的节点h_i,i=1、2、……、N,N+1为当前发送周期内允许发送的数据数目,节点h_0为所述尾节点,节点h_N为哈希链的头节点。

[0231] 可选的,处理单元601,用于:

[0232] 在根据目标数据的发送序号确定目标数据是当前发送周期内待发送的第二条数据时,获取哈希链的头节点作为目标数据对应的节点;

[0233] 在根据目标数据的发送序号确定目标数据是位于所述第二条数据之后待发送的数据时,获取哈希链中位于第三节点之后且与第三节点相邻的第四节点作为目标数据对应的节点,第三节点是最近上一次发送的哈希链中的节点。

[0234] 可选的,第一消息还包括发送目标数据的第一时间戳。

[0235] 可选的,处理单元601,还用于通过私钥信息对首条数据和哈希链的头节点进行签名得到第二验证码,第二验证码用于接收端对首条数据进行验证;

[0236] 发送单元602,还用于发送第二消息,第二消息包括验证信息、首条数据、第二验证码和首条数据对应的节点,验证信息包括与该私钥信息相匹配的公钥信息。

[0237] 可选的,处理单元601,用于:

[0238] 根据首条数据和所述哈希链的头节点生成第一摘要信息;

[0239] 使用私钥信息对第一摘要信息进行签名得到第二验证码。

[0240] 可选的,第二消息还包括发送目标数据的第二时间戳。

[0241] 可选的，该验证信息为数字证书，该数字证书包括公钥信息；或者，该验证信息为公钥信息，该公钥信息为发送端的身份标识信息。

[0242] 在本申请实施例中，发送单元可以直接向接收端发送第一消息或第二消息，这样第一消息和第二消息可以不经过服务器转发，减小了第一消息和第二消息传输的延时，提高消息发送的效率。另外，由于发送的消息中包括目标数据对应哈希链中的节点，哈希链中的节点为单向映射关系，目标数据对应的节点是根据目标数据的发送序号确定的，这样发送单元在当前发送周期内连续发送多条消息时，可以使接收端根据每条消息中节点验证每条消息的连续性，对于不连续的消息可能是其他设备伪造发送端的消息，使接收端及时验证出伪造的消息，提高了消息传输的安全性。

[0243] 参见图7，本申请实施例提供了一种验证消息的装置700，所述装置700可以是上述任一实施例的接收端或接收端中的部分，包括：

[0244] 接收单元701，用于接收第一消息，第一消息包括目标数据、目标数据对应的哈希链中的一个节点、第一验证码和目标数据在目标发送周期中的发送序号，目标数据是目标发送周期内在发送首条数据之后发送的数据，哈希链包括的节点数目等于目标发送周期内允许发送的数据数目；

[0245] 处理单元702，用于根据目标数据对应的节点、目标数据对应的发送序号和第一验证码对目标数据进行验证。

[0246] 可选的，处理单元702，用于：

[0247] 根据目标数据的发送序号确定已接收的第一数据对应的节点，第一数据是发送端在发送目标数据之前最近发送的数据；

[0248] 根据第一数据对应的节点对目标数据对应的节点进行验证；

[0249] 在验证目标数据对应的节点通过时，对目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果；

[0250] 在第一哈希结果与第一验证码匹配时，对目标数据验证通过。

[0251] 可选的，第一数据为首条数据，首条数据对应的节点为哈希链的头节点，处理单元702，用于当目标数据对应的节点与首条数据对应的头节点相等时，对目标数据对应的节点验证通过。

[0252] 可选的，第一数据为所述目标发送周期内在发送首条数据之后发送的数据，处理单元702，用于：

[0253] 对目标数据对应的节点进行哈希运算得到第二哈希结果；

[0254] 在第二哈希结果与第一数据对应的节点相等时，对目标数据对应的节点验证通过。

[0255] 可选的，第一消息还包括发送目标数据的第一时间戳；

[0256] 处理单元702，用于：

[0257] 获取第一时间戳和接收目标数据的第三时间戳之间的第一差值；

[0258] 在第一差值不超过第一阈值时，根据目标数据对应的节点、目标数据对应的发送序号和第一验证码对目标数据进行验证。

[0259] 可选的，接收单元701，还用于接收第二消息，第二消息包括首条数据、首条数据对应的哈希链的头节点、第二验证码和验证信息，验证信息包括公钥信息；

[0260] 处理单元702，还用于根据第二验证码和该公钥信息对首条数据进行验证。

[0261] 可选的，处理单元702，用于：

[0262] 使用该公钥信息对第二验证码进行解密得到第一摘要信息；

[0263] 根据首条数据和首条数据对应的头节点生成第二摘要信息；

[0264] 在第一摘要信息与第二摘要信息匹配时，对首条数据验证通过。

[0265] 可选的，验证信息为数字证书，数字证书包括该公钥信息，

[0266] 处理单元702，用于：

[0267] 使用数字证书的颁发者公钥信息验证所述数字证书；

[0268] 在验证数字证书通过后，使用该公钥信息对所述第二验证码进行解密得到第一摘要信息。

[0269] 可选的，处理单元702，用于：

[0270] 将第二消息缓存在消息缓存区中；

[0271] 在接收消息的时间长度达到第二阈值时，对接收到的Z个消息中的数字证书进行验证，所述Z个消息是消息缓存区中缓存的包括数字证书的消息，Z为大于0的整数；

[0272] 在对Z个消息中的数字证书进行验证未通过时，使用数字证书的颁发者公钥信息验证所述数字证书。

[0273] 可选的，处理单元702，用于：

[0274] 对Z个消息中的数字证书进行哈希运算，得到Z个消息中的数字证书的哈希值；

[0275] 计算Z个消息中的数字证书的哈希值的乘积得到第一数值；

[0276] 计算Z个消息中的数字证书中的数字签名的乘积得到第二数值；

[0277] 在第二数值的e次方等于第一数值时，对Z个消息中的数字证书进行验证通过。

[0278] 可选的，第二消息还包括发送首条数据的第二时间戳；

[0279] 处理单元702，用于：

[0280] 获取第二时间戳和接收首条数据的第四时间戳之间的第二差值；

[0281] 在第二差值不超过第一阈值时，根据第二验证码和该公钥信息对首条数据进行验证。

[0282] 可选的，处理单元702，用于：

[0283] 将第二消息缓存在消息缓存区中；

[0284] 在接收消息的时间长度达到第二阈值时，同时对接收到的Z个第二消息进行验证，Z个第二消息是消息缓存区中缓存的第二消息；

[0285] 在同时对Z个第二消息验证不通过时，根据第二验证码和该公钥信息对首条数据进行验证。

[0286] 在本申请实施例中，接收单元可以直接接收发送端发送的消息，这样该消息可以不经过服务器转发，减小了该消息传输的延时，提高消息发送的效率。另外，由于发送端发送的消息中包括目标数据对应哈希链中的节点，哈希链中的节点为单向映射关系，目标数据对应的节点是根据目标数据的发送序号确定的，这样发送端在当前发送周期内连续发送多条消息时，处理单元根据每条消息中节点验证每条消息的连续性，提高了消息传输的安全性。

[0287] 参见图8，图8所示为本申请实施例提供的一种发送消息的装置800示意图。该装置

800包括至少一个处理器801,总线系统802,存储器803以及至少一个收发器804。

[0288] 该装置800是一种硬件结构的装置,可以用于实现图6所述的装置中的功能模块。例如,本领域技术人员可以想到图6所示的装置600中的处理单元601可以通过该至少一个处理器801调用存储器803中的代码来实现,图6所示的装置600中的发送单元602可以通过该收发器804来实现。

[0289] 可选的,该装置800还可用于实现上述任一实施例中发送端的功能。

[0290] 可选的,上述处理器801可以是一个通用中央处理器(central processing unit,CPU),微处理器,特定应用集成电路(application-specific integrated circuit,ASIC),或一个或多个用于控制本申请方案程序执行的集成电路。

[0291] 上述总线系统802可包括一通路,在上述组件之间传送信息。

[0292] 上述收发器804,用于与其他设备或通信网络通信。

[0293] 上述存储器803可以是只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(electrically erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0294] 其中,存储器803用于存储执行本申请方案的应用程序代码,并由处理器801来控制执行。处理器801用于执行存储器803中存储的应用程序代码,从而实现本专利方法中的功能。

[0295] 在具体实现中,作为一种实施例,处理器801可以包括一个或多个CPU,例如图8中的CPU0和CPU1。

[0296] 在具体实现中,作为一种实施例,该装置800可以包括多个处理器,例如图8中的处理器801和处理器807。这些处理器中的每一个可以是一个单核(single-CPU)处理器,也可以是一个多核(multi-CPU)处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据(例如计算机程序指令)的处理核。

[0297] 在具体实现中,作为一种实施例,该装置800还可以包括输出设备805和输入设备806。输出设备805和处理器801通信,可以以多种方式来显示信息。例如,输出设备805可以是液晶显示器(liquid crystal display,LCD)等。输入设备806和处理器801通信,可以以多种方式接受用户的输入。例如,输入设备806可以是触摸屏设备或传感设备等。

[0298] 参见图9,图9所示为本申请实施例提供的一种验证消息的装置900示意图。该装置900包括至少一个处理器901,总线系统902,存储器903以及至少一个收发器904。

[0299] 该装置900是一种硬件结构的装置,可以用于实现图7所述的装置中的功能模块。例如,本领域技术人员可以想到图7所示的装置700中的处理单元702可以通过该至少一个处理器901调用存储器903中的代码来实现,图7所示的装置700中的接收单元701可以通过该收发器904来实现。

[0300] 可选的,该装置900还可用于实现上述任一实施例中发送端的功能。

[0301] 可选的,上述处理器901可以是一个通用中央处理器(central processing unit,CPU),微处理器,特定应用集成电路(application-specific integrated circuit,ASIC),或一个或多个用于控制本申请方案程序执行的集成电路。

[0302] 上述总线系统902可包括一通路,在上述组件之间传送信息。

[0303] 上述收发器904,用于与其他设备或通信网络通信。

[0304] 上述存储器903可以是只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(electrically erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0305] 其中,存储器903用于存储执行本申请方案的应用程序代码,并由处理器801来控制执行。处理器901用于执行存储器903中存储的应用程序代码,从而实现本专利方法中的功能。

[0306] 在具体实现中,作为一种实施例,处理器901可以包括一个或多个CPU,例如图9中的CPU0和CPU1。

[0307] 在具体实现中,作为一种实施例,该装置900可以包括多个处理器,例如图9中的处理器801和处理器907。这些处理器中的每一个可以是一个单核(single-CPU)处理器,也可以是一个多核(multi-CPU)处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据(例如计算机程序指令)的处理核。

[0308] 在具体实现中,作为一种实施例,该装置900还可以包括输出设备905和输入设备906。输出设备905和处理器901通信,可以以多种方式来显示信息。例如,输出设备905可以是液晶显示器(liquid crystal display,LCD)等。输入设备906和处理器901通信,可以以多种方式接受用户的输入。例如,输入设备806可以是触摸屏设备或传感设备等。

[0309] 参见图10,本申请实施例提供了一种通信系统1000,所述通信系统1000包括:图6所述的装置和图7所述的装置,或者,图8所述的装置和图9所述的装置。在实现时,图6所述的装置或图8所述的装置可以为发送端,以及,图7所述的装置或图9所述的装置可以为接收端。

[0310] 上述本申请实施例序号仅仅为了描述,不代表实施例的优劣。

[0311] 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。

[0312] 以上所述仅为本申请的可选实施例,并不用以限制本申请,凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

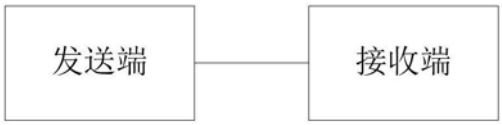


图1-1

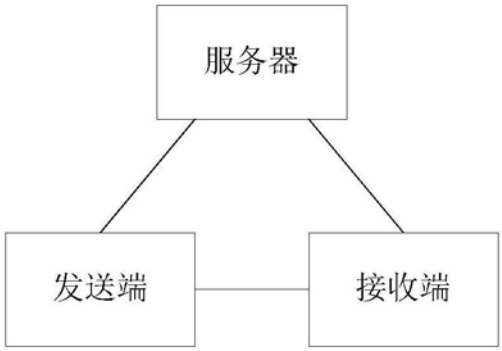


图1-2

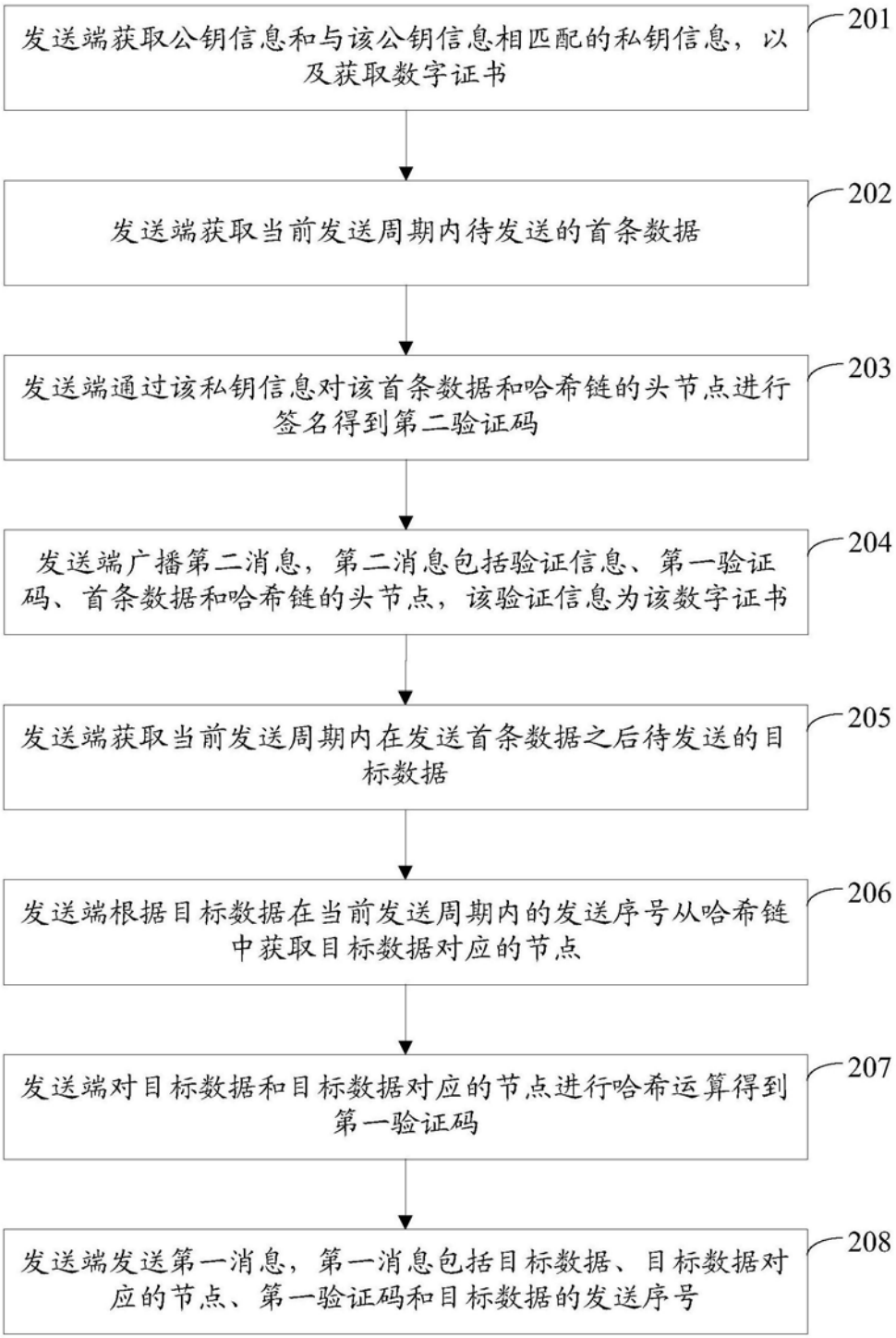

发送端获取公钥信息和与该公钥信息相匹配的私钥信息，以及获取数字证书
201
发送端获取当前发送周期内待发送的首条数据
202
发送端通过该私钥信息对该首条数据和哈希链的头节点进行签名得到第二验证码
203
发送端广播第二消息，第二消息包括验证信息、第一验证码、首条数据和哈希链的头节点，该验证信息为该数字证书
204
发送端获取当前发送周期内在发送首条数据之后待发送的目标数据
205
发送端根据目标数据在当前发送周期内的发送序号从哈希链中获取目标数据对应的节点
206
发送端对目标数据和目标数据对应的节点进行哈希运算得到第一验证码
207
发送端发送第一消息，第一消息包括目标数据、目标数据对应的节点、第一验证码和目标数据的发送序号
208

图2-1

<table>
<tr><td colspan="2">Version</td></tr>
<tr><td colspan="2">Serial Number</td></tr>
<tr><td colspan="2">Signature Algorithm ID</td></tr>
<tr><td colspan="2">Issuer(CA)X500 Name</td></tr>
<tr><td colspan="2">Validity Period</td></tr>
<tr><td colspan="2">Subject X500 Name</td></tr>
<tr><td rowspan="2">Subject Public Key Info</td><td>Algorithm ID</td></tr>
<tr><td>Public Key Value</td></tr>
<tr><td colspan="2">Issuer Unique ID</td></tr>
<tr><td colspan="2">Subject Unique ID</td></tr>
<tr><td colspan="2">Extension</td></tr>
<tr><td colspan="2">CA Digital Signature</td></tr>
</table>

图2-2

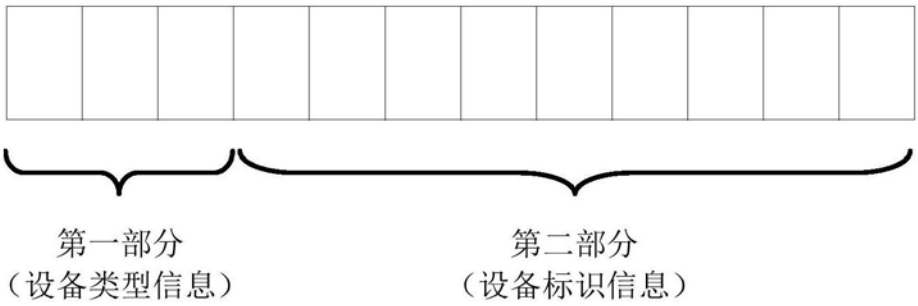


图2-3

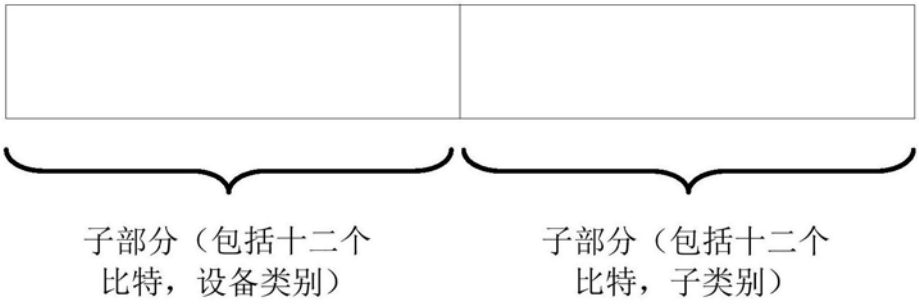

子部分（包括十二个
比特，设备类别）
子部分（包括十二个
比特，子类别）

图2-4


第一子部分
（设备生产商标识信息）
第二子部分
（生产日期）
第三子部分
（生产序号）

图2-5

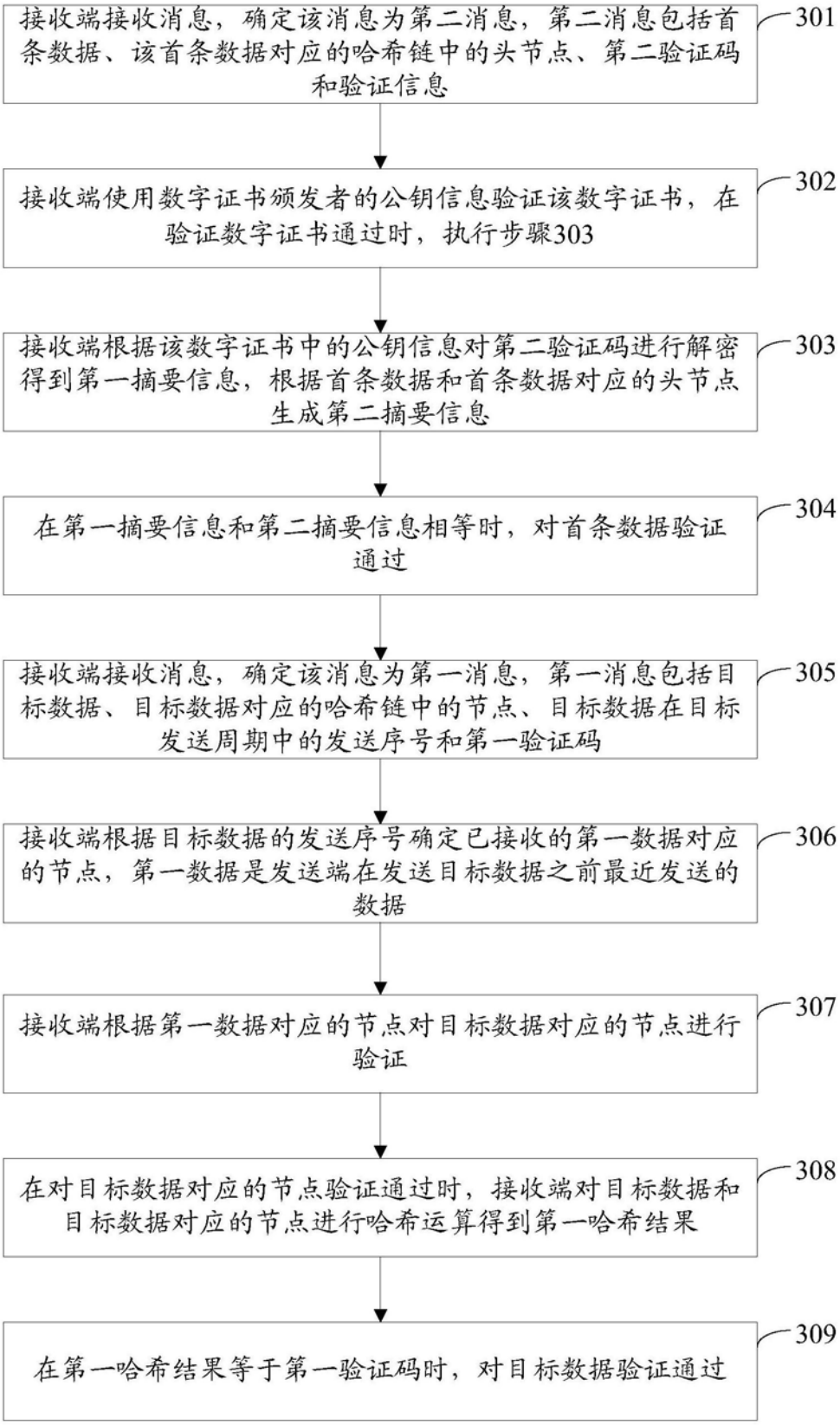

接收端接收消息，确定该消息为第二消息，第二消息包括首条数据、该首条数据对应的哈希链中的头节点、第二验证码和验证信息
301
接收端使用数字证书颁发者的公钥信息验证该数字证书，在验证数字证书通过时，执行步骤303
302
接收端根据该数字证书中的公钥信息对第二验证码进行解密得到第一摘要信息，根据首条数据和首条数据对应的头节点生成第二摘要信息
303
在第一摘要信息和第二摘要信息相等时，对首条数据验证通过
304
接收端接收消息，确定该消息为第一消息，第一消息包括目标数据、目标数据对应的哈希链中的节点、目标数据在目标发送周期中的发送序号和第一验证码
305
接收端根据目标数据的发送序号确定已接收的第一数据对应的节点，第一数据是发送端在发送目标数据之前最近发送的数据
306
接收端根据第一数据对应的节点对目标数据对应的节点进行验证
307
在对目标数据对应的节点验证通过时，接收端对目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果
308
在第一哈希结果等于第一验证码时，对目标数据验证通过
309

图3

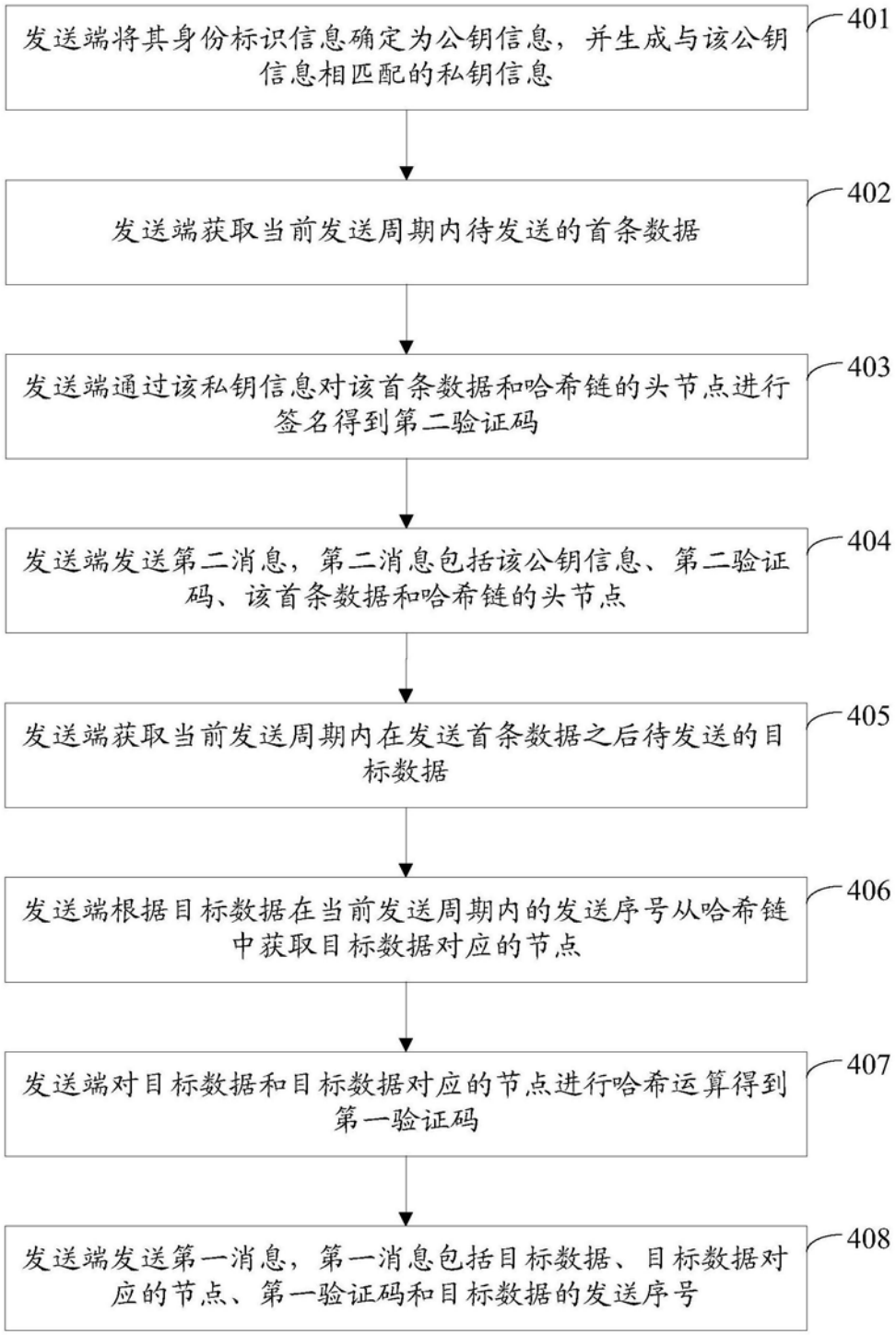

发送端将其身份标识信息确定为公钥信息，并生成与该公钥信息相匹配的私钥信息
401
发送端获取当前发送周期内待发送的首条数据
402
发送端通过该私钥信息对该首条数据和哈希链的头节点进行签名得到第二验证码
403
发送端发送第二消息，第二消息包括该公钥信息、第二验证码、该首条数据和哈希链的头节点
404
发送端获取当前发送周期内在发送首条数据之后待发送的目标数据
405
发送端根据目标数据在当前发送周期内的发送序号从哈希链中获取目标数据对应的节点
406
发送端对目标数据和目标数据对应的节点进行哈希运算得到第一验证码
407
发送端发送第一消息，第一消息包括目标数据、目标数据对应的节点、第一验证码和目标数据的发送序号
408

图4

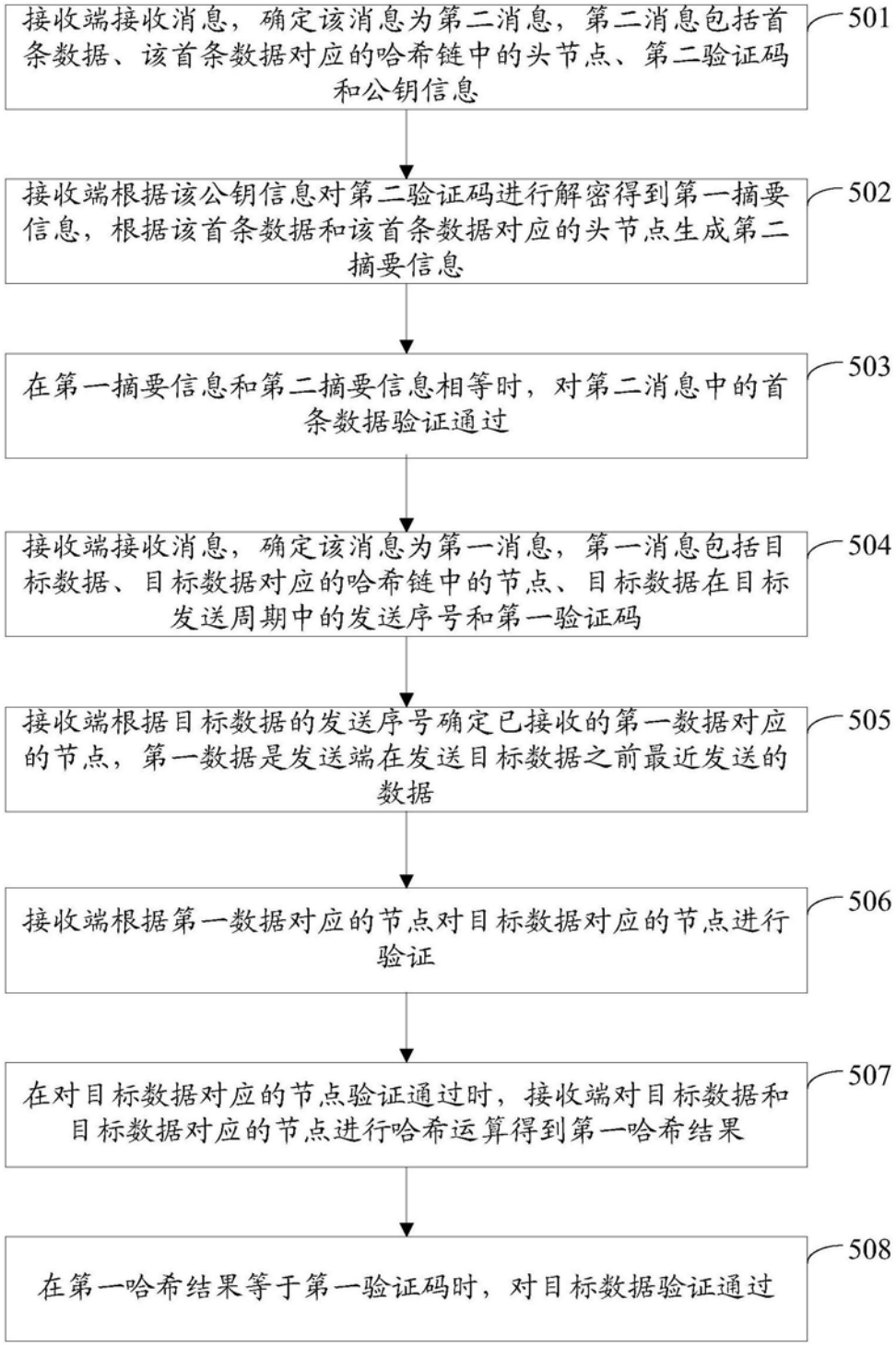

接收端接收消息，确定该消息为第二消息，第二消息包括首条数据、该首条数据对应的哈希链中的头节点、第二验证码和公钥信息
501
接收端根据该公钥信息对第二验证码进行解密得到第一摘要信息，根据该首条数据和该首条数据对应的头节点生成第二摘要信息
502
在第一摘要信息和第二摘要信息相等时，对第二消息中的首条数据验证通过
503
接收端接收消息，确定该消息为第一消息，第一消息包括目标数据、目标数据对应的哈希链中的节点、目标数据在目标发送周期中的发送序号和第一验证码
504
接收端根据目标数据的发送序号确定已接收的第一数据对应的节点，第一数据是发送端在发送目标数据之前最近发送的数据
505
接收端根据第一数据对应的节点对目标数据对应的节点进行验证
506
在对目标数据对应的节点验证通过时，接收端对目标数据和目标数据对应的节点进行哈希运算得到第一哈希结果
507
在第一哈希结果等于第一验证码时，对目标数据验证通过
508

图5

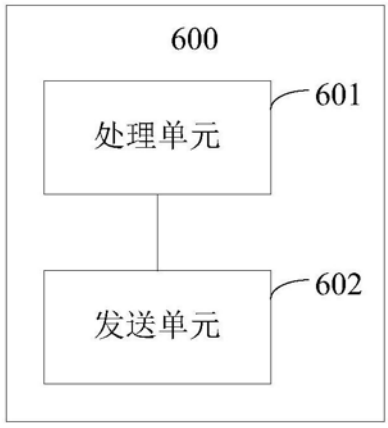

600
601
处理单元
602
发送单元

图6

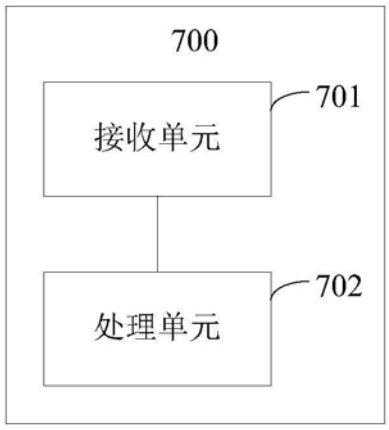

700
701
接收单元
702
处理单元

图7

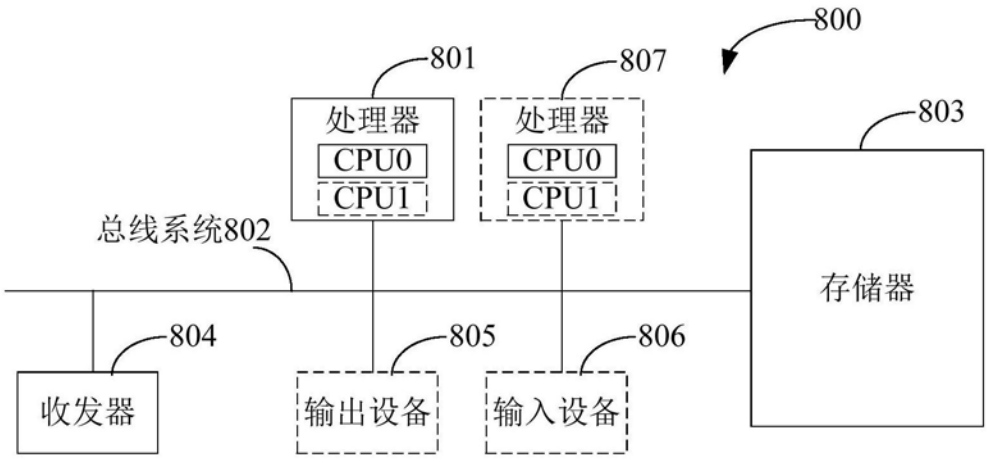

800
801
807
处理器
CPU0
CPU1
处理器
CPU0
CPU1
803
总线系统802
存储器
804
805
806
收发器
输出设备
输入设备

图8

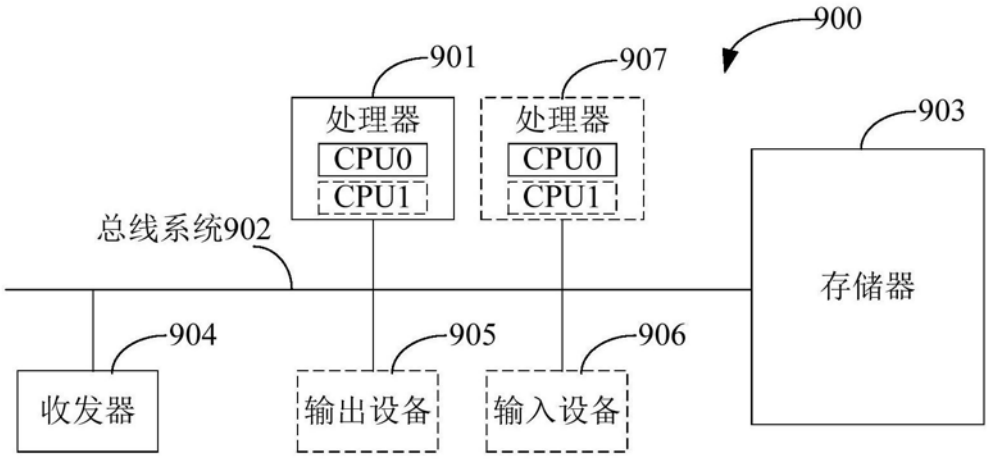

900
901
907
处理器
CPU0
CPU1
处理器
CPU0
CPU1
903
总线系统902
存储器
904
905
906
收发器
输出设备
输入设备

图9

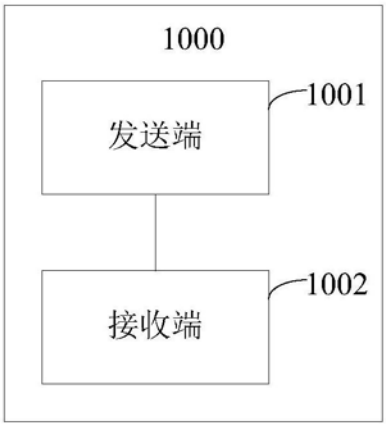

1000
1001
发送端
1002
接收端

图10