[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610076227.X

[43] 公开日 2007 年 10 月 24 日

[11] 公开号 CN 101060405A

[22] 申请日 2006.4.19
[21] 申请号 200610076227.X
[71] 申请人 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 林志斌 单长虹

[74] 专利代理机构 北京凯特来知识产权代理有限公司
代理人 郑立明

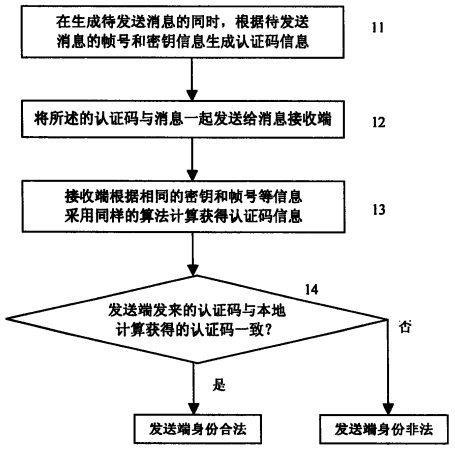
权利要求书 3 页 说明书 11 页 附图 2 页

[54] 发明名称

防止重放攻击的方法及系统

[57] 摘要

本发明涉及一种防止重放攻击的方法及系统。本发明主要包括：在信息发送端，根据包括密钥和帧号的参考信息采用预定的算法生成认证码，并将所述的认证码与待发送的消息一起发送给接收端；在接收端，根据收到的帧号和密钥并采用所述预定算法生成校验认证码，并利用校验认证码对收到的认证码进行一致性检验，确定发送端的合法性。因此，本发明提供的在无线系统中防止重放攻击的实现方案中，不需要终端和网络各自维护 PN 值，但在用户终端切换到目标基站后，仍然可以有效避免重放攻击问题的出现。



1、一种防止重放攻击的方法，其特征在于，包括:

A、在信息发送端，根据包括当前密钥和帧号的参考信息采用预定的算法生成认证码，并将所述的认证码与待发送的消息一起发送给接收端;

B、接收端接收到所述的消息后，根据收到的帧号和密钥并采用所述预定算法生成校验认证码;

C、在接收端，利用校验认证码对收到的认证码进行一致性检验，确定发送端的合法性。

2、根据权利要求1所述的方法，其特征在于，所述的参考信息还包括:时间参数，所述的时间参数信息将发送给信息接收端用于信息接收端识别该信息是否为当前帧号循环周期内的合法消息。

3、根据权利要求2所述的方法，其特征在于，所述的时间参数包括:

安全上下文已经存在的时间，或者，安全上下文生命周期的剩余时间，或者，当前时间信息，或者，根据安全上下文已经存在的时间或当前的时间信息或安全上下文生命周期的剩余时间确定的时间信息。

4、根据权利要求3所述的方法，其特征在于，所述的安全上下文已经存在的时间是由最近一次成功认证至当前时刻的时间信息。

5、根据权利要求3所述的方法，其特征在于，所述的时间参数信息在网络侧由鉴权器维护，基站从鉴权器获取所述的时间参数信息。

6、根据权利要求2至5中任一项所述的方法，其特征在于，所述的步骤C还包括:

判断收到的信息发送端发来的时间参数与本地维护的时间参数是否一致或者两者之间的差值是否小于预定的数值，若是且认证码正确，则确认信息发送端合法，否则，确认信息发送端非法。

7、根据权利要求1至5中任一项所述的方法，其特征在于，所述的信息发送端为用户终端或基站，与信息发送端对应的信息接收端为基站或用户终端。

8、根据权利要求7所述的方法，其特征在于，当信息发送端为用户终端时，所述的密钥为上行链路消息完整性保护密钥，当信息发送端为基站时，所述的密钥为下行链路消息完整性保护密钥。

9、一种防止重放攻击的发送装置，其特征在于，包括:

参考信息获取单元，设置于信息发送端，用于当需要发送信息时获取包括密钥和帧号的参考信息，并提供给认证码计算单元;

认证码计算单元，设置于信息发送端，用于根据所述包括密钥和帧号的参考信息采用预定的算法计算生成认证码，并提供给消息发送单元;

消息发送单元，设置于信息发送端，用于将所述的认证码随消息一起发送。

10、根据权利要求9所述的装置，其特征在于，所述的参考信息获取单元还包括:

时间参数获取单元，用于获取信息发送端维护的时间参数信息，并作为参考信息提供给认证码计算单元和消息发送单元。

11、根据权利要求9或10所述的装置，其特征在于，所述的信息发送端为用户终端或基站。

12、一种防止重放攻击的接收装置，其特征在于，包括:

认证码计算单元，设置于信息接收端，用于根据收到的消息对应的包括密钥和帧号的参考信息采用预定的与发送端相同算法计算生成认证码，并提供给合法性判断单元;

消息接收单元，设置于信息接收端，用于接收消息，并将该消息对应的包括密钥和帧号的参考信息提供给认证计算单元，将消息中的认证码提供给

合法性判断单元;

合法性判断单元，设置于信息接收端，用于根据消息中的认证码和计算获得认证码的一致性判断信息发送端的合法性。

13、根据权利要求12所述的装置，其特征在于，所述的合法性判断单元还包括:

时间参数判断单元，用于根据消息接收单元接收的时间参考信息与本地维护的时间参数信息的一致性判断信息发送端的合法性。

14、根据权利要求12或13所述的装置，其特征在于，所述的信息接收端为用户终端或基站。

15、一种防止重放攻击的系统，其特征在于，包括:

防止重放攻击的信息发送装置，用于向信息接收装置发送包含认证码，或包含认证码和时间参数信息的信息;

防止重放攻击的信息接收装置，用于接收防止重放攻击的信息发送装置发来的认证码信息，或者，认证码信息和时间参数信息，并根据所述信息判断信息发送端的合法性。

防止重放攻击的方法及系统

技术领域

本发明涉及无线通信技术领域，尤其涉及一种可防止重放攻击的技术。

背景技术

在无线通信系统中，为保证通信的安全性，用户终端如果需要与基站进行通信，则两者必须建立相同的授权密钥上下文，即AK上下文。所述的AK上下文包括以下信息:

授权密钥（AK）、授权密钥标识（AKID）、授权密钥序列号（AK Sequence Number）、授权密钥生存期（AK Lifetime）、对偶主密钥序列号（PMK Sequence Number）、上行链路消息完整性保护密钥（HMAC/CMAC_KEY_U）、上行链路消息防止重放攻击包序列号（HMAC/CMAC_PN_U，简称PN_U）、下行链路消息完整性保护密钥（HMAC/CMAC_KEY_D）、下行链路消息防止重放攻击包序列号（HMAC/CMAC_PN_D，简称PN_D）、密钥加密密钥（KEK）、完整性加密密钥（EIK）。

其中，所述的HMAC/CMAC_KEY_U、HMAC/CMAC_KEY_D是由基站根据AK、终端媒体接入控制（MAC）地址、基站标识计算得到，分别用于对上下行链路消息提供完整性保护;

所述的PN_U和PN_D是两个32位计数器，在AK上下文建立时，所述的两个计数器的值都为0，之后，每使用HMAC/CMAC_KEY_U对上行消息提供一次完整性保护，终端就把PN_U的值增加1；每使用HMAC/CMAC_KEY_D对下行消息提供一次完整性保护，基站就把PN_D的值增加1。如果PN_U或P

N_D的数值空间耗尽（即这两个值中任一个到达2^32-1），或是AK上下文中AK生存期到期，则该AK生存期结束。为保证通信过程的不中断，在AK生存期结束之前应当重新申请新的AK。

当终端切换到目标基站后，可以不进行重鉴权操作，但是相应的AK是需要更新的。如果终端切换到目标基站后，AK上下文中的PN_U和PN_D重新计数，则当终端两次进入同一基站时，便可能受到重放攻击。

在现有技术中，为避免用户终端发生切换后受到重放攻击，主要采用了以下两种实现解决方案。

（一）目前采用的第一种实现方案为AK缓存技术，即在终端和基站两侧缓存AK上下文。终端每到一个基站，便创建一个AK上下文，即使终端离开该基站后也不删除为该基站创建的AK上下文。同样，在基站侧，每有一个终端接入，就向鉴权器申请一个AK，并生成上下文，这样，当终端在基站之间移动时，不同的基站使用不同的AK上下文，以避免重放攻击。

不难看出，这种实现方案在终端和网络侧基站需要缓存的AK上下文数量较大时，将会给该方案的实现带来了很大的困难。

（二）目前采用的另一种实现方案为上下文传递技术，即终端和网络都只保存一个AK上下文，终端在移动时，AK可以变化，但PN值连续使用。由于这种方法中，为使得PN值连续使用，新的基站需要从老的基站获得当前的PN值，这就要求两个基站之间需要互相信任，然而，在具体实现过程中很难保证两个基站之间的相互信任。

因此，目前还没有一种便于实现的技术方案可以有效解决用户终端切换后可能引发的重放攻击问题。

发明内容

本发明的目的是提供一种防止重放攻击的方法及系统，从而可以采用较

为简便地手段在无线通信网络中有效防止重放攻击问题的出现。

本发明的目的是通过以下技术方案实现的:

本发明提供了一种防止重放攻击的方法，包括:

A、在信息发送端，根据包括当前密钥和帧号的参考信息采用预定的算法生成认证码，并将所述的认证码与待发送的消息一起发送给接收端;

B、接收端接收到所述的消息后，根据收到的帧号和密钥并采用所述预定算法生成校验认证码;

C、在接收端，利用校验认证码对收到的认证码进行一致性检验，确定发送端的合法性。

所述的参考信息还包括: 时间参数，所述的时间参数信息将发送给信息接收端用于信息接收端识别该信息是否为当前帧号循环周期内的合法消息。

所述的时间参数包括:

安全上下文已经存在的时间，或者，安全上下文生命周期的剩余时间，或者，当前时间信息，或者，根据安全上下文已经存在的时间或当前的时间信息或安全上下文生命周期的剩余时间确定的时间信息。

所述的安全上下文已经存在的时间是由最近一次成功认证至当前时刻的时间信息。

所述的时间参数信息在网络侧由鉴权器维护，基站从鉴权器获取所述的时间参数信息。

所述的步骤C还包括:

判断收到的信息发送端发来的时间参数与本地维护的时间参数是否一致或者两者之间的差值是否小于预定的数值，若是且认证码正确，则确认信息发送端合法，否则，确认信息发送端非法。

所述的信息发送端为用户终端或基站，与信息发送端对应的信息接收端为基站或用户终端。

本发明中，当信息发送端为用户终端时，所述的密钥为上行链路消息完整性保护密钥，当信息发送端为基站时，所述的密钥为下行链路消息完整性保护密钥。

本发明还提供了一种防止重放攻击的发送装置，包括：

参考信息获取单元，设置于信息发送端，用于当需要发送信息时获取包括密钥和帧号的参考信息，并提供给认证码计算单元；

认证码计算单元，设置于信息发送端，用于根据所述包括密钥和帧号的参考信息采用预定的算法计算生成认证码，并提供给消息发送单元；

消息发送单元，设置于信息发送端，用于将所述的认证码随消息一起发送。

所述的参考信息获取单元还包括：

时间参数获取单元，用于获取信息发送端维护的时间参数信息，并作为参考信息提供给认证码计算单元和消息发送单元。

所述的信息发送端为用户终端或基站。

本发明还提供了一种防止重放攻击的接收装置，包括：

认证码计算单元，设置于信息接收端，用于根据收到的消息对应的包括密钥和帧号的参考信息采用预定的与发送端相同算法计算生成认证码，并提供给合法性判断单元；

消息接收单元，设置于信息接收端，用于接收消息，并将该消息对应的包括密钥和帧号的参考信息提供给认证计算单元，将消息中的认证码提供给合法性判断单元；

合法性判断单元，设置于信息接收端，用于根据消息中的认证码和计算获得认证码的一致性判断信息发送端的合法性。

所述的合法性判断单元还包括：

时间参数判断单元，用于根据消息接收单元接收的时间参考信息与本地

维护的时间参数信息的一致性判断信息发送端的合法性。

所述的信息接收端为用户终端或基站。

本发明还提供了一种防止重放攻击的系统，包括：

防止重放攻击的信息发送装置，用于向信息接收装置发送包含认证码，或包含认证码和时间参数信息的信息；

防止重放攻击的信息接收装置，用于接收防止重放攻击的信息发送装置发来的认证码信息，或者，认证码信息和时间参数信息，并根据所述信息判断信息发送端的合法性。

由上述本发明提供的技术方案可以看出，本发明由于采用了基于帧号获得消息传输过程中需要的认证码信息，因此，本发明提供的在无线系统中防止重放攻击的实现方案中，不需要终端和网络各自维护PN值，仍然可以保证在用户终端切换到目标基站后，能够有效避免重放攻击问题的出现。

另外，本发明在基于帧号的基础上还考虑了时间参数信息的引入，从而可以进一步确保当帧号的使用超过一个循环周期后，仍可以保证不会受到重放攻击。

附图说明

图1为本发明所述的方法的具体实现过程示意图一；

图2为本发明所述的方法的具体实现过程示意图二；

图3为本发明所述的系统的具体实现结构示意图。

具体实施方式

在无线通信系统中，通信的一方在生成一个需要发送给对端的消息时，同时还生成一个认证码，所述的认证码需要随着消息一起传给对端。即在空口传递的信息内容包括消息和认证元组，其中，所述的认证元组包括认证码

和其它参数。所述的消息认证码包括上行消息认证码和下行消息认证码，获得两个认证码的具体方式如下：

上行消息认证码=f（上行消息完整性保护密钥，其它参数）；

下行消息认证码=f（下行消息完整性保护密钥，其它参数）；

其中，f为一种运算方式，即将密钥和其他参数采用f算法便可以获得相应的认证码信息。

认证码用于在消息的接收端识别消息的来源是否合法，即发送消息的用户身份是否合法，基于此，本发明便通过对认证码的获得方式的改进避免可能引发的重发攻击问题。

在无线通信系统中，一个消息必须承载在某一个或几个特定的帧上，而每个帧都有帧号。而攻击者即使截获了某个消息，也不可能在同一帧里就重放该帧，因此，可以利用帧号来保护消息。

这样，本发明便可以利用帧号获得认证码信息，即当通信的发送方在向对端发送一个消息时，同时还发送一个认证元组，所述的认证元组中至少包含一个认证码，所述的认证码是利用密钥和帧号采用预定的函数运算方式计算获得，在运算过程中还可以在密钥和帧号的基础上再利用其他参数信息，如消息体等；从而使得接收方能够根据认证元组包含的信息识别该消息的有效性，避免重放攻击。

在所述的认证元组中，还可以包含一个时间参数，所述的时间参数可以为安全上下文已经存在的时间，即最近一次成功认证至今的时间长；所述的时间参数也可以为其他信息，例如，安全上下文生命周期的剩余时间，或者，当前的绝对时间信息，或者，基于密钥对应的上下文已经存在的时间信息或安全上下文生命周期的剩余时间或当前的绝对时间信息确定的时间信息，等等。

而且，本发明中，在网络侧所述的时间参数信息可以由鉴权器维护，并

在基站需要时传给基站。

当认证元组中包含所述时间参数信息时，则所述的认证码的计算函数中也需要考虑该时间参数信息。

当接收方收到包含时间参数的消息后，如果消息中的时间参数和本地的时间参数的误差大于预定的值，便可以认为该消息无效，否则，认为该消息为有效消息，并可以继续后续的消息处理过程。

为便于对本发明有进一步的理解，下面将结合一个具体的应用实例对本发明提供的方法进行详细说明。

如图1所示，本发明具体包括以下处理步骤：

步骤11：在生成待发送消息的同时，根据待发送消息的帧号和密钥信息生成认证码信息；

也就是说，在通信过程中的消息发送端，当生成一个需要发送给对端的消息时，还需要根据帧号生成一个认证码，而且，所述的认证码需要与消息一起传送给对端；

具体一点讲，所述的认证码是使用之前已经获得的密钥对消息进行完整性保护处理，即令认证码=f1（密钥，帧号等），f1代表一种运算方法，将密钥、帧号等信息经过f1代表的运算方法进行运算处理后便可以获得需要的认证码，计算过程中还可以引入其他参数信息，如消息体信息等；

步骤12：将所述的认证码与消息一起发送给消息接收端；

即在空口传递的内容包括：消息、认证元组，其中，所述的认证元组包括步骤11中计算获得的认证码，在所述的认证元组中除认证码外还可以包括其他参数。

步骤13：接收端接收发送端发来的信息后，根据收到信息的帧号采用同样的算法，即仍参照步骤11采用所述f1算法根据相同的密钥和帧号等信息计

算获得认证码信息;

步骤14：判断发送端发来的认证码与本地计算获得的认证码是否一致，如果一致，则确定发送端的身份合法，否则，确定发送端身份不合法，从而可以有效避免重放攻击问题的出现。

在一些无线通信系统中，可能出现帧号的周期小于密钥的生命周期的情况，此时，当帧号循环一圈之后，即便采用上述方案，重方攻击问题仍然可能出现。为此，本发明还提供了另外一种具体实现方案，

如图2所示，本发明提供的另一种具体实现方案包括以下处理过程:

步骤21：在生成待发送消息的同时，根据待发送消息的帧号、密钥信息和时间参数信息生成认证码信息;

所述的时间参数信息用于作为信息接收端识别该信息是否为当前帧号循环周期内的合法消息的依据;

且所述的时间参数表示密钥对应的上下文已经存在的时间，或者，安全上下文生命周期的剩余时间，或者，也可以表示发送消息端当前的绝对时间信息，或者，基于密钥对应的上下文已经存在的时间信息或安全上下文生命周期的剩余时间或当前的绝对时间信息确定的时间信息，等等;

所述的时间参数可以使用多种计量单位，例如，以秒、半个帧号循环周期等作为计量单位，只要所述的时间参的计量单位小于帧号循环周期即可;

所述的时间参数作为安全上下文的一部分，需要在MS和网络侧各自维护；其中，在网络侧，可以由鉴权器维护所述的时间参数信息，并在基站需要时传给基站使用;

所述的认证码具体是使用之前已经获得的密钥对消息进行完整性保护处理，即令认证码=f2（密钥，帧号，时间参数等），f2代表一种运算方法，将密钥、帧号和时间参数等信息经过f2代表的运算方法进行运算处理后便可以

获得需要的认证码，计算过程中还可以引入其他参数信息；

步骤22：将所述的认证码及时间参数与消息一起发送给消息接收端；

即在空口传递的内容包括：消息、认证元组，其中，所述的认证元组包括步骤21中计算获得的认证码和时间参数，在所述的认证元组中除认证码外还可以包括其他参数；

在该步骤中，所述的时间参数以明文的形式和消息一起传给对端，作为获得认证码的一个参数；

步骤23：接收端接收发送端发来的信息后，根据收到信息的帧号及所述的时间参数采用同样的算法，即仍参照步骤21采用所述f2算法根据相同的密钥、帧号和时间参数等信息计算获得认证码信息；

步骤24：判断发送端发来的认证码与本地计算获得的认证码是否一致，同时，还需要判断收到的时间参数与本地对应的时间参数信息是否一致，如果均一致，则确定发送端的身份合法，否则，确定发送端身份不合法，从而可以有效避免重放攻击问题的出现；

在进行时间参数信息的一致性判断过程中，网络和终端对于所述的时间参数不需要严格一致，只要误差值远小于帧号的周期便可以认为一致。

本发明还提供了一种防止重放攻击的系统，包括防止重放攻击的信息发送装置和防止重放攻击的信息接收装置，具体如下：

防止重放攻击的信息发送装置，设置于信息发送端，用于向信息接收装置发送包含认证码，或包含认证码和时间参数信息的信息，所述的信息发送端为用户终端或基站。

防止重放攻击的信息接收装置，设备于信息接收端，用于接收防止重放攻击的信息发送装置发来的认证码信息，或者，认证码信息和时间参数信息，并根据所述信息判断信息发送端的合法性，与信息发送端对应，所述的

信息接收端为基站或用户终端。

所述的系统的具体实施方式如图3所示，其中：

所述的防止重放攻击的发送装置，具体包括以下处理单元：

（1）参考信息获取单元

用于当需要发送信息时获取包括密钥和帧号的参考信息，并提供给认证码计算单元；

所述的参考信息获取单元还包括：

时间参数获取单元，用于获取信息发送端维护的时间参数信息，并作为参考信息提供给认证码计算单元和消息发送单元。

（2）认证码计算单元

用于根据所述包括密钥和帧号的参考信息采用预定的算法计算生成认证码，并提供给消息发送单元；

其中，所述的密钥包括：上行链路完整性保护密钥和下行链路完整性保护密钥；

（3）消息发送单元

用于将所述的认证码随消息一起发送。

所述的防止重放攻击的接收装置，具体包括以下处理单元：

（1）认证码计算单元

用于根据收到的消息对应的包括密钥和帧号的参考信息采用预定的与发送端相同算法计算生成认证码，并提供给合法性判断单元；

（2）消息接收单元

用于接收消息，并将该消息对应的包括密钥和帧号的参考信息提供给认证计算单元，将消息中的认证码提供给合法性判断单元；

（3）合法性判断单元

用于根据消息中的认证码和计算获得认证码的一致性判断信息发送端的

合法性，所述的合法性判断单元还包括：

时间参数判断单元，用于根据消息接收单元接收的时间参考信息与本地维护的时间参数信息的一致性判断信息发送端的合法性。

综上所述，本发明提供的技术方案彻底解决了无线接口可能出现的重放攻击问题，而且在该方案中不需要在基站之间传递安全上下文，使得防止重放攻击的实现方案易于实现。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

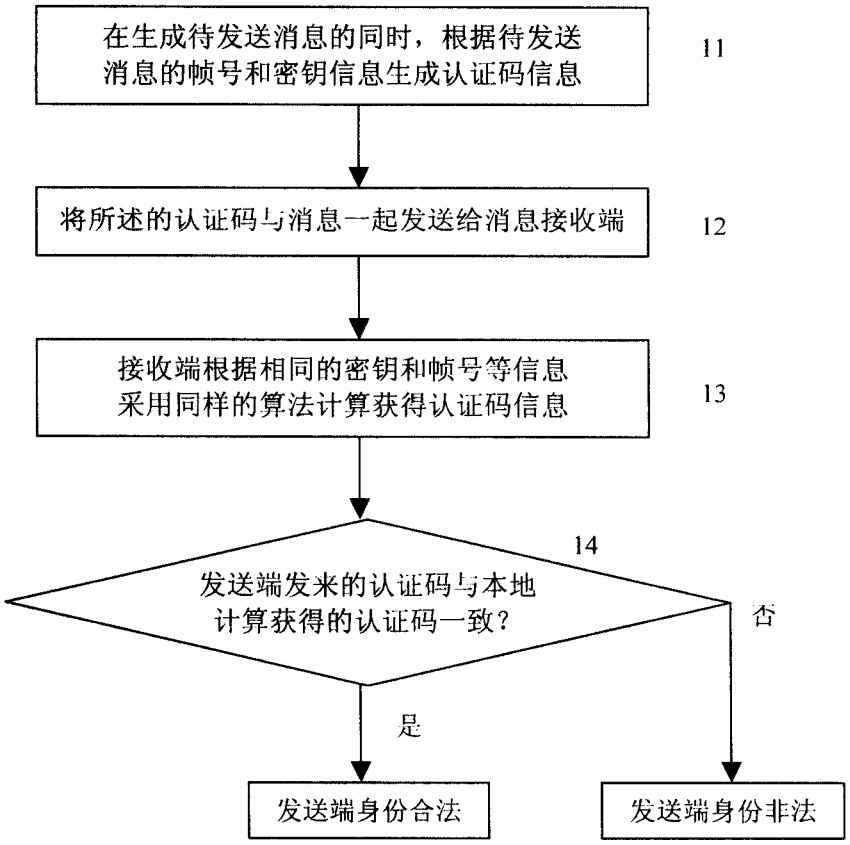

在生成待发送消息的同时，根据待发送消息的帧号和密钥信息生成认证码信息
11
将所述的认证码与消息一起发送给消息接收端
12
接收端根据相同的密钥和帧号等信息采用同样的算法计算获得认证码信息
13
14
发送端发来的认证码与本地计算获得的认证码一致？
否
是
发送端身份合法
发送端身份非法

图1

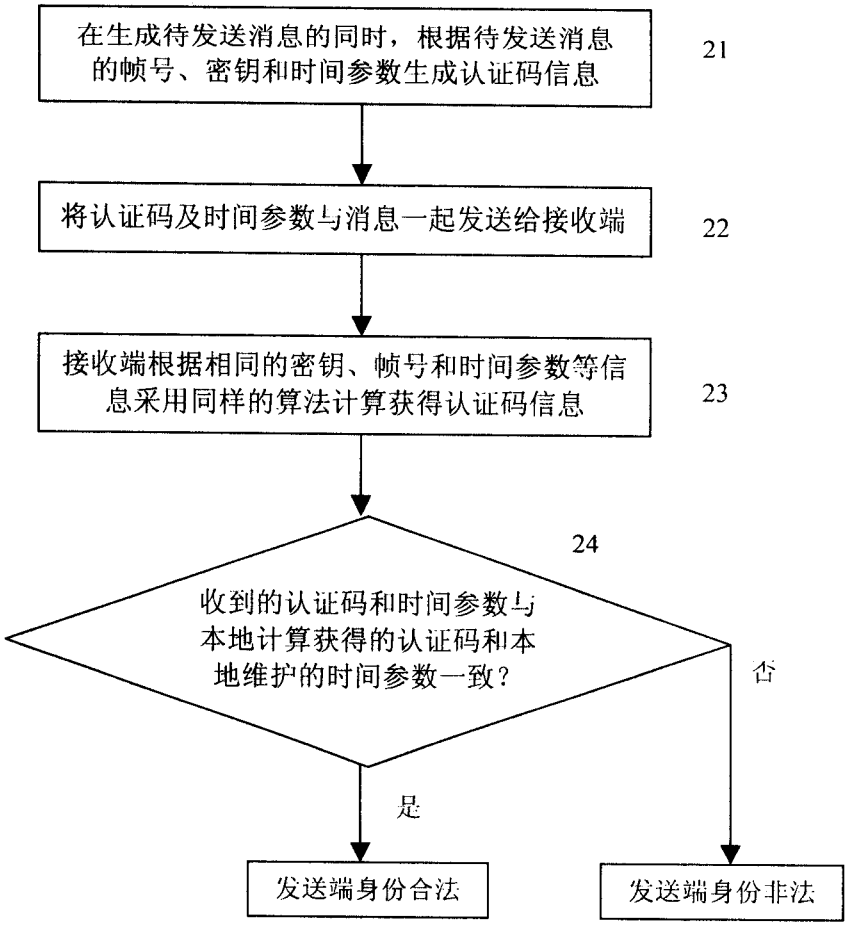

在生成待发送消息的同时，根据待发送消息的帧号、密钥和时间参数生成认证码信息
21
将认证码及时间参数与消息一起发送给接收端
22
接收端根据相同的密钥、帧号和时间参数等信息采用同样的算法计算获得认证码信息
23
24
收到的认证码和时间参数与本地计算获得的认证码和本地维护的时间参数一致？
否
是
发送端身份合法
发送端身份非法

图2

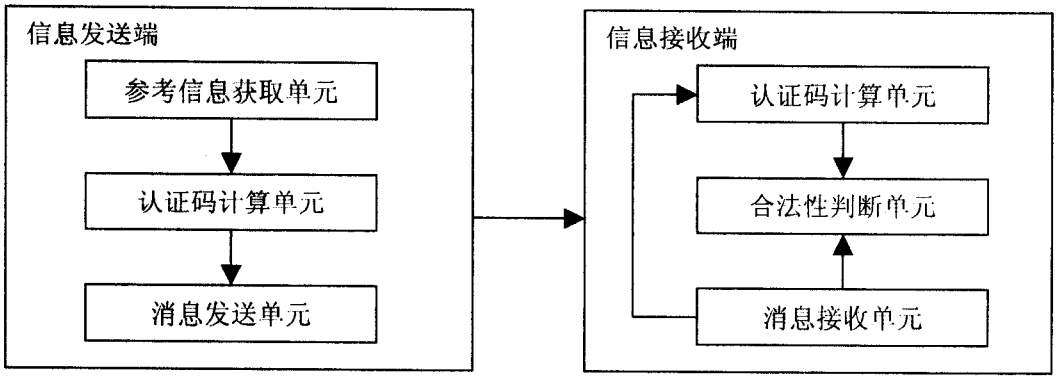

信息发送端
参考信息获取单元
认证码计算单元
消息发送单元
信息接收端
认证码计算单元
合法性判断单元
消息接收单元

图3