



(12)发明专利申请

(10)申请公布号 CN 107360573 A

(43)申请公布日 2017. 11. 17

(21)申请号 201610307103.1

(22)申请日 2016.05.10

(71)申请人 上海中兴软件有限责任公司

地址 201203 上海市浦东新区碧波路889号

(72)发明人 余万涛

(74)专利代理机构 北京安信方达知识产权代理

有限公司 11262

代理人 解婷婷 龙洪

(51)Int.Cl.

H04W 12/06(2009.01)

H04W 12/08(2009.01)

H04W 12/12(2009.01)

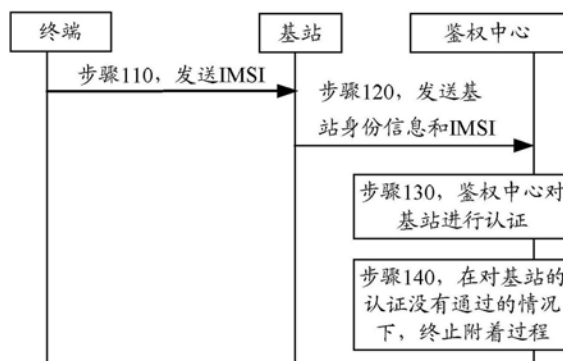
权利要求书4页 说明书11页 附图3页

(54)发明名称

一种终端接入方法和装置

(57)摘要

本发明提供一种终端接入方法和装置,该方法包括:终端将用户身份信息发送给基站;终端接收基站所述发送的认证挑战信息和基站响应信息;终端检测所述基站响应信息,在检测通过的情况下,终端根据认证挑战信息接入到基站中。通过该方案,在终端接入过程中,由鉴权中心对终端所附着的基站进行认证,可以由鉴权中心根据对基站的认证结果决定是否终止接入过程,也可以由鉴权中心将对基站的认证结果发送给终端,由终端确定是否连接到基站,通过该流程,改善了恶意基站通过欺骗的方式使得终端从一个合法基站转移附着到该恶意基站上的情况,提高了终端接入基站时的安全性。



1. 一种终端接入方法,其特征在于,所述方法包括:
终端将用户身份信息发送给基站;
终端接收基站所述发送的认证挑战信息和基站响应信息;
终端检测所述基站响应信息,在检测通过的情况下,终端根据认证挑战信息接入到基站中。

2. 根据权利要求1所述的终端接入方法,其特征在于,所述终端检测所述基站响应信息包括如下方式的任一种:

方式1-1,在基站响应信息的携带内容包括基站身份信息的情况下,终端获取基站响应信息对应的基站身份信息;

终端判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致;如果不一致,则对基站响应信息的检测结果为不通过;如果一致,则对基站响应信息的检测结果为通过;

方式1-2,在基站响应信息的携带内容包括基站认证结果的情况下,终端获取基站响应信息对应的基站认证结果,如果基站认证结果为非法基站,则对基站响应信息的检测结果为不通过;如果基站认证结果为合法基站,则对基站响应信息的检测结果为通过;

其中,终端通过认证挑战信息获取会话密钥信息,通过所述会话密钥信息得到基站响应信息的携带内容。

3. 根据权利要求2所述的终端接入方法,其特征在于,所述通过所述会话密钥信息得到基站响应信息的携带内容包括:

在会话密钥信息包括加密密钥Ck的情况下,终端通过会话密钥信息中的加密密钥Ck对基站响应信息进行第三处理,得到基站响应信息对应的基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程;

在会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,终端通过会话密钥信息中的完整性保护密钥Ik对基站响应信息进行第四处理,并通过会话密钥信息中的加密密钥Ck对第四处理的结果进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程,第四处理是与所述第二处理对应的逆处理过程;

其中,第一处理是指鉴权中心为获取基站响应信息而通过加密密钥Ck对基站响应信息的携带内容进行的处理;第二处理是指鉴权中心为获取基站响应信息而通过完整性保护密钥Ik对第一处理的结果进行的处理。

4. 一种终端接入方法,其特征在于,所述方法包括:
鉴权中心接收基站发送的基站身份信息和用户身份信息;
鉴权中心根据所述基站身份信息对基站进行认证,根据用户身份信息对终端进行认证;

在对终端的认证通过的情况下,生成对应的认证信息,并将所述认证信息发送给基站。

5. 根据权利要求4所述的终端接入方法,其特征在于,在所述鉴权中心根据所述基站身份信息对基站进行认证之后,所述方法还包括:

在对基站的认证通过的情况下,执行所述生成对应的认证信息的步骤;

在对基站的认证没有通过的情况下,终止终端的接入过程。

6. 根据权利要求4所述的终端接入方法,其特征在于,在所述鉴权中心根据所述基站身

份信息对基站进行认证之后,所述方法还包括:

方式2-1:在对基站的认证通过的情况下,执行所述生成对应的认证信息的步骤;生成基站响应信息,并将所述基站响应信息发送给基站;在对基站的认证没有通过的情况下,终止终端的接入过程;

或,

方式2-2:生成基站响应信息,并将所述基站响应信息发送给基站;其中,根据对基站的认证结果设置对应的基站响应信息。

7.根据权利要求6所述的终端接入方法,其特征在于,所述认证信息包括认证挑战信息、会话密钥信息,以及认证响应信息;

在方式2-1的情况下,所述基站响应信息的携带内容包括基站身份信息;

在方式2-2的情况下,所述基站响应信息的携带内容包括基站身份信息和基站认证结果,所述基站认证结果包括用于表示基站非法或合法的标识信息;

所述生成基站响应信息包括:

通过所述会话密钥信息对基站响应信息的携带内容进行处理从而得到对应的基站响应信息。

8.根据权利要求7所述的终端接入方法,其特征在于,通过会话密钥信息对基站响应信息的携带内容进行处理包括:

在鉴权中心生成的会话密钥信息包括加密密钥Ck的情况下,鉴权中心通过加密密钥Ck对基站响应信息的携带内容进行第一处理从而得到对应的基站响应信息;

或,

在鉴权中心生成的会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,鉴权中心先通过加密密钥Ck对基站响应信息的携带内容进行第一处理,再通过完整性保护密钥Ik对第一处理的结果进行第二处理,从而得到基站响应信息的携带内容对应的基站响应信息。

9.一种终端接入方法,其特征在于,所述方法包括:

基站接收终端发送的用户身份信息;

基站将基站身份信息以及所述用户身份信息发送给鉴权中心

基站接收鉴权中心发送的认证信息;

基站将认证信息中的认证挑战信息发送给终端。

10.根据权利要求9所述的终端接入方法,其特征在于,在所述将基站身份信息以及所述用户身份信息发送给鉴权中心之后,所述方法还包括:

基站接收鉴权中心发送基站响应信息;

基站将所述基站响应信息发送给终端。

11.一种终端接入装置,设置在终端上,其特征在于,所述装置包括:

第一发送单元,用于将用户身份信息发送给基站;

第一接收单元,用于接收基站所述发送的认证挑战信息和基站响应信息;

检测单元,用于检测所述基站响应信息;

接入单元,用于在检测通过的情况下,根据认证挑战信息接入到基站中。

12.根据权利要求11所述的终端接入装置,其特征在于,所述检测单元包括模块中的至

少一个：

第一检测模块，用于在基站响应信息的携带内容包括基站身份信息的情况下，终端获取基站响应信息对应的基站身份信息；

判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致；如果不一致，则对基站响应信息的检测结果为不通过；如果一致，则对基站响应信息的检测结果为通过；

第二检测模块，用于在基站响应信息的携带内容包括基站认证结果的情况下，获取基站响应信息对应的基站认证结果，如果基站认证结果为非法基站，则对基站响应信息的检测结果为不通过；如果基站认证结果为合法基站，则对基站响应信息的检测结果为通过；

其中，第一检测模块和/或第二检测模块通过认证挑战信息获取会话密钥信息，通过所述会话密钥信息得到基站响应信息的携带内容。

13. 根据权利要求12所述的终端接入装置，其特征在于，通过所述会话密钥信息得到基站响应信息的携带内容包括：

在会话密钥信息包括加密密钥Ck的情况下，通过会话密钥信息中的加密密钥Ck对基站响应信息进行第三处理，得到基站响应信息的携带内容；其中，第三处理是与所述第一处理对应的逆处理过程；

在密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下，通过会话密钥信息中的完整性保护密钥Ik对基站响应信息进行第四处理，并通过会话密钥信息中的加密密钥Ck对第四处理的结果进行第三处理，得到基站响应信息的携带内容；其中，第三处理是与所述第一处理对应的逆处理过程，第四处理是与所述第二处理对应的逆处理过程；

其中，第一处理是指鉴权中心为获取基站响应信息而通过加密密钥Ck对基站身份信息或基站认证结果进行的处理；第二处理是指鉴权中心为获取基站响应信息而通过完整性保护密钥Ik对第一处理的结果进行的处理。

14. 一种终端接入装置，设置在鉴权中心，其特征在于，所述装置包括：

第二接收单元，用于接收基站发送的基站身份信息和用户身份信息；

认证单元，用于根据所述基站身份信息对基站进行认证，根据用户身份信息对终端进行认证；

处理单元，用于在对终端的认证通过的情况下，生成对应的认证信息，并将所述认证信息发送给基站。

15. 根据权利要求14所述的终端接入装置，其特征在于，所述处理单元包括第一处理模块，用于在对基站的认证通过的情况下，执行所述生成对应的认证信息的过程；在对基站的认证没有通过的情况下，终止终端的接入过程。

16. 根据权利要求14所述的终端接入装置，其特征在于，所述处理单元包括如下模块的任一个：

第二处理模块，用于在对基站的认证通过的情况下，执行所述生成对应的认证信息的过程；并生成基站响应信息，并将所述基站响应信息发送给基站；在对基站的认证没有通过的情况下，终止终端的接入过程；

第三处理模块，用于生成基站响应信息，并将所述基站响应信息发送给基站；其中，根据对基站的认证结果设置对应的基站响应信息。

17. 根据权利要求16所述的终端接入装置, 其特征在于, 所述认证信息包括认证挑战信息、会话密钥信息, 以及认证响应信息;

第二处理模块生成的所述基站响应信息的携带内容包括基站身份信息;

第三处理模块生成的基站响应信息的携带内容包括基站身份信息和基站认证结果, 所述基站认证结果包括用于表示基站非法或合法的标识信息;

所述第二处理模块和/或第三处理模块生成基站响应信息包括:

通过所述会话密钥信息对基站响应信息的携带内容进行处理从而得到对应的基站响应信息。

18. 根据权利要求17所述的终端接入装置, 其特征在于, 通过会话密钥信息对基站响应信息的携带内容进行处理包括:

在鉴权中心生成的会话密钥信息包括加密密钥Ck的情况下, 鉴权中心通过加密密钥Ck对基站响应信息的携带内容进行第一处理从而得到对应的基站响应信息;

或,

在鉴权中心生成的会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下, 鉴权中心先通过加密密钥Ck对基站响应信息的携带内容进行第一处理, 再通过完整性保护密钥Ik对第一处理的结果进行第二处理, 从而得到基站响应信息的携带内容对应的基站响应信息。

19. 一种终端接入装置, 设置在基站, 其特征在于, 所述装置包括:

第三接收单元, 用于接收终端发送的用户身份信息;

第三发送单元, 用于将基站身份信息以及所述用户身份信息发送给鉴权中心;

所述第三接收单元还用于接收鉴权中心发送的认证信息;

所述第三发送单元还用于将认证信息中的认证挑战信息发送给终端。

20. 根据权利要求19所述的终端接入装置, 其特征在于,

所述第三接收单元还用于接收鉴权中心发送基站响应信息;

所述第三发送单元还用于将所述基站响应信息发送给终端。

一种终端接入方法和装置

技术领域

[0001] 本发明涉及数据通信领域,尤指一种终端接入方法和装置。

背景技术

[0002] 目前,现有EGPRS安全架构采用单向认证方式,认证和密钥协商过程需要经过基站转发认证信息。在基于EGPRS的蜂窝物联网中,蜂窝物联网(CIoT,Cellular Internet of Things)终端设备在附着到网络时,先向基站发送终端设备的用户身份信息,然后,接收基站转发的认证信息和密钥协商挑战信息。CIoT终端设备根据认证信息生成会话密钥和认证响应信息,并将认证响应信息发送给基站。在这个过程中,CIoT设备不需要,也无法确定基站是合法基站还是恶意基站。

[0003] 在基于EGPRS的CIoT(Cellular IoT)系统中,对于蜂窝物联网(CIoT,Cellular Internet of Things)终端设备,在附着时,由于现有EGPRS安全架构采用单向认证方式,因此,CIoT终端设备无法识别接收到的认证和密钥协商信息是否来自合法基站。恶意基站有可能通过欺骗的方式使得CIoT终端设备从一个合法基站转移附着到该恶意基站上。这将导致CIoT终端设备相关信息的泄露。

发明内容

[0004] 为了解决上述问题,本发明提出了一种终端接入方法和装置,能够提高终端接入的安全性。

[0005] 为了达到上述目的,本发明提出了一种终端接入方法,其特征在于,所述方法包括:

[0006] 终端将用户身份信息发送给基站;

[0007] 终端接收基站所述发送的认证挑战信息和基站响应信息;

[0008] 终端检测所述基站响应信息,在检测通过的情况下,终端根据认证挑战信息接入到基站中。

[0009] 优选地,所述终端检测所述基站响应信息包括如下方式的任一种:

[0010] 方式1-1,在基站响应信息的携带内容包括基站身份信息的情况下,终端获取基站响应信息对应的基站身份信息;

[0011] 终端判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致;如果不一致,则对基站响应信息的检测结果为不通过;如果一致,则对基站响应信息的检测结果为通过;

[0012] 方式1-2,在基站响应信息的携带内容包括基站认证结果的情况下,终端获取基站响应信息对应的基站认证结果,如果基站认证结果为非法基站,则对基站响应信息的检测结果为不通过;如果基站认证结果为合法基站,则对基站响应信息的检测结果为通过;

[0013] 其中,终端通过认证挑战信息获取会话密钥信息,通过所述会话密钥信息得到基站响应信息的携带内容。

[0014] 优选地,所述通过所述会话密钥信息得到基站响应信息的携带内容包括:

[0015] 在会话密钥信息包括加密密钥Ck的情况下,终端通过会话密钥信息中的加密密钥Ck对基站响应信息进行第三处理,得到基站响应信息对应的基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程;

[0016] 在会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,终端通过会话密钥信息中的完整性保护密钥Ik对基站响应信息进行第四处理,并通过会话密钥信息中的加密密钥Ck对第四处理的结果进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程,第四处理是与所述第二处理对应的逆处理过程;

[0017] 其中,第一处理是指鉴权中心为获取基站响应信息而通过加密密钥Ck对基站响应信息的携带内容进行的处理;第二处理是指鉴权中心为获取基站响应信息而通过完整性保护密钥Ik对第一处理的结果进行的处理。

[0018] 为了达到上述目的,本发明还提出了一种终端接入方法,所述方法包括:

[0019] 鉴权中心接收基站发送的基站身份信息和用户身份信息;

[0020] 鉴权中心根据所述基站身份信息对基站进行认证,根据用户身份信息对终端进行认证;

[0021] 在对终端的认证通过的情况下,生成对应的认证信息,并将所述认证信息发送给基站。

[0022] 优选地,在所述鉴权中心根据所述基站身份信息对基站进行认证之后,所述方法还包括:

[0023] 在对基站的认证通过的情况下,执行所述生成对应的认证信息的步骤;

[0024] 在对基站的认证没有通过的情况下,终止终端的接入过程。

[0025] 优选地,在所述鉴权中心根据所述基站身份信息对基站进行认证之后,所述方法还包括:

[0026] 方式2-1:在对基站的认证通过的情况下,执行所述生成对应的认证信息的步骤;生成基站响应信息,并将所述基站响应信息发送给基站;在对基站的认证没有通过的情况下,终止终端的接入过程;

[0027] 或,

[0028] 方式2-2:生成基站响应信息,并将所述基站响应信息发送给基站;其中,根据对基站的认证结果设置对应的基站响应信息。

[0029] 优选地,所述认证信息包括认证挑战信息、会话密钥信息,以及认证响应信息;

[0030] 在方式2-1的情况下,所述基站响应信息的携带内容包括基站身份信息;

[0031] 在方式2-2的情况下,所述基站响应信息的携带内容包括基站身份信息和基站认证结果,所述基站认证结果包括用于表示基站非法或合法的标识信息;

[0032] 所述生成基站响应信息包括:

[0033] 通过所述会话密钥信息对基站响应信息的携带内容进行处理从而得到对应的基站响应信息。

[0034] 优选地,通过会话密钥信息对基站响应信息的携带内容进行处理包括:

[0035] 在鉴权中心生成的会话密钥信息包括加密密钥Ck的情况下,鉴权中心通过加密密钥Ck对基站响应信息的携带内容进行第一处理从而得到对应的基站响应信息;

[0036] 或,

[0037] 在鉴权中心生成的会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,鉴权中心先通过加密密钥Ck对基站响应信息的携带内容进行第一处理,再通过完整性保护密钥Ik对第一处理的结果进行第二处理,从而得到基站响应信息的携带内容对应的基站响应信息。

[0038] 为了达到上述目的,本发明还提出了一种终端接入方法,所述方法包括:

[0039] 基站接收终端发送的用户身份信息;

[0040] 基站将基站身份信息以及所述用户身份信息发送给鉴权中心

[0041] 基站接收鉴权中心发送的认证信息;

[0042] 基站将认证信息中的认证挑战信息发送给终端。

[0043] 优选地,在所述将基站身份信息以及所述用户身份信息发送给鉴权中心之后,所述方法还包括:

[0044] 基站接收鉴权中心发送基站响应信息;

[0045] 基站将所述基站响应信息发送给终端。

[0046] 为了达到上述目的,本发明还提出了一种终端接入装置,设置在终端上,所述装置包括:

[0047] 第一发送单元,用于将用户身份信息发送给基站;

[0048] 第一接收单元,用于接收基站所述发送的认证挑战信息和基站响应信息;

[0049] 检测单元,用于检测所述基站响应信息;

[0050] 接入单元,用于在检测通过的情况下,根据认证挑战信息接入到基站中。

[0051] 优选地,所述检测单元包括模块中的至少一个:

[0052] 第一检测模块,用于在基站响应信息的携带内容包括基站身份信息的情况下,终端获取基站响应信息对应的基站身份信息;

[0053] 判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致;如果不一致,则对基站响应信息的检测结果为不通过;如果一致,则对基站响应信息的检测结果为通过;

[0054] 第二检测模块,用于在基站响应信息的携带内容包括基站认证结果的情况下,获取基站响应信息对应的基站认证结果,如果基站认证结果为非法基站,则对基站响应信息的检测结果为不通过;如果基站认证结果为合法基站,则对基站响应信息的检测结果为通过;

[0055] 其中,第一检测模块和/或第二检测模块通过认证挑战信息获取会话密钥信息,通过所述会话密钥信息得到基站响应信息的携带内容。

[0056] 优选地,通过所述会话密钥信息得到基站响应信息的携带内容包括:

[0057] 在会话密钥信息包括加密密钥Ck的情况下,通过会话密钥信息中的加密密钥Ck对基站响应信息进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程;

[0058] 在密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,通过会话密钥信息中的完整性保护密钥Ik对基站响应信息进行第四处理,并通过会话密钥信息中的加密密钥Ck对第四处理的结果进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述

第一处理对应的逆处理过程,第四处理是与所述第二处理对应的逆处理过程;

[0059] 其中,第一处理是指鉴权中心为获取基站响应信息而通过加密密钥Ck对基站身份信息或基站认证结果进行的处理;第二处理是指鉴权中心为获取基站响应信息而通过完整性保护密钥Ik对第一处理的结果进行的处理。

[0060] 为了达到上述目的,本发明还提出了一种终端接入装置,设置在鉴权中心,所述装置包括:

[0061] 第二接收单元,用于接收基站发送的基站身份信息和用户身份信息;

[0062] 认证单元,用于根据所述基站身份信息对基站进行认证,根据用户身份信息对终端进行认证;

[0063] 处理单元,用于在对终端的认证通过的情况下,生成对应的认证信息,并将所述认证信息发送给基站。

[0064] 优选地,所述处理单元包括第一处理模块,用于在对基站的认证通过的情况下,执行所述生成对应的认证信息的过程;在对基站的认证没有通过的情况下,终止终端的接入过程。

[0065] 优选地,所述处理单元包括如下模块的任一个:

[0066] 第二处理模块,用于在对基站的认证通过的情况下,执行所述生成对应的认证信息的过程;并生成基站响应信息,并将所述基站响应信息发送给基站;在对基站的认证没有通过的情况下,终止终端的接入过程;

[0067] 第三处理模块,用于生成基站响应信息,并将所述基站响应信息发送给基站;其中,根据对基站的认证结果设置对应的基站响应信息。

[0068] 优选地,所述认证信息包括认证挑战信息、会话密钥信息,以及认证响应信息;

[0069] 第二处理模块生成的所述基站响应信息的携带内容包括基站身份信息;

[0070] 第三处理模块生成的基站响应信息的携带内容包括基站身份信息和基站认证结果,所述基站认证结果包括用于表示基站非法或合法的标识信息;

[0071] 所述第二处理模块和/或第三处理模块生成基站响应信息包括:

[0072] 通过所述会话密钥信息对基站响应信息的携带内容进行处理从而得到对应的基站响应信息。

[0073] 优选地,通过会话密钥信息对基站响应信息的携带内容进行处理包括:

[0074] 在鉴权中心生成的会话密钥信息包括加密密钥Ck的情况下,鉴权中心通过加密密钥Ck对基站响应信息的携带内容进行第一处理从而得到对应的基站响应信息;

[0075] 或,

[0076] 在鉴权中心生成的会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,鉴权中心先通过加密密钥Ck对基站响应信息的携带内容进行第一处理,再通过完整性保护密钥Ik对第一处理的结果进行第二处理,从而得到基站响应信息的携带内容对应的基站响应信息。

[0077] 为了达到上述目的,本发明还提出了一种终端接入装置,设置在基站,所述装置包括:

[0078] 第三接收单元,用于接收终端发送的用户身份信息;

[0079] 第三发送单元,用于将基站身份信息以及所述用户身份信息发送给鉴权中心;

- [0080] 所述第三接收单元还用于接收鉴权中心发送的认证信息；
- [0081] 所述第三发送单元还用于将认证信息中的认证挑战信息发送给终端。
- [0082] 优选地，所述第三接收单元还用于接收鉴权中心发送基站响应信息；
- [0083] 所述第三发送单元还用于将所述基站响应信息发送给终端。
- [0084] 与现有技术相比，本发明提供的技术方案包括：终端将用户身份信息发送给基站；终端接收基站所述发送的认证挑战信息和基站响应信息；终端检测所述基站响应信息，在检测通过的情况下，终端根据认证挑战信息接入到基站中。通过本发明的方案，在终端接入过程中，由鉴权中心对终端所附着的基站进行认证，可以由鉴权中心根据对基站的认证结果决定是否终止接入过程，也可以由鉴权中心将对基站的认证结果发送给终端，由终端确定是否连接到基站，通过该流程，改善了恶意基站通过欺骗的方式使得终端从一个合法基站转移附着到该恶意基站上的情况，提高了终端接入基站时的安全性。

附图说明

- [0085] 下面对本发明实施例中的附图进行说明，实施例中的附图是用于对本发明的进一步理解，与说明书一起用于解释本发明，并不构成对本发明保护范围的限制。
- [0086] 图1A和图1B为本发明实施例提供的一种终端接入方法的流程图；
- [0087] 图2为本发明实施例提供的另一种终端接入方法的流程图；
- [0088] 图3为本发明实施例提供的又一种终端接入方法的流程图；
- [0089] 图4为本发明实施例提供的一种终端接入装置的结构组成示意图；
- [0090] 图5为本发明实施例提供的另一种终端接入装置的结构组成示意图；
- [0091] 图6为本发明实施例提供的又一种终端接入装置的结构组成示意图。

具体实施方式

- [0092] 为了便于本领域技术人员的理解，下面结合附图对本发明作进一步的描述，并不能用来限制本发明的保护范围。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的各种方式可以相互组合。
- [0093] 参见图1A，本发明提出了一种终端接入方法，所述方法包括：
- [0094] 步骤110，终端将用户身份信息IMSI发送给基站；
- [0095] 步骤120，基站将基站身份信息和上述用户身份信息IMSI发送给鉴权中心；
- [0096] 步骤130，鉴权中心对基站进行认证；
- [0097] 步骤140，在对基站的认证没有通过的情况下，终止接入过程；
- [0098] 此外，鉴权中心还会对终端进行认证；在对终端的认证没有通过的情况下，也会终止接入过程，即附着过程。
- [0099] 在图1A所示的终端接入方法的基础上，如图1B所示，在步骤130之后，还包括：
- [0100] 步骤150，在鉴权中心对基站和终端的认证均通过的情况下，鉴权中心生成终端对应的认证信息；
- [0101] 本发明实施例中，认证信息包括认证挑战信息、会话密钥信息，以及认证响应信息。其中，会话密钥信息包括加密密钥Ck，或者会话密钥信息包括加密密钥Ck和完整性保护密钥Ik。

- [0102] 步骤160,鉴权中心将认证信息发送给基站;
- [0103] 步骤170,基站将认证信息中的认证挑战信息发送给终端;
- [0104] 基站获取认证信息中的会话密钥信息和认证响应信息,基站用获取的认证响应信息和终端发送的认证响应信息进行比对,以完成对终端的认证。在终端成功接入之后,基站将根据认证信息中获取的会话密钥信息与终端进行安全通信。
- [0105] 步骤180,终端接收基站发送的认证挑战信息,并根据认证挑战信息生成会话密钥信息和认证响应信息;
- [0106] 步骤190,终端根据认证响应信息接入到基站中。
- [0107] 其中,终端将生成的认证响应信息发送给基站,基站对从认证信息中获取的认证响应信息与终端发送的认证响应信息进行比对,在比对符合的情况下,允许终端接入到基站。在终端成功接入之后,终端将通过根据认证挑战信息生成的会话密钥信息与终端进行安全通信。
- [0108] 参见图2,本发明还提出了另一种终端接入方法,所述方法包括:
- [0109] 步骤210,终端将用户身份信息IMSI发送给基站;
- [0110] 步骤220,基站将基站身份信息和上述用户身份信息IMSI发送给鉴权中心;
- [0111] 其中,步骤220包括,基站将基站身份信息和上述用户身份信息IMSI发送给SGSN;SGSN将收到的基站身份信息和上述用户身份信息IMSI转发给鉴权中心;
- [0112] 步骤230,鉴权中心对基站和终端进行认证;在认证通过的情况下,鉴权中心生成基站响应信息和认证信息;在认证没有通过的情况下,终止附着过程。
- [0113] 其中,鉴权中心对基站和终端进行认证;在认证通过的情况下,鉴权中心生成基站响应信息和认证响应信息;鉴权中心对基站认证;在认证通过的情况下,鉴权中心生成基站响应信息;鉴权中心对终端进行认证;在认证通过的情况下,鉴权中心生成终端对应的认证信息。其中,对基站的认证和对终端的认证可以分别执行。
- [0114] 其中,步骤230具体包括:
- [0115] 步骤231,鉴权中心对基站身份信息进行验证,在验证通过的情况下,并执行步骤232,否则,终止附着过程。
- [0116] 步骤232,在对基站和终端的认证均通过的情况下,鉴权中心生成认证信息和基站响应信息,
- [0117] 其中,鉴权中心根据用户身份信息生成认证信息;
- [0118] 其中,生成的认证信息包括:认证挑战信息、会话密钥信息,以及认证响应信息;
- [0119] 其中,在会话密钥信息包括加密密钥Ck的情况下,
- [0120] 鉴权中心生成基站响应信息包括:鉴权中心通过加密密钥Ck对基站身份信息进行第一处理从而得到对应的基站响应信息;
- [0121] 或者,
- [0122] 在会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,
- [0123] 鉴权中心生成基站响应信息包括:鉴权中心先通过加密密钥Ck对基站身份信息进行第一处理,再通过完整性保护密钥Ik对第一处理的结果进行第二处理,从而得到基站身份信息对应的基站响应信息。
- [0124] 步骤240,鉴权中心将认证信息和基站响应信息发送给基站;

[0125] 步骤240具体包括:鉴权中心将认证信息和基站响应信息发送给SGSN;SGSN收到的将认证信息和基站响应信息转发给基站。

[0126] 步骤250,基站将收到的基站响应信息和认证信息中的认证挑战信息发送给终端;

[0127] 步骤260,终端根据收到的认证挑战信息和基站响应信息,获取所述基站响应信息对应的基站身份信息;

[0128] 可选地,终端通过认证挑战信息获取会话密钥信息,会话密钥信息包括加密密钥Ck,终端通过加密密钥Ck对基站响应信息进行第三处理,得到基站响应信息对应的基站身份信息;其中,第三处理是与所述第一处理对应的逆处理过程。

[0129] 可选地,终端通过认证挑战信息获取会话密钥信息,会话密钥信息包括加密密钥Ck和完整性保护密钥Ik,终端通过完整性保护密钥Ik对基站响应信息进行第四处理,并通过加密密钥Ck对第四处理的结果进行第三处理,得到基站响应信息对应的基站身份信息;其中,第三处理是与所述第一处理对应的逆处理过程,第四处理是与所述第二处理对应的逆处理过程。

[0130] 步骤270,终端判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致;如果不一致,则终端终止附着过程;如果一致,则执行步骤280。

[0131] 步骤280,在判断结果为一致的情况下,终端接入到基站中。

[0132] 其中,终端根据认证挑战生成认证响应信息,并将生成的认证响应信息发送给基站,基站对从认证信息中获取的认证响应信息与终端发送的认证响应信息进行比对,在比对符合的情况下,允许终端接入到基站。在终端成功接入之后,终端将通过根据认证挑战信息生成的会话密钥信息与终端进行安全通信。

[0133] 本发明实施例中,终端为CIoT终端设备。

[0134] 下面结合一个具体的应用场景进行说明。在终端附近存在合法基站A1和非法基站X1,两个基站位置相近,在终端设备接入到A1的过程,合法基站从鉴权中心获取终端对应的认证信息和基站响应信息之后,非法基站X1截获该合法基站A1获取的认证信息和基站响应信息,并将认证信息和基站响应信息发送给终端,终端在接收到非法基站X1发送的认证信息和基站响应信息之后,将执行接入到非法基站X1流程,根据本发明实施例的终端接入方法,终端在接收到非法基站X1发送的认证信息和基站响应信息之后,将判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致,由于基站响应信息对应的基站身份信息未合法基站A1的身份信息,而终端检测到的基站身份信息是非非法基站X1,不一致,因此,终端将终止接入到非法基站X1的附着过程。

[0135] 参见图3,本发明还提出了另一种终端接入方法,所述方法包括:

[0136] 步骤310,终端将用户身份信息IMSI发送给基站;

[0137] 步骤320,基站将基站身份信息和上述用户身份信息IMSI发送给鉴权中心;

[0138] 其中,步骤320包括,基站将基站身份信息和上述用户身份信息IMSI发送给SGSN;SGSN将收到的基站身份信息和上述用户身份信息IMSI转发给鉴权中心;

[0139] 步骤330,鉴权中心对基站和终端进行认证;在对终端的认证通过的情况下,鉴权中心生成基站响应信息和认证响应信息,根据对基站的认证结果设置基站响应信息;在终端认证没有通过的情况下,终止附着过程。

[0140] 其中,鉴权中心对基站和终端进行认证;在终端认证通过的情况下,鉴权中心生成

基站响应信息和认证响应信息包括：鉴权中心对终端进行认证；在对终端的认证通过的情况下，鉴权中心生成终端对应的认证信息，鉴权中心对基站认证；根据基站认证结果，设置对应的基站响应信息。其中，对基站的认证和对终端的认证可以分别执行。

[0141] 其中，步骤330具体包括：

[0142] 步骤331，鉴权中心对终端进行认证；

[0143] 步骤332，在对终端的认证通过的情况下，鉴权中心生成终端对应的认证信息，并根据对基站身份信息的认证结果，生成对应的基站响应信息。

[0144] 其中，鉴权中心根据用户身份信息生成认证信息；

[0145] 其中，生成的认证信息包括：认证挑战信息、会话密钥信息、以及认证响应信息；

[0146] 基站响应信息中包括基站身份信息和基站认证结果；

[0147] 其中，基站认证结果可以是用于表示基站非法或合法的标识信息；

[0148] 根据对基站身份信息的认证结果，生成对应的基站响应信息包括：在对基站的认证通过的情况下，在基站认证结果中携带表示基站合法的标识信息；在对基站的认证没有通过的情况下，在基站认证结果中携带表示基站非法的标识信息。

[0149] 其中，在会话密钥信息包括加密密钥Ck的情况下，鉴权中心通过加密密钥Ck对基站身份信息和基站认证结果进行第一处理从而得到对应的基站响应信息；

[0150] 或者，

[0151] 在会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下，鉴权中心先通过加密密钥Ck对基站身份信息和基站认证结果进行第一处理，再通过完整性保护密钥Ik对第一处理的结果进行第二处理，从而得到对应的基站响应信息。

[0152] 步骤340，鉴权中心将认证信息和基站响应信息发送给基站；

[0153] 步骤340具体包括：鉴权中心将认证信息和基站响应信息发送给SGSN；SGSN收到的将认证信息和基站响应信息转发给基站。

[0154] 步骤350，基站将收到的基站响应信息和认证信息中的认证挑战信息发送给终端；

[0155] 步骤360，终端根据收到的认证挑战信息和基站响应信息，获取认证信息中携带的基站认证结果；

[0156] 可选地，终端通过认证挑战信息获取会话密钥信息，在会话密钥信息包括加密密钥Ck的情况下，终端通过加密密钥Ck对基站响应信息进行第三处理，得到基站响应信息对应的基站身份信息和基站认证结果；其中，第三处理是与所述第一处理对应的逆处理过程。

[0157] 可选地，终端通过认证挑战信息获取会话密钥信息，在会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下，终端通过完整性保护密钥Ik对基站响应信息进行第四处理，并通过加密密钥Ck对第四处理的结果进行第三处理，得到基站响应信息对应的基站身份信息和基站认证结果；其中，第三处理是与所述第一处理对应的逆处理过程，第四处理是与所述第二处理对应的逆处理过程。

[0158] 步骤370，终端检测所述基站认证结果；如果基站认证结果为非法基站，则终端终止附着过程；如果基站认证结果为合法基站，则执行步骤380。

[0159] 步骤380，在基站认证结果为合法基站的情况下，终端接入到基站中。

[0160] 其中，终端根据认证挑战生成认证响应信息，并将生成的认证响应信息发送给基站，基站对从认证信息中获取的认证响应信息与终端发送的认证响应信息进行比对，在比

对符合的情况下,允许终端接入到基站。在终端成功接入之后,终端将通过根据认证挑战信息生成的会话密钥信息与终端进行安全通信。

[0161] 下面通过一个表1对上述各个实施例中鉴权中心的处理进行说明。其中,认证结果为1说明认证通过,为0表示认证没有通过,其中,对于终端和基站认证均不通过的处理为终止接入过程,在表1中没有示出。

[0162]

	认证情况 1		认证情况 2		认证情况 3	
认证目标	终端	基站	终端	基站	终端	基站
认证结果	1	1	1	0	0	1
根据图 1 方法的处理结果	发送认证信息		终止接入过程		终止接入过程	
根据图 2 方法的处理结果	发送认证信息和基站响应信息,基站响应信息中携带基站身份信息		终止接入过程		终止接入过程	
根据图 3 方法的处理结果	发送认证信息和基站响应信息,基站响应信息中携带表示合法基站的基站认证结果		发送认证信息和基站响应信息,基站响应信息中携带表示非法基站的基站认证结果		终止接入过程	

[0163] 表1 鉴权中心根据认证结果执行不同处理流程的示意图

[0164] 基于与上述实施例相同或相似的构思,本发明实施例还提供一种终端接入装置,设置在终端上,参见图4,本发明实施例提出的一种终端接入装置包括:

[0165] 第一发送单元10,用于将用户身份信息发送给基站;

[0166] 第一接收单元20,用于接收基站所述发送的认证挑战信息和基站响应信息;

[0167] 检测单元30,用于检测所述基站响应信息;

[0168] 接入单元40,用于在检测通过的情况下,根据认证挑战信息接入到基站中。

[0169] 本发明实施例中,所述检测单元30包括以下模块中的至少一个:

[0170] 第一检测模块,用于在基站响应信息的携带内容包括基站身份信息的情况下,终端获取基站响应信息对应的基站身份信息;

[0171] 判断基站响应信息对应的基站身份信息和终端检测到的基站身份信息是否一致;如果不一致,则对基站响应信息的检测结果为不通过;如果一致,则对基站响应信息的检测结果为通过;

[0172] 第二检测模块,用于在基站响应信息的携带内容包括基站认证结果的情况下,获取基站响应信息对应的基站认证结果,如果基站认证结果为非法基站,则对基站响应信息的检测结果为不通过;如果基站认证结果为合法基站,则对基站响应信息的检测结果为通过。

[0173] 其中,第一检测模块和/或第二检测模块通过认证挑战信息获取会话密钥信息,通过所述会话密钥信息得到基站响应信息的携带内容。

[0174] 本发明实施例中,通过所述会话密钥信息得到基站响应信息的携带内容包括:

[0175] 在会话密钥信息包括加密密钥Ck的情况下,通过会话密钥信息中的加密密钥Ck对基站响应信息进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程;

[0176] 在密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下,通过会话密钥信息中的完整性保护密钥Ik对基站响应信息进行第四处理,并通过会话密钥信息中的加密密钥Ck对第四处理的结果进行第三处理,得到基站响应信息的携带内容;其中,第三处理是与所述第一处理对应的逆处理过程,第四处理是与所述第二处理对应的逆处理过程;

[0177] 其中,第一处理是指鉴权中心为获取基站响应信息而通过加密密钥Ck对基站身份信息或基站认证结果进行的处理;第二处理是指鉴权中心为获取基站响应信息而通过完整性保护密钥Ik对第一处理的结果进行的处理。

[0178] 基于与上述实施例相同或相似的构思,本发明实施例还提供一种终端接入装置,设置在鉴权中心上,参见图5,本发明实施例提出的一种终端接入装置包括:

[0179] 第二接收单元50,用于接收基站发送的基站身份信息和用户身份信息;

[0180] 认证单元60,用于根据所述基站身份信息对基站进行认证,根据用户身份信息对终端进行认证;

[0181] 处理单元70,用于在对终端的认证通过的情况下,生成对应的认证信息,并将所述认证信息发送给基站。

[0182] 本发明实施例中,所述处理单元70包括第一处理模块,用于在对基站的认证通过的情况下,执行所述生成对应的认证信息的过程;在对基站的认证没有通过的情况下,终止终端的接入过程。

[0183] 本发明实施例中,在另一个示例中,所述处理单元包括如下模块的任一个:

[0184] 第二处理模块,用于在对基站的认证通过的情况下,执行所述生成对应的认证信息的过程;并生成基站响应信息,并将所述基站响应信息发送给基站;在对基站的认证没有通过的情况下,终止终端的接入过程;

[0185] 第三处理模块,用于生成基站响应信息,并将所述基站响应信息发送给基站;其中,根据对基站的认证结果设置对应的基站响应信息。

[0186] 本发明实施例中,所述认证信息包括认证挑战信息、会话密钥信息,以及认证响应

信息；

[0187] 第二处理模块生成的所述基站响应信息的携带内容包括基站身份信息；

[0188] 第三处理模块生成的所述基站响应信息的携带内容包括基站身份信息和基站认证结果，所述基站认证结果包括用于表示基站非法或合法的标识信息；

[0189] 所述第二处理模块和/或第三处理模块生成基站响应信息包括：

[0190] 通过所述会话密钥信息对基站响应信息的携带内容进行处理从而得到对应的基站响应信息。

[0191] 本发明实施例中，通过会话密钥信息对基站响应信息的携带内容进行处理包括：

[0192] 在鉴权中心生成的会话密钥信息包括加密密钥Ck的情况下，鉴权中心通过加密密钥Ck对基站响应信息的携带内容进行第一处理从而得到对应的基站响应信息；

[0193] 或，

[0194] 在鉴权中心生成的会话密钥信息包括加密密钥Ck和完整性保护密钥Ik的情况下，鉴权中心先通过加密密钥Ck对基站响应信息的携带内容进行第一处理，再通过完整性保护密钥Ik对第一处理的结果进行第二处理，从而得到基站响应信息的携带内容对应的基站响应信息。

[0195] 基于与上述实施例相同或相似的构思，本发明实施例还提供一种终端接入装置，设置在基站上，参见图6，本发明实施例提出的一种终端接入装置包括：

[0196] 第三接收单元80，用于接收终端发送的用户身份信息；

[0197] 第三发送单元90，用于将基站身份信息以及所述用户身份信息发送给鉴权中心；

[0198] 所述第三接收单元80还用于接收鉴权中心发送的认证信息；

[0199] 所述第三发送单元90还用于将认证信息中的认证挑战信息发送给终端。

[0200] 本发明实施例中，

[0201] 所述第三接收单元80还用于接收鉴权中心发送基站响应信息；

[0202] 所述第三发送单元90还用于将所述基站响应信息发送给终端。

[0203] 基于与上述实施例相同或相似的构思，本发明实施例还提供一种终端，所述终端包括本发明实施例提供的任一设置在终端上的终端接入装置。

[0204] 基于与上述实施例相同或相似的构思，本发明实施例还提供一种基站，所述基站包括本发明实施例提供的任一设置在基站上的终端接入装置。

[0205] 基于与上述实施例相同或相似的构思，本发明实施例还提供一种鉴权中心，所述鉴权中心包括本发明实施例提供的任一设置在鉴权中心上的终端接入装置。

[0206] 需要说明的是，以上所述的实施例仅是为了便于本领域的技术人员理解而已，并不用于限制本发明的保护范围，在不脱离本发明的发明构思的前提下，本领域技术人员对本发明所做出的任何显而易见的替换和改进等均在本发明的保护范围之内。

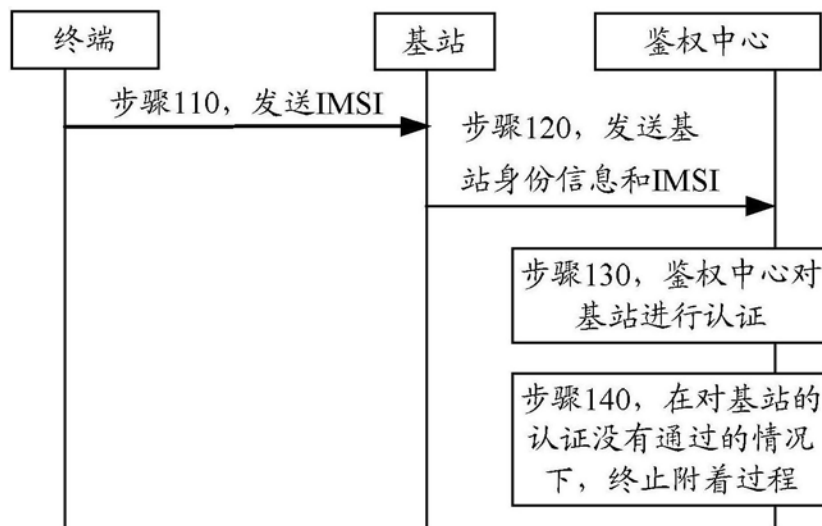


图1A

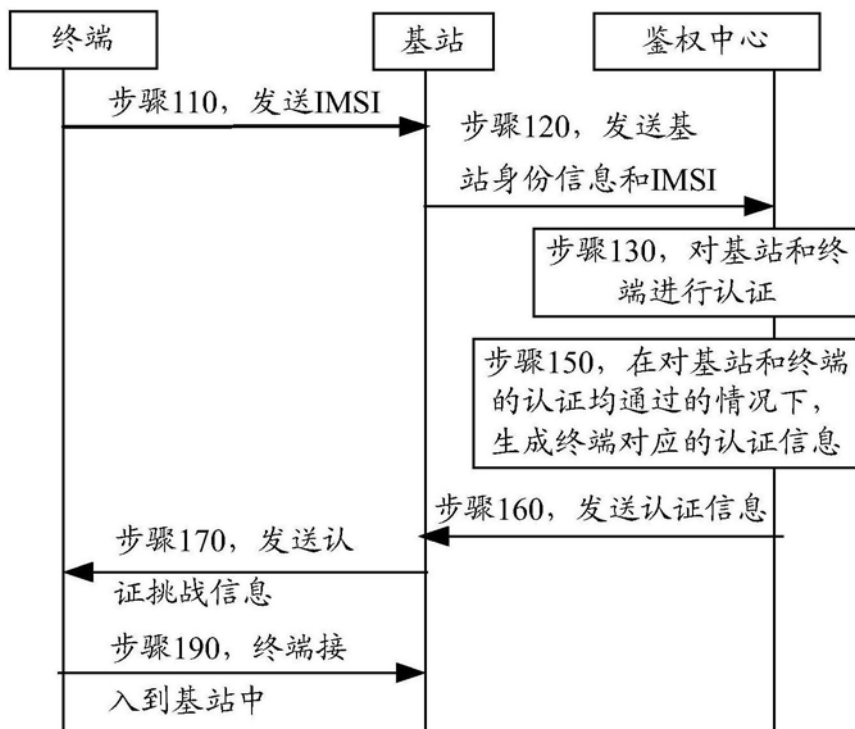


图1B

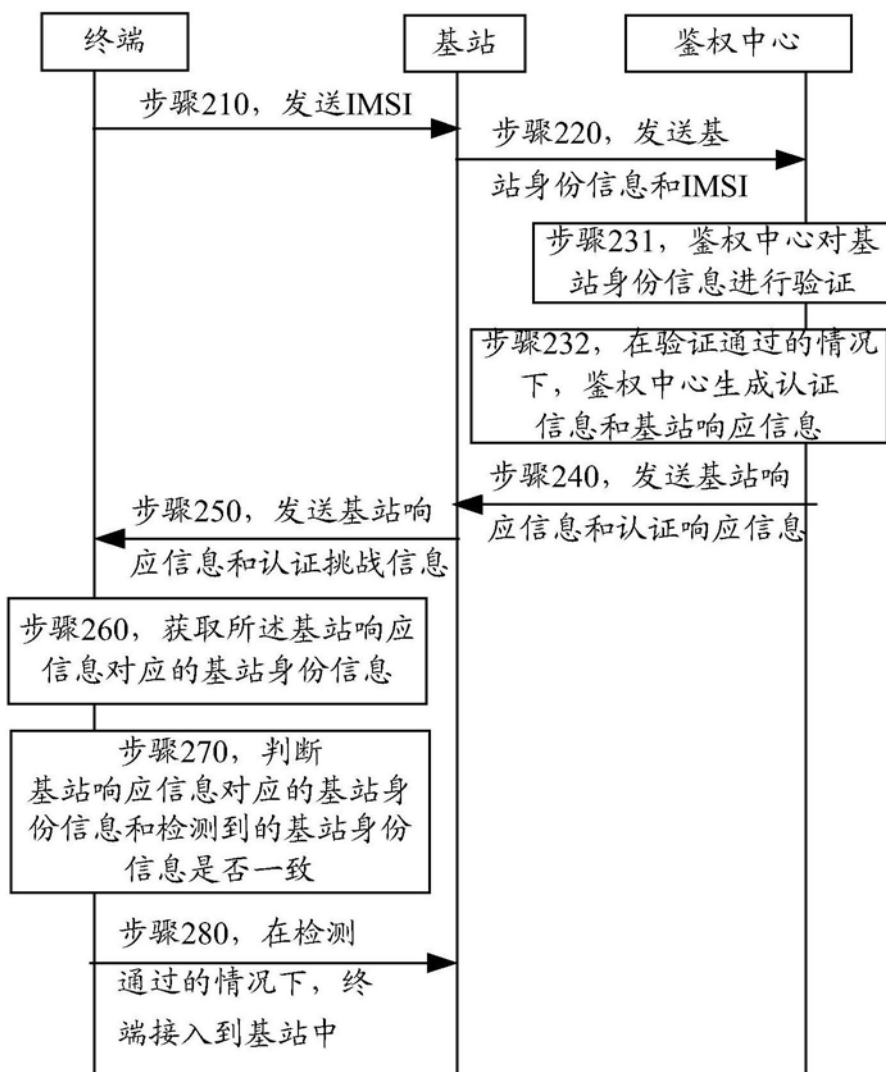


图2

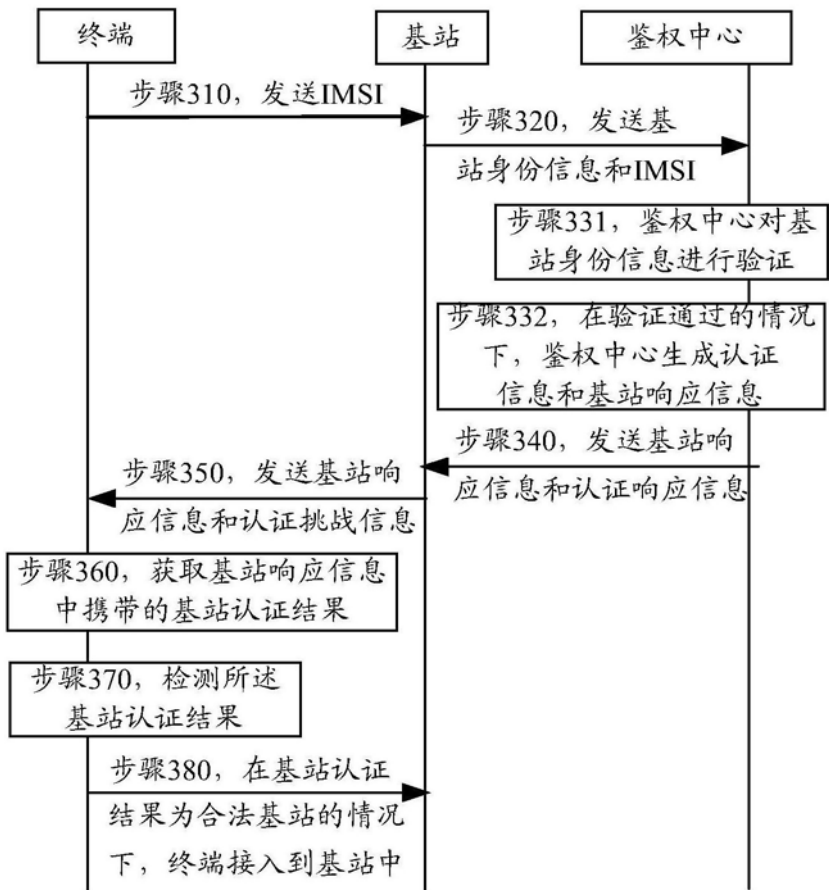


图3

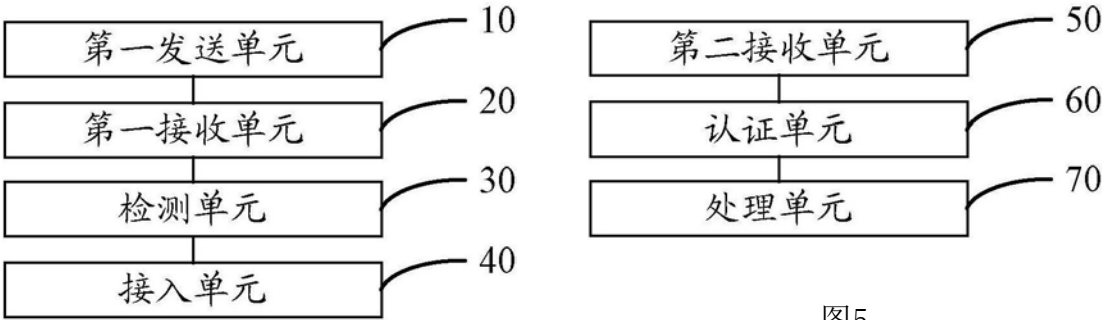


图5

图4

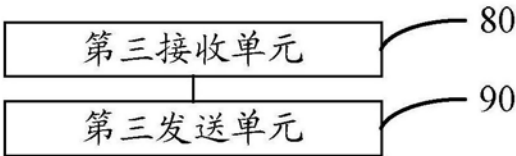


图6