(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 101640887 B
(45)授权公告日 2012.10.03

(21)申请号 200810041298.5

(22)申请日 2008.07.29

(73)专利权人 上海华为技术有限公司
地址 200121 上海市浦东新区宁桥路615号

(72)发明人 刘菁 陈璟 彭炎 张爱琴

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 逯长明

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)

(56)对比文件
WO 2007/046630 A2,2007.04.26, 全文.
CN 1802018 A,2006.07.12, 全文.
3GPP.3GPP TS 33.102 V7.1.0,“3G Security
Security architecture(Release 7)”.《3GPP》.2006, 全文.
A.Niemi 等.RFC 3310,“Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”.《RFC》.2002, 全文.
周星 等.基于AKA的IMS接入认证机制.《中兴通讯技术》.2007, 第13卷(第6期),42-47.
范絮妍等.基于GSM-R网络的端到端通信认证机制.《GSM-R移动通信及无线电管理学术会议论文集(2006)》.2006,39-43.

审查员 王宇锋

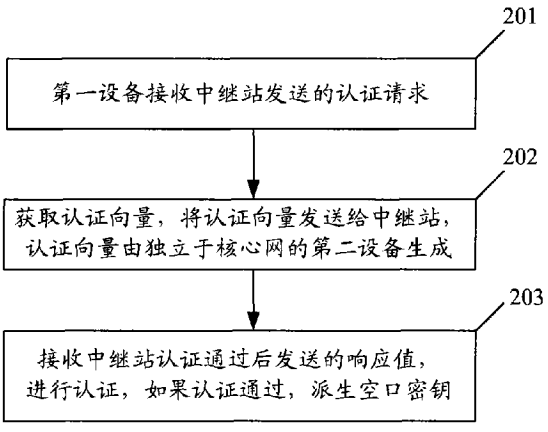
权利要求书 2 页 说明书 9 页 附图 6 页

(54)发明名称

鉴权方法、通信装置和通信系统

(57)摘要

本发明实施例公开了鉴权方法、通信装置和通信系统,鉴权方法包括:第一设备接收中继站发送的认证请求,认证请求包含中继站身份标识;获取认证向量,向中继站发送所述认证向量,指示中继站对认证向量进行认证,认证向量由独立于核心网的第二设备生成,与中继站身份标识对应;接收中继站对所述认证向量认证通过后发送的响应值,对响应值进行认证,当认证通过时,派生空口密钥。本发明实施例通过在接入网侧引入一个逻辑实体,由接入网侧完成对中继站的身份认证及密钥派生,将中继站的鉴权功能完全限定在接入网侧实现,从而避免接入网引入中继站后对核心网的改动,使得引入中继站后的系统对整个网络的影响达到最小化。



CN 101640887 B

1. 一种鉴权方法，其特征在于，包括：

第一设备接收中继站发送的认证请求，所述认证请求包含中继站身份标识；

所述第一设备获取认证向量，向所述中继站发送所述认证向量，指示所述中继站对所述认证向量进行认证，所述认证向量由独立于核心网的第二设备生成，与所述中继站身份标识对应；

所述第一设备接收所述中继站对所述认证向量认证通过后发送的响应值，对所述响应值进行认证，当认证通过时，派生空口密钥；

其中，所述第一设备为基站，所述第二设备为中继站数据库 RSDA。

2. 根据权利要求 1 所述的鉴权方法，其特征在于，所述中继站数据库 RSDA 与所述基站相连；

所述第一设备获取认证向量的步骤具体为：

所述第一设备接收所述第二设备发送的认证向量。

3. 根据权利要求 1 所述的鉴权方法，其特征在于，所述中继站数据库 RSDA 的物理位置与所述基站集成在一起，或者，所述中继站数据库 RSDA 的物理位置与所述基站不重合。

4. 根据权利要求 1 至 3 任一项所述的鉴权方法，其特征在于，所述独立于核心网的第二设备生成认证向量的步骤具体为：

所述独立于核心网的第二设备查找与所述中继站身份标识对应的共享密钥，产生随机数，生成与所述共享密钥和所述随机数对应的所述认证向量。

5. 根据权利要求 1 至 3 任一项所述的鉴权方法，其特征在于，所述认证向量包括期望响应值；

所述对所述响应值进行认证的步骤具体为：

将所述响应值与所述认证向量中的所述期望响应值进行比较，如果一致，认证通过。

6. 根据权利要求 2 或 3 所述的鉴权方法，其特征在于，所述派生空口密钥的步骤后还包括：

基站派生与所述空口密钥对应的加密密钥和完整性保护的密钥。

7. 根据权利要求 3 所述的鉴权方法，其特征在于，所述派生空口密钥的步骤后还包括：

中继站数据库 RSDA 将所述空口密钥发送给基站，指示所述基站派生与所述空口密钥对应的加密密钥和完整性保护的密钥。

8. 一种通信装置，其特征在于，包括：

请求接收单元，用于接收中继站发送的认证请求，所述认证请求包含中继站身份标识；

获取单元，用于获取认证向量，所述认证向量由独立于核心网的第二设备生成，与所述中继站身份标识对应，所述第二设备为中继站数据库 RSDA；

认证向量发送单元，用于向所述中继站发送所述获取单元获取的所述认证向量，指示所述中继站对所述认证向量进行认证；

响应值接收单元，用于接收所述中继站对所述认证向量发送单元发送的所述认证向量认证通过后发送的响应值；

认证单元，用于对所述响应值接收单元接收的所述响应值进行认证；

空口密钥派生单元，用于在所述认证单元对所述响应值认证通过时，派生空口密钥。

9. 根据权利要求 8 所述的通信装置，其特征在于，还包括：

密钥派生单元，用于派生与所述空口密钥派生单元派生的所述空口密钥对应的加密密钥和完整性保护的密钥。

10. 一种通信系统，其特征在于，包括：

中继站，用于向第一设备发送认证请求，所述认证请求包含中继站身份标识，接收第一设备发送的认证向量，对所述认证向量进行认证，认证通过后生成响应值，向第一设备发送所述响应值；

第一设备，用于接收所述中继站发送的认证请求，获取认证向量，向所述中继站发送所述认证向量，接收所述中继站对所述认证向量认证通过后发送的所述响应值，对所述响应值进行认证，当认证通过时，派生空口密钥；

独立于核心网的第二设备，用于生成认证向量，所述认证向量与所述中继站身份标识对应；

所述第一设备为基站，所述第二设备为中继站数据库 RSDA。

11. 根据权利要求 10 所述的通信系统，其特征在于，所述中继站数据库 RSDA 与所述基站相连。

12. 根据权利要求 10 所述的通信系统，其特征在于，所述中继站数据库 RSDA 的物理位置与所述基站集成在一起，或者，所述中继站数据库 RSDA 的物理位置与所述基站不重合。

鉴权方法、通信装置和通信系统

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及鉴权方法、通信装置和通信系统。

背景技术

[0002] 随着移动系统的覆盖范围越来越大，用户接入系统的数目逐渐增多，服务提供商提供的服务多元化发展，使得网络的复杂程度不断提高，如何保证网络和业务信息的安全是一个当前迫切需要解决的问题。

[0003] 在移动通信系统中，为了保证运营业务的安全性，网络侧需要对接入的用户设备(User Equipment，UE)进行鉴权处理，使得非法UE无法得到网络侧提供的服务，保障运营商的利益；同时，UE也需要验证网络侧发送的鉴权信息是否有效，即UE对网络侧进行鉴权处理，防止非法网络侧利用合法网络侧已经使用过的鉴权信息对UE进行重放攻击，使UE相信该非法网络侧合法。

[0004] 现有长期演进(Long Term Evolved，LTE)网络系统中，UE和演进的基站(E-UTRAN Node B，eNB)之间的空口链路是单跳的，采用演进的分组系统(Evolved Packet System，EPS)认证和密钥协商(Authentication and KeyAgreement，AKA)协议来完成用户和网络侧的鉴权过程，即包括身份认证和密钥协商的处理，其实现的基础是用户和网络侧预共享一个永久性对称密钥。整个鉴权过程包含在一个鉴权处理中进行，并且采用鉴权元组的方式来进行认证，鉴权元组包括：包括：随机数(RAND)、期望响应(Expected userResponse，XRES)、密钥(K_{ASME})和鉴权令牌(Authentication token，AUTN)，其中，密钥是由加密密钥(Cipher Key，CK)和完整性密钥(Integrity Key，IK)共同派生的；其中，AUTN进一步包括鉴权序列号(Sequence Number，SQN)、鉴权管理域(Authentication Management Field，AMF)和消息鉴权编码(Message Authentication Code，MAC)三个部分。

[0005] 引入中继站(Relay Station，RS)后，LTE系统中UE和eNB之间的空口链路被分段，包括UE和RS之间的接入链路，以及RS和eNB之间的中继链路。RS的网络接入过程中，可以将RS看作为UE进行网络接入，即RS采用与传统UE相同的鉴权过程，具体接入过程参见图1，RS接入过程中的鉴权处理流程为：

[0006] 步骤101：RS向移动性管理实体(Mobility Management Entity，MME)发送认证请求，该消息中携带了RS的国际移动用户标识(International MobileSubscriber Identity，IMSI)、RS的能力(即所支持的加密和完整性保护算法)、以及派生密钥(K_{ASME})所对应的密钥标识符(KSI_{ASME})等内容；

[0007] 步骤102：MME向归属用户服务器(Home Subscriber Server，HSS)转发RS的认证请求，该消息中携带了RS的身份标识IMSI、服务网络标识等内容，HSS根据RS的IMSI找到该用户对应的共享密钥K，并随机产生一个RAND，然后根据RAND、自身当前保存的鉴权SQN、RS和HSS共享密钥K及其它信息生成该RS对应的认证向量(Authentication Vector，AV)，其中AV包括RAND、XRES、K_{ASME}和AUTN；

[0008] 步骤103：HSS向MME返回认证响应，该消息中携带了该用户的认证向量AV，以及

密钥 K_{ASME} 所对应的密钥标识符 KSI_{ASME} 等内容，MME 将收到的该 RS 的认证向量进行保存；

[0009] 步骤 104：MME 向 RS 发送 RS 认证请求，该消息中携带了该 RS 认证向量中对应的 RAND 和 AUTN，以及密钥 K_{ASME} 所对应的密钥标识符 KSI_{ASME} 等内容；

[0010] 步骤 105：RS 根据收到的 RAND 和 AUTN，进行校验，包括：根据 RAND、AUTN 中的 SQN 和与网络侧共享的密钥 K 共同计算出一个 MAC 值，并比较该 MAC 值和从接收到的 AUTN 中解析的 MAC 值是否一致，如果一致，则 RS 对网络侧的鉴权通过，则利用 RAND 和与网络侧共享的密钥 K 共同计算出一个响应 (Response，RES) 发送给 MME；

[0011] 步骤 106：MME 比较从 RS 接收到的 RES 与本地存贮该用户 AV 中的 XRES 是否一致，如果一致，网络侧对 RS 的鉴权通过，则 MME 根据密钥 K_{ASME} 进一步派生出空口密钥 K_{eNB}，并通过安全模式命令 (Security Mode Command，SMC) 将该空口密钥以及 RS 所支持的加密和完整性保护算法下发给 eNB；

[0012] 步骤 107：eNB 根据收到的 RS 所支持的加密和完整性保护算法，以及自身支持的加密和完整性保护算法，确定空口用户面和控制面的加密和完整性保护密钥的算法，并将选定的算法通过 SMC 下发给 RS，此时，RS 和 eNB 可以各自利用空口密钥 K_{eNB} 通过选定的密钥算法进一步派生出用户空口加密和完整性保护的密钥。

[0013] 在实现本发明的过程中，发明人发现上述技术方案至少存在如下缺陷：

[0014] 接入网和核心网分属于不同的网络运营商，随着不同接入技术的不断出现，核心网运营商不希望由于接入网的变化而导致核心网的频繁变动。然而，在现有技术中，在引入 RS 后的 LTE 系统中，RS 的鉴权过程必然需要对核心网的 HSS 进行相应的修改，即增加 HSS 对 RS 的安全上下文信息的存贮。

发明内容

[0015] 本发明实施例提供鉴权方法、通信装置和通信系统，能够避免接入网引入 RS 后对核心网的改动。

[0016] 为解决上述问题，本发明实施例是通过以下技术方案来实现的：

[0017] 一种鉴权方法，包括：

[0018] 第一设备接收中继站发送的认证请求，认证请求包含中继站身份标识；

[0019] 第一设备获取认证向量，向中继站发送认证向量，指示中继站对认证向量进行认证，认证向量由独立于核心网的第二设备生成，与中继站身份标识对应；

[0020] 第一设备接收中继站对认证向量认证通过后发送的响应值，对响应值进行认证，当认证通过时，派生空口密钥。

[0021] 一种通信装置，包括：

[0022] 请求接收单元，用于接收中继站发送的认证请求，认证请求包含中继站身份标识；

[0023] 获取单元，用于获取认证向量，认证向量由独立于核心网的第二设备生成，与中继站身份标识对应；

[0024] 认证向量发送单元，用于向中继站发送获取单元获取的认证向量，指示中继站对认证向量进行认证；

[0025] 响应值接收单元，用于接收中继站对认证向量发送单元发送的认证向量认证通过

后发送的响应值；

[0026] 认证单元，用于对响应值接收单元接收的响应值进行认证；

[0027] 空口密钥派生单元，用于在认证单元对所述响应值认证通过时，派生空口密钥。

[0028] 一种通信系统，包括：

[0029] 中继站，用于向第一设备发送认证请求，上述认证请求包含中继站身份标识，接收第一设备发送的认证向量，对上述认证向量进行认证，认证通过后生成响应值，向第一设备发送所述响应值；

[0030] 第一设备，用于接收中继站发送的认证请求，上述认证请求包含中继站的身份标识，获取认证向量，向中继站发送上述认证向量，接收中继站对上述认证向量认证通过后发送的上述响应值，对上述响应值进行认证，当认证通过时，派生空口密钥；

[0031] 独立于核心网的第二设备，用于生成认证向量，上述认证向量与上述中继站身份标识对应。

[0032] 可见，由于本发明实施例接入网侧接收 RS 发送的认证请求，生成认证向量并发送给 RS，接收 RS 对认证向量认证通过后发送的响应值，对响应值进行认证，认证通过后派生空口密钥，完成对 RS 的鉴权。在接入网侧引入一个网络逻辑实体，由接入网侧的逻辑实体与中继站共享了共享密钥，由接入网侧完成对 RS 的身份认证及密钥派生，从而完成中继站的网络安全接入，因此中继站的网络安全接入不需要对核心网进行改动就可以实现，使得引入 RS 后的系统对整个网络的影响达到最小化。

附图说明

[0033] 图 1 是现有技术中继站接入鉴权的信令图；

[0034] 图 2 是实现本发明实施例一的方法的流程图；

[0035] 图 3 是实现本发明实施例二的方法的信令图；

[0036] 图 4 是实现本发明实施例三的方法的信令图；

[0037] 图 5 是实现本发明实施例四的方法的信令图；

[0038] 图 6 是实现本发明实施例通信装置的示意图；

[0039] 图 7 是实现本发明实施例通信系统的组成框图。

具体实施方式

[0040] 本发明实施例提供鉴权方法、通信装置和通信系统，能够避免由于接入网引入 RS 后而造成对核心网的改动。

[0041] RS 是一种接入网设备，大多数情况下，RS 在网络中可能是由接入网运营商直接部署的，即 RS 和 eNB 同属于一个运营商。为了使得引入 RS 后对整个网络的影响最小化，可以考虑将引入 RS 的影响只限定在接入网侧，即通过在接入网引入一个逻辑实体 (Relay Station Database，RSDA)，由 RSDA 完成对 RS 的身份验证及密钥派生等鉴权功能，该逻辑实体存贮了 RS 所有相关的上下文信息。因此，引入 RS 后的 LTE 系统，不需要对核心网进行改动就可以使得 RS 安全的接入网络，从而达到对网络影响最小化。

[0042] 本发明实施例提出的鉴权方法，其实现的基础是 RS 和逻辑实体 RSDA 之间预共享一个永久性密钥 K，并采用 AKA 协议完成 RS 和网络侧的身份认证和密钥派生。

[0043] 本发明实施例根据 RSDA 的物理位置与 eNB 是否重合以及由 eNB 还是 RSDA 对 RS 进行身份认证，给出了相应的实施例，以下分别进行详细说明。

[0044] 实施例一

[0045] 本实施例提供的方案中，由接入网侧的第一设备和第二设备一起完成对 RS 的鉴权，引入 RS 后支持对称性密钥认证方式的各种系统都可以对 RS 进行鉴权，因此后续实施例中的 eNB 都可以为支持对称性密钥认证方式的基站。

[0046] 参见图 2，该方法包括：

[0047] 步骤 201：第一设备接收 RS 发送的认证请求，认证请求包含中继站身份标识；

[0048] 认证请求可以被包含在认证请求消息中。

[0049] 步骤 202：第一设备获取认证向量，，将认证向量发送给所述 RS，指示 RS 对认证向量进行认证，上述认证向量由独立于核心网的第二设备生成，与 RS 身份标识对应；

[0050] 独立于核心网的第二设备查找与 RS 身份标识对应的共享密钥，产生随机数，生成与共享密钥和随机数对应的认证向量。

[0051] 上述第一设备可以为基站，独立于核心网的第二设备为逻辑实体，基站与逻辑实体相连。

[0052] 第一设备为基站，独立于核心网的第二设备为逻辑实体，所述逻辑实体集成在所述基站中。

[0053] 第一设备和独立于核心网的第二设备为同一逻辑实体。

[0054] 上述基站也可以是 eNB。

[0055] 步骤 203：接收 RS 认证通过后发送的响应值，对所述响应值进行认证，如果认证通过，派生空口密钥。

[0056] 接收 RS 认证通过后发送的响应值，将响应值与认证向量中的期望响应值进行比较，如果一致，认证通过，派生空口密钥，确定与所述 RS 的能力对应的密钥派生算法，还可以将所述密钥派生算法发送给 RS，RS 才能派生与密钥派生算法对应的加密和完整性保护密钥。

[0057] 至此，接入网侧已经完成对 RS 的鉴权，为了后续 RS 和接入网侧能够安全通信，还可以包含一个步骤：派生与所述空口密钥对应的加密密钥和完整性保护的密钥。

[0058] 上述派生加密密钥和完整性保护的密钥由接入网侧的基站派生，也可以是由 eNB 派生。

[0059] 本实施例中，接入网侧通过接收 RS 发送的认证请求，生成认证向量并发送给 RS，接收 RS 对认证向量认证通过后发送的响应值，对响应值进行认证，认证通过后派生空口密钥，完成对 RS 的鉴权。本实施例将 RS 的鉴权功能完全限定在接入网侧，从而避免接入网引入 RS 后对核心网的改动，使得引入 RS 后的系统对整个网络的影响达到最小化。

[0060] 实施例一是从接入网侧实现鉴权的方法，实施例二是通过 RS 和 eNB/RSDA 之间具体的信令交互来说明实现鉴权的方法。

[0061] 实施例二

[0062] 本实施例是当 RSDA 的物理位置与 eNB 集成在一起，由 eNB/RSDA 来完成对 RS 的鉴权。引入 RS 后支持对称性密钥认证方式的各种系统都可以对 RS 进行鉴权，因此本实施例中的 eNB 都可以为支持对称性密钥认证方式的基站。下面结合附图进行详细说明。

[0063] 参见图 3，下面对实现实施例二的方法的具体步骤进行详细介绍：

[0064] 步骤 301：RS 向 eNB/RSDA 发送认证请求；

[0065] 所述认证请求可以被包含在认证请求消息中，该消息中携带了 RS 身份标识、所支持的加密和完整性保护算法，以及 eNB/RSDA 派生密钥 $K_{ASME-RS}$ 所对应的密钥标识符 $KSI_{ASME-RS}$ 等内容，其中 RS 的身份标识可以是 RS 的 IMSI，也可以是 RS 的 MAC 地址等。

[0066] 步骤 302：eNB/RSDA 生成 AV；

[0067] eNB/RSDA 根据 RS 身份标识找到该 RS 对应的共享密钥 K，并随机产生一个 RAND，然后根据 RAND、自身当前保存的 SQN、RS 和 RSDA 之间共享的密钥 K 及其它信息生成该 RS 对应的 AV，其中，AV 包括 RAND、XRES、$K_{ASME-RS}$、AUTN；还可以采用其它的参数来生成 AV，本发明实施例并不限定生成 AV 的参数。

[0068] 步骤 303：eNB/RSDA 向 RS 返回认证响应；

[0069] 该响应消息中携带了该 RS 的 AV 中对应的 RAND 和 AUTN，以及密钥 $K_{ASME-RS}$ 所对应的密钥标识符 $KSI_{ASME-RS}$ 等内容。

[0070] 步骤 304：RS 进行认证，并生成 RES 值；

[0071] RS 根据收到的 RAND 和 AUTN，进行校验，包括：根据 RAND、AUTN 中的 SQN 和与 RSDA 共享的密钥 K 共同计算出一个 MAC 值，并比较该 MAC 值和从接收到的 AUTN 中解析的 MAC 值是否一致，如果一致，RS 对网络侧鉴权通过，则利用 RAND 和与 RSDA 共享的密钥 K 共同计算出一个 RES 值。

[0072] 步骤 305：RS 向 eNB/RSDA 返回 RES 值；

[0073] 步骤 306：eNB/RSDA 进行认证，并派生出空口密钥 K_{eNB-RS}；

[0074] eNB/RSDA 比较从 RS 接收到的 RES 与之前生成该 RS 的 AV 中的 XRES 是否一致，如果一致，网络侧对 RS 的鉴权通过，则 eNB/RSDA 根据密钥 $K_{ASME-RS}$ 进一步派生出空口密钥 K_{eNB-RS}。

[0075] 至此，已经实现接入网侧的 eNB/RSDA 对 RS 的鉴权，为了后续 RS 与接入网侧之间安全通信，还可以执行以下的步骤。

[0076] 步骤 307：eNB/RSDA 通过 SMC 向 RS 发送空口密钥 K_{eNB-RS} 和确定的加密算法和完整性保护算法；

[0077] eNB/RSDA 结合 RS 支持的加密和完整性保护算法以及自身支持的加密和完整性保护算法，确定空口用户面和控制面加密密钥和完整性保护密钥的密钥派生算法，并通过 SMC 将空口密钥 K_{eNB-RS} 和确定的密钥派生算法发送给 RS。

[0078] 步骤 308：RS 和 eNB/RSDA 派生出空口加密密钥和完整性保护的密钥。

[0079] RS 和 eNB/RSDA 就可以各自利用空口密钥 K_{eNB-RS} 通过选定的密钥算法进一步派生出空口加密密钥和完整性保护的密钥。

[0080] 本实施例通过在接入网侧将 RSDA 和 eNB 集成在一起，将 RS 的鉴权功能完全限定在接入网侧，从而避免由于接入网引入 RS 后而造成对核心网的改动，使得引入 RS 后的系统对整个网络的影响达到最小化。

[0081] 实施例二是 RSDA 的物理位置与 eNB 重合，由 RS 和 eNB/RSDA 实体来完成对 RS 的鉴权的实现本发明的方法，下面介绍当 RSDA 的物理位置和 eNB 不重合时实现本发明方法的实施例，而根据身份认证位置的不同，又可以分为两种情况，给出了对应的实施例。

[0082] 实施例三

[0083] 在本实施例中，身份认证位于 eNB 上，则由 eNB 完成 RS 的鉴权功能。引入 RS 后支持对称性密钥认证方式的各种系统都可以对 RS 进行鉴权，因此本实施例中的 eNB 都可以为支持对称性密钥认证方式的基站。下面结合附图进行详细说明。

[0084] 参见图 4，下面对实现实施例三的方法的具体步骤进行详细介绍：

[0085] 步骤 401：RS 向 eNB 发送认证请求；

[0086] 所述认证请求可以被包含在认证请求消息中，该消息中携带了 RS 身份标识、所支持的加密和完整性保护算法，以及派生密钥 $K_{ASME-RS}$ 对应的密钥标识符 $KSI_{ASME-RS}$ 等内容，其中 RS 的身份标识可以是 RS 的 IMSI，也可以是 RS 的 MAC 地址等。

[0087] 步骤 402：eNB 向 RSDA 转发 RS 的认证请求；

[0088] 该消息中携带了 RS 的身份标识、服务网络标识等内容。

[0089] 步骤 403：RSDA 生成该 RS 对应的 AV；

[0090] RSDA 根据 RS 的身份标识找到该 RS 对应的共享密钥 K，并随机产生一个 RAND，然后根据 RAND、自身当前保存的 SQN、RS 和 RSDA 之间共享的密钥 K 及其它信息生成该 RS 对应的 AV，其中 AV 包括 RAND、XRES、$K_{ASME-RS}$、AUTN；还可以采用其它的参数来生成 AV，本发明实施例并不限定生成 AV 的参数。

[0091] 步骤 404：RSDA 向 eNB 返回认证响应；

[0092] 该消息中携带了该 RS 的 AV 中对应的 RAND 和 AUTN，以及密钥 $K_{ASME-RS}$ 所对应的密钥标识符 $KSI_{ASME-RS}$ 等内容，eNB 将收到的该 RS 的 AV 进行保存。

[0093] 步骤 405：eNB 向 RS 发送 RS 认证请求消息；

[0094] 该消息中携带了该 RS 的 AV 中对应的 RAND 和 AUTN，以及密钥 $K_{ASME-RS}$ 对应的密钥标识符 $KSI_{ASME-RS}$ 等内容。

[0095] 步骤 406：RS 进行认证，并生成 RES 值；

[0096] RS 根据收到的 RAND 和 AUTN，进行校验，包括：根据 RAND、AUTN 中的 SQN 和与 RSDA 共享的密钥 K 共同计算出一个 MAC 值，并比较该 MAC 值和从接收到的 AUTN 中解析的 MAC 值是否一致，如果一致，RS 对网络侧的鉴权通过，则利用 RAND 和与 RSDA 共享的密钥 K 共同计算出一个 RES。

[0097] 步骤 407：RS 通过发送 RS 认证响应消息将 RES 值发送给 eNB；

[0098] 步骤 408：eNB 进行认证，并派生出空口密钥 K_{eNR-RS}；

[0099] eNB 比较从 RS 接收到的 RES 与本地存贮该 RS 的 AV 中的 XRES 是否一致，如果一致，网络侧对 RS 的鉴权通过，则 eNB 根据密钥 $K_{ASME-RS}$ 进一步派生出空口密钥 K_{eNB-RS}。

[0100] 至此，接入网侧已经完成对 RS 的鉴权，为了后续 RS 与接入网侧之间安全通信，还可以执行以下的步骤。

[0101] 步骤 409：eNB 通过 SMC 向 RS 发送空口密钥 K_{eNB-RS} 和确定的加密算法和完整性保护算法；

[0102] eNB 结合 RS 支持的加密和完整性保护算法以及自身支持的加密和完整性保护算法，确定用户面和控制面加密密钥和完整性保护密钥的密钥派生算法，并通过 SMC 将空口密钥 K_{eNB-RS} 和确定的密钥派生算法发送给 RS。

[0103] 步骤 410：RS 和 eNB 派生出空口加密密钥和完整性保护的密钥。

[0104] RS 和 eNB 就可以各自利用空口密钥 K_{eNB-RS} 通过选定的密钥算法进一步派生出空口

加密密钥和完整性保护的密钥。

[0105] 本实施例通过在接入网侧引入一个 RSDA，存贮了 RS 的上下文信息，RS 和 RSDA 预共享一个永久性密钥 K，RSDA 通过有线或无线的方式和 eNB 相连，由 eNB 完成 RS 的鉴权功能，因而将 RS 接入鉴权完全限定在接入网侧，从而避免由于接入网引入 RS 后而造成对核心网的改动，使得引入 RS 后的系统对整个网络的影响达到最小化。

[0106] 实施例三是身份认证位于 eNB 上，由 eNB 完成 RS 的鉴权功能的实施例，下面介绍一种身份认证位于 RSDA 上，由 RSDA 完成 RS 的鉴权功能的实施例。

[0107] 实施例四

[0108] 在本实施例中，身份认证位于 RSDA 上，则由 RSDA 完成 RS 的鉴权功能。本实施例的方案要求 RSDA 上需要配备所有通过有线相连的 eNB 的网络标识。引入 RS 后支持对称性密钥认证方式的各种系统都可以对 RS 进行鉴权，因此本实施例中的 eNB 都可以为支持对称性密钥认证方式的基站。下面结合附图进行详细说明。

[0109] 参见图 5，下面对实现实施例四的方法的具体步骤进行详细介绍：

[0110] 步骤 501：RS 向 RSDA 发送认证请求；

[0111] 所述认证请求可以被包含在认证请求消息中，该消息中携带了 RS 身份标识、所支持的加密和完整性保护算法，以及派生密钥 $K_{ASME-RS}$ 对应的密钥标识符 $KSI_{ASME-RS}$ 等内容，其中 RS 的身份标识可以是 RS 的 IMSI，也可以是 RS 的 MAC 地址等。

[0112] 步骤 502：RSDA 生成 AV；

[0113] RSDA 根据 RS 身份标识找到该 RS 对应的共享密钥 K，并随机产生一个 RAND，然后根据 RAND、自身当前保存的 SQN、RS 和 RSDA 之间共享的密钥 K 及其它信息生成该 RS 对应的 AV，其中，AV 包括 RAND、XRES、$K_{ASME-RS}$、AUTN；还可以采用其它的参数来生成 AV，本发明实施例并不限定生成 AV 的参数。

[0114] 步骤 503：RSDA 向 RS 返回认证响应；

[0115] 该消息中携带了该 RS 的 AV 中对应的 RAND 和 AUTN，以及密钥 $K_{ASME-RS}$ 所对应的密钥标识符 $KSI_{ASME-RS}$ 等内容。

[0116] 步骤 504 与步骤 304，此处不再赘述；

[0117] 步骤 505：RS 向 RSDA 返回 RES 值；

[0118] 步骤 506：RSDA 进行认证，并派生出空口密钥 K_{eNB-RS}；

[0119] RSDA 比较从 RS 接收到的 RES 与之前生成该 RS 的 AV 中的 XRES 是否一致，如果一致，网络侧对 RS 的鉴权通过，则 RSDA 根据密钥 $K_{ASME-RS}$ 进一步派生出空口密钥 K_{eNB-RS}。

[0120] 至此，接入网侧已经完成对 RS 的鉴权，为了后续 RS 与接入网侧之间安全通信，还可以执行以下的步骤。

[0121] 步骤 507：RSDA 通过 SMC 将该派生密钥 K_{eNB-RS} 以及 RS 所支持的加密和完整性算法发送给 eNB；

[0122] 步骤 508：eNB 通过 SMC 向 RS 发送确定的加密算法和完整性保护算法；

[0123] eNB 根据收到 RS 支持的加密和完整性保护算法以及自身支持的加密和完整性保护算法，确定空口用户面和控制面加密密钥和完整保护性密钥的密钥派生算法，并通过 SMC 将该选定的算法发送给 RS。

[0124] 步骤 509 与步骤 410 相同，此处不再赘述。

[0125] 本实施例通过在接入网侧引入一个 RSDA，存贮了 RS 的上下文信息，RS 和 RSDA 预共享一个永久性密钥 K，RSDA 通过有线或无线的方式和 eNB 相连，由 RSDA 完成 RS 的鉴权功能，因而将 RS 接入鉴权完全限定在接入网侧，从而避免由于接入网引入 RS 后而造成对核心网的改动，使得引入 RS 后的系统对整个网络的影响达到最小化。

[0126] 上面的实施例介绍了几种 RS 接入鉴权的方法，下面介绍相关装置。

[0127] 参见图 6，一种通信装置，包括：

[0128] 请求接收单元 110，用于接收 RS 发送的认证请求，认证请求包含 RS 身份标识；

[0129] 获取单元 111，用于获取认证向量，认证向量由独立于核心网的第二设备生成，与 RS 身份标识对应；

[0130] 获取单元 111 可以是在接收请求接收单元 110 中的认证请求后获取认证向量。

[0131] 认证向量发送单元 112，用于向 RS 发送获取单元 111 获取的认证向量，指示 RS 对认证向量进行认证；

[0132] 响应值接收单元 113，用于接收 RS 对认证向量发送单元 112 发送的认证向量认证通过后发送的响应值；

[0133] 认证单元 114，用于对响应值接收单元 113 接收的响应值进行认证；

[0134] 空口密钥派生单元 115，用于在认证单元 114 对响应值认证通过时，派生空口密钥。

[0135] 其中，通信装置还包括：密钥派生单元，用于派生与所述空口密钥派生单元派生的所述空口密钥对应的加密密钥和完整性保护的密钥。

[0136] 参见图 7，一种通信系统，包括：

[0137] 中继站 121，用于向第一设备 122 发送认证请求，所述认证请求包含 RS 身份标识，接收第一设备 122 发送的认证向量，对认证向量进行认证，认证通过后生成响应值，向第一设备 122 发送响应值；

[0138] 第一设备 122，用于接收中继站 121 发送的认证请求，认证请求包含中继站的身份标识，获取认证向量，向中继站 121 发送认证向量，接收中继站 121 对认证向量认证通过后发送的响应值，对响应值进行认证，当认证通过时，派生空口密钥；

[0139] 独立于核心网的第二设备 123，用于生成认证向量，认证向量与中继站身份标识对应。

[0140] 其中，第一设备 122 为基站，独立于核心网的第二设备 123 为逻辑实体，逻辑实体与所述基站向量。

[0141] 其中，第一设备 122 为基站，独立于核心网的第二设备 123 为逻辑实体，逻辑实体集成在所述基站中。

[0142] 其中，第一设备 122 和独立于核心网的第二设备 123 为同一逻辑实体。

[0143] 其中，基站还用于派生与所述空口密钥对应的加密密钥和完整性保护的密钥。

[0144] 本发明实施例接入网侧接收 RS 发送的认证请求，生成认证向量并发送给 RS，接收 RS 对认证向量认证通过后发送的响应值，对响应值进行认证，认证通过后派生空口密钥，完成对 RS 的鉴权。在接入网侧引入一个网络逻辑实体，由接入网侧的逻辑实体与中继站共享了共享密钥，由接入网侧完成对 RS 的身份认证及密钥派生，从而完成中继站的网络安全接入，因此中继站的网络安全接入不需要对核心网进行改动就可以实现，使得引入 RS 后的系

统对整个网络的影响达到最小化。

[0145] 进一步，可以通过在接入网侧将 RSDA 和 eNB 集成在一起，将 RS 的鉴权功能完全限定在接入网侧；通过在接入网侧引入一个 RSDA，存贮了 RS 的上下文信息，RS 和 RSDA 共享了共享密钥，RSDA 通过有线或无线的方式和 eNB 相连，由 eNB 完成 RS 的鉴权功能或由 RSDA 完成 RS 的鉴权功能，将 RS 接入鉴权完全限定在接入网侧。

[0146] 以上对本发明实施例所提供的鉴权方法、通信装置和通信系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

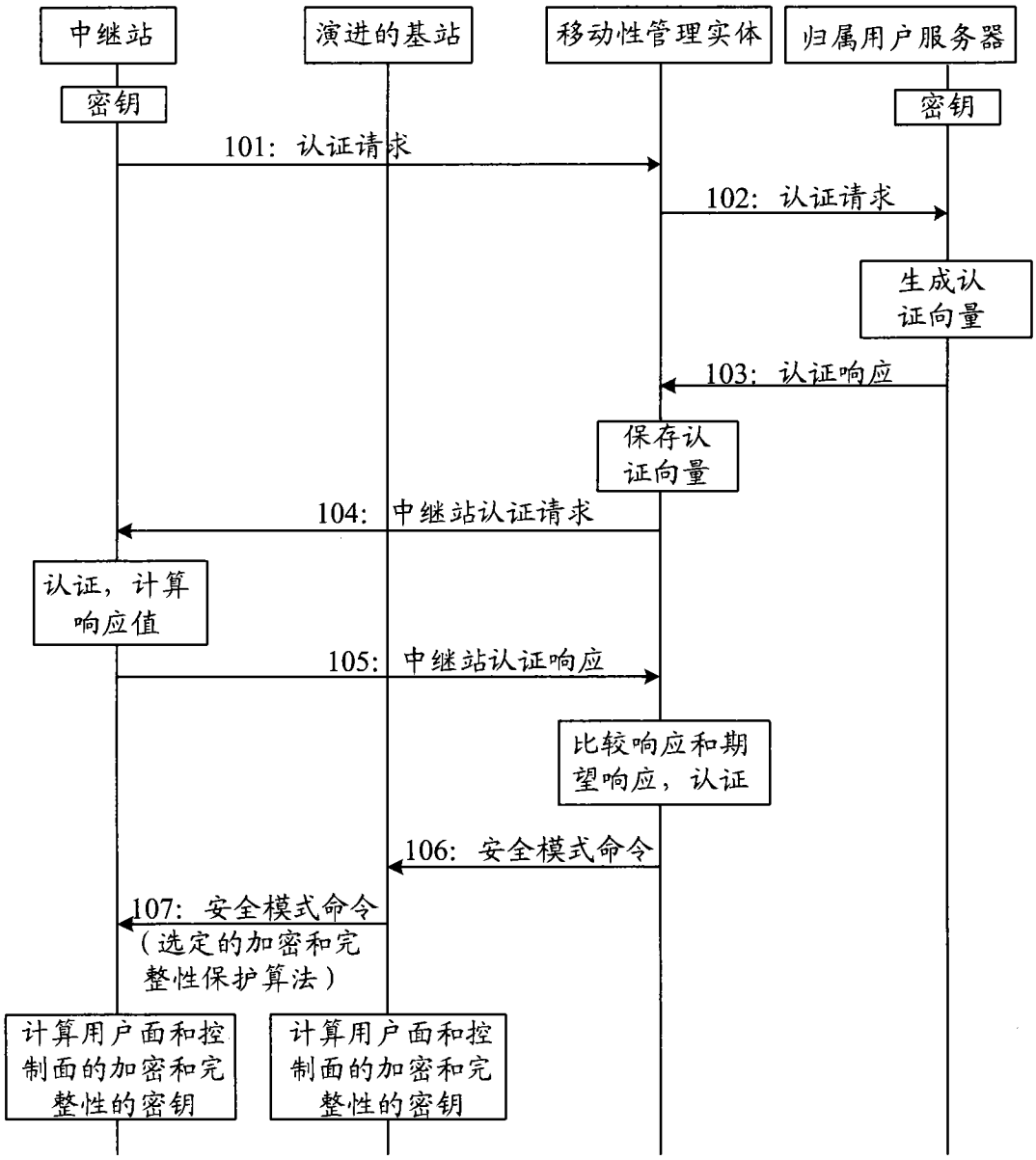

中继站
演进的基站
移动性管理实体
归属用户服务器
密钥
密钥
101: 认证请求
102: 认证请求
生成认证向量
103: 认证响应
保存认证向量
104: 中继站认证请求
认证，计算响应值
105: 中继站认证响应
比较响应和期望响应，认证
106: 安全模式命令
107: 安全模式命令（选定的加密和完整性保护算法）
计算用户面和控制面的加密和完整性的密钥
计算用户面和控制面的加密和完整性的密钥

图 1

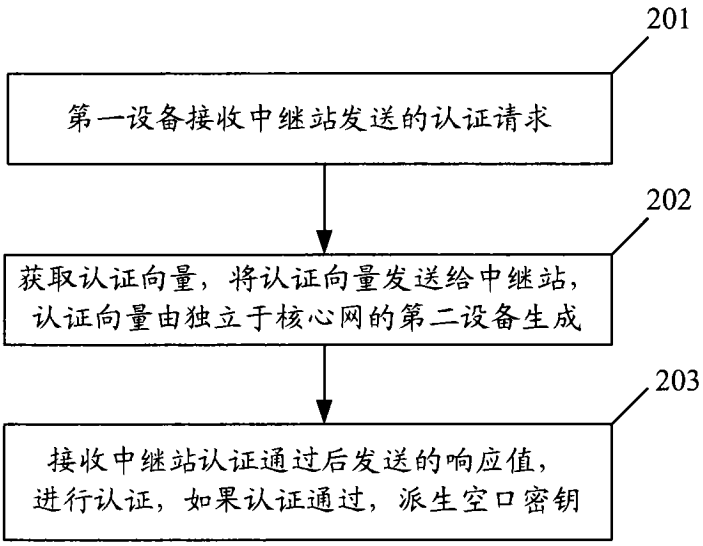

201
第一设备接收中继站发送的认证请求
202
获取认证向量，将认证向量发送给中继站，
认证向量由独立于核心网的第二设备生成
203
接收中继站认证通过后发送的响应值，
进行认证，如果认证通过，派生空口密钥

图 2

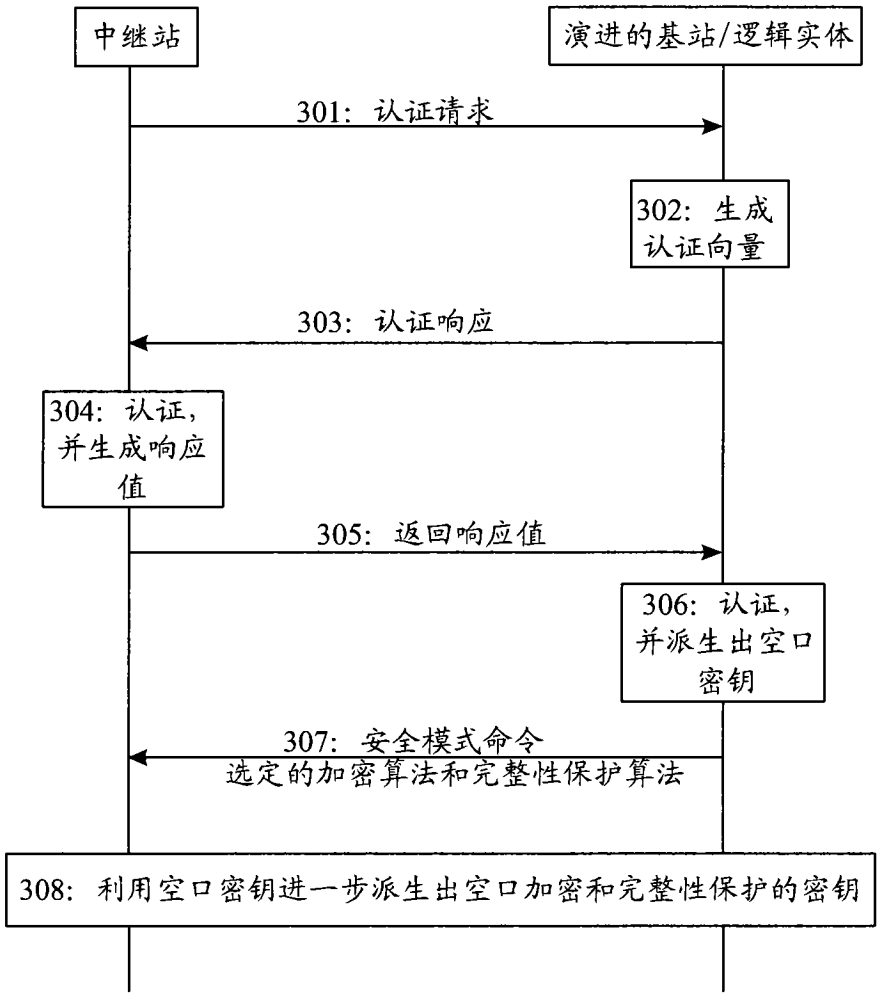

中继站
演进的基站/逻辑实体
301: 认证请求
302: 生成认证向量
303: 认证响应
304: 认证，并生成响应值
305: 返回响应值
306: 认证，并派生出空口密钥
307: 安全模式命令
选定的加密算法和完整性保护算法
308: 利用空口密钥进一步派生出空口加密和完整性保护的密钥

图 3

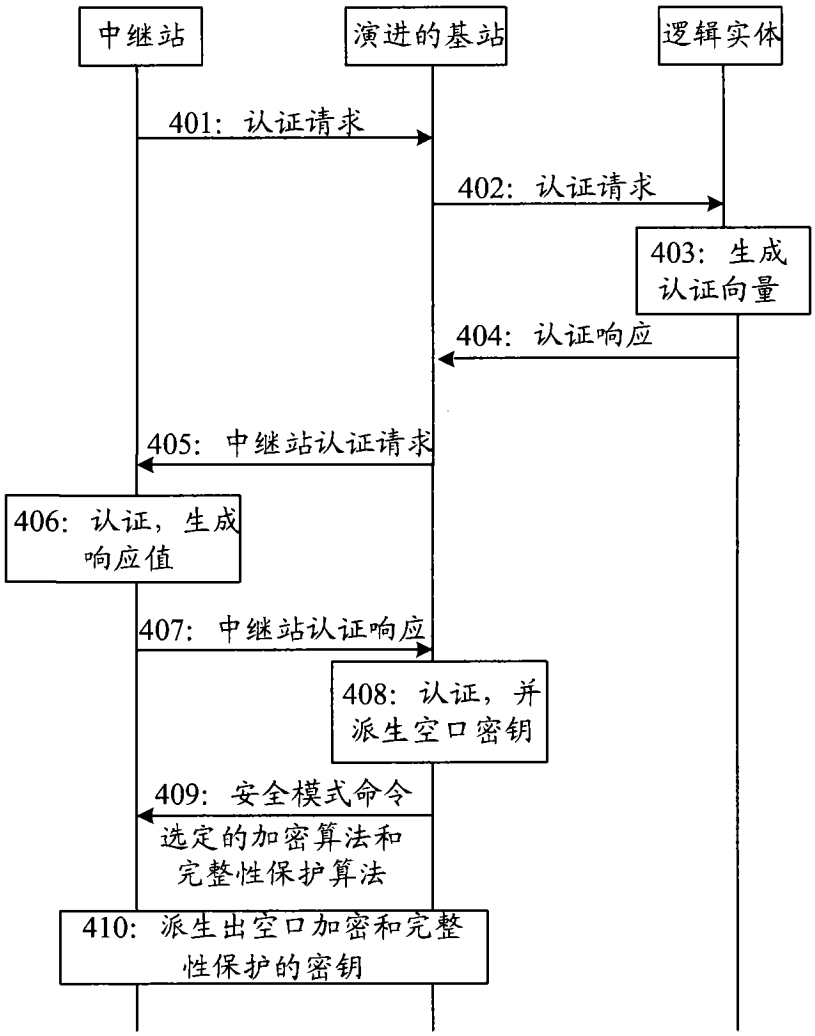

中继站
演进的基站
逻辑实体
401：认证请求
402：认证请求
403：生成认证向量
404：认证响应
405：中继站认证请求
406：认证，生成响应值
407：中继站认证响应
408：认证，并派生空口密钥
409：安全模式命令
选定的加密算法和完整性保护算法
410：派生出空口加密和完整性保护的密钥

图 4

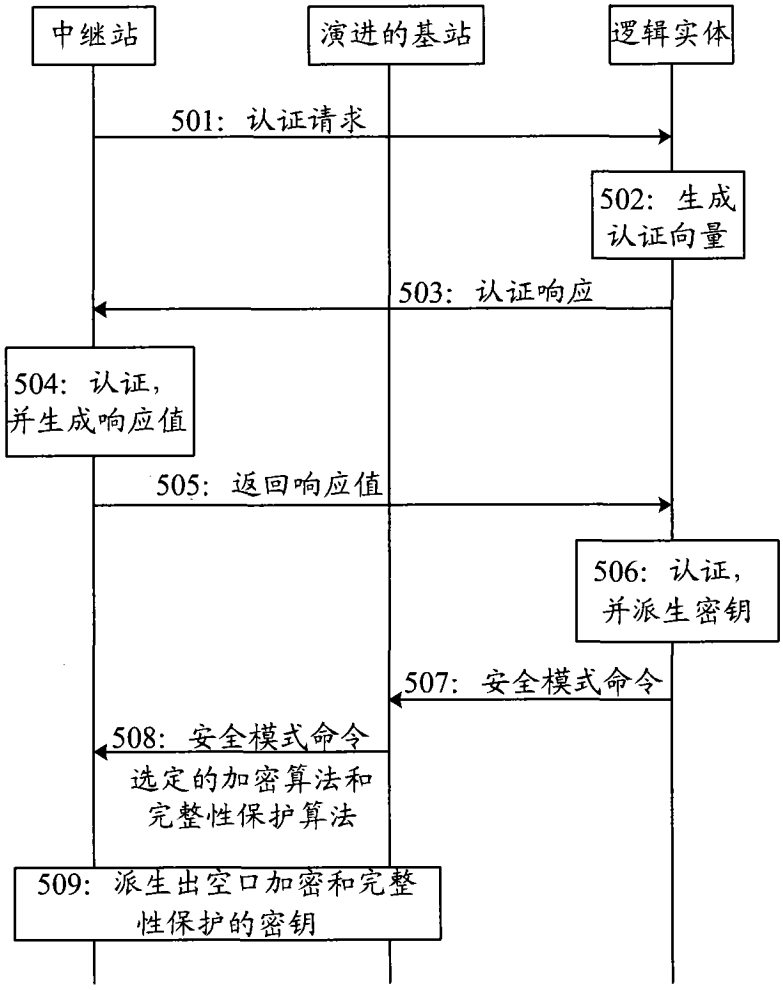

中继站
演进的基站
逻辑实体
501: 认证请求
502: 生成认证向量
503: 认证响应
504: 认证，并生成响应值
505: 返回响应值
506: 认证，并派生密钥
507: 安全模式命令
508: 安全模式命令
选定的加密算法和完整性保护算法
509: 派生出空口加密和完整性保护的密钥

图 5

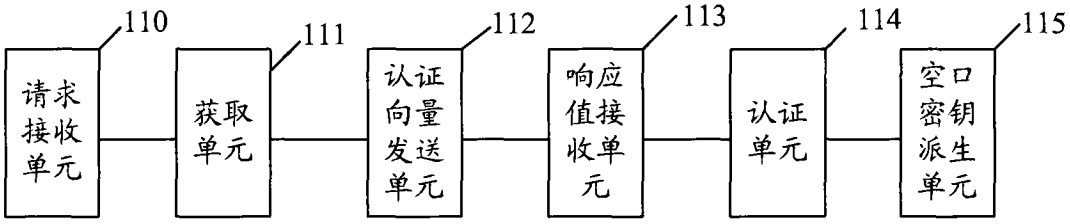

110
请求接收单元
111
获取单元
112
认证向量发送单元
113
响应值接收单元
114
认证单元
115
空口密钥派生单元

图 6

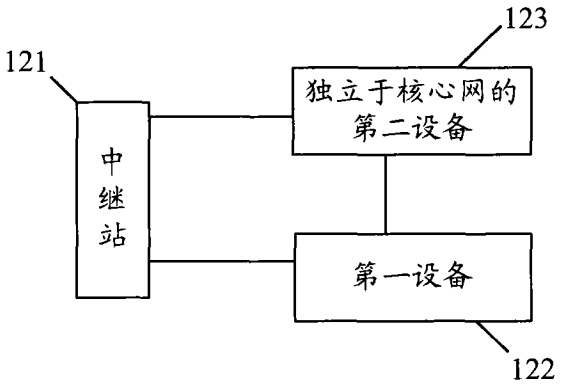


图 7