(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 106257945 B
(45)授权公告日 2024.04.09

(21)申请号 201510335272.1

(22)申请日 2015.06.16

(65)同一申请的已公布的文献号
申请公布号 CN 106257945 A

(43)申请公布日 2016.12.28

(73)专利权人 北京佰才邦技术股份有限公司
地址 100080 北京市海淀区北清路81号一区1号楼9层、10层

(72)发明人 周明宇 白炜

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
专利代理师 韩建伟 张永明

(51)Int.Cl.
H04W 12/06(2021.01)

(56)对比文件
CN 101442402 A,2009.05.27
CN 102300284 A,2011.12.28
CN 204929264 U,2015.12.30
CN 101730098 A,2010.06.09
CN 104378751 A,2015.02.25
US 2009117876 A1,2009.05.07

审查员 潘小丹

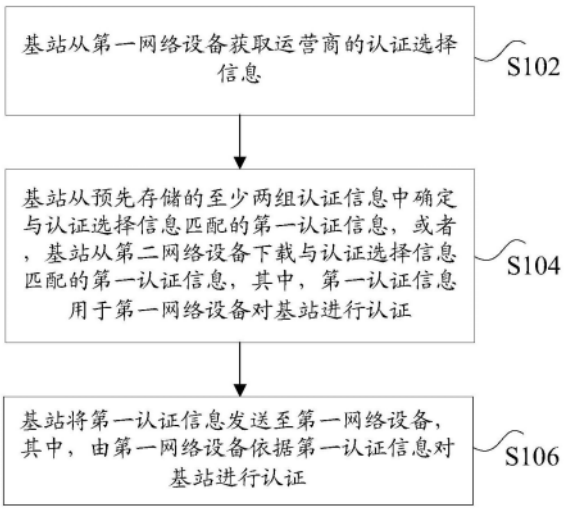
权利要求书4页 说明书12页 附图5页

(54)发明名称

基站的认证方法、装置及系统

(57)摘要

本发明公开了一种基站的认证方法、装置及系统。其中,该方法包括:基站从第一网络设备获取运营商的认证选择信息;所述基站从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证;所述基站将所述第一认证信息发送至所述第一网络设备,其中,由所述第一网络设备依据所述第一认证信息对所述基站进行认证。本发明解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。



CN 106257945 B

1.一种基站的认证方法,其特征在于,包括:

基站从第一网络设备获取运营商的认证选择信息,其中,所述认证选择信息包括以下一种或几种的组合:公共陆地移动网络PLMN信息、所述第一网络设备的IP地址、所述运营商的名称,基站通过非运营商部署的连接方式连接到核心网;

所述基站从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC,在所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,所述方法还包括:所述基站在预先存储的至少两组认证信息中查找是否存在与所述认证选择信息匹配的所述第一认证信息;其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述基站从所述第二网络设备下载所述第一认证信息;

所述基站将所述第一认证信息发送至所述第一网络设备,其中,由所述第一网络设备依据所述第一认证信息对所述基站进行认证。

2.根据权利要求1所述的方法,其特征在于,所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息包括:

所述基站将所述基站的设备身份标识ID发送至所述第二网络设备;所述基站接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述设备ID确定与所述认证选择信息匹配的所述第一认证信息;

或者,

所述基站将第一请求发送至所述第二网络设备,其中,由所述基站依据所述认证选择信息生成所述第一请求,所述第一请求包含所述第一认证信息的标识;所述基站接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述第一认证信息的标识确定所述第一认证信息。

3.根据权利要求1至2中任一项所述的方法,其特征在于,所述由所述第一网络设备依据所述第一认证信息对所述基站进行认证:

由所述第一网络设备采用扩展认证协议-密匙协商机制EAP-AKA技术,基于所述第一认证信息对所述基站进行认证。

4.一种基站的认证方法,其特征在于,包括:

第一网络设备将运营商的认证选择信息发送至基站,其中,所述认证选择信息包括以下一种或几种的组合:公共陆地移动网络PLMN信息、所述第一网络设备的IP地址、所述运营商的名称,基站通过非运营商部署的连接方式连接到核心网,由所述基站从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,由所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC,所述第一认证信息用于所述第一网络设备对所述基站进行认证,在所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,所述方法还包括:所述基站在预先存储的至少两组认证信息中查找是否存在与所述认证选

择信息匹配的所述第一认证信息;其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述基站从所述第二网络设备下载所述第一认证信息;

所述第一网络设备接收所述基站返回的所述第一认证信息;

所述第一网络设备依据所述第一认证信息对所述基站进行认证。

5.根据权利要求4所述的方法,其特征在于,所述由所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息包括:

所述基站将所述基站的设备身份标识ID发送至所述第二网络设备;所述基站接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述设备ID确定与所述认证选择信息匹配的所述第一认证信息;

或者,

所述基站将第一请求发送至所述第二网络设备,其中,由所述基站依据所述认证选择信息生成所述第一请求,所述第一请求包含所述第一认证信息的标识;所述基站接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述第一认证信息的标识确定所述第一认证信息。

6.根据权利要求4至5中任一项所述的方法,其特征在于,所述第一网络设备依据所述第一认证信息对所述基站进行认证包括:

所述第一网络设备采用扩展认证协议-密匙协商机制EAP-AKA技术,基于所述第一认证信息对所述基站进行认证。

7.一种基站,其特征在于,包括:

通信处理器,用于从第一网络设备获取运营商的认证选择信息,其中,所述认证选择信息包括以下一种或几种的组合:公共陆地移动网络PLMN信息、所述第一网络设备的IP地址、所述运营商的名称,基站通过非运营商部署的连接方式连接到核心网;

认证信息选择器,与所述通信处理器连接,用于从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC,在所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,还包括:所述基站在预先存储的至少两组认证信息中查找是否存在与所述认证选择信息匹配的所述第一认证信息;其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述基站从所述第二网络设备下载所述第一认证信息;

所述通信处理器,还用于将所述第一认证信息发送至所述第一网络设备,其中,由所述第一网络设备依据所述第一认证信息对所述基站进行认证。

8.根据权利要求7所述的基站,其特征在于,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC;

其中,在所述第一认证信息包括所述不可编写的SIM卡的情况下,所述基站还包括:至少两个SIM卡卡槽,用于容纳所述不可编写的SIM卡;

在所述第一认证信息包括所述证书的情况下,所述基站还包括:至少两个认证信息存储器,用于存储所述证书;

在所述第一认证信息包括所述可重复编写的SIM卡的情况下,所述基站还包括:至少一个SIM卡卡槽,用于容纳所述可重复编写的SIM卡。

9.根据权利要求8所述的基站,其特征在于,

所述嵌入式UICC为采用表面黏着技术SMD贴片封装工艺,将SIM卡芯片直接焊接在所述基站内部的芯片上所得到的;或者,

所述嵌入式UICC为采用系统级封装SIP工艺,将SIM卡芯片和所述基站内部的芯片封装在一体所得到的。

10.根据权利要求7至9中任一项所述的基站,其特征在于,所述通信处理器包括:

第一发送电路,用于将所述基站的设备身份标识ID发送至所述第二网络设备;

第一接收电路,用于接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述设备ID确定与所述认证选择信息匹配的所述第一认证信息。

11.根据权利要求7至9中任一项所述的基站,其特征在于,所述通信处理器包括:

第二发送电路,用于将第一请求发送至所述第二网络设备,其中,由所述认证信息选择器依据所述认证选择信息生成所述第一请求,所述第一请求包含所述第一认证信息的标识;

第二接收电路,用于接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述第一认证信息的标识确定所述第一认证信息。

12.根据权利要求7至9中任一项所述的基站,其特征在于,

所述认证信息选择器,还用于在从所述第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,在预先存储的至少两组认证信息中查找是否存在与所述认证选择信息匹配的所述第一认证信息;

其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述认证信息选择器从所述第二网络设备下载所述第一认证信息。

13.一种第一网络设备,其特征在于,包括:

发送器,用于将运营商的认证选择信息发送至基站,其中,所述认证选择信息包括以下一种或几种的组合:公共陆地移动网络PLMN信息、所述第一网络设备的IP地址、所述运营商的名称,基站通过非运营商部署的连接方式连接到核心网,由所述基站从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,由所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC,在所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,所述基站在预先存储的至少两组认证信息中查找是否存在与所述认证选择信息匹配的所述第一认证信息;其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述基站从所述第二网络设备下载所述第一认证信息;

接收器,用于接收所述基站返回的所述第一认证信息;

认证信息处理器,与所述接收器连接,用于依据所述第一认证信息对所述基站进行认证。

14.根据权利要求13所述的第一网络设备,其特征在于,所述认证信息处理器用于执行以下步骤依据所述第一认证信息对所述基站进行认证:

采用扩展认证协议-密匙协商机制EAP-AKA技术,基于所述第一认证信息对所述基站进行认证。

15.一种基站的认证系统,其特征在于,包括:如权利要求7至12中任一项所述的基站,以及与所述基站建立连接的如权利要求13至14中任一项所述的第一网络设备。

基站的认证方法、装置及系统

技术领域

[0001] 本发明涉及通信领域,具体而言,涉及一种基站的认证方法、装置及系统。

背景技术

[0002] 在传统系统中,宏基站(例如覆盖1公里半径的区域)通常被设置在高处便于无线信号的传输以及无线覆盖的扩大,并且宏基站和与之连接的核心网通常由运营商部署,通过核心网中的服务器和其它设备共同实现移动通信系统的各种功能,包括为移动终端提供通信服务、对移动终端计费、对移动终端鉴权等;其中,宏基站与核心网之间的连接也由运营商来负责部署,例如铺设光纤等方式,该连接仅被运营商控制和管理。

[0003] 然而,随着人们对移动通信需求的快速增长和移动通信可用频谱逐渐减少,宏基站的运营方式的缺点逐渐显现,小基站(包括微基站、家庭基站等)逐渐变得重要,每个小基站覆盖的区域远小于宏基站,这样,相同的无线频谱就可以发挥更大的价值(例如,20MHz带宽在宏基站覆盖范围内被1000个UE分享,而在小基站覆盖范围内仅被10个UE分享,从而后者能为单个UE带来更快的传输速率)。对于小基站来说,由于其覆盖区域较小,因此数目会远多于宏基站,运营商更多地利用现有的固定宽带接入作为其与核心网通信的连接方式,通过该连接方式传输的信息则与普通用户接入家庭宽带后传输的信息相同,通常是在网络上公开,例如通过Internet连接。

[0004] 由于小基站通过非运营商部署的连接方式连接到核心网,小基站与核心网的连接就存在认证的过程,核心网通过这个过程认可小基站的合法身份和安全性等,从而才会与小基站进行移动通信相关的信令和数据传输,例如认证通过之后核心网的HSS/HLR才会将用户数据发送给小基站用于认证用户。

[0005] 在现有技术中,不同运营商的核心网设备和宏基站设备是不同的,其所拥有的网络也是不同的,因此一个运营商通常会发布该运营商所要求的小基站的技术规范,便于能够与该运营商的核心网互联互通、与宏基站协同配合以提供更优的移动通信服务等等,该技术规范中就会对小基站的认证方式加以限制;通常,由于运营商只会考虑所采购的小基站接入该运营商的需求和场景,还可能为了与其它运营商的竞争而避免该小基站接入其它运营商的功能,因此小基站通常只能接入一个运营商,造成小基站使用上的不灵活。

[0006] 针对上述的问题,目前尚未提出有效的解决方案。

发明内容

[0007] 本发明实施例提供了一种基站的认证方法、装置及系统,以至少解决由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

[0008] 根据本发明实施例的一个方面,提供了一种基站的认证方法,包括:基站从第一网络设备获取运营商的认证选择信息;上述基站从预先存储的至少两组认证信息中确定与上述认证选择信息匹配的第一认证信息,或者,上述基站从第二网络设备下载与上述认证选择信息匹配的上述第一认证信息,其中,上述第一认证信息用于上述第一网络设备对上述

基站进行认证;上述基站将上述第一认证信息发送至上述第一网络设备,其中,由上述第一网络设备依据上述第一认证信息对上述基站进行认证。

[0009] 根据本发明实施例的另一方面,还提供了一种基站的认证方法,包括:第一网络设备将运营商的认证选择信息发送至基站,其中,由上述基站从预先存储的至少两组认证信息中确定与上述认证选择信息匹配的第一认证信息,或者,由上述基站从第二网络设备下载与上述认证选择信息匹配的上述第一认证信息,其中,上述第一认证信息用于上述第一网络设备对上述基站进行认证;上述第一网络设备接收上述基站返回的上述第一认证信息;上述第一网络设备依据上述第一认证信息对上述基站进行认证。

[0010] 根据本发明实施例的另一方面,还提供了一种基站,包括:通信处理器,用于从第一网络设备获取运营商的认证选择信息;认证信息选择器,与上述通信处理器连接,用于从预先存储的至少两组认证信息中确定与上述认证选择信息匹配的第一认证信息,或者,从第二网络设备下载与上述认证选择信息匹配的上述第一认证信息,其中,上述第一认证信息用于上述第一网络设备对上述基站进行认证;上述通信处理器,还用于将上述第一认证信息发送至上述第一网络设备,其中,由上述第一网络设备依据上述第一认证信息对上述基站进行认证。

[0011] 根据本发明实施例的另一方面,还提供了一种第一网络设备,包括:发送器,用于将运营商的认证选择信息发送至基站,其中,由上述基站从预先存储的至少两组认证信息中确定与上述认证选择信息匹配的第一认证信息,或者,由上述基站从第二网络设备下载与上述认证选择信息匹配的上述第一认证信息,其中,上述第一认证信息用于上述第一网络设备对上述基站进行认证;接收器,用于接收上述基站返回的上述第一认证信息;认证信息处理器,与上述接收器连接,用于依据上述第一认证信息对上述基站进行认证。

[0012] 根据本发明实施例的另一方面,还提供了一种基站的认证系统,包括:具有上述任意特征的基站以及与上述基站建立连接的具有上述任意特征的第一网络设备。

[0013] 在本发明实施例中,采用基站从第一网络设备获取运营商的认证选择信息;基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息,或者,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,其中,第一认证信息用于第一网络设备对基站进行认证;基站将第一认证信息发送至第一网络设备,其中,由第一网络设备依据第一认证信息对基站进行认证的方式,通过在基站中预先存储至少两组认证信息或从第二网络设备下载认证信息,达到了灵活根据不同的运营商确定不同认证信息的目的,从而实现了增加基站在使用上的灵活性的技术效果,进而解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

附图说明

[0014] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0015] 图1是根据本发明实施例的一种可选的基站的认证方法的流程示意图;

[0016] 图2是根据本发明实施例的一种可选的用于运行基站的认证方法的网络架构的示意图;

[0017] 图3是根据本发明实施例的一种可选的基站的认证方法的交互示意图;

[0018] 图4是根据本发明实施例的另一种可选的用于运行基站的认证方法的网络架构的示意图；

[0019] 图5是根据本发明实施例的另一种可选的基站的认证方法的流程示意图；

[0020] 图6是根据本发明实施例的一种可选的基站的结构示意图；

[0021] 图7是根据本发明实施例的一种可选的通信处理器的结构示意图；

[0022] 图8是根据本发明实施例的另一种可选的通信处理器的结构示意图；

[0023] 图9是根据本发明实施例的一种可选的第一网络设备的结构示意图；

[0024] 图10是根据本发明实施例的一种可选的基站的认证系统的结构示意图。

具体实施方式

[0025] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0026] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 实施例1

[0028] 根据本发明实施例，还提供了一种基站的认证方法的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0029] 在上述运行环境下，本申请提供了如图1所示的基站的认证方法。图1是根据本发明实施例一的基站的认证方法的流程图。

[0030] 如图1所示，该基站的认证方法可以包括如下实现步骤：

[0031] 步骤S102，基站从第一网络设备获取运营商的认证选择信息。

[0032] 本申请上述步骤S102中，基站可以为小基站(包括微基站、微微基站、家庭基站等)，第一网络设备可以为核心网。基站通过非运营商部署的连接方式连接到核心网，基站与核心网的连接就存在认证的过程，核心网通过这个过程认可小基站的合法身份和安全性等，从而才会与小基站进行移动通信相关的信令和数据传输，因此，基站首先需要获取运营商的认证选择信息。

[0033] 步骤S104，基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息，或者，基站从第二网络设备下载与认证选择信息匹配的第一认证信息，其中，第一认证信息用于第一网络设备对基站进行认证。

[0034] 本申请上述步骤S104中,一种实现方式为,基站中包括至少两组认证信息,例如小基站中包括多个SIM(Subscriber Identity Module,客户识别模块)卡(例如,同手机上安装的SIM卡),或者包括多个证书,或者其它身份标识信息。

[0035] 本申请上述步骤S104中,另一种实现方式为,基站包括可重复编写认证信息,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,可编辑认证信息例如是可重复编写的SIM卡(认证信息的信息量一般很小,一般可以支持较多认证信息,比如十几个),或者嵌入式UICC。对于嵌入式UICC有两种实现方式,一种是采用SMD(Surface Mounted Devices,表面黏着技术)贴片封装工艺,就是将SIM卡芯片直接焊接在基站内部的芯片上;一种是采用SIP(Simple in Package,系统级封装)工艺,就是将SIM卡芯片和基站内部的芯片封装在一体,外表看起来就是一块芯片,好像没有SIM卡了。可编辑认证信息较上一个实施例的好处在于,只需在基站内部嵌入一个“软”SIM卡即可,通过可重复编写的方式,可以降低基站的尺寸和成本。

[0036] 步骤S106,基站将第一认证信息发送至第一网络设备,其中,由第一网络设备依据第一认证信息对基站进行认证。

[0037] 本申请上述步骤S106中,基站在确定了该第一认证信息之后,可以将第一认证信息发送至第一网络设备,以便第一网络设备依据第一认证信息对基站进行认证,可选地,第一网络设备采用EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement,扩展认证协议-密匙协商机制)技术,基于第一认证信息对基站进行认证,认证方法后续实施例中会进行详细描述,此处不赘述。

[0038] 由此可知,本申请通过在基站中预先存储至少两组认证信息或从第二网络设备下载认证信息,达到了灵活根据不同的运营商确定不同认证信息的目的,从而实现了增加基站在使用上的灵活性的技术效果,进而解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

[0039] 可选地,基站从第二网络设备下载与认证选择信息匹配的第一认证信息包括:基站将基站的设备身份标识ID发送至第二网络设备;基站接收第二网络设备返回的第一认证信息,其中,由第二网络设备根据设备ID确定与认证选择信息匹配的第一认证信息;或者,基站将第一请求发送至第二网络设备,其中,由基站依据认证选择信息生成第一请求,第一请求包含第一认证信息的标识;基站接收第二网络设备返回的第一认证信息,其中,由第二网络设备根据第一认证信息的标识确定第一认证信息。

[0040] 本发明实施例中可以由基站来确定下载哪个认证信息,可以由第二网络设备根据运营商的认证选择信息来确定基站需要哪个认证信息,例如,基站将基站的设备ID发送至第二网络设备,第二网络设备根据设备ID来确定该第一认证信息,进而返回给基站,均应在本发明实施例的保护范围之内。

[0041] 作为一种可选的实施方式,在基站从第二网络设备下载与认证选择信息匹配的第一认证信息之前,方法还可以包括:

[0042] 步骤S10,基站在预先存储的至少两组认证信息中查找是否存在与认证选择信息匹配的第一认证信息。

[0043] 其中,在预先存储的至少两组认证信息中不存在与认证选择信息匹配的第一认证信息的情况下,基站从第二网络设备下载第一认证信息。

[0044] 本申请上述步骤S10中,基站不仅可以包括固定的SIM卡(不可编写),还可以包括可重复编写的SIM卡,后者支持认证信息的写入,从而可以灵活改变认证信息。例如,该基站为中国移动定制的基站,固定的SIM卡存储了中国移动的认证信息;可重复编写的SIM卡则作为一个更灵活的方式能够通过其它运营商的认证,例如可以通过中国联通和/或中国电信的认证,该认证可以作为前一种认证方式的备份方案,例如首选通过中国移动的认证信息来认证,如果与中国移动的核心网的连接发生中断时,则自动切换到可重复编写的SIM卡用于与中国联通的认证,从而能够保证通信不中断,等等。

[0045] 可选地,认证选择信息包括以下一种或几种的组合:PLMN(Public Land Mobile Network,公共陆地移动网络)信息、第一网络设备的IP(Internet Protocol,网络之间互连的协议)地址、运营商的名称。

[0046] 可选地,第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC。

[0047] 下面,以上述基站为小基站为例,对本发明实施例提供的基站的认证方法进行详细描述:

[0048] 作为第一种实现方式,小基站中可以存储有至少两组认证信息,例如小基站中包括多个SIM卡(同手机上安装的SIM卡)、多个证书或者其它身份标识信息。

[0049] 以SIM卡为例进行说明,小基站中包括多个SIM卡,每个SIM卡例如用于认证一个运营商(如中国移动),这样,该小基站就可以用于认证多个运营商的核心网(相当于上述的第一网络设备)。例如,运营商将该小基站销售给用户并由用户部署在家庭环境中,当用户搬家后,可能由于新家的固定宽带传输的限制而无法支持小基站到原运营商的核心网的连接,这样,该用户就可以更换运营商(如中国联通)并继续通过该小基站享受移动通信服务(前提是小基站能够达到这些多个运营商的技术规范,随着LTE(Long-Term Evolution,长期演进)技术逐渐得到普及以及LTE的小基站标准化越来越广泛被接受,这一点将容易实现);或者该用户出国旅游时,也可以通过该方式、使用小基站中包括的第二个SIM卡信息来通过旅游国家的运营商(例如美国Sprint)的核心网对该小基站的认证,从而继续享受高速移动通信服务。或者在其它场景中,可以通过该方式获取多于一个运营商所提供的服务。小基站更换运营商前后,使用不同的认证信息来通过运营商核心网的认证。例如,小基站接入用户的家庭宽带网络(例如小区提供的宽带),用户搬家前,小基站使用其中的SIM卡1来认证中国移动的核心网,搬家后则使用其中的SIM卡2来认证中国联通的核心网,其中连接到小基站的网关可以连接到不同运营商的核心网,或者小基站直接连接到不同运营商的核心网。

[0050] 进一步地,该方法还能获得小基站的RAN sharing(Radio Access Network sharing,无线接入网络共享)技术带来的好处。在现有系统中,每个运营商根据自身情况部署网络设备(包括基站和核心网等),这些网络设备通常就是各个运营商自身的资产,通常不会与其它运营商共享;然而,小基站通常被部署在热点地区、办公或家庭等室内环境中,这些地区通常受到各方面的限制而不便于部署多个运营商的设备(例如每个家庭通常不会购买多个小基站、某个热点地区可用于架设小基站的抱杆等基础设施较稀缺等),因此,使用了本发明的基站的认证方法,可以简单地通过更换认证信息的方式来达到共享小基站的作用,也即是,小基站可以连接到多个运营商的核心网,从而达到多个运营商的用户都可以

通过同一小基站接入各个运营商的网络的效果,如图2所示。

[0051] 在图2中,小基站连接到网关,网关再连接到多个运营商的核心网,从而实现本发明的方法。其中,连接的方式不做限定,可以是有线或无线连接,被部署在用户家庭中,通过家庭宽带连接到网关,网关再通过骨干网连接到多个运营商的核心网。其中,小基站上包括多个SIM卡插槽,可以容纳多个SIM卡用于认证不同运营商。可以理解的是,小基站还可以直接连接到不同的运营商(即小基站与核心网之间可以没有安全网关),例如通过Internet(英特网)连接。为了保证安全性,还可以提前建立安全隧道,例如IPSec(Internet Protocol Security,Internet协议安全性)。

[0052] 在本发明中,小基站还包括认证信息选择器,例如,中国移动的网络设备向小基站发送运营商的认证选择信息包括中国移动的PLMN(Public Land Mobile Network,公共陆地移动网络)信息(例如PLMN ID),认证信息选择器则根据该PLMN信息、选择SIM卡1来通过认证核心网。运营商的认证选择信息还可以是其它信息,例如核心网的IP地址、运营商的名称等,本发明不限定。

[0053] 可选地,小基站通过安全网关与核心网设备通信,以完成核心网对小基站的认证,例如,小基站被用户部署在家庭中,对于运营商而言处于不安全的区域,安全网关和核心网设备由运营商部署,对于运营商而言处于安全区域,其中,AAA服务器主要作用是验证、授权和记账(Authentication、Authorization、Accounting),也即是验证用户的权限、授权用户享受相应服务、并记录用户使用网络资源的情况,HSS(Home Subscriber Server,归属用户服务器)/HLR(Home Location Register,归属位置寄存器)是核心网中用于存储用户签约信息的服务器。

[0054] 例如,小基站与安全网关之间可以基于SIM卡中的信息进行认证(鉴权),下面给出使用IKEv2实现小基站与核心网之间的EAP-AKA双向鉴权的例子,其中,小基站设备标识和使用者标识(预存储的,类似于手机号)存储在小基站内置的USIM(Universal Subscriber Identity Module,全球用户识别卡)卡中,还可以通过USIM卡对网络进行认证,并根据输入的参数计算鉴权结果。

[0055] 其中,如图3所示,为第一网络设备(例如AAA服务器)采用EAP-AKA技术对小基站进行的过程:

[0056] 步骤a、小基站发送IKE_SA_INIT请求给安全网关。

[0057] 步骤b、安全网关发送IKE_SA_INIT响应。

[0058] 步骤c、小基站在第一条鉴权消息中发送小基站的设备标识和使用者标识,安全网关判断使用EAP认证。

[0059] 其中,小基站的设备标识和使用者标识均为小基站内置USIM卡的IMSI。

[0060] 步骤d、安全网关发送一条空EAP AVP的鉴权请求消息给AAA服务器,携带在IKE_AUTH中获得的身份标识。

[0061] 步骤e、AAA服务器从HSS/HLR中获得设备文件和鉴权向量。

[0062] 其中,设备文件可以包括用户的信息、套餐信息等;鉴权向量用于对终端进行鉴权,鉴别是否为合法的终端。

[0063] 步骤f、AAA服务器发起鉴权挑战。

[0064] 步骤g、安全网关发送IKE_AUTH响应给小基站。

[0065] 其中,IKE_AUTH响应中可以包含从AAA服务器收到的EAP-Request或AKA-Challenge,还可以包括安全网关的标识、证书和AUTH参数,以便小基站对安全网关进行认证。

[0066] 步骤h、小基站发送鉴权挑战的响应。

[0067] 其中,小基站可以验证安全网关的证书,并计算EAP-AKA RES。

[0068] 步骤I、安全网关发送EAP-Response或AKA-Challenge给AAA服务器。

[0069] 步骤J、当所有认证都成功,AAA服务器发送鉴权结果。

[0070] 其中,鉴权结果包含一个EAP成功和安全网关的key material(关键信息)。key material应该包含认证过程中产生的MSK。所有认证包括小基站对安全网关的认证、AAA对安全网关发送消息的认证。

[0071] 步骤K、安全网关用MSK产生AUTH认证IKE_SA_INIT的AUTH载荷。

[0072] 即,安全网关根据MSK来生成一个AUTH载荷,其用于认证之前的IKE_SA_INIT。

[0073] 步骤L、安全网关将EAP成功消息发送给小基站。

[0074] 在本发明中,不同运营商的核心网通过不同的认证信息对小基站进行认证,认证使用的技术相同,例如上文提到的IKEv2技术,使小基站能够适配不同的运营商核心网。

[0075] 同理,小基站中也可以包括多个证书,这些证书在小基站出厂之前就已经存储在小基站内,或者出厂之后通过人工下载到小基站内,从而达到同样的效果,这里不再赘述。

[0076] 作为第二种实现方式,小基站中包括可重复编写认证信息,可编辑认证信息例如是可重复编写的SIM,或者嵌入式UICC。对于后者有两种实现方式,一种是采用SMD贴片封装工艺,就是将SIM卡芯片直接焊接在终端模组芯片(相当于上述的基站内部的芯片)上;一种是采用SIP封装工艺,就是将SIM卡芯片和终端模块芯片封装在一体,外表看起来就是一块芯片,好像没有SIM卡了。可编辑认证信息较上一个实施例的好处在于,只需在小基站内部嵌入一个“软”SIM卡即可,通过可重复编写的方式,降低小基站的尺寸和成本。

[0077] 在本发明中,创造性地将可重复编写的SIM或者嵌入式UICC应用于基站中,从而使基站侧存储的认证信息可以被灵活改变,同样能够达到上述效果。

[0078] 具体地,用户可以将小基站连接到认证信息输入装置,并将认证信息下载到小基站上,再将该认证信息用于核心网的认证。下载的方式不限,例如通过有线连接下载或无线的方式下载,无线的方式包括NFC(Near Field Communication,近场通信)、蓝牙、Wifi(Wireless-Fidelity,无线保真)等方式。特别地,在小基站连接到第二网络设备之后,直接从第二网络设备获取认证信息,下载到小基站之后,再用于核心网对小基站的认证。

[0079] 在本发明中所提到的对小基站进行认证的“核心网”,通常是包括能够认证小基站合法性或安全性的网络设备,具体网元不限,例如HSS/HLR,或者安全网关等等。

[0080] 作为第三种实现方式,如图4所示,小基站还可以包括两类认证信息,一类是可编辑认证信息,另一类是固定的认证信息。

[0081] 在图4中,小基站不仅包括了固定的SIM卡(不可编写),还包括可重复编写的SIM卡,后者支持认证信息的写入,从而可以灵活改变认证信息。这样,该小基站还可以获得上述两种认证信息存储装置所带来的好处,例如,该小基站为中国移动定制的小基站,固定的SIM卡存储了中国移动的认证信息;可重复编写的SIM卡则作为一个更灵活的方式能够通过其它运营商的认证,例如可以通过中国联通和/或中国电信的认证,该认证可以作为前一种

认证方式的备份方案,例如首选通过中国移动的认证信息来认证,如果与中国移动的核心网的连接发生中断时,则自动切换到可重复编写的SIM卡用于与中国联通的认证,从而能够保证通信不中断。

[0082] 本发明中的终端,可以是移动电话机(或手机),或者其它能够发送或接收无线信号的设备,包括PDA(Personal Digital Assistant,个人数字助理)、无线调制调解器、无线通信装置、手持装置、膝上型计算机、无绳电话、WLL(Wireless Local Loop,无线本地回路)站、能够将移动信号转换为Wifi信号的CPE(Customer Premise Equipment,客户终端设备)或Wifi(便携式宽带无线装置)、智能家电、或其它不通过人的操作就能自发与移动通信网络通信的设备等。

[0083] 基站的形式不限,可以是宏基站(Macro Base Station)、微基站(Pico Base Station)、Node B、ENB(Evolved Node B,增强型基站)、家庭增强型基站、中继站、接入点、RRU(Remote Radio Unit,射频拉远单元)、RRH(Remote Radio Head,射频拉远头)等。

[0084] 基站与终端之间的空中接口不限,可以是CDMA(Code Division Multiple Access,码分多址)2000、WCDMA(Wideband CDMA,宽带码分多址)、WiMAX(Worldwide Interoperability for Microwave Access,全球微波互联接入)、LTE、LTE-Advanced等。

[0085] 本发明实施例的基站的认证方法至少具有以下优点:

[0086] 1、解决了现有技术中小基站只能连接到一个运营商的核心网的问题,第一次实现小基站可以“带着走”(搬家、出国等场景更换运营商)。

[0087] 2、进一步带来RAN sharing的好处,小基站可以连接到多个运营商的核心网,有利于提高小基站的利用效率和小基站的推广使用。

[0088] 3、获得这些功能带来的好处的同时,尽量不影响小基站的尺寸和成本。

[0089] 在本发明实施例中,采用基站从第一网络设备获取运营商的认证选择信息;基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息,或者,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,其中,第一认证信息用于第一网络设备对基站进行认证;基站将第一认证信息发送至第一网络设备,其中,由第一网络设备依据第一认证信息对基站进行认证的方式,通过在基站中预先存储至少两组认证信息或从第二网络设备下载认证信息,达到了灵活根据不同的运营商确定不同认证信息的目的,从而实现了增加基站在使用上的灵活性的技术效果,进而解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

[0090] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0091] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算

机,服务器,或者网络设备等)执行本发明各个实施例的方法。

[0092] 实施例2

[0093] 根据本发明实施例,还提供了基站的认证方法的方法实施例,需要说明的是,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0094] 在上述运行环境下,本申请提供了如图5所示的基站的认证方法。图5是根据本发明实施例二的基站的认证方法的流程图。

[0095] 步骤S502,第一网络设备将运营商的认证选择信息发送至基站,其中,由基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息,或者,由基站从第二网络设备下载与认证选择信息匹配的第一认证信息,其中,第一认证信息用于第一网络设备对基站进行认证。

[0096] 本申请上述步骤S502中,基站可以为小基站(包括微基站、微微基站、家庭基站等),第一网络设备可以为核心网。基站通过非运营商部署的连接方式连接到核心网,基站与核心网的连接就存在认证的过程,核心网通过这个过程认可小基站的合法身份和安全性等,从而才会与小基站进行移动通信相关的信令和数据传输,因此,基站首先需要获取运营商的认证选择信息。

[0097] 可选地,一种实现方式为,基站中包括至少两组认证信息,例如小基站中包括多个SIM卡(例如,同手机上安装的SIM卡),或者包括多个证书,或者其它身份标识信息。另一种实现方式为,基站包括可重复编写认证信息,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,可编辑认证信息例如是可重复编写的SIM卡(认证信息的信息量一般很小,一般可以支持较多认证信息,比如十几个),或者嵌入式UICC。对于嵌入式UICC有两种实现方式,一种是采用SMD贴片封装工艺,就是将SIM卡芯片直接焊接在基站内部的芯片上;一种是采用SIP(Simple in Package,系统级封装)工艺,就是将SIM卡芯片和基站内部的芯片封装在一体,外表看起来就是一块芯片,好像没有SIM卡了。可编辑认证信息较上一个实施例的好处在于,只需在基站内部嵌入一个“软”SIM卡即可,通过可重复编写的方式,可以降低基站的尺寸和成本。

[0098] 其中,由基站从第二网络设备下载与认证选择信息匹配的第一认证信息包括:基站将基站的设备身份标识ID发送至第二网络设备;基站接收第二网络设备返回的第一认证信息,其中,由第二网络设备根据设备ID确定与认证选择信息匹配的第一认证信息;或者,基站将第一请求发送至第二网络设备,其中,由基站依据认证选择信息生成第一请求,第一请求包含第一认证信息的标识;基站接收第二网络设备返回的第一认证信息,其中,由第二网络设备根据第一认证信息的标识确定第一认证信息。

[0099] 可选地,认证选择信息包括以下一种或几种的组合:公共陆地移动网络PLMN信息、第一网络设备的IP地址、运营商的名称;第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC。

[0100] 步骤S504,第一网络设备接收基站返回的第一认证信息。

[0101] 本申请上述步骤S504中,基站在确定了该第一认证信息之后,可以将第一认证信息发送至第一网络设备,以便第一网络设备依据第一认证信息对基站进行认证。

[0102] 步骤S506,第一网络设备依据第一认证信息对基站进行认证。

[0103] 其中,第一网络设备依据第一认证信息对基站进行认证包括:第一网络设备采用扩展认证协议-密匙协商机制EAP-AKA技术,基于第一认证信息对基站进行认证。

[0104] 在本发明实施例中,采用基站从第一网络设备获取运营商的认证选择信息;基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息,或者,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,其中,第一认证信息用于第一网络设备对基站进行认证;基站将第一认证信息发送至第一网络设备,其中,由第一网络设备依据第一认证信息对基站进行认证的方式,通过在基站中预先存储至少两组认证信息或从第二网络设备下载认证信息,达到了灵活根据不同的运营商确定不同认证信息的目的,从而实现了增加基站在使用上的灵活性的技术效果,进而解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

[0105] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0106] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,或者网络设备等)执行本发明各个实施例的方法。

[0107] 实施例3

[0108] 根据本发明实施例,还提供了一种用于实施上述方法实施例的装置实施例,本申请上述实施例所提供的装置可以在基站上运行。

[0109] 图6是根据本申请实施例三的基站的结构示意图。

[0110] 如图6所示,该基站可以包括通信处理器602和认证信息选择器604。

[0111] 其中,通信处理器602,用于从第一网络设备获取运营商的认证选择信息;认证信息选择器604,与所述通信处理器602连接,用于从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证;所述通信处理器602,还用于将所述第一认证信息发送至所述第一网络设备,其中,由所述第一网络设备依据所述第一认证信息对所述基站进行认证。

[0112] 可选地,所述第一认证信息包括以下一种或几种的组合:不可编写的客户识别模块SIM卡,可重复编写的SIM卡、证书、嵌入式通用集成电路卡UICC;其中,在所述第一认证信息包括所述不可编写的SIM卡的情况下,所述基站还包括:至少两个SIM卡卡槽,用于容纳所述不可编写的SIM卡。

[0113] 在所述第一认证信息包括所述证书的情况下,所述基站还包括:至少两个认证信息存储器,用于存储所述证书。

[0114] 在所述第一认证信息包括所述可重复编写的SIM卡的情况下,所述基站还包括:至少一个SIM卡卡槽,用于容纳所述可重复编写的SIM卡。

[0115] 可选地,所述嵌入式UICC为采用表面黏着技术SMD贴片封装工艺,将SIM卡芯片直接焊接在所述基站内部的芯片上所得到的;或者,所述嵌入式UICC为采用系统级封装SIP工艺,将SIM卡芯片和所述基站内部的芯片封装在一体所得到的。

[0116] 可选地,如图7所示,所述通信处理器602包括:第一发送电路702和第一接收电路704。

[0117] 其中,第一发送电路702,用于将所述基站的设备身份标识ID发送至所述第二网络设备;第一接收电路704,用于接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述设备ID确定与所述认证选择信息匹配的所述第一认证信息。

[0118] 可选地,如图8所示,所述通信处理器602包括:第二发送电路802和第二接收电路804。

[0119] 其中,第二发送电路802,用于将第一请求发送至所述第二网络设备,其中,由所述认证信息选择器依据所述认证选择信息生成所述第一请求,所述第一请求包含所述第一认证信息的标识;第二接收电路804,用于接收所述第二网络设备返回的所述第一认证信息,其中,由所述第二网络设备根据所述第一认证信息的标识确定所述第一认证信息。

[0120] 可选地,所述认证信息选择器604,还用于在从所述第二网络设备下载与所述认证选择信息匹配的所述第一认证信息之前,在预先存储的至少两组认证信息中查找是否存在与所述认证选择信息匹配的所述第一认证信息;其中,在所述预先存储的至少两组认证信息中不存在与所述认证选择信息匹配的所述第一认证信息的情况下,所述认证信息选择器从所述第二网络设备下载所述第一认证信息。

[0121] 在本发明实施例中,采用基站从第一网络设备获取运营商的认证选择信息;基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息,或者,基站从第二网络设备下载与认证选择信息匹配的第一认证信息,其中,第一认证信息用于第一网络设备对基站进行认证;基站将第一认证信息发送至第一网络设备,其中,由第一网络设备依据第一认证信息对基站进行认证的方式,通过在基站中预先存储至少两组认证信息或从第二网络设备下载认证信息,达到了灵活根据不同的运营商确定不同认证信息的目的,从而实现了增加基站在使用上的灵活性的技术效果,进而解决了由于小基站通常只能接入一个运营商造成的小基站灵活性较差的技术问题。

[0122] 实施例4

[0123] 根据本发明实施例,还提供了一种用于实施上述方法实施例的装置实施例,本申请上述实施例所提供的装置可以在第一网络设备上运行。

[0124] 图9是根据本申请实施例四的第一网络设备的结构示意图。

[0125] 如图9所示,该第一网络设备可以包括:发送器902、接收器904和认证信息处理器906。

[0126] 其中,发送器902,用于将运营商的认证选择信息发送至基站,其中,由所述基站从预先存储的至少两组认证信息中确定与所述认证选择信息匹配的第一认证信息,或者,由所述基站从第二网络设备下载与所述认证选择信息匹配的所述第一认证信息,其中,所述第一认证信息用于所述第一网络设备对所述基站进行认证;接收器904,用于接收所述基站

返回的所述第一认证信息;认证信息处理器906,与所述接收器904连接,用于依据所述第一认证信息对所述基站进行认证。

[0127] 可选地,认证信息处理器906用于执行以下步骤依据所述第一认证信息对所述基站进行认证:采用扩展认证协议-密匙协商机制EAP-AKA技术,基于所述第一认证信息对所述基站进行认证。

[0128] 根据本发明实施例,还提供了一种基站的认证系统,图10是根据本发明实施例的一种基站的认证系统的结构示意图。

[0129] 该系统包括:具有上述任意特征的基站100以及与所述基站100建立连接的具有上述任意特征的第一网络设备102。

[0130] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0131] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0132] 在本申请所提供的几个实施例中,应该理解到,所揭露的技术内容,可通过其它的方式实现。其中,以上所描述的装置实施例仅仅是示意性的,例如所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,单元或模块的间接耦合或通信连接,可以是电性或其它的形式。

[0133] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0134] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0135] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0136] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

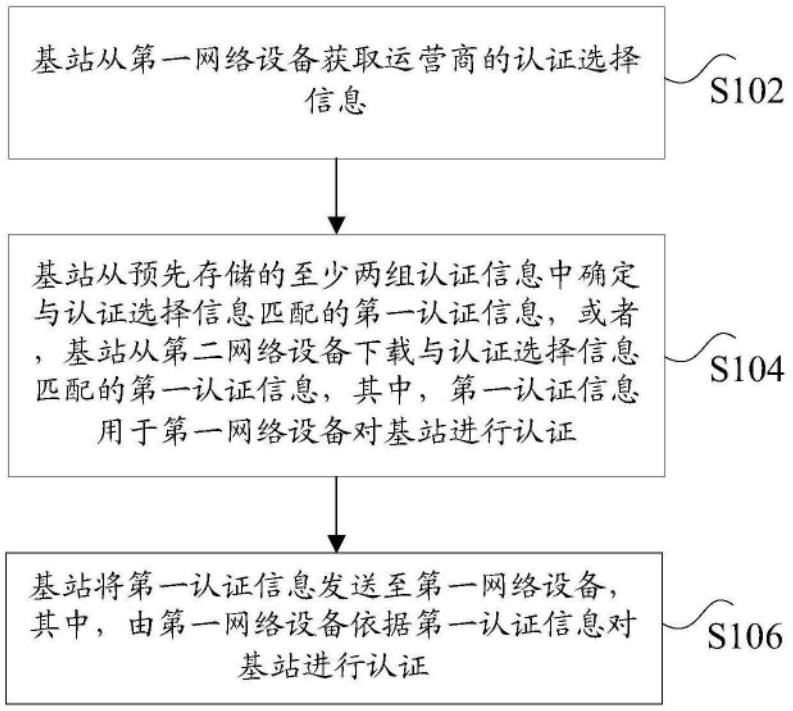

基站从第一网络设备获取运营商的认证选择信息
S102
基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息，或者，基站从第二网络设备下载与认证选择信息匹配的第一认证信息，其中，第一认证信息用于第一网络设备对基站进行认证
S104
基站将第一认证信息发送至第一网络设备，其中，由第一网络设备依据第一认证信息对基站进行认证
S106

图1

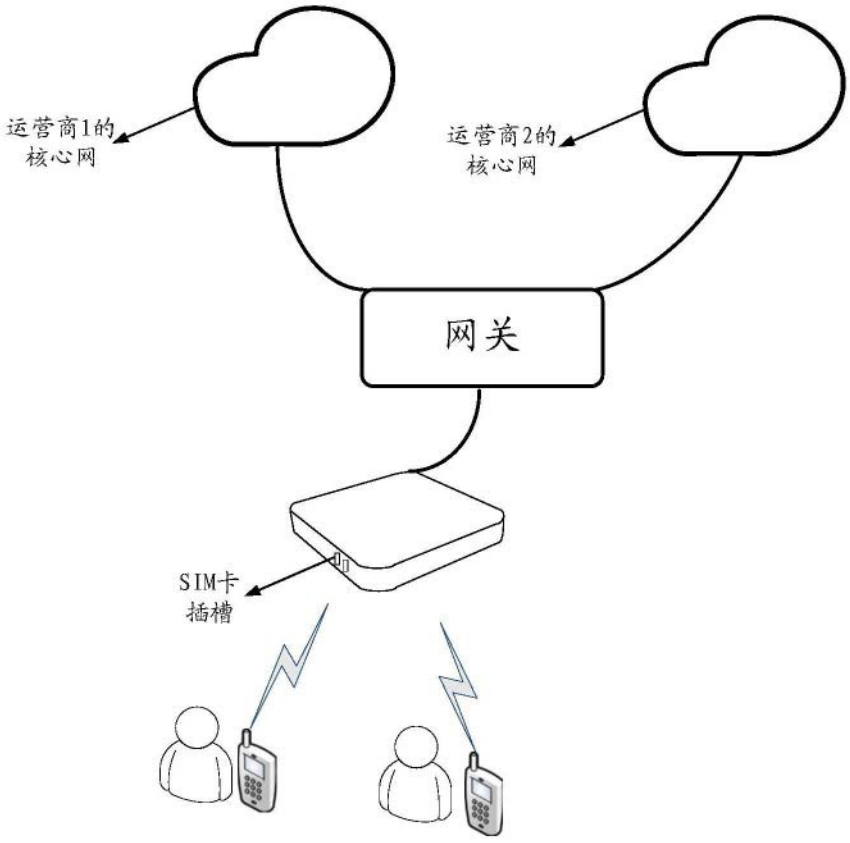

运营商1的核心网
运营商2的核心网
网关
SIM卡插槽

图2

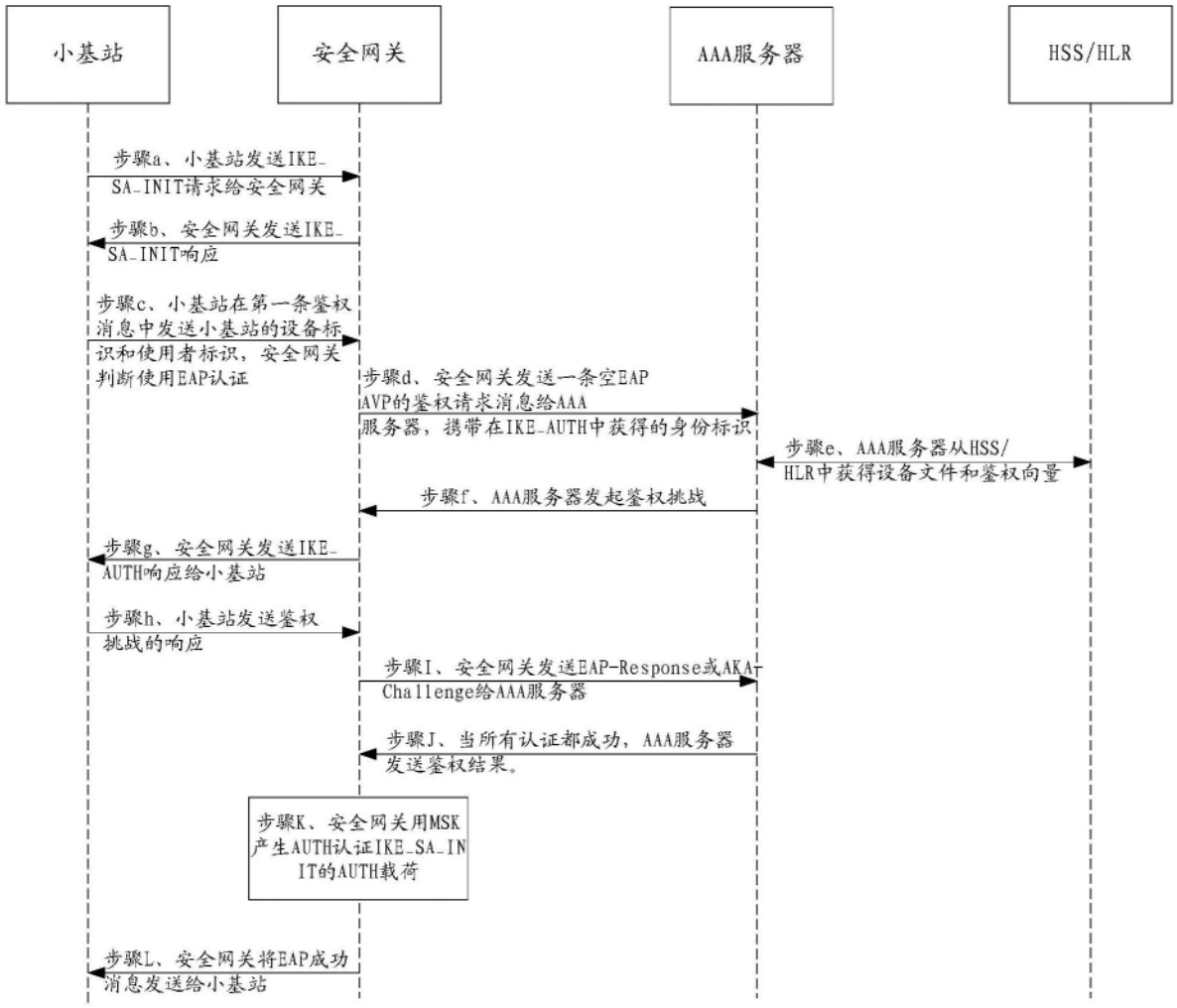

小基站
安全网关
AAA服务器
HSS/HLR
步骤a、小基站发送IKE_SA_INIT请求给安全网关
步骤b、安全网关发送IKE_SA_INIT响应
步骤c、小基站在第一条鉴权消息中发送小基站的设备标识和使用者标识，安全网关判断使用EAP认证
步骤d、安全网关发送一条空EAP AVP的鉴权请求消息给AAA服务器，携带在IKE_AUTH中获得的身份标识
步骤e、AAA服务器从HSS/HLR中获得设备文件和鉴权向量
步骤f、AAA服务器发起鉴权挑战
步骤g、安全网关发送IKE_AUTH响应给小基站
步骤h、小基站发送鉴权挑战的响应
步骤I、安全网关发送EAP-Response或AKA-Challenge给AAA服务器
步骤J、当所有认证都成功，AAA服务器发送鉴权结果。
步骤K、安全网关用MSK产生AUTH认证IKE_SA_INIT的AUTH载荷
步骤L、安全网关将EAP成功消息发送给小基站

图3

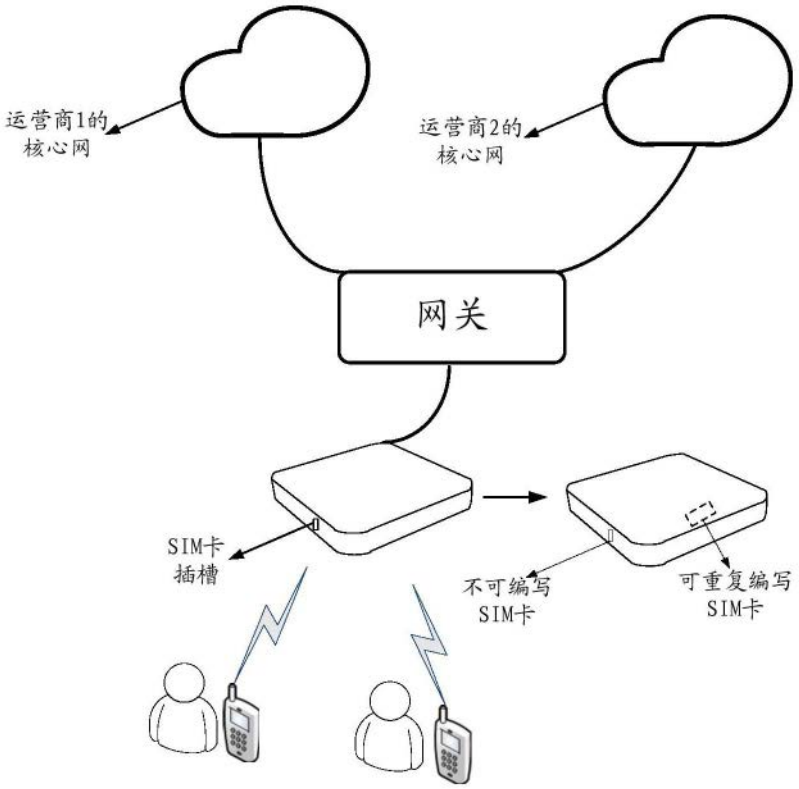

运营商1的
核心网
运营商2的
核心网
网关
SIM卡
插槽
不可编写
SIM卡
可重复编写
SIM卡

图4

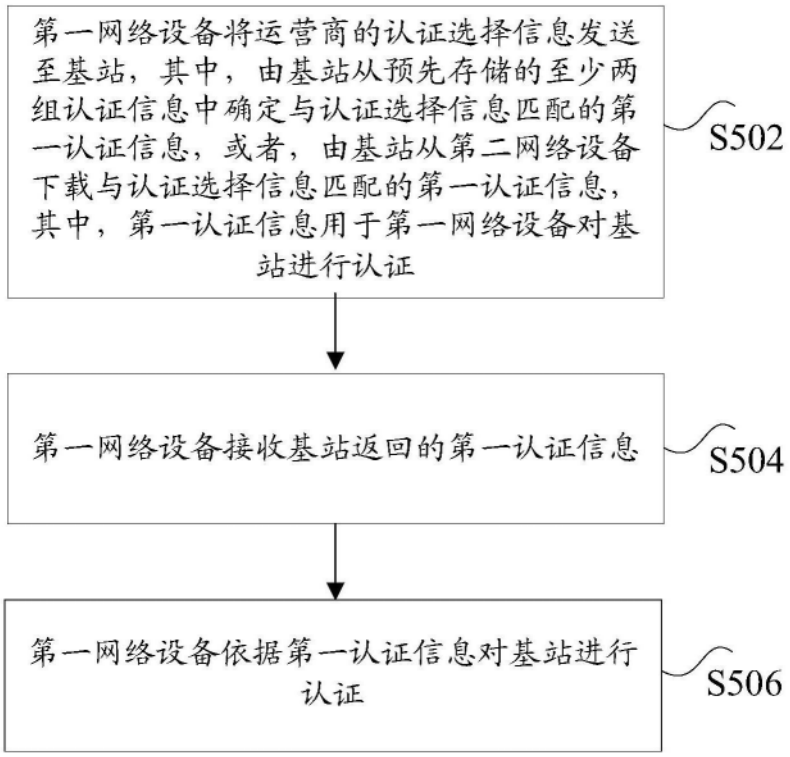

第一网络设备将运营商的认证选择信息发送至基站，其中，由基站从预先存储的至少两组认证信息中确定与认证选择信息匹配的第一认证信息，或者，由基站从第二网络设备下载与认证选择信息匹配的第一认证信息，其中，第一认证信息用于第一网络设备对基站进行认证
S502
第一网络设备接收基站返回的第一认证信息
S504
第一网络设备依据第一认证信息对基站进行认证
S506

图5

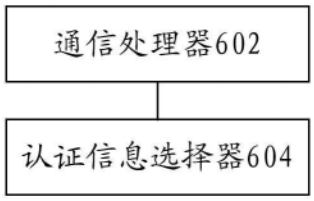

通信处理器602
认证信息选择器604

图6

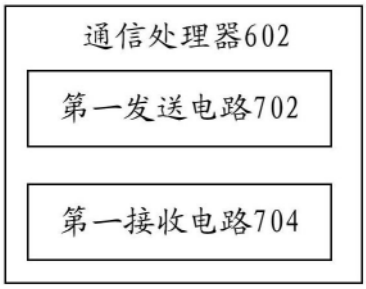

通信处理器602
第一发送电路702
第一接收电路704

图7


通信处理器602
第二发送电路802
第二接收电路804

图8

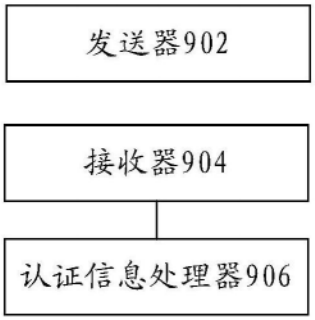

发送器902
接收器904
认证信息处理器906

图9

图10