(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112235799 A
(43)申请公布日 2021.01.15

(21)申请号 202011099106.3

(22)申请日 2020.10.14

(71)申请人 中国电力科学研究院有限公司
地址 100192 北京市海淀区清河小营东路15号

(72)发明人 汪洋 胡悦 王智慧 丁慧霞 吴赛 孟萨出拉 段钧宝 杨德龙 马宝娟

(74)专利代理机构 北京中巡通大知识产权代理有限公司 11703
代理人 钱宇婧

(51)Int.Cl.
H04W 12/06(2021.01)
H04W 12/041(2021.01)
H04W 12/0433(2021.01)

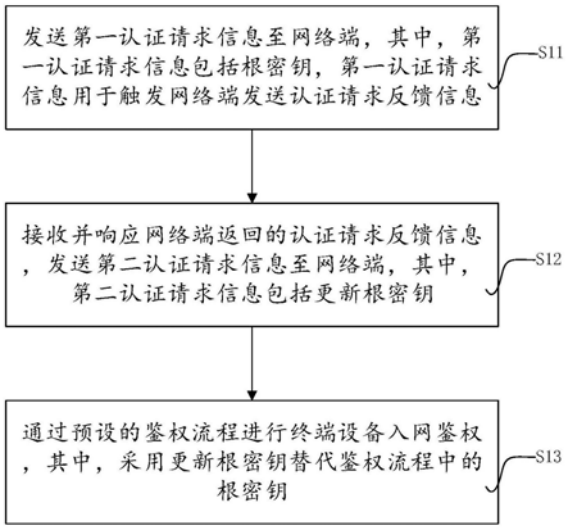
权利要求书2页 说明书8页 附图4页

(54)发明名称

终端设备入网鉴权方法及系统

(57)摘要

本发明属于通信技术领域，公开了一种终端设备入网鉴权方法及系统，包括以下步骤：发送第一认证请求信息至网络端，其中，第一认证请求信息包括根密钥，第一认证请求信息用于触发网络端发送认证请求反馈信息；接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥；通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥。解决了终端设备和网络之间的相互认证安全性不高的缺点，通过修改根密钥的方法来增强终端设备入网鉴权的安全性。



CN 112235799 A

1.一种终端设备入网鉴权方法,其特征在于,包括以下步骤:

发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;

接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥;

通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥。

2.根据权利要求1所述的终端设备入网鉴权方法,其特征在于,所述更新根密钥按照根密钥的格式要求随机生成。

3.根据权利要求1所述的终端设备入网鉴权方法,其特征在于,所述更新根密钥由根密钥通过预设的哈希算法计算得到。

4.根据权利要求1所述的终端设备入网鉴权方法,其特征在于,所述第二认证请求信息在接收网络端返回的认证请求反馈信息后的预设时间内发送;否则,鉴权失败。

5.根据权利要求1所述的终端设备入网鉴权方法,其特征在于,所述鉴权流程为5G AKA鉴权流程或EAP-AKA'鉴权流程。

6.一种终端设备入网鉴权方法,其特征在于,包括以下步骤:

发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;

接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新密钥交换常量;

通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

7.根据权利要求6所述的终端设备入网鉴权方法,其特征在于,所述更新密钥交换常量基于终端设备类型进行设定并存储。

8.一种终端设备入网鉴权方法,其特征在于,包括以下步骤:

发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;

接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥和更新密钥交换常量;

通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥,采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

9.一种终端设备入网鉴权系统,其特征在于,包括:

第一认证请求模块,用于发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;

第二认证请求模块,用于接收网络端返回的认证请求反馈信息,并发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥;以及入网鉴权模块,用于通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥。

10.一种终端设备入网鉴权系统,其特征在于,包括:

第一认证请求模块,用于发送第一认证请求信息至网络端,其中,第一认证请求信息用

于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥；

第二认证请求模块，用于接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新密钥交换常量；

以及入网鉴权模块，用于通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

终端设备入网鉴权方法及系统

技术领域

[0001] 本发明属于通信技术领域,涉及一种终端设备入网鉴权方法及系统。

背景技术

[0002] 随着5G通信技术的不断发展,以及5G通信技术与物联网技术相互渗透和深度融合,以用户为中心的万物互联时代的到来,随之对网络安全提出了更高的要求。其中,随着技术的发展和各类移动智能终端设备的需求,eSIM也将逐步替代传统的实体SIM卡,使移动终端无需使用可插拔SIM卡也可与蜂窝网络的连接。第三代合作伙伴计划(3rd Generation Partnership Project,3GPP)标准TS33.501,定义了一种5G认证与密钥协商协议(5G Authentication and Key Agreement,5GAKA)用于终端和网络间的认证。

[0003] 目前,主要依靠存储在用户SIM卡中的根密钥K实现终端和网络之间的相互认证,并导出会话密钥。安全的条件是根密钥K除了网络运营商外,别人都不知道。然而根密钥K非常可能在SIM卡的生产阶段就已经被泄漏,因此这种安全的条件并不可靠。被动攻击者可以使用从根密钥K,以及终端和网络之间的交换消息衍生的会话密钥来窃听通信。一个主动攻击者可能会利用偷来的大量根密钥伪造基站而发起攻击。

[0004] 从目前技术发展来看,针对根密钥K值的暴力破解手段同样可以对eSIM进行破解,因此,现有eSIM根密钥K的安全性较低,进而导致终端设备和网络之间的相互认证安全性不高,易发生非法终端的接入以及终端软硬件恶意篡改行为。

发明内容

[0005] 本发明的目的在于克服上述现有技术中,终端设备和网络之间的相互认证安全性不高的缺点,提供一种终端设备入网鉴权方法及系统。

[0006] 为达到上述目的,本发明采用以下技术方案予以实现:

[0007] 本发明第一方面,一种终端设备入网鉴权方法,包括以下步骤:

[0008] 发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;

[0009] 接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥;

[0010] 通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥。

[0011] 本发明终端设备入网鉴权方法进一步的改进在于:

[0012] 所述更新根密钥按照根密钥的格式要求随机生成。

[0013] 所述更新根密钥由根密钥通过预设的哈希算法计算得到。

[0014] 所述第二认证请求信息在接收网络端返回的认证请求反馈信息后的预设时间内发送;否则,鉴权失败。

[0015] 所述鉴权流程为5G AKA鉴权流程或EAP-AKA'鉴权流程。

[0016] 本发明第二方面，一种终端设备入网鉴权方法，其特征在于，包括以下步骤：

[0017] 发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥；

[0018] 接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新密钥交换常量；

[0019] 通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0020] 本发明终端设备入网鉴权方法进一步的改进在于：

[0021] 所述更新密钥交换常量基于终端设备类型进行设定并存储。

[0022] 本发明第二方面，一种终端设备入网鉴权方法，包括以下步骤：

[0023] 发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥；

[0024] 接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥和更新密钥交换常量；

[0025] 通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0026] 本发明第四方面，一种终端设备入网鉴权系统，包括：

[0027] 第一认证请求模块，用于发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥；

[0028] 第二认证请求模块，用于接收网络端返回的认证请求反馈信息，并发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥；以及入网鉴权模块，用于通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥。

[0029] 本发明第五方面，一种终端设备入网鉴权系统，包括：

[0030] 第一认证请求模块，用于发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥；

[0031] 第二认证请求模块，用于接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新密钥交换常量；

[0032] 以及入网鉴权模块，用于通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0033] 与现有技术相比，本发明具有以下有益效果：

[0034] 本发明终端设备入网鉴权方法，针对根密钥容易被窃取，进而导致终端设备和网络之间的相互认证安全性不高的问题，通过发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥，即在终端设备处主动修改根密钥的方式并发送至网络端，后续的鉴权流程中采用更新根密钥进行，有效防止攻击者使用窃取的根密钥进行鉴权，实现提升网络安全特性的目的，且只涉及在终端设备和网络端的改动，涉及网元少、实现难度低，通过从根密钥入手提高各层密钥推导的安全性，进而确保整个鉴权过程的安全性。

[0035] 本发明终端设备入网鉴权方法，通过修改鉴权流程中的密钥交换常量，使得在鉴权时采用不同的密钥交换常量进行各级派生密钥的计算，这样的设置，使得即使终端设备

的根密钥被泄露，但是由于攻击者并不清楚更新密钥交换常量的具体情况，依然无法实现正确的终端设备入网鉴权，从而有效提升终端设备入网鉴权的安全性。同时，该操作虽涉及到设备终端、接入网以及核心网中多个网元，但无需修改密钥派生算法的计算流程，只需修改参与运算的密钥交换常量，即可有效降低终端设备侧的风险，便于实现。

附图说明

[0036] 图1为本发明一实施例的终端设备入网鉴权方法流程框图；

[0037] 图2为本发明一实施例的5G AKA鉴权流程的流程框图；

[0038] 图3为本发明一实施例的EAP-AKA'鉴权流程的流程框图；

[0039] 图4为本发明再一实施例的终端设备入网鉴权方法流程框图；

[0040] 图5为本发明一实施例的密钥派生流程的流程框图；

[0041] 图6为本发明再一实施例的终端设备入网鉴权方法流程框图；

[0042] 图7为本发明一实施例的终端设备入网鉴权系统结构框图。

具体实施方式

[0043] 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。

[0044] 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。

[0045] 下面结合附图对本发明做进一步详细描述：

[0046] 参见图1，本发明一个实施例中，提供一种终端设备入网鉴权方法，通过对终端设备的根密钥进行改变，采用生成更新根密钥的方式，解决根密钥容易被窃取进而导致的鉴权安全问题，能够有效防止非法终端设备的接入以及终端设备软硬件的恶意篡改行为等，提高网络的安全性。具体的，该终端设备入网鉴权方法包括以下步骤：

[0047] S11：发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥。

[0048] 具体的，基于入网需求，终端设备一般会向电网发送第一认证请求信息至网络端，来告诉网络端当前的终端设备需要入网。一般来说，这个第一认证请求信息包括根密钥，可以用来表征终端设备的身份，传统的鉴权方法就是通过该根密钥实现在网络端的归属运行商(Home PLMN)和访问运行商(Visited PLMN)中进行入网鉴权认证。本实施例中，以该根密钥作为身份识别，网络端接收该根密钥并基于此判断是否进行后续的鉴权。同时，这个第一

认证请求信息中也可以包括当前终端设备的用户标识符(SUPI),网络端可根据用户标识符和根密钥的组合,判断当前终端设备是否进行后续的鉴权。

[0049] 第一认证请求信息用于触发网络端发送认证请求反馈信息,当网络端检测到有存储的相同的根密钥时,网络端发送认证请求反馈信息至终端设备。

[0050] S12:接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥。

[0051] 具体的,接收网络端返回的认证请求反馈信息,在收到网络端返回的认证请求反馈信息后,终端设备会将更新根密钥以第二认证请求信息的形式发送至网络端,以进行和网络端的协商,期望使用更新根密钥进行鉴权流程。

[0052] 其中,优选的,所述更新根密钥按照根密钥的格式要求随机生成,采用随机生成的方式,仅有格式要求的限制,在内容上灵活多变,增加更新根密钥的不确定性,进而增大破解的难度。

[0053] 优选的,所述更新根密钥也可以由根密钥通过预设的哈希算法计算得到。其中,哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值,这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式,如果散列一段明文而且哪怕只更改该段落的一个字母,随后的哈希都将产生不同的值,要找到散列为同一个值的两个不同的输入,在计算上是不可能的,所以数据的哈希值可以检验数据的完整性,一般用于快速查找和加密算法。

[0054] 采用基于哈希算法生成根密钥的方式,比如,通过终端设备esim上的程序实现哈希运算,便于自动化更新根密钥。

[0055] 优选的,所述第二认证请求信息在接收网络端返回的认证请求反馈信息后的预设时间内发送;否则,鉴权失败。通过给定的预设时间限制,网络端不能无限制的等待第二认证请求信息,在规定的预设时间内,终端设备没有将第二认证请求信息发送至网络端,即网络端没有在规定的时间内收到第二认证请求信息,那就表示此次鉴权失败。

[0056] S13:通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥。

[0057] 具体的,本实施例中,鉴权流程可以5G AKA(Authentication and Key Agreemen,身份验证和密钥协议)鉴权流程或EAP-AKA'鉴权流程,5G AKA鉴权流程或EAP-AKA'(可扩展认证协议方法或第三代认证和密钥协议)鉴权流程均在3GPP TS 33.501中具有详细的描述,根据其描述的5G AKA鉴权流程或EAP-AKA'鉴权流程进行鉴权即可,本实施例中,参见图2,示出了5G AKA鉴权流程的具体过程,其中,UE为用户设备,SEAF(security anchor function)为安全锚功能,AUSF(Authentication server function)为鉴权服务功能,参见图3,示出了EAP-AKA'鉴权流程的具体过程。

[0058] 本实施例中,以5G AKA鉴权流程或EAP-AKA'鉴权流程为基础,不同的是,鉴权流程中使用的根密钥采用更新根密钥替代,网络端及终端设备基于更新根密钥进行整个鉴权流程。

[0059] 综上所述,本实施例终端设备入网鉴权方法,针对根密钥容易被窃取,进而导致终端设备和网络之间的相互认证安全性不高的问题,通过发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥,即在终端设备处主动修改根密钥的方式并发送

至网络端，后续的鉴权流程中采用更新根密钥进行，有效防止攻击者使用窃取的根密钥进行鉴权，实现提升网络安全特性的目的，且只涉及在终端设备和网络端的改动，涉及网元少、实现难度低，通过从根密钥入手提高各层密钥推导的安全性，进而确保整个鉴权过程的安全性。

[0060] 参见图4，本发明再一个实施例中，提供一种终端设备入网鉴权方法，包括以下步骤。

[0061] S21：发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥。

[0062] S22：接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新密钥交换常量。

[0063] S23：通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0064] 相较于上一实施例中，本实施例的终端设备入网鉴权方法中区别在于，没有修改根密钥的值，但是修改了鉴权流程中需要使用到的密钥交换常量，依然是采用上一实施例中的方式，通过设备终端发送第二认证请求信息至网络端，只不过在第二认证请求信息中包括更新密钥交换常量，采用该更新密钥交换常量替代鉴权流程中的密钥交换常量进行鉴权流程，同样的，鉴权流程也可选择5G AKA鉴权流程或EAP-AKA'鉴权流程。

[0065] 其中，更新密钥交换常量是提前根据特定的规则，人为设定好并存储在设别终端内部，依据3GPP标准规范3GPP TS 33.501和3GPP TS 33.220中对密钥推导函数KDF(Key Derivation Function)的规定，密钥派生函数的输入参数是八位字符串，单个输入参数的长度不超过65535个八位字节。参见图5，示出了根密钥分散得到各级网元密钥的密钥派生流程，其中，CK加密密钥，IK完整性密钥，供终端设备计算出与网络端进行一致性检查的密钥，K_{AUSF}是一个关密钥派生的，通过ME和AUSF来自CK'，IK'在EAP-AKA'的情况下，CK'和IK'被AUSF接收为来自ARPF的变换AV的一部分；要么，通过来自CK的ME和ARPF，在5G AKA的情况下IK，K_{AUSF}被AUSF作为来自ARPF的5G HE AV的一部分接收。K_{SEAF}是由ME和AUSF从K_{AUSF}导出的锚密钥。K_{SEAF}由AUSF提供给服务网络中的SEAF，K_{AMF}是来自K_{SEAF}的ME和SEAF衍生的密钥。当执行水平密钥导出时，通过ME和源AMF进一步导出K_{AMF}。K_{nasint}是来自K_{AMF}的ME和AMF(验证管理字段)导出的密钥，其仅用于通过特定完整性算法保护NAS信令。K_{nasenc}是来自K_{AMF}的ME和AMF导出的密钥，其仅用于通过特定加密算法保护NAS信令。K_{gNB}是来自K_{AMF}的ME和AMF衍生的密钥。当执行水平或垂直密钥导出时，由ME和源gNB进一步导出K_{gNB}。K_{gNB}用作ME和ng-eNB之间的K基站。K_{upenc}是由ME和来自K的TFgNB导出的密钥，其仅用于通过特定加密算法保护UP业务。K_{upint}是由ME和gNB从K_{gNB}导出的密钥，其仅用于通过特定的完整性算法来保护ME和gNB之间的UP业务。K_{rrcint}是由ME和来自K的TFgNB导出的密钥，其仅用于利用特定完整性算法来保护RRC信令。K_{rrcenc}是由ME和来自K_{gNB}的gNB导出的密钥，其仅用于利用特定加密算法保护RRC信令。NH是由ME和AMF派生的密钥；K_{N3IWF}是由ME和AMF从K_{AMF}导出的用于非3GPP接入的密钥。

[0066] 密钥派生流程中，密钥派生算法的计算流程中涉及到的密钥交换常量FC在3GPP TS 33.501中使用范围为0x69～0x76，如表1所示。

[0067] 表1更新密钥交换常量与密钥交换常量对照表

[0068]

Key	密钥交换常量	更新密钥交换常量	含义
Kausf	0x6A	XX	认证服务器功能密钥交换（Authentication Server Function key exchange）
Kseaf	0x6C	XX	安全锚功能键交换（SEcurity Anchor Function key exchange）
Kamf	0x6D	XX	身份验证管理字段密钥交换（Authentication Management Field key exchange）
kgNB	0x6E	XX	NR 节点 B 密钥交换（NR Node B key exchange）
NH	0x6F	XX	

[0069] 其中，XX为代指，意为可以从0x69～0x76的范围内任意取值，可以是随机取值的方式，也可以是其他的预设规则的取值方式。

[0070] 优选的，所述更新密钥交换常量基于终端设备类型进行设定并存储，基于终端设备类型与更新密钥交换常量的对应关系，可以从网络端分析当前进行鉴权的终端设备的类型，便于进行专项管理。

[0071] 综上所述，本实施例终端设备入网鉴权方法，通过修改鉴权流程中的密钥交换常量，使得在鉴权时采用不同的密钥交换常量进行各级派生密钥的计算，这样的设置，使得即使终端设备的根密钥被泄露，但是由于攻击者并不清楚更新密钥交换常量的具体情况，依然无法实现正确的终端设备入网鉴权，从而有效提升终端设备入网鉴权的安全性。同时，该操作虽涉及到设备终端、接入网以及核心网中多个网元，但无需修改密钥派生算法的计算流程，只需修改参与运算的密钥交换常量，即可有效降低终端设备侧的风险，便于实现。

[0072] 参见图6，本发明再一个实施例中，提供一种终端设备入网鉴权方法，包括以下步骤。

[0073] S31：发送第一认证请求信息至网络端，其中，第一认证请求信息用于触发网络端发送认证请求反馈信息，第一认证请求信息包括用于认证的根密钥。

[0074] S32：接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥和更新密钥交换常量。

[0075] S33：通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0076] 本实施例中，采用修改根密钥及密钥交换常量结合的方式，根密钥的修改可参见图1所示实施例中提供的方法，密钥交换常量的修改可参见图4所示实施例中提供的方法，通过双重修改进一步提高终端设备入网鉴权的安全性。

[0077] 本发明再一个实施例中，发明人发现，随着5G的发展，其为垂直行业的企业带来了一场全新的变局，既带来了机遇也带来了挑战，暂且把网络安全问题交给专网或者公网的解决方案来保障，对垂直行业的电力行业用户来说，仍需考虑空口通信的安全，提高电力5G模组自身的安全性，达到提高电力终端的安全性，本实施例中以电力模组eSIM为终端设备进行说明本发明终端设备入网鉴权方法，针对电力模组eSIM泄密的问题，通过对电力终端设备eSIM的根密钥改进来增强系统密钥安全性的方法，提升电力专网安全性并实现在电力5G模组安全方向的升级改造，进而有效防止非法通信终端的接入以及通信终端软硬件的恶

意篡改行为等,提高电力专网的安全性。

[0078] 具体的,终端设备eSIM发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;然后,终端设备eSIM接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥;这里的更新根密钥利用哈希算法计算得到,然后通过预设的鉴权流程进行终端设备入网鉴权,其中,在鉴权流程中,采用更新根密钥替代根密钥。

[0079] 采用在网络侧UDM/ARPF(Unified Data Management/Authentication credentialRepository and Processing Function,统一数据管理平台/认证凭证存储库和处理功能)以及终端设备eSIM侧,修改根密钥K,本实施例中利用哈希算法计算出新的根密钥K的方法来增强入网鉴权安全性,只涉及在终端设备eSIM侧和网络侧UDM/ARPF的改动,即可实现电力特色5G专网的安全特性,同时从根密钥入手也提高了各层密钥推导的安全性。

[0080] 同时,终端设备eSIM发送的第二认证请求信息中还包括更新密钥交换常量,本实施例中,更新密钥交换常量在3GPP TS 33.501中规定的密钥交换常量使用范围0x69～0x76中取值,但是其具体值根据电力设备的类型确定,形成密钥交换常量与电力设备的类型一一对应的关系,这样便于从网络侧分析当前鉴权的终端设备eSIM所处电力设备的类型;也可以按照其他的设计要求自行设定。通过预设的鉴权流程进行终端设备入网鉴权时,其中,在鉴权流程中,采用更新密钥交换常量替代密钥交换常量。

[0081] 通过电力专网自定义的一套密钥交换常量参与各级密钥派生算法的运算,得到各层分散密钥,可达到进一步增强入网认证安全性的目标,该操作虽涉及到通信终端、接入网及核心网中多个网元,但无需修改密钥算法计算流程,只需修改参与运算的密钥交换常量,即可有效降低终端侧风险,同时可自主可控地完成国家电网特色5G专网方案和建设。

[0082] 参见图7,本发明再一个实施例中,提供一种终端设备入网鉴权系统,该终端设备入网鉴权系统能够实现图1所示实施例中的终端设备入网鉴权方法,具体的,该终端设备入网鉴权系统包括第一认证请求模块、第二认证请求模块以及入网鉴权模块。

[0083] 其中,第一认证请求模块用于发送第一认证请求信息至网络端,其中,第一认证请求信息用于触发网络端发送认证请求反馈信息,第一认证请求信息包括用于认证的根密钥;第二认证请求模块用于接收网络端返回的认证请求反馈信息,并发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新根密钥;入网鉴权模块用于通过预设的鉴权流程进行终端设备入网鉴权,其中,采用更新根密钥替代鉴权流程中的根密钥。

[0084] 本发明再一个实施例中,提供一种终端设备入网鉴权系统,该终端设备入网鉴权系统能够实现图4所示实施例中的终端设备入网鉴权方法,具体的,该终端设备入网鉴权系统的组成与上一实施例中的终端设备入网鉴权系统的结构相同,不同之处在于各模块实现的功能。

[0085] 具体的,相较于上一实施例中的终端设备入网鉴权系统,本实施例终端设备入网鉴权系统中的第二认证请求模块以及入网鉴权模块与上一实施例不同,本实施例中,第二认证请求模块用于接收并响应网络端返回的认证请求反馈信息,发送第二认证请求信息至网络端,其中,第二认证请求信息包括更新密钥交换常量;入网鉴权模块用于通过预设的鉴

权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量。

[0086] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0087] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0088] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0089] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0090] 最后应当说明的是：以上实施例仅用以说明本发明的技术方案而非对其限制，尽管参照上述实施例对本发明进行了详细的说明，所属领域的普通技术人员应当理解：依然可以对本发明的具体实施方式进行修改或者等同替换，而未脱离本发明精神和范围的任何修改或者等同替换，其均应涵盖在本发明的权利要求保护范围之内。

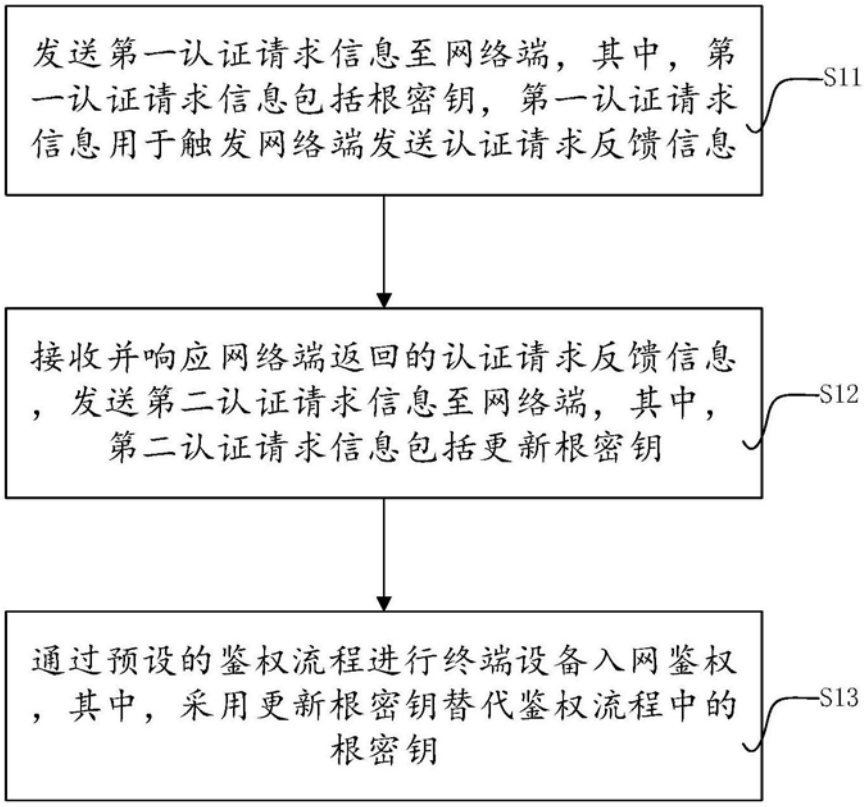

发送第一认证请求信息至网络端，其中，第一认证请求信息包括根密钥，第一认证请求信息用于触发网络端发送认证请求反馈信息
S11
接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥
S12
通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥
S13

图1

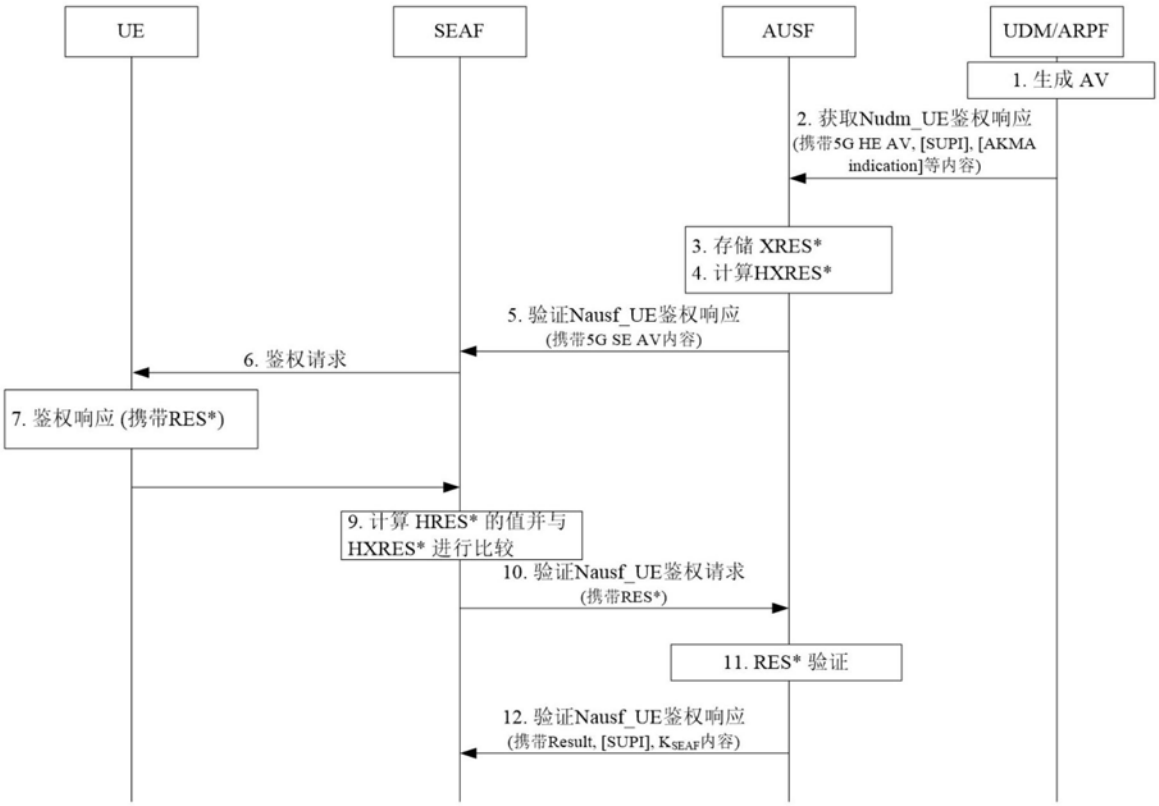

UE
SEAF
AUSF
UDM/ARPF
1. 生成 AV
2. 获取Nudm_UE鉴权响应
(携带5G HE AV, [SUPI], [AKMA indication]等内容)
3. 存储 XRES*
4. 计算HXRES*
5. 验证Nausf_UE鉴权响应
(携带5G SE AV内容)
6. 鉴权请求
7. 鉴权响应 (携带RES*)
9. 计算 HRES* 的值并与 HXRES* 进行比较
10. 验证Nausf_UE鉴权请求
(携带RES*)
11. RES* 验证
12. 验证Nausf_UE鉴权响应
(携带Result, [SUPI], K_{SEAF}内容)

图2

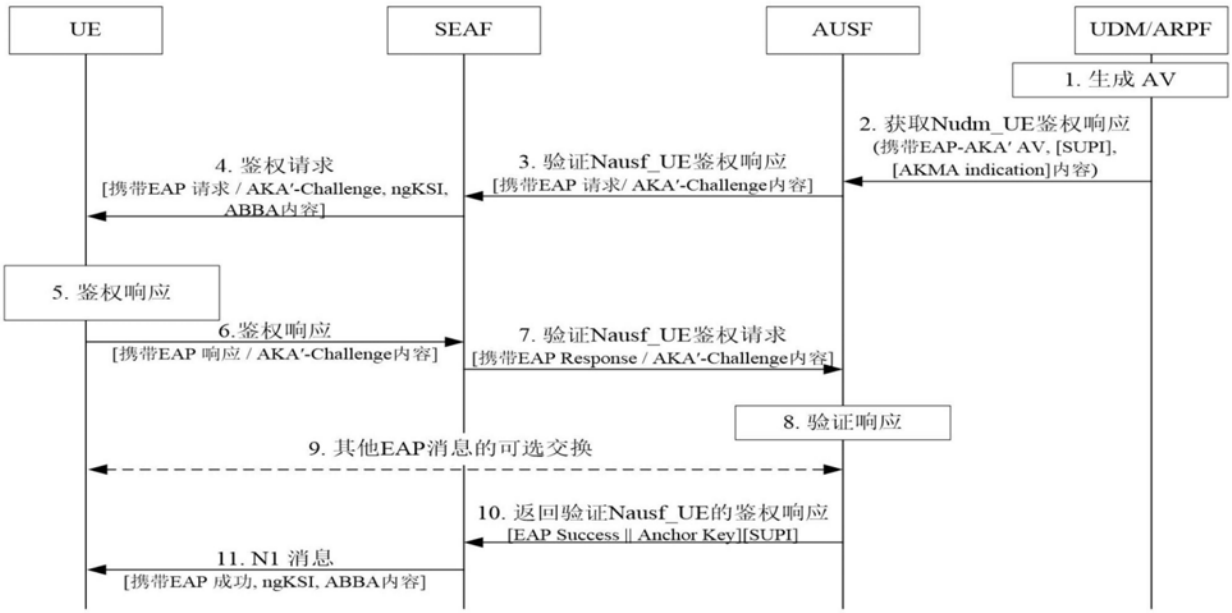

UE
SEAF
AUSF
UDM/ARPF
1. 生成 AV
2. 获取Nudm_UE鉴权响应
(携带EAP-AKA′ AV, [SUPI], [AKMA indication]内容)
3. 验证Nausf_UE鉴权响应
[携带EAP 请求/ AKA′-Challenge内容]
4. 鉴权请求
[携带EAP 请求 / AKA′-Challenge, ngKSI, ABBA内容]
5. 鉴权响应
6.鉴权响应
[携带EAP 响应 / AKA′-Challenge内容]
7. 验证Nausf_UE鉴权请求
[携带EAP Response / AKA′-Challenge内容]
8. 验证响应
9. 其他EAP消息的可选交换
10. 返回验证Nausf_UE的鉴权响应
[EAP Success || Anchor Key][SUPI]
11. N1 消息
[携带EAP 成功, ngKSI, ABBA内容]

图3

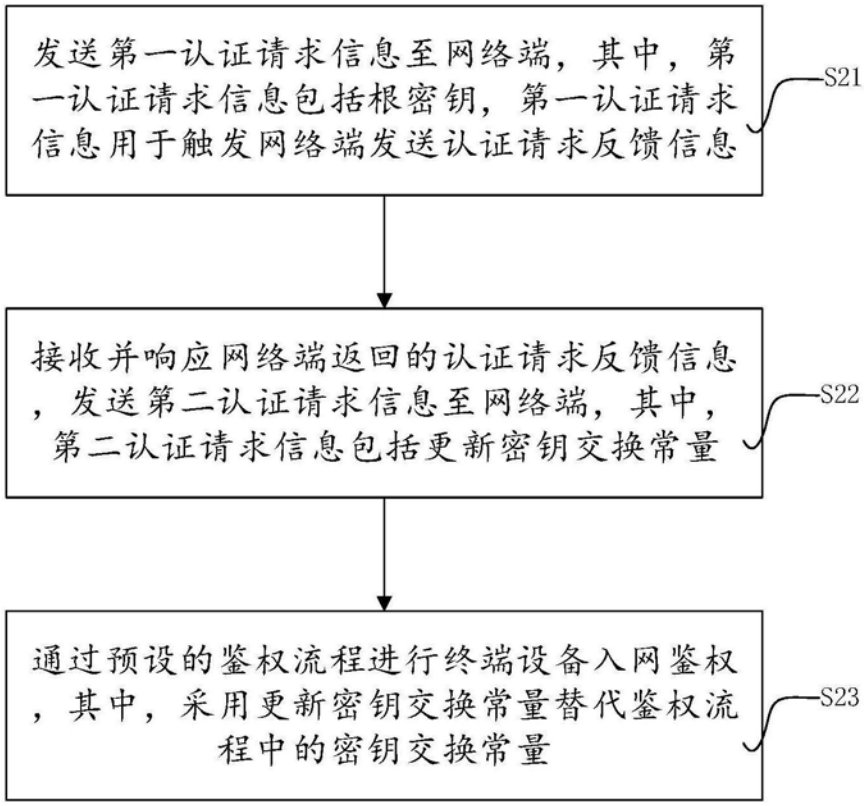

发送第一认证请求信息至网络端，其中，第一认证请求信息包括根密钥，第一认证请求信息用于触发网络端发送认证请求反馈信息
S21
接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新密钥交换常量
S22
通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新密钥交换常量替代鉴权流程中的密钥交换常量
S23

图4

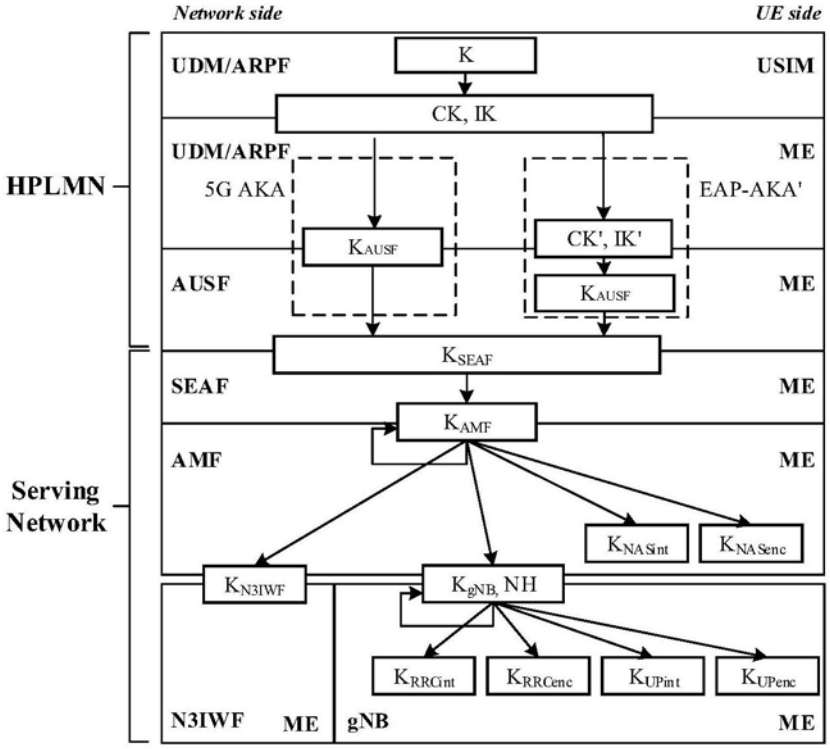

Network side
UE side
HPLMN
Serving Network
UDM/ARPF
K
USIM
CK, IK
UDM/ARPF
ME
5G AKA
EAP-AKA'
KAUSF
CK', IK'
AUSF
KAUSF
ME
KSEAF
SEAF
ME
KAMF
AMF
ME
KNASint
KNASenc
KN3IWF
KgNB, NH
KRRCint
KRRCenc
KUPint
KUPenc
N3IWF
ME
gNB
ME

图5

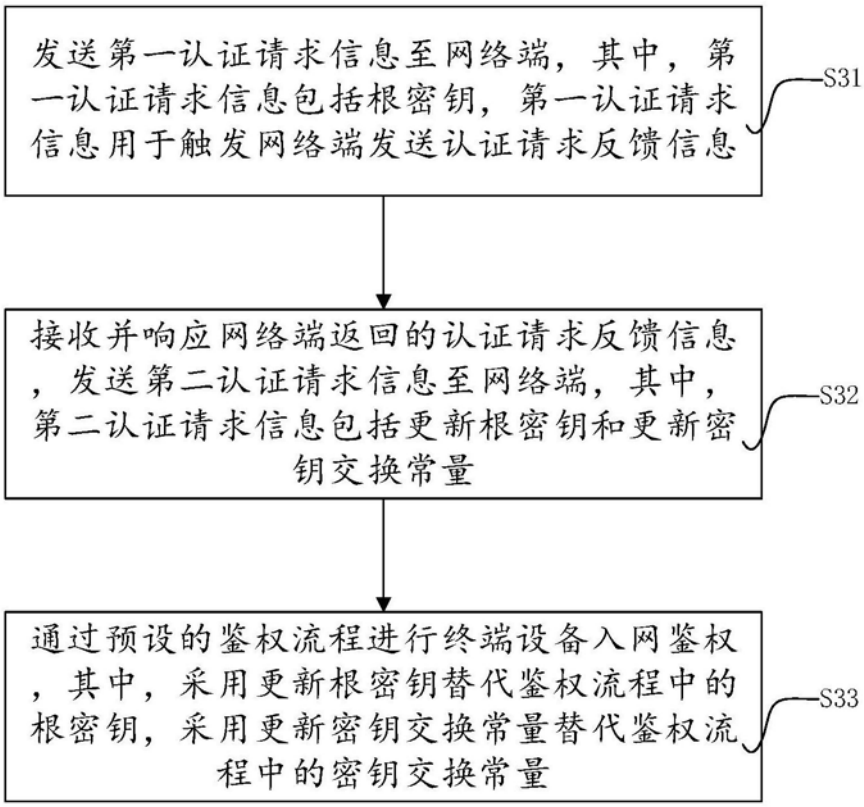

发送第一认证请求信息至网络端，其中，第一认证请求信息包括根密钥，第一认证请求信息用于触发网络端发送认证请求反馈信息
S31
接收并响应网络端返回的认证请求反馈信息，发送第二认证请求信息至网络端，其中，第二认证请求信息包括更新根密钥和更新密钥交换常量
S32
通过预设的鉴权流程进行终端设备入网鉴权，其中，采用更新根密钥替代鉴权流程中的根密钥，采用更新密钥交换常量替代鉴权流程中的密钥交换常量
S33

图6

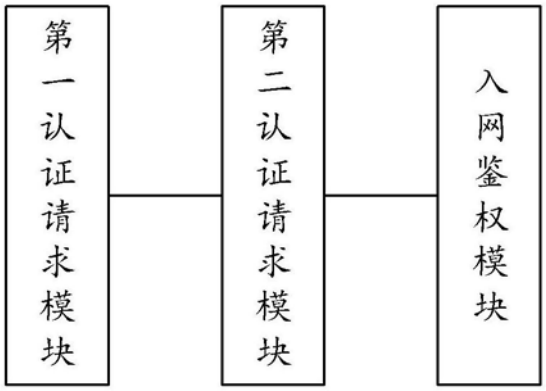

第一认证请求模块
第二认证请求模块
入网鉴权模块

图7