(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 3 月 15 日 (15.03.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/045983 A1

(51) 国际专利分类号:
H04W 8/26 (2009.01)

(21) 国际申请号: PCT/CN2017/100915

(22) 国际申请日: 2017 年 9 月 7 日 (07.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610815121.0 2016年9月9日 (09.09.2016) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 游世林 (YOU, Shilin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 蔡继燕 (CAI, Jiyan); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 林兆骥 (LIN, Zhaoji); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 彭锦 (PENG, Jin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 梁爽 (LIANG, Shuang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 李志军 (LI, Zhijun); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 赵孝武 (ZHAO, Xiaowu); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(54) **Title:** INFORMATION PROCESSING METHOD AND DEVICE, AND NETWORK SYSTEM

(54) **发明名称**: 信息处理方法、装置以及网络系统

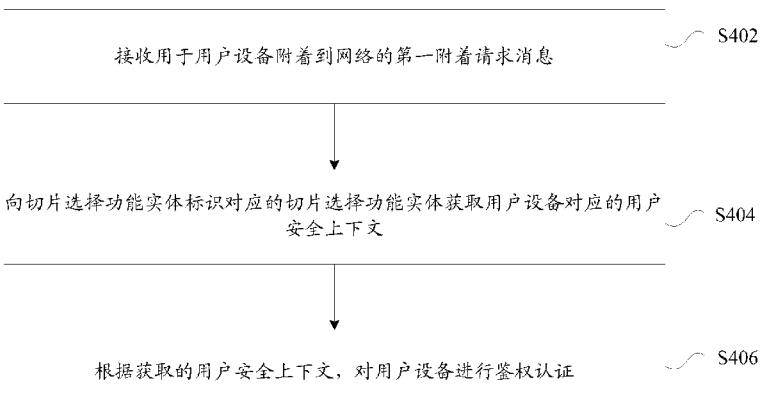

图 4

S402 RECEIVE A FIRST ATTACHMENT REQUEST MESSAGE FOR MAKING A USER EQUIPMENT BE ATTACHED TO A NETWORK
S404 OBTAIN USER SECURITY CONTEXT CORRESPONDING TO THE USER EQUIPMENT FROM A SLICE SELECTION ENTITY CORRESPONDING TO A SLICE SELECTION ENTITY IDENTIFIER
S406 PERFORM AUTHENTICATION ON THE USER EQUIPMENT ACCORDING TO THE OBTAINED USER SECURITY CONTEXT

(57) **Abstract:** The present invention provides an information processing method and device, and a network system. The method comprises: receiving a first attachment request message for making a user equipment be attached to a network, wherein the first attachment request message carries a slice selection entity identifier used for identifying a slice selection entity; obtaining user security context corresponding to the user equipment from the slice selection entity corresponding to the slice selection entity identifier; and performing authentication on the user equipment according to the obtained user security context. The present invention resolves the problem in

WO 2018/045983 A1

[见续页]

(74) 代理人：北京康信知识产权代理有限责任公司(KANGXIN PARTNERS,P.C.)；中国北京市海淀区知春路甲48号盈都大厦A座16层, Beijing 100098 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告(条约第21条(3))。

the related art of the increased processing load of a user data center caused by the requirement of frequent interaction with the user data center during a user registration process, and achieves the effects of reducing the signaling load and lowering the processing load of the user data center.

(57) 摘要：本公开提供了一种信息处理方法、装置以及网络系统，其中，该方法包括：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。通过本公开，解决了相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题，达到了降低信令负荷、减少用户数据中心处理负荷的效果。

信息处理方法、装置以及网络系统

技术领域

本公开涉及通信领域，具体而言，涉及一种信息处理方法、装置以及网络系统。

背景技术

移动通信在二十多年时间里得到了飞速发展，给人们的生活方式、工作方式以及社会政治、经济等各方面都带来了巨大的影响。人类社会进入高效的信息化时代，各个方面业务应用需求呈现爆发式增长，给未来无线移动带宽系统在频率、技术以及运营等各方面都带来了巨大的挑战。

未来的移动网络除了为人人通信提供服务外，还将为越来越多的物联网终端提供接入服务。物联网接入给移动网络带来了新的挑战和机遇。不同类型的物联网对网络的需求千差万别，有的要求网络提供高实时高可靠服务，如远程医疗，有的则要求提供有规律的小数据量传输服务，如远程抄表系统。针对不同的业务需求，移动网络可能需要适当优化才能满足业务需求。越来越多的物联网对移动网络提出了越来越多不同的优化需求，其中，有些优化需求还可能相互矛盾，因此，一张融合的核心网越来越无法满足各种不同的物联网需求。

随着网络功能虚拟化（Network Function Virtualization，简称为 NFV）的出现，核心网功能可以基于通用硬件构建，而毋须基于专用硬件平台。NFV 的出现使得运营商为不同的网络业务需求构建不同的虚拟核心网络成为可能。为不同网络业务需求构建的虚拟核心网称为一个网络切片。虚拟核心网中的各网络功能可根据网络业务需求进行优化、定制。基于 NFV 技术的网络切片可根据需求快速部署，以快速满足不同场景的需求。

图 1 是相关技术中网络切片的示意图。如图 1 所示，示例了三个网络切片（网络切片 A、B、C）。其中每个切片都包括无线接入网络、通用网

络功能实体，切片控制面功能实体和切片用户面功能实体。其中通用功能实体包括移动性管理实体、会话管理实体和鉴权认证实体（切片 A 和 B）。如果切片无通用网络功能实体，则切片通用功能实体包含在切片控制面功能实体中（切片 C），另外网络还包含用户数据中心，保存用户设备的用户签约数据和安全数据（根密钥），用户设备（User Equipment，简称为 UE）通过无线接入网络接入网络，通过切片选择功能实体选择合适的切片进行业务。

图 2 是相关技术中用户设备接入网络选择合适的切片的初始注册和重注册的流程示意图，如图 2 所示，该流程包括如下步骤：

步骤 S202，用户设备向无线接入网络发送初始的附着请求消息，无线接入网络向切片选择功能实体转发所述附着请求消息，所述消息携带用户标识。

步骤 S204，切片选择功能实体根据用户标识从用户数据中心获取用户签约信息和安全上下文，对用户和网络进行相互认证。

上述认证过程包括：切片选择功能实体向用户数据中心发送鉴权认证请求消息，用户数据中心向切片选择功能实体回送鉴权认证请求响应消息，所述消息携带用户安全上下文，即安全向量组，切片选择功能实体向用户设备发送用户鉴权认证请求消息，所述消息携带认证令牌，用户设备通过认证令牌验证网络的合法性，并计算出期望的响应值，向切片选择功能实体回送用户鉴权认证请求响应消息，所述携带期望的响应值，切片选择功能实体将安全上下文中的期望的响应值和收到的期望的响应值比对，如果相等，认证用户设备合法，向用户数据中心获取用户签约数据，切片选择功能实体保存安全上下文和用户签约数据。

步骤 S206，切片选择功能实体根据用户签约数据中的信息选择合适的切片，即，切片选择功能实体选择合适的切片标识。

步骤 S208，切片选择功能实体向无线接入网络发送切片选择消息，该消息携带切片标识。

步骤 S210，无线接入网络根据对应的切片标识选择对应的切片。

步骤 S212a，无线接入网络向选择的切片的切片移动性管理实体发送附着请求消息，切片移动性管理实体选择合适的切片鉴权认证实体并向切片鉴权认证实体转发附着请求消息。

步骤 S212b，切片鉴权认证实体向用户数据中心获取用户签约数据，认证用户是否能够合法接入切片。

该鉴权认证过程包括：切片鉴权认证实体向用户数据中心发送鉴权认证请求消息，用户数据中心向切片鉴权认证实体回送鉴权认证请求响应消息，该消息携带用户安全上下文，即安全向量组，切片鉴权认证实体向用户设备发送用户鉴权认证请求消息，该消息携带认证令牌，用户设备通过认证令牌验证网络的合法性，并计算出期望的响应值，向切片鉴权认证实体回送用户鉴权认证请求响应消息，所述携带期望的响应值，切片鉴权认证实体将安全上下文中的期望的响应值和收到的期望的响应值比对，如果相等，认证用户设备合法，向用户数据中心获取用户签约数据，切片鉴权认证实体保存安全上下文和用户签约数据。

步骤 S212c，同用户面网关建立用户面连接（可选步骤）。

步骤 S212d，切片鉴权认证实体认证成功后，向切片移动性管理实体回送附着响应消息，切片移动性管理实体向无线网络管理实体回送附着响应消息。

步骤 S214，无线接入网络向用户设备消息回送附着响应消息，该消息携带切片标识。

步骤 S202-S214 完成用户设备的初始注册。

步骤 S216，用户设备向无线接入网络发起重注册请求消息，该消息携带切片标识。

步骤 S218，无线接入网络直接向切片管理实体转发重注册请求消息。

步骤 S220，按照步骤 206-步骤 207 完成重注册过程。

从上述流程可以看出，在用户的初始注册过程中需要2次向用户数据中心获取用户安全上下文和用户签约数据，另外在用户的重注册过程中，也需要向用户数据中心获取用户安全上下文和用户签约数据，而用户数据中心位于用户的归属域，这样的过程需要多次到归属域获取用户安全上下文和用户签约数据，将增加信令负荷，而且一般来说用户数据中心管理的用户较多，这样将增加用户数据中心的处理负荷。

因此，相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题。

发明内容

本公开实施例提供了一种信息处理方法、装置以及网络系统，以至少解决相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题。

根据本公开的一个实施例，提供了一种信息处理方法，包括：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。

可选地，在鉴权认证结果为所述用户设备合法的情况下，在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证之后，还包括：为所述用户设备分配用于标识所述用户设备的第一标识信息；向所述用户设备发送附着响应消息，其中，所述附着响应消息携带有所述第一标识信息。

可选地，在向所述用户设备发送所述附着响应消息之后，还包括：接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第一标识信息；根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；根据获取的所述安全上下文，对所述用户设备进行鉴权认证。

可选地，在向所述用户设备发送所述附着响应消息之后，还包括：接

收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第一标识信息；根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述预设网元。

可选地，在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证的过程中，还包括：向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的另一个实施例，提供了一种信息处理方法，包括：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

可选地，在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：接收所述鉴权认证实体发送的第一附着响应消息；为所述用户设备分配用于标识所述用户设备的第二标识信息；向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

可选地，在向所述用户设备发送所述第二附着响应消息之后，还包括：接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述鉴权认证实体。

可选地，在向所述用户设备发送所述第二附着响应消息之后，还包括：接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述预设网元。

可选地，在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的又一个实施例，提供了一种信息处理装置，包括：第一接收模块，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；获取模块，设置为向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；鉴权模块，设置为根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。

可选地，所述装置还包括：分配模块，设置为在鉴权模块的鉴权认证结果为所述用户设备合法的情况下，为所述用户设备分配用于标识所述用户设备的第一标识信息；发送模块，设置为向所述用户设备发送附着响应消息，其中，所述附着响应消息携带有所述第一标识信息。

可选地，所述第一接收模块，还设置为接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第一标识信息；所述获取模块，还设置为根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；所述鉴权模块，还设置为根据获取的所述安全上下文，对所述用户设备进行鉴权认证。

可选地，所述接收模块，还设置为接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第一标识信息；所述获取模块，还设置为根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；所述发送模块，还设置为将获取的所述安全上下文发送给所述预设网元。

可选地，所述获取模块，还设置为向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的又一个实施例，提供了一种鉴权认证实体，包括：上述任一项所述的装置。

根据本公开的又一个实施例，提供了一种信息处理装置，包括：接收

模块，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；获取模块，设置为向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；发送模块，设置为将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

可选地，所述装置还包括：分配模块，其中，所述接收模块，还设置为接收所述鉴权认证实体发送的第一附着响应消息；所述分配模块，设置为为所述用户设备分配用于标识所述用户设备的第二标识信息；所述发送模块，还设置为向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

可选地，所述接收模块，还设置为接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第二标识信息；所述获取模块，还设置为根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；所述发送模块，还设置为将获取的所述安全上下文发送给所述鉴权认证实体。

可选地，所述接收模块，还设置为接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息；所述获取模块，还设置为根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；所述发送模块，设置为将获取的所述安全上下文发送给所述预设网元。

可选地，所述获取模块，还设置为向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的又一个实施例，提供了一种移动性管理实体，包括：上述任一项所述的装置。

根据本公开的又一个实施例，提供了一种网络系统，该网络系统包括切片选择功能实体、鉴权认证实体和移动性管理实体，所述切片选择功能

实体与所述鉴权认证实体之间通过接口进行交互，所述鉴权认证实体包括权利要求上述任一项所述的装置，和/或，所述切片选择功能实体与所述移动性管理实体之间通过接口进行交互，所述移动性管理实体包括上述任一项所述的装置。

根据本公开的又一个实施例，还提供了一种存储介质。该存储介质设置为存储用于执行以下步骤的程序代码：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在鉴权认证结果为所述用户设备合法的情况下，在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证之后，还包括：为所述用户设备分配用于标识所述用户设备的第一标识信息；向所述用户设备发送附着响应消息，其中，所述附着响应消息携带有所述第一标识信息。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在向所述用户设备发送所述附着响应消息之后，还包括：接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第一标识信息；根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；根据获取的所述安全上下文，对所述用户设备进行鉴权认证。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在向所述用户设备发送所述附着响应消息之后，还包括：接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第一标识信息；根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述预设网元。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证的过程中，还包括：向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的又一个实施例，还提供了一种存储介质。该存储介质设置为存储用于执行以下步骤的程序代码：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：接收所述鉴权认证实体发送的第一附着响应消息；为所述用户设备分配用于标识所述用户设备的第二标识信息；向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在向所述用户设备发送所述第二附着响应消息之后，还包括：接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述鉴权认证实体。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在向所述用户设备发送所述第二附着响应消息之后，还包括：接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述预设网元。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：向所述切片选择实体获取所述用户设备的用户签约数据。

根据本公开的又一个实施例，还提供了一种处理器，所述处理器用于运行程序，其中，所述程序运行时执行上述任一项所述的方法。

通过本公开，通过切片选择功能实体标识从切片选择功能实体中获取用户安全上下文，对用户设备进行鉴权认证，由于增加切片选择功能实体与切片通用网络功能实体或者切片控制面功能实体接口，减少了用户数据中心的处理负荷，因此，可以解决相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题，达到降低信令负荷、减少用户数据中心处理负荷的效果。

附图说明

此处所说明的附图用来提供对本公开的理解，构成本申请的一部分，本公开的示意性实施例及其说明用于解释本公开，并不构成对本公开的不当限定。在附图中：

图 1 是相关技术中网络切片的示意图；

图 2 是相关技术中用户设备接入网络选择合适的切片的初始注册和重注册的流程示意图；

图 3 是本公开实施例的一种信息处理方法的鉴权认证实体的硬件结构框图；

图 4 是根据本公开实施例的信息处理方法的流程图一；

图 5 是根据本公开实施例的信息处理方法的流程图二；

图 6 是根据本公开优选实施例的网络切片的架构示意图；

图 7 是根据本公开优选实施例的用户设备接入网络选择合适的切片的初始注册和重注册的流程示意图；

图 8 是根据本公开实施例的信号处理装置的结构框图一；

图 9 是根据本公开实施例的信号处理装置的结构框图二;

图 10 是根据本公开实施例的鉴权认证实体的结构框图;

图 11 是根据本公开实施例的信号处理装置的结构框图三;

图 12 是根据本公开实施例的信号处理装置的结构框图四;

图 13 是根据本公开实施例的移动性管理实体的结构框图;

图 14 是根据本公开实施例的网络系统的结构框图。

具体实施方式

下文中将参考附图并结合实施例来详细说明本公开。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特征可以相互组合。

需要说明的是，本公开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。

实施例 1

本申请实施例 1 所提供的方法实施例可以在鉴权认证实体、移动性管理实体、计算机终端或者类似的运算装置中执行。以运行在鉴权认证实体上为例，图 3 是本公开实施例的一种信息处理方法的鉴权认证实体的硬件结构框图。如图 3 所示，鉴权认证实体 30 可以包括一个或多个（图中仅示出一个）处理器 32（处理器 32 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 34、以及用于通信功能的传输装置 36。本领域普通技术人员可以理解，图 3 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，鉴权认证实体 30 还可包括比图 3 中所示更多或者更少的组件，或者具有与图 3 所示不同的配置。

存储器 34 可用于存储应用软件的软件程序以及模块，如本公开实施例中的信息处理方法对应的程序指令/模块，处理器 32 通过运行存储在存储器 34 内的软件程序以及模块，从而执行各种功能应用以及数据处理，

即实现上述的方法。存储器 34 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 34 还可包括相对于处理器 32 远程设置的存储器，这些远程存储器可以通过网络连接至鉴权认证实体 30。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

传输装置 36 用于经由一个网络接收或者发送数据。上述网络的实例可包括鉴权认证实体 30 的通信供应商提供的无线网络。在一个实例中，传输装置 36 包括一个网络适配器（Network Interface Controller，简称为 NIC），其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置 36 可以为射频（Radio Frequency，简称为 RF）模块，其用于通过无线方式与互联网进行通讯。

在本实施例中提供了一种运行于上述鉴权认证实体的信息处理方法，图 4 是根据本公开实施例的信息处理方法的流程图一，如图 4 所示，该流程包括如下步骤:

步骤 S402，接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识;

步骤 S404，向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文;

步骤 S406，根据获取的用户安全上下文，对用户设备进行鉴权认证。

通过上述步骤，通过切片选择功能实体标识从切片选择功能实体中获取用户安全上下文，对用户设备进行鉴权认证，解决了相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题，降低了信令负荷、减少了用户数据中心的处理负荷。

可选地，在鉴权认证结果为用户设备合法的情况下，该方法还可以包括：为用户设备分配用于标识用户设备的第一标识信息；向用户设备发送附着响应消息，其中，附着响应消息携带有第一标识信息。通过为用户分

配用户标识用户设备的第一标识信息，可以使用该标识信息代替原有消息中使用的用户码，可以对用户码起到保护作用。

可选地，在向用户设备发送附着响应消息之后，还可以在用户进行重注册的过程中，使用上述分配的第一标识信息进行重注册流程。例如，可以接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第一标识信息；根据第一标识信息，获取本地保存的用户设备对应的用户安全上下文；根据获取的用户安全上下文，对用户设备进行鉴权认证。

可选地，在向用户设备发送附着响应消息之后，还可以根据第一标识信息向其他预设网元发送本地保存的用户设备对应的用户安全上下文。例如，可以接收预设网元发送的用于获取用户设备的用户安全上下文的预设消息，其中，预设消息中携带有第一标识信息，根据第一标识信息，获取本地保存的用户设备对应的用户安全上下文，将获取的安全上下文发送给预设网元。通过上述方式，可以在预设场景下（例如，预设网络需要安全上下文的场景）为预设网元提供用户设备对应的用户安全上下文。通常情况下，通用网络功能实体之间的交互代价远小于通用网络功能实体与用户数据中心的交互代价，通过方式为预设网元提供用户安全上下文，可以减少需要的网络资源开销。

可选地，可以通过多种方式获取用户设备的用户签约数据，例如，可以从用户数据中心获取用户签约数据，又例如，还可以在根据获取的用户安全上下文，对用户设备进行鉴权认证的过程中，向切片选择功能实体获取用户设备的用户签约数据。再例如，还可以在根据对用户设备进行鉴权认证，确定用户设备合法以后，向切片选择功能实体获取用户设备的用户签约数据。

在本实施例中还提供了一种运行于移动性管理实体的信息处理方法，该移动性管理实体的结构如图 3 所示。图 5 是根据本公开实施例的信息处理方法的流程图二，如图 5 所示，该流程包括如下步骤：

步骤 S502，接收用于用户设备附着到网络的第一附着请求消息，其

中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识；

步骤 S504，向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文；

步骤 S506，将获取的安全上下文发送给鉴权认证实体，其中，安全上下文用于鉴权认证实体对用户设备进行鉴权认证。

通过上述步骤，通过切片选择功能实体标识从切片选择功能实体中获取用户安全上下文，将获取的用户安全上下文发送至鉴权认证实体，用于所述鉴权认证实体对用户设备进行鉴权认证，解决了相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题，降低了信令负荷、减少了用户数据中心的处理负荷。

可选地，在将获取的安全上下文发送给鉴权认证实体之后，还可以包括：接收鉴权认证实体发送的第一附着响应消息；为用户设备分配用于标识用户设备的第二标识信息；向用户设备发送第二附着响应消息，其中，第二附着响应消息携带有第二标识信息。

可选地，在向用户设备发送第二附着响应消息之后，还可以包括：接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第二标识信息；根据第二标识信息，获取本地保存的用户设备对应的安全上下文；将获取的安全上下文发送给鉴权认证实体。

可选地，在向用户设备发送第二附着响应消息之后，还可以包括：接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第二标识信息；根据第二标识信息，获取本地保存的用户设备对应的安全上下文；将获取的安全上下文发送给预设网元。

可选地，在将获取的安全上下文发送给鉴权认证实体之后，还可以包括：向切片选择功能实体获取用户设备的用户签约数据。

基于上述实施例及优选实施方式，为说明方案的整个流程交互，在本优选实施例中，提供了一种用户安全上下文传递方法，该方法包括：切片

选择功能实体从用户数据中心获取用户安全上下文后，实现对用户设备的双向认证，并为用户设备选择合适的切片；切片通过切片选择功能实体标识向切片选择功能实体获取用户安全上下文，完成切片对用户设备的认证。

切片通过切片选择功能实体标识向切片选择功能实体获取用户安全上下文可以为切片鉴权认证实体（作用与前述鉴权认证实体的功能类似）和/或切片移动性管理实体（作用与前述移动性管理实体的功能类似）通过切片选择功能实体标识向切片选择功能实体获取用户安全上下文。

可选地，切片鉴权认证实体还可以根据切片选择功能实体标识向切片选择功能实体获取用户安全上下文和用户签约数据。

可选地，切片移动性管理实体还可以根据切片选择功能实体标识向切片选择功能实体获取用户签约数据。

可选地，切片鉴权认证实体可以向切片移动性管理实体发送用户签约数据。

可选地，切片选择功能实体可以向切片移动性管理实体、或切片鉴权认证实体发送切片选择功能实体标识。

可选地，无线接入网络向用户设备回送切片选择功能实体标识、或者切片标识，或者切片移动性管理标识，或者切片鉴权管理标识。

可选地，切片选择功能实体标识、或者切片标识，或者切片移动性管理标识，或者切片鉴权管理标识可以为各实体为用户设备分配临时标识。

可选地，临时标识可以包括所述实体的公共标识信息。

本优选实施例还提供了一种用户安全上下文传递系统，相对于现有系统，增加切片选择功能实体与切片通用网络功能实体或者切片控制面功能实体接口，用于用户设备初始注册或者重注册中切片选择功能实体向切片通用网络功能实体或者切片控制面功能实体发送用户安全上下文或者用户签约数据。

下面结合附图对本公开优选实施例的方法进行详细说明。

图 6 是根据本公开优选实施例的网络切片的架构示意图，如图 6 所示，相对于现有的架构，增加切片选择功能实体与切片通用网络功能实体或者切片控制面功能实体接口，用于用户设备初始注册或者重注册中切片选择功能实体向切片通用网络功能实体或者切片控制面功能实体发送用户安全上下文或者用户签约数据。

图 7 是根据本公开优选实施例的用户设备接入网络选择合适的切片的初始注册和重注册的流程示意图。在该流程中，切片选择功能实体从用户数据中心获取用户安全上下文后，实现对用户设备的双向认证，并为用户设备选择合适的切片，切片通过切片选择功能实体标识向切片选择功能实体获取用户安全上下文，完成切片对用户设备的认证。如图 7 所示，该流程包括如下步骤:

步骤 S702，用户设备向无线接入网络发送初始的附着请求消息，无线接入网络向切片选择功能实体转发该附着请求消息，该消息携带用户标识。

步骤 S704,，切片选择功能实体根据用户标识从用户数据中心获取用户签约信息和安全上下文，对用户和网络进行相互认证，该认证过程包括:切片选择功能实体向用户数据中心发送鉴权认证请求消息，用户数据中心向切片选择功能实体回送鉴权认证请求响应消息，该消息携带用户安全上下文，即安全向量组，切片选择功能实体向用户设备发送用户鉴权认证请求消息，该消息携带认证令牌，用户设备通过认证令牌验证网络的合法性，并计算出期望的响应值，向切片选择功能实体回送用户鉴权认证请求响应消息，该携带期望的响应值，切片选择功能实体将安全上下文中的期望的响应值和收到的期望的响应值比对，如果相等，认证用户设备合法，向用户数据中心获取用户签约数据，切片选择功能实体保存安全上下文和用户签约数据。

步骤 S706，切片选择功能实体根据用户签约数据中的信息选择合适

的切片，即切片选择功能实体选择合适的切片标识。

步骤 S708，切片选择功能实体向无线接入网络发送切片选择消息，该消息携带切片标识，该消息可以携带切片选择功能实体标识，该切片选择功能实体标识可以包含切片选择功能实体标识，也可以包括切片选择功能实体为用户设备分配的临时标识 1。

步骤 S710，无线接入网络根据对应的切片标识选择对应的切片。

步骤 S712a，无线接入网络向选择的切片的切片移动性管理实体发送附着请求消息，切片移动性管理实体选择合适的切片鉴权认证实体并向切片鉴权认证实体转发附着请求消息，该附着请求消息携带切片选择功能实体标识。

步骤 S712b，从切片选择功能实体获取用户签约数据信息，切片认证用户。

可以是切片移动性管理实体从切片选择功能实体获取用户签约数据信息，也可以是切片鉴权认证实体从切片选择功能实体获取用户签约数据信息。对于第一种情况，切片移动性管理实体根据切片选择功能实体标识向切片选择功能实体获取用户签约数据和用户安全上下文，保存用户签约数据，将用户安全上下文发送给切片鉴权认证实体。对于第二种情况，切片鉴权认证实体根据切片选择功能实体标识向切片选择功能实体获取用户安全上下文和/或用户签约数据。

切片鉴权认证实体根据用户安全上下文或者用签约数据认证用户是否能够合法接入切片，该鉴权认证过程包括：切片鉴权认证实体向用户设备发送用户鉴权认证请求消息，该消息携带认证令牌，用户设备通过认证令牌验证网络的合法性，并计算出期望的响应值，向切片鉴权认证实体回送用户鉴权认证请求响应消息，该携带期望的响应值，切片鉴权认证实体将用户安全上下文中的期望的响应值和收到的期望的响应值比对，如果相等，认证用户设备合法。在认证用户设备合法以后，如果在前述过程中切片鉴权认证实体并未获取用户签约数据，切片鉴权认证实体则可以向用户

数据中心获取用户签约数据。切片鉴权认证实体和切片移动性管理实体保存安全上下文和/或用户签约数据（保存的内容根据前述获取到的内容而定）。

切片移动性管理实体可以为用户设备分配切片移动性管理实体标识，该标识为用户临时标识 2，该临时标识 2 可以包括用于标识移动性管理实体的标识信息，还可以包括切片移动性管理实体为用户设备分配的标识信息（作用同前述第二标识信息）。切片鉴权认证实体可以为用户设备分配切片鉴权认证实体标识，该标识为用户临时标识 3，该临时标识 3 可以包括用于标识切片鉴权认证实体的标识信息，还可以包括切片鉴权认证实体为用户设备分配的标识信息（作用同前述第一标识信息）。

完成上述鉴权认证后，移动性管理实体还需向用户数据中心发起位置更新请求，用户数据中心保存移动性管理实体标识，向移动性管理实体回送位置更新请求响应。

步骤 S712c，同用户面网关建立用户面连接（可选步骤）。

步骤 S712d，切片鉴权认证实体认证成功后，向切片移动性管理实体回送附着响应消息，该消息可以携带用户临时标识 3，切片移动性管理实体向无线网络管理实体回送附着响应消息，该消息可以携带用户临时标识 3 和/或用户临时标识 2。

步骤 S714，无线接入网络向用户设备消息回送附着响应消息，该消息携带切片标识，和/或用户临时标识 1（或者切片选择功能实体标识），和/或用户临时标识 2，和/或用户临时标识 3。

步骤 S702 至 S714 完成用户设备的初始注册。

步骤 S716，用户设备向无线接入网络发起重注册请求消息，该消息可以携带有以下标识信息中的至少一种：切片标识，用户临时标识 1（或者切片选择功能实体标识），用户临时标识 2，用户临时标识 3。

步骤 S718，无线接入网络根据切片标识直接向切片管理实体转发重注册请求消息，该消息可以携带以下标识信息中的至少之一：用户临时标

识 1，用户临时标识 2，用户临时标识 3。

步骤 S720，按照步骤 S712-步骤 S714 完成重注册过程，其中步骤 S712b 中如果切片移动性管理实体或者切片鉴权认证能实体能能够根据用户临时标识 2 和/或用户临时标识 3，查找到用户签约数据或者用户安全上下文，则可以直接认证用户设备是否能够接入切片，否则，可以根据用户临时标识 1（或者切片选择功能实体标识）向切片选择功能实体用户签约数据或者用户安全上下文。

用户数据中心位于用户的归属域，一般不和网络切片在一个地方，在初始注册或者重注册的过程中需要多次到归属域获取用户安全上下文和用户签约数据，将增加信令负荷，而且一般来说用户数据中心管理的用户较多，这样将增加用户数据中心的处理负荷。通过本公开优选实施例的上述技术方案，通过增加切片选择功能实体与切片通用网络功能实体或者切片控制面功能实体接口，解决了在初始注册或者重注册中，多次向用户数据中心获取用户安全上下文或者用户签约数据的问题。

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，本公开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）执行本公开各个实施例所述的方法。

实施例 2

在本实施例中提供了一种信号处理装置，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是

可能并被构想的。

图 8 是根据本公开实施例的信号处理装置的结构框图一，如图 8 所示，该装置包括：

接收模块 82，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识；

获取模块 84，连接至上述接收模块 82，设置为向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文；

鉴权模块 86，连接至上述获取模块 84，设置为根据获取的用户安全上下文，对用户设备进行鉴权认证。

图 9 是根据本公开实施例的信号处理装置的结构框图二，如图 9 所示，该装置除包括图 8 所示的所有模块外，还包括：

分配模块 92，设置为在鉴权模块的鉴权认证结果为用户设备合法的情况下，为用户设备分配用于标识用户设备的第一标识信息；

发送模块 94，连接至上述分配模块 92，设置为向用户设备发送附着响应消息，其中，附着响应消息携带有第一标识信息。

可选地，接收模块 82，还可以设置为接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第一标识信息；获取模块 84，还可以设置为根据第一标识信息，获取本地保存的用户设备对应的安全上下文；鉴权模块 86，还可以设置为根据获取的安全上下文，对用户设备进行鉴权认证。

可选地，接收模块 82，还可以设置为接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第一标识信息；获取模块 84，还设置为根据第一标识信息，获取本地保存的用户设备对应的安全上下文；发送模块 94，还设置为将获取的安全上下文发送给预设网元。

可选地，获取模块 84，还可以设置为向切片选择功能实体获取用户设备的用户签约数据。

在本实施例中还提供了一种鉴权认证实体，图 10 是根据本公开实施例的鉴权认证实体的结构框图，如图 10 所述，上述鉴权认证实体包括图 8 或 9 中的数据处理装置 102。

在本实施例中还提供了数据处理方法，图 11 是根据本公开实施例的信号处理装置的结构框图三，如图 11 所示，该装置包括：

接收模块 112，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识；

获取模块 114，连接至上述接收模块 112，设置为向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文；

发送模块 116，连接至上述获取模块 114，设置为将获取的安全上下文发送给鉴权认证实体，其中，安全上下文用于鉴权认证实体对用户设备进行鉴权认证。

图 12 是根据本公开实施例的信号处理装置的结构框图四，如图 12 所示，该装置除包括图 11 所示的所有模块外，还包括：分配模块 122，其中，

接收模块 112，还设置为接收鉴权认证实体发送的第一附着响应消息；

分配模块 122，设置为为用户设备分配用于标识用户设备的第二标识信息；

发送模块 116，还设置为向用户设备发送第二附着响应消息，其中，第二附着响应消息携带有第二标识信息。

可选地，接收模块 112，还可以设置为接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第二标识信息；获取模块 114，还可以设置为根据第二标识信息，获取本地保存的用户设备对应的安全上下文；发送模块 116，还可以设置为将获取的安全上

下文发送给预设网元。

可选地，获取模块 114，还设置为向切片选择功能实体获取用户设备的用户签约数据。

在本实施例中还提供了一种移动性管理实体，图 13 是根据本公开实施例的移动性管理实体的结构框图，如图 13 所示，上述移动性管理实体包括图 11 或 12 中所示的数据处理装置 132。

需要说明的是，上述各个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述各个模块以任意组合的形式分别位于不同的处理器中。

实施例 3

在本实施例中提供了一种网络系统，图 14 是根据本公开实施例的网络系统的结构框图，如图 14 所示，该网络系统包括：切片选择功能实体 142、鉴权认证实体 144 和移动性管理实体 146，其中，切片选择功能实体 142 与鉴权认证实体 144 之间通过接口进行交互，鉴权认证实体 144 包括图 8 或图 9 所示的第一数据处理装置 1442，和/或，切片选择功能实体 142 与移动性管理实体 146 之间通过接口进行交互，移动性管理图 11 或图 12 所示的第二数据处理装置 1462。

实施例 4

本公开的实施例还提供了一种存储介质。该存储介质包括存储的程序，其中，上述程序运行时执行上述任一项所述的方法

可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码：

S1，接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识；

S2，向切片选择功能实体标识对应的切片选择功能实体获取用户设备

对应的用户安全上下文;

S3，根据获取的用户安全上下文，对用户设备进行鉴权认证。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在鉴权认证结果为用户设备合法的情况下，在根据获取的用户安全上下文，对用户设备进行鉴权认证之后，还包括:

S1，为用户设备分配用于标识用户设备的第一标识信息;

S2，向用户设备发送附着响应消息，其中，附着响应消息携带有第一标识信息。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在向用户设备发送附着响应消息之后，还包括:

S1，接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第一标识信息;

S2，根据第一标识信息，获取本地保存的用户设备对应的安全上下文;

S3，根据获取的安全上下文，对用户设备进行鉴权认证。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在向用户设备发送附着响应消息之后，还包括:

S1，接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第一标识信息;

S2，根据第一标识信息，获取本地保存的用户设备对应的安全上下文;

S3，将获取的安全上下文发送给预设网元。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在根据获取的用户安全上下文，对用户设备进行鉴权认证的过程中，还包括:

向切片选择功能实体获取用户设备的用户签约数据。

可选地，在本实施例中，上述存储介质可以包括但不限于: 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。

在本实施例中，处理器根据存储介质中已存储的程序代码执行：接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向切片选择实体标识对应的切片选择实体获取用户设备对应的用户安全上下文；根据获取的用户安全上下文，对用户设备进行鉴权认证。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在鉴权认证结果为用户设备合法的情况下，在根据获取的用户安全上下文，对用户设备进行鉴权认证之后，还包括：为用户设备分配用于标识用户设备的第一标识信息；向用户设备发送附着响应消息，其中，附着响应消息携带有第一标识信息。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在向用户设备发送附着响应消息之后，还包括：接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第一标识信息；根据第一标识信息，获取本地保存的用户设备对应的安全上下文；根据获取的安全上下文，对用户设备进行鉴权认证。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在向用户设备发送附着响应消息之后，还包括：接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第一标识信息；根据第一标识信息，获取本地保存的用户设备对应的安全上下文；将获取的安全上下文发送给预设网元。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在根据获取的用户安全上下文，对用户设备进行鉴权认证的过程中，还包括：向切片选择实体获取用户设备的用户签约数据。

可选地，本实施例中的可选示例可以参考上述实施例及可选实施方式

中所描述的示例，本实施例在此不再赘述。

实施例 5

本实施例提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码:

S1，接收用于用户设备附着到网络的第一附着请求消息，其中，第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识;

S2，向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文;

S3，将获取的安全上下文发送给鉴权认证实体，其中，安全上下文用于鉴权认证实体对用户设备进行鉴权认证。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在将获取的安全上下文发送给鉴权认证实体之后，还包括:

S1，接收鉴权认证实体发送的第一附着响应消息;

S2，为用户设备分配用于标识用户设备的第二标识信息;

S3，向用户设备发送第二附着响应消息，其中，第二附着响应消息携带有第二标识信息。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在向用户设备发送第二附着响应消息之后，还包括:

S1，接收用户设备发送的第二附着请求消息，其中，第二附着请求消息中携带有第二标识信息;

S2，根据第二标识信息，获取本地保存的用户设备对应的安全上下文;

S3，将获取的安全上下文发送给鉴权认证实体。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

在向用户设备发送第二附着响应消息之后，还包括:

S1，接收预设网元发送的用于获取用户设备的安全上下文的预设消息，其中，预设消息中携带有第二标识信息；

S2，根据第二标识信息，获取本地保存的用户设备对应的安全上下文；

S3，将获取的安全上下文发送给预设网元。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在将获取的安全上下文发送给鉴权认证实体之后，还包括：向切片选择功能实体获取用户设备的用户签约数据。

可选地，在本实施例中，上述存储介质可以包括但不限于：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。

在本实施例中，处理器根据存储介质中已存储的程序代码执行：接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择实体的切片选择实体标识；向所述切片选择实体标识对应的切片选择实体获取所述用户设备对应的用户安全上下文；将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：接收所述鉴权认证实体发送的第一附着响应消息；为所述用户设备分配用于标识所述用户设备的第二标识信息；向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在向所述用户设备发送所述第二附着响应消息之后，还包括：接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述鉴权

认证实体。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在向所述用户设备发送所述第二附着响应消息之后，还包括：接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息；根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文；将获取的所述安全上下文发送给所述预设网元。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：向所述切片选择实体获取所述用户设备的用户签约数据。

本公开的实施例还提供了一种处理器，该处理器用于运行程序，其中，该程序运行时执行上述任一项方法中的步骤。

可选地，本实施例中的可选示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

显然，本领域的技术人员应该明白，上述的本公开的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本公开不限制于任何特定的硬件和软件结合。

以上所述仅为本公开的优选实施例而已，并不用于限制本公开，对于本领域的技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

工业实用性

本公开的实施例，通过切片选择功能实体标识从切片选择功能实体中获取用户安全上下文，对用户设备进行鉴权认证，由于增加切片选择功能实体与切片通用网络功能实体或者切片控制面功能实体接口，减少了用户数据中心的处理负荷，因此，可以解决相关技术中用户的注册过程需要与用户数据中心多次交互，增加用户数据中心处理负荷的问题，达到降低信令负荷、减少用户数据中心处理负荷的效果。

权 利 要 求 书

1. 一种信息处理方法，包括:

接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识;

向所述切片选择功能实体标识对应的切片选择功能实体获取所述用户设备对应的用户安全上下文;

根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。

2. 根据权利要求 1 所述的方法，其中，在鉴权认证结果为所述用户设备合法的情况下，在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证之后，还包括:

为所述用户设备分配用于标识所述用户设备的第一标识信息;

向所述用户设备发送附着响应消息，其中，所述附着响应消息携带有所述第一标识信息。

3. 根据权利要求 2 所述的方法，其中，在向所述用户设备发送所述附着响应消息之后，还包括:

接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第一标识信息;

根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文;

根据获取的所述安全上下文，对所述用户设备进行鉴权认证。

4. 根据权利要求 2 所述的方法，其中，在向所述用户设备发送所述附着响应消息之后，还包括:

接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第一标识信息;

根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；

将获取的所述安全上下文发送给所述预设网元。

5. 根据权利要求 1 至 4 中任一项所述的方法，其中，在根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证的过程中，还包括：

向所述切片选择功能实体获取所述用户设备的用户签约数据。

6. 一种信息处理方法，包括：

接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识；

向所述切片选择功能实体标识对应的切片选择功能实体获取所述用户设备对应的用户安全上下文；

将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

7. 根据权利要求 6 所述的方法，其中，在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括：

接收所述鉴权认证实体发送的第一附着响应消息；

为所述用户设备分配用于标识所述用户设备的第二标识信息；

向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

8. 根据权利要求 7 所述的方法，其中，在向所述用户设备发送所述第二附着响应消息之后，还包括：

接收所述用户设备发送的第二附着请求消息，其中，所述第二附

着请求消息中携带有所述第二标识信息;

根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文;

将获取的所述安全上下文发送给所述鉴权认证实体。

9. 根据权利要求 7 所述的方法，其中，在向所述用户设备发送所述第二附着响应消息之后，还包括:

接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息;

根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文;

将获取的所述安全上下文发送给所述预设网元。

10. 根据权利要求 6 至 9 中任一项所述的方法，其中，在将获取的所述安全上下文发送给所述鉴权认证实体之后，还包括:

向所述切片选择功能实体获取所述用户设备的用户签约数据。

11. 一种信息处理装置，包括:

接收模块，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识;

获取模块，设置为向所述切片选择功能实体标识对应的切片选择功能实体获取所述用户设备对应的用户安全上下文;

鉴权模块，设置为根据获取的所述用户安全上下文，对所述用户设备进行鉴权认证。

12. 根据权利要求 11 所述的装置，其中，还包括:

分配模块，设置为在鉴权模块的鉴权认证结果为所述用户设备合

法的情况下，为所述用户设备分配用于标识所述用户设备的第一标识信息；

发送模块，设置为向所述用户设备发送附着响应消息，其中，所述附着响应消息携带有所述第一标识信息。

13. 根据权利要求 12 所述的装置，其中，

所述接收模块，还设置为接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第一标识信息；

所述获取模块，还设置为根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；

所述鉴权模块，还设置为根据获取的所述安全上下文，对所述用户设备进行鉴权认证。

14. 根据权利要求 12 所述的装置，其中，

所述接收模块，还设置为接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第一标识信息；

所述获取模块，还设置为根据所述第一标识信息，获取本地保存的所述用户设备对应的所述安全上下文；

所述发送模块，还设置为将获取的所述安全上下文发送给所述预设网元。

15. 根据权利要求 11 至 14 中任一项所述的装置，其中，

所述获取模块，还设置为向所述切片选择功能实体获取所述用户设备的用户签约数据。

16. 一种鉴权认证实体，包括：权利要求 11 至 15 中任一项所述的装置。

17. 一种信息处理装置，包括:

接收模块，设置为接收用于用户设备附着到网络的第一附着请求消息，其中，所述第一附着请求消息中携带有用于标识切片选择功能实体的切片选择功能实体标识;

获取模块，设置为向所述切片选择功能实体标识对应的切片选择功能实体获取所述用户设备对应的用户安全上下文;

发送模块，设置为将获取的所述安全上下文发送给鉴权认证实体，其中，所述安全上下文用于所述鉴权认证实体对所述用户设备进行鉴权认证。

18. 根据权利要求 17 所述的装置，其中，还包括: 分配模块，其中，

所述接收模块，还设置为接收所述鉴权认证实体发送的第一附着响应消息;

所述分配模块，设置为为所述用户设备分配用于标识所述用户设备的第二标识信息;

所述发送模块，还设置为向所述用户设备发送第二附着响应消息，其中，所述第二附着响应消息携带有所述第二标识信息。

19. 根据权利要求 18 所述的装置，其中，

所述接收模块，还设置为接收所述用户设备发送的第二附着请求消息，其中，所述第二附着请求消息中携带有所述第二标识信息;

所述获取模块，还设置为根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文;

所述发送模块，还设置为将获取的所述安全上下文发送给所述鉴权认证实体。

20. 根据权利要求 18 所述的装置，其中，

所述接收模块，还设置为接收预设网元发送的用于获取所述用户设备的安全上下文的预设消息，其中，所述预设消息中携带有所述第二标识信息;

所述获取模块，还设置为根据所述第二标识信息，获取本地保存的所述用户设备对应的所述安全上下文;

所述发送模块，还设置为将获取的所述安全上下文发送给所述预设网元。

21. 根据权利要求 17 至 20 中任一项所述的装置，其中，

所述获取模块，还设置为向所述切片选择功能实体获取所述用户设备的用户签约数据。

22. 一种移动性管理实体，包括：权利要求 17 至 21 中任一项所述的装置。

23. 一种网络系统，包括切片选择功能实体、鉴权认证实体和移动性管理实体，所述切片选择功能实体与所述鉴权认证实体之间通过接口进行交互，所述鉴权认证实体包括权利要求 11 至 15 中任一项所述的装置，和/或，所述切片选择功能实体与所述移动性管理实体之间通过接口进行交互，所述移动性管理实体包括权利要求 17 至 21 中任一项所述的装置。

24. 一种存储介质，所述存储介质包括存储的程序，其中，所述程序运行时执行权利要求 1 至 10 中任一项所述的方法。

25. 一种处理器，所述处理器用于运行程序，其中，所述程序运行时执行权利要求 1 至 10 中任一项所述的方法。

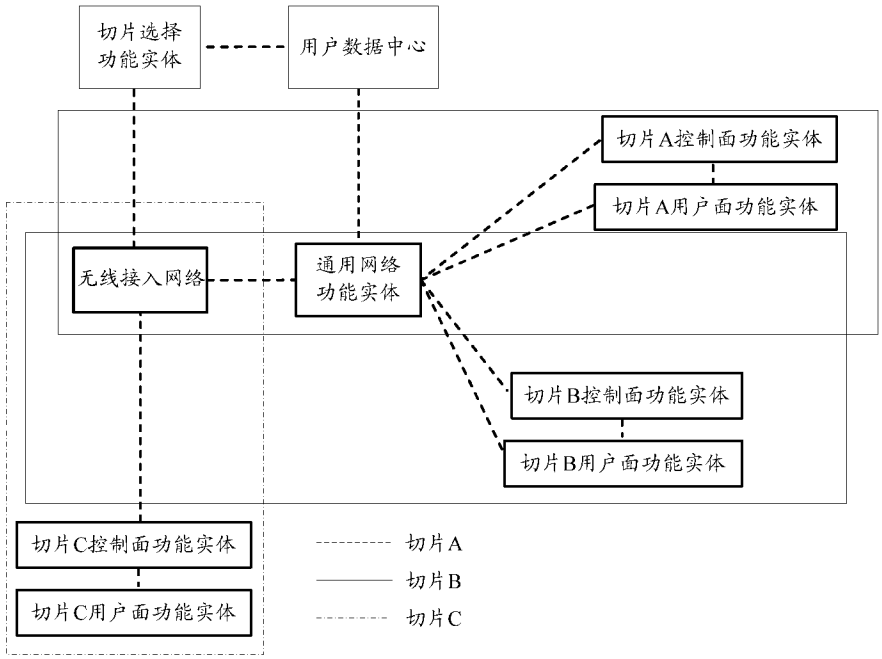
切片选择
功能实体
用户数据中心
切片A控制面功能实体
切片A用户面功能实体
无线接入网络
通用网络
功能实体
切片B控制面功能实体
切片B用户面功能实体
切片C控制面功能实体
切片C用户面功能实体
切片A
切片B
切片C

图 1

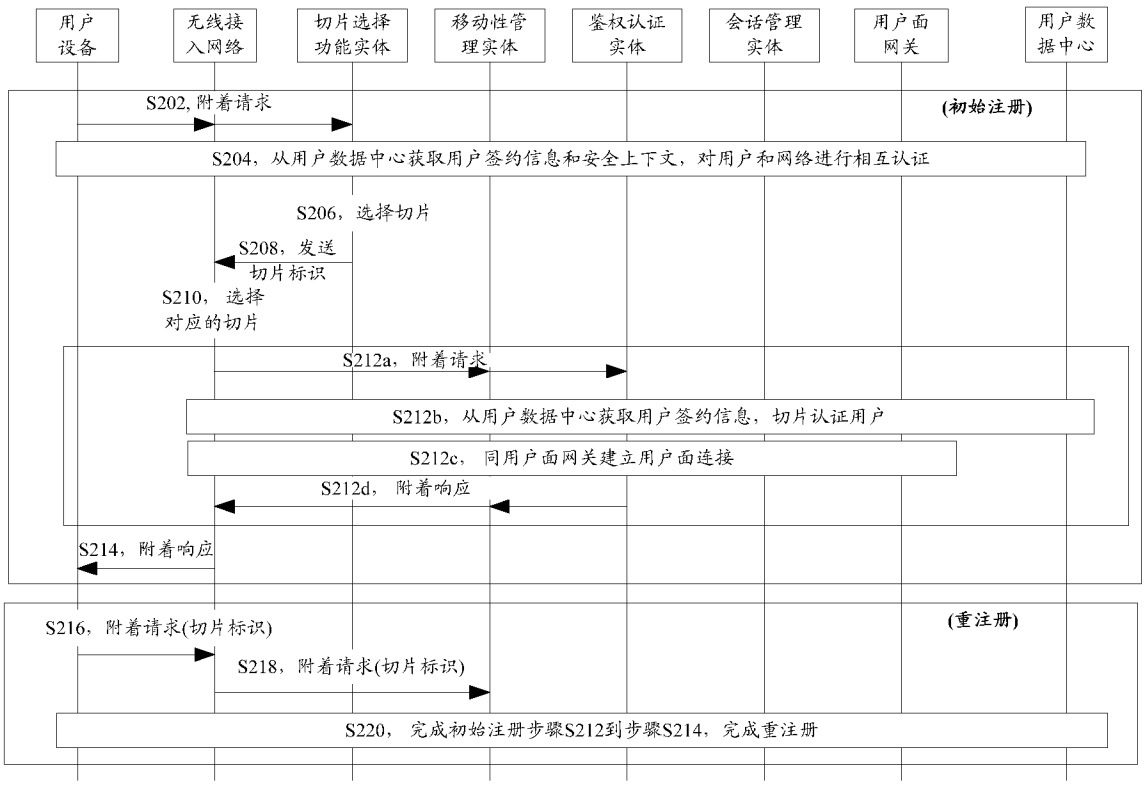
用户
设备
无线接
入网络
切片选择
功能实体
移动性管
理实体
鉴权认证
实体
会话管理
实体
用户面
网关
用户数
据中心
S202, 附着请求
(初始注册)
S204，从用户数据中心获取用户签约信息和安全上下文，对用户和网络进行相互认证
S206，选择切片
S208，发送
切片标识
S210， 选择
对应的切片
S212a，附着请求
S212b，从用户数据中心获取用户签约信息，切片认证用户
S212c， 同用户面网关建立用户面连接
S212d， 附着响应
S214，附着响应
S216，附着请求(切片标识)
(重注册)
S218，附着请求(切片标识)
S220， 完成初始注册步骤S212到步骤S214，完成重注册

图 2

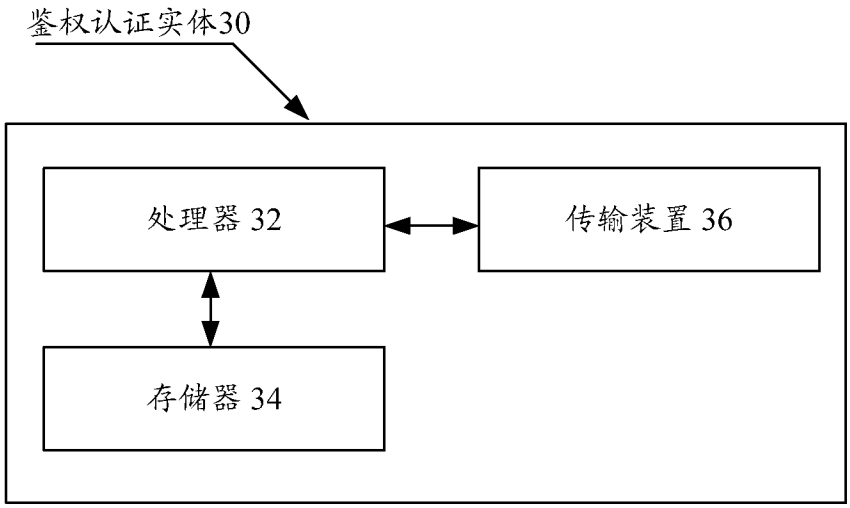

图 3

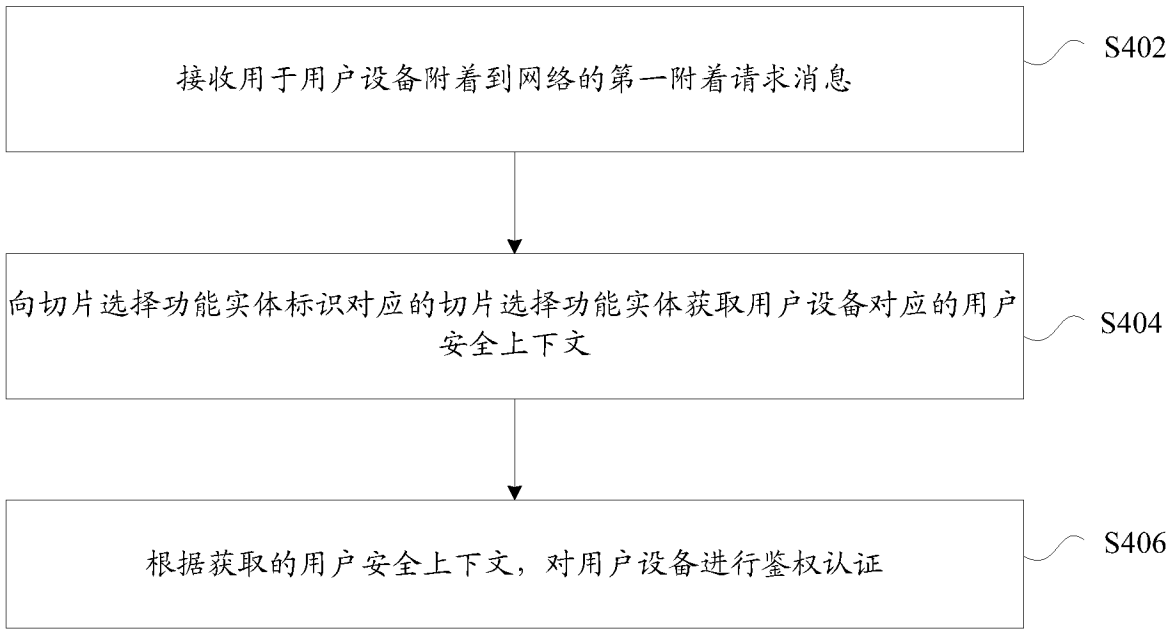
接收用于用户设备附着到网络的第一附着请求消息
S402
向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文
S404
根据获取的用户安全上下文，对用户设备进行鉴权认证
S406

图 4

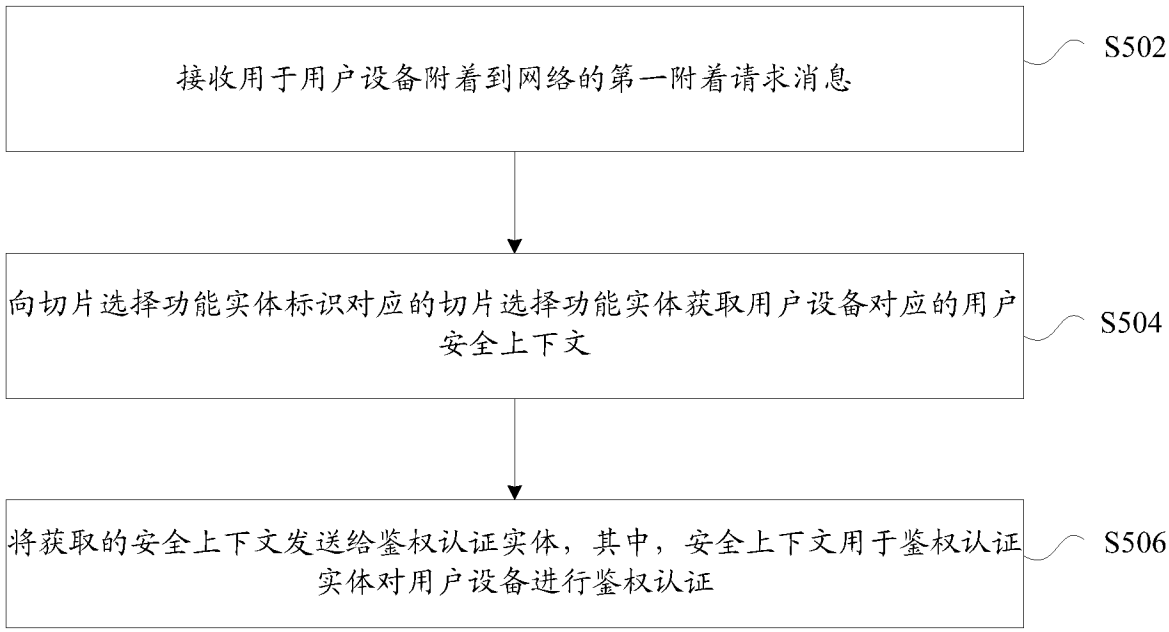
接收用于用户设备附着到网络的第一附着请求消息
S502
向切片选择功能实体标识对应的切片选择功能实体获取用户设备对应的用户安全上下文
S504
将获取的安全上下文发送给鉴权认证实体，其中，安全上下文用于鉴权认证实体对用户设备进行鉴权认证
S506

图 5

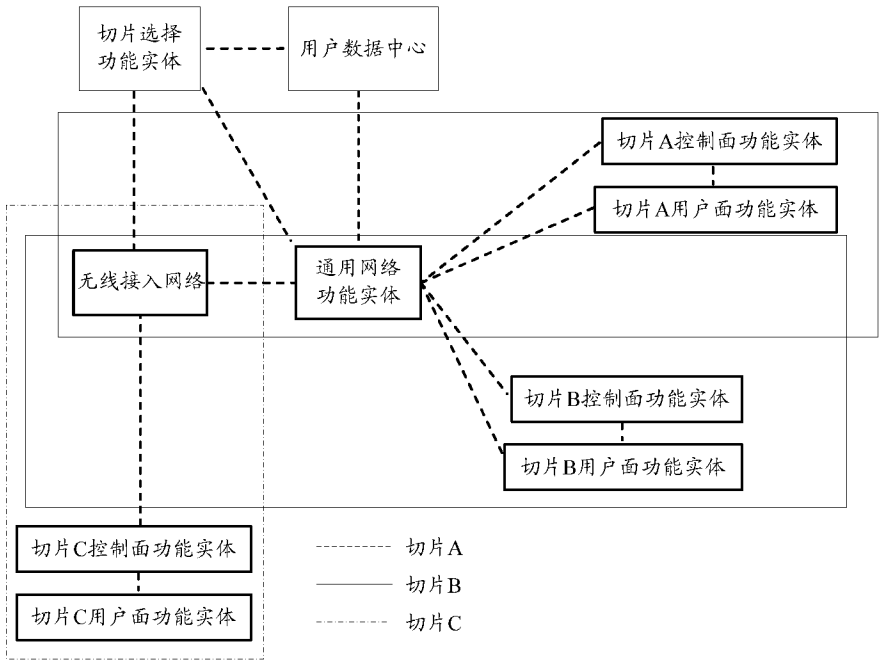
切片选择功能实体
用户数据中心
切片A控制面功能实体
切片A用户面功能实体
无线接入网络
通用网络功能实体
切片B控制面功能实体
切片B用户面功能实体
切片C控制面功能实体
切片C用户面功能实体
切片A
切片B
切片C

图 6

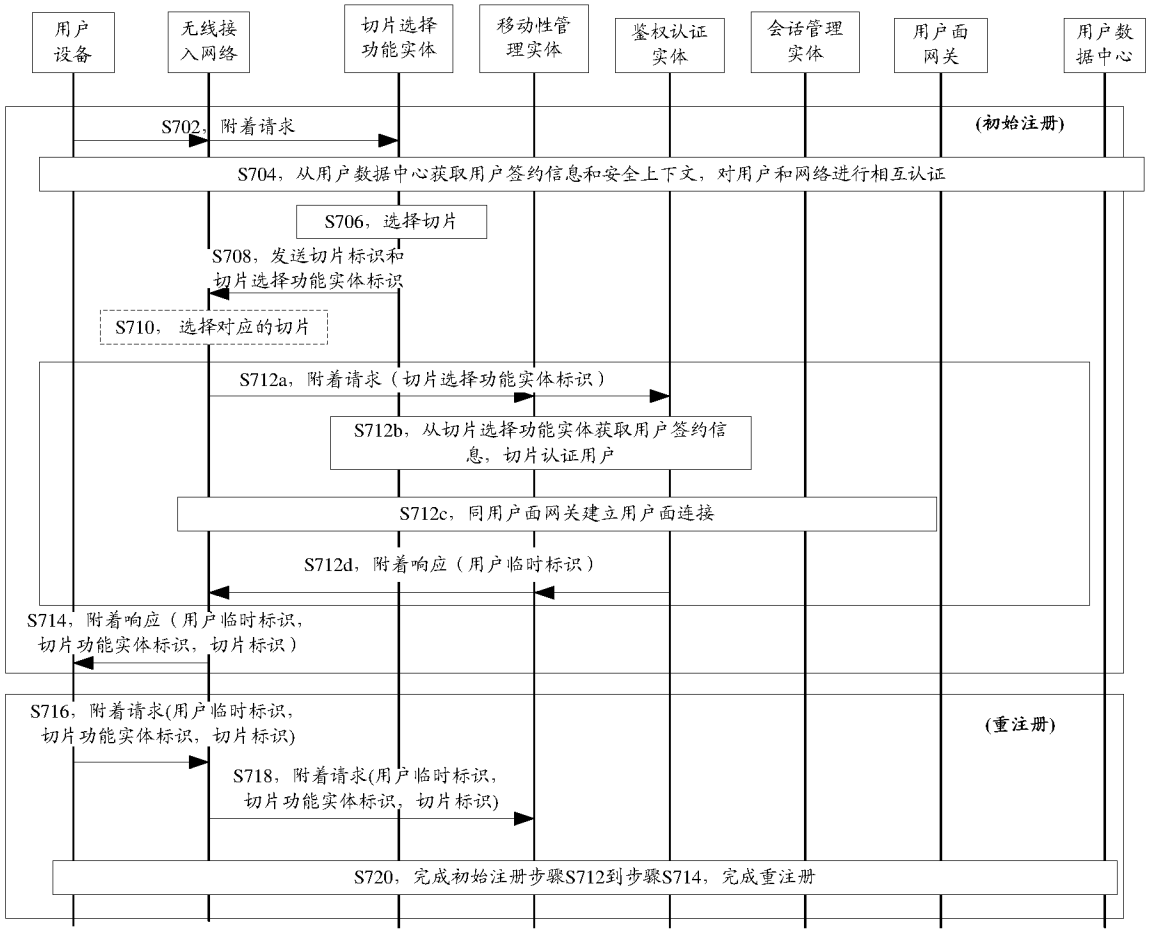
用户设备
无线接入网络
切片选择功能实体
移动性管理实体
鉴权认证实体
会话管理实体
用户面网关
用户数据中心
(初始注册)
S702，附着请求
S704，从用户数据中心获取用户签约信息和安全上下文，对用户和网络进行相互认证
S706，选择切片
S708，发送切片标识和切片选择功能实体标识
S710，选择对应的切片
S712a，附着请求（切片选择功能实体标识）
S712b，从切片选择功能实体获取用户签约信息，切片认证用户
S712c，同用户面网关建立用户面连接
S712d，附着响应（用户临时标识）
S714，附着响应（用户临时标识，切片功能实体标识，切片标识）
S716，附着请求(用户临时标识，切片功能实体标识，切片标识)
(重注册)
S718，附着请求(用户临时标识，切片功能实体标识，切片标识)
S720，完成初始注册步骤S712到步骤S714，完成重注册

图 7

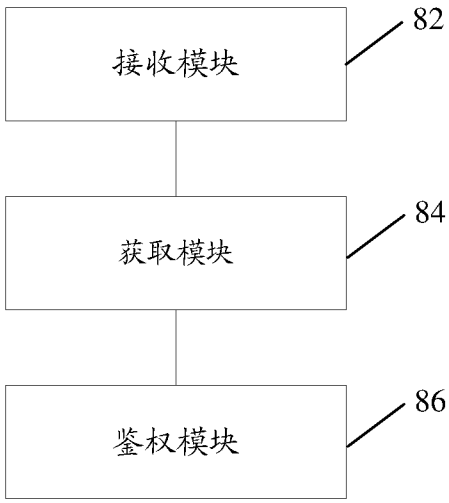
接收模块
82
获取模块
84
鉴权模块
86

图 8

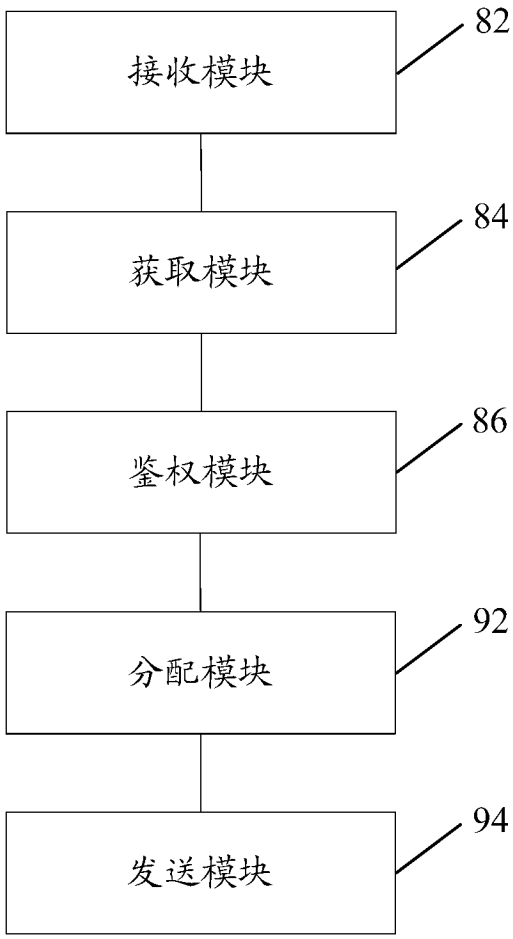

图 9

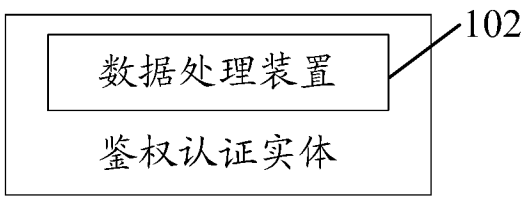

图 10

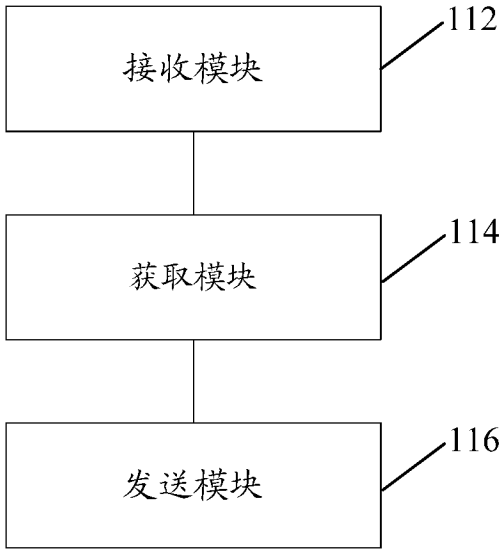
接收模块
112
获取模块
114
发送模块
116

图 11

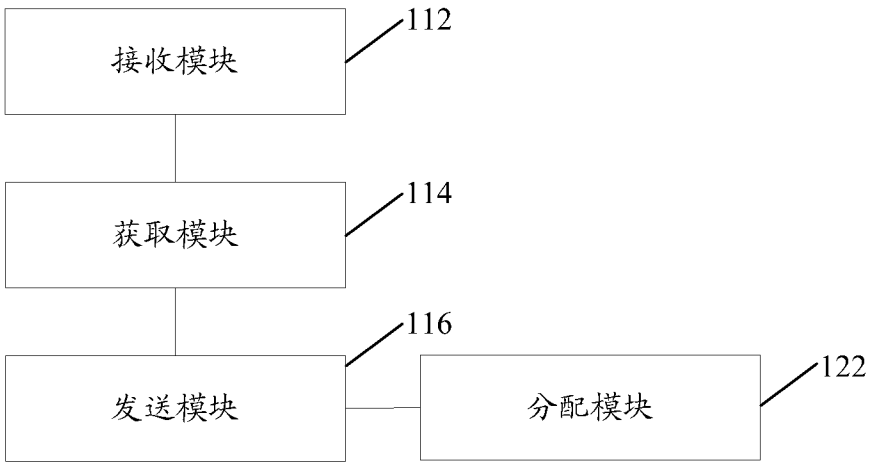
接收模块
112
获取模块
114
发送模块
116
分配模块
122

图 12

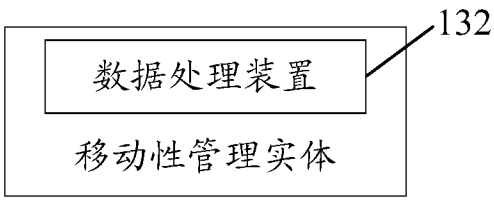
数据处理装置
132
移动性管理实体

图 13

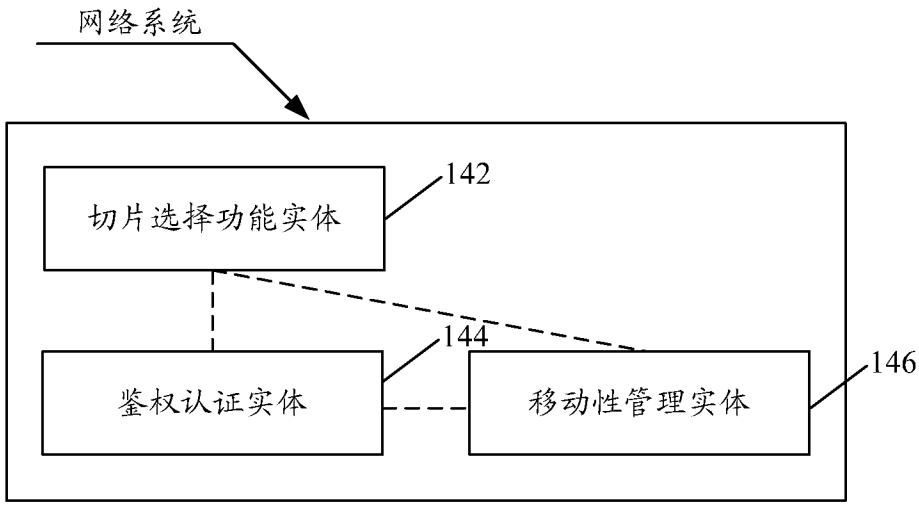

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/100915

A. CLASSIFICATION OF SUBJECT MATTER

H04W 8/26 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; CNKI; 3GPP: 切片, 选择, 认证, 鉴权, 网络功能虚拟化, 附着, 安全, 上下文, slice, function, selection, nfv, authentication, authorize, attach, security, context

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105900518 A (HUAWEI TECHNOLOGIES CO., LTD.), 24 August 2016 (24.08.2016), entire document	1-25
A	QUALCOMM INCORPORATED., "Solution Forkey Issue 1 on Network Slicing: Network Slice and Network Functions Selection Based on Evolved eDECOR Model", SA WG2 Meeting #115 S2-162339, 27 May 2016 (27.05.2016), page 5	1-25
A	HUAWEI et al., "Common Network Functions for Network Slicing", SA WG2 Meeting #116BIS S2-164510, 02 September 2016 (02.09.2016), entire document	1-25
A	"Study on Architecture for Next Generation System (Release 14)", 3GPP TR23.799 v0.7.0, 31 August 2016 (31.08.2016), entire document	1-25
A	SO, Tricci 等. "支持多业务的网络切片技术研究", 邮电设计技术, 31 July 2016 (31.07.2016), entire document (TRICCI, S. et al., "Research on Network Slicing Technology Supporting Multi-Service", Designing Techniques of Posts and Telecommunications)	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 November 2017	01 December 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIAO, Jiajia Telephone No. (86-10) 62413304

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/100915

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105900518 A	24 August 2016	WO 2015031512 A1	05 March 2015
		US 2015063166 A1	05 March 2015
		EP 3028528 A1	08 June 2016

国际检索报告

国际申请号
PCT/CN2017/100915

A. 主题的分类

H04W 8/26(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT; WPI; EPODOC; CNKI; 3GPP: 切片，选择，认证，鉴权，网络功能虚拟化，附着，安全，上下文，slice, function, selection, nfv, authentication, authorize, attach, security, context

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 105900518 A (华为技术有限公司) 2016年 8月 24日 (2016-08-24) 全文	1-25
A	QUALCOMM INCORPORATED. "Solution forkey issue 1 on Network Slicing: Network Slice and Network Functions Selection based on evolved eDECOR model" SA WG2 Meeting #115 S2-162339, 2016年 5月 27日 (2016-05-27), 第5页	1-25
A	HUAWEI等. "Common Network Functions for Network Slicing" SA WG2 Meeting #116BIS S2-164510, 2016年 9月 2日 (2016-09-02), 全文	1-25
A	"Study on Architecture for Next Generation System (Release 14)" 3GPP TR23.799 v0.7.0, 2016年 8月 31日 (2016-08-31), 全文	1-25
A	SO, Tricci等. "支持多业务的网络切片技术研究" 邮电设计技术, 2016年 7月 31日 (2016-07-31), 全文	1-25

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 11月 10日	2017年 12月 1日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	廖佳佳
传真号 (86-10)62019451	电话号码 (86-10)62413304

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/100915

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	105900518	A	2016年 8月 24日	WO	2015031512	A1	2015年 3月 5日
				US	2015063166	A1	2015年 3月 5日
				EP	3028528	A1	2016年 6月 8日