

WO 2018/126534 A1

(81) 指定国(除另有指明, 要求每一种可提供的国家保护¹⁾): 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,

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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 associated relationship between the remote device and the relay device and, after determining that the verification of the associated relationship is successful, sends to the base station an initial context establishment request message. The present technical solution uses the mobile management entity of the remote device to perform authorisation verification of the remote device and the relay device, reducing network configuration demands, reducing network overheads, and improving verification efficiency.

(57) 摘要: 本申请实施例提供一种授权验证方法和装置。其中, 该方法包括: 中继设备根据远端设备发送的通信请求生成第一无线资源控制消息并将其发送给基站, 基站根据该第一无线资源控制消息识别出远端设备请求通过中继设备接入网络, 以及通过初始设备消息将获取到的中继设备的标识和远端设备的非接入层消息发送给远端设备的移动管理实体, 远端设备的移动管理实体接收并根据该初始设备消息触发对远端设备和中继设备的关联关系的验证, 且在判断所述关联关系验证通过后, 向基站发送初始上下文建立请求消息。该技术方案利用远端设备的移动管理实体对远端设备和中继设备进行授权验证, 降低了网络配置需求、减少了网络开销、提高了验证效率。

授权验证方法和装置

技术领域

5 本申请涉及无线通信技术领域，尤其涉及一种授权验证方法和装置。

背景技术

在演进分组系统（Evolved Packet System，简称 EPS）中，可穿戴设备等远端设备通过中继设备连接到网络中，从而达到降低远端设备功耗的目的。在远端设备通过中继设备连接到网络中时，远端设备需要用到中继设备的无线承载，故网络上需要完成远端设备与
10 中继设备之间数据承载关系的映射，因此，需要网络来验证远端设备和中继设备的合法性以及远端设备和中继设备的关联关系。

现有技术中，当中继设备是层 3 中继时，网络中没有存储远端设备的上下文关系，基站与网络之间不存在远端设备的数据通道，此时基站与网络通过中继设备的数据通道对远端设备的数据进行传输。此时，网络通过如下方式实现远端设备和中继设备之间关联关系的验证。具体的，首先，远端设备从短距离功能实体（Proximity Service Function，简称 PF）获取中继发现参数和密钥管理功能实体（ProSe key Management Function，简称 PKMF）的地址，然后根据 PKMF 地址从 PKMF 获取发现安全参数，以及向 PKMF 发送密钥请求以获取用于中继通信的根密钥；其次，中继设备从 PF 获取中继发现参数和 PKMF 的地址，
15 并从 PKMF 获取发现安全参数；进而如果远端设备需要通过中继设备接入网络，则远端设备与中继设备基于从 PF 获取的参数进行发现过程；然后，在成功完成发现过程后，远端设备向中继设备发送通信请求，从而触发中继设备向 PKMF 中继发送授权和密钥请求，PKMF 对远端设备是否允许通过中继设备接入网络进行授权检查并生成短距离通信密钥，并向中继设备反馈包含通信密钥、密钥生成参数等内容的密钥响应。中继设备将密钥生成参数转发给远端设备，远端设备根据密钥生成参数生成通信密钥，若远端设备侧生成的通信密钥与中继设备接收到的通信密钥一致则表明认证和授权检查通过，从而远端设备可通过
20 中继设备连接到网络。

然而，远端设备也可通过层 2 中继连接到网络，由于层 2 中继的协议栈结构与层 3 中继的不同，当中继设备选用层 2 中继时，基站与核心网络上为远端设备建立了相应的上下文信息以及远端设备的数据通道，此时若仍然采用层 3 中继对应的授权验证方法来验证远端设备与中继设备之间的关联关系，会要求执行上述层 3 方案的复杂繁琐的参数配置流程和授权检查流程，使得整个认证和授权过程的网络配置需求高、网络开销大、验证效率低。
30

发明内容

35 本申请实施例提供一种授权验证方法和装置，以解决远端设备和中继设备之间的关联关系认证和授权过程网络配置需求高、网络开销大、验证效率低的问题。

本申请实施例第一方面提供一种授权验证方法，该方法是从中继设备的移动管理实体的角度描述，该方法包括：中继设备的移动管理实体接收中继设备发送的包括远端设

备的标识的第一请求消息，并根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证，以及在判断该关联关系验证通过后，生成第一响应消息，将该第一响应消息发送给中继设备，其中，根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：向远端设备的移动管理实体发送包括远端设备的标识的第二请求消息，
5 并接收远端设备的移动管理实体根据第二请求消息对远端设备进行安全处理后发送的第二响应消息。

该方法针对层 2 中继设备，设计了一套远端设备与中继设备的关联关系验证方案，在中继设备的移动管理实体侧根据从中继设备发送来的第一请求消息触发对远端设备和中继设备的关联关系的验证，可选的，可以在中继设备的移动管理实体侧实现关联关系
10 验证，也可以在远端设备的移动管理实体侧实现关联关系验证，这样能够避免现有层 3 中继方案中所需执行的复杂繁琐的参数配置流程和授权检查流程，使得本申请的层 2 解决方案与现有层 3 解决方案相比，降低了网络配置需求、减少了网络开销、提高了验证效率。

可选的，所述中继设备的移动管理实体根据所述第一请求消息，触发对所述远端设备
15 和所述中继设备的关联关系的验证，还包括：中继设备的移动管理实体根据所述第一请求消息获取第一授权信息，并根据远端设备的标识、中继设备的标识以及该第一授权信息，验证是否允许远端设备通过中继设备接入网络。可选的，当中继设备的移动管理实体自身来验证远端设备和中继设备的关联关系时，其需要首先获取中继设备的上下文，从上下文中获取与该中继设备有授权关系的远端设备列表，即第一授权信息，进而
20 实现关联关系的验证。当中继设备的移动管理实体获知远端设备的标识、中继设备的标识以及上述第一授权信息后，判断该第一授权信息中是否包含中继设备与远端设备的关联关系，当该第一授权信息中包含中继设备与远端设备的关联关系时，表明允许该远端设备通过该中继设备接入网络，否则，不允许该远端设备通过该中继设备接入网络。

可选的，所述中继设备的移动管理实体根据所述第一请求消息获取第一授权信息，
25 包括：在所述中继设备成功注册到网络之后，根据所述中继设备的标识从用户数据管理实体和/或近距离功能实体获取所述第一授权信息。也即，在中继设备成功注册到网络之后，网络中用户数据管理实体和/或近距离功能实体中均存储有中继设备的与远端设备相关的第一授权信息。对于用户数据管理实体中的中继设备与远端设备相关的第一授权信息，中继设备的移动管理实体直接从用户数据管理实体获取上述第一授权信息。而对于
30 中继设备的移动管理实体从近距离功能实体获取该第一授权信息的方式，可以为：当中继设备的移动管理实体可直接与近距离功能实体通信时，即两者之间存在直接接口，中继设备的移动管理实体直接从近距离功能实体获取上述第一授权信息；而当中继设备的移动管理实体不能直接与近距离功能实体通信时，即两者之间不存在直接接口，则近距离功能实体通过 HSS 将上述第一授权信息发送给中继设备的移动管理实体。

35 可选的，若第一请求消息，还包括：中继服务码；则中继设备的移动管理实体根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：中继设备的移动管理实体根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息，验证是否允许远端设备通过中继设备接入网络。

当远端设备发送给中继设备的通信请求中还包括中继服务码时，中继设备整合生成

的第一请求消息中也包括中继服务码，该中继服务码用于表征远端设备要请求的业务类型，不同的中继服务码对应不同的业务类型，因此，中继设备的移动管理实体验证远端设备与中继设备的关联关系时，还依据中继服务码，此时的第一授权信息为中继设备有授权关系的远端设备以及对应的中继服务码的关系列表。

5 可选的，本申请的授权验证方法，还包括：中继设备的移动管理实体向近距离功能实体发送包括远端设备的标识、中继设备的标识的第三请求消息，以使近距离功能实体根据第三请求消息验证是否允许远端设备通过中继设备接入网络。作为一种示例，关于终端设备的移动管理实体触发对远端设备和中继设备的关联关系验证的实现方式，除了中继设备的移动管理实体可自身进行验证、以及向远端设备的移动管理实体发送第二请求消息，以使该远端设备的移动管理实体验证外，中继设备的移动管理实体还可向近距离功能实体发送第三请求消息，以使该近距离功能实体进行验证。

可选的，本申请的授权验证方法，还包括：中继设备的移动管理实体接收远端设备的移动管理实体发送的密钥和生成该密钥所需的安全参数，并将该密钥和生成密钥所需的安全参数发送给所述中继设备。

15 远端设备想要通过中继设备接入到网络中，远端设备和中继设备需要具有保护两者之间通信的密钥，所以，中继设备的移动管理实体还需要接收远端设备的移动管理实体发送的密钥和生成该密钥所需的安全参数，并将其发送给中继设备，以使中继设备持有该密钥和生成该密钥的所需的安全参数。

20 可选的，当中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体对远端设备和中继设备关联关系的验证通过时，但中继设备的移动管理实体接收到的第二响应消息中未携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，那么中继设备的移动管理实体向安全功能实体发送密钥请求消息，安全功能实体则根据该密钥请求消息中远端设备的标识，查找并获取用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数，以及将该密钥和生成密钥所需的安全参数反馈给中继设备的移动管理实体，最后中继设备的移动管理实体再将密钥和生成该密钥所需的安全参数反馈给中继设备，以使中继设备对该密钥和安全参数进行相应处理。

30 这样，即使中继设备的移动管理实体生成的第一响应消息中未携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，中继设备也能获取到用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数，从而保证远端设备可通过该中继设备接入网络

35 可选的，在第一请求消息还包括：远端设备的非接入层消息、非接入层消息的校验码时，第二请求消息还包括：远端设备的非接入层消息、非接入层消息的校验码。此时，远端设备的移动管理实体还可对远端设备的非接入层消息进行验证，具体的是根据远端设备的非接入层上下文信息对远端设备的非接入层消息的校验码进行验证。

本申请实施例第二方面提供一种授权验证方法，该方法是从远端设备的移动管理实体的角度描述，该方法包括：远端设备的移动管理实体接收中继设备的移动管理实体发送的包括远端设备的标识的第二请求消息，并根据第二请求消息对远端设备进行安全处理，以及在远端设备进行安全处理后，向中继设备的移动管理实体发送的第二响应消

息。

作为一种示例，在中继设备的移动管理实体触发对远端设备和中继设备的关联关系的验证时，该远端设备的移动管理实体可接收中继设备的移动管理实体发送的第二请求消息，并根据第二请求消息对远端设备进行安全处理或者对远端设备与中继设备的关联关系进行进一步验证处理，以及根据安全处理的结果生成第二响应消息，并将该第二响应消息反馈给中继设备的移动管理实体。通过远端设备的移动管理实体对授权关系进行验证，降低了网络配置需求，减少了网络开销、提高了验证效率。

可选的，远端设备的移动管理实体根据第二请求消息对远端设备进行安全处理，包括：远端设备的移动管理实体根据第二请求消息获取第二授权信息，根据远端设备的标识、中继设备的标识以及第二授权信息，验证是否允许远端设备通过中继设备接入网络。可选的，远端设备的移动管理实体根据第二请求消息获取第二授权信息，包括：所述远端设备的移动管理实体在所述远端设备成功注册到网络之后，根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述第二授权信息；该远端设备再根据第二请求消息中的远端设备标识，查找并获取其上下文信息中的第二授权信息。

远端设备的移动管理实体在远端设备成功注册到网络之后，网络中用户数据管理实体和/或近距离功能实体中存储有远端设备与中继设备相关的第二授权信息，便可根据远端设备的标识从用户数据管理实体和/或近距离功能实体获取第二授权信息，进而可根据远端设备的标识、中继设备的标识以及获取的第二授权信息，判断该第二授权信息中是否包含远端设备与中继设备的关联关系。当第二授权信息中包含远端设备与中继设备的关联关系时，表明允许该远端设备通过该中继设备接入网络，否则，不允许该远端设备通过该中继设备接入网络。可选地，第二授权信息为与远端设备有授权关系的中继设备的列表。

可选的，若第二请求消息，还包括：中继服务码；则远端设备的移动管理实体根据第二请求消息对所述远端设备进行安全处理，包括：远端设备的移动管理实体根据所述远端设备的标识、所述中继设备的标识、所述中继服务码以及所述第二授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。此时，第二授权信息为与远端设备有授权关系的中继设备以及对应的中继服务码的关系列表。这样远端设备的移动管理实体在判定远端设备和中继设备的关联关系时，在判定条件中增加了中继服务码，即增加了远端设备请求业务的业务类型，判定结果更准确。

可选的，远端设备的移动管理实体根据第二请求消息对远端设备进行安全处理，包括：远端设备的移动管理实体根据第二请求消息中的远端设备的标识，获取远端设备的非接入层上下文信息，并根据非接入层上下文信息对远端设备的非接入层消息的校验码进行验证，此时第二请求消息包括：远端设备的非接入层消息、非接入层消息的校验码以及远端设备的标识。

在本实施例中，在第一请求消息还包括：远端设备的非接入层消息、非接入层消息的校验码时，第二请求消息中也包括：远端设备的非接入层消息、非接入层消息的校验码。此时，远端设备的移动管理实体还可对远端设备的非接入层消息进行验证，具体的是根据远端设备的非接入层上下文信息对远端设备的非接入层消息的校验码进行验证，这样通过检查非接入层消息的完整性从而完成远端设备和中继设备的安全认证。

可选的，所述授权验证方法，还包括：远端设备的移动管理实体根据第二请求消息中远端设备的标识，获取远端设备的非接入层上下文信息，根据所述非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥，将该密钥和生成所述密钥所需的安全参数发送给中继设备的移动管理实体。

5 在本实施例中，为了保证远端设备与中继设备的通信安全，远端设备的移动管理实体根据需要通信的远端设备的标识获取该远端设备的非接入层上下文消息，该非接入层上下文消息中存储有生成密钥所需的安全参数。此外，由于远端设备的移动管理实体与中继设备之间一般不直接通信，所以，当远端设备的移动管理实体中生成用于保护远端设备和中继设备之间通信安全的密钥之后，需要将该密钥和生成密钥所需的安全参数发
10 送给中继设备的移动管理实体，进而使其发送给中继设备。

可选的，所述授权验证方法，还包括：远端设备的移动管理实体向安全功能实体发送包括远端设备的标识的密钥请求消息，以使得安全功能实体根据该密钥请求消息，获取用于保护远端设备和中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将其反馈给远端设备的移动管理实体，进而通过中继设备的移动管理实体发送给中继
15 设备。

可选地，当中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体对远端设备和中继设备的关联关系验证通过，但远端设备的 NAS 消息完整性校验没有通过，或者远端设备的 NAS 消息没有完整性保护，或者第一请求消息和第二请求消息没有携带远端设备的 NAS 消息，则可以通过安全功能实体获取用于保护远端设备和中继设备
20 之间通信安全的密钥和生成该密钥所需的安全参数，能够保证远端设备和中继设备之间的正常通信。

本申请实施例第三方面提供一种授权验证方法，该方法是从中继设备的角度描述，该方法包括：中继设备接收远端设备发送的包括远端设备的标识的通信请求，根据该通信请求，生成第一请求消息，并将第一请求消息发送给中继设备的移动管理实体，以及
25 接收中继设备的移动管理实体在判断关联关系验证通过后发送的第一响应消息，根据所述第一响应消息向所述远端设备发送通信响应。

本方法在通信响应表征验证关系通过，且远端设备生成了用于保护远端设备和中继设备两者通信安全的密钥时，远端设备则可通过该中继设备连接到网络中，实现方案简单，网络开销小，验证效率低。

30 可选的，该授权验证方法，还包括：中继设备接收中继设备的移动管理实体发送的用于保护远端设备和中继设备之间通信安全的密钥和生成所述密钥所需的安全参数时，上述根据所述第一响应消息向所述远端设备发送通信响应，包括：中继设备将安全参数通过通信响应发送给所述远端设备，以使远端设备根据安全参数生成用于保护远端设备和中继设备之间通信安全的密钥。

35 中继设备接收到密钥和生成密钥所需的安全参数后，则其自己保存该密钥，并且通过通信响应的形式将生成密钥所需的安全参数发送给远端设备，这样远端设备则可根据该安全参数自己生成保护远端设备和中继设备之间通信安全的密钥。如果远端设备侧的密钥与中继设备侧的密钥一致，则表明远端设备和中继设备之间的认证和授权检查成功，远端设备可以通过中继设备发送数据到网络。

本申请实施例第四方面提供一种授权验证方法，该方法是从网络侧设备的角度描述，该网络侧设备可以是中继设备的移动管理实体，也可以是远端设备的移动管理实体，还可以是近距离功能实体，该方法包括：网络侧设备接收中继设备发送的包括远端设备的标识的第一请求消息，根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证，并在判断该关联关系验证通过后，向中继设备发送第一响应消息。

当远端设备的移动管理实体和中继设备的移动管理实体为同一个移动管理实体时，可以将上述远端设备的移动管理实体和中继设备的移动管理实体称为网络侧设备，也即，本实施例中的网络侧设备可通过远端设备的移动管理实体、中继设备的移动管理实体其中的任意一个实现。当然，在一实施例中，该网络侧设备也可通过近距离功能实体实现。

可选的，上述网络侧设备根据所述第一请求消息，触发对所述远端设备和中继设备的关联关系的验证，包括：所述网络侧设备根据第一请求消息，获取第一授权信息，并根据远端设备的标识、中继设备的标识以及第一授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。其中，网络侧设备根据第一请求消息，获取第一授权信息，包括：在中继设备、远端设备成功注册到网络之后，网络侧设备从用户数据管理实体和/或近距离功能实体获取第一授权信息并存储在远端设备上下文信息中和/或中继设备上下文信息中；然后，网络侧设备根据第一请求消息中的远端设备标识和/或中继设备标识查找获取第一授权信息。

在一种实施例中，当该网络侧设备为中继设备的移动管理实体时，该网络侧设备在中继设备成功注册到网络之后，根据中继设备的标识从用户数据管理实体和/或近距离功能实体获取第一授权信息，此时，第一授权信息指的是中继设备的授权信息。

在另一种实施例中，当该网络侧设备为远端设备的移动管理实体时，该网络侧设备在远端设备成功注册到网络之后，根据远端设备的标识从用户数据管理实体和/或近距离功能实体获取该第一授权信息，此时，第一授权信息指的是远端设备的授权信息。

在再一种实施例中，当该网络侧设备为近距离功能实体时，该网络侧设备在远端设备、中继设备成功注册到网络之后，根据中继设备的标识、远端设备的标识分别从用户数据管理实体和/或近距离功能实体获取第一授权信息，此时，第一授权信息既包括远端设备的授权信息，也包括中继设备的授权信息。

可选的，若第一请求消息，还包括：中继服务码；则网络侧设备根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：网络侧设备根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息，验证是否允许远端设备通过中继设备接入网络。

可选的，网络侧设备根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：网络侧设备向第一移动管理实体发送第二请求消息，以使第一移动管理实体根据第二请求消息验证是否允许远端设备通过中继设备接入网络；此时，网络侧设备为中继设备的移动管理实体时，第一移动管理实体为近距离功能实体或远端设备的移动管理实体；或者网络侧设备为远端设备的移动管理实体时，第一移动管理实体为近距离功能实体或中继设备的移动管理实体；或者网络侧设备为近距离功能实体时，第一移动管理实体为远端设备的移动管理实体或中继设备的移动管理实体。

可选的，在第一请求消息中包括远端设备的非接入层消息以及非接入层消息的校验码时，第二请求消息包括：远端设备的非接入层消息、非接入层消息的校验码以及远端设备的标识，则网络侧设备根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：网络侧设备向远端设备的移动管理实体发送第二请求消息，以使远端设备的移动管理实体根据第二请求消息对远端设备进行安全处理；此时，网络侧设备为中继设备的移动管理实体，或者网络侧设备为近距离功能实体。

可选的，网络侧设备为远端设备的移动管理实体时，网络侧设备接收中继设备发送的第一请求消息，包括：网络侧设备接收中继设备通过基站转发处理的第一请求消息，该第一请求消息还包括：中继设备的标识。

可选的，第一请求消息包括远端设备的非接入层消息以及非接入层消息的校验码，网络侧设备根据第一请求消息，触发对远端设备和中继设备的关联关系的验证，包括：网络侧设备根据远端设备的标识，获取远端设备的非接入层上下文信息，并根据所述非接入层上下文信息对非接入层消息的校验码进行验证。

可选的，该授权验证方法还包括：网络侧设备向第一移动管理实体发送第二请求消息，以使第一移动管理实体根据远端设备的标识，获取远端设备的非接入层上下文信息，并根据非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥，以及将密钥和生成该密钥所需的安全参数反馈给网络侧设备，网络侧设备将密钥和生成该密钥所需的安全参数发送给中继设备，从而使中继设备将安全参数返回给远端设备，使远端设备根据安全参数生成用于保护远端设备和中继设备之间通信安全的所述密钥；此时，网络侧设备为中继设备的移动管理实体，第一移动管理实体为近距离功能实体或远端设备的移动管理实体。

可选的，该授权验证方法还包括：网络侧设备根据远端设备的标识，获取远端设备的非接入层上下文信息，并根据非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，以及将该密钥和生成密钥所需的安全参数反馈给中继设备的移动管理实体并转发给中继设备，以使中继设备将所述安全参数返回给远端设备，从而使远端设备根据安全参数生成用于保护所述远端设备和所述中继设备之间通信安全的所述密钥；此时，网络侧设备为远端设备的移动管理实体或者近距离功能实体。

可选的，所述密钥由所述远端设备的移动管理实体根据所述远端设备的基础安全密钥生成。

可选的，所述中继设备的移动管理实体中存储有所述中继设备的上下文信息，所述远端设备的移动管理实体中存储有所述远端设备的上下文信息，近距离功能实体中存储有所述中继设备的上下文信息和所述远端设备的上下文信息。

可选的，该授权验证方法还包括：网络侧设备向安全功能实体发送包括远端设备的标识的密钥请求消息，以使得安全功能实体根据所述密钥请求消息，获取用于保护远端设备和中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将密钥和生成该密钥所需的安全参数反馈给网络侧设备，所述密钥请求消息，包括：所述远端设备的标识。

本申请实施例第五方面提供一种授权验证装置，所述装置包括用于执行上述第一方面以及第一方面的各种实现方式所提供的方法的模块或手段（means）。

本申请实施例第六方面提供一种授权验证装置，所述装置包括用于执行上述第二方面以及第二方面的各种实现方式所提供的方法的模块或手段（means）。

本申请实施例第七方面提供一种授权验证装置，所述装置包括用于执行上述第三方面以及第三方面的各种实现方式所提供的方法的模块或手段（means）。

5 本申请实施例第八方面提供一种授权验证装置，所述装置包括用于执行上述第四方面以及第四方面的各种实现方式所提供的方法的模块或手段（means）。

本申请实施例第九方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第一方面提供的方法。

10 本申请实施例第十方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第二方面提供的方法。

本申请实施例第十一方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第三方面提供的方法。

15 本申请实施例第十二方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第四方面提供的方法。

本申请实施例第十三方面提供一种授权验证装置，包括用于执行以上第一方面的方法的至少一个处理元件（或芯片）。

20 本申请实施例第十四方面提供一种授权验证装置，包括用于执行以上第二方面的方法的至少一个处理元件（或芯片）。

本申请实施例第十五方面提供一种授权验证装置，包括用于执行以上第三方面的方法的至少一个处理元件（或芯片）。

25 本申请实施例第十六方面提供一种授权验证装置，包括用于执行以上第四方面的方法的至少一个处理元件（或芯片）。

本申请实施例第十七方面提供一种程序，该程序在被处理器执行时用于执行以上第一方面的方法。

30 本申请实施例第十八方面提供一种程序产品，例如计算机可读存储介质，包括第十七方面的程序。

本申请实施例第十九方面提供一种程序，该程序在被处理器执行时用于执行以上第二方面的方法。

本申请实施例第二十方面提供一种程序产品，例如计算机可读存储介质，包括第十九方面的程序。

35 本申请实施例第二十一方面提供一种程序，该程序在被处理器执行时用于执行以上第三方面的方法。

本申请实施例第二十二方面提供一种程序产品，例如计算机可读存储介质，包括第二十一方面的程序。

本申请实施例第二十三方面提供一种程序，该程序在被处理器执行时用于执行以上

第四方面的方法。

本申请实施例第二十四方面提供一种程序产品，例如计算机可读存储介质，包括第二十三方面的程序。

5 本申请实施例第二十五方面提供一种授权验证方法，该方法是从远端设备的移动管理实体的角度描述，该方法包括：

远端设备的移动管理实体接收基站发送的初始设备消息，所述初始设备消息包括：远端设备的非接入层消息和中继设备的标识；

所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证；

10 所述远端设备的移动管理实体在判断所述关联关系验证通过后，向基站发送初始上下文建立请求消息。

可选的，所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证，包括：

所述远端设备的移动管理实体根据所述远端设备的标识获取授权关系信息；

15 所述远端设备的移动管理实体根据所述远端设备的标识、所述中继设备的标识以及所述授权关系信息，验证是否允许所述远端设备通过所述中继设备接入网络；

所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远端设备的标识包含在所述初始设备消息中。

20 可选的，在所述远端设备的移动管理实体接收基站发送的初始设备消息之前，所述远端设备的移动管理实体根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述授权关系信息，并将所述授权关系信息存储在所述远端设备的移动管理实体。

可选的，所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证，包括：

25 所述远端设备的移动管理实体根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并对所述远端设备的非接入层消息进行完整性校验。

可选的，所述方法还包括：

所述远端设备的移动管理实体根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息；

30 所述远端设备的移动管理实体根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥；

所述远端设备的移动管理实体将所述密钥和生成所述密钥所需的安全参数通过所述初始上下文建立请求消息发送给所述基站。

可选的，所述方法还包括：

35 所述远端设备的移动管理实体向所述中继设备的移动管理实体发送第一验证请求消息，以使所述中继设备的移动管理实体根据所述第一验证请求消息对所述远端设备和所述中继设备的关联关系进行验证，所述第一验证请求消息包括：所述远端设备的标识和所述中继设备的标识。

可选的，所述方法还包括：

所述远端设备的移动管理实体向安全功能实体发送密钥请求消息，以使得所述安全

功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给所述远端设备的移动管理实体，所述密钥请求消息，包括：所述远端设备标识。

5 本申请实施例第二十六方面提供一种授权验证方法，该方法是从基站的角度描述，该方法包括：

 基站接收中继设备发送的第一无线资源控制消息，所述第一无线资源控制消息包括远端设备的非接入层消息；

 所述基站根据所述第一无线资源控制消息，识别出远端设备请求通过所述中继设备接入网络，获取所述中继设备的标识，以及通过初始设备消息将所述中继设备的标识和所述
10 远端设备的非接入层消息发送给远端设备的移动管理实体；

 所述基站接收所述远端设备的移动管理实体在判断所述远端设备和所述中继设备的关联关系验证通过后发送的初始上下文建立请求消息；

 所述基站根据所述初始上下文建立请求消息为所述远端设备建立上下文信息，并向所述
15 中继设备发送第二无线资源控制消息。

 可选的，所述基站获取所述中继设备的标识，包括：

 所述基站从所述基站存储的中继设备的上下文信息中获取所述中继设备的标识，或所述基站从所述第一无线资源控制消息中获取所述中继设备的标识。

 可选的，所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远
20 端设备的标识包含在所述初始设备消息中。

 可选的，所述方法，还包括：

 所述基站根据所述初始上下文建立请求消息，建立所述远端设备和所述中继设备的映射关系。

 可选的，在所述远端设备的移动管理实体生成用于保护所述远端设备和所述中继设备之间通信安全的密钥时，所述方法还包括：

 所述基站接收所述中继设备的移动管理实体发送的用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

 可选的，所述方法，还包括：

 所述基站向所述远端设备发送第三无线资源控制消息，以使所述远端设备根据所述第三无线资源控制消息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，所述
30 第三无线资源控制消息，包括：生成所述密钥所需的安全参数。

 本申请实施例第二十七方面提供一种授权验证方法，该方法是从中继设备的角度描述，该方法包括：

 中继设备接收远端设备发送的通信请求；

 所述中继设备根据所述通信请求生成第一无线资源控制消息，并将所述第一无线资源控制消息发送给基站；
35

 所述中继设备接收所述基站为所述远端设备建立上下文信息后发送的第二无线资源控制消息，以根据所述第二无线资源控制消息确定允许所述远端设备通过所述中继设备接入网络。

可选的，该方法还包括：

所述中继设备将所述中继设备的标识通过所述第一无线资源控制消息发送给所述基站，以使所述基站识别远端设备请求通过所述中继设备接入网络。

可选的，所述方法，还包括：

- 5 所述中继设备根据所述基站发送的所述第二无线资源控制消息，建立所述远端设备和所述中继设备的映射关系。

可选的，所述第二无线资源控制消息，包括：用于保护所述远端设备和所述中继设备之间通信安全的密钥。

- 10 本申请实施例第二十八方面提供一种授权验证装置，所述装置包括用于执行上述第二十五方面以及第二十五方面的各种实现方式所提供的方法的模块或手段（means）。

本申请实施例第二十九方面提供一种授权验证装置，所述装置包括用于执行上述第二十六方面以及第二十六方面的各种实现方式所提供的方法的模块或手段（means）。

本申请实施例第三十方面提供一种授权验证装置，所述装置包括用于执行上述第二十七方面以及第二十七方面的各种实现方式所提供的方法的模块或手段（means）。

- 15 本申请实施例第三十一方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第二十五方面提供的方法。

- 20 本申请实施例第三十二方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第二十六方面提供的方法。

本申请实施例第三十三方面提供一种授权验证装置，所述装置包括处理器和存储器，存储器用于存储程序，处理器调用存储器存储的程序，以执行本申请第二十七方面提供的方法。

- 25 本申请实施例第三十四方面提供一种授权验证装置，包括用于执行以上第二十五方面的方法的至少一个处理元件（或芯片）。

本申请实施例第三十五方面提供一种授权验证装置，包括用于执行以上第二十六方面的方法的至少一个处理元件（或芯片）。

本申请实施例第三十六方面提供一种授权验证装置，包括用于执行以上第二十七方面的方法的至少一个处理元件（或芯片）。

- 30 本申请实施例第三十七方面提供一种程序，该程序在被处理器执行时用于执行以上第二十五方面的方法。

本申请实施例第三十八方面提供一种程序产品，例如计算机可读存储介质，包括第三十七方面的程序。

- 35 本申请实施例第三十九方面提供一种程序，该程序在被处理器执行时用于执行以上第二十六方面的方法。

本申请实施例第四十方面提供一种程序产品，例如计算机可读存储介质，包括第三十九方面的程序。

本申请实施例第四十一方面提供一种程序，该程序在被处理器执行时用于执行以上第二十七方面的方法。

本申请实施例第四十二方面提供一种程序产品，例如计算机可读存储介质，包括第四十一方面的程序。

在以上各个方面中，中继设备接收远端设备发送的通信请求，并根据该通信请求生成第一无线资源控制消息，并将其发送给基站，基站接收该第一无线资源控制消息，该第一无线资源控制消息包括远端设备的非接入层消息，并根据该第一无线资源控制消息，识别出远端设备请求通过中继设备接入网络，获取该中继设备的标识，以及通过初始设备消息将中继设备的标识和远端设备的非接入层消息发送给远端设备的移动管理实体，这样远端设备的移动管理实体接收并根据该初始设备消息，触发对远端设备和中继设备的关联关系的验证，且在判断所述关联关系验证通过后，向基站发送初始上下文建立请求消息，从而基站根据该初始上下文建立请求消息为远端设备建立上下文信息，并向中继设备发送第二无线资源控制消息，最后中继设备根据该第二无线资源控制消息确定允许远端设备通过中继设备接入网络。本申请的技术方案针对层 2 中继设备，设计了一套远端设备与中继设备的关联关系验证方案，避免了现有层 3 中继方案中所需执行的复杂繁琐的参数配置流程和授权检查流程，使得本申请的层 2 解决方案和现有层 3 解决方案相比，降低了网络配置需求、减少了网络开销、提高了验证效率。

附图说明

图 1 为本申请实施例提供的授权验证方法实施例一的交互图；
图 2 为本申请实施例提供的授权验证方法实施例二的流程图；
图 3 为本申请实施例提供的授权验证方法实施例三的流程图；
图 4 为本申请实施例提供的授权验证方法实施例四的流程图；
图 5 为本申请实施例提供的授权验证方法实施例五的流程图；
图 6 为本申请实施例提供的授权验证方法实施例六的交互图；
图 7 为本申请实施例提供的授权验证方法实施例七的交互图；
图 8 为本申请实施例提供的授权验证方法实施例八的流程图；
图 9 为本申请实施例提供的授权验证方法实施例九的流程图；
图 10 为本申请实施例提供的授权验证方法实施例十的流程图；
图 11 为本申请实施例提供的授权验证方法实施例十一的交互图；
图 12 为本申请实施例提供的授权验证方法实施例十二的交互图；
图 13 为本申请实施例提供的授权验证方法实施例十三的交互图；
图 14 为本申请实施例提供的授权验证方法实施例十四的交互图；
图 15 为本申请实施例提供的授权验证方法实施例十五的交互图；
图 16 为本申请实施例提供的一种授权验证装置的结构示意图；
图 17 为本申请实施例提供的另一种授权验证装置的结构示意图；
图 18 为本申请实施例提供的再一种授权验证装置的结构示意图；
图 19 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 20 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 21 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 22 为本申请实施例提供的又一种授权验证装置的结构示意图；

图 23 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 24 为本申请实施例提供的授权验证方法实施例十六的交互图；
图 25 为本申请实施例提供的授权验证方法实施例十七的流程示意图；
图 26 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 27 为本申请实施例提供的又一种授权验证装置的结构示意图；
图 28 为本申请实施例提供的又一种授权验证装置的结构示意图。

具体实施方式

以下，对本申请实施例中的部分用语进行解释说明，以便于本领域技术人员理解：

远端设备：可以是一种无线终端，其可以指向用户提供语音和/或其他业务数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。为了降低功耗，远端设备一般通过中继设备接入到网络中。远端设备也可以称为系统、订户单元 (Subscriber Unit)、订户站 (Subscriber Station)、移动站 (Mobile Station)、移动台 (Mobile)、远程站 (Remote Station)、远程终端 (Remote Terminal)、接入终端 (Access Terminal)、用户终端 (User Terminal)、用户代理 (User Agent)、用户设备 (User Device or User Equipment)，在此不作限定。

中继设备：也称网络中继器，连接在远端设备与网络中间的仪器设备，可以是在无线网络层面 (如 PDCP 层) 为远端设备的网络连接提供中继的设备，也可以是连接在远端设备与网络中间的仪器设备，它可以对传输的信号进行放大并可重发，从而可以避免信号在传输过程中的衰减，有效地提高传输的可靠性。中继设备也可以被理解为在物理层面建设性地实现网络的互联设备，本申请实施例并不对中继设备的具体表现形式进行限定。

移动性管理实体 (Mobile Management Entity, 简称 MME)：主要功能是支持非接入层 (Non Access stratum, 简称 NAS) 信令及其安全、跟踪区域列表的管理、分组数据网络网关 (Packet Data Network Gateway, 简称 P-GW) 和服务网关 (Serving Gateway, 简称 S-GW) 的选择、跨 MME 切换时进行 MME 的选择、在向 2G/3G 接入系统切换过程中进行服务 GPRS 支持节点 (Service GPRS Support Node, 简称 SGSN) 的选择、用户的鉴权、漫游控制以及承载管理、3GPP 不同接入网络的核心网络节点之间的移动性管理，以及 UE 在空闲状态下可达性管理。本申请实施例中的 MME 可以包括中继设备的 MME、远端设备的 MME，中继设备的 MME 指的是当前服务该中继设备的 MME，远端设备的 MME 指的是当前服务该远端设备的 MME，从功能上来说，两个 MME 没有区别，因此，当前服务中继设备的 MME 与当前服务远端设备的 MME 可以是同一个 MME，本申请所有实施例中的涉及的 MME 一般指此类 MME。本申请也不排除另一类 MME，即，中继设备的 MME 指的是专门用于服务中继设备的 MME，远端设备的 MME 指的是专门用于服务远端设备的 MME，此时从功能上来说，两个 MME 可能有所区别；当然也可以包括集成中继设备的 MME 和远端设备的 MME 功能于一体的 MME。这些 MME 可以用于验证是否允许远端设备通过中继设备接入网络。该 MME 还可以是未来 5G 网络中的移动性管理功能实体，如访问移动性管理功能实体 (access and mobility management function, 简称 AMF)。

基站：又称为无线接入网（Radio Access Network, RAN）设备，是一种将终端接入到无线网络的设备，可以是全球移动通讯（Global System of Mobile communication, 简称 GSM）或码分多址（Code Division Multiple Access, 简称 CDMA）中的基站（Base Transceiver Station, 简称 BTS），也可以是宽带码分多址（Wideband Code Division Multiple Access, 简称 WCDMA）中的基站（NodeB, 简称 NB），还可以是长期演进（Long Term Evolution, 简称 LTE）中的演进型基站（Evolutional Node B, 简称 eNB 或 eNodeB），或者中继站或接入点，或者未来 5G 网络中的基站等，在此并不限定。

本申请实施例中，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

本申请所有实施例中，如果当前服务中继设备的 MME 与当前服务远端设备的 MME 是同一个 MME 时，则两个 MME 之间的交互可以省略或者属于 MME 内部交互。

图 1 为本申请实施例提供的授权验证方法实施例一的交互图。本申请实施例以中继设备的移动管理实体、终端设备移动管理实体以及中继设备的交互进行说明。如图 1 所示，本申请实施例提供的授权验证方法可以包括如下步骤：

步骤 101、中继设备接收远端设备发送的通信请求。

作为一种示例，该通信请求包括：远端设备的标识。

可选的，该通信请求中还包括以下内容中的一个或几个：远端设备的非接入层消息、中继服务码（Relay service code）、第一随机数。可选的，该第一随机数是远端设备生成的，可以直接携带在通信请求中。可选地，如果存在第一随机数，所述第一随机数还可以包含在远端设备的非接入层消息中，而不是直接携带在通信请求中。

在本申请实施例中，远端设备可选为可穿戴设备（wearable device, 简称 WD），该远端设备（WD）希望通过中继设备（relay）连接到网络中，从而需要在允许远端设备通过中继设备接入到网络之前，实现对中继设备和远端设备的关联关系验证。

可选的，在中继设备接收远端设备发送的通信请求之前，中继设备和远端设备需完成以下发现过程，具体的，中继设备和远端设备均需要接入到网络中获取用于发现过程的配置参数，从而根据这些配置参数实现远端设备和中继设备之间的互相发现过程。

可选的，远端设备向中继设备发送通信请求，该通信请求中至少需携带远端设备的标识。

作为一种示例，远端设备的标识可以直接包含在通信请求中。作为另一种示例，若通信请求还包含远端设备的 NAS 消息，则远端设备的标识也可以被远端设备封装在自己的 NAS 消息中，此时，通信请求中包含的远端设备的 NAS 消息中包括该远端设备的标识。作为再一种示例，远端设备的标识还可以同时包含在通信请求中以及通信请求中的远端设备的 NAS 消息中。因此，通信请求包含远端设备的标识的实现形式可以有多种，本申请实施例并不对其进行限定。

在本申请实施例中，可选地，远端设备的 NAS 消息中携带有 MAC-I 校验值，用于远端设备的 MME 根据远端设备的 NAS 安全上下文进行完整性保护，远端设备的 MME 可以通过验证该 NAS 消息的 MAC-I 来认证远端设备。

值得说明的是，本申请实施例所述的远端设备的标识可能包含至少两种不同的形

式，其中，一种形式适用于进行授权验证，另一种形式适用于中继设备的移动管理实体寻找远端设备的移动管理实体以及用于获取远端设备的上下文信息。例如，可选地，通信请求中的远端设备标识包括标识 1，该标识 1 用于中继设备的移动管理实体寻找远端设备的移动管理实体；通信请求中的远端设备标识包括标识 2，该标识 2 用于中继设备的移动管理实体或者远端设备的移动管理实体实现对中继设备和远端设备的关联关系进行授权验证；包含在远端设备的 NAS 消息中的远端设备标识包括标识 3，标识 3 用于获取远端设备的上下文信息，可选地，标识 1 和标识 3 可以是同一个标识。本实施例中并没有对远端设备的标识的具体形式进行区分。

可选的，标识 1 和标识 3 可以是全球唯一临时 UE 标识(Globally Unique Temporary UE Identity, 简称 GUTI)，或国际移动用户识别码(International Mobile Subscriber Identity, 简称 IMSI)，或者临时识别码(Temporary Mobile Subscriber Identity, 简称 TMSI)等。可选地，标识 2 可以是近距离功能实体分配的标识。

步骤 102、中继设备根据通信请求，生成第一请求消息。

该第一请求消息包括：远端设备的标识。可选的，该第一请求消息为中继设备(relay)和移动管理实体(MME)之间的非接入层(NAS)消息。

作为一种示例，中继设备接收到远端设备的通信请求之后，可以将该通信请求的相关内容封装到自己的第一请求消息中。

作为另一种示例，中继设备还可以既将通信请求的相关内容封装到自己的第一请求消息中，也将验证远端设备与中继设备的关联关系所需要的其他相关参数整合到第一请求消息中，例如，可选地，该第一请求消息中还可以包括中继设备的标识。

具体的，封装到第一请求消息中的相关内容，包括步骤 101 中的远端设备的标识，还可能包括步骤 101 中的远端设备的 NAS 消息。可选的，在步骤 101 中的通信请求还包括中继服务码(Relay service code)或者第一随机数时，封装到第一请求消息中的相关内容还包括该中继服务码或者第一随机数。中继服务码用于表征远端设备要请求的业务类型，用于远端设备和中继设备关联关系的验证。第一随机数是远端设备生成的，用于后续密钥的生成，关于密钥的具体生成方式参见后续步骤 502 中的记载。其中，第一随机数的携带方式可以参考步骤 101 中所述的方式。

步骤 103、中继设备将该第一请求消息发送给中继设备的移动管理实体。

当中继设备根据通信请求生成第一请求消息后，便发送给中继设备的移动管理实体，由中继设备的移动管理实体根据第一请求消息的内容触发对远端设备和中继设备的关联关系进行验证。

步骤 104、中继设备的移动管理实体接收第一请求消息。

该第一请求消息中的内容参见步骤 102 中的记载。

步骤 105、中继设备的移动管理实体根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证。

可选的，在本申请的一实施例中，当中继设备的移动管理实体接收到中继设备发送的第一请求消息之后，可以执行如下多种操作中的任意一种。第一种操作：中继设备的移动管理实体根据第一请求消息中的内容触发自身对远端设备和中继设备的关联关系的验证；第二种操作：中继设备的移动管理实体将第一请求消息中内容发送给远端设备的

移动管理实体或者近距离功能实体，以使远端设备的移动管理实体或者近距离功能实体进行进一步的安全处理；第三种操作：执行第一种操作和第二种操作对应的内容。

可选地，中继设备的移动管理实体在按照第三种操作执行时，本申请实施例并不限定第一种操作和第二种操作的执行顺序。例如，第一种操作中中继设备的移动管理实体根据第一请求消息中的内容触发自身对远端设备和中继设备的关联关系的验证，可以放在如下步骤 105d 中执行，可选地，远端设备和中继设备的关联关系的验证可能用到如下步骤 105c 步骤中返回的信息，如远端设备的标识 IMSI。

步骤 106、中继设备的移动管理实体在判断关联关系验证通过后，生成第一响应消息，并向中继设备发送该第一响应消息。

可选的，在本申请实施例中，中继设备的移动管理实体判断关联关系验证通过，具体可以包括如下至少一种：中继设备的移动管理实体自身判断得出远端设备和中继设备的关联关系验证通过、远端设备的移动管理实体判断远端设备和中继设备的关联关系验证通过，或者近距离功能实体判断得出远端设备和中继设备的关联关系验证通过。

作为一种示例，当远端设备和中继设备的关联关系验证仅需要在中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体中的任意一处验证，并且关联关系验证通过时，会生成第一响应消息，并将该第一响应消息反馈给中继设备。

作为另一种示例，当远端设备和中继设备的关联关系验证需要在中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体中的任意两处、或者三处验证时，只有对应的两处或者三处均验证通过，才表明关联关系验证通过，此时，中继设备的移动管理实体生成第一响应消息，并反馈给中继设备。

步骤 107、中继设备接收该第一响应消息。

作为一种示例，在远端设备和中继设备的关联关系验证通过时，该第一响应消息中可以携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数。

作为另一种示例，在远端设备和中继设备的关联关系验证通过时，但远端设备的 NAS 消息完整性校验没有通过，或者远端设备的 NAS 消息没有完整性保护，或者第一请求消息和第二请求消息没有携带远端设备的 NAS 消息，那么 MME（中继设备的 MME 或者远端设备的 MME）则向安全功能实体发送密钥请求消息，以获取用于保护远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

作为再一种示例，在远端设备和中继设备的关联关系验证失败时，该第一响应消息中可以包含失败的原因等参数。

值得说明的是，上述关于第一响应消息的具体包含内容，本申请实施例并不对其进行限定。

步骤 108、中继设备根据第一响应消息向远端设备发送通信响应。

可选的，中继设备会根据接收到的第一响应消息将远端设备与中继设备之间的关联关系验证的结果生成通信响应发送给终端设备，该通信响应作为上述通信请求的结果一种表现形式。可选地，若第一响应消息中携带有用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，则通信响应中包含生成密钥所需的安全参数，以使得远端设备同样生成用于保护远端设备和中继设备两者通信安全的密钥。

当通信响应表征验证关系通过，且远端设备生成了用于保护远端设备和中继设备两者通信安全的密钥时，远端设备则可通过该中继设备连接到网络中。

可选的，在本申请的一实施例中，上述步骤 105，可通过步骤 105a 实现，相应的，本申请实施例的授权验证方法，还包括步骤 105b~步骤 105d。

5 步骤 105a、中继设备的移动管理实体向远端设备的移动管理实体发送第二请求消息。

该第二请求消息包括：远端设备的标识。

作为一种示例，在中继设备的移动管理实体触发对远端设备和中继设备的关联关系的验证时，还可根据第一请求消息中远端设备的标识向远端设备的移动管理实体发送第
10 二请求消息，以使远端设备的移动管理实体根据第二请求消息对远端设备进行安全处理或者对远端设备与中继设备的关联关系进行进一步验证处理。

可选地，该第二请求消息还包括：中继设备的标识。该中继设备的标识和远端设备的标识用于远端设备的 MME 实现对中继设备和远端设备的关联关系进行授权验证。

可选的，该第二请求消息中中继设备的标识可以通过如下方式中的任意一种方式获取到：其一，中继设备的移动管理实体可以从其内部存储的中继设备上下文信息中获取，进而将其封装到第二请求消息中；其二，当第一请求消息中包含中继设备的标识时，中继设备的移动管理实体也可以从上报的第一请求消息中获取到。关于中继设备的标识的具体获取方式本申请实施例并不具体限定。

可选地，该第二请求消息还包括：从第一请求消息中获取的远端设备的 NAS 消息。
20 可选的，该第二请求消息还包括远端设备生成的第一随机数。其中，NAS 消息的内容，以及第一随机数的携带方式可以参考步骤 101 中的所述方法。

可选地，第一请求消息中包括远端设备的标识，该远端设备的标识用于中继设备的 MME 寻找远端设备的 MME，具体的，中继设备的 MME 根据该远端设备的标识确定远端设备的 MME，进而向其发送第二请求消息。此处，远端设备的标识的具体体现形式参见
25 步骤 101 中的记载，此处不再赘述，

步骤 105b、远端设备的移动管理实体接收第二请求消息，并根据第二请求消息对远端设备进行安全处理。

可选的，如果第二请求消息包括：从第一请求消息中获取的远端设备的非接入层（NAS）消息，该安全处理可以包括对远端设备的 NAS 消息的完整性验证。

30 可选地，该安全处理也可以包括根据第二请求消息中的中继设备的标识和/或远端设备的标识，对远端设备和中继设备的关联关系的验证。

可选地，远端设备的 MME 还可以根据第二请求消息中远端设备的标识，获取远端设备的非接入层上下文信息，并根据该非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥。可选的，该标识可以是 GUTI，或 TMSI，或 IMSI 等；具体的，可参见步骤 101 中的记载，此处不再赘述。关于远端设备的标识的获取方式，远端设备的 MME 可以直接从第二请求消息中直接获取，或者从第二请求消息中携带的远端设备的 NAS 消息中获取。

可选地，在远端设备和中继设备的关联关系验证通过时，但远端设备的 NAS 消息完整性校验没有通过，或者远端设备的 NAS 消息没有完整性保护，或者第一请求消息和第

二请求消息没有携带远端设备的 NAS 消息，那么远端设备的 MME 则向安全功能实体发送密钥请求消息，以获取用于保护远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

可选地，在步骤 105b 中，远端设备的 MME 生成的（第一）密钥可以直接作为 PC5 口通信密钥用于 PC5 口的通信保护，即 Relay 根据接收到的（第一）密钥直接对通信响应进行安全保护（如，完整性保护），则相应地，WD 也根据接收到的生成密钥所需的安全参数生成（第一）密钥，即 PC5 口通信密钥，然后对通信响应消息进行安全验证（如，完整性验证）。可选地，PC5 口通信密钥也可以为 Relay 根据步骤 105c 中远端设备的 MME 所生成的（第一）密钥再进一步生成的（第二）密钥，即 Relay 根据接收到的（第一）密钥生成（第二）密钥，作为 PC5 口通信密钥，对通信响应进行安全保护（如，完整性保护），则相应地，WD 根据接收到的生成密钥所需的安全参数生成（第一）密钥后，再根据（第一）密钥生成（第二）密钥，该（第二）密钥即为 PC5 口通信密钥，然后对通信响应消息进行安全验证（如，完整性验证）。

步骤 105c、远端设备的移动管理实体在对远端设备进行安全处理后，向中继设备的移动管理实体发送的第二响应消息。

远端设备的移动管理实体根据第二请求消息的内容对远端设备进行安全处理后，根据安全处理的结果生成第二响应消息，并将该第二响应消息反馈给中继设备的移动管理实体。

可选的，当远端设备的 MME 生成了用于保护远端设备和中继设备之间通信安全的密钥时，该第二响应消息中包含有密钥和生成该密钥所需的安全参数。

可选的，中继设备的移动管理实体接收的密钥和生成密钥所需的安全参数相当于第二响应消息内容的一种表现形式。可选的，该第二响应消息可以包含远端设备的移动管理实体生成的非接入层消息。可选地，该第二响应消息中的非接入层消息使用远端设备的 NAS 安全上下文进行完整性保护，并通过中继设备的移动管理实体发送给中继设备进而发送给远端设备，以使得远端设备通过对所述非接入层消息的完整性验证来认证网络。可选地，所述密钥生成参数可以包含在所述非接入层消息中。

步骤 105d、中继设备的移动管理实体接收该第二响应消息。

本申请实施例提供的授权验证方法，中继设备接收远端设备发送的通信请求，该通信请求中包括终端设备的标识，并根据该通信请求，生成第一请求消息以及将第一请求消息发送给中继设备的移动管理实体，中继设备的移动管理实体接收该第一请求消息，并触发对远端设备和中继设备的关联关系的验证，以及向远端设备的移动管理实体发送第二请求消息，远端设备的移动管理实体接收该第二请求消息，并根据该第二请求消息对远端设备进行安全处理，以及在对远端设备进行安全处理后，向中继设备的移动管理实体发送的第二响应消息，中继设备的移动管理实体接收该第二响应消息，并在判断上述关联关系验证通过后生成第一响应消息，并发送给中继设备，中继设备根据该第一响应消息向远端设备发送通信响应。本申请的技术方案，针对层 2 中继设备，设计了一套远端设备与中继设备的关联关系验证方案，避免了现有层 3 中继方案中所需执行的复杂繁琐的参数配置流程和授权检查流程，使得本申请的层 2 解决方案和现有层 3 解决方案相比，降低了网络配置需求、减少了网络开销、提高了验证效率。

在图 1 所示实施例的基础上，图 2 为本申请实施例提供的授权验证方法实施例二的流程图。如图 2 所示，在本申请实施例提供的授权验证方法中，上述步骤 105（中继设备的移动管理实体根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证）还可包括如下步骤：

步骤 201、中继设备的移动管理实体根据第一请求消息获取第一授权信息。

具体的，当中继设备的移动管理实体自身来验证远端设备和中继设备的关联关系时，其需要首先获取中继设备的上下文，从上下文中获取与该中继设备有授权关系的远端设备列表，即第一授权信息。

可选的，作为一种示例，中继设备的移动管理实体在中继设备成功注册到网络之后，根据中继设备的标识从用户数据管理实体和/或近距离功能实体获取该第一授权信息。

在本实施例中，当中继设备成功注册到网络之后，网络中用户数据管理实体和/或近距离功能实体中均存储有中继设备与远端设备相关的第一授权信息。对于用户数据管理实体中的中继设备与远端设备相关的第一授权信息，中继设备的移动管理实体直接从用户数据管理实体（例如，归属用户服务器（Home Subscriber Server，简称 HSS），或者，5G 系统中的用户数据管理实体（User data management，简称 UDM））获取上述第一授权信息。而对于中继设备的移动管理实体从近距离功能实体获取该第一授权信息的方式，可以为：当中继设备的移动管理实体可直接与近距离功能实体通信时，即两者之间存在直接接口，中继设备的移动管理实体直接从近距离功能实体获取上述第一授权信息；而当中继设备的移动管理实体不能直接与近距离功能实体通信时，即两者之间不存在直接接口，则近距离功能实体通过 HSS 将上述第一授权信息发送给中继设备的移动管理实体。

步骤 202、中继设备的移动管理实体根据远端设备的标识、中继设备的标识以及上述第一授权信息，验证是否允许远端设备通过该中继设备接入网络。

在关联关系验证之前，中继设备的移动管理实体首先获取中继设备的标识。关于中继设备的标识的获取方式，具体可参见上述步骤 105a 中记载，即，可选的，中继设备的移动管理实体可以从其内部存储列表中获取或者中继设备的移动管理实体从上报的第一请求消息中获取，此处不再赘述。

当中继设备的移动管理实体获知远端设备的标识、中继设备的标识以及上述第一授权信息后，判断该第一授权信息中是否包含中继设备与远端设备的关联关系，当该第一授权信息中包含中继设备与远端设备的关联关系时，表明允许该远端设备通过该中继设备接入网络，否则，不允许该远端设备通过该中继设备接入网络。

本申请实施例提供的授权验证方法，当中继设备的移动管理实体根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证时，可根据第一请求消息获取第一授权信息，进而根据远端设备的标识、中继设备的标识以及上述第一授权信息，验证是否允许远端设备通过该中继设备接入网络。这样关联关系验证方法简单，容易实现。

可选的，在图 1 所示实施例的基础上，作为一种示例，当第一请求消息，还包括：

中继服务码时，上述步骤 105 可通过如下可能实现方式实现，具体如下：

中继设备的移动管理实体根据第一请求消息获取第一授权信息，并根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息，验证是否允许该远端设备通过中继设备接入网络。此时，第一授权信息为与中继设备有授权关系的远端设备以及对应的中继服务码的关系列表。

当远端设备发送给中继设备的通信请求中还包括中继服务码时，中继设备整合生成的第一请求消息中也包括中继服务码，该中继服务码用于表征远端设备要请求的业务类型，不同的中继服务码对应不同的业务类型，所以，在本实施例中，中继设备的移动管理实体验证远端设备与中继设备的关联关系时，还依据中继服务码。具体的，中继设备的移动管理实体根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息，验证是否允许该远端设备通过中继设备接入网络。

实际上，该步骤是对图 2 所示实施例的进一步限定，只是判定条件增加了中继服务码。对于第一授权信息的获取方式参见步骤 201 中的记载，对于中继设备的标识的获取方式参见步骤 105a 中的记载，此处不再赘述。

可选的，在上述实施例的基础上，本申请实施例提供的授权验证方法，还包括如下步骤。

中继设备的移动管理实体向近距离功能实体发送第三请求消息，以使近距离功能实体根据该第三请求消息验证是否允许远端设备通过中继设备接入网络。

其中，第三请求消息包括：远端设备的标识、中继设备的标识。

作为一种示例，关于终端设备的移动管理实体触发对远端设备和中继设备的关联关系验证的实现方式，除了中继设备的移动管理实体可自身进行验证、以及向远端设备的移动管理实体发送第二请求消息，以使该远端设备的移动管理实体验证外，中继设备的移动管理实体还可向近距离功能实体发送第三请求消息，以使该近距离功能实体进行验证。

值得说明的是，该第三请求消息中至少包括远端设备的标识、中继设备的标识。可选的，第三请求消息中远端设备的标识、中继设备的标识可以从上报的第一请求消息中获取到。可选的，当通信请求中包括中继服务码时，第一请求消息、第二请求消息以及第三请求消息中均可能包括中继服务码。可选的，中继服务码用于表征远端设备要请求的业务类型，参与到远端设备和中继设备关联关系的验证中。

进一步的，在上述任一实施例的基础上，图 3 为本申请实施例提供的授权验证方法实施例三流程图。如图 3 所示，本申请实施例提供的授权验证方法还包括如下步骤：

步骤 301、中继设备的移动管理实体向安全功能实体发送密钥请求消息，以使得该安全功能实体根据密钥请求消息，获取用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数，并将密钥和生成密钥所需的安全参数反馈给中继设备的移动管理实体。

该所述密钥请求消息，包括：远端设备的标识。

步骤 302、中继设备的移动管理实体将密钥和生成该密钥所需的安全参数发送给中继设备。

作为一种示例，当中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体对远端设备和中继设备关联关系的验证通过时，但中继设备的移动管理实体接收到的第二响应消息中未携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，那么中继设备的移动管理实体向安全功能实体发送密钥请求消息，安全功能实体则根据该密钥请求消息中远端设备的标识，查找并获取用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数，以及将该密钥和生成密钥所需的安全参数反馈给中继设备的移动管理实体，最后中继设备的移动管理实体再将密钥和生成该密钥所需的安全参数反馈给中继设备，以使中继设备对该密钥和安全参数进行相应处理。

这样，即使中继设备的移动管理实体接收到的第二响应消息中未携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，中继设备也能获取到用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数，从而保证远端设备可通过该中继设备接入网络。

在图1所示实施例的基础上，图4为本申请实施例提供的授权验证方法实施例四的流程图。如图4所示，在本申请实施例提供的授权验证方法中，上述步骤105b（远端设备的移动管理实体接收第二请求消息，并根据第二请求消息对远端设备进行安全处理）可具体包括如下步骤：

步骤401、远端设备的移动管理实体根据第二请求消息获取第二授权信息。

具体的，远端设备的移动管理实体在远端设备成功注册到网络之后，根据远端设备的标识从用户数据管理实体和/或近距离功能实体获取第二授权信息。

本步骤与上述步骤201类似，区别在于步骤201用于获取与该中继设备有授权关系的远端设备列表，即第一授权信息，而本步骤用于获取与该远端设备有授权关系的中继设备列表，即第二授权信息。类似的，当远端设备成功注册到网络之后，网络中用户数据管理实体和/或近距离功能实体中均存储有远端设备的与中继设备相关的第二授权信息。对于用户数据管理实体中的中继设备与远端设备相关的第二授权信息，远端设备的移动管理实体直接从用户数据管理实体获取上述第二授权信息。而对于远端设备的移动管理实体从近距离功能实体获取该第二授权信息的方式，可以为：在远端设备的移动管理实体与近距离功能实体之间存在直接接口时，远端设备的移动管理实体直接从近距离功能实体获取上述第二授权信息；而当远端设备的移动管理实体与近距离功能实体通信之间不存在直接接口时，则远端设备的移动管理实体通过HSS从近距离功能实体中获取该第二授权信息。

步骤402、远端设备的移动管理实体根据远端设备的标识、中继设备的标识以及第二授权信息，验证是否允许远端设备通过中继设备接入网络。

与上述步骤202类似，远端设备的移动管理实体在验证远端设备和中继设备的关联关系时，远端设备的移动管理实体根据远端设备的标识、中继设备的标识以及获取的第二授权信息，判断该第二授权信息中是否包含远端设备与中继设备的关联关系。当第二授权信息中包含远端设备与中继设备的关联关系时，表明允许该远端设备通过该中继设备接入网络，否则，不允许该远端设备通过该中继设备接入网络。

作为一种示例，在第二请求消息，还包括：中继服务码时，上述步骤 105b（远端设备的移动管理实体接收第二请求消息，并根据第二请求消息对远端设备进行安全处理）的具体实现方式如下：

远端设备的移动管理实体根据远端设备的标识、中继设备的标识、中继服务码以及第二授权信息，验证是否允许远端设备通过中继设备接入网络。此时，第二授权信息为与远端设备有授权关系的中继设备以及对应的中继服务码的关系列表。

该步骤是对上述步骤 402 的进一步说明，判定条件增加了中继服务码，即增加了远端设备请求业务的业务类型，关于具体的判定方式与中继设备的移动管理实体根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息对远端设备和中继设备的关联关系进行验证的方式类似，此处不再赘述。

可选的，如图 4 所示，在本申请实施例提供的授权验证方法中，上述步骤 105b 还包括如下步骤：

步骤 403：远端设备的移动管理实体根据第二请求消息中的远端设备的标识，获取远端设备的非接入层上下文信息，并根据非接入层上下文信息对远端设备的非接入层消息的校验码进行验证。

其中，第二请求消息包括：远端设备的非接入层消息、非接入层消息的校验码。

在本实施例中，在第一请求消息还包括：远端设备的非接入层消息、非接入层消息的校验码时，第二请求消息中也包括：远端设备的非接入层消息、非接入层消息的校验码。此时，远端设备的移动管理实体还可对远端设备的非接入层消息进行验证，具体的是根据远端设备的非接入层上下文信息对远端设备的非接入层消息的校验码进行验证。

值得说明的是，上述步骤 401、步骤 402 和步骤 403 的执行均是远端设备的移动管理实体对远端设备进行安全处理的一种可选方式，也即，在一实施例中，远端设备的移动管理实体可以执行步骤 401、步骤 402 和步骤 403 中的一个或多个，而且，在执行多个步骤时，本申请实施例也不限定每个步骤的执行顺序。

本申请实施例提供的授权验证方法，远端设备的移动管理实体不仅根据第二请求消息获取第二授权信息，还在第二请求消息还包括中继服务码时，根据远端设备的标识、中继设备的标识、中继服务码以及第二授权信息，验证是否允许远端设备通过中继设备接入网络，此外，还根据第二请求消息中的远端设备的标识，获取远端设备的非接入层上下文信息，并根据非接入层上下文信息对远端设备的非接入层消息的校验码进行验证，这样通过检查非接入层消息的完整性从而完成远端设备和中继设备的安全认证。

进一步的，在上述实施例的基础上，图 5 为本申请实施例提供的授权验证方法实施例五的流程图。如图 5 所示，在本申请实施例提供的授权验证方法中，还包括：

步骤 501、远端设备的移动管理实体根据第二请求消息中远端设备的标识，获取远端设备的非接入层上下文信息。

在本实施例中，为了保证远端设备与中继设备的通信安全，远端设备的移动管理实体根据需要通信的远端设备的标识获取该远端设备的非接入层上下文消息，该非接入层上下文消息中存储有生成密钥所需的安全参数。

步骤 502、远端设备的移动管理实体根据该非接入层上下文信息生成用于保护远端设

备和中继设备之间通信安全的密钥。

为了实现远端设备和中继设备的通信安全，远端设备的移动管理实体可根据该非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥。可选的，在远端设备发送的通信请求中附带第一随机数时，远端设备的移动管理实体将第一随机数作为生成该密钥的输入参数。其中，第一随机数是远端设备生成的。可选地，在远端设备的移动管理实体生成第二随机数时，远端设备的移动管理实体将第二随机数作为生成该密钥的输入参数。可选的，第一随机数是被封装在随通信请求由远端设备发送给中继设备，随后被中继设备封装到第一请求消息中发送给中继设备的移动管理实体，最后被中继设备的移动管理实体通过第二请求消息发送给远端设备的移动管理实体。

可选地，远端设备的移动管理实体根据远端设备的标识获取远端设备 NAS 消息的安全上下文，然后基于 NAS 消息的安全上下文生成用于保护远端设备和中继设备之间通信安全的密钥，即，密钥生成参数为远端设备 NAS 消息的安全上下文中的参数。可选地，进一步地，生成密钥所需的安全参数可以为远端设备 NAS 消息的安全上下文中的密钥 K_{asme}。可选地，生成密钥所需的安全参数还可以包括其它参数，比如，MME-WD 生成的第二随机数，和/或 WD 生成的第一随机数。

步骤 503、远端设备的移动管理实体将该密钥和生成密钥所需的安全参数发送给中继设备的移动管理实体。

具体的，由于远端设备的移动管理实体与中继设备之间一般不直接通信，所以，当远端设备的移动管理实体中生成用于保护远端设备和中继设备之间通信安全的密钥之后，需要将该密钥和生成密钥所需的安全参数发送给中继设备的移动管理实体，进而使其发送给中继设备。可选的，由于第一随机数是远端设备自己生成的，其可后续生成密钥时不需获取，所以，本申请实施例中所述的生成密钥所需的安全参数主要包括第二随机数，且该第二随机数被封装在远端设备的移动管理实体的非接入层消息中。

相应的，在中继设备的移动管理实体和中继设备侧，均还需要执行相应的接收操作。具体参照步骤 504 所示的内容。

步骤 504、中继设备的移动管理实体接收远端设备的移动管理实体发送的密钥和生成密钥所需的安全参数。

可选的，中继设备的移动管理实体接收的密钥和生成密钥所需的安全参数相当于第二响应消息内容的一种表现形式。可选的，该第二响应消息可以包含远端设备的移动管理实体生成的非接入层消息。可选地，该第二响应消息中的非接入层消息使用远端设备的 NAS 安全上下文进行完整性保护，并通过中继设备的移动管理实体发送给中继设备进而发送给远端设备，以使得远端设备通过对所述非接入层消息的完整性验证来认证网络。可选地，所述密钥生成参数可以包含在所述非接入层消息中。

步骤 505、中继设备的移动管理实体将密钥和生成该密钥所需的安全参数发送给中继设备。

远端设备想要通过中继设备接入到网络中，远端设备和中继设备需要具有保护两者之间通信的密钥，所以，中继设备的移动管理实体还需要将接收到的密钥和生成该密钥所需的安全参数发送给中继设备，以使中继设备持有该密钥和生成该密钥的所需的安全参数。

步骤 506、中继设备接收用于保护该远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数。

相应的，上述步骤 108 可替换为步骤 507：

步骤 507：中继设备将安全参数通过通信响应发送给远端设备，以使远端设备根据安全参数生成用于保护远端设备和中继设备之间通信安全的密钥。

当中继设备接收到密钥和生成密钥所需的安全参数后，则其自己保存该密钥，并且通过通信响应的形式将生成密钥所需的安全参数发送给远端设备，这样远端设备则可根据该安全参数自己生成保护远端设备和中继设备之间通信安全的密钥。如果远端设备侧的密钥与中继设备侧的密钥一致，则表明远端设备和中继设备之间的认证和授权检查成功，远端设备可以通过中继设备发送数据到网络。

本申请实施例提供的授权验证方法，远端设备的移动管理实体根据第二请求消息中远端设备的标识，生成用于保护远端设备和中继设备之间通信安全的密钥，并将该密钥和生成密钥所需的安全参数发送给中继设备的移动管理实体，中继设备的移动管理实体将接收到的密钥和生成该密钥所需的安全参数发送给中继设备，中继设备再将安全参数通过通信响应发送给远端设备，以使远端设备根据安全参数生成用于保护远端设备和中继设备之间通信安全的密钥，这样远端设备在通过中继设备接入网络时，使可通过利用密钥保护短距离通信的安全，安全性高。

可选的，在本申请实施例提供的授权验证请求中，当中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体对远端设备和中继设备的关联关系验证通过，但远端设备的移动管理实体并没有执行上述步骤 502 中生成密钥的操作，也即当远端设备发送给中继设备的通信请求中不携带远端设备的 NAS 消息，或者远端设备发送给中继设备的通信请求中携带远端设备的 NAS 消息但该 NAS 消息的完整性校验失败，或者远端设备发送给中继设备的通信请求中携带远端设备的 NAS 消息没有完整性保护，那么远端设备的移动管理实体还可执行如下操作：

远端设备的移动管理实体向安全功能实体发送密钥请求消息，以使得安全功能实体根据密钥请求消息，获取用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数，并将其反馈给远端设备的移动管理实体。

其中，密钥请求消息，包括：远端设备标识。

该步骤与上述图 3 所示实施例中中继设备的移动管理实体向安全功能实体发送密钥请求消息，以获取保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数的步骤类似，此处不再赘述。

结合以上实施例，下述实施例对授权验证方法的完整流程进行说明。在下图中远端设备以可穿戴设备 (WD)、中继设备 (Relay)、远端设备的移动管理实体 (MME-WD)、中继设备的移动管理实体 (MME-relay)、基站 (eNB)、归属用户服务器 (Home Subscriber Server, 简称 HSS) 以及近距离功能实体 (ProSe Function, 简称 PF) 等进行说明。

图 6 为本申请实施例提供的授权验证方法实施例六的交互图。如图 6 所示，本申请实施例提供的授权验证方法，包括：

步骤 601、WD 和 Relay 成功注册到网络。

步骤 602、WD 向 Relay 发送通信请求。

该通信请求中包含远端设备的 NAS 消息，关于通信请求中的其他内容参照图 1 所示实施例中步骤 101 的记载，此处不再赘述。

步骤 603、Relay 生成了第一请求消息，并将该第一请求消息发给 MME-relay。

5 具体的，Relay 将 WD 的通信请求中的内容封装到自己的 NAS 消息中，即生成了第一请求消息。可选的，该第一请求消息为中继设备（relay）和移动管理实体（MME）之间的 NAS 消息。

步骤 604、MME-relay 根据该第一请求消息验证 Relay 和 WD 的关联关系。

10 可选的，当 MME-relay 接收到 Relay 发送的第一请求消息之后，可以执行如下多种操作中的任意一种或几种。第一种操作：MME-relay 根据第一请求消息中的内容触发自身对 Relay 和 WD 的关联关系的验证；第二种操作：MME-relay 将第一请求消息中内容发送给 MME-WD 或者 PF，以使 MME-WD 或者 PF 进行进一步的安全处理；第三种操作：执行第一种操作和第二种操作对应的内容。

对于 MME-relay 根据该第一请求消息验证 Relay 和 WD 的关联关系的具体实现参见图 1 所示实施例中步骤 105 中的记载，此处不再赘述。

15 步骤 605、MME-relay 向 MME-WD 发送第二请求消息。

关于第二请求消息中的内容参见图 1 所示实施例中步骤 105a 的记载，此处不再赘述。

其中，MME-relay 可以根据第一请求消息中携带的 WD ID 找到对应的 MME-WD。

20 步骤 606、MME-WD 验证第二请求消息的完整性，对 Relay 和 WD 的关联关系进行验证，生成密钥。

可选的，MME-WD 接收到第二请求消息之后，可以执行如下操作中的一种或几种：验证第二请求消息的完整性、对 Relay 和 WD 的关联关系进行验证、生成密钥。该密钥是用于保护远端设备和中继设备之间通信安全的密钥。

25 其中，该密钥可以是 PC5 口通信密钥，生成密钥所需的安全参数包括：第一随机数（可选的）、MME-WD 生成的第二随机数（可选的）、基础密钥（例如，Kasme）以及中继服务码（Relay service code）（可选的），可选的，第二随机数封装在第二 NAS 消息中最终返回给 WD。关于密钥生成的具体操作参见图 5 所示实施例中的步骤 502，此处不再赘述。

步骤 607、MME-WD 将密钥和生成密钥所需的安全参数返回给 MME-relay。

30 可选的，在 MME-WD 生成用于保护远端设备和中继设备之间通信安全的密钥时，MME-WD 则将其返回给 MME-relay。或者在 MME-WD 对 Relay 和 WD 的关联关系验证时，将验证后的结果反馈给 MME-relay。

35 可选的，生成密钥所需的安全参数主要指远端设备的移动管理实体生成的第二随机数。此时，可选地，MME-WD 将该第二随机数封装在自己的 NAS 消息中发送给 MME-relay。

步骤 608、MME-relay 通过第一响应消息将密钥和生成密钥所需的安全参数返回给 relay。

步骤 609、relay 接收该密钥和生成密钥所需的安全参数，将生成密钥所需的安全参数通过通信响应发给 WD。

当 relay 接收到密钥（比如，PC5 通信密钥）和生成密钥所需的安全参数，则表明对 WD 和 relay 的认证和授权通过，WD 可以通过 relay 进行业务。

步骤 610、WD 对通信响应进行完整性验证，根据生成密钥所需的安全参数生成密钥。

5 可选地，通信响应中包括远端设备的移动性管理实体生成的第二 NAS 消息，则具体的，WD 对通信响应中的第二 NAS 消息进行完整性验证。

可选地，在步骤 606 中，MME-WD 生成的（第一）密钥可以直接作为 PC5 口通信密钥用于 PC5 口的通信保护，即 Relay 根据接收到的（第一）密钥直接对通信响应进行安全保护（如，完整性保护），则相应地，WD 也根据接收到的生成密钥所需的安全参数生成（第一）密钥，即 PC5 口通信密钥，然后对通信响应消息进行安全验证（如，完整性验证）。
10 可选地，PC5 口通信密钥也可以为 Relay 根据步骤 606 中 MME-WD 所生成的（第一）密钥再进一步生成的（第二）密钥，即 Relay 根据接收到的（第一）密钥生成（第二）密钥，作为 PC5 口通信密钥，对通信响应进行安全保护（如，完整性保护），则相应地，WD 根据接收到的生成密钥所需的安全参数生成（第一）密钥后，再根据（第一）密钥生成（第二）密钥，该（第二）密钥即为 PC5 口通信密钥，然后对通信响应消息进行安全验证（如，完整性验证）。

可选的，关于远端设备和中继设备的关联关系可以采用好友列表或者业务类型的形式表示：

好友列表：比如，Relay ID: WD1 ID、WD2 ID、……。

20 业务类型：比如，WD ID: (relay service code1:service1-1,service1-2,...); (relay service code2:service2-1,service2-2,...); ……。

值得说明的是，上述关联关系还可以是其它类型的权限，本申请实施例不作限定。

此外，本申请的授权验证方法可能还需要注意如下几点：

25 可选地，第一：步骤 604 和步骤 606 中的关联关系验证，可能只需要执行其中一个，也可能两处都执行。

可选地，第二：用于保护远端设备和中继设备之间通信安全的密钥是可选的，即步骤 606 中可能不需要生成密钥。此时，上述第一随机数和第二随机数也不需要生成及传递，但是，远端设备的 NAS 消息和 MME-WD 的 NAS 消息还是需要传递的，作用是通过检查远端设备的 NAS 消息的完整性来完成 WD 和 relay 之间的安全认证。

30 可选地，第三：如果用于保护远端设备和中继设备之间通信安全的密钥需要生成，可选的，WD 和 MME-WD 之间的交互也可能不需要封装在 NAS 消息中，即第一随机数和 WD ID 不需要封装在远端设备的 NAS 消息中，第二随机数也不需要封装在 MME-WD 的 NAS 消息中。

35 可选地，第四：若 WD ID 不包含在通信请求中的远端设备的 NAS 消息中，则在步骤 604 和步骤 605 中，第一请求消息和第二请求中的远端设备的 NAS 消息中也不包括 WD ID，此时，步骤 605 中，WD ID 作为通信请求的一个信元。

本实施例中各步骤的实现原理参见图 1 至图 5 所示实施例中的相关记载，此处不再赘述。

图 7 为本申请实施例提供的授权验证方法实施例七的交互图。如图 7 所示，本申请实

施例提供的授权验证方法与图 6 所示实施例类似，区别仅在于 PF 也可进行授权验证。可选的，如图 7 所示，上述图 6 中的步骤 604 可替换为步骤 701~703，步骤 606 替换为步骤 704。

步骤 701、MME-relay 根据第一请求消息向 PF 发送第三请求消息。

5 其中，第三请求消息包括：远端设备的标识、中继设备的标识。可选的，第三请求消息中还包括中继服务码。

步骤 702、PF 对 Relay 和 WD 的关联关系进行验证并生成第三响应消息。

具体的，PF 根据第三请求消息对 Relay 和 WD 的关联关系进行验证。可选的，网络中用户数据管理实体和/或近距离功能实体中均存储有中继设备与远端设备相关的第一授权信息以及远端设备与中继设备相关的第二授权信息，因此，当 PF 接收到第三请求消息后，其根据远端设备的标识和中继设备的标识对中继设备与远端设备的关联关系进行验证。

步骤 703、PF 向 MME-relay 反馈第三响应消息。

该第三响应消息是 PF 验证的结果。

15 步骤 704、MME-WD 验证第二请求消息的完整性，并生成用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数。

关于 MME-WD 对第二请求消息完整性的验证和密钥的生成方法参见图 5 所示实施例中步骤 501 和步骤 502 中的记载，此处不再赘述。

20 值得说明的是，本申请的授权验证方法除了需要注意图 6 所示实施例需要注意的几点之外，还需要注意：

Relay APP ID(中继设备客户端的标识)：WD1 app ID(第一远端设备客户端的标识)、WD2 app ID、……。

可选的，图 8 为本申请实施例提供的授权验证方法实施例八的流程图。如图 8 所示，本申请实施例提供的授权验证方法，包括：

25 步骤 801、网络侧设备接收中继设备发送的第一请求消息。

该第一请求消息包括：远端设备的标识。

步骤 802、网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证。

30 步骤 803、该网络侧设备在判断上述关联关系验证通过后，向中继设备发送第一响应消息。

值得说明的是，当上述实施例中远端设备的移动管理实体和中继设备的移动管理实体集成到同一个移动管理实体上时，可以将上述远端设备的移动管理实体和中继设备的移动管理实体称为网络侧设备，也即，本实施例中的网络侧设备可通过远端设备的移动管理实体、中继设备的移动管理实体其中的任意一个实现。

35 可选的，在本申请的另一实施例中，该网络侧设备也可通过近距离功能实体实现。

在本申请实施例中，中继设备的移动管理实体根据接收到的中继设备发送的第一请求消息触发对远端设备和中继设备的关联关系的验证，具体参见图 1 所示实施例中步骤 101 至步骤 106 的记载，远端设备的移动管理实体对远端设备和中继设备的关联关系的验证，具体参见图 1 所示实施例中步骤 105a 至步骤 105d 的记载，其实现原理和技术效果与

图 1 所示实施例中的远端设备的移动管理实体、中继设备的移动管理实体的实现方案类似，此处不再赘述。近距离功能实体对远端设备和中继设备的关联关系的验证与中继设备的移动管理实体、远端设备的验证方法类似，此处也不再赘述。

可选的，在图 8 所示实施例的基础上，图 9 为本申请实施例提供的授权验证方法实施例九的流程图。如图 9 所示，在本申请实施例提供的授权验证方法中，上述步骤 802（网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证），包括：

步骤 901、网络侧设备根据第一请求消息，获取第一授权信息。

具体的，在中继设备、远端设备成功注册到网络之后，该网络侧设备根据第一请求消息，从用户数据管理实体和/或近距离功能实体获取第一授权信息。

在一种实施例中，当该网络侧设备为中继设备的移动管理实体时，该网络侧设备在中继设备成功注册到网络之后，根据中继设备的标识从用户数据管理实体和/或近距离功能实体获取第一授权信息，此时，第一授权信息指的是中继设备的授权信息。可选的，中继设备的授权信息的具体获取方法参见步骤 201 中的记载，此处不再赘述。

在另一种实施例中，当该网络侧设备为远端设备的移动管理实体时，该网络侧设备在远端设备成功注册到网络之后，根据远端设备的标识从用户数据管理实体和/或近距离功能实体获取该第一授权信息，此时，第一授权信息指的是远端设备的授权信息。可选的，远端设备的授权信息的具体获取方法参见步骤 401 中的记载，此处不再赘述。

在再一种实施例中，当该网络侧设备为近距离功能实体时，该网络侧设备在远端设备、中继设备成功注册到网络之后，根据中继设备的标识、远端设备的标识分别从用户数据管理实体和/或近距离功能实体获取第一授权信息，此时，第一授权信息既包括远端设备的授权信息，也包括中继设备的授权信息。

步骤 902、网络侧设备根据远端设备的标识、中继设备的标识以及第一授权信息，验证是否允许远端设备通过所述中继设备接入网络。

本实施例的技术方案，与图 2 所示实施例中中继设备验证是否允许远端设备通过中继设备接入网络的技术方案，或者与图 4 所示实施例中远端设备验证是否允许远端设备通过中继设备接入网络的技术方案类似，具体参见图 2 和图 4 所示实施例中的记载，此处不再赘述。

进一步的，当上述第一请求消息，还包括：中继服务码时，上述步骤 802（网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证）可替换为如下步骤：

网络侧设备根据远端设备的标识、中继设备的标识、中继服务码以及第一授权信息，验证是否允许远端设备通过中继设备接入网络。

可选的，在网络侧设备为中继设备的移动管理实体时，该步骤的具体实现方案参见步骤 202 中的记载，在网络侧设备为远端设备的移动管理实体时，该步骤的具体实现方案参见步骤 402 中的记载，近距离功能实体的验证方法类似，具体可参见图 2 和图 4 所示实施例中的记载，此处不再赘述。

作为一种示例，在图 8 所示的实施例中，上述步骤 802（网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证），可包括如下步骤：

网络侧设备向第一移动管理实体发送第二请求消息，以使第一移动管理实体根据该

第二请求消息验证是否允许远端设备通过中继设备接入网络。

在本实施例中，当网络侧设备通过不同方式实现时，第一移动管理实体也不相同，关于多种可能组合方式具体如下：

第一种方式：网络侧设备为中继设备的移动管理实体时，该第一移动管理实体为近
5 距离功能实体或远端设备的移动管理实体；或者

第二种方式：网络侧设备为远端设备的移动管理实体时，该第一移动管理实体为近
距离功能实体或中继设备的移动管理实体；或者

第三种方式：网络侧设备为近距离功能实体时，第一移动管理实体为远端设备的移
动管理实体或中继设备的移动管理实体。

10 该步骤是远端设备和中继设备的关联关系验证在中继设备的移动管理实体、远端设备的移动管理实体或者近距离功能实体中的任意两处执行时的方案，每处验证操作的均相互独立，具体验证方法参见图 9 所示实施例中的记载，此处不再赘述。

可选的，在本申请图 8 或图 9 中的任一实施例中，在第一请求消息中包括远端设备的
15 非接入层消息以及非接入层消息的校验码时，第二请求消息中也包括：远端设备的非接入层消息、该非接入层消息的校验码。

相应的，上述步骤 802（网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证），包括：

网络侧设备向远端设备的移动管理实体发送第二请求消息，以使远端设备的移动管理
实体根据该第二请求消息对远端设备进行安全处理。

20 其中，该网络侧设备为中继设备的移动管理实体，或者该网络侧设备为近距离功能实体。

当网络侧设备为中继设备的移动管理实体或近距离功能实体中的任意一个时，中继设备的移动管理实体或近距离功能实体还向远端设备的移动管理实体发送第二请求消息，从而使远端设备的移动管理实体根据该第二请求消息对远端设备进行安全处理。对远端设备的安全处理参见图 1 所示实施例中步骤 105a 至步骤 105d 中的记载，此处不再赘述。
25

可选的，在本申请图 8 或图 9 中的任一实施例中，作为一种示例，若网络侧设备为远端设备的移动管理实体，则上述步骤 801（网络侧设备接收中继设备发送的第一请求消息）通过如下可能实现方式实现：

30 网络侧设备接收中继设备通过基站转发处理的第一请求消息，该第一请求消息还包括：中继设备的标识。

在一种可行实现方式中，中继设备还可将第一请求消息发送给基站，经过基站选择对应的远端设备的移动管理实体，并通过初始远端设备信息上报远端设备的标识、中继设备的标识等相关内容。

当网络侧设备为远端设备的移动管理实体，且第一请求消息包括远端设备的非接入
35 层消息以及非接入层消息的校验码时，上述步骤 802（网络侧设备根据该第一请求消息，触发对远端设备和中继设备的关联关系的验证）的一种可能实现方式如下：

网络侧设备根据远端设备的标识，获取该远端设备的非接入层上下文信息，并根据非接入层上下文信息对非接入层消息的校验码进行验证。

具体的，远端设备和远端设备的移动管理实体之间约定有一套完整性保护密钥和一

套 NAS 算法、NAS 消息计算器（上行和下行），远端设备的移动管理实体将完整性保护密钥、NAS 消息计算器的数值、NAS 消息本身等作为 NAS 算法的输入，其会生成一个校验值（mac-integrity），置于 NAS 消息的末尾。同理，远端设备也执行上述 NAS 算法的操作，也会产生一个校验值，远端设备将这两个校验值进行比较，若两者一致，则表明完整性校验通过，否则表明完整性校验未通过。

可选的，由于近距离功能实体和远端设备的移动管理实体均能够根据远端设备的标识生成用于保护远端设备和中继设备之间通信安全的密钥，那么，当网络侧设备为中继设备的移动管理实体时，将近距离功能实体和远端设备的移动管理实体上位成第一移动管理实体进行说明，故本申请实施例提供的授权验证方法，还包括如下步骤，具体参见图 10 所示实施例。

图 10 为本申请实施例提供的授权验证方法实施例十的流程图。如图 10 所示，本申请实施例提供的授权验证方法，还包括：

步骤 1001、网络侧设备向第一移动管理实体发送第二请求消息。

步骤 1002、该第一移动管理实体根据第二请求消息中远端设备的标识，获取远端设备的非接入层上下文信息，并根据该非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥。

步骤 1003、第一移动管理实体将该密钥和生成密钥所需的安全参数反馈给网络侧设备。

步骤 1004、网络侧设备将接收到的密钥和生成密钥所需的安全参数发送给中继设备。

步骤 1005、中继设备将生成密钥所需的安全参数返回给远端设备。

步骤 1006、远端设备根据接收到的安全参数生成用于保护远端设备和中继设备之间通信安全的所述密钥。

本实施例提供的授权验证方法，以第一移动管理实体（近距离功能实体或远端设备的移动管理实体）生成用于保护远端设备和中继设备之间通信安全的密钥进行说明，其实现原理与有益效果与图 5 所示实施例的技术方案类似，具体参见图 5 所示实施例，此处不再赘述。

可选的，当网络侧设备为远端设备的移动管理实体或者近距离功能实体时，其自身可执行密钥生成的方式，具体操作如下所示：

网络侧设备根据远端设备的标识，获取远端设备的非接入层上下文信息，并根据该非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥，以及将密钥和生成密钥所需的安全参数反馈给中继设备的移动管理实体并转发给中继设备，以使中继设备将该安全参数返回给远端设备，进而使远端设备根据安全参数生成用于保护远端设备和中继设备之间通信安全的密钥。

其中，网络侧设备为远端设备的移动管理实体或者近距离功能实体。

可选的，上述密钥由远端设备的移动管理实体根据远端设备的基础安全密钥生成。

此外，中继设备的移动管理实体中存储有中继设备的上下文信息，远端设备的移动管理实体中存储有远端设备的上下文信息，近距离功能实体中存储有中继设备的上下文

信息和远端设备的上下文信息。

进一步的，在上述各实施例的基础上，本申请实施例提供的授权验证方法，还包括：

网络侧设备向安全功能实体发送密钥请求消息，以使得该安全功能实体根据密钥请求消息，获取用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数，并将密钥和生成密钥所需的安全参数反馈给网络侧设备，该密钥请求消息，包括：远端设备的标识。

该步骤是在网络侧设备判断出远端设备和中继设备的关联关系验证通过，但网络侧设备最后得到的响应消息中未携带用于保护远端设备和中继设备两者通信安全的密钥以及生成密钥所需的安全参数，那么，其则直接向安全功能实体发送密钥请求消息，进而使安全功能实体获取用于保护远端设备和中继设备之间通信安全的密钥和生成密钥所需的安全参数，从而保证远端设备可通过该中继设备接入网络。

下面结合上述实施例，列举详细的示例对授权验证方法进行具体说明：

与图 6 和图 7 所示实施例类似，以下各图中远端设备为可穿戴设备（WD）、中继设备（Relay）、远端设备的移动管理实体（MME-WD）、中继设备的移动管理实体（MME-relay）、基站（eNB）、归属用户服务器（Home Subscriber Server，简称 HSS）以及近距离功能实体（ProSe Function，简称 PF）等进行说明。

图 11 为本申请实施例提供的授权验证方法实施例十一的交互图。如图 11 所示，本申请实施例提供的授权验证方法与图 6 所示实施例类似，具体步骤如下：

步骤 1101、WD 和 Relay 成功注册到网络。

步骤 1102、WD 向 Relay 发送通信请求。

该通信请求中携带远端设备的标识（WD ID）。可选的，该通信请求中还包括第一 NAS 消息（WD 的 NAS 消息）和/或中继服务码（Relay service code）。关于通信请求中的具体内容参见图 1 所示实施例中步骤 101 中的记载，此处不再赘述。

步骤 1103、Relay 给基站（eNB）发送 RRC 信令。

其中，RRC 信令中包括上述通信请求中的相关内容。可选的，RRC 信令中还包括 relay 的标识。

步骤 1104、eNB 发起与 MME-WD 的 S1-AP 连接建立，并通过初始远端设备消息将 RRC 信令中的相关内容发送给 MME-WD。

步骤 1105、MME-WD 验证第一 NAS 消息的完整性，对 Relay 和 WD 的关联关系进行验证。

可选的，MME-WD 接收到第一 NAS 消息之后的具体操作可参见图 6 所示实施例中步骤 604 的记载，此处不再赘述。当通信请求中包括第一 NAS 消息时，MME-WD 验证第一 NAS 消息的完整性。关于完整性校验的具体实现参见步骤 403 中的记载此处不再赘述。

步骤 1106、MME-WD 向 MME-relay 发送 WD ID、Relay ID。

可选的，MME-WD 还可能向 MME-relay 发送包含验证 Relay 和 WD 的关联关系所需要的其他相关参数。此外，MME-WD 还可能向 MME-relay 发送中继服务码等内容。

步骤 1107、MME-relay 对 Relay 和 WD 的关联关系进行验证，并向 MME-WD 反馈第二响应消息。

步骤 1108、MME-WD 生成密钥。

具体的，MME-WD 根据 WD ID 获取生成密钥所需的安全参数，然后生成用于保护 WD 和 Relay 之间通信安全的密钥。

关于密钥具体生成的方法以及所需要的安全参数具体可参见步骤 502 中的记载，此处不再赘述。

步骤 1109、MME-WD 将密钥和生成密钥所需的安全参数返回给 eNB。

可选的，MME-WD 通过初始上下文建立请求将密钥和生成密钥所需的安全参数返回给 eNB。

步骤 1110、eNB 建立 WD 和 Relay 的承载映射和绑定。

步骤 1111、eNB 将密钥和生成密钥所需的安全参数反馈给 Relay，eNB 与 Relay 之间实现无线控制协议连接配置。

步骤 1112、eNB 将生成密钥所需的安全参数反馈给 WD，eNB 与 WD 之间实现无线控制协议连接配置。

步骤 1113、WD 根据生成密钥所需的安全参数生成密钥。

步骤 1114、WD 向 eNB 发送无线控制协议连接配置完成的消息。

步骤 1115、eNB 向 MME-WD 反馈初始上下文完成消息。

本实施例中各步骤的实现原理参见上述实施例中的相关记载，此处不再赘述。

值得说明的是，本申请的授权验证方法还可能需要注意如下几点：

可选的，第一：步骤 1105 和步骤 1107 中的关联关系验证，可能只需要执行其中一个，也可能两处都执行。

可选的，第二：用于保护远端设备和中继设备之间通信安全的密钥是可选的，即步骤 1108 中可能不需要生成密钥。此时，WD 生成的第一随机数和 MME-WD 生成的第二随机数也不需要生成及传递，但是，远端设备的 NAS 消息和 MME-WD 的 NAS 消息还是需要传递的，作用是通过检查远端设备的 NAS 消息的完整性来完成 WD 和 relay 之间的安全认证。

可选的，第三：如果用于保护远端设备和中继设备之间通信安全的密钥需要生成，可选的，WD 和 MME-WD 之间的交互也可能不需要封装在 NAS 消息中，即第一随机数和 WD ID 不需要封装在远端设备的 NAS 消息中，第二随机数也不需要封装在 MME-WD 的 NAS 消息中。

可选的，第四：若 WD ID 不包含在通信请求中的远端设备的 NAS 消息中，则在步骤 604 和步骤 605 中，第一请求消息和第二请求中的远端设备的 NAS 消息中也不包括 WD ID。

图 12 为本申请实施例提供的授权验证方法实施例十二的交互图。如图 12 所示，本申请实施例提供的授权验证方法与图 11 所示实施例类似，区别仅在于 PF 也可进行授权验证。具体的，如图 12 所示，上述图 11 中的步骤 1106 可替换为步骤 1201、步骤 1107 可替换为步骤 1202。

步骤 1201、MME-WD 向 PF 发送 WD ID、Relay ID。

可选的，与上述步骤 1106 类似，MME-WD 还可能向 PF 发送包含验证 Relay 和 WD 的关联关系所需要的其他相关参数。此外，MME-WD 还可能向 MME-relay 发送中继服务

码等内容。

步骤 1202、PF 对 Relay 和 WD 的关联关系进行验证，并向 MME-WD 反馈第二响应消息。

关于 PF 对 Relay 和 WD 的关联关系验证的具体实现方案参见上述步骤 702 中的记载，此处不再赘述。

值得说明的是，本申请实施例提供的授权验证方法，还可能需要注意如下几点：

可选的，第一：用于保护远端设备和中继设备之间通信安全的密钥是可选的，即步骤 1108 中可能不需要生成密钥。此时，WD 生成的第一随机数和 MME-WD 生成的第二随机数也不需要生成及传递，但是，远端设备的 NAS 消息和 MME-WD 的 NAS 消息还是需要传递的，作用是通过检查远端设备的 NAS 消息的完整性来完成 WD 和 relay 之间的安全认证。

可选的，第二：如果用于保护远端设备和中继设备之间通信安全的密钥需要生成，可选的，WD 和 MME-WD 之间的交互也可能不需要封装在 NAS 消息中，即第一随机数和 WD ID 不需要封装在远端设备的 NAS 消息中，第二随机数也不需要封装在 MME-WD 的 NAS 消息中。

可选的，第三：若 WD ID 不包含在通信请求中的远端设备的 NAS 消息中，则在步骤 604 和步骤 605 中，第一请求消息和第二请求中的远端设备的 NAS 消息中也不包括 WD ID。

图 13 为本申请实施例提供的授权验证方法实施例十三的交互图。如图 13 所示，本申请实施例提供的授权验证方法，具体步骤如下：

步骤 1301、WD 和 Relay 成功注册到网络。

步骤 1302、PF 或者 HSS 上发生了授权信息的更新。

可选的，PF 和/或 HSS 可能会发生 relay 相关的第一授权信息更新，和/或 WD 相关的第二授权信息更新。

步骤 1303、MME-WD 和/或 MME-relay 实现授权信息的更新。

可选的，PF 和/或 HSS 将更新的第一授权信息配置到 MME-relay 上。

可选的，PF 和/或 HSS 将更新的第二授权信息配置到 MME-WD 上。

步骤 1304、MME-WD 存储 WD 相关的第二授权信息。MME-relay 存储 relay 相关的第一授权信息。

步骤 1305、WD 和 Relay 之间实现通信接口的发现过程。

步骤 1306、WD 向 Relay 发送通信请求。

该通信请求中携带远端设备的标识（WD ID）。可选的，该通信请求中还包括第一 NAS 消息（WD 的 NAS 消息）和/或中继服务码（Relay service code）。关于通信请求中的其他内容参照图 1 所示实施例中步骤 101 的记载，此处不再赘述。

步骤 1307、Relay 生成第一请求消息，并将该第一请求消息发送给 PF。

步骤 1308、PF 对 Relay 和 WD 的关联关系进行验证，并生成密钥。

可选的，PF 接收到第一请求消息后，可执行如下操作中的一种或几种：第一，PF 对 Relay 和 WD 的关联关系进行验证；第二，PF 生成密钥。可选的，该密钥是用于保护 WD

和 Relay 之间通信的安全密钥。

步骤 1309、PF 将密钥和生成密钥所需的安全参数反馈给 Relay。

可选的，PF 通过第一响应消息将密钥和生成密钥所需的安全参数反馈给 Relay。

步骤 1310、Relay 将生成密钥所需的安全参数反馈给 WD。

5 在一实施例中，Relay 通过通信响应将生成密钥所需的安全参数反馈给 WD。

步骤 1311、WD 向 MME-WD 发送服务请求。

可选的，该服务请求中携带 WD-ID、relay-ID。可选地，该服务请求中还携带中继服务码。

步骤 1312、MME-WD 对 Relay 和 WD 的关联关系进行验证。

10 可选的，该步骤还可以通过 MME-relay 对 Relay 和 WD 的关联关系进行验证，或者该步骤通过 MME-WD 和 MME-relay 两者对 Relay 和 WD 的关联关系进行验证。

可选地，如果步骤 1308 中没有生成密钥，则 MME-WD 生成用于保护 WD 和 Relay 之间通信的安全密钥。

15 步骤 1313、MME-WD 向 eNB 发送建立初始上下文请求，该初始上下文请求中携带 WD-ID 和 relay-ID。

步骤 1314、eNB 完成 WD 和 Relay 的承载映射和绑定。

步骤 1315、eNB 与 Relay 之间实现无线控制协议连接配置。

步骤 1316、eNB 与 WD 之间实现无线控制协议连接配置。

步骤 1317、eNB 向 MME-WD 反馈初始上下文完成消息。

20 本实施例中各步骤的实现原理和技术效果参见上述所示实施例中的相关记载，此处不再赘述。

图 14 为本申请实施例提供的授权验证方法实施例十四的交互图。如图 14 所示，本申请实施例提供的授权验证方法与图 6 所示实施例类似，具体包括如下步骤：

步骤 1401、WD 和 Relay 成功注册到网络。

25 步骤 1402、WD 向 MME-WD 发送远端设备的 NAS 消息。

该远端设备的 NAS 消息中携带远端设备的标识（WD ID）、中继设备的标识（Relay ID）。可选地，该远端设备的 NAS 消息中还包括中继服务码（Relay service code）和/或第一随机数。

30 步骤 1403、MME-WD 验证远端设备的 NAS 消息的完整性，并对 Relay 和 WD 的关联关系进行验证。

可选的，MME-WD 可以执行如下操作中的一种或几种：验证远端设备的 NAS 消息的完整性、对 Relay 和 WD 的关联关系进行验证。

步骤 1404、MME-WD 向 MME-relay 发送第一授权验证请求消息。

35 步骤 1405、MME-relay 验证 Relay 和 WD 的关联关系，并向 MME-WD 反馈第一授权验证响应消息。

对于 MME-relay 验证 Relay 和 WD 的关联关系的具体实现参见图 1 所示实施例中步骤 105 中的记载，此处不再赘述。

步骤 1406、MME-WD 生成密钥。

具体的，MME-WD 根据 WD ID 生成用于保护 WD 和 Relay 之间通信安全的密钥和生

成密钥所需的安全参数。关于密钥生成的具体操作参见图 5 所示实施例中的步骤 502，此处不再赘述

步骤 1407、MME-WD 将密钥和生成密钥所需的安全参数返回给 eNB。

可选的，MME-WD 通过配对请求将密钥和生成密钥所需的安全参数返回给 eNB。

5 步骤 1408、eNB 建立 WD 和 Relay 的承载映射和绑定。

步骤 1409、eNB 将密钥和生成密钥所需的安全参数反馈给 Relay，eNB 与 Relay 之间实现无线控制协议连接配置。

步骤 1410、eNB 向 MME-WD 反馈配对响应。

步骤 1411、MME-WD 将生成密钥所需的安全参数反馈给 WD。

10 步骤 1412、WD 根据生成密钥所需的安全参数，生成密钥。

步骤 1413、WD 向 Relay 发送通信请求。

步骤 1414、Relay 向 WD 反馈通信响应。

值得说明的是，本申请的授权验证方法还可能需要注意如下几点：

15 可选的，第一：步骤 1403 和步骤 1405 中的关联关系验证，可能只需要执行其中一个，也可能两处都执行。

可选的，第二：用于保护远端设备和中继设备之间通信安全的密钥是可选的，即步骤 1406 中可能不需要生成密钥。此时，生成密钥所需要的 WD 生成的第一随机数和 MME-WD 生成的第二随机数也不需要生成及传递。

本实施例中各步骤的实现原理参见上述实施例中的相关记载，此处不再赘述。

20 图 15 为本申请实施例提供的授权验证方法实施例十五的交互图。如图 15 所示，本申请实施例提供的授权验证方法与图 14 所示实施例类似，区别仅在于 PF 也可进行授权验证。具体的，如图 15 所示，上述图 14 中的步骤 1403 可替换为步骤 1501~1504。

步骤 1501、MME-WD 验证远端设备的 NAS 消息的完整性。

25 关于 MME-WD 对远端设备的 NAS 消息的完整性验证参见图 5 所示实施例中步骤 501 中的记载，此处不再赘述。

步骤 1502、MME-WD 向 PF 发送第二授权验证请求消息。

MME-WD 根据远端设备的 NAS 消息向 PF 发送第二授权验证请求消息。

步骤 1503、PF 对 Relay 和 WD 的关联关系进行验证，生成第二授权验证响应消息。

可选的，PF 根据授权验证请求消息对 Relay 和 WD 的关联关系进行验证。

30 关于 PF 对 Relay 和 WD 的关联关系验证的具体实现方案参见上述步骤 702 中的记载，此处不再赘述。

步骤 1504、PF 向 MME-WD 反馈第二授权验证响应消息。

其中，第三请求消息中携带的内容与第一请求消息中的内容一致。

35 本实施例中各步骤的实现原理和技术效果参见图 1 至图 5 所示实施例中的相关记载，此处不再赘述。

图 16 为本申请实施例提供的一种授权验证装置的结构示意图。该装置可以位于中继设备的移动管理实体中，如图 16 所示，本实施例的装置可以包括：接收模块 1601、处理模块 1602 和发送模块 1603。

其中，接收模块 1601，用于接收中继设备发送的第一请求消息，该第一请求消息包括：远端设备的标识。

处理模块 1602，用于根据所述第一请求消息，触发对所述远端设备和所述中继设备的关联关系的验证。

5 发送模块 1603，用于在处理模块 1602 判断所述关联关系验证通过后，生成第一响应消息，向所述中继设备发送所述第一响应消息。

该发送模块 1603，还用于向所述远端设备的移动管理实体发送第二请求消息，所述第二请求消息包括：远端设备的标识。

10 该接收模块 1601，还用于接收所述远端设备的移动管理实体根据所述第二请求消息对所述远端设备进行安全处理后发送的第二响应消息。

本实施例的装置，可以用于执行图 1 所示方法实施例中中继设备的移动管理实体的技术方案，其实现原理和技术效果类似，此处不再赘述。

15 可选的，所述处理模块 1602，具体用于根据所述第一请求消息获取第一授权信息，并根据所述远端设备的标识、所述中继设备的标识以及所述第一授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

可选的，所述处理模块 1602，具体用于在所述中继设备成功注册到网络之后，根据所述中继设备的标识从用户数据管理实体和近距离功能实体中的任意一个或两个中获取所述第一授权信息。

20 进一步的，在上述第一请求消息，还包括：中继服务码时，上述处理模块 1602，具体用于根据所述第一请求消息获取第一授权信息，并根据所述远端设备的标识、所述中继设备的标识、所述中继服务码以及所述第一授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

作为一种示例，所述接收模块 1601，还用于接收所述远端设备的移动管理实体发送的密钥和生成所述密钥所需的安全参数。

25 所述发送模块 1603，还用于将所述密钥和生成所述密钥所需的安全参数发送给所述中继设备。

30 可选的，在一实施例中，所述发送模块 1603，还用于向安全功能实体发送密钥请求消息，以使得所述安全功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给所述中继设备的移动管理实体，所述密钥请求消息，包括：所述远端设备的标识。

所述发送模块 1603，还用于将所述密钥和生成所述密钥所需的安全参数发送给所述中继设备。

35 可选的，在另一实施例中，所述发送模块 1603，还用于向近距离功能实体发送第三请求消息，以使所述近距离功能实体根据所述第三请求消息验证是否允许所述远端设备通过所述中继设备接入网络，所述第三请求消息包括：远端设备的标识、中继设备的标识。

进一步的，在上述各实施例中，当第一请求消息还包括：远端设备的非接入层消息、非接入层消息的校验码时，所述第二请求消息还包括：所述远端设备的非接入层消

息、所述非接入层消息的校验码。

上述装置可用于执行上述方法实施例提供的方法，具体实现方式和技术效果类似，这里不再赘述。

5 图 17 为本申请实施例提供的另一种授权验证装置的结构示意图。该装置可以位于远端设备的移动管理实体中。如图 17 所示，本实施例的装置可以包括：接收模块 1701、处理模块 1702 和发送模块 1703。

该接收模块 1701，用于接收中继设备的移动管理实体发送的第二请求消息，所述第二请求消息包括：远端设备的标识。

10 处理模块 1702，用于所述远端设备的移动管理实体根据所述第二请求消息对所述远端设备进行安全处理。

发送模块 1703，用于在所述处理模块 1702 对所述远端设备进行安全处理后，向所述中继设备的移动管理实体发送的第二响应消息。

本实施例的装置，可以用于执行图 1 所示方法实施例中远端设备的移动管理实体的技术方案，其实现原理和技术效果类似，此处不再赘述。

15 可选的，在一实施例中，所述处理模块 1702，具体用于根据所述第二请求消息获取第二授权信息，并根据所述远端设备的标识、所述中继设备的标识以及所述第二授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

20 作为一种示例，该处理模块 1702，具体用于在所述远端设备成功注册到网络之后，根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述第二授权信息。

25 可选的，在另一实施例中，当第二请求消息，还包括：中继服务码时，所述处理模块 1702，用于根据所述第二请求消息获取第二授权信息，并根据所述远端设备的标识、所述中继设备的标识、所述中继服务码以及所述第二授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

30 可选的，在再一实施例中，所述处理模块 1702，具体用于根据所述第二请求消息中的所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并根据所述非接入层上下文信息对所述远端设备的非接入层消息的校验码进行验证，所述第二请求消息包括：所述远端设备的非接入层消息、所述非接入层消息的校验码以及所述远端设备的标识。

可选的，在又一实施例中，所述处理模块 1702，还用于根据所述第二请求消息中所述远端设备的标识，获取所述远端设备的非接入层上下文信息，根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥；

35 所述发送模块 1703，还用于将所述密钥和生成所述密钥所需的安全参数发送给所述中继设备的移动管理实体。

可选的，在又一实施例中，所述发送模块 1703，还用于向安全功能实体发送密钥请求消息，以使得所述安全功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给所述远端设备的移动管理实体，所述密钥请求消

息，包括：所述远端设备标识。

上述装置可用于执行上述方法实施例提供的方法，具体实现方式和技术效果类似，这里不再赘述。

5 图 18 为本申请实施例提供的再一种授权验证装置的结构示意图。该装置可以位于中继设备中。如图 18 所示，本实施例的装置可以包括：接收模块 1801、处理模块 1802 和发送模块 1803。

接收模块 1801，用于接收远端设备发送的通信请求，所述通信请求包括：远端设备的标识。

10 处理模块 1802，用于根据所述通信请求，生成第一请求消息，所述第一请求消息包括：远端设备的标识。

发送模块 1803，用于将所述第一请求消息发送给所述中继设备的移动管理实体。

所述接收模块 1801，还用于接收所述中继设备的移动管理实体在判断所述关联关系验证通过后发送的第一响应消息。

15 所述发送模块 1803，还用于根据所述第一响应消息向所述远端设备发送通信响应。

本实施例的装置，可以用于执行图 1 所示方法实施例中中继设备的技术方案，其实现原理和技术效果类似，此处不再赘述。

20 可选的，在本申请的一实施例中，所述接收模块 1801，还用于接收所述中继设备的移动管理实体发送的用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

所述发送模块 1803，还用于将所述安全参数通过所述通信响应发送给所述远端设备，以使所述远端设备根据所述安全参数生成用于保护所述远端设备和所述中继设备之间通信安全的所述密钥。

25 上述装置可用于执行上述方法实施例提供的方法，具体实现方式和技术效果类似，这里不再赘述。

30 图 19 为本申请实施例提供的又一种授权验证装置的结构示意图。该装置可以位于中继设备的移动管理实体中，也可以位于远端设备的移动管理实体，还可以位于近距离功能实体中。如图 19 所示，本实施例的装置可以包括：接收模块 1901、处理模块 1902 和发送模块 1903。

接收模块 1901，用于接收中继设备发送的第一请求消息，所述第一请求消息包括：远端设备的标识；

处理模块 1902，用于根据所述第一请求消息，触发对所述远端设备和所述中继设备的关联关系的验证；

35 发送模块 1903，用于在所述处理模块 1902 判断所述关联关系验证通过后，向所述中继设备发送第一响应消息。

可选的，在本申请的一实施例中，所述处理模块 1902，具体用于根据第一请求消息，获取第一授权信息，并根据所述远端设备的标识、所述中继设备的标识以及所述第一授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

作为一种示例，所述处理模块 1902，具体用于在所述中继设备、所述远端设备成功注册到网络之后，根据第一请求消息，从用户数据管理实体和近距离功能实体中的任意一个或两个中获取所述第一授权信息。

可选的，在本申请的另一实施例中，当所述第一请求消息，还包括：中继服务码时，所述处理模块 1902，具体用于根据第一请求消息，获取第一授权信息，并根据所述远端设备的标识、所述中继设备的标识、所述中继服务码以及所述第一授权信息，验证是否允许所述远端设备通过所述中继设备接入网络。

可选的，在本申请的再一实施例中，所述发送模块 1903，还用于向第一移动管理实体发送第二请求消息，以使所述第一移动管理实体根据所述第二请求消息验证是否允许所述远端设备通过所述中继设备接入网络。

在该实施例中，当该授权验证装置位于中继设备的移动管理实体中时，所述第一移动管理实体为近距离功能实体或所述远端设备的移动管理实体；或者当该授权验证装置位于远端设备的移动管理实体中时，所述第一移动管理实体为近距离功能实体或所述中继设备的移动管理实体；或者当该授权验证装置位于近距离功能实体时，所述第一移动管理实体为所述远端设备的移动管理实体或所述中继设备的移动管理实体。

可选的，在本申请的又一实施例中，在第一请求消息中包括所述远端设备的非接入层消息以及所述非接入层消息的校验码时，所述第二请求消息包括：所述远端设备的非接入层消息、所述非接入层消息的校验码以及所述远端设备的标识时，所述处理模块 1902，用于向所述远端设备的移动管理实体发送第二请求消息，以使所述远端设备的移动管理实体根据所述第二请求消息对所述远端设备进行安全处理。

在本实施例中，该授权验证装置可以位于中继设备的移动管理实体中，或者该授权验证装置可以位于近距离功能实体中。

可选的，在本申请的又一实施例中，当该授权验证装置位于远端设备的移动管理实体中时，所述接收模块 1901，具体用于接收所述中继设备通过所述基站转发处理的所述第一请求消息，所述第一请求消息还包括：所述中继设备的标识。

可选的，在本申请的上述实施例中，当所述第一请求消息包括所述远端设备的非接入层消息以及所述非接入层消息的校验码时，所述处理模块 1902，具体用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并根据所述非接入层上下文信息对所述非接入层消息的校验码进行验证。

可选的，在本申请的又一实施例中，所述发送模块 1903，还用于向所述第一移动管理实体发送第二请求消息，以使所述第一移动管理实体根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，以及将所述密钥和生成所述密钥所需的安全参数反馈给该授权验证装置。

所述发送模块 1903，还用于将所述密钥和生成所述密钥所需的安全参数发送给所述中继设备，以使所述中继设备将所述安全参数返回给所述远端设备，使所述远端设备根据所述安全参数生成用于保护所述远端设备和所述中继设备之间通信安全的所述密钥。

在本实施例中，该授权验证装置可以位于中继设备的移动管理实体中，所述第一移动管理实体为近距离功能实体或所述远端设备的移动管理实体。

可选的，在本申请的又一实施例中，所述处理模块 1902，还用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，以及将所述密钥和生成所述密钥所需的安全参数反馈给所述中继设备的移动管理实体并转发给所述中继设备，以使所述中继设备将所述安全参数返回给所述远端设备，使所述远端设备根据所述安全参数生成用于保护所述远端设备和所述中继设备之间通信安全的所述密钥。

在本实施例中，该授权验证装置可以位于远端设备的移动管理实体或者近距离功能实体中。

可选的，在本申请的上述实施例中，所述密钥由所述远端设备的移动管理实体根据所述远端设备的基础安全密钥生成。

可选的，在本申请的上述实施例中，所述中继设备的移动管理实体中存储有所述中继设备的上下文信息，所述远端设备的移动管理实体中存储有所述远端设备的上下文信息，近距离功能实体中存储有所述中继设备的上下文信息和所述远端设备的上下文信息。

可选的，在本申请的又一实施例中，所述发送模块 1903，还用于向安全功能实体发送密钥请求消息，以使得所述安全功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给所述网络侧设备，所述密钥请求消息，包括：所述远端设备的标识。

另外，本申请实施例提供的授权验证装置，还可以实现上述各种可选实施例中用于授权验证装置的方法的各个步骤，具体实现原理和有益效果请参照上述方法实施例，此处不再赘述。

需要说明的是，应理解以上装置的各个模块的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。且这些模块可以全部以软件通过处理元件调用的形式实现；也可以全部以硬件的形式实现；还可以部分模块通过处理元件调用软件的形式实现，部分模块通过硬件的形式实现。例如，确定模块可以为单独设立的处理元件，也可以集成在上述装置的某一个芯片中实现，此外，也可以以程序代码的形式存储于上述装置的存储器中，由上述装置的某一个处理元件调用并执行以上确定模块的功能。其它模块的实现与之类似。此外这些模块全部或部分可以集成在一起，也可以独立实现。这里所述的处理元件可以是一种集成电路，具有信号的处理能力。在实现过程中，上述方法的各步骤或以上各个模块可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。

例如，以上这些模块可以是被配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路（Application Specific Integrated Circuit，简称 ASIC），或，一个或多个微处理器（digital signal processor，简称 DSP），或，一个或者多个现场可编程门阵列（Field Programmable Gate Array，简称 FPGA）等。再如，当以上某个模块通过处理元件调度程序代码的形式实现时，该处理元件可以是通用处理器，例如中央处理器（Central Processing Unit，简称 CPU）或其它可以调用程序代码的处理器。再如，这些模块可以集成在一起，以片上系统（system-on-a-chip，简称 SOC）的形式实现。

图 20 为本申请实施例提供的又一种授权验证装置的结构示意图。本实例提供的授权验证装置，包括：处理器 2001、存储器 2002、收发器 2003、通信接口 2004 和系统总线 2005，存储器 2002 和通信接口 2004 通过系统总线 2005 与处理器 2001 和收发器 2003 连接并完成相互间的通信，存储器 2002 用于存储计算机执行指令，通信接口 2004 用于和其他设备进行通信，处理器 2001 和收发器 2003 用于运行计算机执行指令，使授权验证装置执行如上应用于授权验证方法中中继设备的移动管理实体的各个步骤。

具体的，在上述图 16 中，接收模块 1601 和发送模块 1603 对应收发器 2003，处理模块 1602 对应处理器 2001 等。

图 21 为本申请实施例提供的又一种授权验证装置的结构示意图。本实例提供的授权验证装置，包括：处理器 2101、存储器 2102、收发器 2103、通信接口 2104 和系统总线 2105，存储器 2102 和通信接口 2104 通过系统总线 2105 与处理器 2101 和收发器 2103 连接并完成相互间的通信，存储器 2102 用于存储计算机执行指令，通信接口 2104 用于和其他设备进行通信，处理器 2101 和收发器 2103 用于运行计算机执行指令，使授权验证装置执行如上应用于授权验证方法中远端设备的移动管理实体的各个步骤。

具体的，在上述图 17 中，接收模块 1701 和发送模块 1703 对应收发器 2103，处理模块 1702 对应处理器 2101 等。

图 22 为本申请实施例提供的又一种授权验证装置的结构示意图。本实例提供的授权验证装置，包括：处理器 2201、存储器 2202、收发器 2203、通信接口 2204 和系统总线 2205，存储器 2202 和通信接口 2204 通过系统总线 2205 与处理器 2201 和收发器 2203 连接并完成相互间的通信，存储器 2202 用于存储计算机执行指令，通信接口 2204 用于和其他设备进行通信，处理器 2201 和收发器 2203 用于运行计算机执行指令，使授权验证装置终端认证装置执行如上应用于授权验证方法中中继设备的各个步骤。

具体的，在上述图 18 中，接收模块 1801 和发送模块 1803 对应收发器 2203，处理模块 1802 对应处理器 2201 等。

图 23 为本申请实施例提供的又一种授权验证装置的结构示意图。本实例提供的授权验证装置，包括：处理器 2301、存储器 2302、收发器 2303、通信接口 2304 和系统总线 2305，存储器 2302 和通信接口 2304 通过系统总线 2305 与处理器 2301 和收发器 2303 连接并完成相互间的通信，存储器 2302 用于存储计算机执行指令，通信接口 2304 用于和其他设备进行通信，处理器 2301 和收发器 2303 用于运行计算机执行指令，使授权验证装置执行如上应用于授权验证方法中网络侧设备的各个步骤。

具体的，在上述图 19 中，接收模块 1901 和发送模块 1903 对应收发器 2303，处理模块 1902 对应处理器 2301 等。

上述图 20 至图 23 中提到的系统总线可以是外设部件互连标准（Peripheral Pomponent Interconnect, 简称 PCI）总线或扩展工业标准结构（Extended Industry Standard Architecture, 简称 EISA）总线等。该系统总线可以分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。通信接口用于实现数据库访问装置与其他设备（例如客户端、读写库和只读库）之间的通信。存储器可能包含随机存取存储器（Random Access Memory, 简称 RAM），也可能还包括非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。

上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，简称 CPU）、网络处理器（Network Processor，简称 NP）等；还可以是数字信号处理器（Digital Signal Processing，简称 DSP）、专用集成电路（Application Specific Integrated Circuit，简称 ASIC）、现场可编程门阵列（Field-Programmable Gate Array，简称 FPGA）或者其他
5 可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

可选的，图 24 为本申请实施例提供的授权验证方法实施例十六的交互图。如图 24 所示，本申请实施例提供的授权验证方法，包括：

步骤 2401、中继设备接收远端设备发送的通信请求。

10 作为一种示例，该通信请求中包括远端设备的非接入层（NAS）消息，可选的，该非接入层消息中包含远端设备的标识，可选的，远端设备的标识直接包含在该通信请求中。可选的，在中继设备与远端设备之间的通信接口（例如，PC5 口）的建立过程中，远端设备通过该通信请求将远端设备的 NAS 消息发送给中继设备。

15 作为另一种示例，该通信请求中并不包含远端设备的 NAS 消息，在中继设备与远端设备之间的通信接口（例如，PC5 口）的建立过程中或者建立过程结束之后，远端设备将远端设备的 NAS 消息发送给中继设备。

20 可选的，该通信请求中还可以包括以下内容中的一个或多个：中继服务码、第一随机数。可选的，该第一随机数是远端设备生成的，可以直接携带在通信请求中。可选地，在通信请求中包括远端设备的非接入层消息时，该第一随机数还可以包含在远端设备的非接入层消息中，而不是直接携带在通信请求中。

步骤 2402、中继设备根据上述通信请求生成第一无线资源控制消息，并将第一无线资源控制消息发送给基站。

25 可选的，所述第一无线资源控制消息为远端设备的无线资源控制消息，或者，所述第一无线资源控制消息为中继设备的无线资源控制消息。可选的，第一无线资源控制消息为无线资源控制（RRC）连接建立完成消息。

可选的，在一实施例中，中继设备接收到远端设备的通信请求之后，将该通信请求中的内容封装到第一无线资源控制信息中发送给基站。

30 在另一实施例中，中继设备除了将接收到的通信请求的内容封装到第一无线资源控制信息中，比如，远端设备的 NAS 消息；也可以将验证远端设备与中继设备关联关系所需要的其他相关参数整合到第一请求消息中，比如，第一无线资源控制信息中包括中继设备的标识等。

35 即，中继设备将该中继设备的标识通过第一无线资源控制消息发送给基站，以使基站识别远端设备请求通过中继设备接入网络。这样基站可以根据第一无线资源控制消息确定出中继设备的标识和远端设备的标识，并在识别出远端设备请求通过该中继设备接入网络时，向远端设备的移动管理实体发送初始设备消息，进而使远端设备的移动管理实体触发对中继设备和远端设备的关联关系的验证。

步骤 2403、基站接收中继设备发送的第一无线资源控制消息。

可选的，该第一无线资源控制消息包括远端设备的非接入层消息。

在本实施例中，当远端设备发送给中继设备的通信请求中包含远端设备的非接入层消

息时，该远端设备的非接入层消息将会被中继设备封装到第一无线资源控制信息中，从而基站接收到的该第一无线资源控制消息中也包含远端设备的非接入层消息。

步骤 2404、基站根据第一无线资源控制消息，识别出远端设备请求通过中继设备接入网络，获取中继设备的标识。

5 基站接收到该第一无线资源控制消息后，可以根据第一无线资源控制消息，识别出远端设备请求通过中继设备接入网络。例如，可选地，基站识别出接收到的第一无线资源控制消息是远端设备的无线资源控制消息，则判断远端设备请求通过中继设备接入网络；可选地，基站识别出第一无线资源控制消息是中继设备的无线资源控制消息，但包含了远端设备的标识，则判断远端设备请求通过中继设备接入网络。

10 可选的，基站识别出远端设备请求通过中继设备接入网络的同时，其将获取中继设备的标识，进而将中继设备的标识和远端设备的非接入层消息均发送给远端设备的移动管理实体，以触发远端设备的移动管理实体对远端设备和中继设备之间的关联关系进行验证。

在本申请实施例中，基站获取中继设备的标识可通过如下可能实现方式中的一种实现：

15 作为一种示例，当中继设备与基站建立连接之后，基站便会建立中继设备的上下文信息并存储起来，也即，基站中存储有该中继设备的上下文信息，包括中继设备的标识。所以，当基站根据第一无线资源控制消息识别出远端设备请求通过中继设备接入网络时，会触发基站从该基站存储的中继设备的上下文信息中获取中继设备的标识。

20 作为另一种示例，当中继设备将通信请求中的相关内容封装到第一无线资源控制消息中的同时，也将自己的标识封装到了该第一无线资源控制消息时，那么基站也可从该第一无线资源控制消息中获取中继设备的标识。

步骤 2405、基站通过初始设备消息将中继设备的标识和远端设备的非接入层消息发送给远端设备的移动管理实体。

25 在本实施例中，若想验证远端设备和中继设备的关联关系，基站则根据获取到的中继设备的标识和远端设备的非接入层消息生成远端设备的初始设备消息，进而通过该初始设备消息将中继设备的标识和远端设备的非接入层消息发送给远端设备的移动管理实体，进而使远端设备的移动管理实体触发对远端设备和中继设备的关联关系进行验证，关于实现关联关系验证的多种实现方式参见如下步骤 2407 中的记载，此处不再赘述。

30 对于远端设备的标识，该远端设备的标识可包含在第一无线资源控制消息中远端设备的非接入层消息中，和/或直接包含在第一无线资源控制消息中。因此，可选的，基站从第一无线资源控制消息中获取远端设备的标识并将其包含在初始设备消息中。所以，远端设备的标识可包含在初始设备消息中远端设备的非接入层消息中，和/或远端设备的标识直接包含在该初始设备消息中。

步骤 2406、远端设备的移动管理实体接收基站发送的初始设备消息。

35 可选的，该初始设备消息包括：远端设备的非接入层消息和中继设备的标识。

可选的，该初始设备消息还直接包括远端设备的标识。

步骤 2407、远端设备的移动管理实体根据该初始设备消息，触发对远端设备和中继设备的关联关系的验证。

可选的，远端设备的移动管理实体触发对远端设备和中继设备的关联关系进行验证，

包括如下可能实现方式中的一种或多种：第一种，触发远端设备的移动管理实体自身根据该初始设备消息对远端设备和中继设备的关联关系进行验证；第二种，触发远端设备的移动管理实体将远端设备的标识和中继设备的标识发送给中继设备的移动管理实体，以使中继设备的移动管理实体对上述关联关系进行验证；第三种，触发远端设备的移动管理实体将远端设备的标识和中继设备的标识发送给近距离功能实体，以使近距离功能实体对上述关联关系进行验证。

值得说明的是，当不需要执行上述第二种时，远端设备的移动管理实体不需要与中继设备的移动管理实体进行交互，当不需要执行上述第三种方式时，远端设备的移动管理实体不需要与近距离功能实体进行交互。

值得说明的是，当远端设备的移动管理实体执行如上可能实现方式中的多种时，本实施例并不限定多种可能实现方式的执行顺序，任意组合的执行顺序均属于申请的保护范围。

可选的，在本实施例中，当远端设备的标识包含在远端设备的非接入层消息中时，远端设备的移动管理实体可根据该非接入层消息中携带的远端设备的标识获取授权关系信息，该授权关系信息可以表示与该远端设备有关联关系的中继设备列表。因此，远端设备的移动管理实体可根据该初始设备消息对远端设备和中继设备的关联关系进行验证，具体的验证方法参见下述图 25 所示实施例中的记载，此处不再赘述。

可选的，在另一实施例中，远端设备和中继设备的关联关系还可由中继设备的移动管理实体进行验证。具体的，远端设备的移动管理实体向中继设备的移动管理实体发送第一验证请求消息，该第一验证请求消息包括：远端设备的标识和中继设备的标识，这样中继设备的移动管理实体便可根据第一验证请求消息对远端设备和中继设备的关联关系进行验证。值得说明的是，中继设备的移动管理实体中也存储有与该中继设备有关联关系的远端设备列表，故中继设备的移动管理实体便可结合远端设备的标识和中继设备的标识实现对远端设备和中继设备的关联关系验证。

可选的，在再一实施例中，远端设备和中继设备的关联关系还可由近距离功能实体进行验证。具体的，远端设备的移动管理实体向近距离功能实体发送第二验证请求消息，该第二验证请求消息包括：远端设备的标识、中继设备的标识，由于近距离功能实体中存储有与中继设备有关联关系的远端设备列表和/或与远端设备有关联关系的中继设备列表，所以，近距离功能实体也可实现对远端设备和中继设备的关联关系验证。

可选的，由于该初始设备消息中包括远端设备的非接入层消息，那么远端设备的移动管理实体还可根据远端设备的标识，获取远端设备的非接入层上下文信息，并对该远端设备的非接入层消息进行完整性校验。具体的，远端设备的移动管理实体根据该非接入层上下文信息对远端设备的非接入层消息的校验码进行验证。

举例来说，远端设备和远端设备的移动管理实体之间建立有一套完整性保护密钥和一套 NAS 算法、NAS 消息计算器（上行和下行），远端设备将完整性保护密钥、NAS 消息计算器的数值、NAS 消息本身等作为 NAS 算法的输入，其会生成一个校验值（mac-integrity），置于 NAS 消息的末尾。同理，远端设备的移动管理实体也执行上述 NAS 算法的操作，也会产生一个校验值，远端设备的移动管理实体将这两个校验值进行比较，若两者一致，则表明完整性校验通过，否则表明完整性校验未通过。

可选地，远端设备的移动管理实体还可以根据初始设备消息中的远端设备的标识，获取远端设备的非接入层上下文信息，并根据该非接入层上下文信息生成用于保护远端设备和中继设备之间通信安全的密钥，最后将密钥和生成密钥所需的安全参数通过初始上下文建立请求消息发送给基站。其中，远端设备的标识包含在 NAS 消息中或者直接包含在初始设备消息。

可选地，在判断远端设备和中继设备的关联关系验证通过时，但远端设备的 NAS 消息完整性校验没有通过，或者远端设备的 NAS 消息没有完整性保护，那么远端设备的移动管理实体则向安全功能实体发送密钥请求消息，以使得该安全功能实体根据密钥请求消息获取用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数，并将该密钥和生成密钥所需的安全参数反馈给远端设备的移动管理实体，该密钥请求消息，包括：远端设备标识。其中，可选的，所述安全功能实体可以为用户数据管理实体，认证服务器功能实体，可穿戴功能管理实体等。

步骤 2408、远端设备的移动管理实体在判断远端设备和中继设备的关联关系验证通过后向基站发送初始上下文建立请求消息。

可选的，在本实施例中，当远端设备和中继设备的关联关系验证通过后，远端设备的移动管理实体则向基站发送初始上下文建立请求消息，该初始上下文建立请求消息中包括中继设备的标识。

步骤 2409、基站接收上述初始上下文建立请求消息。

在本实施例中，由上述步骤 2408 可知，该初始上下文建立请求消息是远端设备的移动管理实体在判断出远端设备和中继设备的关联关系验证通过后发送的。

可选的，在远端设备的移动管理实体生成用于保护远端设备和中继设备之间通信安全的密钥时，远端设备的移动管理实体还向基站发送该用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数，相应的，该基站还接收中继设备的移动管理实体发送的用于保护远端设备和中继设备之间通信安全的密钥和生成该密钥所需的安全参数。

步骤 2410、基站根据上述初始上下文建立请求消息为远端设备建立上下文信息。

可选的，当基站接收远端设备的移动管理实体在判断出远端设备和中继设备的关联关系验证通过后发送的该初始上下文建立请求消息时，基站则根据接收到的初始上下文建立请求消息为远端设备建立上下文信息并存储远端设备的上下文信息。

可选的，基站还可根据该初始上下文建立请求消息，建立远端设备和中继设备的映射关系，从而为远端设备进行数据和信令的路由传输。可选的，进一步的，远端设备和中继设备的映射关系包括：远端设备和中继设备之间的数据无线承载（Data Radio Bearer, DRB）的映射关系，和/或远端设备和中继设备之间的信令无线承载（Signalling Radio Bearers, SRB）的映射关系。

步骤 2411、基站向中继设备发送第二无线资源控制消息。

可选的，基站通过该第二无线资源控制消息向中继设备反馈远端设备和中继设备之间的关联关系验证通过。作为一种示例，当远端设备的移动管理实体生成了用于保护远端设备和中继设备之间通信安全的密钥时，基站接收到的初始上下文建立请求消息中包含该密钥和生成该密钥的安全参数，那么基站向中继设备发送的第二无线资源控制消息中也可包

括该密钥，以使中继设备与远端设备生成的密钥进行对比，从而保护远端设备和中继设备之间的通信安全。

步骤 2412、中继设备接收上述第二无线资源控制消息，以根据第二无线资源控制消息确定允许远端设备通过中继设备接入网络。

5 可选的，中继设备根据基站发送的第二无线资源控制消息，建立远端设备和中继设备的映射关系，从而为远端设备进行数据和信令的路由传输。可选的，进一步的，所述远端设备和中继设备的映射关系包括：远端设备和中继设备之间的 DRB 的映射关系，和/或远端设备和中继设备之间的 SRB 的映射关系。

10 可选的，该第二无线资源控制消息，包括：用于保护所述远端设备和所述中继设备之间通信安全的密钥。这样中继设备可利用该密钥验证远端设备的密钥是否正确，以保证远端设备和中继设备之间的通信安全。

可选的，在本实施例中，该授权验证方法，还包括：如下步骤 2413。

步骤 2413、基站向远端设备发送第三无线资源控制消息。

15 远端设备接收到基站发送的第三无线资源控制消息后，远端设备可根据该第三无线资源控制消息生成用于保护远端设备和中继设备之间通信安全的密钥，其中，第三无线资源控制消息，包括：生成密钥所需的安全参数。

20 可选的，远端设备接收到该生成密钥所需的安全参数时，远端设备可根据接收到的生成密钥所需的安全参数生成一个密钥，远端设备基于该密钥对后续远端设备和中继设备之间的信令和数据进行安全保护，而中继设备基于从基站接收的密钥对远端设备和中继设备之间的信令和数据进行安全验证，包括解密和/或完整性保护。其中，当中继设备成功验证了远端设备的第一条信令的完整性校验后，中继设备确认成功认证了远端设备并且允许远端设备通过该中继设备接入网络。其中，所述远端设备的第一条信令为远端设备生成密钥后发送给中继设备的第一条信令。

25 本申请实施例提供的授权验证方法，中继设备根据从远端设备接收到的通信请求生成第一无线资源控制消息，将该第一无线资源控制消息发送给基站，基站接收包括远端设备的非接入层消息的第一无线资源控制消息，识别出远端设备请求通过该中继设备接入网络，并获取中继设备的标识，通过初始设备消息将中继设备的标识和远端设备的非接入层消息发送给远端设备的移动管理实体，触发该远端设备的移动管理实体根据该初始设备消息对远端设备和中继设备的关联关系进行验证，并在验证通过后向基站发送初始上下文建立请求消息，基站根据该初始上下文建立请求消息为远端设备建立上下文信息并向中继设备发送第二无线资源控制消息，从而使中继设备根据第二无线资源控制消息确定允许远端设备通过中继设备接入网络。该技术方案降低了网络配置需求、减少了网络开销、提高了授权验证效率。

35 在上述实施例的基础上，图 25 为本申请实施例提供的授权验证方法实施例十七的流程示意图。本实施例是对上述步骤 2407（远端设备的移动管理实体根据该初始设备消息，触发对远端设备和中继设备的关联关系的验证）中由远端设备的移动管理实体执行关联关系验证情况的详细说明。如图 25 所示，在本申请实施例提供的授权验证方法中，上述步骤 2407，包括：

步骤 2501、远端设备的移动管理实体根据远端设备的标识获取授权关系信息。

当远端设备的移动管理实体来验证远端设备和中继设备的关联关系时，其需要首先获取远端设备的上下文信息，进而从远端设备的上下文信息中获取与该远端设备有授权关系的中继设备列表，即授权关系信息。

5 可选的，在远端设备的移动管理实体接收基站发送的初始设备消息之前，该远端设备的移动管理实体根据远端设备的标识从用户数据管理实体和/或近距离功能实体获取上述授权关系信息，并将该授权关系信息存储在远端设备的移动管理实体中，这样远端设备的移动管理实体便能够根据远端设备的标识直接获取到获取授权关系信息。

10 可选的，网络中用户数据管理实体和/或近距离功能实体中均存储有远端设备与中继设备相关的授权关系信息。对于用户数据管理实体中存储的远端设备与中继设备相关的授权关系信息，远端设备的移动管理实体直接从用户数据管理实体（例如，归属用户服务器（Home Subscriber Server，简称 HSS），或者，5G 系统中的用户数据管理实体（User data management，简称 UDM））获取得到。而对于近距离功能实体中存储的授权关系信息：
15 当远端设备的移动管理实体可直接与近距离功能实体通信时，即两者之间存在直接接口，远端设备的移动管理实体可直接从近距离功能实体获取上述授权关系信息；而当远端设备的移动管理实体不能直接与近距离功能实体通信时，即两者之间不存在直接接口，则远端设备的移动管理实体通过 HSS 从近距离功能实体获取上述授权关系信息。

步骤 2502、远端设备的移动管理实体根据远端设备的标识、中继设备的标识以及上述授权关系信息，验证是否允许远端设备通过该中继设备接入网络。

20 其中，远端设备的标识包含在远端设备的非接入层消息中，和/或远端设备的标识包含在初始设备消息中。

可选的，当远端设备的移动管理实体获取到远端设备的标识、中继设备的标识以及授权关系信息后，其便可以对远端设备与中继设备的关联关系进行验证。即，当授权关系信息中包含远端设备与中继设备的关联关系时，表明允许远端设备通过该中继设备接入网络，
25 否则，不允许该远端设备通过该中继设备接入网络。

可选的，在本实施例中，当远端设备发送给中继设备的通信请求中包括中继服务码时，当远端设备的移动管理实体获取到授权关系信息时，该远端设备的移动管理实体则根据远端设备的标识、中继设备的标识、中继服务码以及授权关系信息，验证是否允许该远端设备通过中继设备接入网络。此时，该授权关系信息为与远端设备有授权关系的中继
30 设备以及对应的中继服务码的关系列表。

可选的，该中继服务码用于表征远端设备要请求的业务类型，不同的中继服务码对应不同的业务类型，所以，在本实施例中，远端设备的移动管理实体验证远端设备与中继设备的关联关系时，还依据中继服务码。

值得说明的是，对于上述步骤 2407 中由中继设备的移动管理实体或者近距离功能实体来执行关联关系验证的实现步骤类似，此处不再赘述。
35

本申请实施例提供的授权验证方法，远端设备的移动管理实体根据远端设备的标识首先获取授权关系信息，进而根据远端设备的标识、中继设备的标识和该授权关系信息，验证是否允许远端设备通过中继设备接入网络。该技术方案关联关系验证方法简单，容易实现。

图 26 为本申请实施例提供的又一种授权验证装置的结构示意图。该装置可以位于远端设备的移动管理实体中，如图 26 所示，本实施例的装置可以包括：接收模块 2601、处理模块 2602 和发送模块 2603。

5 该接收模块 2601，用于接收基站发送的初始设备消息，所述初始设备消息包括：远端设备的非接入层消息和中继设备的标识；

该处理模块 2602，用于根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证；

10 该发送模块 2603，用于在判断所述关联关系验证通过后，向基站发送初始上下文建立请求消息。

可选的，所述处理模块 2602 具体，用于根据所述远端设备的标识获取授权关系信息，根据所述远端设备的标识、所述中继设备的标识以及所述授权关系信息，验证是否允许所述远端设备通过所述中继设备接入网络；

15 其中，所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远端设备的标识包含在所述初始设备消息中。

可选的，所述处理模块 2602，还用于在所述接收模块 2601 接收基站发送的初始设备消息之前，根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述授权关系信息，并将所述授权关系信息存储在远端设备的移动管理实体中。

20 可选的，所述处理模块 2602，具体用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并对所述远端设备的非接入层消息进行完整性校验。

可选的，所述处理模块 2602，还用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥；

25 所述发送模块 2603，还用于将所述密钥和生成所述密钥所需的安全参数通过所述初始上下文建立请求消息发送给所述基站。

可选的，所述发送模块 2603，还用于向所述中继设备的移动管理实体发送第一验证请求消息，以使所述中继设备的移动管理实体根据所述第一验证请求消息对所述远端设备和所述中继设备的关联关系进行验证，所述第一验证请求消息包括：所述远端设备的标识和所述中继设备的标识。

30 可选的，所述发送模块 2603，还用于向安全功能实体发送密钥请求消息，以使得所述安全功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给远端设备的移动管理实体，所述密钥请求消息，包括：所述远端设备标识。

35 本实施例提供的授权验证装置可用于执行图 24 和图 25 所示方法实施例中远端设备的移动管理实体的技术方案，具体实现方式和技术效果类似，这里不再赘述。

图 27 为本申请实施例提供的又一种授权验证装置的结构示意图。该装置可以位于基站中。如图 27 所示，本实施例的装置可以包括：接收模块 2701、处理模块 2702 和发送模块 2703。

其中，该接收模块 2701，用于接收中继设备发送的第一无线资源控制消息，所述第一无线资源控制消息包括远端设备的非接入层消息；

该处理模块 2702，用于根据所述第一无线资源控制消息，识别出远端设备请求通过所述中继设备接入网络，获取所述中继设备的标识；

5 该发送模块 2703，用于通过初始设备消息将所述中继设备的标识和所述远端设备的非接入层消息发送给远端设备的移动管理实体；

该接收模块 2701，还用于接收所述远端设备的移动管理实体在判断所述远端设备和所述中继设备的关联关系验证通过后发送的初始上下文建立请求消息；

10 该处理模块 2702，还用于根据所述初始上下文建立请求消息为所述远端设备建立上下文信息；

该发送模块 2703，还用于向所述中继设备发送第二无线资源控制消息。

可选的，所述处理模块 2702，具体用于从基站存储的中继设备的上下文信息中获取所述中继设备的标识，或从所述第一无线资源控制消息中获取所述中继设备的标识。

15 可选的，所述接收模块 2701，还用于在所述远端设备的移动管理实体生成用于保护所述远端设备和所述中继设备之间通信安全的密钥时，接收所述中继设备的移动管理实体发送的用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

20 可选的，所述发送模块 2703，还用于向所述远端设备发送第三无线资源控制消息，以使所述远端设备根据所述第三无线资源控制消息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，所述第三无线资源控制消息，包括：生成所述密钥所需的安全参数。

本实施例提供的授权验证装置可用于执行图 24 所示方法实施例中基站的技术方案，具体实现方式和技术效果类似，这里不再赘述。

25 图 28 为本申请实施例提供的又一种授权验证装置的结构示意图。该装置可以位于中继设备中。如图 28 所示，本实施例的装置可以包括：接收模块 2801、处理模块 2802 和发送模块 2803。

其中，该接收模块 2801，用于接收远端设备发送的通信请求；

该处理模块 2802，用于根据所述通信请求生成第一无线资源控制消息；

该发送模块 2803，用于将所述第一无线资源控制消息发送给基站；

30 该接收模块 2801，还用于接收所述基站为所述远端设备建立上下文信息后发送的第二无线资源控制消息；

所述处理模块 2802，还用于根据所述第二无线资源控制消息确定允许所述远端设备通过所述中继设备接入网络。

35 可选的，所述发送模块 2803，还用于将所述中继设备的标识通过所述第一无线资源控制消息发送给所述基站，以使所述基站识别远端设备请求通过所述中继设备接入网络。

本实施例提供的授权验证装置可用于执行图 24 所示方法实施例中中继设备的技术方案，具体实现方式和技术效果类似，这里不再赘述。

权利要求书

1、一种授权验证方法，其特征在于，包括：

远端设备的移动管理实体接收基站发送的初始设备消息，所述初始设备消息包括：远端设备的非接入层消息和中继设备的标识；

5 所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证；

所述远端设备的移动管理实体在判断所述关联关系验证通过后，向基站发送初始上下文建立请求消息。

10 2、根据权利要求 1 所述的方法，其特征在于，所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证，包括：

所述远端设备的移动管理实体根据所述远端设备的标识获取授权关系信息；

所述远端设备的移动管理实体根据所述远端设备的标识、所述中继设备的标识以及所述授权关系信息，验证是否允许所述远端设备通过所述中继设备接入网络；

15 所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远端设备的标识包含在所述初始设备消息中。

3、根据权利要求 2 所述的方法，其特征在于，在所述远端设备的移动管理实体接收基站发送的初始设备消息之前，所述远端设备的移动管理实体根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述授权关系信息，并将所述授权关系信息存储在该远端设备的移动管理实体。

20 4、根据权利要求 1-3 任一项所述的方法，其特征在于，所述远端设备的移动管理实体根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证，包括：

所述远端设备的移动管理实体根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并对所述远端设备的非接入层消息进行完整性校验。

25 5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述方法还包括：

所述远端设备的移动管理实体根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息；

所述远端设备的移动管理实体根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥；

30 所述远端设备的移动管理实体将所述密钥和生成所述密钥所需的安全参数通过所述初始上下文建立请求消息发送给所述基站。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述方法还包括：

35 所述远端设备的移动管理实体向所述中继设备的移动管理实体发送第一验证请求消息，以使所述中继设备的移动管理实体根据所述第一验证请求消息对所述远端设备和所述中继设备的关联关系进行验证，所述第一验证请求消息包括：所述远端设备的标识和所述中继设备的标识。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述方法还包括：

所述远端设备的移动管理实体向安全功能实体发送密钥请求消息，以使得所述安全

功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给所述远端设备的移动管理实体，所述密钥请求消息，包括：所述远端设备标识。

5

8、一种授权验证方法，其特征在于，包括：

基站接收中继设备发送的第一无线资源控制消息，所述第一无线资源控制消息包括远端设备的非接入层消息；

10 所述基站根据所述第一无线资源控制消息，识别出远端设备请求通过所述中继设备接入网络，获取所述中继设备的标识，以及通过初始设备消息将所述中继设备的标识和所述远端设备的非接入层消息发送给远端设备的移动管理实体；

所述基站接收所述远端设备的移动管理实体在判断所述远端设备和所述中继设备的关联关系验证通过后发送的初始上下文建立请求消息；

15 所述基站根据所述初始上下文建立请求消息为所述远端设备建立上下文信息，并向所述中继设备发送第二无线资源控制消息。

9、根据权利要求 8 所述的方法，其特征在于，所述基站获取所述中继设备的标识，包括：

所述基站从所述基站存储的中继设备的上下文信息中获取所述中继设备的标识，或所述基站从所述第一无线资源控制消息中获取所述中继设备的标识。

20 10、根据权利要求 8 或 9 所述的方法，其特征在于，

所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远端设备的标识包含在所述初始设备消息中。

11、根据权利要求 8-10 任一项所述的方法，其特征在于，所述方法，还包括：

25 所述基站根据所述初始上下文建立请求消息，建立所述远端设备和所述中继设备的映射关系。

12、根据权利要求 8-11 任一项所述的方法，其特征在于，在所述远端设备的移动管理实体生成用于保护所述远端设备和所述中继设备之间通信安全的密钥时，所述方法还包括：

30 所述基站接收所述中继设备的移动管理实体发送的用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

13、根据权利要求 8-12 任一项所述的方法，其特征在于，所述方法，还包括：

所述基站向所述远端设备发送第三无线资源控制消息，以使所述远端设备根据所述第三无线资源控制消息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，所述第三无线资源控制消息，包括：生成所述密钥所需的安全参数。

35

14、一种授权验证方法，其特征在于，包括：

中继设备接收远端设备发送的通信请求；

所述中继设备根据所述通信请求生成第一无线资源控制消息，并将所述第一无线资源控制消息发送给基站；

所述中继设备接收所述基站为所述远端设备建立上下文信息后发送的第二无线资源控制消息，以根据所述第二无线资源控制消息确定允许所述远端设备通过所述中继设备接入网络。

15、根据权利要求 14 所述的方法，其特征在于，还包括：

5 所述中继设备将所述中继设备的标识通过所述第一无线资源控制消息发送给所述基站，以使所述基站识别远端设备请求通过所述中继设备接入网络。

16、根据权利要求 14 或 15 所述的方法，其特征在于，所述方法，还包括：

所述中继设备根据所述基站发送的所述第二无线资源控制消息，建立所述远端设备和所述中继设备的映射关系。

10 17、根据权利要求 14-16 任一项所述的方法，其特征在于，所述第二无线资源控制消息，包括：用于保护所述远端设备和所述中继设备之间通信安全的密钥。

18、一种授权验证装置，其特征在于，包括：

接收模块，用于接收基站发送的初始设备消息，所述初始设备消息包括：远端设备的非接入层消息和中继设备的标识；

15 处理模块，用于根据所述初始设备消息，触发对所述远端设备和所述中继设备的关联关系的验证；

发送模块，用于在判断所述关联关系验证通过后，向基站发送初始上下文建立请求消息。

20 19、根据权利要求 18 所述的装置，其特征在于，所述处理模块具体，用于根据所述远端设备的标识获取授权关系信息，根据所述远端设备的标识、所述中继设备的标识以及所述授权关系信息，验证是否允许所述远端设备通过所述中继设备接入网络；

其中，所述远端设备的标识包含在所述远端设备的非接入层消息中，和/或所述远端设备的标识包含在所述初始设备消息中。

25 20、根据权利要求 19 所述的装置，其特征在于，所述处理模块，还用于在所述接收模块接收基站发送的初始设备消息之前，根据所述远端设备的标识从用户数据管理实体和/或近距离功能实体获取所述授权关系信息，并将所述授权关系信息存储在远端设备的移动管理实体中。

30 21、根据权利要求 18-20 任一项所述的装置，其特征在于，所述处理模块，具体用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，并对所述远端设备的非接入层消息进行完整性校验。

22、根据权利要求 18-21 任一项所述的装置，其特征在于，所述处理模块，还用于根据所述远端设备的标识，获取所述远端设备的非接入层上下文信息，根据所述非接入层上下文信息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥；

35 所述发送模块，还用于将所述密钥和生成所述密钥所需的安全参数通过所述初始上下文建立请求消息发送给所述基站。

23、根据权利要求 18-22 任一项所述的装置，其特征在于，所述发送模块，还用于向所述中继设备的移动管理实体发送第一验证请求消息，以使所述中继设备的移动管理实体根据所述第一验证请求消息对所述远端设备和所述中继设备的关联关系进行验证，所述第一验证请求消息包括：所述远端设备的标识和所述中继设备的标识。

24、根据权利要求 18-23 任一项所述的装置，其特征在于，所述发送模块，还用于向安全功能实体发送密钥请求消息，以使得所述安全功能实体根据所述密钥请求消息，获取用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数，并将所述密钥和生成所述密钥所需的安全参数反馈给远端设备的移动管理实体，所述密钥请求消息，包括：所述远端设备标识。

25、一种授权验证装置，其特征在于，包括：

接收模块，用于接收中继设备发送的第一无线资源控制消息，所述第一无线资源控制消息包括远端设备的非接入层消息；

处理模块，用于根据所述第一无线资源控制消息，识别出远端设备请求通过所述中继设备接入网络，获取所述中继设备的标识；

发送模块，用于通过初始设备消息将所述中继设备的标识和所述远端设备的非接入层消息发送给远端设备的移动管理实体；

所述接收模块，还用于接收所述远端设备的移动管理实体在判断所述远端设备和所述中继设备的关联关系验证通过后发送的初始上下文建立请求消息；

所述处理模块，还用于根据所述初始上下文建立请求消息为所述远端设备建立上下文信息；

所述发送模块，还用于向所述中继设备发送第二无线资源控制消息。

26、根据权利要求 25 所述的装置，其特征在于，所述处理模块，具体用于从基站存储的中继设备的上下文信息中获取所述中继设备的标识，或从所述第一无线资源控制消息中获取所述中继设备的标识。

27、根据权利要求 25 或 26 所述的装置，其特征在于，所述接收模块，还用于在所述远端设备的移动管理实体生成用于保护所述远端设备和所述中继设备之间通信安全的密钥时，接收所述中继设备的移动管理实体发送的用于保护所述远端设备和所述中继设备之间通信安全的密钥和生成所述密钥所需的安全参数。

28、根据权利要求 25-27 任一项所述的装置，其特征在于，所述发送模块，还用于向所述远端设备发送第三无线资源控制消息，以使所述远端设备根据所述第三无线资源控制消息生成用于保护所述远端设备和所述中继设备之间通信安全的密钥，所述第三无线资源控制消息，包括：生成所述密钥所需的安全参数。

29、一种授权验证装置，其特征在于，包括：

接收模块，用于接收远端设备发送的通信请求；

处理模块，用于根据所述通信请求生成第一无线资源控制消息；

发送模块，用于将所述第一无线资源控制消息发送给基站；

所述接收模块，还用于接收所述基站为所述远端设备建立上下文信息后发送的第二无线资源控制消息；

所述处理模块，还用于根据所述第二无线资源控制消息确定允许所述远端设备通过所述中继设备接入网络。

30、根据权利要求 29 所述的装置，其特征在于，所述发送模块，还用于将所述中继设备的标识通过所述第一无线资源控制消息发送给所述基站，以使所述基站识别远端设备请求通过所述中继设备接入网络。

1/17

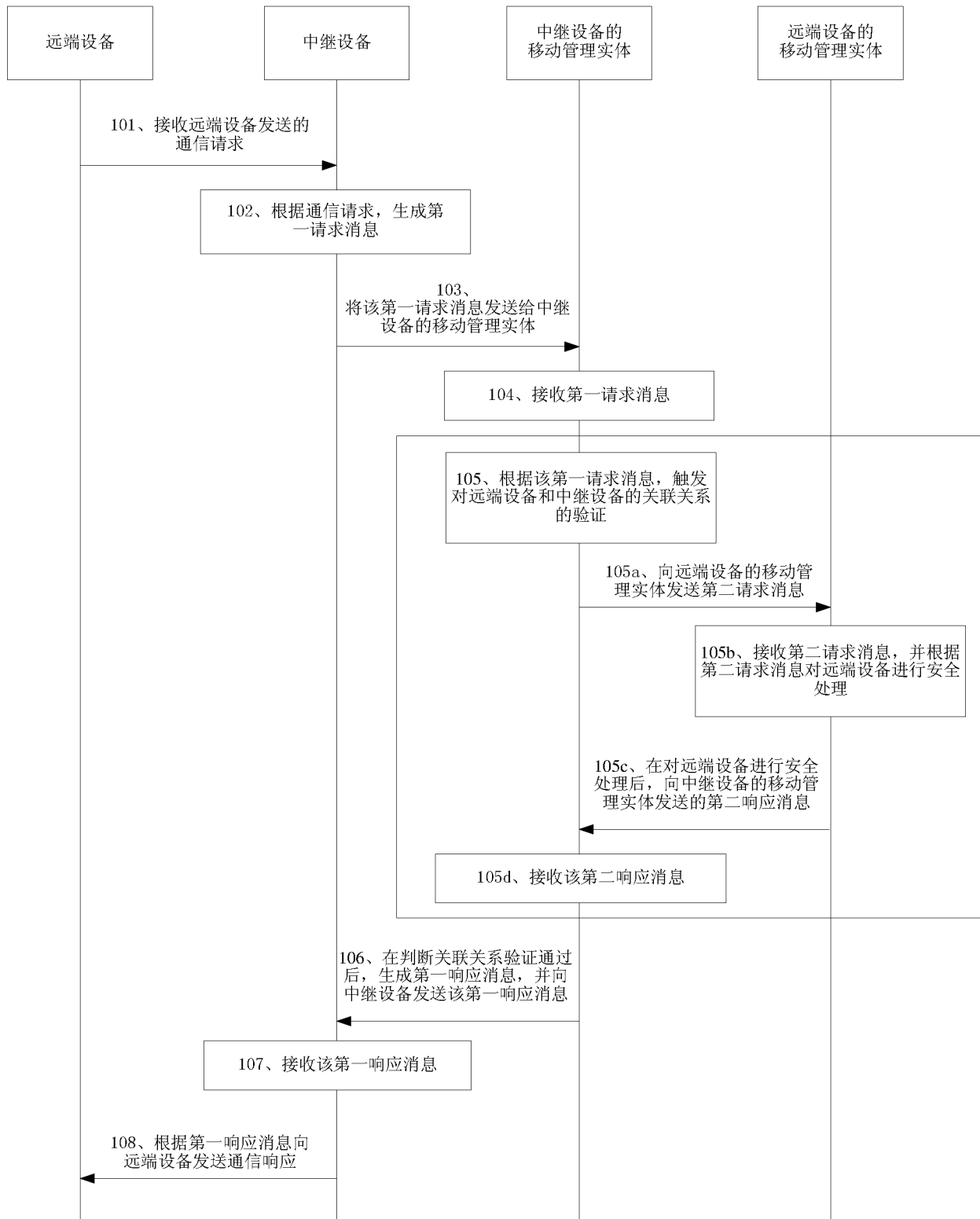


图 1

2/17

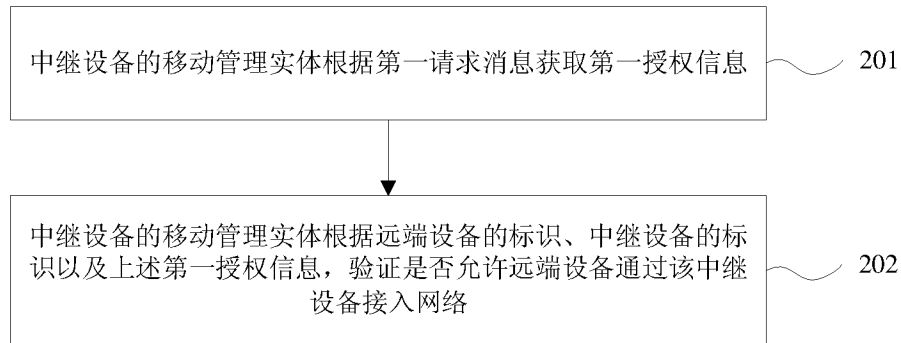


图 2

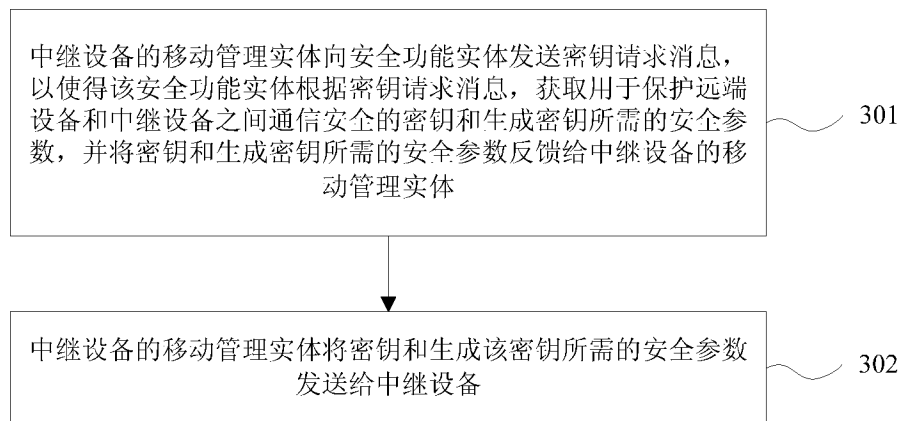


图 3

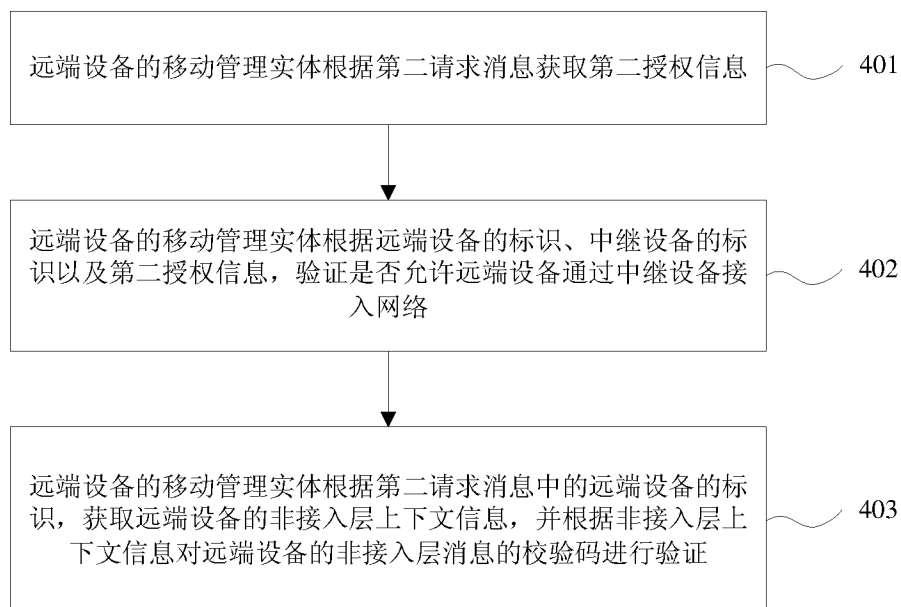


图 4

3/17

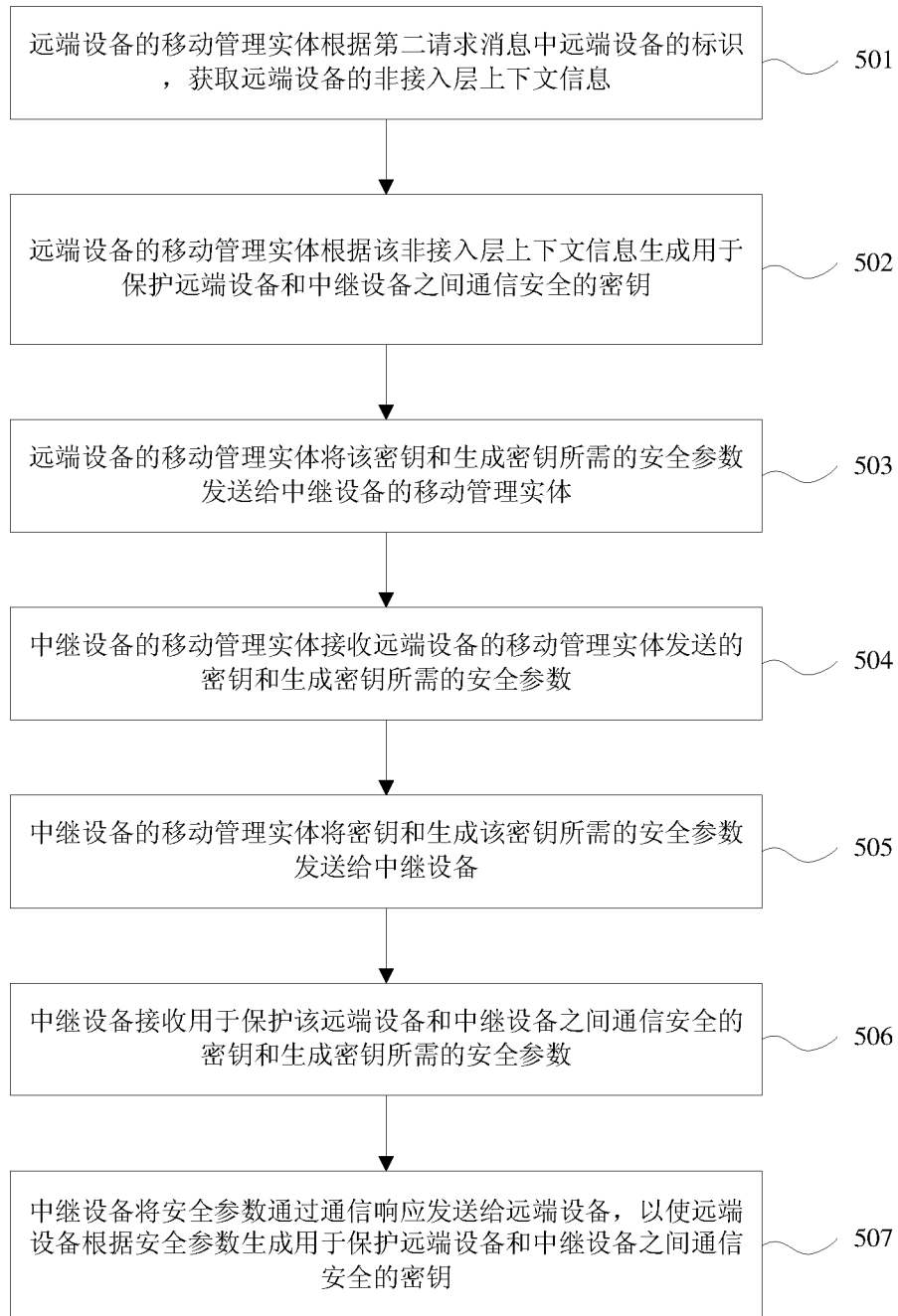


图 5

4/17

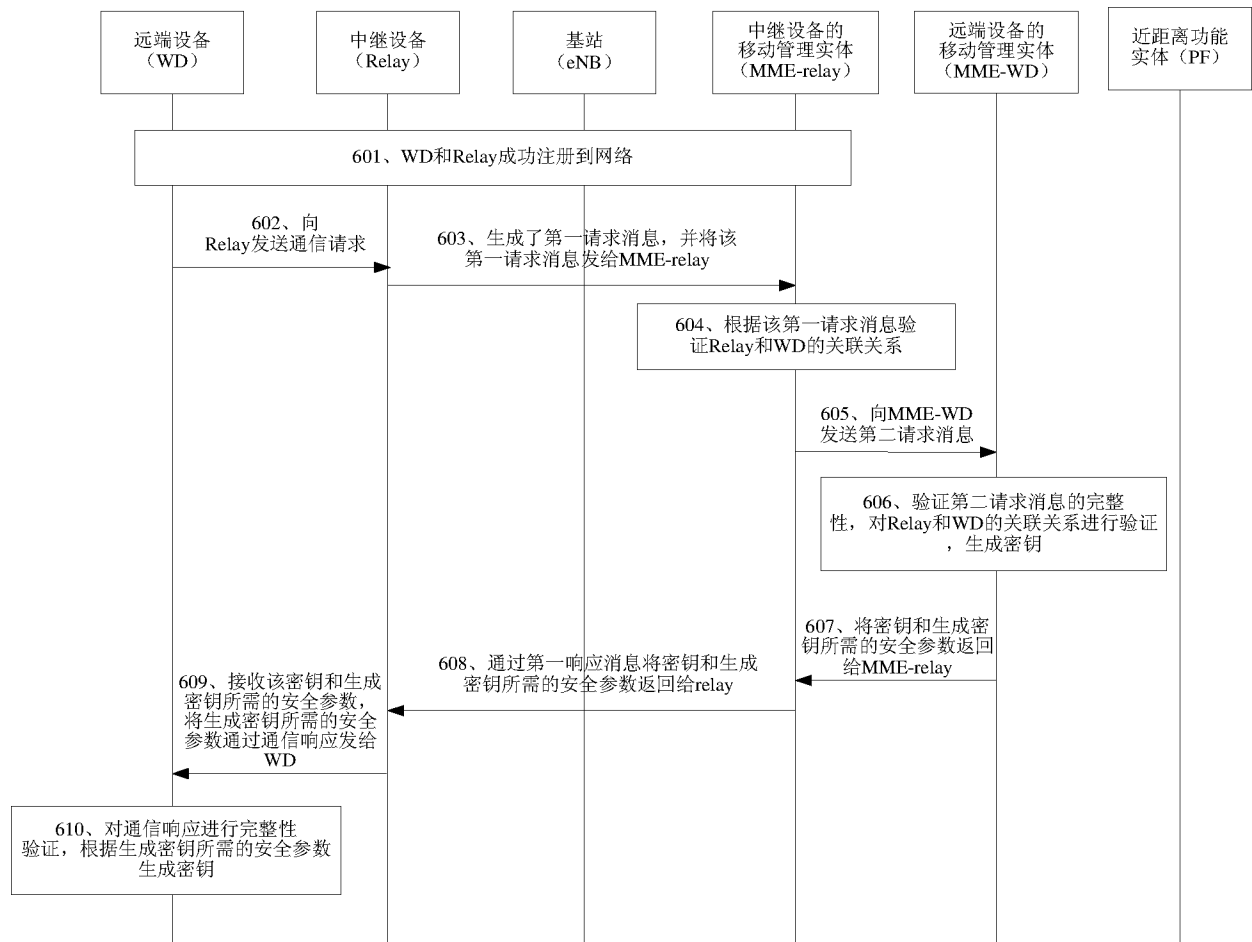


图 6

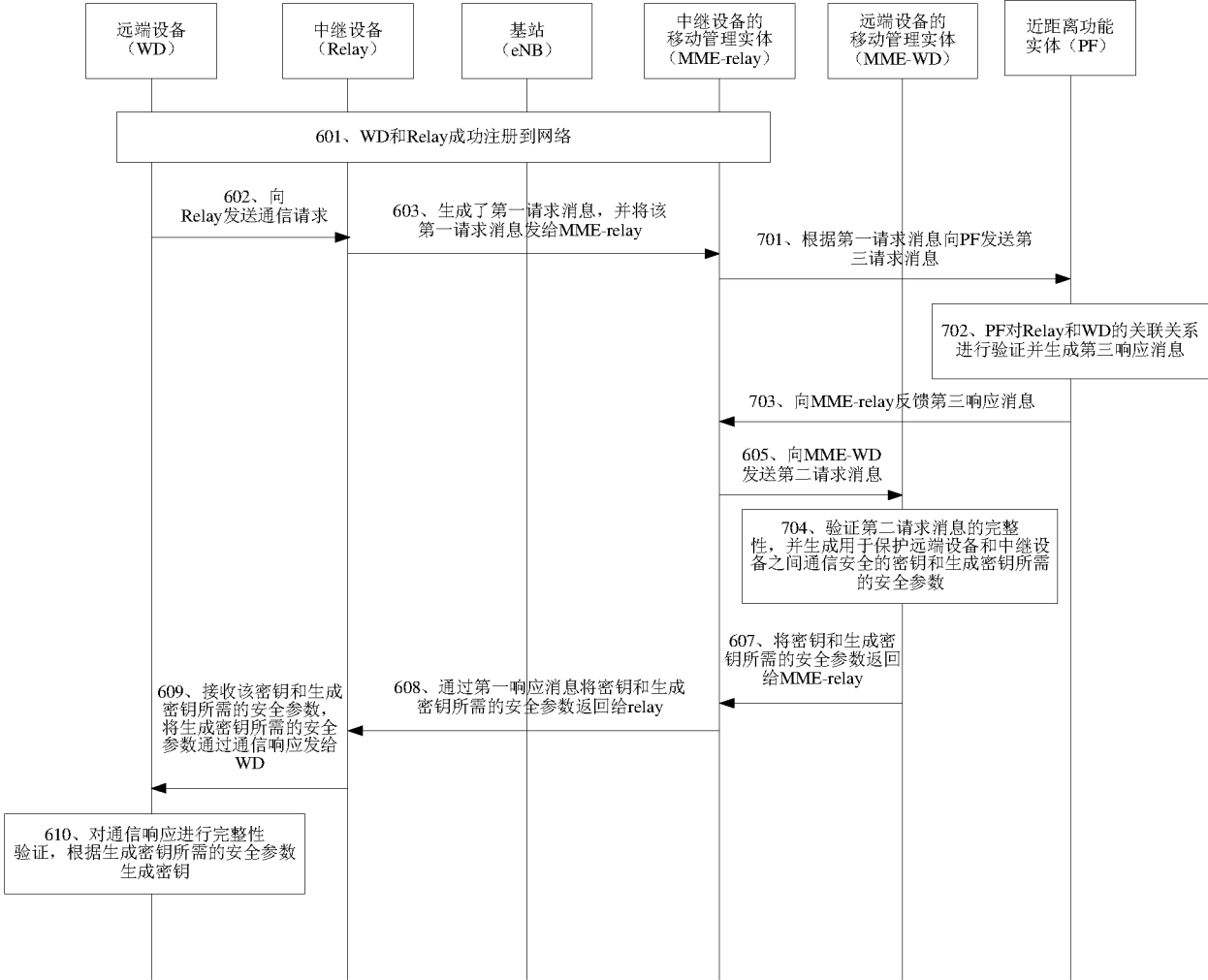


图 7

6/17

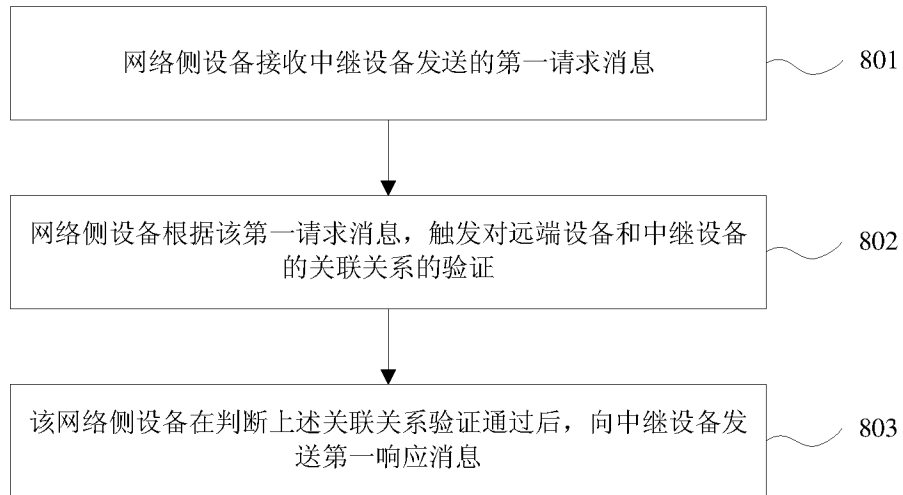


图 8

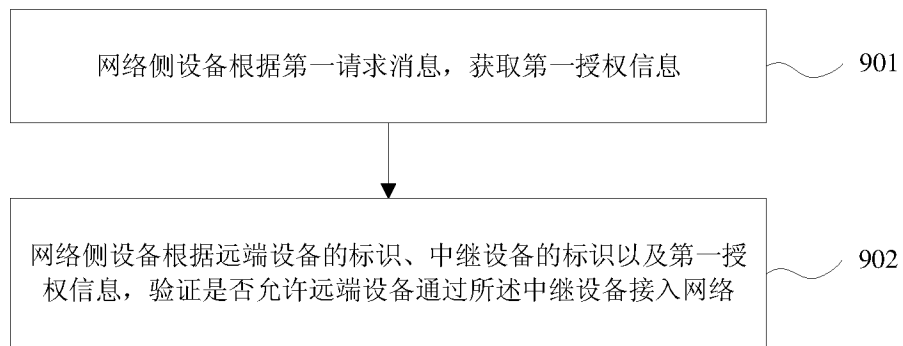


图 9

7/17

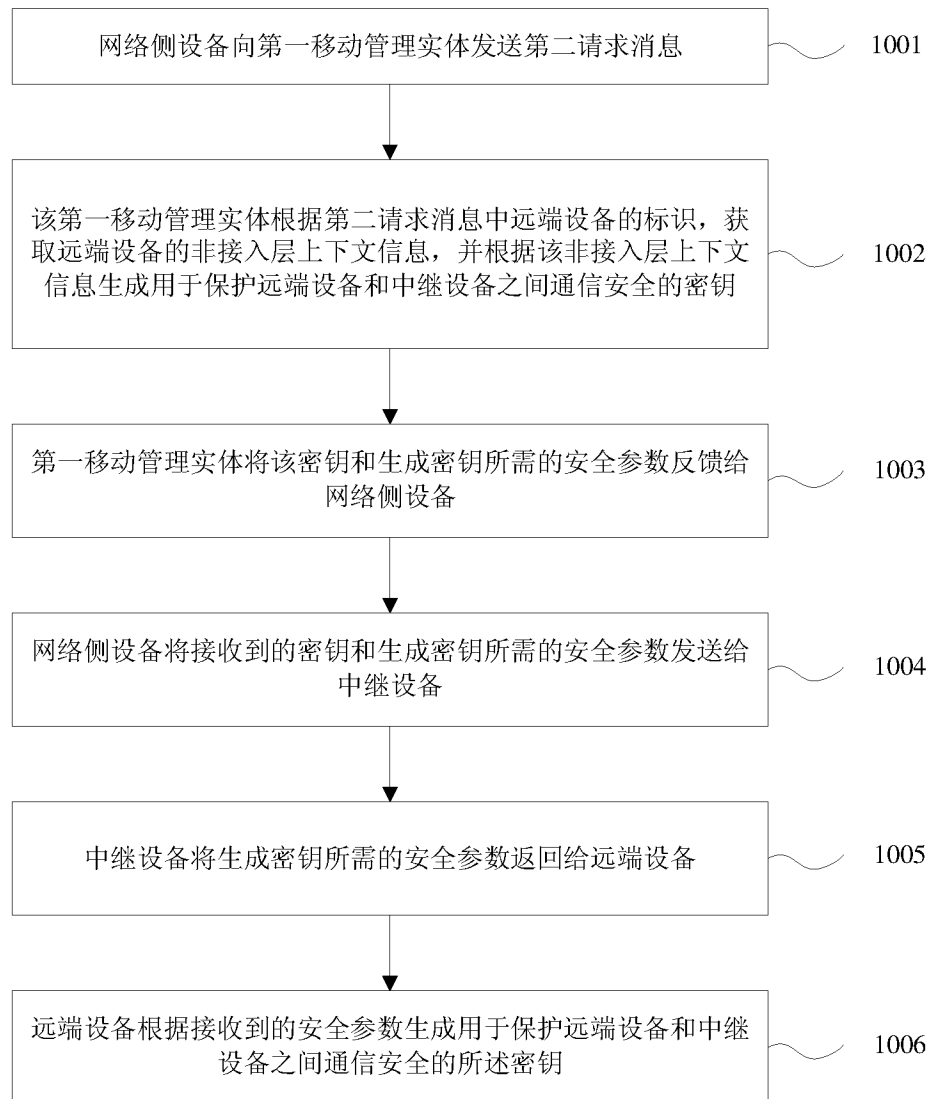


图 10

8/17

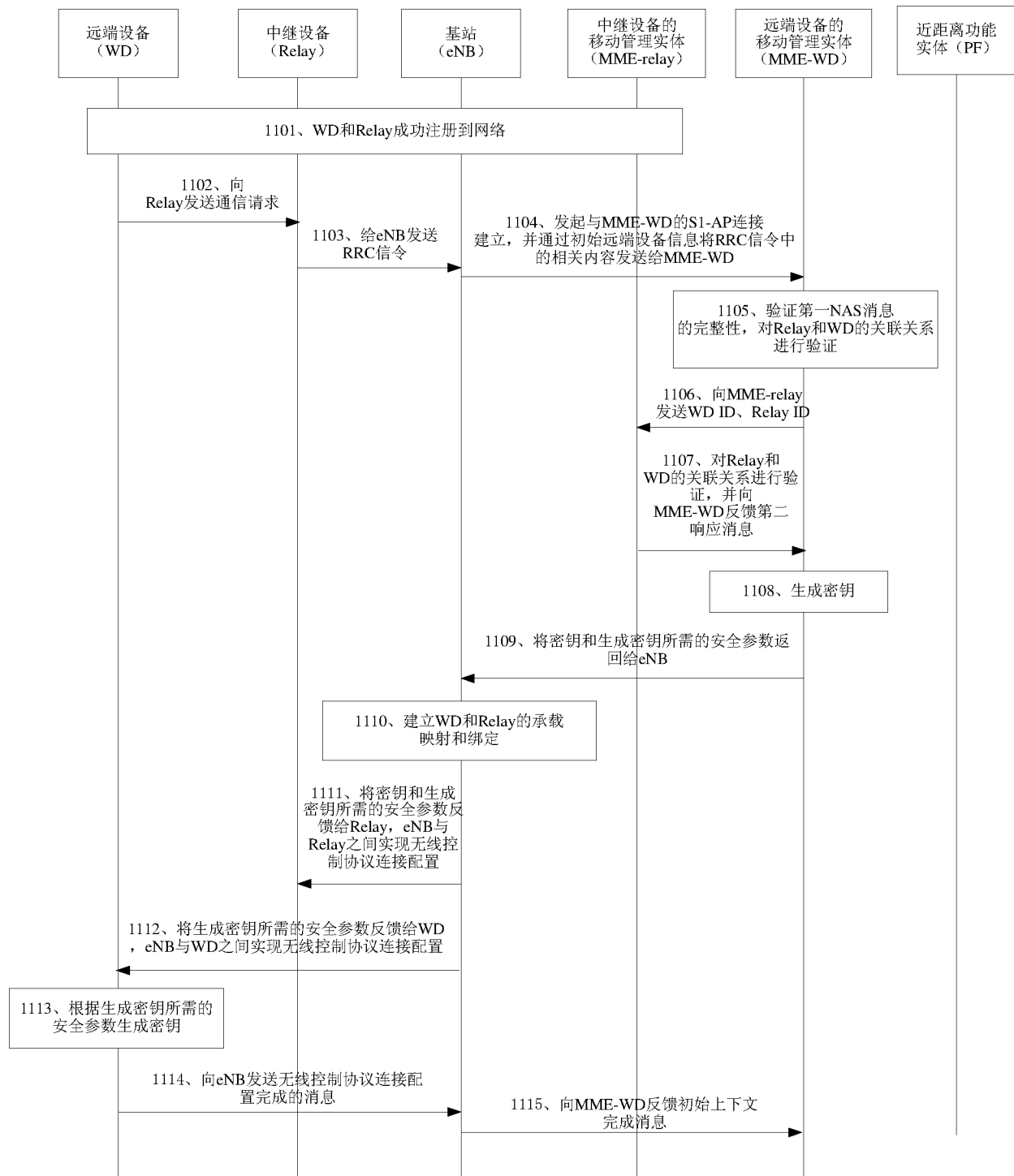


图 11

9/17

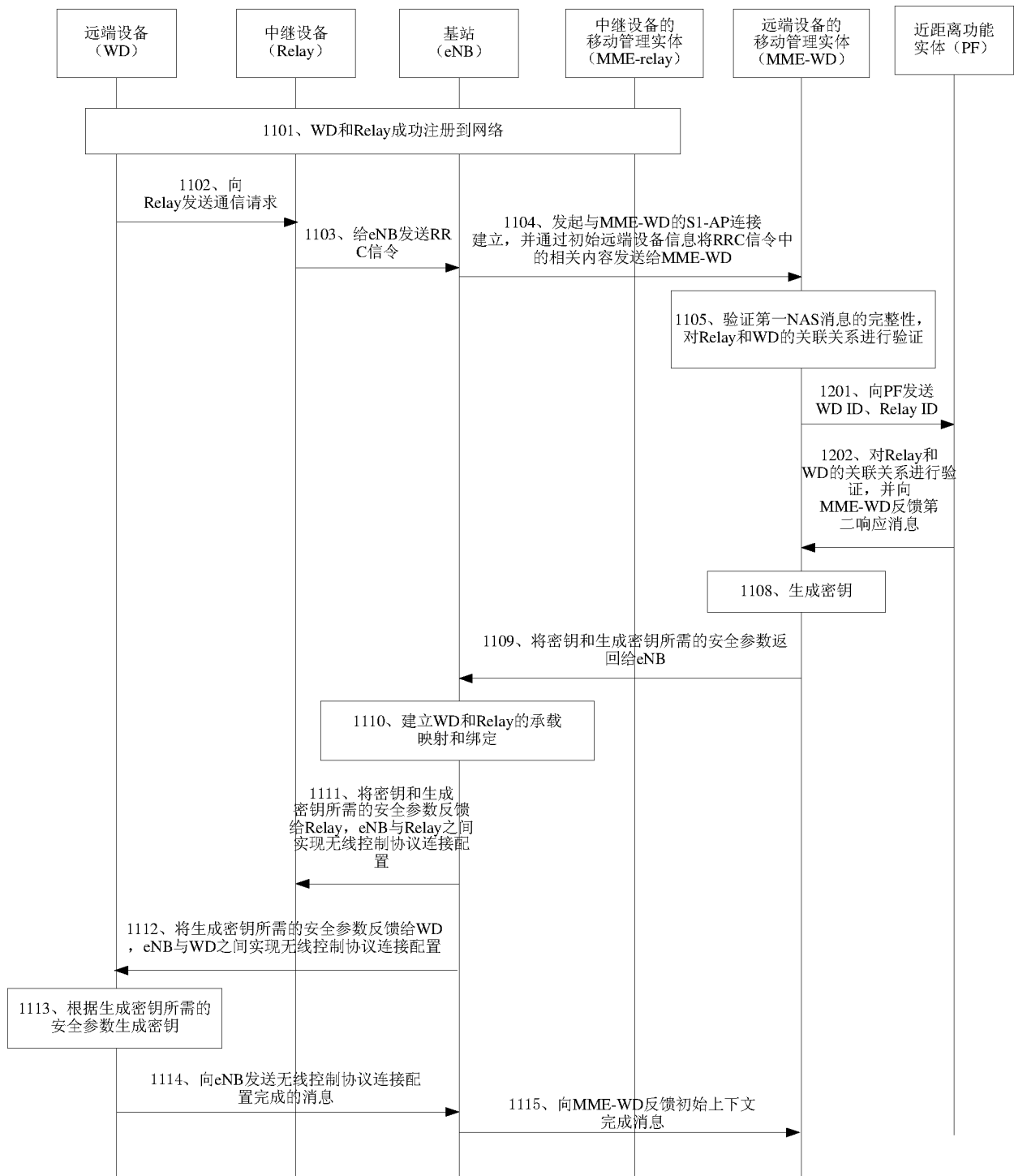


图 12

10/17

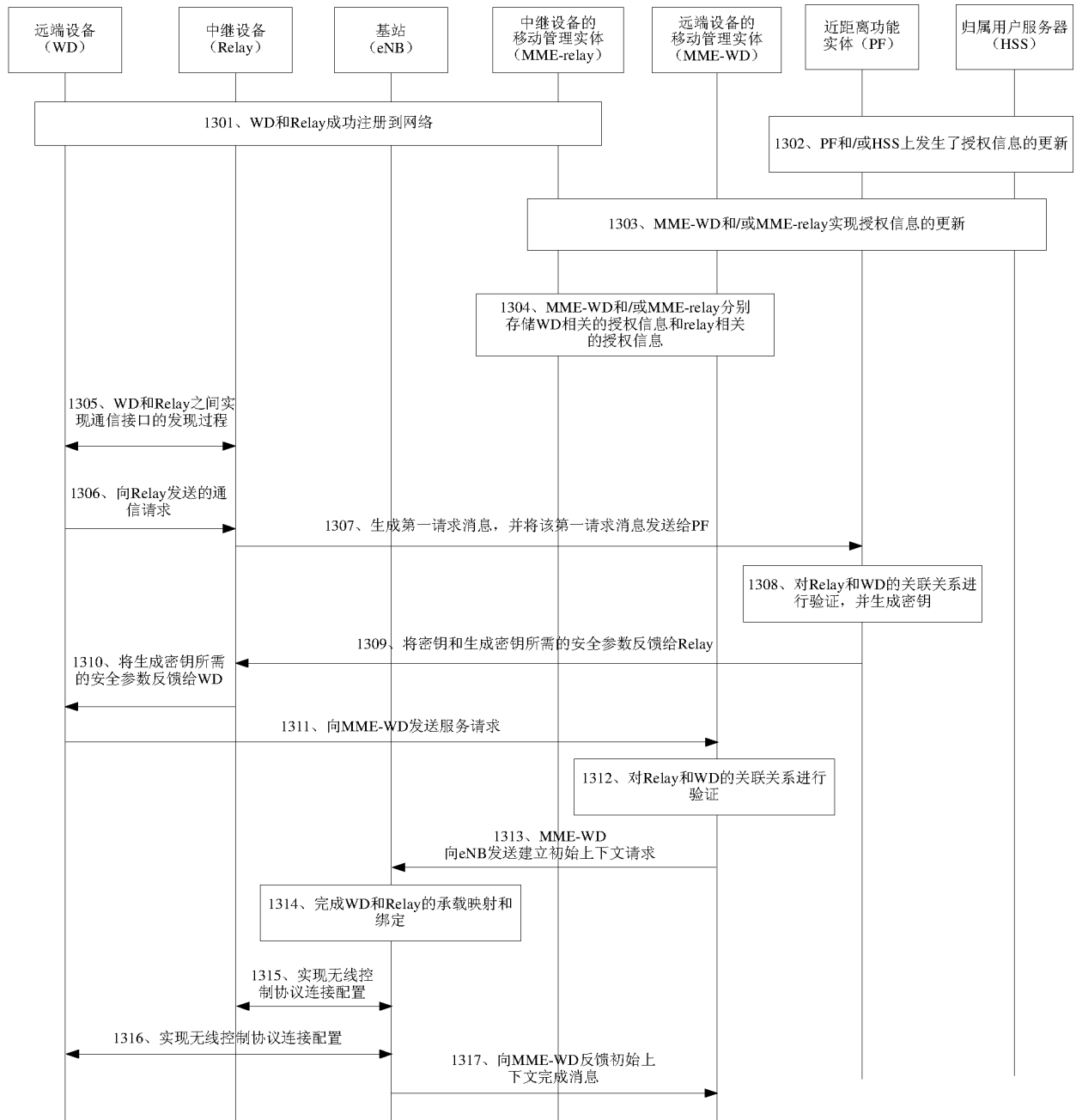


图 13

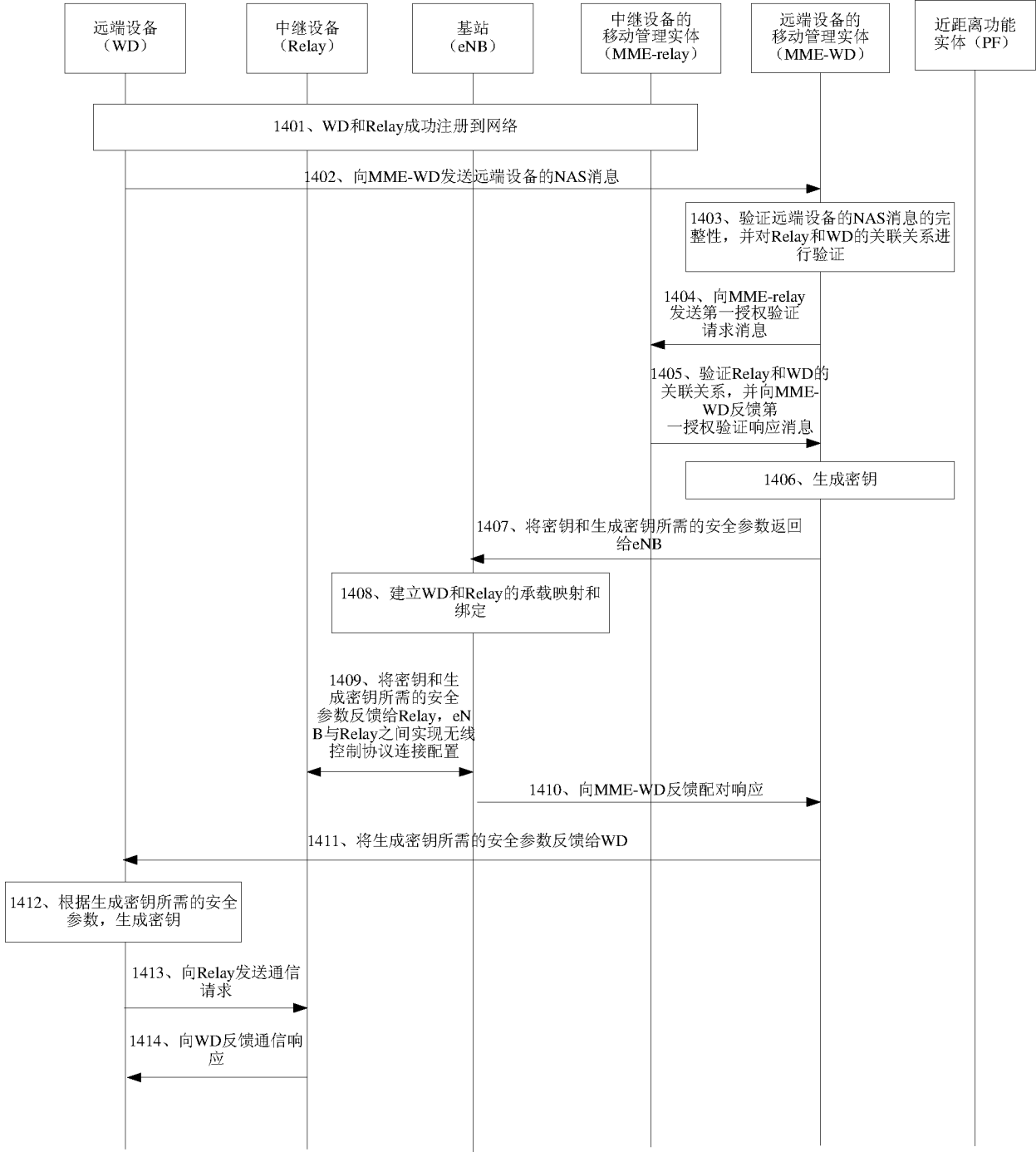


图 14

12/17

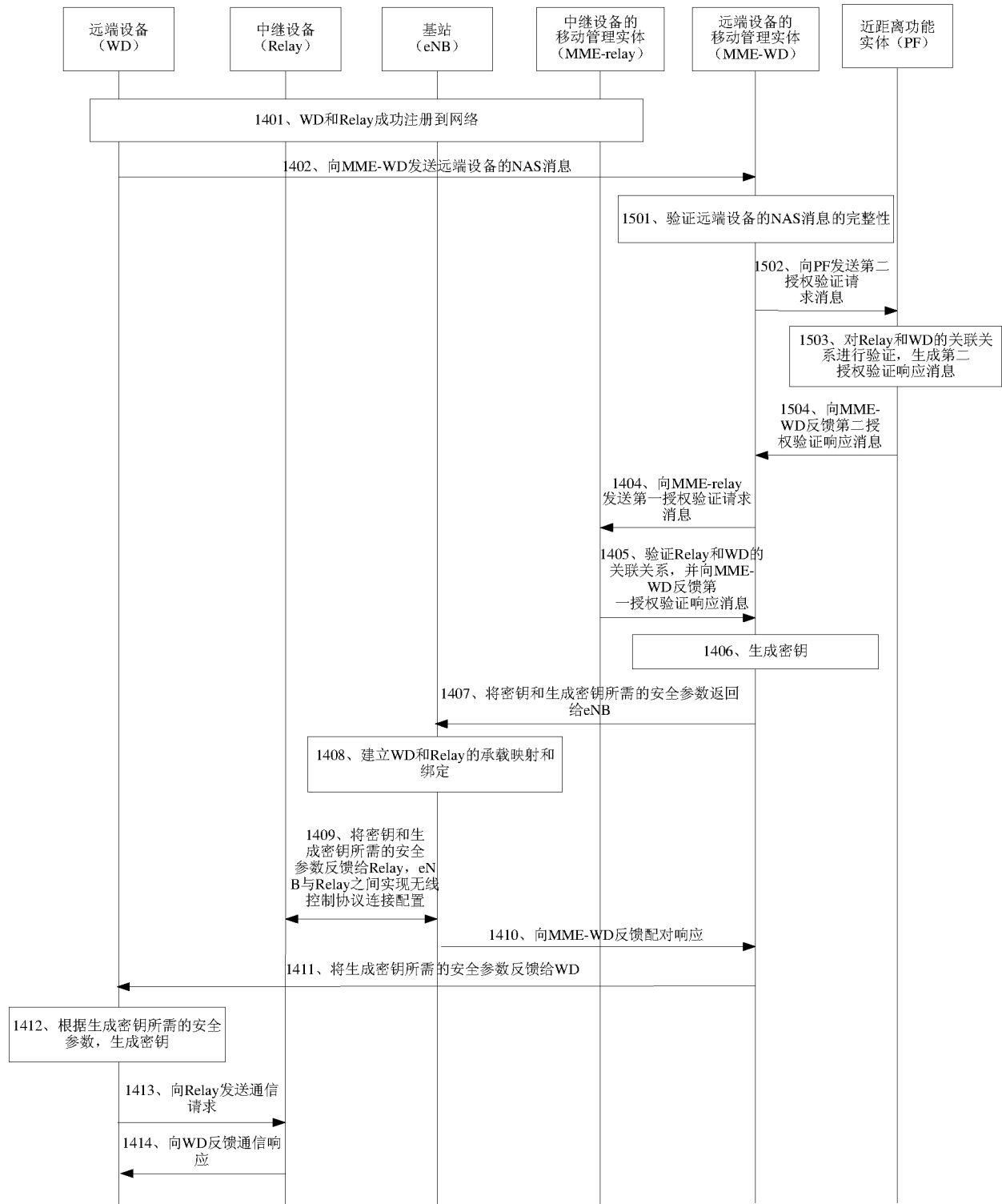


图 15

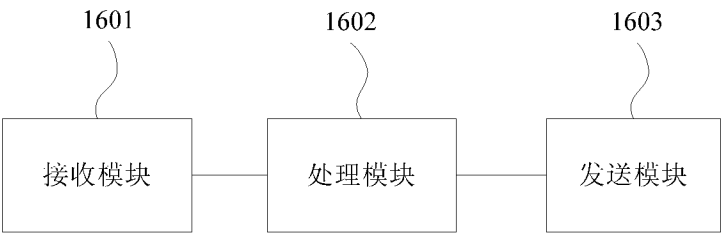


图 16

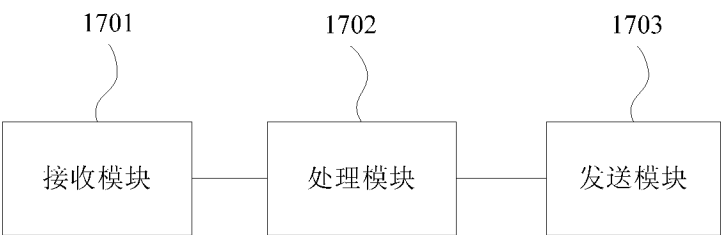


图 17

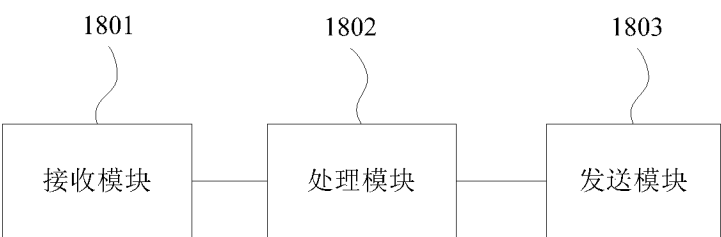


图 18

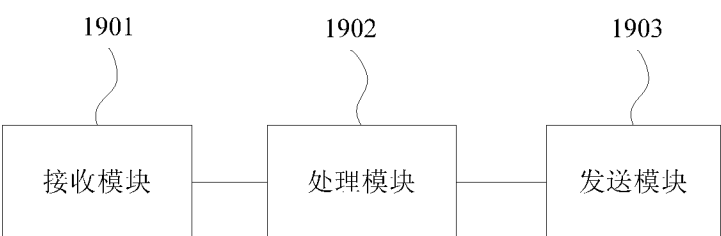


图 19

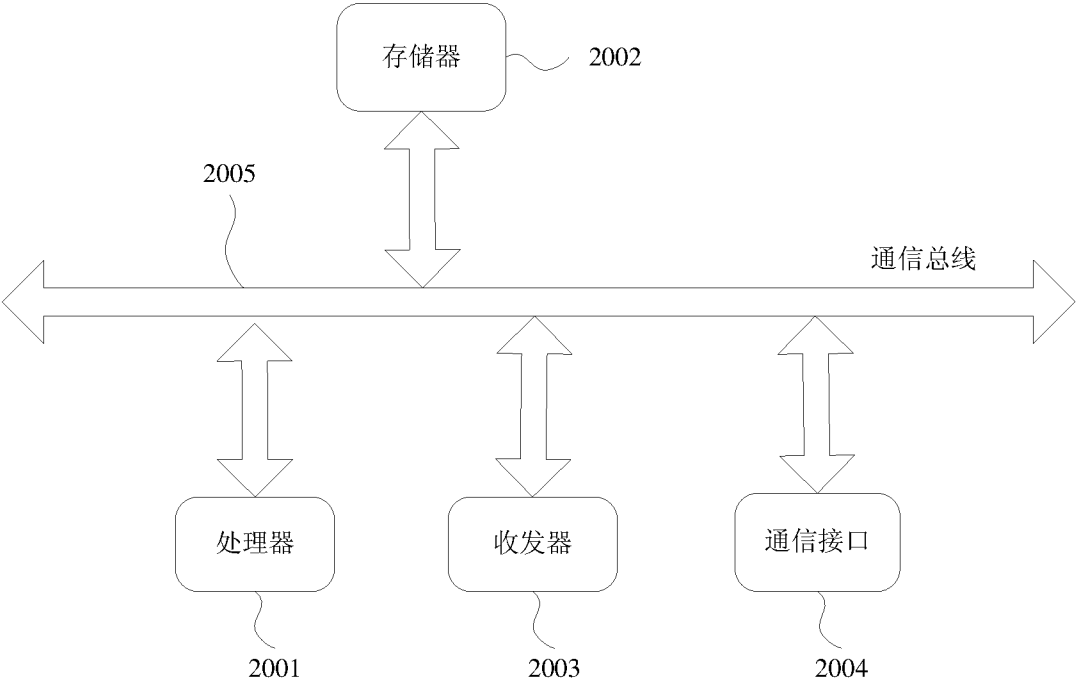


图 20

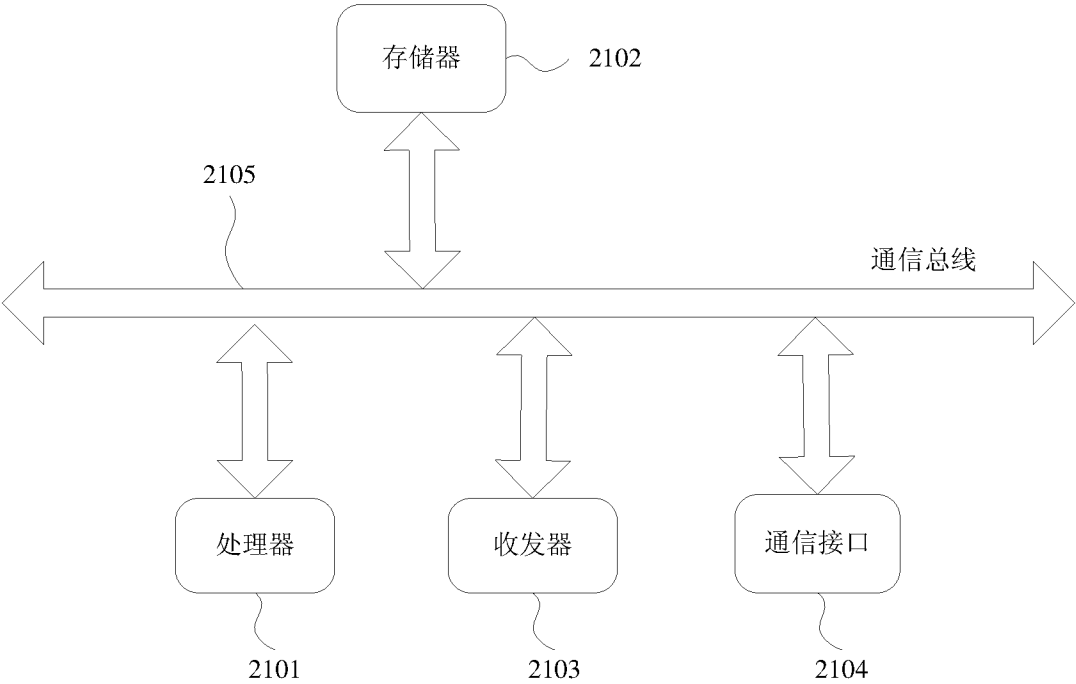


图 21

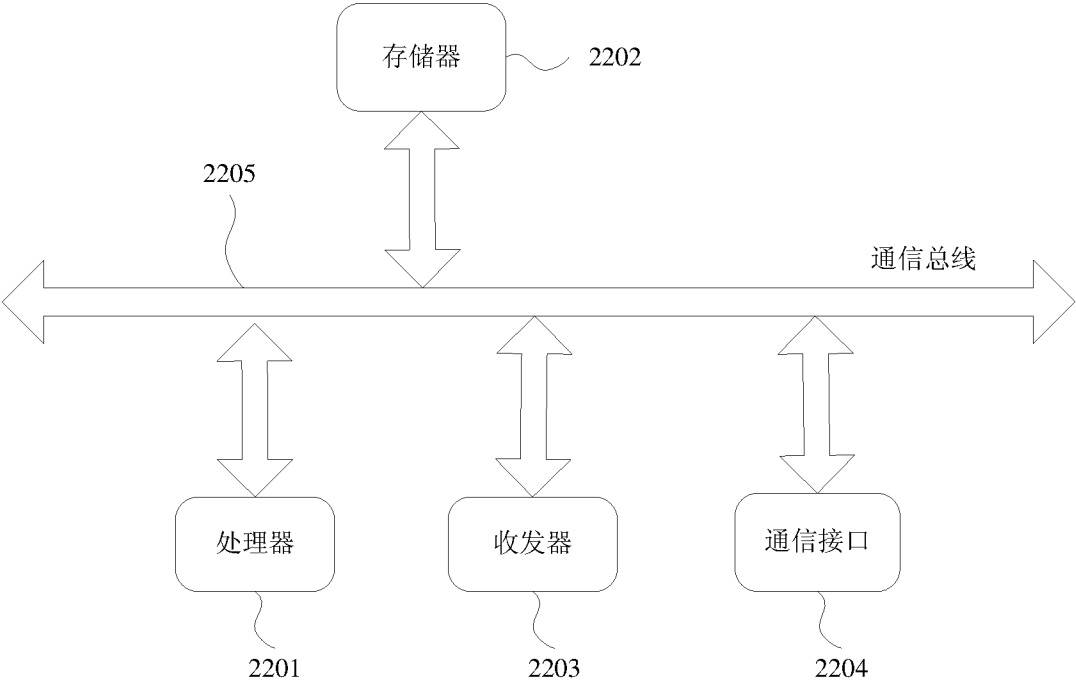


图 22

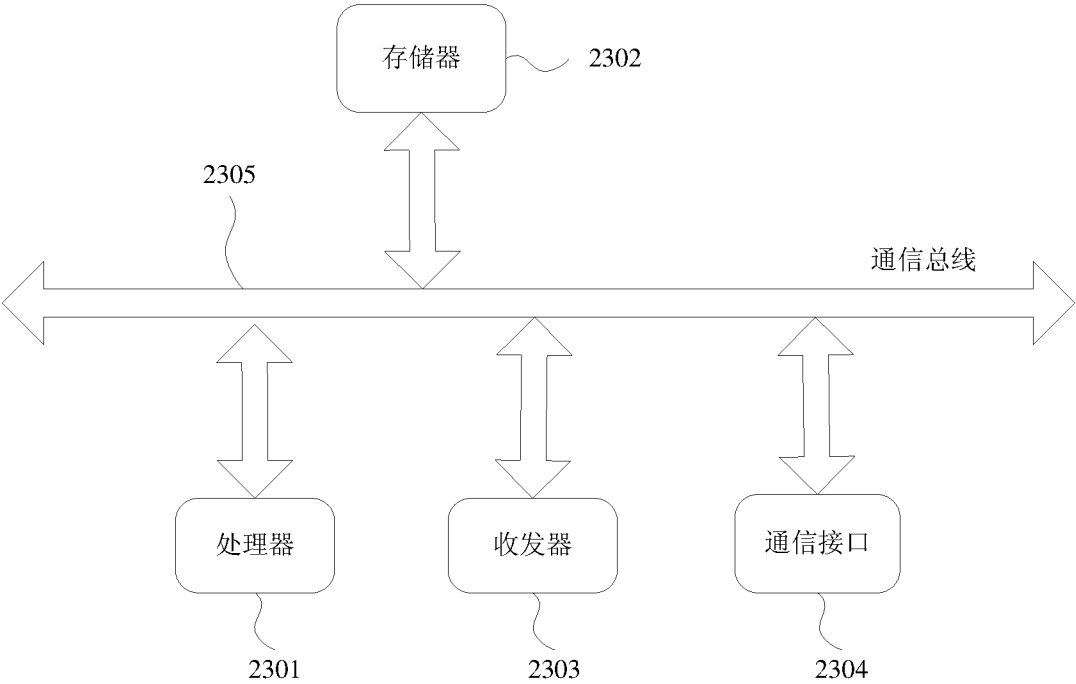


图 23

16/17

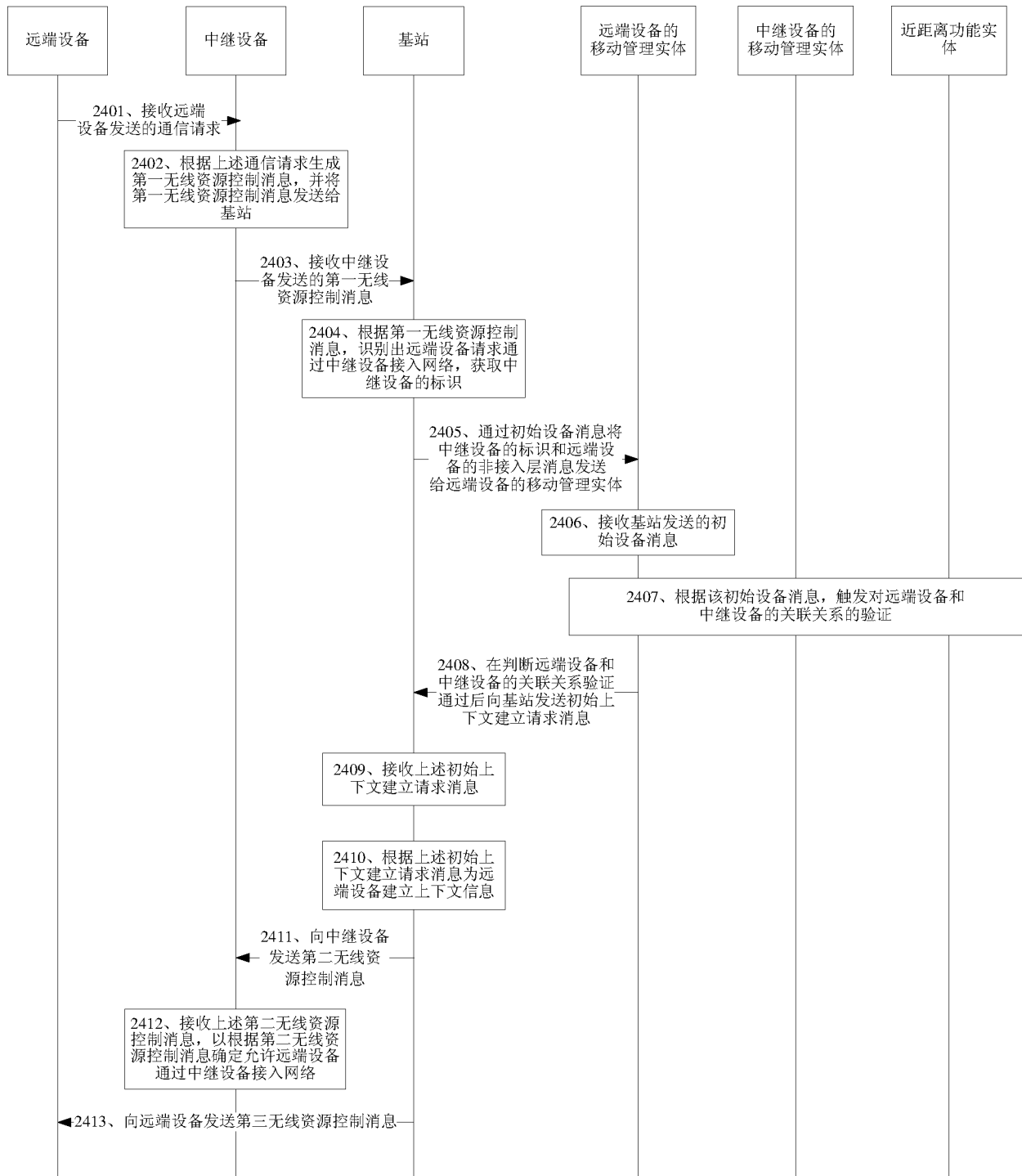


图 24

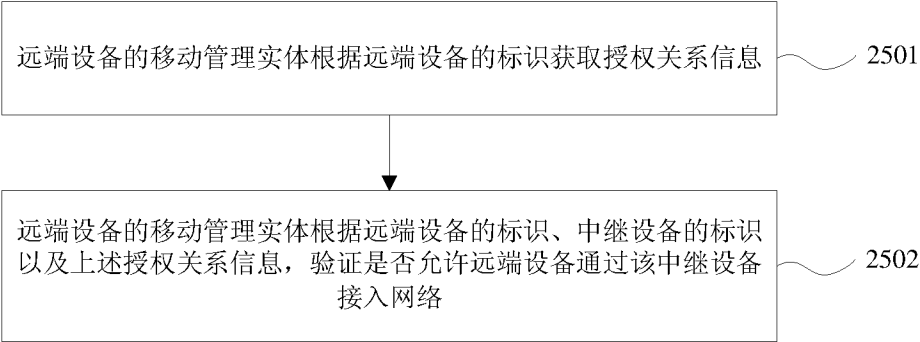


图 25

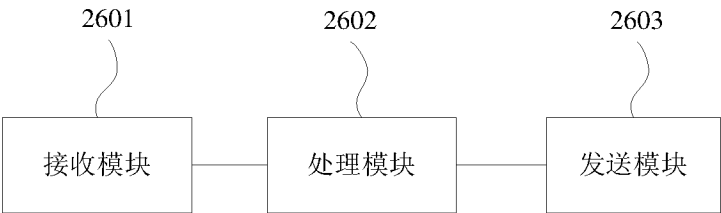


图 26

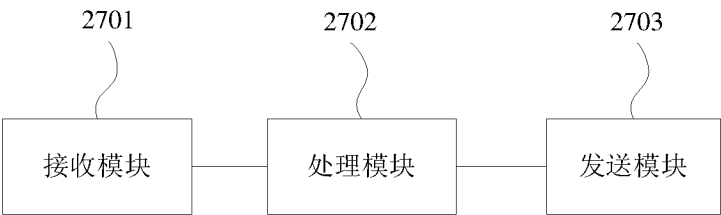


图 27

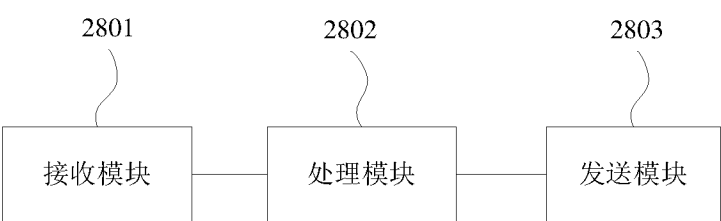


图 28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077271

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; H04W 88/00 (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 12/, H04W 88/

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)

CNTEXT, CNABS, VEN, USTXT, CNKI: 非接入层消息, 非接入子层消息, 中继, 移动管理实体, MME, 上下文, 授权, 验证, 校验, 认证, 鉴别, 鉴权, 初始, non-access stratum message, non-access layer message, NAS, relay, mobile management entity, mobility management entity, MME, context, authentication, grant, identif+, initial

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101902835 A (CHINA MOBILE COMMUNICATIONS CORPORATION) 01 December 2010 (01.12.2010), description, pages 3-5, and claims 1-12	1-30
A	US 2016262068 A1 (SAMSUNG ELECTRONICS CO., LTD.) 08 September 2016 (08.09.2016), entire document	1-30
A	CN 103460743 A (NTT DOCOMO INC.) 18 December 2013 (18.12.2013), entire document	1-30
A	CN 102595395 A (ZTE CORPORATION) 18 July 2012 (18.07.2012), entire document	1-30
A	US 2014241236 A1 (GENERAL DYNAMICS BROADBAND INC.) 28 August 2014 (28.08.2014), entire document	1-30

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"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	"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
"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)	"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
"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	"&" document member of the same patent family

Date of the actual completion of the international search 13 September 2017	Date of mailing of the international search report 25 September 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 QI, Ji Telephone No. (86-10) 62411484

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077271

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014241237 A1 (GENERAL DYNAMICS BROADBAND INC.) 28 August 2014 (28.08.2014), entire document	1-30

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077271

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

- [1] (1) claims 1, 8, 18, 25, (2) claims 14, 29
[2] The inventions respectively defined in (1) and (2) do not share a same or corresponding special technical feature, and do not meet the requirement of unity of invention.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077271

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101902835 A	01 December 2010	CN 101902835 B	10 September 2014
		EP 2405703 A1	11 January 2012
		WO 2010099705 A1	10 September 2010
		US 2012002592 A1	05 January 2012
US 2016262068 A1	08 September 2016	CN 101827449 A	08 September 2010
		WO 2016140507 A1	09 September 2016
		US 2017041752 A1	09 February 2017
		KR 20160106520 A	12 September 2016
CN 103460743 A	18 December 2013	KR 20130137037 A	13 December 2013
		ZA 201307833 A	28 January 2015
		RU 2013146040 A	10 May 2015
		US 9002324 B2	07 April 2015
		JP 2012217110 A	08 November 2012
		AU 2012239436 A8	14 November 2013
		RU 2573418 C2	20 January 2016
		ID 201403111 A	28 August 2014
		ES 2620412 T3	28 June 2017
		JP 5021820 B1	12 September 2012
		WO 2012137643 A1	11 October 2012
		AU 2012239436 A1	31 October 2013
		IN 201303127 P2	14 February 2014
		AU 2012239436 B2	02 July 2015
		US 2014094145 A1	03 April 2014
		KR 20140140596 A	09 December 2014
		MX 328020 B	19 February 2015
		EP 2696616 B1	28 December 2016
		CN 103460743 B	31 December 2014
		EP 2696616 A1	12 February 2014

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077271

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
		MX 2013011315 A	31 December 2013
CN 102595395 A	18 July 2012	WO 2012094920 A1	19 July 2012
US 2014241236 A1	28 August 2014	EP 2770792 A1	27 August 2014
		US 8934400 B2	13 January 2015
		EP 2770792 B1	22 June 2016
US 2014241237 A1	28 August 2014	EP 2773161 A1	03 September 2014
		US 8934401 B2	13 January 2015
		EP 2773161 B1	15 June 2016

国际检索报告

国际申请号

PCT/CN2017/077271

A. 主题的分类

H04W 12/06(2009.01)i; H04W 88/00(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)

H04W12/, H04W88/

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))

CNXT, CNABS, VEN, USTXT, CNKI: 非接入层消息, 非接入子层消息, 中继, 移动管理实体, MME, 上下文, 授权, 验证, 校验, 认证, 鉴别, 鉴权, 初始, non-access stratum message, non-access layer message, NAS, relay, mobile management entity, mobility management entity, MME, context, authentication, grant, ident-tif+, initial

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 101902835 A (中国移动通信集团公司) 2010年 12月 1日 (2010 - 12 - 01) 说明书第3-5页, 权利要求1-12	1-30
A	US 2016262068 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2016年 9月 8日 (2016 - 09 - 08) 全文	1-30
A	CN 103460743 A (株式会社NTT都科摩) 2013年 12月 18日 (2013 - 12 - 18) 全文	1-30
A	CN 102595395 A (中兴通讯股份有限公司) 2012年 7月 18日 (2012 - 07 - 18) 全文	1-30
A	US 2014241236 A1 (GENERAL DYNAMICS BROADBAND INC.) 2014年 8月 28日 (2014 - 08 - 28) 全文	1-30
A	US 2014241237 A1 (GENERAL DYNAMICS BROADBAND INC.) 2014年 8月 28日 (2014 - 08 - 28) 全文	1-30

☐ 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

2017年 9月 13日

国际检索报告邮寄日期

2017年 9月 25日

ISA/CN的名称和邮寄地址

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

传真号 (86-10)62019451

受权官员

齐霁

电话号码 (86-10)62411484

第III栏 缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明，即：

[1] (1) 权利要求1、8、18、25，(2) 权利要求14、29

[2] (1) 与(2) 所分别限定的发明中没有相同或相应的特定技术特征，不具备单一性。

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。
2. ☒ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。
3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求：
4. ☐ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是：

对异议的意见

- ☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。
- ☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。
- ☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/077271

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	101902835	A	2010年 12月 1日	CN	101902835	B	2014年 9月 10日
				EP	2405703	A1	2012年 1月 11日
				WO	2010099705	A1	2010年 9月 10日
				US	2012002592	A1	2012年 1月 5日
				CN	101827449	A	2010年 9月 8日
US	2016262068	A1	2016年 9月 8日	WO	2016140507	A1	2016年 9月 9日
				US	2017041752	A1	2017年 2月 9日
				KR	20160106520	A	2016年 9月 12日
CN	103460743	A	2013年 12月 18日	KR	20130137037	A	2013年 12月 13日
				ZA	201307833	A	2015年 1月 28日
				RU	2013146040	A	2015年 5月 10日
				US	9002324	B2	2015年 4月 7日
				JP	2012217110	A	2012年 11月 8日
				AU	2012239436	A8	2013年 11月 14日
				RU	2573418	C2	2016年 1月 20日
				ID	201403111	A	2014年 8月 28日
				ES	2620412	T3	2017年 6月 28日
				JP	5021820	B1	2012年 9月 12日
				WO	2012137643	A1	2012年 10月 11日
				AU	2012239436	A1	2013年 10月 31日
				IN	201303127	P2	2014年 2月 14日
				AU	2012239436	B2	2015年 7月 2日
				US	2014094145	A1	2014年 4月 3日
				KR	20140140596	A	2014年 12月 9日
				MX	328020	B	2015年 2月 19日
				EP	2696616	B1	2016年 12月 28日
				CN	103460743	B	2014年 12月 31日
				EP	2696616	A1	2014年 2月 12日
				MX	2013011315	A	2013年 12月 31日
CN	102595395	A	2012年 7月 18日	WO	2012094920	A1	2012年 7月 19日
US	2014241236	A1	2014年 8月 28日	EP	2770792	A1	2014年 8月 27日
				US	8934400	B2	2015年 1月 13日
				EP	2770792	B1	2016年 6月 22日
US	2014241237	A1	2014年 8月 28日	EP	2773161	A1	2014年 9月 3日
				US	8934401	B2	2015年 1月 13日
				EP	2773161	B1	2016年 6月 15日

表 PCT/ISA/210 (同族专利附件) (2009年7月)