

一种通信方法及装置

相关申请的交叉引用

本申请要求在2023年09月11日提交中国国家知识产权局、申请号为202311170506.2、申请名称为“一种通信方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及通信技术领域，尤其涉及一种通信方法及装置。

背景技术

10 切换是终端在连接态下的一种过程，由网络侧发起，涉及终端与接入网设备之间的信令交互。例如，接入网设备在感知到终端在自身小区内的信号强度逐渐变弱的情况下，可以将终端切换到信号强度更好的接入网设备（例如，邻居接入网设备）的小区。

为了降低切换时延，目前引入了层1/层2触发的移动性（L1/L2 triggered mobility, LTM）切换，LTM切换可以由层1/层2的信令触发。

15 然而，针对于LTM跨站切换场景，如何实现终端与接入网设备之间的安全通信，仍需进一步研究。

发明内容

本申请提供了一种通信方法及装置，用于实现LTM跨站切换场景中终端和接入网设备之间的安全通信。

20 第一方面，本申请提供了一种通信方法，该方法可以应用于第一接入网设备，或者应用于第一接入网设备中的处理器或芯片或芯片系统或功能模块等；以该方法应用于第一接入网设备为例，第一接入网设备接收多个候选接入网设备中每个接入网设备的容器，所述每个接入网设备的容器包括用于终端切换到所述每个接入网设备的参数；向所述终端发送无线资源控制RRC重配置消息，所述RRC重配置消息包括所述多个候选接入网设备中每个接入网设备的容器；确定所述终端需要切换到所述多个候选接入网设备中的第二接入网设备；向所述终端发送第一媒体接入控制MAC层消息，所述第一MAC层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一NCC的信息，所述第一NCC用于确定所述终端与所述第二接入网设备进行通信所使用的密钥。

采用上述方法，第一接入网设备先向终端发送多个候选接入网设备中每个接入网设备的容器（携带切换参数）；进而，在终端需要切换到第二接入网设备的情况下，第一接入网设备通过第一MAC层消息发送用于指示第一NCC的信息。相比于普通切换流程（在普通切换流程中，源接入网设备确定终端需要切换时，需要先从目标接入网设备获取目标接入网设备的容器（容器中携带NCC和切换参数），进而将容器发送给终端，以触发终端执行切换）来说，由于第一接入网设备在确定终端需要切换时，便可以向终端发送第一MAC层消息来触发终端执行切换，从而能够降低切换时延；且由于第一MAC层消息中携带用于指示第一NCC的信息，便于实现终端与第二接入网设备之间的安全通信。

30 在一种可能的设计中，向所述终端发送MAC层消息，包括：所述第一接入网设备的RRC层将用于指示所述第一NCC的信息传递到所述第一接入网设备的MAC层；所述第一接入网设备的MAC层向所述终端发送所述MAC层消息。

如此，通过第一接入网设备内RRC层与MAC层之间的信息传递，将用于指示第一NCC的信息传递到MAC层，从而使得MAC层可以将用于指示第一NCC的信息和用于触发终端切换到第二接入网设备的信息一起封装到MAC层消息中以发送给终端。

40 在一种可能的设计中，所述方法还包括：接收来自移动管理网元的所述第一下一跳链路计数器NCC；所述第一NCC承载于初始上下文建立请求消息或者路径切换响应消息。

如此，第一NCC是第一接入网设备从初始上下文建立请求消息或者路径切换响应消息获取到的，进而终端可以根据源接入网设备（即第一接入网设备）获得的NCC，来确定终端与目标接入网设备（即第二接入网设备）进行通信所使用的密钥，便于实现密钥更新，提高通信安全。

45 在一种可能的设计中，所述方法还包括：向所述第二接入网设备发送第一候选接入网设备列表，所述第一候选接入网设备列表包括所述多个候选接入网设备中的至少一个候选接入网设备的标识。

如此,第一接入网设备向第二接入网设备发送第一候选接入网设备列表,从而使得第二接入网设备在确定终端需要切换时,可以根据第一候选接入网设备列表,确定是否执行 LTM 切换,便于提高切换的成功率。具体来说,由于在目标接入网设备预先将构造的容器发送给终端的情况下,终端方可通过 LTM 切换成功切换到该目标接入网设备,因此,第二接入网设备在确定终端需要切换到第三接入网设备时,根据从第一接入网设备接收到的第一候选接入网设备列表,若确定第三接入网设备属于第一候选接入网设备列表,则第二接入网设备可以确定执行 LTM 切换,若确定第三接入网设备不属于第一候选接入网设备列表,则第二接入网设备可以确定执行普通切换。

在一种可能的设计中,用于指示第一 NCC 的信息包括以下至少一项:所述第一 NCC;所述第一 NCC 的索引值;所述第一 NCC 加密后的密文。

在一种可能的设计中,所述方法还包括:生成所述第一 MAC 层消息。相比于普通切换流程(在普通切换流程中,源接入网设备确定终端需要切换时,需要先从目标接入网设备获取目标接入网设备构造的容器(容器中携带 NCC 和切换参数),进而将容器发送给终端)来说,由于第一接入网设备在确定终端需要切换时,便可以自行生成包含 NCC 的第一 MAC 层消息并向终端发送第一 MAC 层消息,从而能够降低切换时延。

第二方面,本申请提供了一种通信方法,该方法可以应用于第二接入网设备,或者应用于第二接入网设备中的处理器或芯片或芯片系统或功能模块等;以该方法应用于第二接入网设备为例,第二接入网设备向终端发送所述第二接入网设备的容器,所述容器包括用于终端切换到所述第二接入网设备的参数;在所述终端从第一接入网设备切换到所述第二接入网设备之后,确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备;向所述终端发送第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到所述第三接入网设备的信息和用于指示第二 NCC 的信息,所述第二 NCC 用于确定所述终端与所述第三接入网设备进行通信所使用的密钥。

采用上述方法,第二接入网设备可以先向终端发送第二接入网设备的容器(容器中携带切换参数),在终端根据容器中的参数从第一接入网设备切换到第二接入网设备后,第二接入网设备若确定终端需要切换到第三接入网设备,则可以通过第二 MAC 层消息发送用于指示第二 NCC 的信息。相比于普通切换流程(在普通切换流程中,源接入网设备确定终端需要切换时,需要先从目标接入网设备获取目标接入网设备的容器(容器中携带 NCC 和切换参数),进而将容器发送给终端,以触发终端执行切换)来说,由于第二接入网设备在确定终端需要切换时,便可以向终端发送第二 MAC 层消息来触发终端执行切换,便于降低切换时延;且由于第二 MAC 层消息中携带用于指示第二 NCC 的信息,便于实现终端与第三接入网设备之间的安全通信。

在一种可能的设计中,所述方法还包括:第二接入网设备生成所述第二 MAC 层消息。相比于普通切换流程(在普通切换流程中,源接入网设备确定终端需要切换时,需要先从目标接入网设备获取目标接入网设备的容器(容器中携带 NCC 和切换参数),进而将容器发送给终端)来说,由于第二接入网设备在确定终端需要切换时,便可以自行生成包含 NCC 的第二 MAC 层消息并向终端发送第二 MAC 层消息,从而能够降低切换时延。

在一种可能的设计中,向所述终端发送第二 MAC 层消息,包括:所述第二接入网设备的 RRC 层将用于指示所述第二 NCC 的信息传递到所述第二接入网设备的 MAC 层;所述第二接入网设备的 MAC 层向所述终端发送所述第二 MAC 层消息。

如此,通过第二接入网设备内 RRC 层与 MAC 层之间的信息传递,将用于指示第二 NCC 的信息传递到 MAC 层,从而使得 MAC 层可以将用于指示第二 NCC 的信息和用于触发终端切换到第三接入网设备的信息一起封装到 MAC 层消息中以发送给终端。

在一种可能的设计中,在所述终端切换到所述第二接入网设备之后,所述方法还包括:向移动管理网元发送路径切换请求消息;接收来自所述移动管理网元的路径切换响应消息,所述路径切换响应消息包括所述第二 NCC 和所述第二 NCC 对应的下一跳 NH。

如此,第二 NCC 是第二接入网设备从路径切换响应消息中获得的(即执行 LTM 切换时,发送给终端的第二 NCC 当前的源接入网设备从路径切换响应消息中获得的),便于实现密钥更新,使得终端在多个接入网设备之间来回切换时,不会出现密钥重用的问题。

在一种可能的设计中,确定所述终端需要切换到所述第三接入网设备之后,所述方法还包括:根据所述第二 NCC 对应的 NH,确定所述第三接入网设备与所述终端进行通信所使用的密钥;向所述第三

接入网设备发送所述第三接入网设备与所述终端进行通信所使用的密钥。

如此，第二接入网设备可以根据第二 NCC 对应的 NH，确定第三接入网设备与终端进行通信所使用的密钥，并发送给第三接入网设备，以使得第三接入网设备和终端维护相同的密钥。

5 在一种可能的设计中，所述方法还包括：向终端设备第三 MAC 层消息，所述第三 MAC 层消息包括用于指示所述第二 NCC 的信息，所述第二 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥；根据所述第二 NCC 对应的 NH，确定所述终端与所述第二接入网设备进行通信所使用的密钥。

10 如此，由于终端与第二接入网设备进行通信所使用的密钥是第二接入网设备中存储的第二 NCC 确定，从而使得第一接入网设备无法知晓终端与第二接入网设备进行通信所使用的密钥，便于提高通信安全。

在一种可能的设计中，在向终端发送所述第二接入网设备的容器之后，所述方法还包括：接收来自所述第一接入网设备的第一候选接入网设备列表，所述第一候选接入网设备列表包括所述至少一个候选接入网设备的标识；向所述终端发送第二 MAC 层消息，包括：若确定所述第三接入网设备属于所述第一候选接入网设备列表，则向所述终端发送所述第二 MAC 层消息。

15 如此，由于在目标接入网设备预先将构造的容器发送给终端的情况下，终端方可通过 LTM 切换成功切换到该目标接入网设备，因此，第二接入网设备在确定终端需要切换到第三接入网设备时，根据从第一接入网设备接收到的第一候选接入网设备列表，若确定第三接入网设备属于第一候选接入网设备列表，则第二接入网设备可以确定执行 LTM 切换，从而便于提高切换成功率。

20 在一种可能的设计中，确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备之后，所述方法还包括：向所述第三接入网设备发送第二候选接入网设备列表，所述第二候选接入网设备列表包括所述至少一个候选接入网设备中的部分或全部候选接入网设备的标识。

如此，第二接入网设备向第三接入网设备发送第二候选接入网设备列表，从而使得第三接入网设备在确定终端需要切换到其它接入网设备时，可以根据第二候选接入网设备列表，确定是否执行 LTM 切换，便于提高切换的成功率。

25 第三方面，本申请提供了一种通信方法，该方法可以应用于终端，或者应用于终端中的处理器或芯片或芯片系统或功能模块等；以该方法应用于终端为例，终端接收来自多个候选接入网设备中每个接入网设备的容器，所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数，所述多个候选接入网设备包括第二接入网设备；接收来自第一接入网设备的第一 MAC 层消息，所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一 NCC 的信息；
30 根据所述第二接入网设备的容器中的参数，切换到所述第二接入网设备；根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥。

采用上述方法，终端接收来自第一接入网设备的多个候选接入网设备中每个接入网设备构造的容器（容器中携带切换参数）；进而，在终端需要切换到第二接入网设备的情况下，接收来自第一接入网设备的第一 MAC 层消息（携带 NCC）。相比于普通切换流程（在普通切换流程中，源接入网设备确定终端需要切换时，需先从目标接入网设备获取目标接入网设备构造的容器（容器中携带 NCC 和切换参数），进而将容器发送给终端，以触发终端执行切换）来说，由于第一接入网设备可以向终端发送第一 MAC 层消息来触发终端执行切换，便于降低切换时延；且由于第一 MAC 层消息中携带用于指示第一 NCC 的信息，便于实现终端与第二接入网设备之间的安全通信。

可以理解的是，第一接入网设备可以为终端通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程所接入的接入网设备。在终端接入第一接入网设备后，第一接入网设备和终端可以保存相同的密钥（该密钥用于第一接入网设备和终端进行通信）和相同的 NCC（比如第一 NCC）。

45 在一种可能的设计中，根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥，包括：确定所述第一 NCC 与所述终端存储的 NCC 相同后，根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥，所述第一输入参数包括所述第一 NCC 对应的密钥 KgNB 和所述第二接入网设备上的小区的信息，比如小区的 PCI 和/或载频。

在一种可能的设计中，根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥，包括：所述终端的 MAC 层将用于指示所述第一 NCC 的信息传递到所述终端的 RRC 层；所述终端的 RRC 层根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥。

如此，通过终端内 RRC 层与 MAC 层之间的信息传递，将用于指示第一 NCC 的信息传递到 RRC 层，从而实现由 RRC 层根据第一 NCC 确定密钥。

在一种可能的设计中，所述多个候选接入网设备还包括第三接入网设备；在终端切换到所述第二接入网设备之后，所述方法还包括：接收来自所述第二接入网设备的第二 MAC 层消息，所述第二 MAC 层消息包括用于触发所述终端切换到第三接入网设备的信息和用于指示第二 NCC 的信息；根据所述第三接入网设备的容器中的参数，切换到所述第三接入网设备；根据所述第二 NCC，确定所述终端与所述第三接入网设备进行通信所使用的密钥。

在一种可能的设计中，根据所述第二 NCC，确定所述终端与所述第三接入网设备进行通信所使用的密钥，包括：确定所述第二 NCC 与所述终端存储的 NCC（具体是第一 NCC）不同后，根据第二输入参数推演得到所述终端与所述第三接入网设备进行通信所使用的密钥，所述第二输入参数包括所述第二 NCC 对应的 NH 和所述第三接入网设备上的小区的信息。

如此，由于第二 NCC 与终端存储的 NCC 不同，从而使得终端可以执行垂直推演得到终端与第三接入网设备进行通信所使用的密钥，便于提高通信安全。

在一种可能的设计中，所述方法还包括：确定所述第二 NCC 与所述终端存储的 NCC 不同后，将所述终端存储的 NCC 更新为所述第二 NCC。

第四方面，本申请提供了一种通信方法，该方法可以应用于终端，或者应用于终端中的处理器或芯片或芯片系统或功能模块等；以该方法应用于终端为例，终端接收来自多个候选接入网设备中每个接入网设备的容器，所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数，所述多个候选接入网设备包括第二接入网设备；接收来自第一接入网设备的第一 MAC 层消息，所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息；根据所述第二接入网设备的容器中的参数，切换到所述第二接入网设备；接收来自所述第二接入网设备的第三 MAC 层消息，所述第三 MAC 层消息包括用于指示第二 NCC 的信息；根据所述第二 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥。

如此，由于终端是在切换到第二接入网设备后，接收来自第二接入网设备的用于指示第二 NCC 的信息，并根据第二 NCC，确定终端与第二接入网设备进行通信所使用的密钥，从而使得源接入网设备（即第一接入网设备）无法知晓终端与第二接入网设备进行通信所使用的密钥，便于提高通信安全。

在一种可能的设计中，所述第一 MAC 层消息还包括用于指示第一 NCC 的信息；所述方法还包括：根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥，并存储在接入层 AS 安全上下文中；其中，当根据所述第二 NCC，确定出所述终端与所述第二接入网设备进行通信所使用的密钥时，将所述 AS 安全上下文中的根据所述第一 NCC 确定的所述密钥更新为根据所述第二 NCC 确定的所述密钥。

如此，终端可以先根据第一 NCC，确定终端与第二接入网设备进行通信所使用的密钥，以便于在终端向第二接入网设备切换的过程中，对终端和第二接入网设备之间的通信进行安全保护。

在一种可能的设计中，根据所述第一 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥，包括：确定所述第一 NCC 与所述终端存储的 NCC 相同后，根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥，所述第一输入参数包括所述第一 NCC 对应的密钥 KgNB 和所述第二接入网设备上的小区的信息。

在一种可能的设计中，根据所述第二 NCC，确定所述终端与所述第三接入网设备进行通信所使用的密钥，包括：确定所述第二 NCC 与所述终端存储的 NCC 不同后，根据第三输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥，所述第三输入参数包括所述第二 NCC 对应的 NH 和所述第二接入网设备上的小区的信息。

如此，由于第二 NCC 与终端存储的 NCC 不同，从而使得终端可以执行垂直推演得到终端与第二接入网设备进行通信所使用的密钥，便于提高通信安全。

在一种可能的设计中，所述方法还包括：确定所述第二 NCC 与所述终端存储的 NCC 不同后，将所述终端存储的 NCC 更新为所述第二 NCC。

在一种可能的设计中，根据所述第二 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥，包括：所述终端的 MAC 层将用于指示所述第二 NCC 的信息传递到所述终端的 RRC 层；所述终端的 RRC 层根据所述第二 NCC，确定所述终端与所述第二接入网设备进行通信所使用的密钥。

在一种可能的设计中,所述多个候选接入网设备还包括第三接入网设备;在所述终端切换到所述第二接入网设备之后,所述方法还包括:接收来自所述第二接入网设备的第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到第三接入网设备的信息;根据所述第三接入网设备的容器中的参数,切换到所述第三接入网设备;接收来自所述第三接入网设备的第四 MAC 层消息,所述第四 MAC 层消息包括用于指示第三 NCC 的信息;根据所述第三 NCC,确定所述终端与所述第三接入网设备进行通信所使用的密钥。

在一种可能的设计中,所述第二 MAC 层消息还包括用于指示所述第二 NCC 的信息;所述方法还包括:根据所述第二 NCC,确定所述终端向所述第三接入网设备发送切换完成消息所使用的密钥,并存储在 AS 安全上下文中;其中,当根据所述第三 NCC,确定出所述终端与所述第三接入网设备进行通信所使用的密钥时,将所述 AS 安全上下文中的根据所述第二 NCC 确定的所述密钥更新为根据所述第三 NCC 确定的所述密钥。

上述第一方面至第四方面提供的通信方法相互对应,第一方面至第四方面中相互对应的技术特征的有益效果可以相互参照。

第五方面,本申请提供了一种通信方法,该方法可以应用于第一接入网设备,或者应用于第一接入网设备中的处理器或芯片或芯片系统或功能模块等;以该方法应用于第一接入网设备为例,第一接入网设备向多个候选接入网设备中每个接入网设备发送切换请求消息,所述切换请求消息包括第一 NCC;接收来自所述多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括所述第一 NCC;向所述终端发送 RRC 重配置消息,所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入网设备的容器;确定所述终端需要切换到的第二接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备,所述多个候选接入网设备包括第二接入网设备;向所述终端发送第一 MAC 层消息,所述第一 MAC 层消息用于触发终端切换到所述第二接入网设备。

采用上述方法,由于多个候选接入网设备中每个接入网设备构造的容器携带第一 NCC,进而终端在切换到其中任一接入网设备后,是根据该接入网设备构造的容器中携带的第一 NCC (以及该接入网设备上的小区的信息),来确定终端与该接入网设备进行通信所使用的密钥,实现较为简便;进一步地,在执行 LTM 切换时,第一接入网设备(即源接入网设备)可以判断第二接入网设备(即目标接入网设备)是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备,若是,则可以执行 LTM 切换,否则执行普通切换,从而可以使得终端在多个候选接入网设备之间来回切换时,不会出现密钥重用的问题。

在一种可能的设计中,所述每个接入网设备的容器中包括的所述第一 NCC 用于确定终端与所述每个接入网设备进行通信的密钥。

在一种可能的设计中,所述方法还包括:接收来自移动管理网元的所述第一 NCC,所述第一 NCC 承载于初始上下文建立请求消息或者路径切换响应消息。

在一种可能的设计中,所述方法还包括:向所述第二接入网设备发送 LTM 连续切换次数。

在一种可能的设计中,所述方法还包括:向所述第二接入网设备发送第三候选接入网设备列表,所述第三候选接入网设备列表包括至少一个候选接入网设备的标识。比如,第三候选接入网设备列表包括多个候选接入网设备中、对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

如此,第一接入网设备向第二接入网设备发送第三候选接入网设备列表,从而使得第二接入网设备在确定终端需要切换到第三接入网设备时,可以根据第三候选接入网设备列表,确定第三接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备,使得终端在多个候选接入网设备之间来回切换时,不会出现密钥重用的问题。

第六方面,本申请提供了一种通信方法,该方法可以应用于第二接入网设备,或者应用于第二接入网设备中的处理器或芯片或芯片系统或功能模块等;以该方法应用于第二接入网设备为例,第二接入网设备接收来自第一接入网设备的切换请求消息,所述切换请求消息包括第一 NCC;向所述第一接入网设备发送所述第二接入网设备的容器,所述容器包括所述第一 NCC 和用于终端切换到所述第二接入网设备的参数;所述容器中包括的所述第一 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥;在所述终端切换到所述第二接入网设备后,确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备;向所述终端发送第二 MAC 层消息,所述第二 MAC 层消息用于触发终端切换到所述第三接入网设备。

采用上述方法，由于第二接入网设备构造的容器包括第一 NCC，因此终端可以根据第一 NCC 确定终端与所述第二接入网设备进行通信所使用的密钥，便于实现终端与所述第二接入网设备之间的安全通信；在确定终端需要切换到第三接入网设备时，第二接入网设备（即源接入网设备）可以判断第三接入网设备（即目标接入网设备）是否对于终端的连续 LTM 切换过程中还未被切换过的接入网设备，若是，则可以执行 LTM 切换，否则执行普通切换，从而可以使得终端在多个候选接入网设备之间来回切换时，不会出现密钥重用的问题。

在一种可能的设计中，在所述终端切换到所述第二接入网设备后，所述方法还包括：接收来自移动管理网元的第二 NCC，所述第二 NCC 承载于路径切换响应消息；向所述终端发送第二 MAC 层消息，包括：若所述第二 NCC 的取值不属于预设值，则向所述终端发送第二 MAC 层消息。

在一种可能的设计中，所述方法还包括：若所述第一 NCC 的取值属于所述预设值，则向所述终端发送 RRC 重配置消息，所述 RRC 重配置消息用于触发所述终端切换到所述第三接入网设备。

如此，当 NCC 取值为预设值（预设值可以包括 0 和 7），即当 NCC 即将翻转（取值为 7）或者刚刚翻转（取值为 0）时，可以执行普通切换，以通过切换命令消息向终端发送更新的 NCC，便于保证后续终端和接入网设备推演的密钥一致。

在一种可能的设计中，所述方法还包括：接收来自第一接入网设备的 LTM 连续切换次数；向所述终端发送第二 MAC 层消息，包括：若所述 LTM 连续切换次数小于或等于阈值，则向所述终端发送第二 MAC 层消息。

在一种可能的设计中，所述方法还包括：若所述 LTM 连续切换次数大于所述阈值，则向终端发送 RRC 重配置消息，RRC 重配置消息用于触发所述终端切换到所述第三接入网设备。

如此，当 LTM 连续切换次数大于所述阈值时，可以执行普通切换，以通过切换命令消息向终端发送更新的 NCC，便于保证后续终端和接入网设备推演的密钥一致。

在一种可能的设计中，在所述终端切换到所述第二接入网设备之前，所述方法还包括：接收来自所述第一接入网设备的第三候选接入网设备列表，所述第三候选接入网设备列表包括至少一个候选接入网设备的标识；确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备，包括：若所述第三接入网设备属于所述第三候选接入网设备列表，则确定所述第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备。

在一种可能的设计中，所述方法还包括：向所述第三接入网设备发送第四候选接入网设备列表，所述第四候选接入网设备列表不包括第二候选接入网设备的标识。

如此，每次执行 LTM 切换时，源接入网设备可以向目标接入网设备发送候选接入网设备列表，以便于目标接入网设备在确定终端需要切换时，可以根据接收到的候选接入网设备列表确定是否执行 LTM 切换，实现较为简便。

第七方面，本申请提供了一种通信方法，该方法可以应用于终端，或者应用于终端中的处理器或芯片或芯片系统或功能模块等；以该方法应用于终端为例，终端接收来自第一接入网设备的 RRC 重配置消息，所述 RRC 重配置消息包括多个候选接入网设备中每个接入网设备的容器，所述每个接入网设备的容器包括第一 NCC，所述多个候选接入网设备包括第二接入网设备；接收来自所述第一接入网设备的第一 MAC 层消息，所述第一 MAC 层消息用于触发所述终端切换到所述第二接入网设备；在所述终端切换到所述第二接入网设备之后，使用所述第二接入网设备对应的密钥与所述第二接入网设备进行通信，所述第二接入网设备对应的密钥是根据所述第一 NCC 确定的。

在一种可能的设计中，方法还包括：根据所述第一 NCC，确定所述第二接入网设备对应的密钥。具体地，在所述第一 NCC 与所述终端存储的 NCC 相同的情况下，根据第一输入参数推演得到所述第二接入网设备对应的密钥，所述第一输入参数包括所述第二接入网设备上的小区的信息。

第八方面，本申请提供了一种通信方法，该方法可以应用于第一接入网设备，或者应用于第一接入网设备中的处理器或芯片或芯片系统或功能模块等；以该方法应用于第一接入网设备为例，第一接入网设备向多个候选接入网设备分别发送切换请求消息（也即是向多个候选接入网设备中每个候选接入网设备发送切换请求消息）；接收来自所述多个候选接入网设备中每个接入网设备的容器，所述每个接入网设备的容器包括所述每个接入网设备对应的 NCC；所述每个接入网设备对应的 NCC 用于确定终端与所述每个接入网设备进行通信所使用的密钥；向所述终端发送 RRC 重配置消息，所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入网设备构造的容器；其中，所述每个接入网设备对应的 NCC 不

同, 也即是所述多个候选接入网设备中不同接入网设备对应不同的 NCC。

采用上述方法, 由于多个候选接入网设备中每个接入网设备构造的容器携带每个接入网设备对应的 NCC, 进而终端在切换到其中任一接入网设备后, 是根据该接入网设备构造的容器中携带的 NCC (以及该接入网设备上的小区的信息), 来确定终端与该接入网设备进行通信所使用的密钥, 便于提高通信安全。

在一种可能的设计中, 所述方法还包括: 确定所述多个候选接入网设备, 所述多个候选接入网设备的个数小于或等于阈值, 所述阈值是根据所述第一接入网设备对应的 NCC 确定的。

如此, 便于保证多个候选接入网设备不同接入网设备对应不同的 NCC。比如, 该阈值等于 NCC 的最大值减去第一接入网设备对应的 NCC; 也就是说, 第一接入网设备确定的候选接入网设备的个数应小于或等于阈值, 以避免不同接入网设备对应的 NCC 相同。

在一种可能的设计中, 所述方法还包括: 确定终端需要切换到的第二接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备; 向所述终端发送第一 MAC 层消息, 所述第一 MAC 层消息用于触发终端切换到所述第二接入网设备。

如此, 在执行 LTM 切换时, 第一接入网设备 (即源接入网设备) 可以判断第二接入网设备 (即目标接入网设备) 是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 若是, 则可以执行 LTM 切换, 否则执行普通切换, 从而可以使得终端在多个候选接入网设备之间来回切换时, 不会出现密钥重用的问题。

在一种可能的设计中, 所述方法还包括: 向所述第二接入网设备发送第三候选接入网设备列表, 所述第三候选接入网设备列表包括至少一个候选接入网设备的标识。比如, 第三候选接入网设备列表包括多个候选接入网设备中、对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

如此, 第一接入网设备可以向第二接入网设备发送第三候选接入网设备列表, 以便于第二接入网设备在确定终端需要切换时, 可以根据接收到的第三候选接入网设备列表确定是否执行 LTM 切换, 实现较为简便。

第九方面, 本申请提供了一种通信方法, 该方法可以应用于第二接入网设备, 或者应用于第二接入网设备中的处理器或芯片或芯片系统或功能模块等; 以该方法应用于第二接入网设备为例, 第二接入网设备接收来自第一接入网设备的切换请求消息; 在接收所述切换请求消息之后, 向移动管理网元发送请求消息, 所述请求消息用于请求所述第二接入网设备对应的 NCC; 接收来自所述核心网设备的所述 NCC; 向所述第一接入网设备发送切换请求确认消息, 所述切换请求确认消息包括所述第二接入网设备构造的容器, 所述容器包括所述 NCC, 所述 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥。

如此, 由于第二接入网设备构造的容器中所携带的 NCC 是第二接入网设备从移动管理网元获取的, 从而使得第二接入网设备与其它候选接入网设备对应的 NCC 不同, 便于提高通信安全。

在一种可能的设计中, 所述切换请求消息包括指示信息, 所述指示信息用于指示所述切换请求消息对应 LTM 切换。

如此, 第二接入网设备可响应于切换请求消息, 向移动管理网元请求第二接入网设备对应的 NCC。

在一种可能的设计中, 所述方法还包括: 接收来自所述核心网设备的所述 NCC 对应的 NH; 根据所述 NCC 对应的 NH, 确定与所述终端进行通信所使用的密钥。

在一种可能的设计中, 在所述终端从第一接入网设备切换到所述第二接入网设备之后, 所述方法还包括: 确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备; 向所述终端发送第二 MAC 层消息, 所述第二 MAC 层消息用于触发终端切换到所述第三接入网设备。

如此, 在执行 LTM 切换时, 第二接入网设备 (即源接入网设备) 可以判断第三接入网设备 (即目标接入网设备) 是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 若是, 则可以执行 LTM 切换, 否则执行普通切换, 从而可以使得终端在多个候选接入网设备之间来回切换时, 不会出现密钥重用的问题。

在一种可能的设计中, 在所述终端从第一接入网设备切换到所述第二接入网设备之前, 所述方法还包括: 接收来自所述第一接入网设备的第三候选接入网设备列表; 确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备, 包括: 若所述第三接入网设备

属于所述第三候选接入网设备列表，则确定所述第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备。

在一种可能的设计中，所述方法还包括：向所述第三接入网设备发送第二候选接入网设备列表，所述第二候选接入网设备列表不包括第二候选接入网设备的标识。

5 第十方面，本申请提供了一种通信方法，该方法可以应用于终端，或者应用于终端中的处理器或芯片或芯片系统或功能模块等；以该方法应用于终端为例，终端接收来自第一接入网设备的 RRC 重配置消息，所述 RRC 重配置消息包括多个候选接入网设备的标识和多个 NCC 的对应关系；根据所述多个候选接入网设备对应的 NCC，确定所述多个候选接入网设备对应的密钥；其中，所述多个候选接入网设备中不同接入网设备对应的 NCC 不同；接收来自所述第一接入网设备的第一 MAC 层消息，所述第
10 一 MAC 层消息用于触发所述终端切换到所述第二接入网设备，所述多个候选接入网设备包括第二接入网设备；在所述终端切换到所述第二接入网设备之后，使用所述第二接入网设备对应的密钥，与所述第二接入网设备进行通信。

在一种可能的设计中，根据所述第二接入网设备对应的 NCC，确定所述第二接入网设备对应的密钥，包括：根据第二输入参数，推演得到所述第二接入网设备对应的密钥；所述第二输入参数包括所述
15 第二接入网设备对应的 NCC 所对应的 NH 和所述第二接入网设备上的小区的信息。

在一种可能的设计中，所述方法还包括：根据所述多个 NCC，按照 NCC 升序的方式依次推演所述多个 NCC 对应的 NH。

如此，终端按照 NCC 升序的方式依次推演所述多个 NCC 对应的 NH，从而便于快速推演 NH，节省终端的处理负担。

20 在一种可能的设计中，所述多个候选接入网设备还包括第三接入网设备；所述方法还包括：接收来自所述第二接入网设备的第二 MAC 层消息，所述第二 MAC 层消息用于触发所述终端切换到所述第三接入网设备；在所述终端切换到所述第三接入网设备之后，使用所述第三接入网设备对应的密钥，与所述第三接入网设备进行通信。

在一种可能的设计中，所述方法还包括：响应于所述第二 MAC 层消息，删除第二接入网设备对应的
25 的 NCC。如此，便于及时释放终端的存储资源。

第十一方面，本申请提供一种通信装置，所述通信装置具备实现上述第一方面至第十方面中任一方面涉及的功能，比如，所述通信装置包括执行上述第一方面至第十方面中任一方面涉及操作所对应的模块或单元或手段，所述功能或单元或手段可以通过软件实现，或者通过硬件实现，也可以通过硬件执行相应的软件实现。

30 在一种可能的设计中，所述通信装置包括处理单元、通信单元，其中，通信单元可以用于收发信号，以实现该通信装置和其它装置之间的通信，比如，通信单元用于向终端发送系统信息；处理单元可以用于执行该通信装置的一些内部操作。处理单元、通信单元执行的功能可以和上述第一方面至第十方面中任一方面涉及的操作相对应。

在一种可能的设计中，所述通信装置包括处理器，处理器可以用于与存储器耦合。所述存储器可以
35 保存实现上述第一方面至第十方面中任一方面涉及的功能的必要计算机程序或指令。所述处理器可执行所述存储器存储的计算机程序或指令，当所述计算机程序或指令被执行时，使得所述通信装置实现上述第一方面至第十方面中任一方面任意可能的设计或实现方式中的方法。

在一种可能的设计中，所述通信装置包括处理器和存储器，存储器可以保存实现上述第一方面至第十方面涉及的功能的必要计算机程序或指令。所述处理器可执行所述存储器存储的计算机程序或指令，
40 当所述计算机程序或指令被执行时，使得所述通信装置实现上述第一方面至第十方面中任一方面任意可能的设计或实现方式中的方法。

在一种可能的设计中，所述通信装置包括处理器和接口电路，其中，处理器用于通过所述接口电路与其它装置通信，并执行上述第一方面至第十方面中任一方面任意可能的设计或实现方式中的方法。

可以理解地，上述第三方面中，处理器可以通过硬件来实现也可以通过软件来实现，当通过硬件实现时，该处理器可以是逻辑电路、集成电路等；当通过软件来实现时，该处理器可以是一个通用处理器，
45 通过读取存储器中存储的软件代码来实现。此外，以上处理器可以是一个或多个，存储器可以是一个或多个。存储器可以与处理器集成在一起，或者存储器与处理器分离设置。在具体实现过程中，存储器可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型以及

存储器与处理器的设置方式不做限定。

第十二方面,本申请提供一种通信系统,该通信系统可以包括第一接入网、第二接入网设备和终端。其中,第一接入网设备用于执行上述第一方面所述的方法,第二接入网设备用于执行上述第二方面所述的方法,终端用于执行上述第三方面或第四方面所述的方法;或者,第一接入网设备用于执行上述第五方面所述的方法,第二接入网设备用于执行上述第六方面所述的方法,终端用于执行上述第七方面所述的方法;或者,第一接入网设备用于执行上述第八方面所述的方法,第二接入网设备用于执行上述第九方面所述的方法,终端用于执行上述第十方面所述的方法。

第十三方面,本申请提供一种计算机可读存储介质,所述计算机存储介质中存储有计算机程序(或计算机可读指令),当计算机读取并执行部分或全部所述计算机可读指令时,上述第一方面至第十方面的任一种可能的设计中的方法被执行。

示例性的,计算机可读存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于:计算机可读介质可以包括非瞬态计算机可读介质、随机存取存储器(random-access memory, RAM)、只读存储器(read-only memory, ROM)、电可擦除可编程只读存储器(electrically EPROM, EEPROM)、CD-ROM 或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。

第十四方面,本申请提供一种计算机程序产品,当计算机读取并执行所述计算机程序产品时,使得上述第一方面至第十方面的任一种可能的设计中的方法被执行。

第十五方面,本申请提供一种芯片(或芯片系统),所述芯片包括处理器,所述处理器与存储器耦合,所述存储器中存储有计算机程序;所述处理器用于调用所述存储器中的部分或全部所述计算机程序,使得上述第一方面至第十方面的任一种可能的设计中的方法被执行。

附图说明

- 图 1 为本申请实施例适用的一种网络架构示意图;
- 图 2 为本申请实施例提供的接入网设备和终端执行密钥推演的流程示意图;
- 图 3 为本申请实施例提供的普通跨站切换的一种可能的流程示意图;
- 图 4 为本申请实施例提供的 LTM 跨站切换的一种可能的流程示意图;
- 图 5 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 6 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 7 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 8 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 9 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 10 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 11 为本申请实施例提供的通信方法所对应的流程示意图;
- 图 12 为本申请实施例中所涉及的装置的可能的示例性框图;
- 图 13 为本申请实施例提供的一种通信装置的结构示意图。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚,下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。

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

本申请提供的技术方案可以应用于各种通信系统,例如:第五代(5th generation, 5G)或新无线(new radio, NR)系统、长期演进(long term evolution, LTE)系统、LTE 频分双工(frequency division duplex, FDD)系统、LTE 时分双工(time division duplex, TDD)系统等。本申请提供的技术方案还可以应用

于未来的通信系统，如第六代移动通信系统。本申请提供的技术方案还可以应用于设备到设备（device to device, D2D）通信，车到万物（vehicle-to-everything, V2X）通信，机器到机器（machine to machine, M2M）通信，机器类型通信（machine type communication, MTC），以及物联网（internet of things, IoT）通信系统或者其他通信系统。

5 下面将结合图 1 中的（a）和图 1 中的（b）举例说明本申请实施例适用的 5G 系统。应理解，本文中描述的 5G 系统仅是示例，不应对本申请构成任何限定。还应理解，5G 系统中某些网元之间可以采用服务化接口，或点对点的接口进行通信，下面结合图 1 中的（a）和图 1 中的（b）分别介绍基于点对点接口的 5G 系统框架，以及基于服务化接口的 5G 系统框架。

10 作为示例性说明，图 1 中的（a）示出了本申请实施例适用的 5G 系统 100a 的架构示意图。图 1 中的（a）为基于服务化接口的 5G 网络架构示意图。如图 1 中的（a）所示，该网络架构可以包括但不限于以下网元（或者称为功能网元、功能实体、节点、设备等）：

（无线）接入网（radio access network, (R)AN）设备、接入和移动性管理功能（access and mobility management function, AMF）网元、会话管理功能（session management function, SMF）网元、用户面功能（user plane function, UPF）网元、策略控制功能（policy control function, PCF）网元、统一数据管理（unified data management, UDM）网元、应用功能（application function, AF）网元、数据网络（data network, DN）、认证服务器功能（authentication server function, AUSF）网元、统一数据管理（unified data management, UDM）网元、统一数据存储（unified data repository, UDR）等。

下面对图 1 中的（a）中示出的各网元进行简单介绍：

1、用户设备（user equipment, UE）：可以称为终端设备（terminal equipment）、终端装置、接入终端、用户单元、用户站、移动站、移动台（mobile station, MS）、移动终端（mobile terminal, MT）、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。终端可以是一种向用户提供语音/数据连通性的设备，例如，具有无线连接功能的手持式设备、车载设备等。目前，一些终端的举例可以为：手机（mobile phone）、平板电脑（pad）、带无线收发功能的电脑（如笔记本电脑、掌上电脑等）、移动互联网设备（mobile internet device, MID）、虚拟现实（virtual reality, VR）设备、增强现实（augmented reality, AR）设备、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程医疗（remote medical）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端、蜂窝电话、无绳电话、会话启动协议（session initiation protocol, SIP）电话、无线本地环路（wireless local loop, WLL）站、个人数字助理（personal digital assistant, PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、5G 网络中的终端设备或者未来演进的公用陆地移动通信网络（public land mobile network, PLMN）中的终端等。

此外，终端还可以是物联网（Internet of things, IoT）系统中的终端。IoT 是未来信息技术发展的重要组成部分，其主要技术特点是将物品通过通信技术与网络连接，从而实现人机互连，物物互连的智能化网络。IoT 技术可以通过例如窄带（narrow band, NB）技术，做到海量连接，深度覆盖，终端省电。

此外，终端还可以包括智能打印机、火车探测器等，主要功能包括收集数据（部分终端设备）、接收网络设备的控制信息与下行数据，并发送电磁波，向网络设备传输上行数据。

应理解，终端可以是任何可以接入网络的设备。终端与接入网设备之间可以采用某种空口技术相互通信。

40 可选地，终端可以用于充当基站。例如，终端可以充当调度实体，其在 V2X 或 D2D 等中的终端之间提供侧行链路信号。比如，蜂窝电话和汽车利用侧行链路信号彼此通信。蜂窝电话和智能家居设备之间通信，而无需通过基站中继通信信号。

2、（无线）接入网设备：本申请实施例中简称为接入网设备，用于为特定区域的授权用户设备提供接入网功能，并能够根据用户设备的级别，业务的需求等使用不同服务质量的传输隧道。

45 接入网设备能够管理无线资源，为用户设备提供接入服务，进而完成控制信号和数据在用户设备和核心网之间的转发，接入网设备也可以理解为传统网络中的基站。

示例性地，本申请实施例中的接入网设备可以是用于与用户设备通信的任意一种具有无线收发功能的通信设备。该接入网设备包括但不限于为演进型节点 B（evolved Node B, eNB）或 5G 系统中的 gNB，

或传输点 (TRP 或 TP)，或 5G 系统中的基站的一个或一组 (包括多个天线面板) 天线面板，或者还可以为构成 gNB 或传输点的网络节点，如基带单元 (BBU)，或分布式单元 (distributed unit, DU) 等。

在一些部署中，gNB 可以包括集中式单元 (centralized unit, CU) 和 DU。gNB 还可以包括有源天线单元 (active antenna unit, AAU)。CU 实现 gNB 的部分功能，DU 实现 gNB 的部分功能。比如，CU 负责处理非实时协议和服务，实现无线资源控制 (radio resource control, RRC)，分组数据汇聚层协议 (packet data convergence protocol, PDCP) 层的功能。DU 负责处理物理层协议和实时服务，实现无线链路控制 (radio link control, RLC) 层、媒体接入控制 (media access control, MAC) 层和物理 (physical, PHY) 层的功能。AAU 实现部分物理层处理功能、射频处理及有源天线的相关功能。由于 RRC 层的信息最终会变成 PHY 层的信息，或者由 PHY 层的信息转变而来，因而，在这种架构下，高层信令，如 RRC 层信令，也可以认为是由 DU 发送的，或者，由 DU+AAU 发送的。可以理解的是，接入网设备可以为包括 CU 节点、DU 节点、AAU 节点中一项或多项的设备。此外，可以将 CU 划分为接入网中的接入网设备，也可以将 CU 划分为核心网 (core network, CN) 中的接入网设备，本申请对此不做限定。

3、UPF 网元：用于分组路由和转发以及用户面数据的服务质量 (quality of service, QoS) 处理等。

4、AMF 网元：接入和移动管理功能网元主要用于移动性管理和接入管理等，可以用于实现 MME 功能中除会话管理之外的其它功能，例如接入授权/鉴权等功能。

5、SMF 网元：主要用于会话管理、用户设备的网络互连协议 (internet protocol, IP) 地址分配和管理、选择可管理用户平面功能、策略控制和计费功能接口的终结点以及下行数据通知等。

6、PCF 网元：用于指导网络行为的统一策略框架，为控制面功能网元 (例如 AMF, SMF 等) 提供策略规则信息等。

7、AF：用于进行应用影响的数据路由，无线接入网络开放功能网元，与策略框架交互进行策略控制等。

8、UDM 网元：用于处理 UE 标识，接入鉴权，注册以及移动性管理等。

9、AUSF 网元：用于鉴权服务、产生密钥实现对用户设备的双向鉴权，支持统一的鉴权框架。

10、UDR：用于存储 UDM 网元的签约信息、PCF 网元的策略信息等。

11、DN：DN 是位于运营商网络之外的网络，运营商网络可以接入多个 DN，DN 上可部署多种业务，可为终端设备提供数据和/或语音等服务。例如，DN 是某智能工厂的私有网络，智能工厂安装在车间的传感器可为终端设备，DN 中部署了传感器的控制服务器，控制服务器可为传感器提供服务。传感器可与控制服务器通信，获取控制服务器的指令，根据指令将采集的传感器数据传送给控制服务器等。又例如，DN 是某公司的内部办公网络，该公司员工的手机或者电脑可为终端设备，员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。

图 1 中的 (a) 中 Nausf、Nnef、Npcf、Nudm、Naf、Namf、Nsmf、N1、N2、N3、N4，以及 N6 为接口序列号。这些接口序列号的含义可参见 3GPP 标准协议中定义的含义，在此不做限制。

在图 1 中的 (a) 所示的网络架构中，各网元之间可以通过图中所示的接口通信。比如，UE 和 AMF 之间可以通过 N1 接口进行交互，交互消息例如可以称为 N1 消息 (N1 Message)。RAN 和 AMF 之间可以通过 N2 接口进行交互，N2 接口可以用于非接入层 (non-access stratum, NAS) 消息的发送等。RAN 和 UPF 之间可以通过 N3 接口进行交互，N3 接口可以用于传输用户面的数据等。SMF 和 UPF 之间可以通过 N4 接口进行交互，N4 接口可以用于传输例如 N3 连接的隧道标识信息，数据缓存指示信息，以及下行数据通知消息等信息。UPF 和 DN 之间可以通过 N6 接口进行交互，N6 接口可以用于传输用户面的数据等。其他接口与各网元之间的关系如图 1 中的 (a) 所示，为了简洁，这里不一一详述。

如图 1 中的 (b) 所示，为基于点对点接口的 5G 网络架构示意图，其中的网元的功能的介绍可以参考图 1 中的 (a) 对应的网元的功能的介绍，不再赘述。图 1 中的 (b) 与图 1 中的 (a) 的主要区别在于：图 1 中的 (b) 中的各个网元之间的接口是点对点的接口，而不是服务化的接口。

在图 1 中的 (b) 所示的架构中，各个网元之间的接口名称及功能如下：

1) N7：PCF 与 SMF 之间的接口，用于下发协议数据单元 (protocol data unit, PDU) 会话粒度以及业务数据流粒度控制策略。

2) N15：PCF 与 AMF 之间的接口，用于下发 UE 策略及接入控制相关策略。

3) N5：AF 与 PCF 之间的接口，用于应用业务请求下发以及网络事件上报。

4) N4：SMF 与 UPF 之间的接口，用于控制面与用户面之间传递信息，包括控制面向用户面的转

发规则、QoS 控制规则、流量统计规则等的下发以及用户面的信息上报。

5) N11: SMF 与 AMF 之间的接口, 用于传递 RAN 和 UPF 之间的 PDU 会话隧道信息、传递发送给 UE 的控制消息、传递发送给 RAN 的无线资源控制信息等。

6) N2: AMF 与 RAN 之间的接口, 用于传递核心网侧至 RAN 的无线承载控制信息等。

5 7) N1: AMF 与 UE 之间的接口, 接入无关, 用于向 UE 传递 QoS 控制规则等。

8) N8: AMF 与 UDM 间的接口, 用于 AMF 向 UDM 获取接入与移动性管理相关签约数据与鉴权数据, 以及 AMF 向 UDM 注册 UE 当前移动性管理相关信息等。

9) N10: SMF 与 UDM 间的接口, 用于 SMF 向 UDM 获取会话管理相关签约数据, 以及 SMF 向 UDM 注册 UE 当前会话相关信息等。

10 10) N35: UDM 与 UDR 间的接口, 用于 UDM 从 UDR 中获取用户签约数据信息。

11) N36: PCF 与 UDR 间的接口, 用于 PCF 从 UDR 中获取策略相关签约数据以及应用数据相关信息。

12) N12: AMF 和 AUSF 间的接口, 用于 AMF 向 AUSF 发起鉴权流程, 其中可携带 SUCI 作为签约标识;

13) N13: UDM 与 AUSF 间的接口, 用于 AUSF 向 UDM 获取用户鉴权向量, 以执行鉴权流程。

为了便于理解本申请实施例, 下面对本申请涉及到的部分术语做示例性说明。可以理解的是, 下面给出的术语是以当前 NR 系统为例进行说明的, 但应理解, 在其他通信系统 (如未来第六代通信系统) 中, 以下术语可能有其他名称, 本申请对此不作限定。

20 1、密钥推演

为保证终端与网络侧之间能够安全地进行数据传输, 终端和网络侧都需要执行相同的密钥推演, 确保终端与网络侧使用相同的密钥。其中, “网络侧”可以包括接入网设备 (比如 gNB)。其中, “推演”也可以替换为“派生”或其它描述, 不做限定。

密钥推演相关的参数包括下一跳 (next hop, NH)、NH 链路计数器 (next hop chaining count, NCC)。

25 NH: 每当需要在终端和接入网设备之间建立接入层 (access stratum, AS) 安全性上下文时, 移动管理网元 (如 AMF 网元) 和终端导出 KgNB 和 NH。NH 由终端和 AMF 网元使用链式推衍得到, 即本次生成的 NH 将用于生成下次的 NH, 使得 NH 能够以前向安全的方式从 AMF 网元提供给 gNB。

30 NCC: 由 AMF 网元下发, 与每个 KgNB 和 NH 相关联, 用于统计 NH 密钥链的衍生次数及同步终端和接入网设备之间的密钥链, 决定下一个 KNG-RAN*是从当前的 KgNB 派生还是从新的 NH 派生。每个 KgNB 与 NH 值对应的 NCC 相关联。初始接入时, KgNB 直接从 KAMF 派生, 可以认为 KgNB 与 NCC=0 的虚拟 NH 相关联。初始接入时, 派生出的 NH 与 NCC=1 相关联。

其中, KNG-RAN*是终端和接入网设备在进行水平或垂直密钥派生时的中间密钥。在切换后使用 KNG-RAN*作为 KgNB。KNG-RAN*既可以由当前激活的 KgNB 派生, 也可以由 NH 派生。如果 KNG-RAN*由当前激活的 KgNB 派生, 则称为水平密钥派生, 接入网设备向终端指示不增加 NCC。如果 KNG-RAN*由 NH 派生, 则称为垂直密钥派生, 接入网设备向终端指示增加 NCC。如果当前接入网设备中有未被使用的 {NH, NCC}, 则采用垂直密钥派生。如果当前接入网设备中没有未被使用的 {NH, NCC} 对, 则采用水平密钥派生。比如初始接入时, 由于此时 AMF 网元不向接入网设备发送 NH, 因此下一次切换只能采用水平密钥派生。

下面以网络侧为例具体介绍密钥推演, 终端侧参考理解, 不再赘述。

40 图 2 为接入网设备和终端执行密钥推演的流程示意图。

水平推演:

45 初始接入时, gNB 可以根据密钥 KAMF 和 NAS 上行计数值, 推演初始密钥 KgNB, 并根据初始密钥 KgNB 推演 KgNB1。后续, 若要执行水平推演, 则 gNB 可以根据 KgNB1、终端当前驻留的小区的物理小区标识 (physical cell identifier, PCI) 以及载频 (frequency), 例如下行载频 (DL frequency), 推演密钥 KgNB2。如果继续执行水平推演, 则 gNB 可以根据密钥 KgNB2、终端当前驻留的小区的 PCI 以及载频, 推演密钥 KgNB3。依此类推, 从而迭代更新密钥 KgNB, 以确保通信安全。

垂直推演:

AMF 网元可以更新 NCC (比如切换过程中发生路径迁移或切换时, AMF 网元可以更新 NCC), 如

果 NCC1 更新为 NCC2, 则 AMF 网元根据密钥 KAMF 和 NH1, 推演 NH2, NH2 与 NCC2 关联, 作为新的一对 {NH2, NCC2}, AMF 网元可以将 {NH2, NCC2} 发送给 gNB, 进而 gNB 在接收到 {NH2, NCC2} 后, 在需要推演 KNG-RAN* 时, 可以执行垂直推演, 即根据 NH2、终端当前驻留的小区的 PCI 以及载频, 推演密钥 KgNB4, 以此类推。

- 5 根据图 2 可知, 垂直推演的次数可以由 NCC 取值更新前后的差值决定。例如, 如果 NCC 取值从 NCC0 更新为 NCC1, 则可以根据与 NCC0 相关的 NH0, 执行 1 次垂直推演, 得到与 NCC1 相关的 NH1。如果 NCC 取值从 NCC0 更新为 NCC2, 则可以根据与 NCC0 相关的 NH0, 执行 2 次垂直推演, 得到与 NCC2 相关的 NH2。如果 NCC 取值从 NCC2 更新为 NCC3, 则可以根据与 NCC2 相关的 NH2, 执行 1 次垂直推演, 得到与 NCC3 相关的 NH3。

10 2、切换 (handover)

切换是终端在 RRC 连接态下的一种过程, 由网络侧发起, 涉及终端与接入网设备之间的信令交互。例如, 接入网设备在感知到终端在自身小区内的信号强度逐渐变弱的情况下, 可以将终端切换到信号强度更好的接入网设备 (例如, 邻居接入网设备) 的小区。可以理解的是, 切换可以是终端在不同接入网设备的小区之间切换 (即跨站切换), 比如终端设备从接入网设备 1 的小区切换到接入网设备 2 的小区; 或者, 也可以是指终端在同一接入网设备的小区之间切换, 比如终端设备接入网设备 1 的小区 1 切换到接入网设备 1 的小区 2。本申请实施例将以跨站切换场景为例进行描述。

由层 3 的信令触发的切换流程, 可以称为层 3 切换 (L3 handover) 或普通切换。层 3 可以是指 RRC 层, 下文中的层 1 可以是指物理层, 下文中的层 2 可以是指 MAC 层。

- 20 图 3 为普通跨站切换的一种可能的流程示意图。图 3 所示意的跨站切换包括终端从接入网设备 0 切换到接入网设备 1, 再从接入网设备 1 切换到接入网设备 2。如图 3 所示, 该流程包括:

S301, 终端通过接入网设备 0 连接到 5GC。

终端可以通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程接入到接入网设备 0, 通过接入网设备 0 接入到 5GC。进而, 终端和接入网设备 0 上分别保存密钥 KgNB (为便于描述, 称为 K0) 和 NCC0 (K0 关联 NCC0), AMF 网元上保存 NCC0。

- 25 需要说明的是, 本申请实施例中 NCC 后面所携带的数字仅用于区分不同的 NCC, 并不代表具体的 NCC 值; 比如 NCC0 用于表示接入网设备 0 上使用的 NCC 值, 并不限定 NCC 值为 0。本申请实施例中所使用的符号 K0、K1、K2、K1*、K2* 等, 均指的是终端和接入网设备之间进行安全保护的密钥, 比如图 2 中所涉及的 KgNB、KgNB1 至 KgNB12 等, 而 K0、K1、K2、K1* 或 K2* 具体是指哪个 KgNB 可以与场景相关, 本申请实施例对此不做限定。

- 30 S302, 接入网设备 0 确定终端需要切换。

随着终端的移动, 例如终端逐渐远离接入网设备 0, 接入网设备 0 可以感知到终端的信号强度逐渐减弱。当终端的信号强度减弱到一定程度时, 接入网设备 0 确定该终端需要被切换到信号强度更好的接入网设备, 从而可以从各个候选接入网设备中选择一个信号强度比较好的接入网设备, 比如接入网设备 1。

- 35 作为一种可能的实现, 终端可以对至少一个候选小区进行测量, 并向接入网设备 0 发送测量报告, 测量报告包括至少一个候选小区的信号强度, 至少一个候选小区属于至少一个候选接入网设备; 相应地, 接入网设备 0 可以根据测量报告, 从至少一个候选小区中选择信号强度比较好的小区 (即目标小区), 比如目标小区所属的接入网设备 (即目标接入网设备) 为接入网设备 1。

- 40 S303, 接入网设备 0 向接入网设备 1 发送切换请求 (handover request) 消息。相应的, 接入网设备 1 接收来自接入网设备 0 的切换请求消息。

比如, 接入网设备 0 可以根据 K0、接入网设备 1 上的小区的 PCI 以及载频, 水平推演得到密钥 K1。切换请求消息中可以包括 NCC0 和 K1, 切换请求消息用于请求将终端切换到接入网设备 1; 接入网设备 1 接收到切换请求信息后, 可以保存 NCC0 和 K1。

- 45 可以理解的是, 此处是以接入网设备 0 水平推演得到密钥 K1 (即接入网设备 0 上的 NCC 值未改变) 为例, 在其它示例中, 接入网设备 0 若确定当前 NCC 值较之前 NCC 值增加, 则也可以根据 NH0、接入网设备 1 上的小区的 PCI 以及载频, 垂直推演得到密钥 K1*, 并保存 NCC0 和 K1*。

S304, 接入网设备 1 构造透明容器。

如果接入网设备 1 允许终端切换, 则接入网设备 1 可以构造透明容器, 该容器携带有上述接收到的

NCC0。

透明容器还携带有配置信息，配置信息包括用于终端切换到接入网设备 1 的参数。

本申请实施例中，为便于描述，将透明容器简称为容器。

- 5 S305，接入网设备 1 向接入网设备 0 发送切换请求确认（handover request ACK）消息，消息中携带所述容器。相应的，接入网设备 0 接收来自接入网设备 1 的切换请求确认消息。

切换请求确认消息用于指示接入网设备 1 允许终端切换。例如，接入网设备 1 当前的资源充足，允许有更多的终端切换进来。切换请求确认消息可以包括接入网设备 1 构造的容器。

- 或者，在其它示例中，切换请求确认消息也可以用于指示该接入网设备 1 不允许该终端切换。例如，接入网设备 1 当前的资源不足，不允许有更多的终端切换进来。该流程中是以接入网设备 1 允许终端切换为例进行示意的。

10 S306，接入网设备 0 向终端发送切换命令消息；相应地，终端接收切换命令消息。

切换命令消息可以为 RRC 重配置（RRC reconfiguration）消息，该 RRC 重配置消息携带有所述容器。

S307，终端推演密钥。

- 15 终端可以从上述容器中获得 NCC0，如果从容器中获得 NCC0 与终端本地保存的 NCC 值相同，则终端可以执行水平推演，即根据 K0、接入网设备 1 上的小区的 PCI 以及载频，推演得到密钥 K1。这样，终端和接入网设备 1 维护相同的密钥，即 K1。

- 在其它示例中，如果从容器中获得 NCC0 与终端本地保存的 NCC 值不同，则终端可以先计算与 NCC0 对应的 NH0，然后根据 NH0、接入网设备 1 上的小区的 PCI 以及载频，垂直推演得到密钥 K1*。这样，终端和接入网设备 1 维护相同的密钥，即 K1*。

可以理解的是，通过上述操作，接入网设备 1 无法知道终端和接入网设备 0 共享的密钥（即 K0），从而可以保护过去进行的通信安全不受接入网设备 1 的影响。

S308，终端从接入网设备 0 上去附着，向接入网设备 1 发送切换完成消息。相应的，接入网设备 1 接收来自终端的切换完成消息。

- 25 切换完成消息可以为 RRC 重配置完成（RRC reconfiguration complete）消息。

S309，接入网设备 1 向 AMF 网元发送路径切换请求消息；相应地，AMF 网元接收路径切换请求消息。

S310，AMF 网元向接入网设备 1 发送路径切换响应消息；相应地，接入网设备 1 接收路径切换响应消息，进而完成路径切换。

- 30 路径切换是指终端的数据传输路由由“UPF 网元—接入网设备 0—终端”切换为“UPF 网元—接入网设备 1—终端”。也就是说，在路径切换前，下行数据由 UPF 网元发送给接入网设备 0，进而由接入网设备 0 发送给终端；上行数据由终端发送给接入网设备 0，进而由接入网设备 0 发送给 UPF 网元；在路径切换后，下行数据由 UPF 网元发送给接入网设备 1，进而由接入网设备 1 发送给终端；上行数据由终端发送给接入网设备 1，进而由接入网设备 1 发送给 UPF 网元。

- 35 AMF 网元接收到路径切换请求消息后，可以将本地保存的 NCC 取值更新加 1，得到更新后的 NCC（称为 NCC1），以根据更新后的 NCC 执行密钥推演，得到更新后的 NH（称为 NH1）。NCC1 和 NH1 关联，作为更新后的一对 {NH1, NCC1}。

路径切换响应消息中包括 {NH1, NCC1}，接入网设备 1 接收到路径切换响应消息后，可以保存 {NH1, NCC1}。

- 40 S311，终端与接入网设备 1 使用密钥 K1 进行通信。

此处，“终端与接入网设备 1 使用密钥 K1 进行通信”可以是指：终端与接入网设备 1 使用密钥 K1 本身进行通信；或者也可以是指：终端与接入网设备 1 使用基于密钥 K1 推演出来的机密性保护密钥和完整性保护密钥进行通信。本申请下文中的其它类似描述，均可以参照处理。

S312，接入网设备 1 确定终端需要切换。

- 45 接入网设备 1 确定终端需要切换的具体实现可以参照上述接入网设备 0 确定终端需要切换的描述。接入网设备 1 可以从各个候选接入网设备中选择一个信号强度比较好的接入网设备，比如接入网设备 2。

S313，接入网设备 1 向接入网设备 2 发送切换请求消息。相应的，接入网设备 2 接收来自接入网设备 1 的切换请求消息。

接入网设备 1 可以根据 NH1、接入网设备 2 上的小区的 PCI 以及载频, 推演得到密钥 $K2^*$, 并向接入网设备 2 发送切换请求消息。切换请求消息用于请求将终端切换到接入网设备 2, 切换请求消息中可以包括 NCC1 和 $K2^*$; 接入网设备 1 接收到切换请求消息后, 可以保存 NCC1 和 $K2^*$ 。

S314, 接入网设备 2 构造容器。

- 5 如果接入网设备 2 允许终端切换, 则接入网设备 2 可以构造容器, 该容器携带有上述接收到的 NCC1。容器还携带有配置信息, 配置信息包括用于终端切换到接入网设备 2 的参数。

S315, 接入网设备 2 向接入网设备 1 发送切换请求确认消息。相应的, 接入网设备 1 接收来自接入网设备 2 的切换请求确认消息。

- 10 切换请求确认消息用于指示接入网设备 2 允许终端切换。切换请求确认消息可以包括接入网设备 2 构造的容器。

或者, 在其它示例中, 切换请求确认消息也可以用于指示该接入网设备 1 不允许该终端切换。该流程中是以接入网设备 1 允许终端切换为例进行示意的。

S316, 接入网设备 1 向终端发送切换命令消息; 相应地, 终端接收切换命令消息。

切换命令消息可以为 RRC 重配置消息, 该 RRC 重配置消息携带有上述容器。

- 15 S317, 终端推演密钥。

终端可以从上述容器中获得 NCC1, 由于从容器中获得 NCC1 与终端本地保存的 NCC0 不同, 因此, 终端根据 NCC1 与 NCC0 的差值, 执行相应次数的垂直推演, 得到相应的 NH (即 NH1), 进而根据 NH1、接入网设备 2 上的小区的 PCI 以及载频, 推演得到密钥 $K2^*$ 。这样, 终端和接入网设备 2 维护相同的密钥, 即 $K2^*$ 。

- 20 可以理解的是, 通过上述操作, 接入网设备 2 无法知道终端和接入网设备 1 共享的密钥 (即 $K1$), 从而可以保护过去进行的通信安全不受接入网设备 2 的影响。

S318, 终端从接入网设备 1 上去附着, 向接入网设备 2 发送切换完成消息。相应的, 接入网设备 2 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

- 25 S319, 接入网设备 2 向 AMF 网元发送路径切换请求消息; 相应地, AMF 网元接收路径切换请求消息。

S320, AMF 网元向接入网设备 2 发送路径切换响应消息; 相应地, 接入网设备 2 接收路径切换响应消息, 进而完成路径切换。

- 30 路径切换是指终端的数据传输路由由“UPF 网元—接入网设备 1—终端”切换为“UPF 网元—接入网设备 2—终端”。

AMF 网元接收到路径切换请求消息后, 可以将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC (称为 NCC2), 根据更新后的 NCC 执行推演, 得到更新后的 NH (称为 NH2)。NCC2 和 NH2 关联, 作为更新后的一对 {NH2, NCC2}。

- 35 路径切换响应消息中包括 {NH2, NCC2}, 接入网设备 2 接收到路径切换响应消息后, 可以保存 {NH2, NCC2}。

S321, 终端与接入网设备 2 使用密钥 $K2^*$ 进行通信。

可以理解的是, 后续终端还可以从接入网设备 2 切换到其它接入网设备 (比如接入网设备 3), 具体的实现可以参照终端从接入网设备 1 切换到接入网设备 2 的描述。

- 40 采用上述图 3 所示意的流程, 接入网设备 0 知晓终端和接入网设备 1 共享的密钥 (即 $K1$), 但无法知晓终端和接入网设备 2 共享的密钥 (即 $K2^*$), 也无法知晓终端和后续的目标接入网设备共享的密钥, 从而可以实现两跳安全。

- 45 为了降低切换时延, 引入了 LTM 切换或者称为层 1/层 2 切换, 区别于层 3 切换, LTM 切换可以是由层 1/层 2 的信令触发。由于层 1 和层 2 比 RRC 层 (层 3) 位于更低层次的协议栈, 从而便于降低切换时延。

图 4 为 LTM 跨站切换的一种可能的流程示意图。由于针对于 LTM 跨站切换的安全保护, 目前尚无具体方案, 因此, 此处的流程中不涉及安全相关内容。如图 4 所示, 该流程包括:

S401, 终端通过接入网设备 0 连接到 5GC。

终端可以通过初始接入流程或者普通切换流程或者重建立流程或者小区重选等流程接入到接入网设备 0, 通过接入网设备 0 接入到 5GC。

S402, 接入网设备 0 确定 LTM 切换的多个候选接入网设备。

作为一种可能的实现, 终端可以对多个候选小区进行测量, 并向接入网设备 0 发送测量报告, 测量报告包括多个候选小区的信号强度, 多个候选小区属于多个候选接入网设备; 相应地, 接入网设备 0 可以根据测量报告, 从多个候选小区中选择信号强度比较好的小区, 选择的多个小区所属的接入网设备即为 LTM 切换的候选接入网设备。

作为又一种可能的实现, 接入网设备 0 可以获取终端的历史移动轨迹信息, 根据历史移动轨迹信息, 确定终端频繁切入切出的小区列表, 进而根据终端频繁切入切出的小区列表确定 LTM 切换的多个候选接入网设备。

该流程中, 以 LTM 切换的候选接入网设备包括接入网设备 1 和接入网设备 2 为例进行描述。

S403, 接入网设备 0 向接入网设备 1 发送切换请求消息 1。相应的, 接入网设备 1 接收来自接入网设备 0 的切换请求消息 1。

可选地, 切换请求消息 1 (以及下述切换请求消息 2) 中可以包括 LTM 切换的多个候选接入网设备的标识。

S404, 接入网设备 1 构造容器。

如果接入网设备 1 允许终端执行 LTM 切换, 则接入网设备 1 可以构造容器。容器携带有接入网设备 1 的标识和配置信息, 配置信息包括用于终端切换到接入网设备 1 的参数, 比如接入网设备 1 的 SSB 频点、波束信息等。

S405, 接入网设备 1 向接入网设备 0 发送切换请求确认消息 1。相应的, 接入网设备 0 接收来自接入网设备 1 的切换请求确认消息 1。

S406, 接入网设备 0 向接入网设备 2 发送切换请求消息 2。相应的, 接入网设备 2 接收来自接入网设备 0 的切换请求消息 2。

S407, 接入网设备 2 构造容器。

如果接入网设备 2 允许终端执行 LTM 切换, 则接入网设备 2 可以构造容器。容器携带有接入网设备 2 的标识和配置信息, 配置信息包括用于终端切换到接入网设备 2 的参数, 比如接入网设备 2 的 SSB 频点、波束信息等。

S408, 接入网设备 2 向接入网设备 0 发送切换请求确认消息 2。相应的, 接入网设备 0 接收来自接入网设备 2 的切换请求确认消息 2。

S409, 接入网设备 0 向终端发送 RRC 重配置消息, 该 RRC 重配置消息携带有接入网设备 1 构造的容器和接入网设备 2 构造的容器; 相应地, 终端接收 RRC 重配置消息。

终端从 RRC 重配置消息中获得接入网设备 1 构造的容器和接入网设备 2 构造的容器, 并保存。

S410, 终端向接入网设备 0 发送 RRC 重配置完成消息; 相应的, 接入网设备 0 接收来自终端的 RRC 重配置完成消息。

S411, 接入网设备 0 确定终端需要切换, 切换的目标接入网设备为接入网设备 1。

接入网设备 0 确定目标接入网设备的具体实现有多种, 本申请实施例对此不做限定。比如, 接入网设备 0 可以根据终端上报的测量报告, 确定目标接入网设备为接入网设备 1。

S412, 接入网设备 0 向终端发送切换命令消息。相应的, 终端接收来自接入网设备 0 的切换命令消息。

切换命令消息为 MAC 层消息, 比如 MAC 控制元素 (control element, CE)。切换命令消息包括目标接入网设备的标识, 即接入网设备 1 的标识。

S413, 终端从接入网设备 0 上去附着, 并向接入网设备 1 发送切换完成消息。相应的, 接入网设备 1 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

可选地, 如果切换请求消息 1 中不包括 LTM 切换的多个候选接入网设备的标识, 则接入网设备 0 确定终端需要切换到接入网设备 1 后, 可以通过 Xn 消息向接入网设备 1 发送 LTM 切换的多个候选接入网设备的标识。

S414, 接入网设备 1 向 AMF 网元发送路径切换请求消息; 相应地, AMF 网元接收路径切换请求

消息。

S415, AMF 网元向接入网设备 1 发送路径切换响应消息; 相应地, 接入网设备 1 接收路径切换响应消息, 进而完成路径切换。

5 此处, 路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 0—终端”切换为“UPF 网元—接入网设备 1—终端”。

S416, 终端与接入网设备 1 进行通信 (比如数据传输)。

S417, 接入网设备 1 确定终端需要切换, 切换的目标接入网设备为接入网设备 2。

S418, 接入网设备 1 向终端发送切换命令消息。相应的, 终端接收来自接入网设备 1 的切换命令消息。

10 切换命令消息为 MAC 层消息, 比如 MAC CE。切换命令消息包括目标接入网设备的标识, 即接入网设备 2 的标识。

可以理解的是, 接入网设备 1 可以判断目标接入网设备 (即接入网设备 2) 是否属于 LTM 切换的候选接入网设备, 若目标接入网设备是否属于 LTM 切换的候选接入网设备, 则接入网设备 1 可以向终端发送 MAC CE, 以执行 LTM 跨站切换。可选地, 若目标接入网设备不属于 LTM 切换的候选接入网设备, 则接入网设备 1 可以向终端发送 RRC 重配置消息, 以执行普通跨站切换。

15 S419, 终端从接入网设备 1 上去附着, 并向接入网设备 2 发送切换完成消息。相应的, 接入网设备 2 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

20 可选地, 如果切换请求消息 2 中不包括 LTM 切换的多个候选接入网设备的标识, 则接入网设备 1 确定终端需要切换到接入网设备 2 后, 可以通过 Xn 消息向接入网设备 2 发送 LTM 切换的多个候选接入网设备的标识。

S420, 接入网设备 2 向 AMF 网元发送路径切换请求消息; 相应地, AMF 网元接收路径切换请求消息。

25 S421, AMF 网元向接入网设备 2 发送路径切换响应消息; 相应地, 接入网设备 2 接收路径切换响应消息, 进而完成路径切换。

此处, 路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 1—终端”切换为“UPF 网元—接入网设备 2—终端”。

S422, 终端与接入网设备 2 进行通信 (比如数据传输)。

30 可以理解的是, 如果 LTM 切换的候选接入网设备还包括接入网设备 3, 则后续终端还可以从接入网设备 2 切换到接入网设备 3, 具体的实现可以参照终端从接入网设备 1 切换到接入网设备 2 的描述。

根据上述普通跨站切换流程和 LTM 跨站切换流程可以看出: 普通跨站切换中, 源接入网设备可以选择 1 个目标接入网设备, 并通过 RRC 重配置消息指示终端切换到目标接入网设备, 终端切换到目标接入网设备后, 本次切换结束; 下次切换中, 终端将接收新的 RRC 重配置消息, 即每次切换都会触发 RRC 重配置过程。LTM 跨基站切换中, 源接入网设备确定 LTM 切换的多个候选接入网设备, 并将多个候选接入网设备构造的容器发送给终端; 后续, 源接入网设备可以通过 MAC CE 指示终端切换到目标接入网设备, 即每次切换不触发 RRC 重配过程。

本申请实施例中, 将针对 LTM 跨站切换场景中终端和接入网设备之间的安全通信的相关实现进行研究。

40 示例性地, 本申请实施例提供的通信方法包括三种可能的方案 (方案一、方案二和方案三), 用于实现 LTM 跨站切换场景中终端和接入网设备之间的安全通信。

在方案一中, 第一接入网设备接收多个候选接入网设备中每个接入网设备构造的容器, 并将多个候选接入网设备中每个接入网设备构造的容器发送给终端 (容器中携带切换参数); 后续, 第一接入网设备确定终端需要切换到多个候选接入网设备中的第二接入网设备后, 通过 MAC 层消息向终端发送用于触发终端切换到第二接入网设备的信息和用于指示第一 NCC 的信息; 进而, 终端可以根据预先接收到的第二接入网设备构造的容器中的参数, 切换到第二接入网设备, 以及根据第一 NCC, 确定与第二接入网设备进行通信所使用的密钥。如此, 可以实现终端与第二接入网设备之间的安全通信。

在方案二中, 第一接入网设备向多个候选接入网设备发送第一 NCC, 并接收多个候选接入网设备

中每个接入网设备构造的容器，每个接入网设备构造的容器可以包括第一 NCC；后续，第一接入网设备确定终端需要切换到多个候选接入网设备中的第二接入网设备后，通过 MAC 层消息触发终端切换到第二接入网设备；进而，终端可以根据预先接收到的第二接入网设备构造的容器中的参数，切换到第二接入网设备，以及根据预先接收到的第二接入网设备构造的容器中的第一 NCC，确定与第二接入网设备进行通信所使用的密钥。如此，可以实现终端与第二接入网设备之间的安全通信。

在方案三中，第一接入网设备分别向多个候选接入网设备发送切换请求消息，多个候选接入网设备中的每个接入网设备接收到切换请求消息后，从移动管理网元获取每个接入网设备对应的 NCC，并向第一接入网设备发送每个接入网设备构造的容器，每个接入网设备构造的容器包括每个接入网设备对应的 NCC，多个候选接入网设备中不同接入网设备对应的 NCC 不同；后续，第一接入网设备确定终端需要切换到多个候选接入网设备中的第二接入网设备后，通过 MAC 层消息触发终端切换到第二接入网设备；进而，终端可以根据预先接收到的第二接入网设备构造的容器中的参数，切换到第二接入网设备，以及根据预先接收到的第二接入网设备构造的容器中的 NCC，确定与第二接入网设备进行通信所使用的密钥。如此，可以实现终端与第二接入网设备之间的安全通信。

可以理解的是，上述对方案一至方案三的描述仅是为了让本申请实施例更容易被理解，而不应该视为对本申请所要求的保护范围中的技术特征的严格限定，即上述描述所涉及的技术特征并非全部都是必要技术特征。

下面结合实施例一至实施例七对本申请实施例进行详细描述。

实施例一

在实施例一中，将针对方案一进行详细描述。

图 5 为本申请实施例提供的通信方法所对应的流程示意图。如图 5 所示，该流程可以包括：

S501，第一接入网设备接收来自多个候选接入网设备中每个接入网设备的容器，每个接入网设备的容器包括用于终端切换到每个接入网设备的参数。

此处，每个接入网设备的容器具体可以是指每个接入网设备构造的容器。

第一接入网设备可以为终端通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程所接入的接入网设备。第一接入网设备和终端可以保存相同的密钥（该密钥用于第一接入网设备和终端进行通信）和相同的 NCC（比如第一 NCC）。

比如，若第一接入网设备是终端通过初始接入流程或者小区重选所接入的接入网设备，则 AMF 网元可以通过 NGAP 消息向第一接入网设备发送第一 NCC，进而第一接入网设备可以保存第一 NCC。具体的，在初始接入流程中，所述 NGAP 消息为初始上下文建立请求（initial context setup request）消息。

若第一接入网设备是终端通过重建流程所接入的接入网设备，则第一接入网设备也可以通过索取 UE 上下文响应（retrieve UE context response）消息接收第一 NCC，并保存第一 NCC。若第一接入网设备是终端通过普通切换流程所接入的接入网设备，则第一接入网设备可以通过路径切换响应消息接收第一 NCC，并保存第一 NCC；可选地，第一接入网设备可以通过 RRC 重配置消息对终端进行 RRC 重配置，以使得终端和第一接入网设备保存相同的 NCC（即第一 NCC）；若第一接入网设备未对终端进行 RRC 重配置，则终端和第一接入网设备保存的 NCC 可以不同。本申请实施例中均是以“终端和第一接入网设备保存相同的 NCC”为例进行描述的。

示例性地，第一接入网设备可以确定 LTM 切换的多个候选接入网设备，并分别向多个候选接入网设备发送切换请求消息，用于请求多个候选接入网设备构造容器。其中，多个候选接入网设备中每个接入网设备构造的容器包括用于终端切换到每个接入网设备的参数，比如多个候选接入网设备中第二接入网设备构造的容器包括用于终端切换到第二接入网设备的参数（如 SSB 频点信息、波束信息等），多个候选接入网设备中第三接入网设备构造的容器包括用于终端切换到第三接入网设备的参数（如 SSB 频点信息、波束信息等）。具体可以参照 S402 至 S408 中的描述。

S502，第一接入网设备向终端发送 RRC 重配置消息，RRC 重配置消息包括多个候选接入网设备中每个接入网设备构造的容器；相应地，终端接收 RRC 重配置消息。

终端接收到 RRC 重配置消息后，可以解析 RRC 重配置消息，获得多个候选接入网设备中每个接入网设备构造的容器。可选地，终端可以向第一接入网设备发送 RRC 重配置完成消息。

上述 S501 和 S502 可以理解为切换准备过程。

S503，第一接入网设备确定终端需要切换到多个候选接入网设备中的第二接入网设备。

第一接入网设备确定终端需要切换到第二接入网设备的实现可以有多种。比如,终端可以对至少一个候选小区进行测量,并向第一接入网设备发送测量报告,测量报告包括至少一个候选小区的信号强度;相应地,第一接入网设备可以根据测量报告,从至少一个候选小区中选择信号强度比较好的小区(即目标小区),比如目标小区所属的接入网设备(即目标接入网设备)为第二接入网设备,即第一接入网设备确定终端需要切换到第二接入网设备。

可以理解的是,此处是以第一接入网设备选择的目标接入网设备为多个候选接入网设备中的第二接入网设备为例进行描述的;在其它示例中,第一接入网设备选择的目标接入网设备也可能不属于多个候选接入网设备。若第一接入网设备选择的目标接入网设备不属于多个候选接入网设备,则第一接入网设备可以触发终端执行普通跨站切换。

S504,第一接入网设备向终端发送第一 MAC 层消息(即切换命令消息),第一 MAC 层消息包括用于触发终端切换到第二接入网设备的信息和用于指示第一 NCC 的信息;相应地,终端接收第一 MAC 层消息。

示例性的,用于触发终端切换到第二接入网设备的信息可以包括第二接入网设备的标识。用于指示第一 NCC 的信息可以包括以下至少一项:第一 NCC;第一 NCC 的索引值;第一 NCC 加密后的密文。其中,第一 NCC 可以是第一接入网设备中(比如第一接入网设备的 RRC 层)存储的 NCC。

此处是以用于触发终端切换到第二接入网设备的信息和用于指示第一 NCC 的信息承载于同一 MAC 层消息(即第一 MAC 层消息)消息为例进行描述的,在其它示例中,用于触发终端切换到第二接入网设备的信息和用于指示第一 NCC 的信息也可以承载不同 MAC 层消息。

示例性的,从第一接入网设备的角度来看,第一接入网设备确定终端需要切换到第二接入网设备后,便可生成第一 MAC 层消息,并发送第一 MAC 层消息。相比于普通切换流程(在普通切换流程中,源接入网设备确定终端需要切换时,需要先从目标接入网设备获取目标接入网设备构造的容器(容器中携带 NCC 和切换参数),进而将容器发送给终端)来说,由于第一接入网设备在确定终端需要切换时,便可以自行生成包含用于指示第一 NCC 的信息的第一 MAC 层消息,并向终端发送第一 MAC 层消息,从而能够降低切换时延。

其中,第一接入网设备的 RRC 层可以将用于指示第一 NCC 的信息传递到第一接入网设备的 MAC 层,进而第一接入网设备的 MAC 层生成的第一 MAC 层消息包括用于指示第一 NCC 的信息。比如,第一接入网设备的 RRC 层将第一 NCC 传递到第一接入网设备的 MAC 层,进而第一接入网设备的 MAC 层将第一 NCC 封装到第一 MAC 层消息;又比如,第一接入网设备的 RRC 层根据存储的第一 NCC 得到第一 NCC 的索引值(或者第一 NCC 加密后的密文,此处以第一 NCC 的索引值为例),并将第一 NCC 的索引值传递到第一接入网设备的 MAC 层,进而第一接入网设备的 MAC 层将第一 NCC 的索引值封装到第一 MAC 层消息,并发送给终端。

示例性的,从终端的角度来看,终端接收到第一 MAC 层消息后,可以根据第一 MAC 层消息所携带的第一 NCC,确定终端与第二接入网设备进行通信所使用的密钥(称为密钥 1)。此处的密钥 1 可以为终端与第二接入网设备之间进行安全保护的密钥 KgNB(比如图 2 中所示意的推演流程中的某一 KgNB),或者也可以是基于密钥 KgNB 推演出来的机密性保护密钥和/或完整性保护密钥,具体参照前文 S311 中对“终端与接入网设备 1 使用密钥 K1 进行通信”的介绍;本申请实施例中将主要以“密钥 1 为终端与第二接入网设备之间进行安全保护的密钥 KgNB”为例进行描述,其它类似之处(比如下文的密钥 2)均可以参照理解。

比如,终端的 MAC 层从第一 MAC 层消息中获得用于指示第一 NCC 的信息。终端的 MAC 层将用于指示第一 NCC 的信息传递到终端的 RRC 层,进而终端的 RRC 层可以根据第一 NCC 确定密钥 1。

其中,终端根据第一 NCC 确定密钥 1 的具体实现有多种。比如,终端可以将第一 NCC 与终端本地保存的 NCC 进行比较,由于二者相同,因此,终端可以根据第一输入参数,水平推演得到终端与第二接入网设备进行通信所使用的密钥。其中,第一输入参数包括第二接入网设备的小区的 PCI 以及载频,还包括终端与第一接入网设备之间进行安全保护的密钥 KgNB。

S505,终端根据第二接入网设备构造的容器中的参数,切换到第二接入网设备。

比如,终端可以根据第二接入网设备构造的容器中的参数,向第二接入网设备发起随机接入过程,以通过随机接入过程与第二接入网设备进行同步;在完成同步后,终端可以向第二接入网设备发送切换完成消息。其中,切换完成消息可以为 RRC 重配置完成消息。可以理解的是,在第二接入网设备构造

的容器中的参数包含了接入所需的全部信息时,终端可以不读取系统消息。示例性的,在所述容器中包括波束信息时,终端选择对应的波束,与第二接入网设备建立连接。

示例性的,终端可以根据密钥 1,向第二接入网设备发送切换完成消息。

S506,第二接入网设备从 AMF 网元获取第二 NCC。

- 5 可选地,第二接入网设备还接收来自 AMF 网元的第二 NCC 对应的 NH。第二接入网设备可以保存第二 NCC 和第二 NCC 对应的 NH。

示例性的,第二接入网设备可以向 AMF 网元发送路径切换请求消息,相应地,AMF 网元接收到路径切换请求消息后,可以将本地保存的 NCC 取值(即第一 NCC)更新加 1,得到更新后的 NCC(即第二 NCC),以根据更新后的 NCC 执行密钥推演,得到第二 NCC 对应的 NH,并向第二接入网设备发送路径切换响应消息,路径切换响应消息包括第二 NCC 和第二 NCC 对应的 NH。比如,第二接入网设备可以响应于终端发送的切换完成消息,向 AMF 网元发送路径切换请求消息。

S507,终端和第二接入网设备使用密钥 1 进行通信。

- 也就是说,密钥 1 可以用于在切换过程中终端和第二接入网设备之间的通信(比如终端可以使用密钥 1 向第二接入网设备发送切换完成消息),还可以用于在切换完成后终端和第二接入网设备之间的通信(比如 S507 中所涉及的通信)。

如上已介绍终端确定密钥的实现,从第二接入网设备的角度来看,第二接入网设备可以维护与密钥 1 相同的密钥(为便于描述,也称为密钥 1),以便于使用密钥 1 与终端进行通信,此处对第二接入网设备获取密钥 1 的实现进行描述。作为一种可能的实现,在切换准备过程中,第一接入网设备在确定多个候选接入网设备后,可以分别确定多个候选接入网设备的密钥,并通过切换请求消息发送给相应的接入网设备。以多个候选接入网设备中的第二接入网设备为例,第一接入网设备可以根据第一输入参数,水平推演得到密钥 1,并通过切换请求消息将密钥 1 发送给第二接入网设备。可选地,第一接入网设备在请求第二接入网设备构造容器时,可以向第二接入网设备发送第一 NCC(即切换请求消息可以包括第一 NCC),进而第二接入网设备构造的容器中可以包括第一 NCC,上述第一 MAC 层消息无需携带用于指示第一 NCC 的信息,终端可以从第二接入网设备构造的容器中获得第一 NCC。

- 20 作为又一种可能的实现,第一接入网设备确定终端需要切换到第二接入网设备后,可以根据第一输入参数,水平推演得到密钥 1,并通过 Xn 消息将密钥 1 发送给第二接入网设备(即 Xn 消息包括密钥 1),可选地,Xn 消息还包括第一 NCC。

上述 S506 可以在 S507 之前执行,或者 S506 也可以在 S507 之后执行,又或者 S506 和 S507 同时执行,本申请实施例对步骤的先后执行顺序不做限定。

- 30 可选地,在终端从第一接入网设备切换到第二接入网设备之后,上述方法还包括:

S508,第二接入网设备确定终端需要切换到至少一个候选接入网设备中的第三接入网设备。

此处,第二接入网设备确定终端需要切换到第三接入网设备的实现,可以参照上文中“第一接入网设备确定终端需要切换到第二接入网设备”的描述。

- 35 作为一种可能的实现,至少一个候选接入网设备即为上述多个候选接入网设备。第一接入网设备确定多个候选接入网设备后,可以通过切换请求消息,分别向多个候选接入网设备发送第一候选接入网设备列表,第一候选接入网设备列表包括多个候选接入网设备的标识;或者,第一接入网设备确定终端需要切换到第二接入网设备后,可以通过上述 Xn 消息向第二接入网设备发送第一候选接入网设备列表。

作为又一种可能的实现,至少一个候选接入网设备包括多个候选接入网设备中的部分或全部接入网设备。第一接入网设备确定终端需要切换到第二接入网设备后,可以根据多种可能的因素(比如候选接入网设备上的负载等),从多个候选接入网设备选择部分或全部接入网设备(即选择至少一个候选接入网设备),并通过上述 Xn 消息向第二接入网设备发送第一候选接入网设备列表,第一候选接入网设备列表包括选择的至少一个候选接入网设备的标识。

可选地,针对于该实现,第一接入网设备还可以向第二接入网设备发送多个候选接入网设备的标识,比如通过切换请求消息或上述 Xn 消息发送,具体不做限定。

- 45 S509,第二接入网设备向第三接入网设备发送第三接入网设备与终端进行通信所使用的密钥(称为密钥 2);相应地,第三接入网设备接收该密钥。

第二接入网设备确定终端需要切换到第三接入网设备后,可以根据从 AMF 网元获得的第二 NCC 对应的 NH、第三接入网设备上的小区的 PCI 以及载频,推演得到密钥 2,并通过 Xn 消息将密钥 2 发

送给第三接入网设备, 可选地, Xn 消息还包括第二 NCC。

可选地, Xn 消息还可以包括第二候选接入网设备列表, 第二候选接入网设备列表可以第一候选接入网设备列表中的部分或全部候选接入网设备的标识。比如, 第二接入网设备确定终端需要切换到第三接入网设备后, 可以根据多种可能的因素 (比如候选接入网设备上的负载等), 从多个候选接入网设备
5 选择部分或全部接入网设备 (选择的接入网设备即为第二候选接入网设备列表中的接入网设备), 并通过 Xn 消息向第三接入网设备发送第二候选接入网设备列表。

S510, 第二接入网设备向终端发送第二 MAC 层消息 (即切换命令消息), 第二 MAC 层消息包括用于触发终端切换到第三接入网设备的信息和用于指示第二 NCC 的信息, 第二 NCC 用于确定终端与第三接入网设备进行通信所使用的密钥。

10 用于触发终端切换到第三接入网设备的信息可以包括第三接入网设备的标识。

用于指示第二 NCC 的信息可以包括以下至少一项: 第二 NCC; 第二 NCC 的索引值; 第二 NCC 加密后的密文。其中, 第二 NCC 可以是第二接入网设备中 (比如第二接入网设备的 RRC 层) 存储的第二 NCC。

示例性的, 从第二接入网设备的角度来看, 第二接入网设备确定终端需要切换到第三接入网设备后, 便可生成第二 MAC 层消息, 并发送第二 MAC 层消息。相比于普通切换流程 (在普通切换流程中, 源接入网设备确定终端需要切换时, 需要先从目标接入网设备获取目标接入网设备构造的容器 (容器中携带 NCC 和切换参数), 进而将容器发送给终端) 来说, 由于第二接入网设备在确定终端需要切换时, 便可以自行生成包含用于指示第二 NCC 的信息的第二 MAC 层消息, 并向终端发送第二 MAC 层消息, 从而能够降低切换时延。比如, 第二接入网设备的 RRC 层将用于指示第二 NCC 的信息传递到第二接入网设备的 MAC 层, 进而第二接入网设备的 MAC 层生成的第二 MAC 层消息包括用于指示第二 NCC
20 的信息。

示例性地, 从终端的角度来看, 终端接收到第二 MAC 层消息后, 可以根据第二 MAC 层消息所携带的第二 NCC, 确定终端与第三接入网设备进行通信所使用的密钥 (称为密钥 2)。比如, 终端的 MAC 层从第二 MAC 层消息中获得用于指示第二 NCC 的信息。终端的 MAC 层将用于指示第二 NCC 的信息传递到终端的 RRC 层, 进而终端的 RRC 层可以根据第二 NCC 确定密钥 2。

其中, 终端根据第二 NCC 确定密钥 2 的具体实现有多种。比如, 终端可以将第二 NCC 与终端本地保存的 NCC (即第一 NCC) 进行比较, 由于第二 NCC 不同于第一 NCC, 因此, 终端可以根据第二 NCC 与第一 NCC 的差值, 推演得到第二 NCC 对应的 NH, 以及根据第二 NCC 对应的 NH、第三接入网设备的小区 PCI 以及载频, 推演得到密钥 2。此外, 在确定第二 NCC 不同于终端本地保存的 NCC 后, 终端可以将本地保存的 NCC 更新为第二 NCC。

30 本申请实施例对 S509 和 S510 的先后执行顺序不做限定, S509 可以在 S520 之前执行, 或者 S509 也可以在 S510 之前执行, 又或者 S509 和 S510 同时执行。

S511, 终端根据第三接入网设备构造的容器中的参数, 切换到第三接入网设备。

此处的实现可以参照 S505 的描述。

S512, 第三接入网设备从 AMF 网元获取第三 NCC。

35 示例性的, 响应于终端切换到第三接入网设备 (比如第三接入网设备接收到来自终端的切换完成消息), 第三接入网设备可以从 AMF 网元获取第三 NCC。

可选地, 第三接入网设备还接收来自 AMF 网元的第三 NCC 对应的 NH, 并保存第三 NCC 和第三 NCC 对应的 NH。

比如, 第三接入网设备可以向 AMF 网元发送路径切换请求消息, 相应地, AMF 网元接收到路径切换请求消息后, 可以将本地保存的 NCC 取值 (即第二 NCC) 更新加 1, 得到更新后的 NCC (即第三 NCC), 以根据更新后的 NCC 执行密钥推演, 得到第三 NCC 对应的 NH, 并向第三接入网设备发送路径切换响应消息, 路径切换响应消息包括第三 NCC 和第三 NCC 对应的 NH。

S513, 终端与第三接入网设备使用密钥 2 进行通信。

45 示例性地, 上述终端根据第二 MAC 层消息中所携带的第二 NCC 推演得到了密钥 2, 第三接入网设备从第二接入网设备接收到了密钥 2, 因此, 终端和第三接入网设备可以使用密钥 2 进行通信。

采用上述方法, 第一接入网设备先向终端发送多个候选接入网设备中每个接入网设备构造的容器 (容器携带切换参数); 进而, 在确定终端需要切换到第二接入网设备后, 通过第一 MAC 层消息发送用于指示第一 NCC 的信息。相比于普通切换流程 (在普通切换流程中, 源接入网设备确定终端需要切

换时,需要先从目标接入网设备获取目标接入网设备构造的容器(容器中携带 NCC 和切换参数),进而将容器发送给终端,以触发终端执行切换)来说,由于第一接入网设备在确定终端需要切换时,便可以向终端发送第一 MAC 层消息来触发终端执行切换,便于降低切换时延;且由于第一 MAC 层消息中携带用于指示第一 NCC 的信息,便于实现终端与第二接入网设备之间的安全通信。

5 进一步地,由于 LTM 切换在 S501-S502 中执行一次切换准备过程,因此若在切换准备过程阶段的容器中携带 NCC,则容器中所携带的 NCC 均为第一 NCC,会导致无法实现垂直推演;本申请实施例中,使用 MAC 层消息携带 NCC,便于接入网设备和终端根据更新的 NCC,推演并使用更新的密钥进行安全通信。

可以理解的是,在执行 LTM 切换时,源接入网设备可以通过 MAC 层消息向终端发送源接入网设备获得的 NCC,使得终端可以根据 NCC 确定终端与目标接入网设备进行通信所使用的密钥,便于实现
10 密钥更新,使得终端在多个接入网设备之间来回切换时,不会出现密钥重用的问题。以及,第一接入网设备知晓终端和第二接入网设备共享的密钥(终端和第二接入网设备共享的密钥是水平推演得到的),但无法知晓终端和第三接入网设备共享的密钥(终端和第三接入网设备共享的密钥是垂直推演得到的),也无法知晓终端和后续的目标接入网设备共享的密钥(终端和后续的目标接入网设备共享的密钥是垂直推演得到的),从而可以实现两跳安全。

上述是以“终端根据切换命令消息中所携带的 NCC,确定终端与目标接入网设备进行通信所使用的密钥”为例进行描述的,此种情形下,终端可以根据第一 NCC,确定终端与第二接入网设备进行通信所使用的密钥,并存储在终端的 AS 安全上下文中。在其它可能的示例中,在 S506 之后,第二接入网设备可以向终端发送第三 MAC 层消息,第三 MAC 层消息可以包括第二 NCC(该 NCC 是 S506 中第二接入网设备从 AMF 网元获取的);相应的,终端接收到第三 MAC 层消息后,可以根据第二 NCC,确定
20 终端与第二接入网设备进行通信所使用的密钥;此种情形下,在 S507 中,终端与第二接入网设备进行通信所使用的密钥是根据第二 NCC 确定的密钥。其中,当终端根据第二 NCC 确定出终端与第二接入网设备进行通信所使用的密钥时,终端可以将 AS 安全上下文中的根据第一 NCC 确定的密钥更新为根据第二 NCC 确定的密钥(即终端根据第一 NCC 确定的终端与第二接入网设备进行通信所使用的密钥失效),进而终端和第二接入网设备进行通信便可使用根据第二 NCC 确定的密钥;可选地,终端可以删除第一 NCC 确定的终端与第二接入网设备进行通信所使用的密钥。

也就是说,在终端根据第二 NCC 确定出终端与第二接入网设备进行通信所使用的密钥之前,终端和第二接入网设备之间进行通信所使用的密钥是根据第一 NCC 确定的密钥,在终端根据第二 NCC 确定出终端与第二接入网设备进行通信所使用的密钥后,终端和第二接入网设备之间进行通信所使用的密
30 钥是根据第二 NCC 确定的密钥;比如,在切换过程中终端和第二接入网设备之间进行通信所使用的密钥是根据第一 NCC 确定的密钥,在切换完成后第二接入网设备可以向终端发送第三 MAC 层消息,进而在切换完成后终端和第二接入网设备之间进行通信所使用的密钥是根据第二 NCC 确定的密钥。

类似地,S510 中终端可以根据第二 NCC 确定终端与第三接入网设备进行通信所使用的密钥,并存储在 AS 安全上下文中;在 S511 之后,第三接入网设备可以向终端发送第四 MAC 层消息,第四 MAC
35 层消息可以包括第三 NCC(该 NCC 是 S512 中第三接入网设备从 AMF 网元获取的);相应的,终端接收到第四 MAC 层消息后,可以根据第三 NCC,确定终端与第三接入网设备进行通信所使用的密钥,并将 AS 安全上下文中的根据第二 NCC 确定的密钥更新为根据第三 NCC 确定的密钥(即终端根据第二 NCC 确定的终端与第三接入网设备进行通信所使用的密钥失效);此种情形下,在 S513 中,终端与第三接入网设备进行通信所使用的密钥是根据第三 NCC 确定的密钥。

40 如此,第一接入网设备不知晓终端和第二接入网设备共享的密钥,也不知晓终端和第三接入网设备共享的密钥,从而可以实现一跳安全。

此外,上述实施例一中仅描述了终端从第一接入网设备切换到第二接入网设备,以及从第二接入网设备切换到第三接入网设备的实现,后续终端还可以连续执行一次或多次 LTM 切换,比如从第三接入网设备切换到第四接入网设备。“终端从第三接入网设备切换到第四接入网设备”的具体实现可以参照
45 “终端从第二接入网设备切换到第三接入网设备”的描述。也就是说,上述“终端从第二接入网设备切换到第三接入网设备”的描述可以适用于终端在 LTM 切换的多个候选接入网设备之间的切换。

基于实施例一,下面结合实施例二(对应两跳安全)和实施例三(对应一跳安全)描述两种可能的

实现流程。在实施例二和实施例三中，将以实施例一中的“第一接入网设备”为接入网设备 0，“第二接入网设备”为接入网设备 1，“第三接入网设备”为接入网设备 2 为例进行描述。

实施例二

图 6 为本申请实施例提供的通信方法所对应的流程示意图。如图 6 所示，该流程可以包括：

5 S601，终端通过接入网设备 0 连接到 5GC。

终端可以通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程接入到接入网设备 0，通过接入网设备 0 接入到 5GC。进而，终端和接入网设备 0 上分别保存密钥 KgNB（为便于描述，称为 K0）和 NCC0（K0 关联 NCC0），AMF 网元上保存 NCC0。

S602 至 S611 参照 S402 至 S411 描述。

10 S612，接入网设备 0 向接入网设备 1 发送 Xn 消息；相应地，接入网设备 1 接收来自接入网设备 0 的 Xn 消息。

可选的，接入网设备 0 根据 NCC0、接入网设备 1 上的小区的 PCI 以及载频，水平推演得到密钥 K1。Xn 消息包括 NCC0 和密钥 K1。

作为一种可能的实现（实现 1），接入网设备 0 可以直接通过 Xn 消息将 S602 中确定的多个候选接入网设备的标识发送给接入网设备 1。此种情形下，Xn 消息还包括接入网设备列表 1，接入网设备列表 1 包括 S602 中确定的 LTM 切换的多个候选接入网设备的标识。或者，接入网设备 0 通过切换请求消息 1 向接入网设备 1 发送接入网设备列表 1，此种情形下，Xn 消息可以不包括接入网设备列表 1。

20 作为又一种可能的实现（实现 2），接入网设备 0 可以根据多种可能的因素（比如候选接入网设备上的负载等），从 S602 中确定的多个候选接入网设备选择部分或全部接入网设备，进而通过 Xn 消息将选择的接入网设备的标识发送给接入网设备 1。此种情形下，Xn 消息还包括接入网设备列表 2，接入网设备列表 2 包括接入网设备 0 选择的接入网设备的标识。

可选地，针对于该实现，接入网设备 0 还可以向接入网设备 1 发送 S602 中确定的多个候选接入网设备的标识（即接入网设备列表 1），比如通过切换请求消息 1 或上述 Xn 消息发送，具体不做限定。

25 可以理解的是，在实现 1 中，接入网设备列表 1 即为实施例一中的第一候选接入网设备列表；在实现 2 中，接入网设备列表 2 即为实施例一中的第一候选接入网设备列表。

此外，接入网设备 1 接收到 Xn 消息后，可以获知接入网设备 1 为 LTM 切换的目标接入网设备，不是普通切换的目标接入网设备，进而无需构造容器（如果是普通切换的目标接入网设备，则接入网设备构造容器，参照图 3 中的描述）。

30 在一个示例中，Xn 消息可以为 LTM 切换的专用消息，进而接入网设备 1 接收到 Xn 消息后，可以获知接入网设备 1 为 LTM 切换的目标接入网设备。

在又一个示例中，Xn 消息可以包括指示信息，指示信息用于指示接入网设备 1 为 LTM 切换的目标接入网设备。本申请实施例对该指示信息的具体实现不做限定，比如该指示信息可以包括上述实现 1 中的接入网设备列表 1 或实现 2 中的接入网设备列表 2。

35 本申请实施例对 S612 的发送时机不做限定，比如 S612 可以在 S613 之前执行，或者 S612 可以在 S613 之后执行，或者 S612 与 S613 同时执行。本申请实施例中其它类似于 S612 的步骤都可以参照理解。

S613，接入网设备 0 向终端发送切换命令消息。相应的，终端接收来自接入网设备 0 的切换命令消息。

40 切换命令消息为 MAC 层消息，比如 MAC CE。切换命令消息包括目标接入网设备的标识（即接入网设备 1 的标识）和 NCC0。其中，接入网设备 0 可以将 NCC0 从 RRC 层传递到 MAC 层，并在 MAC 层消息中发送。

45 其中，接入网设备 0 确定终端需要切换到接入网设备 1 后，便可生成切换命令消息，并发送切换命令消息。相比于普通切换流程来说，由于接入网设备 0 在确定终端需要切换时，便可以自行生成包含 NCC0 的切换命令消息，并向终端发送切换命令消息，从而能够降低切换时延。其中，接入网设备 0 的 RRC 层可以将 NCC0 传递到接入网设备 0 的 MAC 层，进而接入网设备 0 的 MAC 层生成的切换命令消息包括 NCC1。

可以理解的是，接入网设备 0 可以判断目标接入网设备（即接入网设备 1）是否属于 LTM 切换的候选接入网设备，若目标接入网设备是否属于 LTM 切换的候选接入网设备，则接入网设备 0 可以执行上述 S612 和 S613，以触发 LTM 跨站切换；可选的，响应于接入网设备 1 的切换请求确认消息 1，S613

中接入网设备 0 发送的切换命令消息（即 MAC 层消息）中可以携带 NCC0。可选地，若目标接入网设备不属于 LTM 切换的候选接入网设备，则接入网设备 0 可以触发普通跨站切换。

在其它示例中，在切换准备过程中，接入网设备 0 在确定多个候选接入网设备后，可以分别确定多个候选接入网设备的密钥，并通过切换请求消息发送给相应的接入网设备。以接入网设备 1 为例，接入网设备 0 可以根据密钥 K0、第二接入网设备上小区的 PCI 以及载频，水平推演得到密钥 K1，并通过 S603 中的切换请求消息 1 将密钥 K1 发送给接入网设备 1。可选地，切换请求消息 1 还可以包括 NCC0，接入网设备 1 构造的容器中可以包括 NCC0。

此种情形下，可选的，S612 中的 Xn 消息可以无需携带 NCC0 和密钥 K1，S613 中的切换命令消息无需携带 NCC0，在 S614 中终端可以根据接入网设备 1 构造的容器中的 NCC0 推演密钥。

此外可选的，S612 中的 Xn 消息可以携带 NCC0 和根据密钥 K1 水平推演的密钥，S613 中的切换命令消息中携带 NCC0，在 S614 中终端可以根据 S613 中的切换命令消息中的 NCC0 和密钥 KI 水平推演密钥。

S614，终端推演密钥。

终端的 MAC 层可以从上述 MAC CE 中获得 NCC0，进而将 NCC0 传递给终端的 RRC 层。由于获得的 NCC0 与终端本地保存的 NCC0 相同，因此，终端的 RRC 层可以执行水平推演，即根据 K0、接入网设备 1 上小区的 PCI 以及载频，推演得到密钥 K1。这样，终端和接入网设备 1 维护相同的密钥，即 K1。

S615，终端从接入网设备 0 上去附着，并向接入网设备 1 发送切换完成消息。相应的，接入网设备 1 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

S616，接入网设备 1 向 AMF 网元发送路径切换请求消息；相应地，AMF 网元接收路径切换请求消息。

S617，AMF 网元向接入网设备 1 发送路径切换响应消息；相应地，接入网设备 1 接收路径切换响应消息，进而完成路径切换。

此处，路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 0—终端”切换为“UPF 网元—接入网设备 1—终端”。

AMF 网元接收到路径切换请求消息后，可以将本地保存的 NCC 取值更新加 1，得到更新后的 NCC（称为 NCC1），以根据更新后的 NCC 执行垂直推演，得到更新后的 NH（称为 NH1）。NCC1 和 NH1 关联，作为更新后的一对 {NH1, NCC1}。

路径切换响应消息中包括 {NH1, NCC1}，接入网设备 1 接收到路径切换响应消息后，保存 {NH1, NCC1}，以用于下一次 LTM 切换推演密钥。

S618，终端与接入网设备 1 使用密钥 K1 进行通信。

S619，接入网设备 1 确定终端需要切换，切换的目标接入网设备为接入网设备 2。

针对于上述实现 1，接入网设备 1 可以判断目标接入网设备（即接入网设备 2）是否属于接入网设备列表 1，若目标接入网设备属于接入网设备列表 1，则接入网设备 1 可以执行 S620 和 S621，以触发 LTM 跨站切换。此外，响应于目标接入网设备属于接入网设备列表 1，S621 中接入网设备 1 发送的切换命令消息（即 MAC 层消息）中可以携带 NCC1。可选地，若目标接入网设备不属于接入网设备列表 1，则接入网设备 1 可以触发普通跨站切换。

针对于上述实现 2，接入网设备 1 可以判断目标接入网设备（即接入网设备 2）是否属于接入网设备列表 2，若目标接入网设备属于接入网设备列表 2，则接入网设备 1 可以执行 S620 和 S621，以触发 LTM 跨站切换。此外，响应于目标接入网设备属于接入网设备列表 2，S621 中接入网设备 1 发送的切换命令消息（即 MAC 层消息）中可以携带 NCC1。可选地，若目标接入网设备不属于接入网设备列表 2，则接入网设备 1 可以触发普通跨站切换。

S620，接入网设备 1 向接入网设备 2 发送 Xn 消息；相应地，接入网设备 2 接收来自接入网设备 1 的 Xn 消息。

接入网设备 1 根据之前保存的 NH1、接入网设备 2 上小区的 PCI 以及载频，推演得到密钥 K2*。Xn 消息包括 NCC1 和密钥 K2*。

作为一种可能的实现，接入网设备 1 可以直接通过 Xn 消息将接入网设备列表 1 发送给接入网设备

2 (此种情形下的接入网设备列表 1 即为实施例一中的第二候选接入网设备列表)。或者,也可以由接入网设备 0 通过切换请求消息 2 向接入网设备 1 发送接入网设备列表 1,此种情形下,Xn 消息可以不包括接入网设备列表 1。

5 作为又一种可能的实现,接入网设备 1 可以根据多种可能的因素(比如候选接入网设备上的负载等),从接入网设备列表 1 中选择部分或全部接入网设备,进而通过 Xn 消息将选择的接入网设备的标识发送给接入网设备 1。此种情形下,Xn 消息还包括接入网设备列表 3,接入网设备列表 3 包括接入网设备 1 选择的接入网设备的标识(接入网设备列表 3 即为实施例一中的第二候选接入网设备列表)。

可选地,针对于该实现,接入网设备 0 还可以通过切换请求消息 2 向接入网设备 2 发送接入网设备列表 1,或者接入网设备 1 还可以通过 Xn 消息向接入网设备 2 发送接入网设备列表 1,具体不做限定。

10 S621,接入网设备 1 向终端发送切换命令消息。相应的,终端接收来自接入网设备 1 的切换命令消息。

切换命令消息为 MAC 层消息,比如 MAC CE。切换命令消息包括目标接入网设备的标识(即接入网设备 2 的标识)和 NCC1。

15 其中,接入网设备 1 确定终端需要切换到接入网设备 2 后,便可生成切换命令消息,并发送切换命令消息。相比于普通切换流程来说,由于接入网设备 1 在确定终端需要切换时,便可以自行生成包含 NCC1 的切换命令消息,并向终端发送切换命令消息,从而能够降低切换时延。其中,接入网设备 1 的 RRC 层可以将 NCC1 传递到接入网设备 1 的 MAC 层,进而接入网设备 1 的 MAC 层生成的切换命令消息包括 NCC1。

S622,终端推演密钥。

20 终端的 MAC 层可以从上述 MAC CE 中获得 NCC1,进而将 NCC1 传递给终端的 RRC 层。由于获得的 NCC1 与终端本地保存的 NCC0 不同,因此,终端的 RRC 层可以将本地保存的 NCC 更新为 NCC1,并根据 NCC1 与 NCC0 的差值,执行相应次数的垂直推演,得到相应的 NH(即 NH1),进而根据 NH1、接入网设备 2 上的小区的 PCI 以及载频,推演得到密钥 K2*。这样,终端和接入网设备 2 维护相同的密钥,即 K2*。

25 S623,终端从接入网设备 1 上去附着,并向接入网设备 2 发送切换完成消息。相应的,接入网设备 2 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

S624,接入网设备 2 向 AMF 网元发送路径切换请求消息;相应地,AMF 网元接收路径切换请求消息。

30 S625,AMF 网元向接入网设备 2 发送路径切换响应消息;相应地,接入网设备 2 接收路径切换响应消息,进而完成路径切换。

此处,路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 1—终端”切换为“UPF 网元—接入网设备 2—终端”。

35 AMF 网元接收到路径切换请求消息后,可以将本地保存的 NCC 取值更新加 1,得到更新后的 NCC(称为 NCC2),以根据更新后的 NCC 执行垂直推演,得到更新后的 NH(称为 NH2)。NCC2 和 NH2 关联,作为更新后的一对{NH2,NCC2}。

路径切换响应消息中包括{NH2,NCC2},接入网设备 1 接收到路径切换响应消息后,保存{NH2,NCC2},以用于下一次 LTM 切换推演密钥。

S626,终端与接入网设备 2 使用 K2*进行通信。

40 可以理解的是,如果 LTM 切换的候选接入网设备还包括接入网设备 3,则后续终端还可以从接入网设备 2 切换到接入网设备 3,具体的实现可以参照终端从接入网设备 1 切换到接入网设备 2 的描述。

此外,图 6 所示意的流程与图 5 所示意的流程相对应,二者的步骤可以相互参照。比如,S501 可以参照 S602 至 S608,S502 可以参照 S609,S503 可以参照 S611,S504 可以参照 S613 和 S614,S505 可以参照 S615,S506 可以参照 S616 和 S617,S507 可以参照 S618,S508 可以参照 S619,S509 可以参照 S620,S510 可以参照 S621 和 S622,S511 可以参照 S623,S512 可以参照 S624 和 S625,S513 可以参照 S626。

采用上述方法,一方面,源接入网设备向终端发送 NCC,使得终端可以根据 NCC 确定密钥,以及源接入网设备可以根据 NCC 对应的 NH 推演密钥并发送给目标接入网设备,从而使得终端和目标接入

网设备可以维护相同的密钥, 保证终端和目标接入网设备之间的安全通信; 且由于每次执行 LTM 切换时, NCC 都会发生更新, 从而可以使得终端在多个接入网设备之间来回切换时, 也不会出现密钥重用的问题。比如, 终端从接入网设备 0 切换到接入网设备 1, 从接入网设备 1 切换到接入网设备 2, 从接入网设备 2 再切换回接入网设备 1, 终端和接入网设备 1 进行通信所使用的密钥在前后两次切换中不同。

- 5 另一方面, 接入网设备 0 知晓终端和接入网设备 1 共享的密钥 (即 $K1$), 但无法知晓终端和接入网设备 2 共享的密钥 (即 $K2^*$), 也无法知晓终端和后续的目标接入网设备共享的密钥, 从而可以实现两跳安全。

实施例三

- 10 图 7 为本申请实施例提供的通信方法所对应的流程示意图。如图 7 所示, 该流程可以包括: S701 至 S717 可以参照 S601 至 S617 的描述, 不再赘述。

S718, 接入网设备 1 推演密钥。

接入网设备 1 根据 $NH1$ 、接入网设备 1 上的小区的 PCI 以及载频, 推演得到密钥 $K1^*$ 。

S719, 接入网设备 1 向终端发送消息 1, 消息 1 包括 $NCC1$; 相应地, 终端接收消息 1。

- 15 消息 1 可以为 MAC 层消息 (比如 MAC CE) 或 RRC 层消息 (比如 RRC 重配置消息), 具体不做限定。

S720, 终端推演密钥。

- 20 终端的 MAC 层可以从上述消息 1 中获得 $NCC1$, 进而将 $NCC1$ 传递给终端的 RRC 层。由于获得的 $NCC1$ 与终端本地保存的 $NCC0$ 不同, 因此, 终端的 RRC 层可以将本地保存的 NCC 更新为 $NCC1$, 并根据 $NCC1$ 与 $NCC0$ 的差值, 执行相应次数的垂直推演, 得到相应的 NH (即 $NH1$), 进而根据 $NH1$ 、接入网设备 1 上的小区的 PCI 以及载频, 推演得到密钥 $K1^*$ 。这样, 终端和接入网设备 1 维护相同的密钥, 即 $K1^*$ 。

S721, 终端与接入网设备 1 使用密钥 $K1^*$ 进行通信。

S722, 接入网设备 1 确定终端需要切换, 切换的目标接入网设备为接入网设备 2。

- 25 S723, 接入网设备 1 向接入网设备 2 发送 Xn 消息; 相应地, 接入网设备 2 接收来自接入网设备 1 的 Xn 消息。

接入网设备 1 根据 $K1^*$ 、接入网设备 2 上的小区的 PCI 以及载频, 推演得到密钥 $K2$ 。 Xn 消息包括 $NCC1$ 和密钥 $K2$ 。

上述 S722 和 S723 可以参照 S619 和 S620 中的描述。

- 30 S724, 接入网设备 1 向终端发送切换命令消息。相应的, 终端接收来自接入网设备 1 的切换命令消息。

切换命令消息为 MAC 层消息, 比如 MAC CE。切换命令消息包括目标接入网设备的标识 (即接入网设备 2 的标识) 和 $NCC1$ 。

S725, 终端推演密钥。

- 35 终端的 MAC 层可以从上述 MAC CE 中获得 $NCC1$, 进而将 $NCC1$ 传递给终端的 RRC 层。由于获得的 $NCC1$ 与终端保存的 $NCC1$ 相同, 因此, 终端的 RRC 层可以执行水平推演, 即根据 $K1^*$ 、接入网设备 2 上的小区的 PCI 以及载频, 推演得到密钥 $K2$ 。这样, 终端和接入网设备 2 维护相同的密钥, 即 $K2$ 。

- 40 S726, 终端从接入网设备 1 上去附着, 并向接入网设备 2 发送切换完成消息。相应的, 接入网设备 2 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

S727, 接入网设备 2 向 AMF 网元发送路径切换请求消息; 相应地, AMF 网元接收路径切换请求消息。

- 45 S728, AMF 网元向接入网设备 2 发送路径切换响应消息; 相应地, 接入网设备 2 接收路径切换响应消息, 进而完成路径切换。

此处, 路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 1—终端”切换为“UPF 网元—接入网设备 2—终端”。

AMF 网元接收到路径切换请求消息后, 可以将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC

(称为 NCC2), 以根据更新后的 NCC 执行垂直推演, 得到更新后的 NH (称为 NH2)。NCC2 和 NH2 关联, 作为更新后的一对 {NH2, NCC2}。

路径切换响应消息中包括 {NH2, NCC2}, 接入网设备 1 接收到路径切换响应消息后, 保存 {NH2, NCC2}。

5 S729, 接入网设备 2 推演密钥。

接入网设备 2 根据 NH2、接入网设备 2 上的小区的 PCI 以及载频, 推演得到密钥 K2*。

S730, 接入网设备 2 向终端发送消息 2, 消息 2 包括 NCC2; 相应地, 终端接收消息 2。

消息 2 可以为 MAC 层消息 (比如 MAC CE) 或 RRC 层消息 (比如 RRC 重配置消息), 具体不做限定。

10 S731, 终端推演密钥。

终端可以从上述消息 2 中获得 NCC2, 由于获得的 NCC2 与终端本地保存的 NCC1 不同, 因此, 终端可以将本地保存的 NCC1 更新为 NCC2, 并根据 NCC2 与 NCC1 的差值, 执行相应次数的垂直推演, 得到相应的 NH (即 NH2), 进而根据 NH2、接入网设备 1 上的小区的 PCI 以及载频, 推演得到密钥 K2*。这样, 终端和接入网设备 2 维护相同的密钥, 即 K2*。

15 S732, 终端与接入网设备 2 使用密钥 K2* 进行通信。

可以理解的是, 后续终端还可以从接入网设备 2 切换到其它接入网设备 (比如接入网设备 3), 具体的实现可以参照终端从接入网设备 1 切换到接入网设备 2 的描述。

此外, 图 7 所示意的流程与图 6 的区别在于: 图 6 用于实现两跳安全, 即接入网设备从 AMF 接收的 NCC 和 NH, 用于终端切换到下一个基站场景下的通信安全保护; 图 7 用于实现一跳安全, 即接入网设备从 AMF 接收的 NCC 和 NH, 用于终端切换到当前基站场景下的通信安全保护; 因此图 7 相比于图 6 多了一些额外步骤, 比如 S718 至 S720、S729 至 S731; 除此区别之外, 二者的步骤可以相互参照, 此处不再一一赘述。

采用上述方法, 接入网设备 0 无法知晓终端和接入网设备 1 所使用的密钥 (即 K1*), 也无法知晓终端和接入网设备 2 所使用的密钥 (即 K2*), 更无法知晓终端和后续的目标接入网设备共享的密钥, 从而可以实现一跳安全。

实施例四

在实施例四中, 将针对方案二进行详细描述。

图 8 为本申请实施例提供的通信方法所对应的流程示意图。如图 8 所示, 该流程可以包括:

30 S801, 第一接入网设备向多个候选接入网设备分别发送切换请求消息, 切换请求消息用于请求多个候选接入网设备构造容器。

此处, 第一接入网设备可以为终端通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程所接入的接入网设备。第一接入网设备和终端可以保存相同的密钥 (该密钥用于第一接入网设备和终端进行通信) 和 NCC (比如第一 NCC)。

35 以多个候选接入网设备中的第二接入网设备为例, 第一接入网设备可以根据第一输入参数推演得到密钥 1, 并向第二接入网设备发送切换请求消息, 切换请求消息包括第一 NCC 和密钥 1。相应地, 第二接入网设备接收到切换请求消息后, 可以获得并保存第一 NCC 和密钥 1。其中, 第一输入参数包括以下一项或多项: 第二接入网设备上的小区的 PCI、该小区的载频、终端与第一接入网设备之间进行安全保护的密钥 KgNB 等。

40 S802, 第一接入网设备接收多个候选接入网设备中每个接入网设备构造的容器, 每个接入网设备构造的容器包括用于终端切换到每个接入网设备的参数和第一 NCC (即从切换请求消息中获得的)。

S803, 第一接入网设备向终端发送 RRC 重配置消息, RRC 重配置消息包括多个候选接入网设备中每个接入网设备构造的容器。

45 此处, 终端从 RRC 重配置消息中获得多个候选接入网设备构造的容器。进一步地, 以多个候选接入网设备中的第二接入网设备为例, 终端可以从第二接入网设备构造的容器获得第一 NCC, 由于获得的第一 NCC 与终端本地保存的 NCC 相同, 因此, 终端可以执行水平推演, 即根据第一输入参数, 水平推演得到终端与第二接入网设备进行通信所使用的密钥, 并保存该密钥与第二接入网设备的标识之间的对应关系。如此, 终端可以保存多个候选接入网设备分别对应的密钥。

本申请实施例对终端确定多个候选接入网设备分别对应的密钥的具体时机不做限定。

上述 S801 和 S803 可以理解为切换准备过程, 相关实现可以参照实施例一中的描述。

S804, 第一接入网设备确定终端需要切换到第二接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

5 第一接入网设备确定终端需要切换到第二接入网设备后, 可以进一步确定第二接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。由于第一接入网设备确定多个候选接入网设备后, 终端尚未切换到多个候选接入网设备中的任一接入网设备上, 因此, 第一接入网设备可以确定这多个候选接入网设备均为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

该实施例中, 第二接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。在
10 其它示例中, 若第二接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备, 则第一接入网设备可以向终端发送 RRC 重配置消息, RRC 重配置消息用于触发终端切换到第二接入网设备(即执行普通跨站切换)。

示例性地, 连续 LTM 切换是指在切换准备阶段获得配置信息后, 通过 L1/L2 消息触发的多次切换, 即在获得配置信息后, 连续的 L1/L2 消息触发切换可以不需要额外的 RRC 配置。

15 连续 LTM 切换过程可以包括终端获取多个候选接入网设备构造的容器的过程(即切换准备过程)和多次连续的 LTM 切换。其中, 多个候选接入网设备即为对于终端的连续 LTM 切换过程中的候选接入网设备。比如, 终端通过初始接入流程或普通切换流程或重建流程或者小区重选流程接入到接入网设备 a 后, 接入网设备 a 接收多个候选接入网设备(比如接入网设备 b 至 d)构造的容器, 并通过 RRC 重配置消息发送给终端; 后续, 终端通过 LTM 切换从接入网设备 a 切换到接入网设备 b(第 1 次 LTM
20 切换), 此时接入网设备 b 为连续 LTM 切换过程中已被切换过的接入网设备, 而接入网设备 c 和 d 为连续 LTM 切换过程中未被切换过的接入网设备; 可选地, 接入网设备 a 可以记录 LTM 连续切换次数为 1, 并向接入网设备 b 发送 LTM 连续切换次数。终端再次通过 LTM 切换从接入网设备 b 切换到接入网设备 c(第 2 次 LTM 切换), 此时接入网设备 b 和 c 均为连续 LTM 切换过程中已被切换过的接入网设备, 而接入网设备 d 为连续 LTM 切换过程中未被切换过的接入网设备; 可选地, 接入网设备 b 可以将 LTM 连续切换次数加 1(即 LTM 连续切换次数为 2), 并向接入网设备 c 发送 LTM 连续切换次数。终端再次通过 LTM 切换从接入网设备 c 切换到接入网设备 d(第 3 次 LTM 切换), 此时接入网设备 b、c 和 d 均为
25 连续 LTM 切换过程中已被切换过的接入网设备。可选地, 接入网设备 c 可以将 LTM 连续切换次数加 1(即 LTM 连续切换次数为 3), 并向接入网设备 d 发送 LTM 连续切换次数。若终端通过普通切换流程或者重建流程或者小区重选流程从接入网设备 d 连接到接入网设备 e, 则终端执行的上述 3 次 LTM
30 切换可以理解为 3 次连续的 LTM 切换; 可选地, 接入网设备 d 可以将 LTM 连续切换次数清零。

其中, LTM 连续切换次数可以是指在对于终端的连续 LTM 切换过程中所执行的 LTM 切换的次数。

此外, 该实施例中是以第一接入网设备根据“第二接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备”来判断执行 LTM 跨站切换还是普通跨站切换为例进行描述的; 即第二接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 则执行 LTM 跨站切换(即
35 S805 和 S806 等步骤); 否则执行普通跨站切换。

在其它可能的实施例中, 第一接入网设备还可以根据 NCC 的值和/或 LTM 连续切换次数, 确定执行 LTM 跨站切换还是普通跨站切换。比如, 若第二接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备、第一接入网设备中存储的 NCC 不属于预设值、LTM 连续切换次数小于阈值, 则可以执行 LTM 跨站切换, 否则(比如满足第二接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备、第一接入网设备中存储的 NCC 为预设值、LTM 连续切换次数大于或等于阈值中的
40 至少一项), 可以执行普通跨站切换。

S805, 第一接入网设备向第二接入网设备发送第三候选接入网设备列表, 第三候选接入网设备列表包括对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

比如, 第一接入网设备确定多个候选接入网设备均为对于终端的连续 LTM 切换过程中还未被切换
45 过的接入网设备, 则第三候选接入网设备列表包括多个候选接入网设备的标识, 即源接入网设备向目标接入网设备发送的候选接入网设备列表不包括源接入网设备。

在其它示例中, 由于终端即将切换到第二接入网设备, 因此, 第三候选接入网设备列表包括多个候选接入网设备中除第二接入网设备以外的其它接入网设备的标识, 即源接入网设备向目标接入网设备发

送的候选接入网设备列表不包括源接入网设备和目标接入网设备。

S806, 第一接入网设备向终端发送第一 MAC 层消息, 第一 MAC 层消息用于触发终端切换到第二接入网设备。

此处, 第一 MAC 层消息可以包括第二接入网设备的标识。

- 5 可选地, 响应于第一 MAC 层消息, 终端可以删除第一接入网设备相关的上下文信息, 比如删除终端和第一接入网设备进行通信所使用的密钥等。需要说明的是, 若终端未在切换准备过程中确定多个候选接入网设备分别对应的密钥, 则响应于第一 MAC 层消息, 终端可以不删除终端和第一接入网设备进行通信所使用的密钥。

S807, 终端根据第二接入网设备构造的容器中的参数, 切换到第二接入网设备。

- 10 可选地, 在终端切换到第二接入网设备之后, 第二接入网设备可以向 AMF 网元发送路径切换请求消息, 相应地, AMF 网元可以根据路径切换请求消息, 向第二接入网设备发送路径切换响应消息。

S808, 终端和第二接入网设备使用密钥 1 进行通信。

- 此处, 终端的 MAC 层从第一 MAC 层消息中获得第二接入网设备的标识后, 可以将第二接入网设备的标识传递给 RRC 层; 进而, 终端的 RRC 层可以根据第二接入网设备的标识获得第二接入网设备对应的密钥 (即密钥 1); 以及, 第二接入网设备可以获得之前保存的密钥 1。进而终端和第二接入网设备可以使用密钥 1 进行通信。
- 15 可以理解的是, 上述是以终端接收到 RRC 重配置消息, 便推演各个接入网设备对应的密钥为例进行描述的, 本申请实施例对终端推演密钥的具体时机不做限定, 比如终端也可以在接收到第一 MAC 层消息后, 再推演终端与第二接入网设备进行通信所使用的密钥。

- 20 可选地, 在终端从第一接入网设备切换到第二接入网设备之后, 上述方法还包括:
- S809, 第二接入网设备确定终端需要切换到的第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

- 示例性的, 第二接入网设备可以判断第三接入网设备是否属于第三候选接入网设备列表, 若第三接入网设备属于第三候选接入网设备列表, 则确定第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备; 若第三接入网设备不属于第三候选接入网设备列表, 则确定第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。
- 25 可以理解的是, 在其它实施例中, 第一接入网设备可以向第二接入网设备发送多个候选接入网设备的标识和第五候选接入网设备列表, 第五候选接入网设备列表包括对于终端的连续 LTM 切换过程中已被切换过的接入网设备。此种情形下, 第二接入网设备可以先判断第三接入网设备是否属于多个候选接入网设备, 若第三接入网设备属于多个候选接入网设备, 则进一步判断第三接入网设备是否属于第五候选接入网设备列表 (若第三接入网设备不属于多个候选接入网设备, 则执行普通切换)。若第三接入网设备不属于第五候选接入网设备列表, 则确定第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备; 若第三接入网设备属于第五候选接入网设备列表, 则确定第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

- 30 此外, 该实施例中是以第二接入网设备根据“第三接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备”来判断执行 LTM 跨站切换还是普通跨站切换为例进行描述的。在其它可能的实施例中, 第二接入网设备还可以根据 NCC 的值和/或 LTM 连续切换次数, 确定执行 LTM 跨站切换还是普通跨站切换。比如, 若第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备、第二接入网设备中存储的 NCC (即从路径切换响应消息中获取的 NCC) 不属于预设值、LTM 连续切换次数小于阈值, 则可以执行 LTM 跨站切换, 否则 (比如满足第三接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备、第二接入网设备中存储的 NCC 为预设值、LTM 连续切换次数大于或等于阈值中的至少一项), 可以执行普通跨站切换。

- 35 此外, 该实施例中是以第二接入网设备根据“第三接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备”来判断执行 LTM 跨站切换还是普通跨站切换为例进行描述的。在其它可能的实施例中, 第二接入网设备还可以根据 NCC 的值和/或 LTM 连续切换次数, 确定执行 LTM 跨站切换还是普通跨站切换。比如, 若第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备、第二接入网设备中存储的 NCC (即从路径切换响应消息中获取的 NCC) 不属于预设值、LTM 连续切换次数小于阈值, 则可以执行 LTM 跨站切换, 否则 (比如满足第三接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备、第二接入网设备中存储的 NCC 为预设值、LTM 连续切换次数大于或等于阈值中的至少一项), 可以执行普通跨站切换。
- 40 S810, 第二接入网设备向第三接入网设备发送第四候选接入网设备列表, 第四候选接入网设备列表包括对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

- 45 比如, 第四候选接入网设备列表包括多个候选接入网设备中除第二接入网设备以外的其它接入网设备的标识, 即源接入网设备向目标接入网设备发送的候选接入网设备列表不包括源接入网设备。

在其它示例中, 由于终端即将切换到第三接入网设备, 因此, 第四候选接入网设备列表包括多个候选接入网设备中除第二接入网设备和第三接入网设备以外的其它接入网设备的标识, 即源接入网设备向

目标接入网设备发送的候选接入网设备列表不包括源接入网设备和目标接入网设备。

S811, 第二接入网设备向终端发送第二 MAC 层消息, 第二 MAC 层消息用于触发终端切换到第三接入网设备。

5 可选地, 响应于第二 MAC 层消息, 终端可以删除第二接入网设备相关的上下文信息, 比如删除终端和第二接入网设备进行通信所使用的密钥等。

S812, 终端根据第三接入网设备构造的容器中的参数, 切换到第三接入网设备。

可选地, 在终端切换到第三接入网设备之后, 第三接入网设备可以向 AMF 网元发送路径切换请求消息, 相应地, AMF 网元可以根据路径切换请求消息, 向第三接入网设备发送路径切换响应消息。

10 S813, 终端根据第一 NCC 确定与第三接入网设备进行通信的密钥, 并根据该密钥与第三接入网设备进行通信。

采用上述方法, 由于多个候选接入网设备中每个接入网设备构造的容器携带第一 NCC, 进而终端在切换到其中任一接入网设备后, 是根据该接入网设备构造的容器中携带的第一 NCC (以及该接入网设备上的小区的信息), 来确定终端与该接入网设备进行通信所使用的密钥, 实现较为简便; 在执行 LTM 切换时, 源接入网设备可以判断目标接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 若是, 则可以执行 LTM 跨站切换, 否则执行普通跨站切换, 从而可以使得终端在多个候选接入网设备之间来回切换时, 不会出现密钥重用的问题。

20 基于实施例四, 下面结合实施例五描述一种可能的实现流程。在实施例五中, 将以实施例四中的“第一接入网设备”为接入网设备 0, “第二接入网设备”为接入网设备 1, “第三接入网设备”为接入网设备 2 为例进行描述。

实施例五

图 9 为本申请实施例提供的通信方法所对应的流程示意图。如图 9 所示, 该流程包括:

S901, 终端通过接入网设备 0 连接到 5GC。

25 终端可以通过初始接入流程或者普通切换流程或者重建立流程或者小区重选等流程接入到接入网设备 0, 通过接入网设备 0 接入到 5GC。进而, 终端和接入网设备 0 上分别保存密钥 KgNB (为便于描述, 称为 K0) 和 NCC0 (K0 关联 NCC0), AMF 网元上保存 NCC0。

S902, 接入网设备 0 确定 LTM 切换的多个候选接入网设备。

此处的描述可以参照 S402。

30 该流程中, 以 LTM 切换的多个候选接入网设备包括接入网设备 1、接入网设备 2.....接入网设备 5 为例进行描述。

S903, 接入网设备 0 向接入网设备 1 发送切换请求消息 1。相应的, 接入网设备 1 接收来自接入网设备 0 的切换请求消息 1。

接入网设备 0 根据 K0、接入网设备 1 的小区的 PCI 以及载频, 推演得到密钥 K1。切换请求消息 1 包括 NCC0 和密钥 K1。接入网设备 1 接收到切换请求消息 1 后, 可以保存 NCC0 和密钥 K1。

35 S904, 接入网设备 1 构造容器。

如果接入网设备 1 允许终端执行 LTM 切换, 则接入网设备 1 可以构造容器。容器携带有接入网设备 1 的标识、NCC0 和配置信息, 配置信息包括用于终端切换到接入网设备 1 的参数。

S905, 接入网设备 1 向接入网设备 0 发送切换请求确认消息 1。相应的, 接入网设备 0 接收来自接入网设备 1 的切换请求确认消息 1。

40 切换请求确认消息 1 包括接入网设备 1 构造的容器。

S906, 接入网设备 0 向接入网设备 2 发送切换请求消息 2。相应的, 接入网设备 2 接收来自接入网设备 0 的切换请求消息 2。

接入网设备 0 根据 K0、接入网设备 2 的小区的 PCI 以及载频, 推演得到密钥 K2。切换请求消息 2 包括 NCC0 和密钥 K2。接入网设备 2 接收到切换请求消息 2 后, 可以保存 NCC0 和密钥 K2。

45 S907, 接入网设备 2 构造容器。

如果接入网设备 2 允许终端执行 LTM 切换, 则接入网设备 2 可以构造容器。容器携带有接入网设备 2 的标识、NCC0 和配置信息, 配置信息包括用于终端切换到接入网设备 2 的参数。

S908, 接入网设备 2 向接入网设备 0 发送切换请求确认消息 2。相应的, 接入网设备 0 接收来自接

入网设备 1 的切换请求确认消息 2。

切换请求确认消息 2 包括接入网设备 2 构造的容器。

可以理解的是,上述仅描述了接入网设备 0 向接入网设备 1 和接入网设备 2 发送切换请求消息,接入网设备 0 还可以向其它 LTM 切换的候选接入网设备发送切换请求信息,具体实现可以参照上述 S903 至 S908,不再赘述。

S909,接入网设备 0 向终端发送 RRC 重配置消息,该 RRC 重配置消息携带有接入网设备 1 构造的容器和接入网设备 2 构造的容器;相应地,终端接收 RRC 重配置消息。

终端从 RRC 重配置消息中获得接入网设备 1 构造的容器和接入网设备 2 构造的容器。进一步地,终端可以从接入网设备 1 构造的容器获得 NCC0,由于获得的 NCC0 与终端本地保存的 NCC0 相同,因此,终端可以执行水平推演,即根据 K0、接入网设备 1 上的小区的 PCI 以及载频,推演得到密钥 K1,并保存密钥 K1 与接入网设备 1 的标识之间的对应关系(比如保存在接入网设备 1 相关的上下文信息中)。终端可以从接入网设备 2 构造的容器获得 NCC0,由于获得的 NCC0 与终端本地保存的 NCC0 相同,因此,终端可以执行水平推演,即根据 K0、接入网设备 2 上的小区的 PCI 以及载频,推演得到密钥 K2,并保存密钥 K2 与接入网设备 2 的标识之间的对应关系(比如保存在接入网设备 2 相关的上下文信息中)。

S910,终端向接入网设备 0 发送 RRC 重配置完成消息;相应的,接入网设备 0 接收来自终端的 RRC 重配置完成消息。

S911,接入网设备 0 确定终端需要切换,切换的目标接入网设备为接入网设备 1。

S912,接入网设备 0 判断执行 LTM 跨站切换还是普通跨站切换。

若目标接入网设备(即接入网设备 1)为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备,则接入网设备 0 可以确定执行 LTM 跨站切换;若目标接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备,则接入网设备 0 可以确定执行普通跨站切换。在该流程中,由于接入网设备 1 为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备,因此,接入网设备 0 可以确定执行 LTM 跨站切换。

S913,接入网设备 0 向接入网设备 1 发送 Xn 消息;相应的,接入网设备 1 接收来自接入网设备 0 的 Xn 消息。

Xn 消息可以包括接入网设备列表 1(即实施例四中的第三候选接入网设备列表),接入网设备列表 1 可以包括 LTM 切换的至少一个候选接入网设备的标识。如前文所述,接入网设备 0 确定了 LTM 切换的多个候选接入网设备(比如接入网设备 1 至接入网设备 5),接入网设备列表 1 可以包括这多个候选接入网设备中的部分或全部。

其中,接入网设备列表 1 中的接入网设备可以均为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。比如,接入网设备列表包括接入网设备 1 至接入网设备 5。

S914,接入网设备 0 向终端发送切换命令消息。相应的,终端接收来自接入网设备 0 的切换命令消息。

切换命令消息为 MAC 层消息,比如 MAC CE。切换命令消息包括目标接入网设备的标识,即接入网设备 1 的标识。

S915,终端从接入网设备 0 上去附着,并向接入网设备 1 发送切换完成消息。相应的,接入网设备 1 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

终端可以根据上述切换命令消息(即 MAC CE)中的接入网设备 1 的标识,获取之前存储的接入网设备 1 构造的容器,进而可以向接入网设备 1 发送切换完成消息。

S916,接入网设备 1 向 AMF 网元发送路径切换请求消息;相应地,AMF 网元接收路径切换请求消息。

S917,AMF 网元向接入网设备 1 发送路径切换响应消息;相应地,接入网设备 1 接收路径切换响应消息,进而完成路径切换。

此处,路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 0—终端”切换为“UPF 网元—接入网设备 1—终端”。

可选地,AMF 网元接收到路径切换请求消息后,可以将本地保存的 NCC 取值更新加 1,得到更新后的 NCC(称为 NCC1),以根据更新后的 NCC 执行垂直推演,得到更新后的 NH(称为 NH1)。NCC1

和 NH1 关联, 作为更新后的一对 {NH1,NCC1}。

路径切换响应消息中包括 {NH1,NCC1}, 接入网设备 1 接收到路径切换响应消息后, 保存 {NH1,NCC1}。

S918, 终端与接入网设备 1 使用密钥 K1 进行通信。

- 5 终端可以根据上述切换命令消息 (即 MAC CE) 中的接入网设备 1 的标识, 获取之前存储的与接入网设备 1 的标识对应的密钥 K1; 而接入网设备 1 也通过切换请求消息接收到了密钥 K1, 因此, 终端与接入网设备 1 可以使用密钥 K1 进行通信。

S919, 接入网设备 1 确定终端需要切换, 切换的目标接入网设备为接入网设备 2。

S920, 接入网设备 1 判断执行 LTM 跨站切换还是普通跨站切换。

- 10 接入网设备 1 可以判断目标接入网设备 (即接入网设备 2) 是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。比如, 若接入网设备 2 属于接入网设备列表 1 中的接入网设备, 说明接入网设备 2 为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 则确定执行 LTM 跨站切换; 否则, 可以确定执行普通跨站切换。

- 15 在该实施例中, 由于接入网设备 2 属于接入网设备列表 1 中的接入网设备, 因此, 接入网设备 1 可以确定执行 LTM 跨站切换。

S921, 接入网设备 1 向接入网设备 2 发送 Xn 消息; 相应的, 接入网设备 2 接收来自接入网设备 1 的 Xn 消息。

- 20 Xn 消息可以包括接入网设备列表 2 (即实施例四中的第四候选接入网设备列表), 接入网设备列表 2 中的接入网设备可以均为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。比如, 由于接入网设备 1 为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备, 因此, 接入网设备 1 可以从接入网设备列表 1 中删除接入网设备 1 的标识, 得到接入网设备列表 2, 即接入网设备列表 2 可以包括接入网设备 2 至接入网设备 5。

S922, 接入网设备 1 向终端发送切换命令消息。相应的, 终端接收来自接入网设备 1 的切换命令消息。

- 25 切换命令消息为 MAC 层消息, 比如 MAC CE。切换命令消息包括目标接入网设备的标识, 即接入网设备 2 的标识。

S923, 终端从接入网设备 1 上去附着, 并向接入网设备 2 发送切换完成消息。相应的, 接入网设备 2 接收来自终端的切换完成消息。

切换完成消息可以为 RRC 重配置完成消息。

- 30 终端可以根据上述切换命令消息 (即 MAC CE) 中的接入网设备 2 的标识, 获取之前存储的接入网设备 2 构造的容器, 进而根据容器接入接入网设备 2 的小区, 并可以向接入网设备 2 发送切换完成消息。

S924, 接入网设备 2 向 AMF 网元发送路径切换请求消息; 相应地, AMF 网元接收路径切换请求消息。

- 35 S925, AMF 网元向接入网设备 2 发送路径切换响应消息; 相应地, 接入网设备 2 接收路径切换响应消息, 进而完成路径切换。

此处, 路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 1—终端”切换为“UPF 网元—接入网设备 2—终端”。

- 40 可选地, AMF 网元接收到路径切换请求消息后, 可以将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC (称为 NCC2), 以根据更新后的 NCC 执行垂直推演, 得到更新后的 NH (称为 NH2)。NCC2 和 NH2 关联, 作为更新后的一对 {NH2,NCC2}。

路径切换响应消息中包括 {NH2,NCC2}, 接入网设备 1 接收到路径切换响应消息后, 可以保存 {NH2,NCC2}。

S926, 终端与接入网设备 2 使用密钥 K2 进行通信。

- 45 终端可以根据上述切换命令消息 (即 MAC CE) 中的接入网设备 2 的标识, 获取之前存储的与接入网设备 2 的标识对应的密钥 K1; 而接入网设备 2 也通过切换请求消息接收到了密钥 K2, 因此, 终端与接入网设备 2 可以使用密钥 K2 进行通信。

可以理解的是, 后续终端还可以从接入网设备 2 切换到其它接入网设备 (比如接入网设备 3), 具

体的实现可以参照终端从接入网设备 1 切换到接入网设备 2 的描述。

上述流程中是以“源接入网设备向目标接入网设备发送的接入网设备列表不包括源接入网设备，但包括目标接入网设备”为例进行描述的，在其它可能的示例中，源接入网设备向目标接入网设备发送的接入网设备列表也可以不包括源接入网设备和目标接入网设备。比如，上述 S913 中，接入网设备 0 向接入网设备 1 发送的接入网设备列表 1 包括接入网设备 2 至接入网设备 5；上述 S921 中，接入网设备 1 向接入网设备 2 发送的接入网设备列表 2 包括接入网设备 3 至接入网设备 5。这是因为终端即将通过 LTM 切换切换到目标接入网设备，因此，接入网设备列表可以不再包括目标接入网设备，从而便于节省传输开销。

此外，图 9 所示意的流程与图 8 所示意的流程相对应，二者的步骤可以相互参照。比如，S801 和 S802 可以参照 S902 至 S908，S803 可以参照 S909，S804 可以参照 S911 和 S912，S805 可以参照 S913，S806 可以参照 S914，S807 可以参照 S915，S808 可以参照 S918，S809 可以参照 S919 和 S920，S810 可以参照 S921，S811 可以参照 S922，S812 可以参照 S923，S813 可以参照 S926。

采用上述方法，接入网设备 0 可以通过切换请求消息向 LTM 切换的各个候选接入网设备发送 NCC0 和相应的密钥，以及终端根据 LTM 切换的各个候选接入网设备构造的容器中所携带的 NCC0，水平推演各个候选接入网设备对应的密钥并保存，后续终端在通过 LTM 切换切换到候选接入网设备时，可以使用对应的密钥。进一步地，以接入网设备 1 为例，在终端从接入网设备 0 切换到接入网设备 1 的情况下，接入网设备 1 可以接收接入网设备列表 1，接入网设备列表 1 包括对于终端的连续 LTM 切换过程中还未被切换过的接入网设备；在接入网设备 1 确定将终端需要切换到接入网设备 2 的情况下，可以根据接入网列表 1 判断接入网设备 2 是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备，若是，则可以执行 LTM 跨站切换，否则执行普通跨站切换，从而使得终端不会通过 LTM 跨站切换重复切换到同一接入网设备，避免密钥重用的问题。

针对于方案二，以图 9 所示意的流程为例，可以理解的是：

1，上述 S909 中是以“终端从 RRC 重配置消息中获得接入网设备 1 构造的容器和接入网设备 2 构造的容器后，便推演得到各个接入网设备对应的密钥”为例进行描述的。在其它可能的示例中，终端也可以是接收到切换命令消息后，再推演当前的目标接入网设备对应的密钥。比如，终端在 S914 中接收到切换命令消息后，可以推演接入网设备 1 对应的密钥；又比如，终端在 S922 中接收到切换命令消息后，可以推演接入网设备 2 对应的密钥。此种情形下，由于推演目标接入网设备（比如接入网设备 1 或接入网设备 2）对应的密钥需要使用密钥 K0，因此，当终端从接入网设备 0 去附着后，可以不删除密钥 K0。此种情形下，终端可能仅需推演多个候选接入网设备中部分候选接入网设备对应的密钥，比如终端未切换到某个候选接入网设备，则终端无需推演该候选接入网设备对应的密钥。

2，以接入网设备 1 为例，在上述 S912 中是以接入网设备 1 根据“接入网设备 2 是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备”来判断执行 LTM 跨站切换还是普通跨站切换为例进行描述的。在其它可能的示例中，接入网设备 1 在确定终端需要切换时，也可以根据 NCC1 的值和/或 LTM 连续切换次数，确定执行 LTM 跨站切换还是普通跨站切换。

比如，若满足以下三项中的至少一项，则接入网设备 1 可以确定执行普通跨站切换，若以下三项都不满足，则接入网设备 1 可以确定执行 LTM 跨站切换：

(1) 选择的目标接入网设备为对于终端的连续 LTM 切换过程中已被切换过的接入网设备。

(2) NCC 取值为预设值；其中，预设值可以包括 0 和 7。

(3) LTM 连续切换次数大于或等于阈值；阈值可以是根据 NCC0 确定的，比如阈值可以等于 NCC 的最大值减去 NCC0，或 NCC 的最大值减去 NCC0+1。举个例子，NCC0 为 0，则阈值可以为 7 或 8。示例性地，LTM 连续切换次数的初始值可以为 0，接入网设备 0 确定执行 LTM 跨站切换后，可以将 LTM 连续切换次数的值加 1，并将 LTM 连续切换次数发送给接入网设备 1，也即接入网设备 1 可以从接入网设备 0 获得 LTM 连续切换次数。当执行普通切换时，可以将 LTM 连续切换次数重置为 0。

此处，对“可以根据 NCC1 的值，确定执行 LTM 跨站切换还是普通跨站切换”的原因进行解释说明（LTM 连续切换次数可以参照理解）：

由于 NCC 在空口上的开销只有 3 个比特，即空口上只能传输 NCC0 至 NCC7（即 NCC 的最大值为 7），若网络侧的 NCC 取值大于空口最大能够表征的取值，如 $NCC8 > NCC7$ ，这种情况下，NCC 取值会在空口上出现翻转。例如，空口上的 NCC 取值为网络侧的 NCC 取值对 8 进行取模运算后的结果，

如从 NCC8 翻转为 NCC0。

根据上述图 9 所示意的流程可以看出, 在执行 LTM 跨站切换时, 接入网设备未向终端发送 NCC, 因此, 终端并不感知网络侧(比如 AMF 网元)上 NCC 的更新, 即终端本地保存的 NCC 始终为 NCC0。

假设执行第 1 次 LTM 跨站切换时, AMF 网元上的 NCC 由 NCC0 更新为 NCC1, 并将{NH1,NCC1}通过路径切换响应消息发送给当前的目标接入网设备; 执行第 2 次 LTM 跨站切换时, AMF 网元上的 NCC 由 NCC1 更新为 NCC2, 并将{NH2,NCC2}通过路径切换响应消息发送给当前的目标接入网设备; 以此类推, 执行第 9 次 LTM 跨站切换时, AMF 网元上的 NCC 更新为 NCC1, 并将{NH9,NCC1}通过路径切换响应消息发送给当前的目标接入网设备。

若第 10 次切换为普通跨站切换时, 则源接入网设备(即第 8 次切换的目标接入网设备)会通过切换命令消息向终端发送 NCC1, 此时, 从终端来看, 终端获得的 NCC1 与终端本地保存的 NCC0 的差值为 1, 从而导致网络侧和终端对 NCC 取值更新前后的差值的理解不一致, 从而导致终端和接入网设备推演的密钥不一致, 影响终端和接入网设备之间的通信。

因此, 本申请实施例提出, 当 NCC 取值为预设值(预设值可以包括 0 和 7), 即当 NCC 即将翻转(取值为 7)或者刚刚翻转(取值为 0)时, 可以执行普通跨站切换, 从而通过切换命令消息向终端发送更新的 NCC, 便于保证后续终端和接入网设备推演的密钥一致。

实施例六

在实施例六中, 将针对方案三进行详细描述。

图 10 为本申请实施例提供的通信方法所对应的流程示意图。如图 10 所示, 该流程可以包括: S1001, 第一接入网设备确定 LTM 切换的多个候选接入网设备。

此处, 第一接入网设备可以为终端通过初始接入流程或者普通切换流程或者重建流程或者小区重选等流程所接入的接入网设备。第一接入网设备和终端可以保存相同的密钥(该密钥用于第一接入网设备和终端进行通信)和 NCC(比如第一 NCC)。

可选的, 第一接入网设备确定的多个候选接入网设备的个数小于或等于阈值, 比如该阈值是根据第一接入网设备中存储的 NCC(即第一 NCC)确定的。比如, 该阈值等于 NCC 的最大值减去第一 NCC。也就是说, 第一接入网设备确定的候选接入网设备的个数应小于或等于阈值, 以避免后续不同接入网设备对应的 NCC 相同。

S1002, 第一接入网设备向多个候选接入网设备分别发送切换请求消息, 切换请求消息用于请求多个候选接入网设备构造容器。

示例性地, 切换请求消息包括指示信息, 指示信息用于指示该切换请求消息对应 LTM 切换。

以多个候选接入网设备中的第二接入网设备为例, 第二接入网设备接收到切换请求消息后, 响应于切换请求消息, 向 AMF 网元发送请求消息, 请求消息用于请求第二接入网设备对应的 NCC。进而, AMF 网元根据请求消息, 将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC(即第二 NCC), 根据更新后的 NCC 执行垂直推演, 得到第二 NCC 对应的 NH, 并向第一接入网设备发送响应消息, 该响应消息包括第二 NCC 和第二 NCC 对应的 NH。

进一步地, 第二接入网设备构造容器, 该容器包括用于终端切换到第二接入网设备的参数, 还包括第二接入网设备对应的 NCC(即第二 NCC)和第二接入网设备的标识。第二接入网设备向第一接入网设备发送切换请求确认消息, 切换请求确认消息包括第二接入网设备构造的容器。

可选地, 第二接入网设备接收到第二 NCC 和第二 NCC 对应的 NH 后, 可以根据第二 NCC 对应的 NH、第二接入网设备上的小区以及载频, 确定第二接入网设备与终端进行通信所使用的密钥。本申请实施例对第二接入网设备确定密钥的具体时机不做限定。

上述是以多个候选接入网设备中的第二接入网设备为例进行描述的, 多个候选接入网设备中的其它接入网设备可以参照实施, 即多个候选接入网设备都根据切换请求消息, 向 AMF 网元请求各自对应的 NCC, 因此, 多个候选接入网设备中不同接入网设备对应不同的 NCC。

S1003, 第一接入网设备接收多个候选接入网设备中每个接入网设备构造的容器, 每个接入网设备构造的容器包括每个接入网设备对应的 NCC。

S1004, 第一接入网设备向终端发送 RRC 重配置消息, RRC 重配置消息包括多个候选接入网设备中每个接入网设备构造的容器。

此处，终端从 RRC 重配置消息中获得多个候选接入网设备构造的容器，每个接入网设备构造的容器包括每个接入网设备对应的 NCC 和每个接入网设备的标识；进而，终端获得多个候选接入网设备分别对应的 NCC。也可以理解为，RRC 重配置消息包括多个候选接入网设备的标识和多个 NCC 的对应关系。终端可以计算多个 NCC 对应的 NH，并存储 NCC 和 NH 的对应关系。

- 5 示例性的，终端按照 NCC 升序的方式，依次推演多个 NCC 对应的 NH。其中，若多个 NCC 中部分 NCC 的取值是翻转后的取值，则可以先确定出这部分 NCC 翻转前的值，进而根据翻转前的值进行排序。举个例子，终端当前存储的 NCC 为 3，若多个 NCC 的取值分别为 4、5、6、7，则由于这多个 NCC 的取值均大于 3，即为未翻转的取值，因此可以直接按照 4、5、6、7 进行升序排列。再举个例子，终端当前存储的 NCC 为 3，若多个 NCC 的取值分别为 4、5、6、7、0、1，则由于部分 NCC 的取值（0、1）小于 3，即为翻转后的取值，因此可以先确定出翻转前的取值（8、9），进而按照 4、5、6、7、8、9 进行升序排列。

终端可以保存接入网设备的标识、NCC 和 NH 这三项中至少两项之间的对应关系，具体实现形式不做限定，比如终端可以保存接入网设备的标识和 NH 之间的对应关系，或者终端可以保存接入网设备的标识和 NCC 之间的对应关系、NCC 和 NH 之间的对应关系。

- 15 可选地，以第二接入网设备为例，终端可以根据第二接入网设备对应的 NCC（即第二 NCC）对应的 NH、第二接入网设备上小区的 PCI 以及载频，推演得到终端与第二接入网设备进行通信所使用的密钥。如此，终端可以得到多个候选接入网设备分别对应的密钥。

上述 S1001 至 S1004 可以理解为切换准备过程，相关实现可以参照实施例一中的描述。

- 20 S1005，第一接入网设备确定终端需要切换到的第二接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

示例性的，S1005 的具体实现可以参照 S804 中的描述。

S1006，第一接入网设备向第二接入网设备发送第三候选接入网设备列表，第三候选接入网设备列表包括对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

- 25 S1007，第一接入网设备向终端发送第一 MAC 层消息，第一 MAC 层消息用于触发终端切换到第二接入网设备。

此处，第一 MAC 层消息可以包括第二接入网设备的标识。

可选地，响应于第一 MAC 层消息，终端可以删除第一接入网设备相关的上下文信息，比如删除第一 NCC、终端和第一接入网设备进行通信所使用的密钥等。

S1008，终端根据第二接入网设备构造的容器中的参数，切换到第二接入网设备。

- 30 S1009，终端根据终端与第二接入网设备进行通信所使用的密钥，与第二接入网设备进行通信。

此处对终端获得终端与第二接入网设备进行通信所使用的密钥的几种实现进行详细描述。

- 实现 1，若终端接收到 RRC 重配置消息后，便确定多个候选接入网设备分别对应的密钥，并存储多个候选接入网设备的标识和多个密钥之间的对应关系，则在 S1009 中，终端可以根据第一 MAC 层消息所携带的第二接入网设备的标识，以及多个候选接入网设备的标识和多个密钥之间的对应关系，得到第二接入网设备对应的密钥。

- 40 实现 2，若终端接收到 RRC 重配置消息后，便确定多个 NCC 对应的 NH，并存储多个候选接入网设备的标识和多个 NH 之间的对应关系，则在 S1009 中，终端可以根据第一 MAC 层消息所携带的第二接入网设备的标识，以及多个候选接入网设备的标识和多个 NH 之间的对应关系，得到第二接入网设备对应的 NH，进而根据第二接入网设备对应的 NH、第二接入网设备上小区的 PCI 以及载频，推演得到终端与第二接入网设备进行通信所使用的密钥。

- 45 实现 3，若终端接收到 RRC 重配置消息后，便确定多个 NCC 对应的 NH，并存储多个候选接入网设备的标识和多个 NCC 之间的对应关系，多个 NCC 和多个 NH 之间的对应关系，则在 S1009 中，终端可以根据第一 MAC 层消息所携带的第二接入网设备的标识，以及多个候选接入网设备的标识和多个 NCC 之间的对应关系，得到第二接入网设备对应的 NCC；根据第二接入网设备对应的 NCC，以及多个 NCC 和多个 NH 之间的对应关系，得到第二接入网设备对应的 NH；进而，根据第二接入网设备对应的 NH、第二接入网设备上小区的 PCI 以及载频，推演得到终端与第二接入网设备进行通信所使用的密钥。

实现 4，若终端接收到 RRC 重配置消息后，存储多个候选接入网设备的标识和多个 NCC 之间的对

应关系（并未推演 NH 和密钥），则在 S1009 中，终端可以根据第一 MAC 层消息所携带的第二接入网设备的标识，以及多个候选接入网设备的标识和多个 NCC 之间的对应关系，得到第二接入网设备对应的 NCC（即第二 NCC），进而推演第二 NCC 对应的 NH，并根据第二 NCC 对应的 NH、第二接入网设备上小区的 PCI 以及载频，推演得到终端与第二接入网设备进行通信所使用的密钥。

- 5 示例性的，终端的 MAC 层从第一 MAC 层消息中获得第二接入网设备的标识后，可以将第二接入网设备的标识传递给 RRC 层；进而，终端的 RRC 层可以根据第二接入网设备的标识获得终端与第二接入网设备进行通信所使用的密钥（比如根据上述实现 1 至实现 4 中的任一种实现获得终端与第二接入网设备进行通信所使用的密钥），进而根据该密钥，与第二接入网设备进行通信。

可选地，在终端从第一接入网设备切换到第二接入网设备之后，上述方法还包括：

- 10 S1010，第二接入网设备确定终端需要切换到的第三接入网设备为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备。

示例性的，S1010 的具体实现可以参照 S809 中的描述。

S1011，第二接入网设备向第三接入网设备发送第四候选接入网设备列表，第四候选接入网设备列表包括对于终端的连续 LTM 切换过程中还未被切换过的接入网设备的标识。

- 15 S1012，第二接入网设备向终端发送第二 MAC 层消息，第二 MAC 层消息用于触发终端切换到第三接入网设备。

可选地，响应于第二 MAC 层消息，终端可以删除第二接入网设备相关的上下文信息，比如删除第二接入网设备对应的 NCC、NH 和密钥等。

S1013，终端根据第三接入网设备构造的容器中的参数，切换到第三接入网设备。

- 20 S1014，终端根据终端与第三接入网设备进行通信的密钥，与第三接入网设备进行通信。

上述 S1005 至 S1014 的相关实现可以参照实施例四中 S804 至 S813 的描述。

可以理解的是，若终端在接收到切换命令消息后，再推演当前的目标接入网设备对应的密钥，则终端可能仅需推演多个候选接入网设备中部分候选接入网设备对应的密钥，比如终端未切换到某个候选接入网设备，则终端无需推演该候选接入网设备对应的密钥。具体参照实施例五中的描述。

- 25 采用上述方法，在切换准备过程中，多个候选接入网设备中的每个候选接入网设备都可以从 AMF 网元获得对应的 NCC，并将该 NCC 封装在容器中；进而终端可以根据候选接入网设备构造的容器中的 NCC，确定终端与候选接入网设备进行通信所使用的密钥。由于不同候选接入网设备对应的 NCC 不同，从而可以实现一跳安全。此外，由于源接入网设备可以判断目标接入网设备是否为对于终端的连续 LTM 切换过程中还未被切换过的接入网设备，若是，则可以执行 LTM 跨站切换，否则执行普通跨站切换，
30 从而可以使得终端在多个接入网设备之间来回切换时，不会出现密钥重用的问题。

基于实施例六，下面结合实施例七描述一种可能的实现流程。在实施例七中，将以实施例四中的“第一接入网设备”为接入网设备 0，“第二接入网设备”为接入网设备 1，“第三接入网设备”为接入网设备 2 为例进行描述。

- 35 实施例七

图 11 为本申请实施例提供的通信方法所对应的流程示意图。如图 11 所示，该流程可以包括：
S1101，终端通过接入网设备 0 连接到 5GC。

- 40 终端可以通过初始接入流程接入到接入网设备 0，通过接入网设备 0 接入到 5GC，完成附着。进而，终端和接入网设备 0 上分别保存密钥 KgNB（为便于描述，称为 K0）和 NCC0（K0 关联 NCC0），AMF 网元上保存 NCC0。

S1102，接入网设备 0 确定 LTM 切换的多个候选接入网设备。

可选的，接入网设备 0 可以根据 NCC0，确定 LTM 切换的候选接入网设备的最大数量 M，该最大数量小于或等于 NCC 的最大值减去 NCC0。也就是说，接入网设备 0 确定的 LTM 切换的候选接入网设备的数量应小于或等于 M，以避免后续不同接入网设备对应的 NCC 相同。

- 45 其中，接入网设备 0 可以参照 S402 中所描述的方法确定 LTM 切换的多个候选接入网设备。该流程中，以 LTM 切换的多个候选接入网设备包括接入网设备 1、接入网设备 2……接入网设备 5 为例进行描述。

S1103，接入网设备 0 向接入网设备 1 发送切换请求消息 1。相应的，接入网设备 1 接收来自接入

网设备 0 的切换请求消息 1。

S1104, 接入网设备 1 向 AMF 网元发送消息 a1, 消息 a1 用于请求接入网设备 1 对应的 NCC 和 NH; 相应的, AMF 网元接收消息 a1。

5 如果接入网设备 1 允许终端执行 LTM 切换, 则可以向 AMF 网元发送消息 a1; 否则也可以不发送消息 a1。

S1105, AMF 网元向接入网设备 1 消息 a2, 消息 a2 包括接入网设备 1 对应的 NCC 和 NH; 相应的, 接入网设备 1 接收来自 AMF 网元的消息 a2。

上述消息 a1 可以为一个专用于请求接入网设备 1 对应的 NCC 和 NH 的特定消息; 或者, 消息 a1 中包括请求信息, 请求信息用于请求接入网设备 1 对应的 NCC 和 NH。如此, AMF 网元接收到消息 a1 后, 可以将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC (称为 NCC1), 以根据更新后的 NCC 10 执行垂直推演, 得到更新后的 NH (称为 NH1)。NCC1 和 NH1 关联, 作为更新后的一对 {NH1, NCC1}。消息 a2 中可以包括接入网设备 1 对应的 NCC (即 NCC1) 和 NH (即 NH1)。

可选地, 接入网设备 1 接收到 NH1 后, 可以根据 NH1、接入网设备 1 的小区的 PCI 以及载频, 推演得到密钥 K1*, 并保存密钥 K1* (比如保存在接入网设备 1 相关的上下文信息中)。本申请实施例不限定接入网设备 1 推演密钥 K1* 的执行时间。比如, 接入网设备 1 也可以在接收到来自终端的切换完成 15 消息后, 再推演密钥 K1*。

S1106, 接入网设备 1 构造容器。

容器携带有接入网设备 1 的标识、NCC1 和配置信息, 配置信息包括用于终端切换到接入网设备 1 的参数。其中, 容器中携带的 NCC1 是接入网设备 1 从 AMF 网元获取到的 (区别于方案二中, 容器中 20 携带的 NCC 是从源接入网设备获取到的)。

S1107, 接入网设备 1 向接入网设备 0 发送切换请求确认消息 1。相应的, 接入网设备 0 接收来自接入网设备 1 的切换请求确认消息 1。

切换请求确认消息 1 包括接入网设备 1 构造的容器。

25 S1108, 接入网设备 0 向接入网设备 2 发送切换请求消息 2。相应的, 接入网设备 2 接收来自接入网设备 0 的切换请求消息 2。

S1109, 接入网设备 2 向 AMF 网元发送消息 b1, 消息 b1 用于请求接入网设备 2 对应的 NCC 和 NH; 相应的, AMF 网元接收消息 b1。

如果接入网设备 2 允许终端执行 LTM 切换, 则可以向 AMF 网元发送消息 b1; 否则也可以不发送消息 b1。

30 S1110, AMF 网元向接入网设备 2 消息 b2, 消息 b2 包括接入网设备 2 对应的 NCC 和 NH; 相应的, 接入网设备 2 接收来自 AMF 网元的消息 a2。

上述消息 b1 可以为一个专用于请求接入网设备 1 对应的 NCC 和 NH 的特定消息; 或者, 消息 b1 中包括请求信息, 请求信息用于请求接入网设备 2 对应的 NCC 和 NH。如此, AMF 网元接收到消息 b1 后, 可以将本地保存的 NCC 取值更新加 1, 得到更新后的 NCC (称为 NCC2), 以根据更新后的 NCC 35 执行垂直推演, 得到更新后的 NH (称为 NH2)。NCC2 和 NH2 关联, 作为更新后的一对 {NH2, NCC2}。消息 b2 中可以包括接入网设备 2 对应的 NCC (即 NCC2) 和 NH (即 NH2)。

可选地, 接入网设备 2 接收到 NH2 后, 可以根据 NH2、接入网设备 2 的小区的 PCI 以及载频, 推演得到密钥 K2*, 并保存密钥 K2* (比如保存在接入网设备 2 相关的上下文信息中)。本申请实施例不限定接入网设备 1 推演密钥 K1* 的执行时间。比如, 接入网设备 1 也可以在接收到来自终端的切换完成 40 消息后, 再推演密钥 K1*。

S1111, 接入网设备 2 构造容器。

容器携带有接入网设备 2 的标识、NCC2 和配置信息, 配置信息用于配置终端切换到接入网设备 2 的参数。其中, 容器中携带的 NCC2 是接入网设备 2 从 AMF 网元获取到的 (区别于方案二中, 容器中 45 携带的 NCC 是从源接入网设备获取到的)。

S1112, 接入网设备 2 向接入网设备 0 发送切换请求确认消息 2。相应的, 接入网设备 0 接收来自接入网设备 2 的切换请求确认消息 2。

切换请求确认消息 2 包括接入网设备 2 构造的容器。

可以理解的是, 上述仅描述了接入网设备 0 向接入网设备 1 和接入网设备 2 发送切换请求消息, 接

入网设备 0 还可以向其它 LTM 切换的候选接入网设备发送切换请求信息,具体实现可以参照上述 S903 至 S912,不再赘述。

S1113,接入网设备 0 向终端发送 RRC 重配置消息,该 RRC 重配置消息携带有接入网设备 1 构造的容器和接入网设备 2 构造的容器;相应地,终端接收 RRC 重配置消息。

5 终端从 RRC 重配置消息中获得 LTM 的各个候选接入网设备构造的容器(比如接入网设备 1 至接入网设备 5 构造的容器),并获得接入网设备 1 至接入网设备 5 分别对应的 NCC(比如 NCC1 至 NCC5)。终端计算各个 NCC 对应的 NH,并存储 NCC 和 NH 的对应关系。

示例性的,终端按照 NCC 升序的方式,依次推演 NCC1 至 NCC5 分别对应的 NH。比如,终端根据 NCC1 与终端本地保存的 NCC0 的差值,执行相应次数的垂直推演,得到相应的 NH(即 NH1);终端根据 NCC2 与 NCC1 的差值,执行相应次数的垂直推演,得到相应的 NH(即 NH2);终端根据 NCC3 与 NCC2 的差值,执行相应次数的垂直推演,得到相应的 NH(即 NH3);以此类推,进而得到 NCC1 至 NCC5 分别对应的 NH。

10 终端可以保存接入网设备的标识、NCC 和 NH 这三项中至少两项之间的对应关系,具体实现形式不做限定,比如终端可以包括接入网设备的标识和 NH 之间的对应关系,或者终端可以保持接入网设备的标识、NCC 和 NH 之间的对应关系。

可选地,终端可以根据 NH1、接入网设备 1 上的小区的 PCI 以及载频,推演得到密钥 $K1^*$,并保存接入网设备 1 与密钥 $K1^*$ 之间的对应关系。终端可以根据 NH2、接入网设备 2 上的小区的 PCI 以及载频,推演得到密钥 $K2^*$,并保存接入网设备 2 与密钥 $K2^*$ 之间的对应关系。以此类推,终端可以得到接入网设备 1 至接入网设备 5 分别对应的密钥。本申请实施例对终端确定 NCC1 至 NCC5 分别对应的 NH 以及接入网设备 1 至接入网设备 5 分别对应的密钥的具体时机不做限定。

20 S1114,终端向接入网设备 0 发送 RRC 重配置完成消息;相应的,接入网设备 0 接收来自终端的 RRC 重配置完成消息。

S1115 至 S1119 可以参照上述 S1011 至 S1015。

25 S1120,接入网设备 1 向 AMF 网元发送路径切换请求消息;相应地,AMF 网元接收路径切换请求消息。

可选的,路径切换请求消息可以包括指示信息,指示信息用于指示 AMF 网元无需执行 NCC 更新。对应的,AMF 网元接收所述指示信息,AMF 跳过 NCC 更新和 NH 计算过程。

S1121,AMF 网元向接入网设备 1 发送路径切换响应消息;相应地,接入网设备 1 接收路径切换响应消息,进而完成路径切换。

30 由于 AMF 网元可以根据指示信息,跳过 NCC 更新和 NH 计算过程,因此,路径切换响应消息无需包括更新的 NCC 和 NH。

此处,路径切换是指终端的数据传输路径由“UPF 网元—接入网设备 0—终端”切换为“UPF 网元—接入网设备 1—终端”。

S1122,终端与接入网设备 1 使用密钥 $K1^*$ 进行通信。

35 终端可以根据上述切换命令消息(即 MAC CE)中的接入网设备 1 的标识,获取与接入网设备 1 的标识对应的密钥 $K1^*$;而接入网设备 1 也推演得到了密钥 $K1^*$,因此,终端与接入网设备 1 可以使用密钥 $K1^*$ 进行通信。

具体来说,如果在 S1113 中,终端接收到 RRC 重配置消息,便确定出接入网设备 1 至接入网设备 5 分别对应的密钥,并保存接入网设备的标识与密钥之间的对应关系,则终端的 MAC 层接收到切换命令消息后,可以将切换命令消息中的接入网设备 1 的标识传递到 RRC 层,进而终端的 RRC 层根据接入网设备 1 的标识,得到与接入网设备 1 的标识对应的密钥 $K1^*$ 。

40 或者,如果在 S1113 中,终端接收到 RRC 重配置消息,便确定出 NCC1 至 NCC5 对应的 NH,并保存接入网设备的标识和 NH 之间的对应关系,则终端的 MAC 层接收到切换命令消息后,可以将切换命令消息中的接入网设备 1 的标识传递到 RRC 层,进而终端的 RRC 层根据接入网设备 1 的标识,得到对应的 NH,进而根据 NH、接入网设备 1 上的小区的标识以及载频,确定密钥 $K1^*$ 。

45 可以理解的是,后续终端还可以从接入网设备 1 切换到其它接入网设备(比如接入网设备 2),具体的实现可以参照终端从接入网设备 0 切换到接入网设备 1 的描述。

此外,图 11 所示意的流程与图 10 所示意的流程相对应,二者的步骤可以相互参照。比如, S1001

可以参照 S1102, S1002 和 S1003 可以参照 S1103 至 S1112, S1004 可以参照 S1113, S1005 可以参照 S1115 和 S1116, S1006 可以参照 S1117, S1007 可以参照 S1118, S1008 可以参照 S1119, S1009 可以参照 S1122。

针对于上述多个实施例, 可以理解的是:

5 (1) 在本申请的各个实施例中, 推演密钥时所涉及的“接入网设备上的小区的 PCI 以及载频”中的小区可以为接入网设备上的任一个小区, 比如接入网设备为目标接入网设备, 则该小区可以为目标小区或者目标小区以外的其它小区, 本申请实施例对此不做限定。

(2) 在本申请的各个实施例中, 如果没有特殊说明以及逻辑冲突, 不同的实施例之间的术语和/或描述具有一致性、且可以相互引用, 不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。此外, 同一实施例中, 不同实现方式或不同示例之间也可以相互引用或参照。

10 (3) 本申请中涉及的各种数字编号仅为描述方便进行的区分, 并不用来限制本申请的范围。上述各个流程图的步骤编号仅为执行流程的一种示例, 并不构成对步骤执行的先后顺序的限制, 即各步骤编号的大小并不意味着执行顺序的先后, 各步骤的执行顺序应以其功能和内在逻辑确定。此外, 各个流程图中所示意的步骤并非全部是必须执行的步骤, 可以根据实际需要在各个流程图的基础上增添或者删除部分步骤。

15

上述主要从终端和接入网设备交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是, 为了实现上述功能, 终端和接入网设备可以包括执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 本申请的实施例能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行, 取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能, 但是这种实现不应认为超出本申请的范围。

20 本申请实施例可以根据上述方法示例对终端和接入网设备进行功能单元的划分, 例如, 可以对应各个功能划分各个功能单元, 也可以将两个或两个以上的功能集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。

25 在采用集成的单元的情况下, 图 12 示出了本申请实施例中所涉及的装置的可能的示例性框图。如图 12 所示, 装置 1200 可以包括: 处理单元 1202 和通信单元 1203。处理单元 1202 用于对装置 1200 的动作进行控制管理。通信单元 1203 用于支持装置 1200 与其他设备的通信。可选地, 通信单元 1203 也称为收发单元, 可以包括接收单元和/或发送单元, 分别用于执行接收和发送操作。装置 1200 还可以包括存储单元 1201, 用于存储装置 1200 的程序代码和/或数据。

30 (1) 该装置 1200 可以为上述实施例中的第一接入网设备。处理单元 1202 可以支持装置 1200 执行上文中各方法示例中第一接入网设备的动作。或者, 处理单元 1202 主要执行方法示例中第一接入网设备的内部动作, 通信单元 1203 可以支持装置 1200 与其它设备之间的通信。

比如, 在一个实施例中, 通信单元 1203 用于: 接收来自多个候选接入网设备中每个接入网设备的容器, 所述每个接入网设备的容器包括用于终端切换到所述每个接入网设备的参数; 向所述终端发送无线资源控制 RRC 重配置消息, 所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入网设备的容器; 通信单元 1203 还用于: 在所述终端需要切换到所述多个候选接入网设备中的第二接入网设备的情况下, 向所述终端发送第一媒体接入控制 MAC 层消息, 所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一 NCC 的信息, 所述第一 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥。

40 在一种可能的设计中, 通信单元 1203 具体用于: 在所述第一接入网设备的 RRC 层将用于指示所述第一 NCC 的信息传递到所述第一接入网设备的 MAC 层后, 通过所述第一接入网设备的 MAC 层向所述终端发送所述 MAC 层消息。

在一种可能的设计中, 通信单元 1203 还用于: 接收来自移动管理网元的所述第一下一跳链路计数器 NCC, 所述第一 NCC 承载于初始上下文建立请求消息或者路径切换响应消息。

45 在一种可能的设计中, 通信单元 1203 还用于: 向所述第二接入网设备发送第一候选接入网设备列表, 所述第一候选接入网设备列表包括所述多个候选接入网设备中的至少一个候选接入网设备的标识。

(2) 该装置 1200 可以为上述实施例中的第二接入网设备。处理单元 1202 可以支持装置 1200 执行上文中各方法示例中第二接入网设备的动作。或者, 处理单元 1202 主要执行方法示例中第二接入网设

备的内部动作,通信单元 1203 可以支持装置 1200 与其它设备之间的通信。

比如,在一个实施例中,通信单元 1203 用于:发送所述第二接入网设备的容器,所述容器包括用于终端切换到所述第二接入网设备的参数;处理单元 1202 用于:在所述终端通过 LTM 切换从第一接入网设备切换到所述第二接入网设备之后,确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备;通信单元 1203 还用于:向所述终端发送第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到所述第三接入网设备的信息和用于指示第二 NCC 的信息,所述第二 NCC 用于确定所述终端与所述第三接入网设备进行通信所使用的密钥。

在一种可能的设计中,通信单元 1203 具体用于:在所述第二接入网设备的 RRC 层将用于指示所述第二 NCC 的信息传递到所述第二接入网设备的 MAC 层后,通过所述第二接入网设备的 MAC 层向所述终端发送所述第二 MAC 层消息。

在一种可能的设计中,在所述终端切换到所述第二接入网设备之后,通信单元 1203 还用于:向移动管理网元发送路径切换请求消息;接收来自所述移动管理网元的路径切换响应消息,所述路径切换响应消息包括所述第二 NCC 和所述第二 NCC 对应的下一跳 NH。

在一种可能的设计中,确定所述终端需要切换到所述第三接入网设备之后,处理单元 1202 还用于:根据所述第二 NCC 对应的 NH,确定所述第三接入网设备与所述终端进行通信所使用的密钥;通信单元 1203 还用于:向所述第三接入网设备发送所述第三接入网设备与所述终端进行通信所使用的密钥。

在一种可能的设计中,通信单元 1203 还用于:向终端设备第三 MAC 层消息,所述第三 MAC 层消息包括用于指示所述第二 NCC 的信息,所述第二 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥;处理单元 1202 还用于:根据所述第二 NCC 对应的 NH,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

在一种可能的设计中,在向终端发送所述第二接入网设备的容器之后,通信单元 1203 还用于:接收来自所述第一接入网设备的第一候选接入网设备列表,所述第一候选接入网设备列表包括所述至少一个候选接入网设备的标识;若确定所述第三接入网设备属于所述第一候选接入网设备列表后,则向所述终端发送所述第二 MAC 层消息。

在一种可能的设计中,确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备之后,通信单元 1203 还用于:向所述第三接入网设备发送第二候选接入网设备列表,所述第二候选接入网设备列表包括所述第一候选接入网设备列表中的部分或全部候选接入网设备的标识。

(3)该装置 1200 可以为上述实施例中的终端。处理单元 1202 可以支持装置 1200 执行上文中各方法示例中终端的动作。或者,处理单元 1202 主要执行方法示例中终端的内部动作,通信单元 1203 可以支持装置 1200 与其它设备之间的通信。

比如,在一个实施例中,通信单元 1203 用于:接收来自多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数,所述多个候选接入网设备包括第二接入网设备;接收来自第一接入网设备的第一 MAC 层消息,所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一 NCC 的信息;处理单元 1202 用于:根据所述第二接入网设备的容器中的参数,切换到所述第二接入网设备;根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

在一种可能的设计中,处理单元 1202 具体用于:在所述第一 NCC 与所述终端存储的 NCC 相同的情况下,根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥,所述第一输入参数包括所述第二接入网设备上的小区的信息。

在一种可能的设计中,处理单元 1202 具体用于:在所述终端的 MAC 层将用于指示所述第一 NCC 的信息传递到所述终端的 RRC 层后,通过所述终端的 RRC 层根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

在一种可能的设计中,所述多个候选接入网设备还包括第三接入网设备;在终端切换到所述第二接入网设备之后,通信单元 1203 还用于:接收来自所述第二接入网设备的第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到第三接入网设备的信息和用于指示第二 NCC 的信息;处理单元 1202 还用于:根据所述第三接入网设备的容器中的参数,切换到所述第三接入网设备;根据所述第二 NCC,确定所述终端与所述第三接入网设备进行通信所使用的密钥。

在一种可能的设计中,处理单元 1202 具体用于:在所述第二 NCC 与所述终端存储的 NCC 不同的

情况下,根据第二输入参数推演得到所述终端与所述第三接入网设备进行通信所使用的密钥,所述第二输入参数包括所述第二 NCC 对应的 NH 和所述第三接入网设备上的小区的信息。

在又一个实施例中,通信单元 1203 用于:接收来自多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数,所述多个候选接入网设备包括第二接入网设备;接收来自第一接入网设备的第一 MAC 层消息,所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息;处理单元 1202 用于:根据所述第二接入网设备的容器中的参数,切换到所述第二接入网设备;通信单元 1203 还用于:接收来自所述第二接入网设备的第三 MAC 层消息,所述第三 MAC 层消息包括用于指示第二 NCC 的信息;处理单元 1202 还用于:根据所述第二 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

在一种可能的设计中,所述第一 MAC 层消息还包括用于指示第一 NCC 的信息;处理单元 1202 还用于:根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥,并存储在接入层 AS 安全上下文中;其中,当根据所述第二 NCC,确定出所述终端与所述第二接入网设备进行通信所使用的密钥时,将所述 AS 安全上下文中的根据所述第一 NCC 确定的所述密钥更新为根据所述第二 NCC 确定的所述密钥。

在一种可能的设计中,处理单元 1202 具体用于:在所述第一 NCC 与所述终端存储的 NCC 相同的情况下,根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥,所述第一输入参数包括所述第一 NCC 对应的 KgNB 和所述第二接入网设备上的小区的信息。

在一种可能的设计中,处理单元 1202 具体用于:在所述第二 NCC 与所述终端存储的 NCC 不同的情况下,根据第三输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥,所述第三输入参数包括所述第二 NCC 对应的 NH 和所述第二接入网设备上的小区的信息。

在一种可能的设计中,处理单元 1202 具体用于:在所述第二 NCC 与所述终端存储的 NCC 不同的情况下,将所述终端存储的 NCC 更新为所述第二 NCC。

在一种可能的设计中,处理单元 1202 具体用于:在所述终端的 MAC 层将用于指示所述第二 NCC 的信息传递到所述终端的 RRC 层后,通过所述终端的 RRC 层根据所述第二 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

应理解以上装置中单元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。且装置中的单元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;还可以部分单元以软件通过处理元件调用的形式实现,部分单元以硬件的形式实现。例如,各个单元可以为单独设立的处理元件,也可以集成在装置的某一个芯片中实现,此外,也可以以程序的形式存储于存储器中,由装置的某一个处理元件调用并执行该单元的功能。此外这些单元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又可以成为处理器,可以是一种具有信号的处理能力的集成电路。在实现过程中,上述方法的各操作或以上各个单元可以通过处理器元件中的硬件的集成逻辑电路实现或者以软件通过处理元件调用的形式实现。

在一个例子中,以上任一装置中的单元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, ASIC),或,一个或多个微处理器(digital singnal processor, DSP),或,一个或者多个现场可编程门阵列(field programmable gate array, FPGA),或这些集成电路形式中至少两种的组合。再如,当装置中的单元可以通过处理元件调度程序的形式实现时,该处理元件可以是处理器,比如通用中央处理器(central processing unit, CPU),或其它可以调用程序的处理器。再如,这些单元可以集成在一起,以 SoC 的形式实现。

以上用于接收的单元是一种该装置的接口电路,用于从其它装置接收信号。例如,当该装置以芯片的方式实现时,该接收单元是该芯片用于从其它芯片或装置接收信号的接口电路。以上用于发送的单元是一种该装置的接口电路,用于向其它装置发送信号。例如,当该装置以芯片的方式实现时,该发送单元是该芯片用于向其它芯片或装置发送信号的接口电路。

基于以上实施例,本申请实施例还提供了一种通信装置,参阅图 13 所示,通信装置 1300 可以包括收发器 1301 和处理器 1302。可选的,所述通信装置 1300 中还可以包括存储器 1303。其中,所述存储器 1303 可以设置于所述通信装置 1300 内部,还可以设置于所述通信装置 1300 外部。其中,所述处理器 1302 可以控制所述收发器 1301 接收和发送消息等。

具体地,所述处理器 1302 可以是中央处理器 (central processing unit, CPU), 网络处理器 (network processor, NP) 或者 CPU 和 NP 的组合。所述处理器 1302 还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路 (application-specific integrated circuit, ASIC), 可编程逻辑器件 (programmable logic device, PLD) 或其组合。上述 PLD 可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD), 现场可编程逻辑门阵列 (field-programmable gate array, FPGA), 通用阵列逻辑 (generic array logic, GAL) 或其任意组合。

其中,所述收发器 1301、所述处理器 1302 和所述存储器 1303 之间相互连接。可选的,所述收发器 1301、所述处理器 1302 和所述存储器 1303 通过总线 1304 相互连接;所述总线 1304 可以是外设部件互连标准 (peripheral component interconnect, PCI) 总线或扩展工业标准结构 (extended industry standard architecture, EISA) 总线等。所述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 13 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。

在一种可选的实施方式中,所述存储器 1303,用于存放程序等。具体地,程序可以包括程序代码,该程序代码包括计算机操作指令。所述存储器 1303 可能包括 RAM,也可能还包括非易失性存储器 (non-volatile memory),例如一个或多个磁盘存储器。所述处理器 1302 执行所述存储器 1303 所存放的应用程序,实现上述功能,从而实现通信装置 1300 的功能。

示例性地,该通信装置 1300 可以是上述实施例中的第一接入网设备,或者也可以是上述实施例中的第二接入网设备,或者也可以是上述实施例中的终端。

在一个实施例中,所述通信装置 1300 在实现上述方法实施例中第一接入网设备的功能时,收发器 1301 可以实现上述方法实施例中的由第一接入网设备执行的收发操作;处理器 1302 可以实现上述方法实施例中由第一接入网设备执行的除收发操作以外的其他操作。具体的相关具体描述可以参见上述实施例中的相关描述,此处不再详细介绍。

在另一个实施例中,所述通信装置 1300 在实现上述方法实施例中第二接入网设备的功能时,收发器 1301 可以实现上述方法实施例中的由第二接入网设备执行的收发操作;处理器 1302 可以实现上述方法实施例中由第二接入网设备执行的除收发操作以外的其他操作。具体的相关具体描述可以参见上述实施例中的相关描述,此处不再详细介绍。

在另一个实施例中,所述通信装置 1300 在实现上述方法实施例中终端的功能时,收发器 1301 可以实现上述方法实施例中的由终端执行的收发操作;处理器 1302 可以实现上述方法实施例中由终端执行的除收发操作以外的其他操作。具体的相关具体描述可以参见上述实施例中的相关描述,此处不再详细介绍。

本申请实施例提供一种通信系统,该通信系统包括终端、第一接入网设备和第二接入网设备中的至少一项,终端用于执行上述实施例中终端侧的功能,第一接入网设备用于执行上述实施例中第一接入网设备侧的功能,第二接入网设备用于执行上述实施例中第二接入网设备侧的功能。

本申请实施例中的术语“系统”和“网络”可被互换使用。“至少一种”是指一种或者多种,“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 的情况,其中 A, B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项 (个)”或其类似表达,是指的这些项中的任意组合,包括单项 (个) 或复数项 (个) 的任意组合。例如“A, B 和 C 中的至少一个”包括 A, B, C, AB, AC, BC 或 ABC。以及,除非有特别说明,本申请实施例提及“第一”、“第二”等序数词是用于对多个对象进行区分,不用于限定多个对象的顺序、时序、优先级或者重要程度。

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

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

指定的功能的装置。

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

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

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些

10 改动和变型在内。

15

权 利 要 求

- 1.一种通信方法,其特征在于,所述方法应用于第一接入网设备或者所述第一接入网设备中的芯片,所述方法包括:
接收来自多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括用于终端
5 切换到所述每个接入网设备的参数;
向所述终端发送无线资源控制 RRC 重配置消息,所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入网设备构造的容器;
在所述终端需要切换到所述多个候选接入网设备中的第二接入网设备的情况下,向所述终端发送第一媒体接入控制 MAC 层消息,所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一下一跳链路计数器 NCC 的信息,所述第一 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥。
2.根据权利要求 1 所述的方法,其特征在于,向所述终端发送 MAC 层消息,包括:
所述第一接入网设备的 RRC 层将用于指示所述第一 NCC 的信息传递到所述第一接入网设备的 MAC 层;
15 所述第一接入网设备的 MAC 层向所述终端发送所述 MAC 层消息。
3.根据权利要求 1 或 2 所述的方法,其特征在于,所述方法还包括:
接收来自移动管理网元的所述第一 NCC;
所述第一 NCC 承载于初始上下文建立请求消息或者路径切换响应消息。
4.根据权利要求 1 至 3 中任一项所述的方法,其特征在于,所述方法还包括:
20 向所述第二接入网设备发送第一候选接入网设备列表,所述第一候选接入网设备列表包括所述多个候选接入网设备中的至少一个候选接入网设备的标识。
5.根据权利要求 1 至 4 中任一项所述的方法,其特征在于,用于指示第一 NCC 的信息包括以下至少一项:
所述第一 NCC;
25 所述第一 NCC 的索引值;
所述第一 NCC 加密后的密文。
6.一种通信方法,其特征在于,所述方法应用于第二接入网设备或者所述第二接入网设备中的芯片,所述方法包括:
向终端发送所述第二接入网设备的容器,所述容器包括用于终端切换到所述第二接入网设备的参数;
30 在所述终端通过层 1/层 2 触发的移动性 LTM 切换从第一接入网设备切换到所述第二接入网设备之后,确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备;
向所述终端发送第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到所述第三接入网设备的信息和用于指示第二 NCC 的信息,所述第二 NCC 用于确定所述终端与所述第三接入网设备进行通信所使用的密钥。
7.根据权利要求 6 所述的方法,其特征在于,向所述终端发送第二 MAC 层消息,包括:
35 所述第二接入网设备的 RRC 层将用于指示所述第二 NCC 的信息传递到所述第二接入网设备的 MAC 层;
所述第二接入网设备的 MAC 层向所述终端发送所述第二 MAC 层消息。
8.根据权利要求 6 或 7 所述的方法,其特征在于,在所述终端切换到所述第二接入网设备之后,所述方法还包括:
40 向移动管理网元发送路径切换请求消息;
接收来自所述移动管理网元的路径切换响应消息,所述路径切换响应消息包括所述第二 NCC 和所述第二 NCC 对应的下一跳 NH。
9.根据权利要求 8 所述的方法,其特征在于,确定所述终端需要切换到所述第三接入网设备之后,
45 所述方法还包括:
根据所述第二 NCC 对应的 NH,确定所述第三接入网设备与所述终端进行通信所使用的密钥;
向所述第三接入网设备发送所述第三接入网设备与所述终端进行通信所使用的密钥。

10.根据权利要求 8 所述的方法,其特征在于,所述方法还包括:

向终端设备第三 MAC 层消息,所述第三 MAC 层消息包括用于指示所述第二 NCC 的信息,所述第二 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥;

根据所述第二 NCC 对应的 NH,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

5 11.根据权利要求 6 至 10 中任一项所述的方法,其特征在于,在向终端发送所述第二接入网设备的容器之后,所述方法还包括:接收来自所述第一接入网设备的第一候选接入网设备列表,所述第一候选接入网设备列表包括所述至少一个候选接入网设备的标识;

向所述终端发送第二 MAC 层消息,包括:若确定所述第三接入网设备属于所述第一候选接入网设备列表后,则向所述终端发送所述第二 MAC 层消息。

10 12.根据权利要求 6 至 11 中任一项所述的方法,其特征在于,确定所述终端需要切换到至少一个候选接入网设备中的第三接入网设备之后,所述方法还包括:

向所述第三接入网设备发送第二候选接入网设备列表,所述第二候选接入网设备列表包括所述至少一个候选接入网设备中的部分或全部候选接入网设备的标识。

13.一种通信方法,其特征在于,所述方法应用于终端或者所述终端中的芯片,所述方法包括:

15 接收来自多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数,所述多个候选接入网设备包括第二接入网设备;

接收来自第一接入网设备的第一 MAC 层消息,所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息和用于指示第一 NCC 的信息;

根据所述第二接入网设备的容器中的参数,切换到所述第二接入网设备;

20 根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

14.根据权利要求 13 所述的方法,其特征在于,根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥,包括:

在所述第一 NCC 与所述终端存储的 NCC 相同的情况下,根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥,所述第一输入参数包括所述第一 NCC 对应的密钥 KgNB 25 和所述第二接入网设备上的小区的信息。

15.根据权利要求 13 或 14 所述的方法,其特征在于,根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥,包括:

所述终端的 MAC 层将用于指示所述第一 NCC 的信息传递到所述终端的 RRC 层;

30 所述终端的 RRC 层根据所述第一 NCC,确定所述终端与所述第二接入网设备进行通信所使用的密钥。

16.根据权利要求 13 至 15 中任一项所述的方法,其特征在于,所述多个候选接入网设备还包括第三接入网设备;

在终端切换到所述第二接入网设备之后,所述方法还包括:

35 接收来自所述第二接入网设备的第二 MAC 层消息,所述第二 MAC 层消息包括用于触发所述终端切换到第三接入网设备的信息和用于指示第二 NCC 的信息;

根据所述第三接入网设备的容器中的参数,切换到所述第三接入网设备;

根据所述第二 NCC,确定所述终端与所述第三接入网设备进行通信所使用的密钥。

17.根据权利要求 16 所述的方法,其特征在于,根据所述第二 NCC,确定所述终端与所述第三接入网设备进行通信所使用的密钥,包括:

40 在所述第二 NCC 与所述终端存储的 NCC 不同的情况下,根据第二输入参数推演得到所述终端与所述第三接入网设备进行通信所使用的密钥,所述第二输入参数包括所述第二 NCC 对应的 NH 和所述第三接入网设备上的小区的信息。

18.根据权利要求 16 或 17 所述的方法,其特征在于,所述方法还包括:

45 在所述第二 NCC 与所述终端存储的 NCC 不同的情况下,将所述终端存储的 NCC 更新为所述第二 NCC。

19.一种通信方法,其特征在于,所述方法应用于终端或者所述终端中的芯片,所述方法包括:

接收来自多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括用于所述终端切换到所述每个接入网设备的参数,所述多个候选接入网设备包括第二接入网设备;

接收来自第一接入网设备的第一 MAC 层消息, 所述第一 MAC 层消息包括用于触发所述终端切换到所述第二接入网设备的信息;

根据所述第二接入网设备的容器中的参数, 切换到所述第二接入网设备;

5 接收来自所述第二接入网设备的第三 MAC 层消息, 所述第三 MAC 层消息包括用于指示第二 NCC 的信息;

根据所述第二 NCC, 确定所述终端与所述第二接入网设备进行通信所使用的密钥。

20. 根据权利要求 19 所述的方法, 其特征在于, 所述第一 MAC 层消息还包括用于指示第一 NCC 的信息;

所述方法还包括:

10 根据所述第一 NCC, 确定所述终端与所述第二接入网设备进行通信所使用的密钥, 并存储在接入层 AS 安全上下文中;

其中, 当根据所述第二 NCC, 确定出所述终端与所述第二接入网设备进行通信所使用的密钥时, 将所述 AS 安全上下文中的根据所述第一 NCC 确定的所述密钥更新为根据所述第二 NCC 确定的所述密钥。

15 21. 根据权利要求 20 所述的方法, 其特征在于, 根据所述第一 NCC, 确定所述终端与所述第二接入网设备进行通信所使用的密钥, 包括:

在所述第一 NCC 与所述终端存储的 NCC 相同的情况下, 根据第一输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥, 所述第一输入参数包括所述第一 NCC 对应的密钥 KgNB 和所述第二接入网设备上的小区的信息。

20 22. 根据权利要求 19 至 21 中任一项所述的方法, 其特征在于, 根据所述第二 NCC, 确定所述终端与所述第三接入网设备进行通信所使用的密钥, 包括:

在所述第二 NCC 与所述终端存储的 NCC 不同的情况下, 根据第三输入参数推演得到所述终端与所述第二接入网设备进行通信所使用的密钥, 所述第三输入参数包括所述第二 NCC 对应的 NH 和所述第二接入网设备上的小区的信息。

25 23. 根据权利要求 19 至 22 中任一项所述的方法, 其特征在于, 所述方法还包括:

在所述第二 NCC 与所述终端存储的 NCC 不同的情况下, 将所述终端存储的 NCC 更新为所述第二 NCC。

24. 根据权利要求 19 至 23 中任一项所述的方法, 其特征在于, 根据所述第二 NCC, 确定所述终端与所述第二接入网设备进行通信所使用的密钥, 包括:

30 所述终端的 MAC 层将用于指示所述第二 NCC 的信息传递到所述终端的 RRC 层;

所述终端的 RRC 层根据所述第二 NCC, 确定所述终端与所述第二接入网设备进行通信所使用的密钥。

25. 根据权利要求 19 至 24 中任一项所述的方法, 其特征在于, 所述多个候选接入网设备还包括第三接入网设备;

35 在所述终端切换到所述第二接入网设备之后, 所述方法还包括:

接收来自所述第二接入网设备的第二 MAC 层消息, 所述第二 MAC 层消息包括用于触发所述终端切换到第三接入网设备的信息;

根据所述第三接入网设备的容器中的参数, 切换到所述第三接入网设备;

40 接收来自所述第三接入网设备的第四 MAC 层消息, 所述第四 MAC 层消息包括用于指示第三 NCC 的信息;

根据所述第三 NCC, 确定所述终端与所述第三接入网设备进行通信所使用的密钥。

26. 根据权利要求 25 所述的方法, 其特征在于, 所述第二 MAC 层消息还包括用于指示所述第二 NCC 的信息;

所述方法还包括:

45 根据所述第二 NCC, 确定所述终端向所述第三接入网设备发送切换完成消息所使用的密钥, 并存储在 AS 安全上下文中;

其中, 当根据所述第三 NCC, 确定出所述终端与所述第三接入网设备进行通信所使用的密钥时, 将所述 AS 安全上下文中的根据所述第二 NCC 确定的所述密钥更新为根据所述第三 NCC 确定的所述密

钥。

27.一种通信方法,其特征在于,所述方法应用于第一接入网设备或者所述第一接入网设备中的芯片,所述方法包括:

5 向多个候选接入网设备中每个接入网设备发送切换请求消息,所述切换请求消息包括第一 NCC;
接收来自所述多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括所述
第一 NCC;

向所述终端发送 RRC 重配置消息,所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入
网设备的容器;

10 确定所述终端需要切换到的第二接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过
的接入网设备,所述多个候选接入网设备包括第二接入网设备;

向所述终端发送第一 MAC 层消息,所述第一 MAC 层消息用于触发终端切换到所述第二接入网
设备。

28.根据权利要求 27 所述的方法,其特征在于,所述方法还包括:

15 接收来自移动管理网元的所述第一 NCC,所述第一 NCC 承载于初始上下文建立请求消息或者路
径切换响应消息。

29.根据权利要求 27 或 28 所述的方法,其特征在于,所述方法还包括:

向所述第二接入网设备发送 LTM 连续切换次数。

30.根据权利要求 27 至 29 中任一项所述的方法,其特征在于,所述方法还包括:

20 向所述第二接入网设备发送第三候选接入网设备列表,所述第三候选接入网设备列表包括至少一个
候选接入网设备的标识。

31.一种通信方法,其特征在于,所述方法应用于第二接入网设备或者所述第二接入网设备中的芯
片,所述方法包括:

接收来自第一接入网设备的切换请求消息,所述切换请求消息包括第一 NCC;

25 向所述第一接入网设备发送所述第二接入网设备的容器,所述容器包括所述第一 NCC 和用于终端
切换到所述第二接入网设备的参数;所述容器中包括的所述第一 NCC 用于确定所述终端与所述第二接
入网设备进行通信所使用的密钥;

在所述终端切换到所述第二接入网设备后,确定终端需要切换到的第三接入网设备为对于所述终端
的连续 LTM 切换过程中还未被切换过的接入网设备;

30 向所述终端发送第二 MAC 层消息,所述第二 MAC 层消息用于触发终端切换到所述第三接入网
设备。

32.根据权利要求 31 所述的方法,其特征在于,在所述终端切换到所述第二接入网设备后,所述方
法还包括:

接收来自移动管理网元的第二 NCC,所述第二 NCC 承载于路径切换响应消息;

35 向所述终端发送第二 MAC 层消息,包括:

若所述第二 NCC 的取值不属于预设值,则向所述终端发送第二 MAC 层消息。

33.根据权利要求 31 或 32 所述的方法,其特征在于,所述方法还包括:

接收来自第一接入网设备的 LTM 连续切换次数;

向所述终端发送第二 MAC 层消息,包括:

若所述 LTM 连续切换次数小于或等于阈值,则向所述终端发送第二 MAC 层消息。

40 34.根据权利要求 31 至 33 中任一项所述的方法,其特征在于,在所述终端切换到所述第二接入网
设备之前,所述方法还包括:

接收来自所述第一接入网设备的第三候选接入网设备列表,所述第三候选接入网设备列表包括至少
一个候选接入网设备的标识;

45 确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接
入网设备,包括:

若所述第三接入网设备属于所述第三候选接入网设备列表,则确定所述第三接入网设备为对于所述
终端的连续 LTM 切换过程中还未被切换过的接入网设备。

35.根据权利要求 31 至 34 中任一项所述的方法,其特征在于,所述方法还包括:

向所述第三接入网设备发送第四候选接入网设备列表,所述第四候选接入网设备列表不包括第二接入网设备的标识。

36.一种通信方法,其特征在于,所述方法应用于终端或者所述终端中的芯片,所述方法包括:

接收来自第一接入网设备的 RRC 重配置消息,所述 RRC 重配置消息包括多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括第一 NCC,所述多个候选接入网设备包括第二接入网设备;

接收来自所述第一接入网设备的第一 MAC 层消息,所述第一 MAC 层消息用于触发所述终端切换到所述第二接入网设备;

在所述终端切换到所述第二接入网设备之后,使用所述第二接入网设备对应的密钥与所述第二接入网设备进行通信,所述第二接入网设备对应的密钥是根据所述第一 NCC 确定的。

37.根据权利要求 36 所述的方法,其特征在于,所述方法还包括:

在所述第一 NCC 与所述终端存储的 NCC 相同的情况下,根据第一输入参数推演得到所述第二接入网设备对应的密钥,所述第一输入参数包括所述第二接入网设备上的小区的信息。

38.一种通信方法,其特征在于,所述方法应用于第一接入网设备或者所述第一接入网设备中的芯片,所述方法包括:

向多个候选接入网设备分别发送切换请求消息;

接收来自所述多个候选接入网设备中每个接入网设备的容器,所述每个接入网设备的容器包括所述每个接入网设备对应的 NCC;所述每个接入网设备对应的 NCC 用于确定终端与所述每个接入网设备进行通信所使用的密钥;

向所述终端发送 RRC 重配置消息,所述 RRC 重配置消息包括所述多个候选接入网设备中每个接入网设备的容器;其中,所述每个接入网设备对应的 NCC 不同。

39.根据权利要求 38 所述的方法,其特征在于,所述方法还包括:

确定所述多个候选接入网设备,所述多个候选接入网设备的个数小于或等于阈值,所述阈值是根据所述第一接入网设备对应的 NCC 确定的。

40.根据权利要求 38 或 39 所述的方法,其特征在于,所述方法还包括:

确定所述终端需要切换到的第二接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备;

向所述终端发送第一 MAC 层消息,所述第一 MAC 层消息用于触发终端切换到所述第二接入网设备。

41.根据权利要求 40 所述的方法,其特征在于,所述方法还包括:

向所述第二接入网设备发送第三候选接入网设备列表,所述第三候选接入网设备列表包括至少一个候选接入网设备的标识。

42.一种通信方法,其特征在于,所述方法应用于第二接入网设备或者所述第二接入网设备中的芯片,所述方法包括:

接收来自第一接入网设备的切换请求消息;

在接收所述切换请求消息之后,向移动管理网元发送请求消息,所述请求消息用于请求所述第二接入网设备对应的 NCC;

接收来自所述核心网设备的所述 NCC;

向所述第一接入网设备发送切换请求确认消息,所述切换请求确认消息包括所述第二接入网设备的容器,所述容器包括所述 NCC,所述 NCC 用于确定所述终端与所述第二接入网设备进行通信所使用的密钥。

43.根据权利要求 42 所述的方法,其特征在于,所述切换请求消息包括指示信息,所述指示信息用于指示所述切换请求消息对应 LTM 切换。

44.根据权利要求 42 或 43 所述的方法,其特征在于,所述方法还包括:

接收来自所述核心网设备的所述 NCC 对应的 NH;

根据所述 NCC 对应的 NH,确定与所述终端进行通信所使用的密钥。

45.根据权利要求 42 至 44 中任一项所述的方法,其特征在于,在所述终端从第一接入网设备切换到所述第二接入网设备之后,所述方法还包括:

确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备；

向所述终端发送第二 MAC 层消息，所述第二 MAC 层消息用于触发终端切换到所述第三接入网设备。

- 5 46.根据权利要求 45 所述的方法，其特征在于，在所述终端从第一接入网设备切换到所述第二接入网设备之前，所述方法还包括：

接收来自所述第一接入网设备的第三候选接入网设备列表；

确定终端需要切换到的第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备，包括：

- 10 若所述第三接入网设备属于所述第三候选接入网设备列表，则确定所述第三接入网设备为对于所述终端的连续 LTM 切换过程中还未被切换过的接入网设备。

47.根据权利要求 45 或 46 所述的方法，其特征在于，所述方法还包括：

向所述第三接入网设备发送第二候选接入网设备列表，所述第二候选接入网设备列表不包括所述第二接入网设备的标识。

- 15 48.一种通信方法，其特征在于，所述方法应用于终端或者所述终端中的芯片，所述方法包括：

接收来自第一接入网设备的 RRC 重配置消息，所述 RRC 重配置消息包括多个候选接入网设备的标识和多个 NCC 的对应关系；

根据所述多个候选接入网设备对应的 NCC，确定所述多个候选接入网设备对应的密钥；其中，所述多个候选接入网设备中不同接入网设备对应的 NCC 不同；

- 20 接收来自所述第一接入网设备的第一 MAC 层消息，所述第一 MAC 层消息用于触发所述终端切换到所述第二接入网设备，所述多个候选接入网设备包括第二接入网设备；

在所述终端切换到所述第二接入网设备之后，使用所述第二接入网设备对应的密钥，与所述第二接入网设备进行通信。

- 25 49.根据权利要求 48 所述的方法，其特征在于，根据所述第二接入网设备对应的 NCC，确定所述第二接入网设备对应的密钥，包括：

根据第二输入参数，推演得到所述第二接入网设备对应的密钥；所述第二输入参数包括所述第二接入网设备对应的 NCC 所对应的 NH 和所述第二接入网设备上的小区的信息。

50.根据权利要求 48 或 49 所述的方法，其特征在于，所述方法还包括：

根据所述多个 NCC，按照 NCC 升序的方式依次推演所述多个 NCC 对应的 NH。

- 30 51.根据权利要求 48 至 50 中任一项所述的方法，其特征在于，所述多个候选接入网设备还包括第三接入网设备；所述方法还包括：

接收来自所述第二接入网设备的第二 MAC 层消息，所述第二 MAC 层消息用于触发所述终端切换到所述第三接入网设备；

- 35 在所述终端切换到所述第三接入网设备之后，使用所述第三接入网设备对应的密钥，与所述第三接入网设备进行通信。

52.根据权利要求 51 所述的方法，其特征在于，所述方法还包括：

响应于所述第二 MAC 层消息，删除所述第二接入网设备对应的 NCC。

- 40 53.一种通信系统，其特征在于，所述通信系统包括第一接入网设备和第二接入网设备；其中，所述第一接入网设备用于执行上述权利要求 1 至 5 中任一项所述的方法，所述第二接入网设备用于执行上述权利要求 6 至 12 中任一项所述的方法。

54.根据权利要求 53 所述的系统，其特征在于，所述通信系统还包括终端，所述终端用于执行上述权利要求 13 至 18 中任一项所述的方法，或用于执行上述权利要求 19 至 26 中任一项所述的方法。

- 45 55.一种通信系统，其特征在于，所述通信系统包括第一接入网设备和第二接入网设备；其中，所述第一接入网设备用于执行上述权利要求 27 至 30 中任一项所述的方法，所述第二接入网设备用于执行上述权利要求 31 至 35 中任一项所述的方法。

56.根据权利要求 55 所述的系统，其特征在于，所述通信系统还包括终端，所述终端用于执行上述权利要求 36 或 37 所述的方法。

57.一种通信系统，其特征在于，所述通信系统包括第一接入网设备和第二接入网设备；其中，所

述第一接入网设备用于执行上述权利要求 38 至 41 中任一项所述的方法,所述第二接入网设备用于执行上述权利要求 42 至 47 中任一项所述的方法。

58.根据权利要求 57 所述的系统,其特征在于,所述终端用于执行上述权利要求 48 至 52 中任一项所述的方法。

5 59.一种通信装置,其特征在于,包括用于执行如权利要求 1 至 52 中任一项所述方法的一个或多个功能模块。

60.一种通信装置,其特征在于,包括处理器,所述处理器和存储器耦合,所述存储器中存储有计算机程序;所述处理器用于调用所述存储器中的部分或全部所述计算机程序,使得如权利要求 1 至 52 中任一所述的方法被执行。

10 61.一种计算机可读存储介质,其特征在于,所述存储介质中存储有计算机程序,当部分或全部所述计算机程序被计算机执行时,使得如权利要求 1 至 52 中任一所述的方法被执行。

62.一种计算机程序产品,其特征在于,当计算机读取并执行所述计算机程序产品时,使得如权利要求 1 至 52 中任一所述的方法被执行。

15