

# 一种安全保护的方法及装置

本申请要求于 2017 年 11 月 17 日提交中国国家知识产权局、申请号为 201711148926.5、申请名称为“一种安全保护的方法及装置”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。

## 技术领域

本申请的实施例涉及无线通信技术领域，尤其涉及一种安全保护的方法及装置。

## 背景技术

在第五代（5th generation, 5G）系统中，终端可以只通过第三代合作伙伴计划（3rd generation partnership project, 3GPP）接入技术接入移动性管理功能（access and mobility management function, AMF）节点，也可以只通过非 3GPP（non-3GPP）接入技术接入 AMF 节点，或者终端还可以同时通过 3GPP 接入技术和 non-3GPP 接入技术接入 AMF 节点。在终端同时通过 3GPP 接入技术和 non-3GPP 接入技术接入 AMF 节点的情况下，终端与 AMF 节点之间同时存在两条非接入层（non access stratum, NAS）连接链路。如果终端使用一套 NAS 密钥和一套非接入层序列号（non access stratum count, NAS count）分别对两条连接链路进行保护，会出现 AMF 节点先接收到通过其中一条链路传输的较小的 NAS count，后接收到通过另一条链路传输的较大的 NAS count 的情况，从而发生重放攻击，导致终端与 AMF 节点之间的 NAS 连接链路传输的数据安全性较差的问题。所以终端与 AMF 之间存在多条 NAS 连接链路的情况下，如何对多条 NAS 连接链路进行安全保护是一个亟待解决的问题。

## 发明内容

本申请的实施例提供一种安全保护的方法及装置，可以实现对多条 NAS 连接链路进行安全保护。

为了达到上述目的，本申请的实施例提供以下技术方案：

本申请的实施例提供一种安全保护的方法，该方法包括：终端确定第一参数，然后根据第一参数、NAS 密钥以及传输 NAS 消息所使用的接入技术对应的 NAS 序列号对 NAS 消息进行安全保护。其中，第一参数是终端在为 NAS 消息进行安全保护的时的输入参数，用于表示传输非接入层 NAS 消息所使用的接入技术，终端能够支持至少两种接入技术，且能够分别为所述至少两种接入技术中的每种接入技术维护对应的 NAS 序列号。

示例性地，终端支持的至少两种接入技术可以包括 3GPP 接入技术、非 3GPP 接入技术、固网接入技术等其他可以与 3GPP 接入技术共同使用 3GPP 网络核心网设备的接入技术

可选地，第一参数还可以用于表示终端传输 NAS 消息所使用的传输路径，终端能够分别为传输 NAS 消息所使用的每条传输路径维护对应的 NAS 序列号。

第一参数可以为加解密或完整性保护过程中新增的一个输入参数，例如接入

(ACCESS) 参数, 可以通过将 ACCESS 参数的比特位设置成不同的值来表示不同的接入技术。示例性地, 若第一参数为 00, 则代表使用的是 3GPP 接入技术, 若第一参数为 01, 则代表使用的是非 3GPP 接入技术。或者, 第一参数还可以为输入参数中的 COUNT 的全部或部分比特位。或者, 第一参数还可以为输入参数中的 BEARER 的全部或部分比特位。

所述 NAS 密钥为终端支持的至少两种接入技术共享的 NAS 密钥。

采用该方法, 终端能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号, 终端在使用不同的接入技术传输 NAS 消息时, 不是共用一套 NAS 序列号, 而是使用为对应的接入技术维护的 NAS 序列号对 NAS 消息进行安全保护, 可以避免核心网设备先接收到通过其中一条链路传输的较小的 NAS 序列号, 后接收到通过另一条链路传输的较大的 NAS 序列号的情况下, 发生重放攻击的问题, 而且本申请在对 NAS 消息进行安全保护时, 还使用了用于区分不同接入技术的第一参数, 所以即使对通过不同的接入技术传输的 NAS 消息进行安全保护时使用的 NAS 密钥和 NAS 序列号均相同, 对 NAS 消息进行安全保护的结果也不同, 降低了发生重放攻击的可能性, 实现了对多条 NAS 连接链路的安全保护。

在一种可能的设计中, 至少两种接入技术包括第一接入技术, 若传输 NAS 消息所使用的接入技术为第一接入技术, 则在终端确定第一参数之前, 终端可确定第一接入技术对应的第一上行 NAS 序列号, 然后终端向核心网设备发送第一消息, 第一消息通过第一上行 NAS 序列号和 NAS 密钥进行安全保护, 第一消息携带第一上行 NAS 序列号的部分或全部。

示例性地, 第一接入技术可以为非 3GPP 接入技术。

在一种可能的实施方式中, 第一上行 NAS 序列号为 0, 其中, 第一上行 NAS 序列号的部分或全部为 0。或者, 第一上行 NAS 序列号为随机数, 具体地, 第一上行 NAS 序列号中的部分或全部比特位为随机数, 例如, 第一上行 NAS 序列号中的序列号部分, 或 NAS overflow 部分为随机数。此时, 其余部分为 0。或者, 至少两种接入技术还包括第二接入技术, 第一上行 NAS 序列号为终端保存的第二接入技术对应的上行 NAS 序列号, 若终端保存了至第二接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号。或者, 至少两种接入技术还包括第二接入技术, 第一上行 NAS 序列号为终端保存的第二接入技术对应的上行 NAS 序列号加 1, 若终端保存了第二接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号加 1。或者, 第一上行 NAS 序列号为终端保存的第一接入技术对应的上行 NAS 序列号, 若终端保存了第一接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号。或者, 第一上行 NAS 序列号为终端保存的第一接入技术对应的上行 NAS 序列号加 1, 若终端保存了第一接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号加 1。

在另一种可能的设计中, 至少两种接入技术包括第一接入技术和第二接入技术, 若传输 NAS 消息所使用的接入技术为第一接入技术, 则在终端确定第一参数之前, 终

端可以向核心网设备发送第一消息,第一消息通过 NAS 密钥和第二接入技术对应的上行 NAS 序列号进行安全保护,第一消息携带第二接入技术对应的上行 NAS 序列号的部分或全部。

其中,第二接入技术为 3GPP 接入技术。可选地,这种设计实现的前提为终端已经通过 3GPP 接入技术接入过核心网设备。

在一种可能的设计中,第一消息可以携带第一指示信息,第一指示信息用于指示第一消息中携带的上行 NAS 序列号的部分或全部对应的接入技术。可选地,第一指示信息还可以用于指示第一消息携带的上行 NAS 序列号的部分或全部对应的传输路径。

在一种可能的设计中,终端接收来自核心网设备的第二消息,第二消息包括第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

可选地,第二消息可以包括第一接入技术对应的第一下行 NAS 序列号。或者,第二消息包括第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号。

可选地,第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号相同。

在一种可能的实施方式中,第二上行 NAS 序列号为 0,其中,第二上行 NAS 序列号的所有或部分比特为 0。或者,第二上行 NAS 序列号为随机数,具体地,第二上行 NAS 序列号中的部分或全部比特位为随机数。例如,第二上行 NAS 序列号中的序列号部分,或 NAS overflow 部分为随机数。此时,其余部分为 0。或者,第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号,若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号,则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者,第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1,若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号,则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者,第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1,若核心网设备保存了第一接入技术对应的至少两个下行 NAS 序列号,则第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。或者,第二上行 NAS 序列号为第一上行 NAS 序列号。或者,第二上行 NAS 序列号为第一上行 NAS 序列号加 1。

在一种可能的设计中,第一下行 NAS 序列号为 0,其中,第一下行 NAS 序列号的所有或部分比特位为 0。或者,第一下行 NAS 序列号为随机数,具体地,第一下行 NAS 序列号中的部分或全部比特位为随机数。例如,第一下行 NAS 序列号中的序列号部分,或 NAS overflow 部分为随机数。此时,其余部分为 0。或者,第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的下行 NAS 序列号,若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号,则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者,第一下行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1,若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号,则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者,第一下行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1,若核心网

设备保存了第一接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。

- 5 在一种可能的设计中，第二消息携带第二指示信息，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的接入技术，可选地，第二消息中还可以携带用于指示第二消息中携带的第二上行 NAS 序列号的指示信息。

可选地，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的传输路径，可选地，第二消息中还可以携带用于指示第二消息中携带的第二上行 NAS 序列号对应的传输路径的指示信息。

第二方面，本申请的实施例提供一种安全保护的方法，该方法包括：

- 10 核心网设备确定第一参数，然后核心网设备根据第一参数、NAS 密钥以及传输 NAS 消息所使用的接入技术对应的 NAS 序列号对 NAS 消息进行安全保护。其中，第一参数用于表示传输非接入层 NAS 消息所使用的接入技术，核心网设备能够分别为终端支持的至少两种接入技术中的每种接入技术维护对应的 NAS 序列号。

- 15 示例性地，终端支持的至少两种接入技术可以包括 3GPP 接入技术、非 3GPP 接入技术、固网接入技术等其他可以与 3GPP 接入技术共同使用 3GPP 网络核心网设备的接入技术

可选地，第一参数还可以用于表示核心网设备传输 NAS 消息所使用的传输路径，核心网设备能够分别为传输 NAS 消息所使用的每条传输路径维护对应的 NAS 序列号。

- 20 第一参数可以为加解密或完整性保护过程中新增的一个输入参数，例如接入（ACCESS）参数，可以通过将 ACCESS 参数的比特位设置成不同的值来表示不同的接入技术。示例性地，若第一参数为 00，则代表使用的是 3GPP 接入技术，若第一参数为 01，则代表使用的是非 3GPP 接入技术。或者，第一参数还可以为输入参数中的 COUNT 的全部或部分比特位。或者，第一参数还可以为输入参数中的 BEARER 的全部或部分比特位。

- 25 所述 NAS 密钥为终端支持的至少两种接入技术共享的 NAS 密钥。

- 采用该方法，核心网设备能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号，核心网设备在使用不同的接入技术传输 NAS 消息时，不是共用一套 NAS 序列号，而是使用为对应的接入技术维护的 NAS 序列号对 NAS 消息进行安全保护，可以避免终端先接收到通过其中一条链路传输的较小的 NAS 序列号，后接收到通过另一条链路传输的较大的 NAS 序列号的情况下，发生重放攻击的问题，而且本申请在对 NAS 消息进行安全保护时，还使用了用于区分不同接入技术的第一参数，所以即使对通过不同的接入技术传输的 NAS 消息进行安全保护时使用的 NAS 密钥和 NAS 序列号均相同，对 NAS 消息进行安全保护的结果也不同，降低了发生重放攻击的可能性，实现了对多条 NAS 连接链路的安全保护。

- 35 在一种可能的设计中，至少两种接入技术包括第一接入技术，若传输 NAS 消息所使用的接入技术为第一接入技术，则在核心网设备确定第一参数之前，核心网设备可以接收第一消息，第一消息通过 NAS 密钥和第一接入技术对应的第一上行 NAS 序列号进行安全保护，第一消息携带第一上行 NAS 序列号。

示例性地，第一接入技术可以为非 3GPP 接入技术。

在一种可能的实施方式中，第一上行 NAS 序列号为 0，其中，第一上行 NAS 序列号的部分或全部为 0。或者，第一上行 NAS 序列号为随机数，具体地，第一上行 NAS 序列号中的部分或全部比特位为随机数。例如，第一上行 NAS 序列号中的序列号部分，或 NAS overflow 部分为随机数。此时，其余部分为 0。或者，至少两种接入技术还包括第二接入技术，第一上行 NAS 序列号为终端保存的第二接入技术对应的上行 NAS 序列号，若终端保存了至第二接入技术对应的至少两个上行 NAS 序列号，则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号。或者，至少两种接入技术还包括第二接入技术，第一上行 NAS 序列号为终端保存的第二接入技术对应的上行 NAS 序列号加 1，若终端保存了第二接入技术对应的至少两个上行 NAS 序列号，则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号加 1。或者，第一上行 NAS 序列号为终端保存的第一接入技术对应的上行 NAS 序列号，若终端保存了第一接入技术对应的至少两个上行 NAS 序列号，则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号。或者，第一上行 NAS 序列号为终端保存的第一接入技术对应的上行 NAS 序列号加 1，若终端保存了第一接入技术对应的至少两个上行 NAS 序列号，则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号加 1。

在另一种可能的设计中，至少两种接入技术包括第一接入技术和第二接入技术，若传输 NAS 消息所使用的接入技术为第一接入技术，则在核心网设备确定第一参数之前，核心网设备可以接收第一消息，第一消息通过 NAS 密钥和第二接入技术对应的上行 NAS 序列号进行安全保护，第一消息携带第二接入技术对应的上行 NAS 序列号的部分或全部。

其中，第二接入技术为 3GPP 接入技术。可选地，这种设计实现的前提为终端已经通过 3GPP 接入技术接入过核心网设备。

在一种可能的设计中，第一消息携带第一指示信息，第一指示信息用于指示第一消息携带的上行 NAS 序列号的部分或全部对应的接入技术。可选地，第一指示信息还可以用于指示第一消息携带的上行 NAS 序列号的部分或全部对应的传输路径。

在一种可能的设计中，在核心网设备接收来自终端的第一消息之后，核心网设备根据第一指示信息指示的接入技术对应的上行 NAS 序列号，对第一消息携带的 NAS 序列号的部分或全部进行验证。

采用本申请的实施例，核心网设备可独立维护 3GPP 接入技术的 NAS 序列号和非 3GPP 接入技术的 NAS 序列号，进而可根据自身维护的上行 NAS 序列号对接收到的上行 NAS 序列号进行验证，降低了出现重放攻击的可能性。

在一种可能的设计中，核心网设备确定第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部，然后核心网设备向终端发送第二消息，第二消息包括第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

可选地，第二消息可以包括第一接入技术对应的第一下行 NAS 序列号。或者，第二消息包括第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号。

可选地，第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号相同。

在一种可能的实施方式中，第二上行 NAS 序列号为 0，其中，第二上行 NAS 序

列号的所有或部分比特为 0。或者，第二上行 NAS 序列号为随机数，具体地，第二上行 NAS 序列号中的部分或全部比特位为随机数。例如，第二上行 NAS 序列号中的序列号部分，或 NAS overflow 部分为随机数。此时，其余部分为 0。或者，第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者，第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者，第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第一接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。或者，第二上行 NAS 序列号为第一上行 NAS 序列号。或者，第二上行 NAS 序列号为第一上行 NAS 序列号加 1。

15 在一种可能的实施方式中，第一下行 NAS 序列号为 0，其中，第一下行 NAS 序列号的所有或部分比特位为 0。或者，第一下行 NAS 序列号为随机数，具体地，第一下行 NAS 序列号中的部分或全部比特位为随机数。例如，第一下行 NAS 序列号中的序列号部分，或 NAS overflow 部分为随机数。此时，其余部分为 0。或者，第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的下行 NAS 序列号，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者，第一下行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者，第一下行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第一接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。

25 在一种可能的设计中，第二消息携带第二指示信息，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的接入技术，可选地，第二消息中还可以携带用于指示第二消息中携带的第二上行 NAS 序列号的指示信息。

30 可选地，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的传输路径，可选地，第二消息中还可以携带用于指示第二消息中携带的第二上行 NAS 序列号对应的传输路径的指示信息。

35 第三方面，本申请实施例提供一种装置，该装置具有实现上述方法设计中终端行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。例如，该装置可以为终端，或者可以为终端中的芯片。

在一种可能的设计中，该装置为终端，终端包括处理器，所述处理器被配置为支持终端执行上述方法中相应的功能。进一步地，终端还可以包括发射器和接收器，所

述发射器和接收器用于支持终端与核心网设备之间的通信。进一步的，终端还可以包括存储器，所述存储器用于与处理器耦合，其保存终端必要的程序指令和数据。

第四方面，本申请实施例提供一种装置，该装置具有实现上述方法设计中核心网设备行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。

- 5 所述硬件或软件包括一个或多个与上述功能相对应的模块。例如，该装置可以为核心网设备，或者可以为核心网设备中的芯片。

在一种可能的设计中，该装置为核心网设备，核心网设备包括处理器，所述处理器被配置为支持核心网设备执行上述方法中相应的功能。进一步地，核心网设备还可以包括发射器和接收器，所述发射器和接收器用于支持核心网设备与终端之间的通信。  
10 进一步的，核心网设备还可以包括存储器，所述存储器用于与处理器耦合，其保存终端必要的程序指令和数据。

第五方面，本申请实施例提供一种通信系统，该系统包括上述方面所述的终端和核心网设备，可选地，该系统还可以包括基站、N3IWF节点以及上述方面所述的终端和核心网设备。

- 15 第六方面，本申请实施例提供一种计算机存储介质，用于储存为上述用于终端所用的计算机软件指令，其包含用于执行上述第一方面所设计的程序。

第七方面，本申请实施例提供一种计算机存储介质，用于储存为上述用于核心网设备所用的计算机软件指令，其包含用于执行上述第二方面所设计的程序。

- 20 第八方面，本申请的实施例提供一种包括指令的计算机程序产品，当其在计算机上运行时，使得计算机执行如上述第一方面所述的方法。

第九方面，本申请的实施例提供一种包括指令的计算机程序产品，当其在计算机上运行时，使得计算机执行如上述第二方面所述的方法。

- 25 第十方面，本申请的实施例提供一种芯片系统，应用于终端中，所述芯片系统包括至少一个处理器，存储器和收发电路，所述存储器、所述收发电路和所述至少一个处理器通过线路互联，所述至少一个存储器中存储有指令；所述指令被所述处理器执行，以执行上述第一方面所述的方法中所述终端的操作。

- 30 第十一方面，本申请的实施例提供一种芯片系统，应用于核心网设备中，所述芯片系统包括至少一个处理器，存储器和收发电路，所述存储器、所述收发电路和所述至少一个处理器通过线路互联，所述至少一个存储器中存储有指令；所述指令被所述处理器执行，以执行上述第二方面所述的方法中所述核心网设备的操作。

- 本申请实施例提供的安全保护的方法，终端能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号，终端在使用不同的接入技术传输 NAS 消息时，不是共用一套 NAS 序列号，而是使用为对应的接入技术维护的 NAS 序列号对 NAS 消息进行安全保护，可以避免核心网设备先接收到通过其中一条链路传输的较小的 NAS 序列号，后接收到通过另一条链路传输的较大的 NAS 序列号的情况下，发生重放攻击的问题，而且本申请在对 NAS 消息进行安全保护时，还使用了用于区分不同接入技术的第一参数，所以即使对通过不同的接入技术传输的 NAS 消息进行安全保护时使用的 NAS 密钥和 NAS 序列号均相同，对 NAS 消息进行安全保护的结果也不同，降低了发生重放攻击的可能性，实现了对多条 NAS 连接链路的安全保护。
- 35

## 附图说明

- 图 1 为本申请的实施例提供的一种可能的网络架构示意图；  
图 2 为本申请的实施例提供的另一种可能的网络架构示意图；  
图 3 为本申请的实施例提供的一种加密和解密的方法的示例性示意图；  
5 图 4 为本申请的实施例提供的一种完整性保护的方法的示例性示意图；  
图 5 为本申请的实施例提供的一种安全保护的方法的流程图；  
图 6 为本申请的实施例提供的另一种加密和解密的方法的示例性示意图；  
图 7 为本申请的实施例提供的又一种加密和解密的方法的示例性示意图；  
图 8 为本申请的实施例提供的再一种加密和解密的方法的示例性示意图；  
10 图 9 为本申请的实施例提供的另一种安全保护的方法的流程图；  
图 10 为本申请的实施例提供的又一种安全保护的方法的流程图；  
图 11 为本申请的实施例提供的再一种安全保护的方法的流程图；  
图 12 为本申请的实施例提供的一种装置的结构示意图；  
图 13 为本申请的实施例提供的一种终端的结构示意图；  
15 图 14 为本申请的实施例提供的另一种装置的结构示意图；  
图 15 为本申请的实施例提供的一种核心网设备的结构示意图。

## 具体实施方式

- 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。其中，在本申请的描述中，除非另有说明，  
20 “多个”的含义是两个或两个以上。

本申请描述的系统架构及业务场景是为了更加清楚的说明本申请的技术方案，并不构成对于本申请提供的技术方案的限定，本领域普通技术人员可知，随着系统架构的演变和新业务场景的出现，本申请提供的技术方案对于类似的技术问题，同样适用。

- 需要说明的是，本申请中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。  
25

本申请的实施例可以应用于下一代无线通信系统中，例如 5G 通信系统，如图 1 所示，图 1 示出了本申请的一种可能的网络架构示意图，该网络架构中包括：

- 30 AMF 节点：为负责移动性管理的网元，可以用于实现移动性管理实体（mobility management entity, MME）功能中除会话管理之外的其它功能，例如合法监听，接入授权等功能。

会话管理功能（session management function, SMF）节点：用于为用户面分配会话资源。

- 35 鉴权服务功能（authentication server function, AUSF）节点：当 AUSF 对终端进行鉴权的时候，负责验证传递待认证参数和认证终端的真实性。主要功能包括：接收安全锚点功能（security anchor function, SEAF）节点发送的鉴权请求；选择鉴权方法。在使用可扩展鉴权协议鉴权和密钥协商（extensible authentication protocol authentication and key agreement, EAP-AKA'）鉴权方法的时候，AUSF

节点可以完成网络侧对终端的鉴权。

SEAF 节点: SEAF 节点可以是 AMF 节点的一部分,也可以是独立的网元,主要负责向 AUSF 发起鉴权请求,在演进分组系统鉴权和密钥协商 (evolved packet system authentication and key agreement, EPS-AKA\*) 鉴权过程中完成网络侧对终端的认证。

用户面功能 (user plane function, UPF) 节点: 为用户面数据的出口,用于连接外部网络。

数据网络 (Data Network, DN): 用于提供外部数据的网络,例如因特网 (Internet) 等。

(无线) 接入网 ((radio) access network, (R) AN) 节点: (R) AN 可以采用不同的接入技术。目前的无线接入技术有 2 种类型: 3GPP 接入技术 (例如 3G、4G 或 5G 系统中采用的无线接入技术) 和 non-3GPP 接入技术。3GPP 接入技术是指符合 3GPP 标准规范的接入技术,采用 3GPP 接入技术的接入网称为无线接入网 (RAN), 其中, 5G 系统中的接入网设备称为下一代基站节点 (next generation node basestation, gNB)。非 3GPP 接入技术是指不符合 3GPP 标准规范的接入技术,例如,以 wifi 接入点 (access point, AP) 为代表的空口技术。

终端: 本申请所称的终端,是一种具有无线收发功能的设备,可以部署在陆地上,包括室内或室外、手持或车载;也可以部署在水面上 (如轮船等);还可以部署在空中 (例如飞机、气球和卫星上等)。该终端可以包括各种类型的用户设备 (user equipment, UE)、手机 (mobile phone)、平板电脑 (pad)、带无线收发功能的电脑、无线数据卡、虚拟现实 (virtual reality, VR) 终端设备、增强现实 (augmented reality, AR) 终端设备、机器类型通信 (machine type communication, MTC) 的终端设备、工业控制 (industrial control) 中的终端设备、无人驾驶 (self driving) 中的终端设备、远程医疗 (remote medical) 中的终端设备、智能电网 (smart grid) 中的终端设备、运输安全 (transportation safety) 中的终端设备、智慧城市 (smart city) 中的终端设备,以及可穿戴设备 (如智能手表,智能手环,计步器等) 等等。在采用不同的无线接入技术的系统中,具备相类似无线通信功能的终端的名称可能会有所不同,仅为描述方便,本申请实施例中,上述具有无线收发通信功能的装置统称为终端。

具体地,本申请中的终端中存储有长期密钥和相关函数,终端在与核心网节点 (如 AMF 节点、AUSF 节点、SEAF 节点等) 进行双向鉴权时,可使用长期密钥和相关函数对验证网络的真实性。

接入网设备: 本申请实施例所涉及到的接入网设备是一种为终端提供无线通信功能的装置。例如,接入网设备可以是基站 (Base Station, BS), 所述基站可以包括各种形式的宏基站,微基站,中继站,接入点等等。在采用不同的无线接入技术的系统中,具备基站功能的设备的名称可能会有所不同,例如在 5G 系统中,称为下一代基站节点,可表示为 gNB,在长期演进 (Long Term Evolution, LTE) 系统中,称为演进的节点 B (evolved NodeB, eNB 或 eNodeB), 在第三代 (3rd Generation, 3G) 通信系统中,称为节点 B (Node B) 等等。为方便描述,本发明实施例中,上述为终端

提供无线通信功能的装置统称为接入网设备。

网络能力开放功能 (network exposure function, NEF) 节点: 主要用于与第三方交互, 使第三方可以间接与某些 3GPP 网络内部的网元进行交互。

网络功能存储 (network function repository function, NRF) 节点: 用于网元间发现, 维护网络功能 (network function, NF)。

策略控制功能 (policy control function, PCF) 节点: PCF 节点中存储有最新的服务质量 (quality of service, QoS) 规则, 基站可根据 SMF 节点提供的 QoS 规则, 为用户面传输通道分配合适的资源。

统一的数据管理 (unified data management, UDM) 节点: 用于存储用户的签约信息。

应用功能 (application function, AF) 节点: AF 节点可以位于 DN 内部, 属于部署在第三方的功能网元, 此网元主要作用是告知 PCF 节点最新的第三方企业对于某个应用的业务要求。PCF 节点可根据业务要求生成相应的 QoS 规则, 确保网络提供的服务满足第三方所提出的要求。

在本申请的实施例中, 终端可以通过至少两种接入技术接入 AMF 节点, 以至少两种接入技术包括 3GPP 接入技术和非 3GPP 接入技术为例, 本申请实施例还提供了一种可能的网络架构示意图, 如图 2 所示, 该网络架构中包括 AMF 节点、AUSF 节点、SMF 节点、UPF 节点、UDM 节点 (或认证凭证存储和处理功能 (authentication credential repository and processing function, APRF) 节点)、终端和非 3GPP 互通功能 (non-3GPP interworking function, N3IWF) 节点。

其中, AMF 节点、AUSF 节点、SMF 节点、UPF 节点、UDM 节点和终端可参考图 1 中的描述, 此处不再赘述。

其中, N3IWF 节点用于支持终端通过非 3GPP 接入技术接入 AMF 节点。

结合图 2 所示的网络架构, 终端可以同时通过 3GPP 接入技术和非 3GPP 接入技术接入 AMF 节点。其中, 3GPP 接入技术可以简单表示为 3GPP, 非 3GPP 接入技术可以简单表示为非 3GPP 或 non-3GPP。图 2 中的路径 1 为终端通过 3GPP 接入 AMF 节点的路径, 路径 2 为终端通过非 3GPP 接入 AMF 节点的路径, 即终端可通过 N3IWF 接入 AMF 节点。在终端同时通过 3GPP 和非 3GPP 接入 AMF 节点的情况下, 若终端需要向 AMF 节点发送 NAS 消息, 在一种可能的实现方式中, NAS 消息可以被拆分为至少两个消息块, 一部分消息块通过 3GPP 传输, 另一部分消息块通过非 3GPP 传输, 示例性地, 可以将 NAS 消息划分为 1、2、3、4、5 这五个消息块, 其中 2、4 消息块通过 3GPP 传输, 1、3、5 消息块通过非 3GPP 传输。在另一种可能的实现方式中, 终端可以通过 3GPP 传输一整条 NAS 消息, 通过非 3GPP 传输另一整条 NAS 消息。

首先对本申请实施例涉及到的相关术语进行解释说明。

(1) NAS count

NAS count 由 24bit 组成, 包括 16bit 的翻转比特位 (overflow counter) 和 8bit 的序列号 (sequence number)。

NAS count 的初始值为 0, 终端每向核心网设备发送一条 NAS 消息, 上行 NAS count 加 1, 核心网设备每向终端发送一条 NAS 消息, 下行 NAS count 加 1。在完成终端向核

心网设备的鉴权流程后，上行 NAS count 和下行 NAS count 均置为 0。

可选地，存在以下两种维护 NAS count 的方法：

方法一为发送 NAS 消息后，将存储的 NAS count 加 1 并存储，再次需要发送 NAS 消息时，使用存储的 NAS count 对 NAS 消息进行安全保护。

- 5       方法二为发送 NAS 消息后，在下一次需要发送 NAS 消息时，将存储的 NAS count 加 1 从而确定一个新的 NAS count，使用新的 NAS count 对 NAS 消息进行安全保护。

10       终端和核心网设备在接收到 NAS 消息后，可以验证接收到的 NAS count 是否被重用，即验证 NAS 消息中携带的 NAS count 是否比上一次接收到的 NAS count 大。示例性地，若 AMF 节点接收到来自终端的上行 NAS count，可以比较此次接收到的上行 NAS count 是否大于上次接收到的上行 NAS count，若大于，则对该 NAS 消息的安全验证通过。

在使用 NAS count 进行加解密和完整性保护时，NAS count 会被填充为 32bit，即在原有的 24bit 的 NAS count 之前填充 8bit，填充的 8bit 可以全为 0。

#### (2) 加密和解密

- 15       如图 3 所示，图 3 为对 NAS 消息进行加密和解密的流程。

其中，KEY 可以为 NAS 密钥。

加解密使用的序列号 (COUNT) 由 32bit 组成，其中前 8bit 为 0，中间 16bit 为翻转比特位，后 8bit 为序列号。

承载信息 (BEARER) 由 5bit 组成，5bit 全为 0。

- 20       数据传输方向 (DIRECTION) 用于表示上下行，为上行 NAS 消息进行加解密时，DIRECTION 表示上行，为下行 NAS 消息进行加解密时，DIRECTION 表示下行。

长度 (LENGTH) 用于表示需要被加密或解密的 NAS 消息的数据长度。

演进分组系统加密算法 (evolved packet system encryption algorithm, EEA)，也可以可简称为 EPS 加密算法，为用于为 NAS 消息进行加密和解密的算法。

- 25       加密流程为将输入参数 (KEY、COUNT、BEARER、DIRECTION 和 LENGTH) 经过 EEA 处理，可以得到密钥流 (KEYSTREAM)，将密钥流和明文 (NAS 消息) 进行模二加可以得到密文 (CIPHERTEXT)。解密流程为将上述输入参数经过 EEA 处理，可以得到密钥流，然后将密钥流和密文进行模二加即可恢复出明文。

#### (3) 完整性保护

- 30       如图 4 所示，图 4 为对 NAS 消息进行完整性保护和验证完整性保护的流程。

其中，消息 (MESSAGE) 是指需要被完整性保护的消息，具体可以为 NAS 消息。

演进分组系统完整性算法 (evolved packet system integrity algorithm, EPS 完整性算法)

- 35       完整性保护的方法为发送端将输入参数 (KEY、COUNT、MESSAGE、BEARER、DIRECTION) 经过 EIA 处理，可以得到完整性保护的预期消息鉴权码 (message authentication code integrity, MAC-I) 或 NAS-MAC，完整性保护验证的方法为将输入参数 (KEY、COUNT、MESSAGE、BEARER、DIRECTION) 经过 EIA 处理，可以得到期望消息鉴权码 (expected message authentication code integrity, XMAC-I) 或 XNAS-MAC，进而将 XMAC-I 与 MAC-I 进行对比，若 XMAC-I 与 MAC-I 一致，则完整性保护验证通过。

以下对本申请提出的技术方案进行详细描述。

基于图 1 和图 2 的网络架构，本申请的实施例提供一种安全保护的方法。该方法中，有关加密和解密，以及完整性保护的流程可以参考图 3 和图 4 的描述。如图 5 所示，该方法包括：步骤 501 和步骤 502。

5 步骤 501、终端确定第一参数。

其中，第一参数是终端在为 NAS 消息进行安全保护的时的输入参数，用于表示传输 NAS 消息所使用的接入技术。其中，终端能够支持至少两种接入技术，且能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号。例如，上述至少两种接入技术可以是 3GPP 接入技术、非 3GPP 接入技术和固网接入技术等其他可以与 3GPP 接入技术共同使用 3GPP 网络核心网设备的接入技术中的至少两种，可选地，第一参数表示传输 NAS 消息所使用的接入技术还可以理解为，第一参数用于表示终端传输 NAS 消息所使用的传输路径。例如，终端和 AMF 节点可以不区分接入技术，分别为每个传输路径维护对应的 NAS 序列号，若传输 NAS 消息所使用的传输路径为路径 1，则使用路径 1 对应的 NAS 序列号；若传输 NAS 消息所使用的传输路径为路径 2，则使用路径 2 对应的 NAS 序列号。可以理解的是，传输路径与接入技术对应，示例性地，参考图 2，路径 1 传输数据时使用的接入技术为 3GPP 接入技术，路径 2 传输数据时使用的接入技术为非 3GPP 接入技术。

其中，第一参数可以是加解密或完整性保护过程中新增的一个新的输入参数，该参数包括预设数量的比特位，可选地，可以通过将比特位设置成不同的值来表示不同的接入技术。

在第一种可能的实现方式中，如图 6 所示，第一参数可以为接入 (ACCESS) 参数，示例性地，若第一参数为 00，则代表使用的是 3GPP 接入技术，若第一参数为 01，则代表使用的是非 3GPP 接入技术。或者，001 代表 3GPP 接入技术，010 代表无线保真 (wireless-fidelity, wifi) 技术，011 代表固网技术。

25 或者，还可以用 001 代表使用的第一种接入技术，010 表示使用的第二接入技术，011 代表使用的第三种接入技术，即每次切换使用的接入技术时，将第一参数加 1，直至第一参数的所有比特位均为 1 时，可以重新将第一参数从 000 开始计数，例如，若终端经过多次切换使用的接入技术，第一参数的所有比特位均变为 1，假设终端此时需要将使用的接入技术由第一接入技术切换至第二接入技术，则为第二接入技术生成的第一参数为 001。可选地、在此种方法中，第一种接入技术、第二种接入技术和第三种接入技术可以是同一种技术，即重新接入某种接入技术时，将第一参数加 1，直至第一参数的所有比特位均为 1 时，可以重新将第一参数从 000 开始计数。

30 可选地，每次输入参数中的 COUNT 重置为 0，或者 NAS 序列号重置为 0 时，也可以将第一参数加 1。

35 可选地，当第一参数的所有比特位均为 1 时，需要更新下一次传输 NAS 消息时使用的 NAS 密钥。

在第二种可能的实现方式中，如图 7 所示，可以使用输入参数中的 COUNT 的全部或部分来表示传输 NAS 消息所使用的接入技术。例如，若 COUNT 由 8bit 全 0 填充位和 NAS 序列号组成，所以第一参数可以为这 8 比特位的部分或全部，示例性地，可以选

取前 3bit 用于表示传输 NAS 消息所使用的接入技术。如何通过比特位的值来区分不同的接入技术可参考第一种实现方式中的相关描述。

在第三种可能的实现方式中，如图 8 所示，可以使用输入参数中的 BEARER 来表示传输 NAS 消息所使用的接入技术，或表示传输 NAS 消息所使用的接入路径，第一参数  
5 可以为 BEARER 的部分或全部。示例性地，可以选取前 3bit 用于表示传输 NAS 消息所使用的接入技术。如何通过比特位的值来区分不同的接入技术可参考第一种实现方式中的相关描述。

在第四种可能的实现方式中，可以增加 NAS 序列号的比特位，第一参数为 NAS 序列号的一部分比特位。例如将 NAS 序列号由 32bit 扩展为 64bit (64bit 的 NAS 序列号  
10 适应于长度为 256bit 的密钥)。扩展后的 NAS 序列号的一部分用于表示接入技术，例如保留 3bit，000 表示 3GPP 接入技术，001 表示 wifi 接入技术，010 表示固网接入技术。

在第五种可能的实现方式中，第一参数可以为 NAS 序列号，通过移除 NAS 序列号的的比特位，用移比特位的数量表示接入技术。

15 可选地，将现有的 NAS 序列号中的 overflow counter 移除预设数量的比特位，用移除比特位的数量表示接入技术。例如，若移除了 1 个比特位，表示接入技术为 3GPP 接入技术；若移除了 2 个比特位，表示接入技术为 wifi 接入技术；若移除了 3 个比特位，表示接入技术为固网接入技术。

或者，将现有的 NAS 序列号的序列号部分移除预设数量的比特位，用移除比特位的数量表示接入技术。例如，若移除了 1 个比特位，表示接入技术为 3GPP 接入技术；  
20 若移除了 2 个比特位，表示接入技术为 wifi 接入技术；若移除了 3 个比特位，表示接入技术为固网接入技术。

可选地，终端中可预先配置每种接入技术对应的第一参数，在终端确定传输 NAS 消息使用的接入技术后，可根据传输 NAS 消息使用的接入技术查找对应的第一参数；  
25 或者，终端在确定传输 NAS 消息使用的接入技术后，生成根据传输 NAS 消息使用的接入技术生成第一参数。

需要说明的是，在第一参数为 NAS 序列号，或者第一参数为 NAS 序列号的一部分比特位的情况下，终端为支持的每种接入技术维护的 NAS 序列号不同，在其他情况下，终端为支持的每种接入技术维护的 NAS 序列号可以相同也可以不同。

30 第一参数可以由终端自行确定，通知给 AMF 节点；也可以由 AMF 节点确定，然后通知给终端。也可以提前在终端和 AMF 节点中配置好。示例性地，若第一参数为 AMF 节点确定，终端可接收到来自 AMF 节点的第一参数，若第一参数为 NAS 序列号中的部分比特位，则终端接收到第一参数后，可将自身保存的 NAS 序列号中的指定比特位替换为第一参数；或者，若第一参数为 BEARER 中的部分比特位，则终端可将 BEARER 中的  
35 的指定比特位替换为第一参数。

步骤 502、终端根据第一参数、NAS 密钥以及传输 NAS 消息所使用的接入技术对应的 NAS 序列号对 NAS 消息进行安全保护。

其中，NAS 序列号可以为 NAS count，或具有防止 NAS 消息重放攻击的作用的参数。NAS 密钥为终端能够支持的至少两种接入技术共享的 NAS 密钥。

终端对 NAS 消息进行安全保护是指对待传输至核心网设备的 NAS 消息进行加密，对接收到的 NAS 消息进行解密，对待传输至核心网设备的 NAS 消息进行完整性保护或者对接收到的 NAS 消息进行完整性保护验证。相应的，对 NAS 消息进行安全保护使用的密钥可以为加密密钥和完整性保护密钥。本申请实施例中将加密密钥和完整性保护密钥统称为 NAS 密钥。本申请的实施例不限制对加密、解密、生产完整性保护和验证完整性保护的执行顺序。

可以理解的是，终端能够为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号，若终端使用 3GPP 接入技术传输 NAS 消息，则使用 3GPP 接入技术对应的第一参数、终端为 3GPP 接入技术维护的上行 NAS 序列号和 NAS 密钥对 NAS 消息进行安全保护。

对应于第一参数的三种实现方式，对 NAS 消息进行加密的方法分别如图 6、图 7 和图 8 所示。

对应于上述第一种实现方式，结合图 4，对 NAS 消息进行安全保护时使用的输入参数也可以为 ACCESS。

对应于上述第二种实现方式，结合图 4，对 NAS 消息进行安全保护时使用的输入参数中的 COUNT 包括第一参数。

对应于上述第三种实现方式，结合图 4，对 NAS 消息进行安全保护时使用的输入参数中的 BEARER 包括第一参数。

可选地，若终端接收到 NAS 消息，可确定传输该 NAS 消息所使用的接入技术对应的第一参数，进而可以使用 NAS 消息中携带的下行 NAS 序列号、传输该 NAS 消息所使用的接入技术对应的第一参数以及 NAS 密钥对 NAS 消息进行解密和/或进行完整性保护验证。

本申请的实施例提供的安全保护的方法，终端能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号，终端在使用不同的接入技术传输 NAS 消息时，不是共用一套 NAS 序列号，而是使用为对应的接入技术维护的 NAS 序列号对 NAS 消息进行安全保护，可以避免核心网设备先接收到通过其中一条链路传输的较小的 NAS 序列号，后接收到通过另一条链路传输的较大的 NAS 序列号的情况下，发生重放攻击的问题，而且本申请在对 NAS 消息进行安全保护时，还使用了用于区分不同接入技术的第一参数，所以即使对通过不同的接入技术传输的 NAS 消息进行安全保护时使用的 NAS 密钥和 NAS 序列号均相同，对 NAS 消息进行安全保护的结果也不同，降低了发生重放攻击的可能性，实现了对多条 NAS 连接链路的安全保护。

对应于图 5 的实施例，在本申请实施例的另一种实现方式中，还提供了核心网设备对 NAS 消息进行安全保护的方法，核心网设备可以为 AMF 节点、SEAF 节点、MME 节点、或其他参与终端鉴权流程的节点、或者其他涉及到密钥生成和密钥存储的节点，在本申请的实施例中，以核心网设备为 AMF 节点为例进行说明，如图 9 所示，该方法包括：

步骤 901、AMF 节点确定第一参数。

第一参数用于表示传输 NAS 消息所使用的接入技术，AMF 节点能够分别为终端支持的至少两种接入技术中的每种接入技术维护对应的 NAS 序列号。

其中, AMF 节点确定第一参数的方法与上述图 5 的步骤 501 中终端确定第一参数的方法相似, 可参考步骤 501 中的相关描述。

步骤 902、AMF 节点根据第一参数、NAS 密钥以及传输 NAS 消息所使用的接入技术对应的 NAS 序列号对 NAS 消息进行安全保护。

5 其中, NAS 序列号可以为 NAS count, 或具有防止 NAS 消息重放攻击的作用的参数。

AMF 节点对 NAS 消息进行安全保护可以为对待传输至终端的 NAS 消息进行加密, 对接收到的 NAS 消息进行解密, 对待传输至终端的 NAS 消息进行完整性保护, 对接收到的 NAS 消息进行完整性保护验证。

10 其中, AMF 节点对 NAS 消息进行安全保护的方法与上述步骤 502 中终端对 NAS 消息进行安全保护的方法相似, 可参考步骤 502 中的相关描述。

本申请的实施例提供的安全保护的方法, 核心网设备能够分别为至少两种接入技术中的每种接入技术维护对应的 NAS 序列号, 终端在使用不同的接入技术传输 NAS 消息时, 不是共用一套 NAS 序列号, 而是使用为对应的接入技术维护的 NAS 序列号对 NAS 消息进行安全保护, 可以避免核心网设备先接收到通过其中一条链路传输的较小的 NAS 序列号, 后接收到通过另一条链路传输的较大的 NAS 序列号的情况下, 发生重放攻击的问题, 而且本申请在对 NAS 消息进行安全保护时, 还使用了用于区分不同接入技术的第一参数, 所以即使对通过不同的接入技术传输的 NAS 消息进行安全保护时使用的 NAS 密钥和 NAS 序列号均相同, 对 NAS 消息进行安全保护的结果也不同, 降低了发生重放攻击的可能性, 实现了对多条 NAS 连接链路的安全保护。

20 可选地, 若传输 NAS 消息所使用的接入技术为第一接入技术, 在图 5 和图 9 的流程之前, 如图 10 所示, 该方法还可以包括: 步骤 1001 至步骤 1007。

步骤 1001、终端确定第一接入技术对应的第一上行 NAS 序列号。

其中, 第一上行 NAS 序列号为 0, 具体地, 第一上行 NAS 序列号的所有或部分比特位为 0; 或者,

25 第一上行 NAS 序列号为随机数。具体地, 第一上行 NAS 序列号中的部分或全部比特位为随机数。例如, 第一上行 NAS 序列号中的序列号部分, 或 NAS overflow 部分为随机数。此时, 其余部分为 0; 或者,

所述至少两种接入技术还包括第二接入技术, 所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号, 若终端保存了至第二接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号; 或者,

30 所述至少两种接入技术还包括第二接入技术, 所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号加 1, 若终端保存了第二接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的最大上行 NAS 序列号加 1; 或者,

第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号, 若终端保存了第一接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号; 或者,

第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号

加 1，若终端保存了第一接入技术对应的至少两个上行 NAS 序列号，则第一上行 NAS 序列号为终端保存的第一接入技术对应的最大的上行 NAS 序列号加 1。

- 5 可选地，第一接入技术和第二接入技术可以分别为 3GPP 接入技术、非 3GPP 接入技术、固网接入技术，或者其他可以接入核心网设备的技术，或者与 3GPP 接入技术共同使用 3GPP 网络核心网设备的任意一种技术。本申请的实施例中以第一接入技术为非 3GPP 接入技术，第二接入技术为 3GPP 接入技术为例进行说明。

可以理解的是，在终端使用非 3GPP 接入技术向 AMF 节点发送 NAS 消息之前，需要确定使用非 3GPP 接入技术传输 NAS 消息时携带的第一上行 NAS 序列号。

- 10 若终端首次通过非 3GPP 接入技术接入 AMF 节点，则可将非 3GPP 接入技术对应的第一上行 NAS 序列号设置为 0 或随机数。或者，在终端已经通过 3GPP 接入技术接入过 AMF 节点的情况下，若 NAS 序列号的维护方法为上文中描述的方法一（发送 NAS 消息后，将 NAS 消息中使用的 NAS count 加 1 并存储，再次需要发送 NAS 消息时，使用此次存储的 NAS count 对 NAS 消息进行安全保护），则可以确定第一上行 NAS 序列号为终端中保存的 3GPP 接入技术对应的上行 NAS 序列号。若终端保存有至少两个 3GPP 接入技术对应的上行 NAS 序列号，且终端无法确定上一条 NAS 消息使用的上行 NAS 序列号，则选择终端保存的 3GPP 接入技术对应的最大的上行 NAS 序列号对 NAS 消息进行安全保护。若 NAS 序列号的维护方法为上文中描述的方法二（发送 NAS 消息后，在下次需要发送 NAS 消息时，将存储的 NAS count 加 1 从而确定一个新的 NAS count，使用新的 NAS count 对 NAS 消息进行安全保护）则可以确定第一上行 NAS 序列号为终端中保存的 3GPP 接入技术对应的上行 NAS 序列号加 1。若终端保存有至少两个 3GPP 接入技术对应的上行 NAS 序列号，且终端无法确定上一条 NAS 消息使用的上行 NAS 序列号，则选择终端保存的 3GPP 接入技术对应的最大的上行 NAS 序列号并加 1，并使用加 1 后的上行 NAS 序列号对 NAS 消息进行安全保护。

- 25 在终端已经通过非 3GPP 接入技术接入过 AMF 节点的情况下，若 NAS 序列号的维护方法为上述方法一，则可确定第一上行 NAS 序列号为终端保存的非 3GPP 接入技术对应的上行 NAS 序列号；若 NAS 序列号的维护方法为上述方法二，则可确定第一上行 NAS 序列号为终端保存的非 3GPP 接入技术对应的上行 NAS 序列号加 1。

步骤 1002、终端向 AMF 节点发送第一消息，第一消息携带第一上行 NAS 序列号的部分或全部。

- 30 其中，第一消息通过第一上行 NAS 序列号和 NAS 密钥进行安全保护。可选地，第一消息中可携带 24bit 的第一上行序列号，也可以只携带第一上行序列号的一部分，例如只携带第一上行 NAS 序列号的最后 4 位或最后 8 位。

- 35 在另一种可能的实现方式中，若终端首次通过非 3GPP 接入技术接入 AMF 节点，且终端已经通过 3GPP 接入技术接入过 AMF 节点，则终端可以直接暂时不确定第一上行 NAS 序列号，先使用非 3GPP 接入技术对应的 NAS 序列号对第一消息进行安全保护，即上述步骤 1001 至步骤 1002 可以替换为步骤 1003。

步骤 1003、终端向 AMF 节点发送第一消息，第一消息携带第二接入技术对应的上行 NAS 序列号的部分或全部。

其中，第一消息通过 NAS 密钥和第二接入技术对应的上行 NAS 序列号进行安全保

护。

- 第一消息中携带的第二接入技术对应的上行 NAS 序列号为终端保存的第二接入技术对应的上行 NAS 序列号的部分或全部，或者为终端保存的第二接入技术对应的上行 NAS 序列号加 1 后得到的新的上行 NAS 序列号的部分或全部。其中，若终端保存了第二技术技术对应的至少两个上行 NAS 序列号，则本步骤中的第二接入技术对应的上行 NAS 序列号为终端保存的第二接入技术对应的最大的上行 NAS 序列号。

- 需要说明的是，可选地，步骤 1002 和步骤 1003 的第一消息中均包括第一指示信息，第一指示信息用于指示第一消息中携带的上行 NAS 序列号的部分或全部对应的接入技术，或者第一指示信息用于指示第一消息中携带的 NAS 序列号的全部或部分对应的传输路径。示例性地，步骤 1002 的第一消息中携带的第一指示信息指示非 3GPP 接入技术，步骤 1003 的第一消息中携带的第一指示信息指示 3GPP 接入技术。再比如，步骤 1002 的第一消息中携带的第一指示信息指示通过路径 1 接入 AMF 的，步骤 1003 的第一消息中携带的第一指示信息指示通过路径 2 接入 AMF 的。

- 在上述步骤 1002 或步骤 1003 之后，还可以执行以下步骤。

- 步骤 1004、AMF 节点接收第一消息。

步骤 1005、AMF 节点根据第一指示信息指示的接入技术对应的上行 NAS 序列号，对第一消息携带的 NAS 序列号进行验证。

- 指示信息可以为显示的指示，还可以是隐示的告知。例如，接入类型信息可以为 N2 消息中的明确告知的接入类型指示信息（如，无线接入技术（radio access technology, RAT） type 接入类型），或者为 NAS 消息中放入的接入类型指示信息。在没有接入类型指示信息的情况下，AMF 可以根据第一消息的来源判断接入类型。比如，消息源地址是基站，则为 3GPP 接入；如果为 N3IWF 节点，则为 non-3GPP 接入；如果为连接固网的设备，则为固网接入。

- 在第一指示信息指示的是非 3GPP 接入技术的情况下，若第一消息携带了完整的第一 NAS 序列号，且 AMF 节点确定该终端之前接入过 AMF 节点，则 AMF 节点判断第一 NAS 序列号是否大于 AMF 节点中保存的上一次接收到的非 3GPP 接入技术对应的上行 NAS 序列号，若大于，则验证成功，若小于，则验证失败，拒绝终端接入并告知终端接入失败原因。可选地，若 AMF 节点确定该终端之前未通过非 3GPP 接入技术接入过 AMF 节点，则 AMF 节点将第一 NAS 序列号保存为非 3GPP 接入技术对应的上行 NAS 序列号，或者 AMF 节点确定非 3GPP 接入技术对应的上行 NAS 序列号为 0。若第一消息携带了第一 NAS 序列号的一部分，则 AMF 节点先恢复出完整的第一 NAS 序列号，再根据上述处理第一 NAS 序列号的方法对第一 NAS 序列号进行验证或者保存。

- 在第一指示信息指示的是 3GPP 接入技术的情况下，若第一消息携带了完整的 3GPP 接入技术对应的 NAS 序列号，则 AMF 节点判断第一 NAS 序列号是否大于 AMF 节点中保存的上一次接收到的 3GPP 接入技术对应的上行 NAS 序列号，若大于，则验证成功，若小于，则验证失败。若第一消息中携带了 3GPP 接入技术对应的 NAS 序列号的一部分，则 AMF 节点先恢复出完整的 NAS 序列号，再采用上述验证 NAS 序列号的方法对恢复出的完整的序列号进行验证。

步骤 1006、AMF 节点确定所述第一接入技术对应的第二上行 NAS 序列号和第一下

行 NAS 序列号之一或全部。

其中，第二上行 NAS 序列号为 0，具体地，第二上行 NAS 序列号的所有或部分比特位为 0。或者，第二上行 NAS 序列号为随机数。具体地，第二上行 NAS 序列号中的部分或全部比特位为随机数。例如，第二上行 NAS 序列号中的序列号部分，或 NAS

- 5 overflow 部分为随机数。此时，其余部分为 0。或者，第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者，第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者，第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第一接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。或者，第二上行 NAS 序列号为第一上行 NAS 序列号。或者，第二上行 NAS 序列号为第一上行 NAS 序列号加 1。

可选地，若 AMF 节点接收到的第一消息中携带了第一上行 NAS 序列号，则 AMF 节点可确定第二上行 NAS 序列号为第一 NAS 序列号，或者第二上行 NAS 序列号为第一上行 NAS 序列号加 1。

- 20 或者，若 AMF 节点接收到的第一消息中携带了第一上行 NAS 序列号，说明终端已经确定了非 3GPP 接入技术对应的 NAS 序列号，则 AMF 节点可以不确定第二 NAS 序列号。

第一下行 NAS 序列号为 0，具体地，第一下行 NAS 序列号的所有或部分比特位为 0。或者，

- 25 第一下行 NAS 序列号为随机数。具体地，第一下行 NAS 序列号中的部分或全部比特位为随机数。例如，第一下行 NAS 序列号中的序列号部分，或 NAS overflow 部分为随机数。此时，其余部分为 0。或者，第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的下行 NAS 序列号，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号。或者，第一下行 NAS 序列号为核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第二接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第二接入技术对应的最大的下行 NAS 序列号加 1。或者，第一下行 NAS 序列号为核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1，若核心网设备保存了第一接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为所核心网设备保存的第一接入技术对应的最大的下行 NAS 序列号加 1。

- 35 可选地，若 AMF 节点接收到的第一消息中携带的是第二接入技术对应的 NAS 序列号，则 AMF 节点确定的第二上行 NAS 序列号可以和第一下行 NAS 序列号相同。

步骤 1007、AMF 节点向终端发送第二消息，第二消息包括第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

相应地，终端接收第二消息。

- 可选地，第二消息携带第二指示信息，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的接入技术，可选地，第二消息中还可以携带用于指示第二消息中携带的第二上行 NAS 序列号的指示信息。可选地，第二指示信息用于指示第二消息中携带的第一下行 NAS 序列号对应的传输路径，可选地，第二消息中还可以携带
- 5 用于指示第二消息中携带的第二上行 NAS 序列号对应的传输路径的指示信息。可以理解的是，由于第二消息中携带的是第一接入技术对应的第一下行 NAS 序列号，所以第二指示信息用于指示第一接入技术，示例性地，若第一接入技术为 3GPP 接入技术，则第二指示信息用于指示 3GPP 接入技术；若第一接入技术为非 3GPP 接入技术，则第二指示信息用于指示非 3GPP 接入技术。
- 10 可以理解的是，终端接收到第二消息后，可以保存第二消息携带的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。在下次需要通过非 3GPP 发送上行 NAS 消息时，可根据第二上行 NAS 序列号对 NAS 消息进行安全保护。或者在接收到下行 NAS 消息后，也可以根据第一下行 NAS 序列号对接收到的下行 NAS 消息中的下行 NAS 序列号进行验证。
- 15 以下结合具体场景对上述实施例描述的安全保护的方法进行介绍，本申请的实施例可以应用于终端已经通过 3GPP 接入技术接入 AMF 节点，之后终端通过非 3GPP 接入技术接入同一个 AMF 节点的场景中，如图 11 所示，图 11 为终端通过非 3GPP 接入技术接入 AMF 节点的注册流程，该方法包括：
- 步骤 1101、终端接入非可信的非 3GPP 网络。
- 20 例如终端接入了一个不可以直接被信任的 WiFi。
- 本步骤中，终端接入非可信的非 3GPP 网络，且终端已通过 3GPP 网络的鉴权，拥有 NAS 安全上下文。其中，NAS 安全上下文包括 NAS 密钥，密钥标识符，3GPP 接入技术对应的 NAS 序列号。可选地，NAS 上下文还包括非 3GPP 接入技术对应的 NAS 序列号。若终端之前已通过非 3GPP 接入技术接入过 AMF 节点，则非 3GPP 接入技术对应的
- 25 NAS 序列号不为 0，若终端之前已经通过非 3GPP 接入技术接入过 AMF 节点，则非 3GPP 接入技术对应的 NAS 序列号为 0。
- 其中，NAS 密钥可以为加密密钥和完整性保护密钥之一或全部。
- 步骤 1102、终端和 N3IWF 节点交互互联网密钥交互协议安全关联初始 (internet key exchange protocol-security association-initial, IKE-SA-INIT) 消息。
- 30 其中，IKE-SA-INIT 消息中携带密钥材料，密钥材料是用于对终端和 N3IWF 节点之间传输的消息进行安全保护的信息。在终端和 N3IWF 节点交互 IKE-SA-INIT 消息之后，终端和 N3IWF 节点可以生成相同的密钥，该密钥用于对终端和 N3IWF 节点后续传输的消息进行安全保护。
- 步骤 1103、终端向 N3IWF 节点发送互联网密钥交互协议鉴权请求 (internet key exchange protocol-authentication-request, IKE-AUTH-Req) 消息。
- 35 相应地，N3IWF 节点接收 IKE-AUTH-Req 消息。
- 步骤 1104、N3IWF 节点向终端发送互联网密钥交互协议鉴权响应消息 (internet key exchange protocol-authentication-response, IKE-AUTH-Res) 消息。
- 相应地，终端接收 IKE-AUTH-Res 消息。

其中, IKE-AUTH-Res 消息中携带可扩展鉴权协议 5G 接入请求 (extensible authentication protocol-5th generation-request, EAP-5G-Req) 消息的 5G 开始 (5G start) 消息, EAP-5G-Req 消息用于请求终端开始 5G 的可扩展鉴权协议 (extensible authentication protocol, EAP) 流程

5 步骤 1105、终端确定第一上行 NAS 序列号。

其中, 第一上行 NAS 序列号为用于对终端向 AMF 节点发送的 NAS 消息进行安全保护的序列号。

该步骤有两种实现方式:

第一种为终端根据 3GPP 接入技术对应的上行 NAS 序列号确定第一上行 NAS 序列号。

10 由于终端已经通过 3GPP 接入技术接入过 AMF 节点, 所以终端已经存储了 3GPP 接入技术对应的 NAS 序列号, 若 NAS 序列号的维护方法为上述方法一, 则可确定第一上行 NAS 序列号为终端保存的 3GPP 接入技术对应的上行 NAS 序列号(若终端保存了 3GPP 接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端保存的 3GPP 接入技术对应的最大的上行 NAS 序列号); 若 NAS 序列号的维护方法为上述方法二,  
15 则可确定第一上行 NAS 序列号为终端保存的非 3GPP 接入技术对应的上行 NAS 序列号加 1 (若终端保存了非 3GPP 接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端保存的非 3GPP 接入技术对应的最大的上行 NAS 序列号加 1)。

第二种为终端生成非 3GPP 接入技术对应的 NAS 序列号, 将非 3GPP 接入技术对应的 NAS 序列号作为第一上行 NAS 序列号。

20 具体地, 第一上行 NAS 序列号可以为 0, 或者可以为一个随机数。

若第一上行 NAS 序列号为 0, 则第一上行 NAS 序列号的所有或部分比特位均为 0。若第一上行 NAS 序列号为随机数, 则第一上行 NAS 序列号中的部分或全部比特位为随机数, 示例性地, 第一上行 NAS 序列号的后 8 位 (序列号部分) 为随机数, 或者 NAS overflow 部分为随机数, 其余部分为 0。

25 可选地, 若终端已经通过非 3GPP 接入技术接入过 AMF 节点, 则终端可以确定第一上行 NAS 序列号为终端中保存的非 3GPP 接入技术对应的上行 NAS 序列号(若终端中保存了非 3GPP 接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端中保存的非 3GPP 接入技术对应的最大的上行 NAS 序列号), 或者终端可以确定第一上行 NAS 序列号为终端中保存的非 3GPP 接入技术对应的 NAS 序列号加 1 (若终端中保存了非 3GPP 接入技术对应的至少两个上行 NAS 序列号, 则第一上行 NAS 序列号为终端中保存的非 3GPP 接入技术对应的最大的上行 NAS 序列号加 1)。  
30

可选地, 若采用第二种实现方式确定第一上行 NAS 序列号, 在终端通过非 3GPP 接入技术接入 AMF 节点的注册流程中, 终端不会通过 3GPP 接入技术发送 NAS 消息。

35 可选地, 终端还可以设置一个指示符, 该指示符相当于图 10 对应的实施例中的第一指示信息, 用于指示第一上行 NAS 序列号对应的为 3GPP 接入技术还是非 3GPP 接入技术。可以理解的是, 若终端通过上述第一种实现方式确定第一上行 NAS 序列号, 则该指示符指示 3GPP 接入技术, 若终端使用上述第二种实现方式确定第一上行 NAS 序列号, 则该指示符指示非 3GPP 接入技术。

步骤 1106、终端向 N3IWF 节点发送 IKE-AUTH-Req 消息。

相应地，N3IWF 节点接收 IKE-AUTH-Req 消息。

其中，IKE-AUTH Req 消息中包括 NAS 协议数据单元(protocol data unit, PDU)和可扩展鉴权协议 5G 接入相应的 5G 非接入层消息(EAP-5G-ReS 消息相应的 5G-NAS 消息)或 5G-NAS 消息。NAS PDU 中包括注册请求消息，注册请求消息用于终端通过 3GPP

5 接入技术向 AMF 节点注册。可选地，上述实施例中的第一消息可以为该注册请求消息。

可选地，注册请求消息可以通过第一上行 NAS 序列号进行完整性保护，注册请求消息中包括第一指示信息和第一上行 NAS 序列号。可选地，注册请求消息中还包括密钥标识符和终端的临时身份标识。

步骤 1107、N3IWF 节点选择 AMF 节点。

10 其中，N3IWF 节点选择 AMF 节点的方法可参考现有技术。

步骤 1108、N3IWF 节点向 AMF 节点转发注册请求消息。

相应地，AMF 节点接收注册请求消息。

步骤 1109、AMF 节点对注册请求消息进行验证。

其中，AMF 节点对注册请求消息的验证包括对注册请求消息的完整性保护验证，  
15 以及对注册请求消息中携带的第一上行 NAS 序列号的验证。AMF 节点对注册请求消息中携带的第一上行 NAS 序列号进行验证对应于上述步骤 1005。

AMF 节点可根据注册请求消息中的临时身份标识和密钥标识符生成完整性保护密钥，根据完整性保护密钥对注册请求消息进行完整性保护验证。

若第一指示信息指示第一上行 NAS 消息对应的接入技术为 3GPP 接入技术，则 AMF  
20 节点验证第一上行 NAS 序列号是否比上一次接收到的 3GPP 接入技术对应的 NAS 序列号大，若是，则验证成功，否则验证失败。

若第一指示信息指示的第一上行 NAS 消息对应的接入技术为非 3GPP 接入技术，且终端未通过非 3GPP 接入技术接入过 AMF 节点，则 AMF 节点将第一 NAS 序列号保存为非 3GPP 接入技术对应的上行 NAS 序列号，或者 AMF 节点确定非 3GPP 接入技术对应的上行  
25 上行 NAS 序列号为 0。终端通过非 3GPP 接入技术接入过 AMF 节点，AMF 节点验证第一上行 NAS 序列号是否比上一次接收到的非 3GPP 接入技术对应的 NAS 序列号大，若是，则验证成功，否则验证失败。

步骤 1110、AMF 节点为 N3IWF 节点生成一个密钥 Kn3iwf。

其中，密钥 Kn3iwf 用于对 AMF 节点与终端之间的双向认证。

30 步骤 1111、AMF 节点确定非 3GPP 接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

可选地，若第一指示信息指示的接入技术为 3GPP 接入技术，说明终端未为非 3GPP 接入技术确定 NAS 序列号，则 AMF 节点可以确定非 3GPP 接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号；若第一指示信息指示的接入技术为非 3GPP 接入技术，  
35 说明终端已经为非 3GPP 接入技术确定了上行 NAS 序列号，则 AMF 节点只需确定非 3DPP 技术对应的第一下行 NAS 序列号，或者 AMF 节点确定第一下行 NAS 序列号，并重新确定非 3GPP 接入技术的上行 NAS 序列号。

具体地，第二上行 NAS 序列号为 0，或者第二上行 NAS 序列号为随机数。

若第二上行 NAS 序列号为 0，则第二上行 NAS 序列号的所有、或部分比特比特位

均为 0。若第二上行 NAS 序列号为随机数，则第二上行 NAS 序列号中的部分或全部比特位为随机数，示例性地，第二上行 NAS 序列号的后 8 位（序列号部分）为随机数，或者 NAS overflow 部分为随机数，其余部分为 0。可选地，若第二上行 NAS 序列号为随机数，则第二上行 NAS 序列号需大于 AMF 节点保存的 3GPP 接入技术对应的下行 NAS 序列号（若 AMF 节点保存了 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号需大于 AMF 节点保存的 3GPP 接入技术对应的最大的下行 NAS 序列号）。

第二上行 NAS 序列号还可以为 AMF 节点保存的 3GPP 接入技术对应的下行 NAS 序列号（若 AMF 节点保存了 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为终端保存的 3GPP 接入技术对应的最大的下行 NAS 序列号）；或者，第二上行 NAS 序列号为为 AMF 节点保存的 3GPP 接入技术对应的下行 NAS 序列号加 1（若 AMF 节点保存了 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为终端保存的 3GPP 接入技术对应的最大的下行 NAS 序列号加 1）；或者，第二上行 NAS 序列号为 AMF 节点保存的非 3GPP 接入技术对应的下行 NAS 序列号加 1（AMF 节点保存了非 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第二上行 NAS 序列号为终端保存的非 3GPP 接入技术对应的最大的下行 NAS 序列号加 1）；或者，第二上行 NAS 序列号为第一上行 NAS 序列号；或者，第二上行 NAS 序列号为第一上行 NAS 序列号加 1。

可选地，第一下行 NAS 序列号可以与第二上行 NAS 序列号相同。

具体地，第一下行 NAS 序列号可以为 0，或者可以为随机数。

若第一下行 NAS 序列号为 0，则第一下行 NAS 序列号的所有比特位或部分比特位均为 0。若第一下行 NAS 序列号为随机数，则第一下行 NAS 序列号中的部分或全部比特位为随机数，示例性地，第一下行 NAS 序列号的后 8 位（序列号部分）为随机数，或者 NAS overflow 部分为随机数，其余部分为 0。可选地，若第一下行 NAS 序列号为随机数，则第一下行 NAS 序列号需大于 AMF 节点保存的 3GPP 接入技术对应的最大的下行 NAS 序列号。

第一下行 NAS 序列号还可以为 AMF 节点保存的 3GPP 接入技术对应的下行 NAS 序列号（若 AMF 节点保存了 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号还可以为 AMF 节点保存的 3GPP 接入技术对应的最大的下行 NAS 序列号）；或者，第一下行 NAS 序列号为 AMF 节点保存的 3GPP 接入技术对应的下行 NAS 序列号加 1（若 AMF 节点保存了 3GPP 接入技术对应的至少两个下行 NAS 序列号，则第一下行 NAS 序列号为 AMF 节点保存的 3GPP 接入技术对应的最大的下行 NAS 序列号加 1）；或者，第一下行 NAS 序列号为 AMF 节点保存的非 3GPP 接入技术对应的下行 NAS 序列号加 1（若 AMF 节点保存了非 3GPP 接入技术对应的下行 NAS 序列号，则第一下行 NAS 序列号为 AMF 节点保存的非 3GPP 接入技术对应的最大的下行 NAS 序列号加 1）。

需要说明的是，AMF 节点可以保存生成的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。AMF 节点可以维护 3GPP 接入技术对应的上行 NAS 序列号和下行 NAS 序列号，还可以另外维护非 3GPP 接入技术对应的上行 NAS 序列号和下行 NAS 序列号。若 AMF 节点生成了第二上行 NAS 序列号和第一下行 NAS 序列号，则保存第二上行 NAS 序列号和第一下行 NAS 序列号，若 AMF 节点只生成了第一下行 NAS 序列号，则保存第一下行 NAS 序列号，此时终端维护的非 3GPP 接入技术对应的上行 NAS 序列号为第一上

行 NAS 序列号。

可以理解的是，AMF 节点分别为 3GPP 接入技术和非 3GPP 接入技术各独立维护了一套 NAS 序列号，即 AMF 节点为 3GPP 接入技术维护的 NAS 序列号和为非 3GPP 接入技术维护的 NAS 序列号之间的大小不会互相影响。AMF 节点在接收到上行 NAS 消息时，

- 5 可根据上行 NAS 消息中的比特位信息、或者根据 N2 消息中的信息确定终端传输该上行 NAS 消息所使用的接入技术或传输路径，若使用的接入技术为 3GPP 接入技术，则可以比较上行 NAS 消息中携带的上行 NAS 序列号是否大于为 3GPP 接入技术维护的最大的上行 NAS 序列号；若使用的接入技术为非 3GPP 接入技术，则可以比较上行 NAS 消息中携带的上行 NAS 序列号是否大于为非 3GPP 接入技术维护的最大的上行 NAS 序列号，以防  
10 发生重放攻击。

步骤 1112、AMF 节点通过 N3IWF 节点向终端发送 NAS 安全模式命令 (security mode command, SMC) 消息。

相应地，终端接收 NAS SMC 消息。

其中，上述实施例中的第二消息可以为该 NAS SMC 消息。

- 15 NAS SMC 消息中携带第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部，可以理解的是，若 AMF 节点只确定了第一下行 NAS 序列号，则 NAS SMC 消息中携带第一下行 NAS 序列号，若 AMF 节点确定了第二上行 NAS 序列号和第一下行 NAS 序列号，则 NAS SMC 消息中携带第二上行 NAS 序列号和第一下行 NAS 序列号。

- 20 可选地，若 NAS 消息中只携带了第一下行 NAS 序列号，则 NAS 消息中还可以携带一个用于指示终端继续使用终端自身确定的上行 NAS 序列号的指示信息。

可选地，NAS SMC 消息中还包括第二指示信息，第二指示信息用于指示 NAS SMC 消息携带的 NAS 序列号对应的接入技术或传输路径，在本实施例的场景下，第二指示信息指示的接入技术为非 3GPP 接入技术。

- 25 步骤 1113、终端根据 NAS SMC 消息确定非 3GPP 接入技术对应的上行 NAS 序列号和下行 NAS 序列号。

其中，终端也可以分别为 3GPP 接入技术和非 3GPP 接入技术各独立维护一套 NAS 序列号，在本实施例的场景下，终端已经存储了 3GPP 接入技术对应的上行 NAS 序列号和下行 NAS 序列号，终端还可以根据本步骤接收到的 NAS SMC 消息确定为非 3GPP 维护的上行 NAS 序列号和下行 NAS 序列号。

- 30 可选地，若 NAS SMC 消息中只包括第一下行 NAS 序列号，则终端确定非 3GPP 接入技术对应上行 NAS 序列号仍为第一上行 NAS 序列号，非 3GPP 接入技术对应的下行 NAS 序列号为第一下行 NAS 序列号；若 NAS SMC 消息中包括第二上行 NAS 序列号和第一下行 NAS 序列号，则终端可确定非 3GPP 接入技术对应上行 NAS 序列号为第二上行 NAS 序列号，非 3GPP 接入技术对应的下行 NAS 序列号为第一下行 NAS 序列号。

- 35 可以理解的是，终端在接收到下行 NAS 消息时，可根据下行 NAS 消息中的比特位信息确定终端传输该下行 NAS 消息所使用的接入技术或传输路径，若使用的接入技术为 3GPP 接入技术，则可以比较下行 NAS 消息中携带的下行 NAS 序列号是否大于为 3GPP 接入技术维护的最大的下行 NAS 序列号；若使用的接入技术为非 3GPP 接入技术，则可以比较下行 NAS 消息中携带的下行 NAS 序列号是否大于为非 3GPP 接入技术维护的最大

的下行 NAS 序列号，以防发生重放攻击。

步骤 1114、终端通过 N3IWF 节点向 AMF 节点发送 NAS 安全模式完成 (security mode complete, SMP) 消息。

相应地，AMF 节点接收 NAS SMP 消息。

5 可选地，上述步骤 502 中的 NAS 消息可以为本步骤中的 NAS SMP 消息。

其中，终端可通过第一参数、上行 NAS 序列号以及 NAS 密钥对 NAS SMP 消息进行完整性保护。第一参数用于表示传输 NAS SMP 消息所使用的接入技术为非 3GPP 接入技术或用于表示传输 NAS SMP 消息的传输路径为图 2 中的路径 2，上行 NAS 序列号为步骤 1113 中终端确定的非 3GPP 接入技术对应的上行 NAS 序列号或路径 2 对应的上行 NAS 序列号。NAS SMP 消息中携带该上行 NAS 序列号。

可以理解的是，AMF 节点接收到 NAS SMP 消息后，可验证 NAS SMP 消息中携带的上行 NAS 序列号是否大于 AMF 节点存储的非 3GPP 接入技术对应的上行 NAS 序列号，或者是否大于路径 2 对应的上行 NAS 序列号，若大于则可根据 NAS 消息中的比特位信息确定传输该 NAS SMP 消息使用的接入技术为非 3GPP 接入技术，进而确定非 3GPP 接入技术对应的第一参数，然后根据第一参数，NAS 密钥以及 NAS SMP 消息中携带的上行 NAS 序列号对 NAS SMP 消息进行完整性校验。若校验成功则执行步骤 1115。可选的，若 AMF 保存有多个上行 NAS 序列号，则可验证 NAS SMP 消息中携带的上行 NAS 序列号是否大于 AMF 节点存储的非 3GPP 接入技术对应的最大的上行 NAS 序列号。

20 步骤 1115、AMF 节点向 N3IWF 节点发送 N2 消息。其中，N2 消息中携带密钥 Kn3iwf 和注册完成消息。

相应地，N3IWF 节点接收 N2 消息。

步骤 1116、N3IWF 节点向终端发送 EAP-5G-Success 消息。

相应地，终端接收 EAP-5G-Success 消息。

25 步骤 1117、终端和 N3IWF 节点通过 Kn3iwf 完成鉴权 (authentication) 参数的计算。

步骤 1118、终端和 N3IWF 节点之间建立网络安全协议 (internet protocol security, IPsec) 连接。

步骤 1119、N3IWF 节点向终端发送注册完成消息。

30 通过本申请的实施例提供的方法，可以实现终端通过非 3GPP 接入技术接入网络，且可以实现终端独立维护 3GPP 接入技术的 NAS 序列号和非 3GPP 接入技术的 NAS 序列号，降低了出现重放攻击的可能性。

在本申请实施例的一种可能的实现方式中，终端的安全上下文可以与运营商信息绑定，示例性地，运营商信息可以为 PLMN ID。当终端通过运营商 A 提供的 3GPP 接入技术入网后，在终端执行图 11 对应的流程时，可以判断非 3GPP 接入技术对应的 N3IWF 节点是否还是运营商 A，若是，才可以继续图 11 对应的流程。

35 在另一种可能的实现方式中，终端在非 3GPP 接入技术侧的安全上下文可以与其他信息绑定，例如签约信息，位置区信息等。示例性地，若终端从基站 A 的覆盖范围移动到了基站 B 的覆盖范围，若终端 A 的覆盖范围内支持非 3GPP 接入技术 C，基站 B 支持非 3GPP 接入技术 D，若终端通过非 3GPP 接入技术 C 接入了网络，当终端从基站 A

的覆盖范围移动到基站 B 的覆盖范围时,若终端的签约信息指示终端没有使用非 3GPP 接入技术 D 的权限,则终端不可以通过非 3GPP 接入技术 D 接入网络。

可选地,上述实施例中,AMF 节点可根据第一指示信息确定传输 NAS 消息所使用的接入技术,本申请的实施例还提供了三种 AMF 节点接收到 N2 消息后,确定 N2 消息,

5 或是 NAS 消息的所使用的接入技术的方法。

方式一、AMF 节点可根据 N2 消息的来源判断传输 N2 消息使用的接入技术,例如,根据源地址信息(比如 IP 地址)判断消息的来源,进而根据消息来源确定传输消息使用的接入技术。若 N2 消息来自使用 3GPP 接入技术的设备,例如基站,则确定可以使用 3GPP 接入技术对应的 NAS 序列号,即 AMF 节点可以使用自身保存的 3GPP 接入技术  
10 对应的上行 NAS 序列号对 N2 消息中携带的上行 NAS 序列号进行验证。若 N2 消息来自使用非 3GPP 接入技术的设备,例如 N3IWF 节点,则确定可以使用非 3GPP 接入技术对应的 NAS 序列号,即 AMF 节点可以使用自身保存的非 3GPP 接入技术对应的上行 NAS 序列号对 N2 消息中携带的上行 NAS 序列号进行验证。

方式二、终端可以通过显示的方式告知 AMF 节点 N2 消息的来源,例如,N2 消息  
15 中可以携带用于表示接入技术的比特位,例如 0 代表 3GPP 接入技术,1 代表为 3GPP 接入技术;或者,N2 消息可以携带字符串,例如“NR”代表 3GPP 接入技术,“wifi”代表非 3GPP 接入技术。

方式三、AMF 节点根据 N2 消息中的接入类型信息判断传输 N2 消息使用的接入技术,例如,接入类型信息为 rat type(接入类型)信息。若 N2 消息来自于 3GPP 接入  
20 技术的设备,例如基站,则 N2 消息中的接入类型指示为 3GPP 接入,则确定可以使用 3GPP 接入技术对应的 NAS 序列号,即 AMF 节点可以使用自身保存的 3GPP 接入技术对应的上行 NAS 序列号对 N2 消息中携带的上行 NAS 序列号进行验证。

相比于现有技术 AMF 节点不会对接收到的消息使用的接入技术进行区分,本申请的实施例通过上述两种方式可以使 AMF 节点确定接收到的消息使用的接入技术,从而  
25 选择接收到的消息使用的接入技术对应的 NAS 序列号。

可选地,在本申请实施例提供的另一种实现方式中,结合图 11 对应的方法流程,若步骤 1111 中,AMF 节点确定了非 3GPP 接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号,则 AMF 节点还可以更新 NAS 密钥,本申请的实施例提供了以下四种更新 NAS 密钥的方法。

30 方法一、用旧的 Kamf(oKamf)生成新的 Kamf(nKamf),在 AMF 节点生成 nKamf 后,再根据 nKamf 生成新的 NAS 密钥。

其中,Kamf 为 AMF 节点的根密钥。

$nKamf = KDF(oKamf, \text{新鲜性参数})$ ,新鲜性参数可以为 AMF 节点上一次接收到的上行 NAS 序列号,或者为 COUNT,或者为终端发给 AMF 节点的参数,或者为终端与  
35 AMF 节点协商的参数。

方法二、用 Kseaf 生成 nKamf,在 AMF 节点生成 nKamf 后,根据 nKamf 生成新的 NAS 密钥。

其中,Kseaf 为 AMF 节点的根密钥。

$nKamf = KDF(Kamf, \text{新鲜性参数})$ ,新鲜性参数可以为 AMF 节点上一次接收到的

上行 NAS 序列号，或者为计数器值。示例性地，计数器值的初始值为 0，AMF 节点每生成一次 NAS 密钥，计数器值加 1，用于表示 AMF 节点生成了新的密钥。

方法三、AMF 节点可以根据旧的 Kamf (oKamf) 和算法生成新的 NAS 密钥。

其中， $nKamf = KDF(oKamf, \text{算法 ID}, \text{选择的算法}, \text{其他参数})$ ，其中，算法 ID 为 AMF 选择的算法的标识符。选择的算法为终端和 AMF 之间对 NAS 消息进行安全保护所使用的算法。

其他参数为用于表示接入技术的参数。具体的，其他参数可以为比特位的形式或者 ID 的形式，比如可以规定：3GPP 接入技术对应的其他参数为 0x01，非 3GPP 接入技术对应的其他参数为 0x10，固网接入技术为 0x11。

其他参数还可以为计数器值。示例性地，计数器值的初始值为 0，AMF 节点每生成一次 NAS 密钥，计数器值加 1，用于表示 AMF 节点生成了新的密钥。

方法四、根据旧的 NAS 密钥生成新的 NAS 密钥。

其中新的 NAS 密钥 = (旧的 NAS 密钥, 计数器值)。示例性地，计数器值的初始值为 0，AMF 节点每生成一次 NAS 密钥，计数器值加 1，用于表示 AMF 节点生成了新的密钥。

需要说明的是，若 AMF 节点生成了新的 NAS 密钥，可以通过图 11 对应的实施例中的 NAS SMC 消息，以显示的方式指示终端更新密钥。终端接收到更新密钥的指示后，可以通过上述四种方法之一更新密钥。其中，终端更新密钥的方法和 AMF 节点更新 NAS 密钥的方法相同，AMF 节点和终端中均预先被配置了更新 NAS 密钥的方法。

可选地，在 AMF 节点与终端之间切换使用的接入技术时可以更新 NAS 密钥，或者由同时使用多种接入技术切换至只使用一种接入技术的情况下，或者减少同时使用的接入技术的数量时，也可以更新 NAS 密钥。

采用该方法，通过进行密钥更新，即使攻击者获得了 AMF 节点与终端同时使用多种接入技术进行通信时的 NAS 密钥，攻击者也无法获取终端与 AMF 节点后续使用单一的接入技术进行通信时的明文，提高了安全性。

需要说明的是，本申请的实施例均以第一接入技术为非 3GPP 接入技术，第二接入技术为 3GPP 接入技术为例进行说明。实际应用中，也可以是：第一接入技术为 3GPP 接入技术，第二接入技术为非 3GPP 接入技术。在第一接入技术和第二接入技术分别为终端支持的两种不同的接入技术的情况下，均可采用上述实施例提供的方法，或者，在终端通过多种接入技术接入核心网设备的情况下，也可采用上述实施例提供的方法。

示例性地，若第一接入技术为固网接入技术，第二接入技术为非 3GPP 接入技术，实现方法与上述实施例中描述的方法类似，图 11 对应的实施例可以应用于终端已经通过 3GPP 接入技术接入 AMF 节点，之后通过固网接入技术接入同一个 AMF 节点的场景中，图 11 的流程可以替换为终端通过固网接入技术接入 AMF 节点的注册流程，在注册流程中的安全保护的方法与图 11 的实施例描述的终端通过非 3GPP 接入技术接入 AMF 节点的安全保护方法类似。

上述主要从不同网元之间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，终端和核心网设备为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。结合本申请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。本领域技术人员可以对每个特定的应用来使用不同的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实施例的技术方案的范围。

5       本申请实施例可以根据上述方法示例对终端和核心网设备等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处理单元中。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。需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

10       在采用集成的单元的情况下，图 12 示出了本申请实施例中提供的又一种装置的示意性框图。该装置 1200 可以以软件的形式存在，也可以为终端，还可以为终端中的芯片。装置 1200 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，例如，处理单元 1202 用于支持装置 1200 执行图 5 中的步骤 501 至步骤 502，图 10 中的步骤 1001，图 11 中的步骤 1101、步骤 1105、步骤 1113、步  
15       骤 1117 和步骤 1118，和/或用于本文所描述的技术的其它过程。通信单元 1203 用于支持装置 1200 和其他网元（例如核心网设备，N3IWF 节点）之间的通信。例如，通信单元 1203 用于支持装置 1200 执行图 10 中的步骤 1002、步骤 1003 和步骤 1007，以及图 11 中的步骤 1102、步骤 1103、步骤 1104、步骤 1106、步骤 1112、步骤 1114、步骤 1116 以及步骤 1119。装置 1200 还可以包括存储单元 1201，用于存储装置 1200 的  
20       程序代码和数据。

其中，处理单元 1202 可以是处理器或控制器，例如可以是中央处理器（Central Processing Unit, CPU），通用处理器，数字信号处理器（Digital Signal Processor, DSP），专用集成电路（Application-Specific Integrated Circuit, ASIC），现场可编程门阵列（Field Programmable Gate Array, FPGA）或者其他可编程逻辑器件、  
25       晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。通信单元 1203 可以是收发器、收发电路或通信接口等。存储单元 1201 可以是存储器。

30       当处理单元 1202 为处理器，通信单元 1203 为收发器，存储单元 1201 为存储器时，本申请实施例所涉及的装置 1200 可以为图 13 所示的终端。

图 13 示出了本申请实施例中所涉及的终端的一种可能的设计结构的简化示意图。所述终端 1300 包括发射器 1301，接收器 1302 和处理器 1303。其中，处理器 1303 也可以为控制器，图 13 中表示为“控制器/处理器 1303”。可选的，所述终端 1300 还可以包括调制解调处理器 1305，其中，调制解调处理器 1305 可以包括编码器 1306、  
35       调制器 1307、解码器 1308 和解调器 1309。

在一个示例中，发射器 1301 调节（例如，模拟转换、滤波、放大和上变频等）该输出采样并生成上行链路信号，该上行链路信号经由天线发射给上述实施例中所述的基站。在下行链路上，天线接收上述实施例中基站发射的下行链路信号。接收器 1302 调节（例如，滤波、放大、下变频以及数字化等）从天线接收的信号并提供输入采样。

在调制解调处理器 1305 中, 编码器 1306 接收要上行链路上发送的业务数据和信令消息, 并对业务数据和信令消息进行处理(例如, 格式化、编码和交织)。调制器 1307 进一步处理(例如, 符号映射和调制)编码后的业务数据和信令消息并提供输出采样。解调器 1309 处理(例如, 解调)该输入采样并提供符号估计。解码器 1308 处理(例如, 解交织和解码)该符号估计并提供发送给终端 1300 的已解码的数据和信令消息。编码器 1306、调制器 1307、解调器 1309 和解码器 1308 可以由合成的调制解调处理器 1305 来实现。这些单元根据无线接入网采用的无线接入技术(例如, LTE 及其他演进系统的接入技术)来进行处理。需要说明的是, 当终端 1300 不包括调制解调处理器 1305 时, 调制解调处理器 1305 的上述功能也可以由处理器 1303 完成。

10 处理器 1303 对终端 1300 的动作进行控制管理, 用于执行上述本申请实施例中由终端 1300 进行的处理过程。例如, 处理器 1303 还用于执行图 5, 以及图 10 至图 11 所示方法中涉及终端的处理过程和/或本申请所描述的技术方案的其他过程。

进一步的, 终端 1300 还可以包括存储器 1304, 存储器 1304 用于存储用于终端 1300 的程序代码和数据。

15 在采用集成的单元的情况下, 图 14 示出了本申请实施例中提供的另一种装置的示意性框图。该装置可以以软件的形式存在, 也可以为核心网设备, 还可以为核心网设备中的芯片。该装置 1400 包括: 处理单元 1402 和通信单元 1403。处理单元 1402 用于对装置 1400 的动作进行控制管理, 例如, 处理单元 1402 用于支持装置 1400 执行图 9 中的步骤 901 和步骤 902, 图 10 中的步骤 1004 至步骤 1006, 以及图 11 中的步骤 1109 至步骤 1111, 和/或用于本文所描述的技术的其它过程。通信单元 1403 用于支持装置 1400 和其他网元(例如终端, N3IWF 节点)之间的通信。例如, 通信单元 1403 用于支持装置 1400 执行图 10 中的步骤 1002 至步骤 1002 和步骤 1007, 图 11 中的步骤 1108、步骤 1112、步骤 1114 和步骤 1115。装置 1400 还可以包括存储单元 1401, 用于存储装置 1400 的程序代码和数据。

25 其中, 处理单元 1402 可以是处理器或控制器, 例如可以是 CPU, 通用处理器, DSP, ASIC, FPGA 或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框, 模块和电路。所述处理器也可以是实现计算功能的组合, 例如包含一个或多个微处理器组合, DSP 和微处理器的组合等等。通信单元 1403 可以是通信接口, 其中, 该通信接口是统称, 在具体实现中, 该通信接口可以包括多个接口, 例如可以包括: 核心网设备与终端之间的接口, 核心网设备与 N3IWF 节点之间的接口和/或其他接口。存储单元 1401 可以是存储器。

当处理单元 1402 为处理器, 通信单元 1403 为通信接口, 存储单元 1401 为存储器时, 本申请实施例所涉及的装置 1400 的结构可以是如图 15 所示的核心网设备的结构。

35 图 15 示出了本申请实施例提供的核心网设备的一种可能的结构示意图。

如图 15 所示, 该核心网设备 1500 包括: 处理器 1502、通信接口 1503、存储器 1501。可选的, 核心网设备 1500 还可以包括总线 1504。其中, 通信接口 1503、处理器 1502 以及存储器 1501 可以通过总线 1504 相互连接; 总线 1504 可以是 PCI 总线或 EISA 总线等。所述总线 1504 可以分为地址总线、数据总线、控制总线等。为便于表

示，图 15 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。

结合本申请公开内容所描述的方法或者算法的步骤可以硬件的方式来实现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于随机存取存储器（Random Access Memory, RAM）、闪存、只读存储器（Read Only Memory, ROM）、可擦除可编程只读存储器（Erasable Programmable ROM, EPROM）、电可擦可编程只读存储器（Electrically EPROM, EEPROM）、寄存器、硬盘、移动硬盘、只读光盘（CD-ROM）或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于核心网接口设备中。当然，处理器和存储介质也可以作为分立组件存在于核心网接口设备中。

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

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

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

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘、硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述的方法。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，在本申请揭露的技术范围内的变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。