

安全策略处理方法以及通信设备

技术领域

本申请实施例涉及通信领域，尤其涉及一种安全策略处理方法和通信设备。

5

背景技术

用户面安全按需保护机制是第五代移动通信技术（5th generation mobile communication technology, 5G）网络中的一种安全机制，该用户面安全按需保护包含用户面加密保护和用户面完整性保护。该用户面安全按需保护机制要求接入网设备根据从核心网设备接收到的用户面安全策略判断是否为终端设备开启用户面加密保护和/或完整性保护。

目前，需要将前述用户面安全按需保护机制应用于第四代移动通信技术（the 4th generation mobile communication technology, 4G）网络中。由于，4G网络中存在未升级的接入网设备和终端设备，前述未升级的接入网设备和未升级的终端设备不支持用户面安全按需保护，因此，当前述未升级的接入网设备和未升级的终端设备收到关于用户面安全按需保护的信元（例如，用户面安全策略）时，可能会因为无法识别前述关于用户面安全按需保护的信元而丢弃或者无法处理该信元。

如何在同时存在升级和未升级的接入网设备/终端设备的4G网络中，实现用户面安全按需保护的机制，是当前标准中亟需解决的问题。

发明内容

本申请实施例提供了一种安全策略处理方法和通信设备，用于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，降低传输复杂度，提升数据传输效率。

第一方面，本申请实施例提供了一种安全策略处理方法，该安全策略处理方法例如可以应用于切换（Handover）、无线资源控制连接恢复（Radio Resource Control Connection Resume, RRC Connection Resume）或 RRC 连接重建（RRC Connection Reestablishment）等流程中。在该方法中，目标接入网设备接收来自源接入网设备的消息 001，该消息 001 包括指示信息 011。然后，该目标接入网设备在该指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，该用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

一种可能的实现方式中，前述源接入网设备可以为终端设备初始接入时为该终端设备提供服务的接入网设备，或者，该源接入网设备为切换、RRC 连接恢复或 RRC 连接重建流程之前，为该终端设备提供服务的接入网设备。该目标接入网设备是切换、RRC 连接恢复或 RRC 连接重建流程之后，为该终端设备提供服务的接入网设备。一般地前述源接入网设备与目标接入网设备之间会有关于终端设备的上下文的传输。

本申请中，由于目标接入网设备能够根据指示信息011确定终端设备是否支持用户面安

全按需保护，若该终端设备支持用户面安全按需保护，该目标接入网设备才向移动管理实体发送用户面安全策略021。避免了当终端设备不支持用户面安全按需保护，且，移动管理实体在未从目标接入网设备收到用户面安全策略时，移动管理实体向该目标接入网设备发送用户面安全策略，而造成目标接入网设备即使收到该用户面安全策略也无法为该终端设备开启用户面安全按需保护的情况。因此，有利于减少移动管理实体向目标接入网设备发送该目标接入网设备不需要的信元，进而有利于简化传输复杂度。

在一种可选的实施方式中，该前述目标接入网设备和源接入网设备为演进型基站 eNB。示例性的，前述目标接入网设备为目标 eNB，前述源接入网设备为源 eNB。

在一种可选的实施方式中，当该目标接入网设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 为该目标接入网设备构建的用户面安全策略 021-1。

在一种可选的实施方式中，该方法还包括：该目标接入网设备确定与该终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；该目标接入网设备构建匹配该用户面安全激活状态的该用户面安全策略 021-1。

由于目标接入网设备未从源接入网设备中收到用户面安全按需保护策略，但是，该指示信息 011 又指示终端设备支持用户面安全按需保护，说明该源接入网设备不支持用户面安全按需保护。此时，目标接入网设备可以采用默认的方式（可以理解为，未升级的方式）为终端设备决策是否开启用户面加密保护和/或用户面完整性保护。其中，默认的方式（或未升级的方式）例如，可以指示为终端设备开启用户面加密保护以及不开启用户面完整性保护。因此，若该目标接入网设备构建的用户面安全策略 021-1 能够匹配终端设备的用户面安全激活状态，则当该目标接入网设备收到与前述用户面安全策略 021-1 相同的用户面安全策略时，该目标接入网设备便可以重新激活终端设备。

在一种可选的实施方式中，该用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，该用户面加密保护策略为需要开启或推荐开启，该用户面完整性保护策略为不需要开启或推荐开启。

本实施方式中，提出了前述用户面安全策略 021-1 可能的实施方式。示例性的，若一个用户面安全策略采用{用户面加密保护策略，用户面完整性保护策略}这种形式表达，则用户面安全策略 021-1 具体可以为如下任意一种实现方式：{需要开启（required），不需要开启（not needed）}；{需要开启（required），推荐开启（preferred）}；{推荐开启（preferred），不需要开启（not needed）}；{推荐开启（preferred），推荐开启（preferred）}。

在一种可选的实施方式中，当该目标接入网设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 可以为预配置在该目标接入网设备中的用户面安全策略 021-2。

本实施方式中，提出当指示信息 011 指示该终端设备支持用户面安全按需保护时，但是，该目标接入网设备没有从源接入网设备收到用户面安全策略时，该目标接入网设备可以根据预配置在本地的用户面安全策略确定所述终端设备对应的用户面安全策略。

在一种可选的实施方式中，该消息 001 还包括该终端设备的 N 个演进无线接入承载（E-UTRAN radio access bearer，E-RAB）的标识，该 N 为大于等于 1 的整数；该路径切换

请求 031 中还包括该 N 个 E-RAB 的标识。

本实施方式中,提出前述用户面安全策略 021 可以是承载粒度的安全策略,例如,E-RAB 粒度的安全策略。具体地,可以将 E-RAB 的标识和该 E-RAB 对应的用户面安全策略 021 一起携带于路径切换请求中发送至移动管理实体。相应的,当该移动管理实体收到前述用户面安全策略 021 和 E-RAB 的标识时,该移动管理实体可以确定该用户面安全策略 021 是 E-RAB 粒度的安全策略,并且,该用户面安全策略 021 是该 E-RAB 的标识对应的用户面安全策略。这样的实施方式中,接入网设备可以为终端设备对应的各个 E-RAB 决策是否开启用户面加密保护和/或完整性保护,有利于精细化管理用户面安全策略。

在一种可选的实施方式中,该路径切换请求 031 包括 N 个该用户面安全策略 021-2,其中,该 N 个演进无线接入承载的标识中每个无线接入承载的标识分别与一个用户面安全策略 021-2 对应。在该实施方式中,当目标接入网设备从源接入网设备接收到 N 个 E-RAB 的标识时,目标接入网设备在向移动管理实体发送的路径切换请求 031 中携带 N 个对应关系,每个对应关系包括一个 E-RAB 的标识和一个用户面安全策略 021-2。这种情况下,可以避免对现网中移动管理实体的改动,移动管理设备即可知道每个 E-RAB 的标识对应的用户面安全策略。

在一种可选的实施方式中,该目标接入网设备向该移动管理实体发送携带该用户面安全策略 021 的路径切换请求 031 之后,该方法还包括:该目标接入网设备从该移动管理实体接收路径切换响应 041,其中,该路径切换响应 041 携带用户面安全策略 022;该目标接入网设备将该用户面安全策略 022 存储于该终端设备的上下文中。

本实施方式中,若目标接入网设备向移动管理实体发送的是用户面安全策略 021,而收到的是用户面安全策略 022,则说明该移动管理实体中的用户面安全策略 022 与目标接入网设备中存储的移动管理实体 021 是不一致的。于是,该目标接入网设备需要采用前述用户面安全策略 022 更新存储于终端设备的上下文中的用户面安全策略 021。

在一种可选的实施方式中,该方法还包括:如果该终端设备当前的用户面安全激活状态与该用户面安全策略 022 不匹配,则该目标接入网设备根据该用户面安全策略 022 重新开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护,该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。例如,该目标接入网设备与该终端设备当前的用户面加密保护开启,完整性保护不开启,而该用户面安全策略 022 为用户面加密保护需要开启(required),用户面完整性保护也是需要开启(required),则该目标接入网设备需要根据该用户面安全策略 022 的要求开启自身与该终端设备之间的用户面加密保护和用户面完整性保护。

在一种可选的实施方式中,该方法还包括:在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下,该目标接入网设备向该移动管理实体发送未携带用户面安全策略的路径切换请求 032;该目标接入网设备从该移动管理实体接收未携带用户面安全策略的路径切换响应 042。

相比于传统技术中,移动管理实体在收到未携带用户面安全策略的路径切换请求之后,该移动管理实体为了尽可能让 4G 网络中的接入网设备和终端设备能够开启用户面完整性

保护，便会向目标接入网设备发送用户面安全策略。此时，目标接入网设备和终端设备很可能无法使用该用户面安全策略。

而本实施方式中，当指示信息011指示终端设备支持用户面安全按需保护时，该目标接入网设备会向移动管理实体发送构建的用户面安全策略021-1或预配置的用户面安全策略021-2。由此可知，若指示信息011指示终端设备不支持用户面安全按需保护，则该目标接入网设备不会向移动管理实体发送用户面安全策略，相应的，移动管理实体也无法从目标接入网设备收到用户面安全策略。此时，移动管理实体可以推断出终端设备不支持用户面安全按需保护，即使向该目标接入网设备提供了用户面安全策略，该目标接入网设备也无法使用该用户面安全策略为该终端设备开启用户面完整性保护。因此，该实施方式设置移动管理实体在收到未携带用户面安全策略的路径切换请求时，向目标接入网设备发送未携带用户面安全策略的路径切换响应，即不向目标接入网设备提供用户面安全策略。因此，降低了目标接入网设备收到不能使用的信元的几率，降低了目标接入网设备与移动管理实体之间的数据传输复杂度。

在一种可选的实施方式中，该方法还包括：在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，该目标接入网设备向该移动管理实体发送未携带用户面安全策略的路径切换请求 033，该路径切换请求 033 携带该指示信息 011；目标接入网设备从该移动管理实体接收携带用户面安全策略 023 的路径切换响应 043；该目标接入网设备将该用户面安全策略 023 存储于该终端设备的上下文中。

在一种可选的实施方式中，该携带用户面安全策略 023 的路径切换响应 043 还携带指示信息 012，其中，该指示信息 012 用于指示终端设备支持与接入网设备之间的用户面安全按需保护。

本实施方式中，若源接入网设备是恶意的，它可以对指示信息011进行恶意篡改，使指示信息011指示终端设备不支持用户面安全按需保护，这将导致目标接入网设备无法向移动管理实体发送安全策略，也无法为终端设备开启安全保护，从而导致降质攻击。因此，可以使目标接入网设备在判断不向移动管理设备发送用户面安全策略后，额外发送指示信息011，以使得移动管理实体可以判断指示信息011是否被篡改，在移动管理实体判断该指示信息011被篡改后，便会向目标接入网设备发送用户面安全策略。这样，可以避免上述降质攻击。

在一种可选的实施方式中，该方法还包括：在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，该目标接入网设备向该移动管理实体发送未携带用户面安全策略的路径切换请求 035，该路径切换请求 035 携带该指示信息 011；该目标接入网设备从该移动管理实体接收未携带用户面安全策略和指示信息的路径切换响应 045。

本实施方式中，在目标接入网设备向移动管理实体发送指示信息 011 之后，若该目标接入网设备收到的路径切换响应 045 未携带用户面安全策略，则说明该指示信息 011 与移动管理实体中存储的指示信息是一致的，该目标接入网设备收到的指示信息 011 未被篡改。因此，有利于避免目标接入网设备和移动管理实体之间的通信遭受降质攻击。

在一种可选的实施方式中，该方法还包括：如果该终端设备当前的用户面安全激活状态与该用户面安全策略023不匹配，则该目标接入网设备根据该用户面安全策略023开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护，该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

在一种可选的实施方式中，当满足如下任意一项时，用户面安全策略与用户面安全激活状态不匹配；

当该用户面加密保护策略指示需要开启，且，该终端设备的用户面安全激活状态为加密保护未开启；

或者，当该用户面加密保护策略指示不需要开启，且，该终端设备的用户面安全激活状态为加密保护开启；

或者，当该用户面完整性保护策略指示需要开启，且，该终端设备的用户面安全激活状态为完整性保护未开启；

或者，当该用户面完整性保护策略指示不需要开启，且，该终端设备的用户面安全激活状态为完整性保护开启。

在一种可选的实施方式中，该指示信息 011 由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。

本实施方式中，由于，无论接入网设备是否升级（即接入网设备是否支持用户面安全按需保护），该接入网设备均能够识别并转发终端设备的演进分组系统安全能力（例如，UE 演进分组系统安全能力），因此，将指示信息 011 携带于终端设备的演进分组系统安全能力中能够保证指示信息 011 在接入网设备之间（例如，支持用户面安全按需保护的接入网设备与不支持用户面安全按需保护的接入网设备之间）或接入网设备与核心网设备之间（不支持用户面安全按需保护的接入网设备与移动管理实体之间）传输时不丢失。而传统技术中，重新定义的一个指示信息用于指示终端设备是否支持用户安全按需保护，该重新定义的指示信息不能够被未升级的接入网设备识别。也就是说，不支持用户面安全按需保护的接入网设备无法识别前述重新定义的指示信息，若该不支持用户面安全按需保护的接入网设备收到前述重新定义的指示信息，则该不支持用户面安全按需保护的接入网设备将丢弃前述重新定义的指示信息而无法发送给其他的接入网设备或核心网设备（例如，移动管理实体等）。

在一种可选的实施方式中，该消息001为切换请求或上下文检索响应。

第二方面，本申请实施例提供了一种通信设备，包括接收模块、处理模块和发送模块。其中，接收模块，用于接收来自源接入网设备的消息 001，该消息 001 包括指示信息 011；处理模块，用于在该指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，控制发送模块向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，该用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

在一种可选的实施方式中，该接入网设备为演进型基站 eNB。

在一种可选的实施方式中，当该通信设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 为该通信设备构建的用户面安全策略 021-1。

5 在一种可选的实施方式中，该处理模块，还用于：确定与该终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；构建匹配该用户面安全激活状态的该用户面安全策略 021-1。

在一种可选的实施方式中，该用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，该用户面加密保护策略为需要开启或推荐开启，该用户面完整性保护策略为不需要开启或推荐开启。

10 在一种可选的实施方式中，当该通信设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 为预配置在该通信设备中的用户面安全策略 021-2。

在一种可选的实施方式中，该消息 001 还包括该终端设备的 N 个演进无线接入承载的标识，该 N 为大于等于 1 的整数；该路径切换请求 031 中还包括该 N 个演进无线接入承载的标识。

15 在一种可选的实施方式中，该路径切换请求 031 包括 N 个该用户面安全策略 021-2，其中，该 N 个演进无线接入承载的标识中每个无线接入承载的标识分别与一个用户面安全策略 021-2 对应。

在一种可选的实施方式中，该接收模块，还用于从该移动管理实体接收路径切换响应 041，其中，该路径切换响应 041 携带用户面安全策略 022；该通信设备还包括存储模块；该
20 存储模块，用于将该用户面安全策略 022 存储于该终端设备的上下文中。

在一种可选的实施方式中，该处理模块，还用于：当该终端设备当前的用户面安全激活状态与该用户面安全策略 022 不匹配时，根据该用户面安全策略 022 开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护，该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启
25 的状态。

在一种可选的实施方式中，该发送模块，还用于：在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，向该移动管理实体发送未携带用户面安全策略的路径切换请求 032；该接收模块，还用于从该移动管理实体接收未携带用户面安全策略的路径切换响应 042。

30 在一种可选的实施方式中，该发送模块，还用于：在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，向该移动管理实体发送未携带用户面安全策略的路径切换请求 033，该路径切换请求 033 携带该指示信息 011；该接收模块，还用于从该移动管理实体接收携带用户面安全策略 023 的路径切换响应 043；该通信设备还包括存储模块；该存储模块，用于将该用户面安全策略 023 存储于该终端设备的上下文
35 中。

在一种可选的实施方式中，该携带用户面安全策略 023 的路径切换响应 043 还携带指示信息 012，其中，该指示信息 012 用于指示终端设备支持与接入网设备之间的用户面安

全按需保护。

在一种可选的实施方式中，该处理模块，还用于：当该终端设备当前的用户面安全激活状态与该用户面安全策略023不匹配时，该用户面安全策略023开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护，该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

在一种可选的实施方式中，该指示信息 011 由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。

10 在一种可选的实施方式中，该消息 001 为切换请求或上下文检索响应。

第三方面，本申请实施例提供了一种安全策略处理方法，该安全策略处理方法可以应用于初始接入、切换、RRC连接恢复或RRC连接重建等流程中。在该方法中，移动管理实体获取指示信息013，该指示信息013用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护；该移动管理实体根据该指示信息013确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略024，该用户面安全策略024用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

本申请中，由于移动管理实体能够根据指示信息013确定终端设备是否支持用户面安全按需保护，并在该终端设备支持用户面安全按需保护时才进一步考虑向为该终端设备提供服务的接入网设备发送用户面安全策略。因此，也有利于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。而传统技术中，移动管理实体没有根据指示信息013进行判断的逻辑。传统技术中的移动管理实体是根据是否收到了来自接入网设备的用户面安全策略来进行判断决策。若该移动管理实体没有收到来自接入网设备的用户面安全策略，则该移动管理实体便会向接入网设备发送用户面安全策略。

在一种可选的实施方式中，该指示信息 013 携带于路径切换请求 034 中，该为该终端设备提供服务的接入网设备为目标接入网设备。该移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，包括：当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该路径切换请求 034 未携带用户面安全策略时，该移动管理实体向该目标接入网设备发送携带该用户面安全策略 024 的路径切换响应 044。

30 在一种可选的实施方式中，该指示信息 013 携带于非接入层消息中，该为该终端设备提供服务的接入网设备为源接入网设备；该移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，包括：当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护时，该移动管理实体向该源接入网设备发送该用户面安全策略 024。

35 在一种可选的实施方式中，该移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024 之前，该方法还包括：该移动管理实体获取指示信息 051，该指示信息 051 用于指示为该终端设备提供服务的接入网设备是否

支持与终端设备之间的用户面安全按需保护；该移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，包括：该移动管理实体根据该指示信息 013 和该指示信息 051 确定是否向为该终端设备提供服务的接入网设备发送该用户面安全策略 024。

5 在一种可选的实施方式中，该指示信息 013 携带于路径切换请求中；或者，该指示信息 013 携带于非接入层消息中；该移动管理实体根据该指示信息 013 和该指示信息 051 确定是否向为该终端设备提供服务的接入网设备发送该用户面安全策略 024，包括：当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该指示信息 051 指示为该终端设备提供服务的接入网设备支持与该终端设备之间的用户面安全按需保护时，该移动管理
10 实体向该接入网设备发送该用户面安全策略 024。

 在一种可选的实施方式中，该指示信息 051 为该移动管理实体从该接入网设备接收的指示信息 051-1；或者，该指示信息 051 为该移动管理实体从网络管理设备获取的指示信息 051-2。

 在一种可选的实施方式中，该移动管理实体获取指示信息 013 之后，该方法还包括：
15 该移动管理实体从归属用户服务器接收该终端设备的签约数据；当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该签约数据包括该用户面安全策略 024 时，该移动管理实体存储该用户面安全策略 024。

 在一种可选的实施方式中，该移动管理实体获取指示信息 013 之后，该方法还包括：
20 该移动管理实体从归属用户服务器接收该终端设备的签约数据；当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该签约数据不包括用户面安全策略时，该移动管理实体根据预配置的用户面安全策略 024-1 确定该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。

 在一种可选的实施方式中，该移动管理实体获取指示信息 051 之后，该方法还包括：
25 该移动管理实体从归属用户服务器接收该终端设备的签约数据；当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护，且，该签约数据包括该用户面安全策略 024 时，该移动管理实体存储该用户面安全策略 024。

 在一种可选的实施方式中，该移动管理实体获取指示信息 051 之后，该方法还包括：
30 该移动管理实体从归属用户服务器接收该终端设备的签约数据；当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护，且，该签约数据不包括用户面安全策略时，该移动管理实体根据预配置的用户面安全策略 024-2 确定该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。

 在一种可选的实施方式中，该指示信息 013 由该终端设备的演进分组系统安全能力的
35 部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。

 第四方面，本申请实施例提供了一种通信设备，包括处理模块，用于：获取指示信息

013, 该指示信息013用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护; 根据该指示信息013确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略024, 该用户面安全策略024用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

5 在一种可选的实施方式中, 该指示信息 013 携带于路径切换请求 034 中, 该为该终端设备提供服务的接入网设备为目标接入网设备; 该处理模块, 具体用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护, 且, 该路径切换请求 034 未携带用户面安全策略时, 控制收发模块向该目标接入网设备发送携带该用户面安全策略024 的路径切换响应 044。

10 在一种可选的实施方式中, 该指示信息 013 携带于非接入层消息中, 该为该终端设备提供服务的接入网设备为源接入网设备; 该处理模块, 具体用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护时, 控制收发模块向该源接入网设备发送该用户面安全策略 024。

在一种可选的实施方式中, 该处理模块, 还用于:

15 获取指示信息 051, 该指示信息 051 用于指示为该终端设备提供服务的接入网设备是否支持与终端设备之间的用户面安全按需保护;

根据该指示信息 013 和该指示信息 051 确定是否控制收发模块向为该终端设备提供服务的接入网设备发送该用户面安全策略 024。

20 在一种可选的实施方式中, 该指示信息 013 携带于路径切换请求中; 或者, 该指示信息 013 携带于非接入层消息中;

当该指示信息 013 指示该终端设备支持用户面安全按需保护, 且, 该指示信息 051 指示为该终端设备提供服务的接入网设备支持与该终端设备之间的用户面安全按需保护时, 控制收发模块向该接入网设备发送该用户面安全策略 024。

25 在一种可选的实施方式中, 该指示信息 051 为该移动管理实体从该接入网设备接收的指示信息 051-1; 或者, 该指示信息 051 为该移动管理实体从网络管理设备获取的指示信息 051-2。

在一种可选的实施方式中, 该收发模块, 用于从归属用户服务器接收该终端设备的签约数据。当该指示信息 013 指示该终端设备支持用户面安全按需保护, 且, 该签约数据包括该用户面安全策略 024 时, 存储模块, 存储该用户面安全策略 024。

30 在一种可选的实施方式中, 该收发模块, 用于从归属用户服务器接收该终端设备的签约数据。当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护, 且, 该签约数据不包括用户面安全策略时, 处理模块根据预配置的用户面安全策略 024-1 确定该用户面安全策略 024, 并将该用户面安全策略 024 存储于该终端设备的上下文中。

35 在一种可选的实施方式中, 收发模块, 用于从归属用户服务器接收该终端设备的签约数据; 当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护, 且, 该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护, 且, 该签约数据包括该用户面安全策略 024 时, 存储模块存储该用户面安全策略 024。

在一种可选的实施方式中，收发模块，用于从归属用户服务器接收该终端设备的签约数据；当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护，且，该签约数据不包括用户面安全策略时，处理模块根据预配置的用户面安全策略 024-2 确定该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。

在一种可选的实施方式中，该指示信息 013 由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。

第五方面，本申请实施例提供了一种通信设备，该通信设备可以是前述实施方式中的接入网设备，也可以是该接入网设备内的芯片。该通信设备可以包括处理模块和收发模块。当该通信设备是接入网设备时，该处理模块可以是处理器，该收发模块可以是收发器；该接入网设备还可以包括存储模块，该存储模块可以是存储器；该存储模块用于存储指令，该处理模块执行该存储模块所存储的指令，以使该接入网设备执行第一方面或第一方面的任一种实施方式中的方法。当该通信设备是接入网设备内的芯片时，该处理模块可以是处理器，该收发模块可以是输入/输出接口、管脚或电路等；该处理模块执行存储模块所存储的指令，以使该接入网设备执行第一方面或第一方面的任一种实施方式中的方法。该存储模块可以是该芯片内的存储模块（例如，寄存器、缓存等），也可以是该接入网设备内的位于该芯片外部的存储模块（例如，只读存储器、随机存取存储器等）。

第六方面，本申请实施例提供了一种通信设备，该通信设备可以是前述实施方式中的移动管理实体，也可以是该移动管理实体内的芯片。该通信设备可以包括处理模块和收发模块。当该通信设备是移动管理实体时，该处理模块可以是处理器，该收发模块可以是收发器；该移动管理实体还可以包括存储模块，该存储模块可以是存储器；该存储模块用于存储指令，该处理模块执行该存储模块所存储的指令，以使该移动管理实体执行第三方面或第三方面的任一种实施方式中的方法。当该通信设备是移动管理实体内的芯片时，该处理模块可以是处理器，该收发模块可以是输入/输出接口、管脚或电路等；该处理模块执行存储模块所存储的指令，以使该移动管理实体执行第三方面或第三方面的任一种实施方式中的方法。该存储模块可以是该芯片内的存储模块（例如，寄存器、缓存等），也可以是该移动管理实体内的位于该芯片外部的存储模块（例如，只读存储器、随机存取存储器等）。

第七方面，本申请提供了一种通信装置，该装置可以是集成电路芯片。该集成电路芯片包括处理器。该处理器与存储器耦合，该存储器用于存储程序或指令，当该程序或指令被该处理器执行时，使得该通信装置执行如第一方面或第一方面的任一种实施方式中的方法。

第八方面，本申请提供了一种通信装置，该装置可以是集成电路芯片。该集成电路芯片包括处理器。该处理器与存储器耦合，该存储器用于存储程序或指令，当该程序或指令被该处理器执行时，使得该通信设备执行如第三方面或第三方面的任一种实施方式中的方法。

第九方面，本申请实施例提供了一种计算机可读存储介质，包括指令，当该指令在计

算机上运行时，以使得计算机执行如前述第一方面以及前述第一方面的各种实施方式中的任一种实施方式所介绍的方法。

第十方面，本申请实施例提供了一种计算机可读存储介质，包括指令，当该指令在计算机上运行时，以使得计算机执行如前述第三方面以及前述第三方面的各种实施方式中的任一种实施方式所介绍的方法。

第十一方面，本申请实施例提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得该计算机执行如前述第一方面以及前述第一方面的各种实施方式中的任一种实施方式所介绍的方法。

第十二方面，本申请实施例提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得该计算机执行如前述第三方面以及前述第三方面的各种实施方式中的任一种实施方式所介绍的方法。

第十三方面，本申请实施例提供了一种通信系统，该通信系统包括移动管理实体以及上述第一方面以及第一方面的任一种实施方式中的目标接入网设备。

在一种可选的实施方式中，该通信系统还包括源接入网设备和终端设备。

第十四方面，本申请实施例提供了一种通信系统，该通信系统包括接入网设备以及上述第三方面以及第三方面的任一种实施方式中的移动管理实体。

在一种可选的实施方式中，该通信系统还包括源接入网设备和终端设备。

从以上技术方案可以看出，本申请实施例具有以下优点：

本申请实施例中，由于目标接入网设备能够根据指示信息011确定终端设备是否支持用户面安全按需保护，若该终端设备支持用户面安全按需保护，该目标接入网设备才向移动管理实体发送用户面安全策略021。避免了当终端设备不支持用户面安全按需保护，且，移动管理实体在未从目标接入网设备收到用户面安全策略时，移动管理实体向该目标接入网设备发送用户面安全策略，而造成目标接入网设备即使收到该用户面安全策略也无法为该终端设备开启用户面安全按需保护的情况。因此，有利于减少移动管理实体向目标接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。

另外，由于移动管理实体能够根据指示信息013确定终端设备是否支持用户面安全按需保护，并在该终端设备支持用户面安全按需保护时才进一步考虑向为该终端设备提供服务的接入网设备发送用户面安全策略。因此，也有利于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例。

图1为本申请中安全策略处理方法适用的4G网络架构图；

图2为本申请中安全策略处理方法的一个实施例的示意图；

图3为本申请中安全策略处理方法在切换场景下的一个示例图；

图4为本申请中安全策略处理方法的另一个实施例的示意图；

图 5 为本申请中安全策略处理方法的另一个实施例的示意图；

图 6 为本申请中安全策略处理方法在 RRC 连接恢复场景下的一个示例图；

图 7 为本申请中安全策略处理方法在接入场景下的一个示例图；

图 8 为本申请中提出的通信设备的一个实施例示意图；

5 图 9 为本申请中提出的通信设备的另一个实施例示意图；

图 10 为本申请中提出的通信设备的另一个实施例示意图；

图 11 为本申请中提出的通信设备的另一个实施例示意图。

具体实施方式

10 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”以及相应术语标号等（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
15 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含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

本申请实施例提供了一种安全策略处理方法和通信设备，用于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，降低传输复杂度，提升数据传输效率。
20 下面先对本申请提出的安全策略处理方法适用的系统架构和应用场景进行介绍：

本申请提出的安全策略处理方法可以应用于 4G 网络架构中。如图 1 所示为当前长期演进（long term evolution, LTE）/系统架构演进（system architecture evolution, SAE）的网络构架。其中，核心网部分主要包括：移动管理实体（mobility management entity, MME）、服务网关（serving gateway, SGW/S-GW）、分组数据网网关（packet data network gateway, PDN GW, PGW/ P-GW）以及归属签约用户服务器（home subscriber server, HSS）、服务 GPRS 支持节点（serving GPRS support node, SGSN）、策略与计费规则功能单元（policy and charging rules function, PCRF）以及运营商的 IP 服务（Operator's IP Services）（例如，IP 多媒体系统（IP multimedia subsystem, IMS）、分组交换业务（packet switching service, PSS））
25 等。其中，核心网可以是演进型分组核心网（evolved packet core, EPC）。此外，图 1 还包括接入网部分，即 UMTS 演进陆地无线接入网（evolution UMTS terrestrial radio access network, E-UTRAN）。该接入网部分主要包括：接入网（radio access network, RAN）设备。此外，图 1 还包括终端设备，例如，用户设备（user equipment, UE）。

其中，移动管理实体 MME：负责管理和存储终端设备的移动管理上下文（例如，终端设备的标识、移动性管理状态以及用户安全参数等），对非接入层（non-access stratum, NAS）信令（例如，附着请求（attach request）、位置更新请求（update location request）、服务请求（service request）以及分组数据网连接请求（PDN connectivity request）等）进行处理，
35

负责 NAS 信令的安全等。

服务网关 S-GW：终结接入网用户面接口的网关，执行合法监听、分组数据路由功能等。该服务网关 S-GW 与移动管理实体 MME 之间的接口是 S11 接口，负责终端设备的会话控制信息等交互。

5 分组数据网网关 P-GW：终结到分组数据网的 SGi 接口的网关，用于提供用户的承载控制、数据转发、IP 地址分配以及非 3GPP 用户接入等功能，是 3GPP 接入和非 3GPP 接入公用数据网（public data network, PDN）的锚点。P-GW 具有分组路由和转发的功能，并负责策略计费增强功能、基于每个用户的分组过滤功能等。P-GW 通过 S5 接口与 S-GW 相连，传递信息建立、修改和删除等控制信息，以及分组数据路由等。此外，该 P-GW 还通过 SGi 接口与运营商的 IP 服务相连。

10 归属签约用户服务器 HSS：用户归属网络中存储用户信息的核心数据库。该 HSS 主要包含用户配置文件、用户签约数据、执行用户的身份验证和授权的相关信息以及有关用户物理位置的信息等。该 HSS 通过 S6a 接口与 MME 连接，以使得 MME 可以从 HSS 获取前述用户配置文件、用户签约数据等信息。

15 策略与计费规则功能单元 PCRF：业务数据流和 IP 承载资源的策略与计费控制策略决策点，可以对用户和业务态服务质量（quality of service, QoS）进行控制，为用户提供差异化的服务。该 PCRF 通过 Gx 与 P-GW 相连，通过 Rx 与运营商的 IP 服务相连。

此外，前述 MME 通过 S1-MME 接口与 E-UTRAN 连接，S-GW 通过 S1-U 和 S11 分别与 E-UTRAN 和 MME 连接。同时 MME 通过 S3 接口，S-GW 通过 S4 接口分别与 2G/3G 20 和 SGSN 连接，分别负责终端设备在对应网络之间的移动性控制面锚点和用户面锚点功能。此外，S-GW 还通过 S12 接口与演进的通用陆地无线接入网络（evolved universal terrestrial radio access network, UTRAN）连接。

接入网设备：是终端设备和核心网设备之间的桥梁，用于无线资源管理、附着流程中 MME 的选择，路由用户数据面至 S-GW 等。本申请中的接入网设备可以是 4G 无线接入网 25 网络设备，也可以是 4G 接入网中在空中接口上通过一个或多个小区与无线终端设备通信的设备。例如，前述接入网设备可以为长期演进 LTE 系统或演进的 LTE 系统（long term evolution advanced, LTE-A）中的演进型基站（evolutional node B, NodeB 或 eNB 或 e-NodeB）。应当注意的是，本申请中涉及的接入网设备可以是升级的接入网设备（例如，支持用户面安全按需保护的接入网设备）或未升级的接入网设备（例如，不支持用户面安全按需保护的接入网设备）。另外，根据为终端设备提供服务的先后顺序的不同，本申请中的接入网设备 30 可以分为源接入网设备（source evolutional node B, S-eNB）和目标接入网设备（target evolutional node B, T-eNB）。其中，源接入网设备为终端设备初始接入时为该终端设备提供服务的接入网设备，或者，源接入网设备为切换、RRC 连接恢复或 RRC 连接重建流程之前，为该终端设备提供服务的接入网设备。目标接入网设备是切换、RRC 连接恢复或 35 RRC 连接重建流程之后，为该终端设备提供服务的接入网设备。一般地前述源接入网设备与目标接入网设备之间会有关于终端设备的上下文的传输。应当理解的是，本申请实施例中的接入网设备可以是上述任意一种设备或上述设备中的芯片，具体此处不做限定。无

论作为设备还是作为芯片，该接入网设备都可以作为独立的产品进行制造、销售或者使用。在本实施例以及后续实施例中，以接入网设备为例进行介绍。

此外，前述终端设备：包括向用户提供语音和/或数据连通性的设备。例如，可以包括具有无线连接功能的手持式设备或连接到无线调制解调器的处理设备。该终端设备可以经无线接入网RAN（例如，前述源接入网设备或前述目标接入网设备）与核心网（例如，前述移动管理实体MME）进行通信，可以与RAN交换语音和/或数据。该终端设备可以包括用户设备UE、无线终端设备、移动终端设备、用户单元（subscriber unit）、用户站（subscriber station）、移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point, AP）、远程终端设备（remote terminal）、接入终端设备（access terminal）、用户终端设备（user terminal）、用户代理（user agent）、或用户装备（user device）等。此外，该终端设备也可以为车载终端，例如，集成在车辆中的车载盒子（telematics box, T-Box）、域控制器（domain controller, DC）、多域控制器（multi domain controller, MDC）或车载单元（on board unit, OBU）。该终端设备还可以为穿戴设备，例如，眼镜、手套、手表、服饰及鞋，或者其他的可以直接穿在身上或是整合到用户的衣服或配件的一种便携式设备，具体本申请不做限定。应当注意的是，本申请中涉及的终端设备可以是升级的终端设备（例如，支持用户面安全按需保护的终端设备）或未升级的终端设备（例如，不支持用户面安全按需保护的终端设备）。应当理解的是，本申请实施例中的终端设备可以是上述任意一种设备或芯片，具体此处不做限定。无论作为设备还是作为芯片，该终端设备都可以作为独立的产品进行制造、销售或者使用。在本实施例以及后续实施例中，仅以终端设备为例进行介绍。

在前述4G网络架构中，一般同时存在升级的接入网设备（例如，支持用户面安全按需保护的接入网设备）和未升级的接入网设备（例如，不支持用户面安全按需保护的接入网设备）。目前，将前述用户面安全按需保护机制应用于4G网络的过程中，为了让支持用户面安全按需保护的终端设备和接入网设备能够开启用户面安全按需保护，设置4G网络中的移动管理实体总是向与该移动管理实体通信的接入网设备发送用户面安全策略。例如，当移动管理实体未收到来自接入网设备的用户面安全策略时，该移动管理实体便向该接入网设备返回用户面安全策略。

在前述传统技术方案中，虽然支持用户面安全按需保护的接入网设备能够利用前述信元为终端设备开启用户面安全按需保护，但是，不支持用户面安全按需保护的接入网设备却总是收到该接入网设备无法使用的信元。因此，提升了移动管理实体与不支持用户面安全按需保护的接入网设备之间的传输复杂度，影响了传输效率。

对此，本申请提出的安全策略处理方法能够在接入网设备侧和/或移动管理实体侧增加判断逻辑，在保证支持用户面安全按需保护的接入网设备和终端设备能够尽可能收到用户面安全策略的情况下，减少移动管理实体发送给不支持用户面安全按需保护的接入网设备的用户面安全策略。

下面基于前述系统架构和应用场景对本申请提出的安全策略处理方法的一种实施方式

进行介绍，如图 2 所示，接入网设备和移动管理实体将执行如下步骤：

步骤 201、源接入网设备向目标接入网设备发送包含指示信息 011 的消息 001。相应的，目标接入网设备接收来自源接入网设备的包含指示信息 011 的消息 001。

本实施例以及后续实施例中，为便于介绍，根据为终端设备提供服务的先后顺序的不同，将先为终端设备提供服务的接入网设备称为源接入网设备，将后为终端设备提供服务的接入网设备称为目标接入网设备。例如，终端设备可以通过切换（Handover）、RRC 连接恢复（RRC Connection Resume）或 RRC 连接重建立（RRC Connection Reestablishment）等流程，从接受前述源接入网设备提供的服务变更为接受目标接入网设备提供的服务。

在此过程中，目标接入网设备可以通过与该源接入网设备之间的信令（例如，前述消息 001）从该源接入网设备接收终端设备的上下文，其中，终端设备的上下文包含前述指示信息 011。可选的，若本实施例应用于切换流程中，则前述消息 001 为切换请求；若本实施例用于 RRC 连接恢复或 RRC 连接重建立流程中，则前述消息 001 为上下文检索响应。

其中，指示信息 011 用于指示终端设备是否支持用户面安全按需保护。或者进一步的，指示信息 011 用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护。所述终端设备是否支持用户面安全按需保护，可以理解为，所述终端设备是否支持开启用户面加密保护和/或是否支持开启用户面完整性保护，即终端设备的用户面加密保护和/或用户面完整性保护不是固定的。终端设备是否支持与接入网设备之间的用户面安全按需保护，可以理解为，所述终端设备是否支持在接入网设备的指示下开启/不开启用户面加密保护和/或用户面完整性保护。这里的接入网设备可以是 eNB，例如，后文提及的源 eNB 或目标 eNB。应当理解的是，关于指示信息 011 的多种表述之间可以相互替换，在后续实施例中，采用“指示信息 011 用于指示终端设备是否支持用户面安全按需保护”这种表述为例进行介绍。

具体地，该指示信息 011 可以由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。示例性的，前述终端设备的演进分组系统安全能力为 UE 演进分组系统安全能力（UE EPS security capabilities），该指示信息 011 可以用终端设备的演进分组系统安全能力中一个预留的比特位来指示，例如 EEA7 或者 EIA7。其中，EEA7 代表 UE 演进分组系统安全能力中为第八个加密算法预留的比特位，EIA7 代表 UE 演进分组系统安全能力中为第八个完整性算法预留的比特位，而本实施例将该比特位用于携带终端设备是否支持用户面安全按需保护的指示。由于，无论接入网设备是否升级（即接入网设备是否支持用户面安全按需保护），该接入网设备均能够识别并转发终端设备的演进分组系统安全能力（例如，UE 演进分组系统安全能力），因此，将指示信息 011 携带于终端设备的演进分组系统安全能力中能够保证指示信息 011 在接入网设备之间（例如，支持用户面安全按需保护的接入网设备与不支持用户面安全按需保护的接入网设备之间）或接入网设备与核心网设备之间（不支持用户面安全按需保护的接入网设备与移动管理实体之间）传输时不丢失。而传统技术中，重新定义的一个指示信息用于指示终端设备是否支持用户面安全按需保护，该重新定义的指示信息不能够被未升级的接入网设备识别。也就是说，不支持用户面安全按需保护的接入网设备无法识别前述重新定义的指示信息，若该不支持用户面安全按需保护的接入网设备

收到前述重新定义的指示信息，则该不支持用户面安全按需保护的接入网设备将丢弃前述重新定义的指示信息而无法发送给其他的接入网设备或核心网设备（例如，移动管理实体等）。

5 可选的，前述消息 001 还包括该终端设备用于建立承载的标识信息，例如演进的无线接入承载（E-UTRAN radio access bearer，E-RAB）的标识等。也可以理解为，前述终端设备的上下文中还包含用于建立承载的 E-RAB 的标识。

进一步地，前述消息 001 中包含前述终端设备的 N 个 E-RAB 的标识，其中，N 为大于等于 1 的整数。

步骤 202、目标接入网设备判断是否满足预设条件。

10 本实施例中，前述预设条件是指示信息 011 相关的预设条件。当目标接入网设备确定满足预设条件时，该目标接入网设备将依次执行步骤 203a 和步骤 203b；当目标接入网设备确定不满足预设条件时，该目标接入网设备将执行步骤 203c 或步骤 203d。可以理解为，目标接入网设备会根据与指示信息 011 相关的预设条件，确定是否获取并向移动管理实体发送用户面安全策略。

15 前述预设条件可以采用如下任意一种实施方式：

在一种可选的实施方式中，该预设条件包括该指示信息 011 指示该终端设备支持用户面安全按需保护。

在另一种可选的实施方式中，该预设条件为：指示信息 011 指示该终端设备支持用户面安全按需保护，并且，该目标接入网设备支持用户面安全按需保护。

20 应当理解的是，目标接入网设备支持用户面安全按需保护；可以理解为，接入网设备是否支持与终端设备之间的用户面安全按需保护；也可以理解为，该接入网设备是否支持为终端设备开启用户面加密保护和/或是否支持开启用户面完整性保护；也可以理解为，所述接入网设备是否能够向终端设备发送某种指示，以使得该终端设备根据前述某种指示开启/不开启用户面加密保护和/或用户面完整性保护。应当理解的是，前述多种表述之间可以相互替换，在后续实施例中，采用“目标接入网设备支持用户面安全按需保护”这种表述为例进行介绍。

30 应当理解的是，当目标接入网设备是升级的接入网设备（即支持用户面安全按需保护的接入网设备）时，该目标接入网设备能够获知自己能够支持用户面安全按需保护。当目标接入网设备是未升级的接入网设备（即不支持用户面安全按需保护的接入网设备）时，该目标接入网设备能够获知自己不支持用户面安全按需保护。

此外，还应理解的是，若将本申请的方案应用于升级的接入网设备中，当该目标接入网设备在判断指示信息 011 是否指终端设备是否支持用户面安全按需保护时，其实，已经说明该目标接入网设备是支持用户面安全按需保护。于是，可选的，可以不用单独为该目标接入网设备设置一个判断自身是否支持用户面安全按需保护的逻辑。

35 步骤 203a、目标接入网设备获取用户面安全策略 021。

其中，用户面安全策略是用于指示是否开启用户面加密保护和/或用户面完整性保护的策略；也可以理解为，用户面安全策略包含用户面加密保护策略和用户面完整性保护策略，

其中，用户面加密保护策略用于指示是否开启用户面加密保护，用户面完整性保护策略用于指示是否开启用户面完整性保护。目前，用户面加密保护策略和用户面完整性保护策略分别包含三种指示：required（需要开启）、preferred（推荐开启）以及 not needed（不开启）。具体的，当用户面加密保护策略为 required 时，表示需要强制开启用户面加密保护；当用户面加密保护策略为 not needed 时，表示需要强制不开启用户面加密保护；当用户面加密保护策略为 preferred 时，表示可以根据实际情况可选的开启用户面加密保护（例如，接入网设备可以根据自身的负载情况，确定是否开启与终端设备之间的用户面加密保护；负载大于阈值的情况下，就不开启用户面加密保护，反之，则开启用户面加密保护）。用户面完整性保护策略的使用同上述用户面加密保护策略，不再赘述。

具体地，该目标接入网设备可以通过如下几种方式获取用户面安全策略 021。

在一种可选的实施方式中，当该目标接入网设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 可以是目标接入网设备构建的用户面安全策略 021-1。

本实施方式中，由于目标接入网设备未从源接入网设备收到用户面安全策略，因此，目标接入网设备可以采用默认的方式（可以理解为，未升级的方式）为终端设备开启用户面安全按需保护，例如，可以开启用户面加密保护以及不开启用户面完整性保护。该目标接入网设备构建的用户面安全策略 021-1 需要匹配终端设备当前的用户面安全激活状态，即用户面加密保护开启以及用户面完整性保护不开启的状态。例如，该目标接入网设备构建的用户面安全策略 021-1 为匹配用户面加密保护开启且用户面完整性保护不开启的用户面安全激活状态的策略。具体地，该用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，该用户面加密保护策略为需要开启（required）或推荐开启（preferred），该用户面完整性保护策略为不需要开启（not needed）或推荐开启（preferred）。

示例性的，若用户面安全策略表示为{用户面加密保护策略，用户面完整性保护策略}，则用户面安全策略 021-1 具体可以为如下任意一种实现方式：{需要开启（required），不需要开启（not needed）}；{需要开启（required），推荐开启（preferred）}；{推荐开启（preferred），不需要开启（not needed）}；{推荐开启（preferred），推荐开启（preferred）}。

应当理解的是，前述用户面安全策略 021-1 可以是 E-RAB 粒度的用户面安全策略。一般地，若一个终端设备对应 N 个 E-RAB，该目标接入网设备可以根据从终端设备的上下文中获取的 E-RAB 的标识为该终端设备的每个 E-RAB 均构建对应的用户面安全策略 021-1，此时，目标接入网设备便可以获得 N 个用户面安全策略 021-1。其中，N 为大于或等于 1 的整数。其中，每个 E-RAB 对应一个用户面安全策略 021-1。但是，不同的 E-RAB 对应的用户面安全策略可以相同也可以不相同。

此外，在后续传输前述用户面安全策略时，该目标接入网设备将用户面安全策略 021-1 和 E-RAB 的标识一起携带于信令中，以表示该用户面安全策略 021-1 用于确定该 E-RAB 的标识对应的 E-RAB 是否需要开启/不开启用户面加密保护和/或用户面完整性保护。具体地，请参阅步骤 203b 中的介绍。本实施方式中，可以使移动管理实体（例如，MME）在判断用户面安全策略时具备更细粒度，从而在某些 E-RAB 对应的用户面安全策略不一致，但是另一些 E-RAB 对应的用户面安全策略一致情况下，减少 MME 回传用户面安全策略的

数量。

在另一种可选的实施方式中，当该目标接入网设备未从该源接入网设备收到用户面安全策略时，该用户面安全策略 021 可以是预配置在目标接入网设备中的用户面安全策略 021-2。

- 5 本实施方式中，目标接入网设备中预配置了用户面安全策略 021-2，该预配置的用户面安全策略 021-2 可以是适用于所有终端设备的策略。该预配置的用户面安全策略可以包含用户面加密保护策略和/或用户面完整性保护策略，其中，用户面加密保护策略可以是需要开启（required）或推荐开启（preferred）或不开启（not needed）中的任意一种，用户面完整性保护策略也可以是
- 10 需要开启（required）或推荐开启（preferred）或不开启（not needed）中的任意一种。

- 具体地，该目标接入网设备可以仅预配置一个适用于所有终端设备的用户面安全策略；然后，将用户面安全策略映射为 N 个 E-RAB 粒度的用户面安全策略用户面安全策略 021-2。在这样的实施方式中，一方面可以减少目标接入网设备配置用户面安全策略的复杂度；另一方面也可以使移动管理实体（例如，MME）在判断用户面安全策略时具备更细粒度，从而在某些 E-RAB 对应的用户面安全策略不一致，但是另一些 E-RAB 对应的用户面安全策略一致情况下，减少 MME 回传用户面安全策略的数量。
- 15

除此之外，前述用户面安全策略 021 还可以是该目标接入网设备从其他设备获取的用户面安全策略 021-3。

- 在一种可能的实施方式中，若前述源接入网设备支持用户面安全按需保护，则前述目标接入网设备与源接入网设备之间的信令便可能携带了用户面安全策略 021-3。此时，所述用户面安全策略 021 可以是所述目标接入设备从源接入网设备接收到的用户面安全策略 021-3。
- 20

- 步骤 203b、目标接入网设备向移动管理实体发送携带该用户面安全策略 021 的路径切换请求（path switch request）031。相应的，移动管理实体从目标接入网设备接收携带用户面安全策略 021 的路径切换请求 031。
- 25

其中，该用户面安全策略 021 可以是步骤 203a 中任意一种实施方式所确定的用户安全策略，例如，可以是用户面安全策略 021-1，用户面安全策略 021-2 或者用户面安全策略 021-3。

- 在一种可选的实施方式中，前述路径切换请求 031 为路径切换请求 031-1，该路径切换请求 031-1 携带一个用户面安全策略 021，例如，该用户面安全策略 021 是终端设备粒度的安全策略，一个终端设备对应一个用户面安全策略。此时，前述路径切换请求 031 除了携带用户面安全策略 021 之外，还可能携带终端设备的标识（例如，eNB UE S1AP ID 或 MME UE S1AP ID）。
- 30

- 在另一种可选的实施方式中，前述路径切换请求 031 为路径切换请求 031-2，路径切换请求 031-2 携带 N 个 E-RAB 粒度的用户面安全策略 021 以及 N 个 E-RAB 的标识，该 N 个 E-RAB 的标识中每个 E-RAB 的标识分别与一个用户面安全策略 021 对应。具体地，该目标接入网设备将该 E-RAB 的标识与该 E-RAB 对应的用户面安全策略均携带于该路径切换
- 35

请求 031-2 中, 以使得该 E-RAB 的标识和该 E-RAB 对应的用户面安全策略能够一起发送至移动管理实体。相应的, 当该移动管理实体收到前述同时携带 E-RAB 的标识和用户面安全策略的路径切换请求 031-2, 该移动管理实体能够获知该用户面安全策略适用于哪个 E-RAB。此外, 前述路径切换请求 031-2 还可能携带终端设备的标识 (例如, eNB UE S1AP ID 或 MME UE S1AP ID), 以表示与前述一个或多个 E-RAB 对应的终端设备。

应当注意的是, 若前路径切换请求 031-2 携带的用户安全策略 021 是由目标接入网设备构建的用户面安全策略 021-1, 那么, 该路径切换请求 031-2 携带的 N 个用户面安全策略 021-1 中, 各个用户面安全策略 021-1 可能相同也可能不同。

示例性的, 路径切换请求 031-2 携带多个用户面安全策略 021-1 的实现方式具体为:
10 {E-RAB1: 用户面安全策略 021-1-1}; {E-RAB2: 用户面安全策略 021-1-2}; {E-RAB3: 用户面安全策略 021-1-3}。其中, 用户面安全策略 021-1-1 的内容、用户面安全策略 021-1-2 的内容以及用户面安全策略 021-1-3 的内容可能相同也可能不相同。

但是, 若前路径切换请求 031-2 携带的用户安全策略 021 是由目标接入网设备将预配置的适用于所有终端设备的用户面安全策略映射出的多个用户面安全策略 021-2, 那么, 该
15 路径切换请求 031-2 携带的 N 个用户面安全策略 021-2 中, 各个用户面安全策略 021-2 的内容是相同的。

示例性的, 路径切换请求 031-2 携带多个用户面安全策略 021-2 的实现方式具体为:
20 {E-RAB1: 用户面安全策略 021-2}; {E-RAB2: 用户面安全策略 021-2}; {E-RAB3: 用户面安全策略 021-2}。其中, 用户面安全策略 021-2 的内容、用户面安全策略 021-2 的内容以及用户面安全策略 021-2 的内容是相同的。

这样的实施方式中, 目标接入网设备可以为终端设备对应的各个 E-RAB 决策是否开启用户面加密保护和/或用户面完整性保护, 有利于精细化管理用户面安全策略以及用户面安全激活状态。

步骤 203c、目标接入网设备向移动管理实体发送未携带用户面安全策略的路径切换请求 032。相应的, 移动管理实体从目标接入网设备接收未携带用户面安全策略的路径切换
25 请求 032。

本实施例中, 若预设条件包括该指示信息 011 指示该终端设备支持用户面安全按需保护, 那么, 当指示信息 011 指示该终端设备不支持用户面安全按需保护时, 该目标接入网设备向移动管理实体发送未携带用户面安全策略的路径切换请求 032。

30 若预设条件为: 指示信息 011 指示该终端设备支持用户面安全按需保护, 并且, 该目标接入网设备支持用户面安全按需保护。此时, 当指示信息 011 指示该终端设备不支持用户面安全按需保护, 或者, 目标接入网设备不支持用户面安全按需保护时, 该目标接入网设备向移动管理实体发送未携带用户面安全策略的路径切换请求 032。

步骤 203d、目标接入网设备向移动管理实体发送未携带用户面安全策略的路径切换请求 033。相应的, 移动管理实体从目标接入网设备接收未携带用户面安全策略的路径切换
35 请求 033。

其中, 前述未携带用户面安全策略的路径切换请求 033 携带了指示信息 011。

相比于传统技术，传统技术中目标接入网设备仅会判断是否从源接入网设备收到了用户面安全策略。若收到，则该目标接入网设备便将该用户面安全策略发送至移动管理实体，否则，该目标接入网设备在与移动管理实体的交互中无法携带用户面安全策略。本申请中，增加了目标接入网设备基于指示信息 011 的判断逻辑，有利于该目标接入网设备在终端设备支持用户面安全按需保护时才向移动管理实体发送用户面安全策略，进而移动管理实体回复的更新的用户面安全策略才可能适用于前述目标接入网设备，即目标接入网设备能够应用该用户面安全策略为终端设备开启或关闭用户面加密保护和/或用户面完整性保护。否则，若该终端设备本就不支持用户面安全按需保护，那么，即使目标接入网设备能够获取用户面安全策略，也无法为该终端设备开启用户面加密保护和用户面完整性保护。因此，降低了接入网设备收到不能使用的信元的几率。

步骤 204、移动管理实体判断路径切换请求中是否携带了用户面安全策略。

其中，该路径切换请求可以是前述路径切换请求 031、路径切换请求 032 以及路径切换请求 033 中任意一项。

在一种可选的实施方式中，若路径切换请求中未携带用户面安全策略，例如，路径切换请求为路径切换请求 032，则该移动管理实体执行步骤 205a；若路径切换请求中携带了用户面安全策略，例如，路径切换请求为路径切换请求 031，则该移动管理实体执行步骤 205b。

在另一种可选的实施方式中，若路径切换请求中未携带用户面安全策略，但是，前述未携带用户面安全策略的切换请求携带指示信息011。也就是说，该移动管理实体收到的是路径切换请求033。此时，该移动管理实体还将对比指示信息011和移动管理实体中的指示信息012。若移动管理实体中的指示信息012指示终端设备支持用户面安全按需保护，则移动管理实体向目标接入网设备发送携带指示信息012和用户面安全策略023的路径切换响应043（图未示）。若指示信息011和移动管理实体中的指示信息012一致，则该移动管理实体执行步骤205a。本实施方式中，若源接入网设备是恶意的，它可以对指示信息011进行恶意篡改，使指示信息011指示终端设备不支持用户面安全按需保护，这将导致目标接入网设备无法向移动管理实体发送用户面安全策略，也无法为终端设备开启用户面安全按需保护，从而导致降质攻击。因此，可以使目标接入网设备在判断不向移动管理设备发送用户面安全策略后，额外发送指示信息011，以使得移动管理实体可以判断指示信息011是否被篡改，在移动管理实体判断该指示信息011被篡改后，便会向目标接入网设备发送用户面安全策略。这样，可以避免上述降质攻击。

其中，指示信息012来自于终端设备，可以由终端设备在初始附着到网络时提供给移动管理实体的。用户面安全策略023相关描述参见步骤205b描述，此处不再赘述。

此外，该目标接入网设备还将该用户面安全策略023存储于该终端设备的上下文中。应当理解的是，若该终端设备的上下文中存储有用户面安全策略（例如，用户面安全策略023'），则该目标接入网设备将采用用户面安全策略023更新存储于终端设备的上下文中的用户面安全策略023'。若该终端设备的上下文中未存储有用户面安全策略，则该目标接入网设备将直接存储用户面安全策略023。

步骤205a、移动管理实体向目标接入网设备发送未携带用户面安全策略的路径切换响应（path switch request acknowledge）042。相应的，目标接入网设备从移动管理实体接收未携带用户面安全策略的路径切换响应042。

5 相比于传统技术中，移动管理实体在收到未携带用户面安全策略的路径切换请求之后，该移动管理实体为了尽可能让4G网络中的接入网设备和终端设备能够开启用户面完整性保护，便会向目标接入网设备发送用户面安全策略。此时，目标接入网设备和终端设备很可能无法使用该用户面安全策略。

而本实施例中，在前述步骤中，当指示信息011指示终端设备支持用户面安全按需保护时，该目标接入网设备会采用步骤203a中任何一种实施方式确定用户面安全策略021，以及
10 将该用户面安全策略021携带于路径切换请求中以发送至移动管理实体。由此可知，若指示信息011指示终端设备不支持用户面安全按需保护，则该目标接入网设备不会向移动管理实体发送用户面安全策略，相应的移动管理实体也无法从目标接入网设备收到用户面安全策略。此时，可以推断出终端设备不支持用户面安全按需保护，即使向该目标接入网设备提供了用户面安全策略，该目标接入网设备也无法使用该用户面安全策略为该终端设备开启
15 用户面完整性保护。因此，设置移动管理实体在收到未携带用户面安全策略的路径切换请求042时，向目标接入网设备发送未携带用户面安全策略的路径切换响应，即不向目标接入网设备提供用户面安全策略。因此，降低了目标接入网设备收到不能使用的信元的几率，降低了目标接入网设备与移动管理实体之间的数据传输复杂度。

步骤205b、移动管理实体根据用户面安全策略021与移动管理实体中的用户安全策略是否一致，确定是否发送携带用户面安全策略022的路径切换响应041。
20

具体地，若用户面安全策略021与移动管理实体中的用户安全策略是一致的，则该移动管理实体向目标接入网设备发送未携带用户面安全策略的路径切换响应。

若用户面安全策略021与移动管理实体中的用户安全策略不一致，则该移动管理实体向目标接入网设备发送携带用户面安全策略022的路径切换响应041。然后，该目标接入网设备还将该用户面安全策略022存储于该终端设备的上下文中。应当理解的是，若该终端设备的
25 上下文中存储有用用户面安全策略（例如，用户面安全策略021），则该目标接入网设备将采用用户面安全策略022更新存储于终端设备的上下文中的用户面安全策略021。若该终端设备的上下文中未存储有用用户面安全策略，则该目标接入网设备将直接存储用户面安全策略023。

30 其中，用户面安全策略022可以根据归属用户服务器HSS获得的用户面安全策略获得，也可以根据移动管理实体预配置的用户面安全策略获得。

可选的，移动管理实体从HSS获得或者预配置的用户面安全策略是接入点名称（access point name, APN）粒度的，移动管理实体将APN粒度的用户面安全策略映射为E-RAB粒度的用户面安全策略后，获得E-RAB粒度的用户面安全策略022。

35 可选的，若步骤203b中的路径切换请求031为路径切换请求031-1，该路径切换请求031-1携带一个用户面安全策略021，该用户面安全策略021为终端设备粒度的安全策略，则该移动管理实体将该移动管理实体中的终端设备粒度的用户面安全策略与该用户面安全策略

021对比。若用户面安全策略021与移动管理实体中的终端设备粒度的用户安全策略是一致的，则该移动管理实体向目标接入网设备发送未携带用户面安全策略的路径切换响应。若用户面安全策略021与移动管理实体中的终端设备粒度的用户安全策略不一致，则该移动管理实体向目标接入网设备发送携带用户面安全策略022的路径切换响应041。此时，该用户面安全策略022是终端设备粒度的安全策略。

特别的，对于步骤205a描述的情况下，移动管理实体获得终端设备对应的所有E-RAB的用户面安全策略022。具体的，移动管理实体从终端设备的上下文中获得终端设备对应的所有E-RAB的标识，并根据每个E-RAB的标识获得对应的APN，再根据APN对应的用户面安全策略获得每个E-RAB对应的用户面安全策略022。

可选的，若步骤203b中路径切换请求携带为路径切换请求031-2，路径切换请求031-2携带N个E-RAB粒度的用户面安全策略021，其中，每个用户面安全策略021为E-RAB粒度的策略。此时，移动管理实体分别对比每个E-RAB对应的用户面安全策略，若每个E-RAB对应的用户面安全策略021与移动管理实体中的对应E-RAB对应的用户安全策略一致，则该移动管理实体向目标接入网设备发送未携带用户面安全策略的路径切换响应；若某一个E-RAB对应的用户面安全策略021与移动管理实体中的同一E-RAB对应的用户安全策略不一致，则该移动管理实体向目标接入网设备发送携带用户面安全策略022的路径切换响应041。其中，用户面安全策略022为E-RAB粒度的安全策略，并且，该用户面安全策略022为与用户面安全策略021不一致的安全策略。在这种实施方式中，移动管理实体中的用户面安全策略与多个用户面安全策略021可能部分不一致，也可能全部不一致，具体此处不做限定。可选的，该携带用户面安全策略022的路径切换响应还可以携带该用户面安全策略022对应的E-RAB的标识。

进一步地，目标接入网设备根据前述用户面安全策略022重新激活终端设备，即根据用户面安全策略022确定是否为终端设备开启用户面加密保护和/或用户面完整性保护。具体地，请参阅后文图3对应实施例中，步骤309b至步骤312中的相关介绍，具体此处不再赘述。

本实施例中，由于目标接入网设备能够根据指示信息011确定终端设备是否支持用户面安全按需保护，若该终端设备支持用户面安全按需保护，该目标接入网设备才向移动管理实体发送用户面安全策略。避免了当终端设备不支持用户面安全按需保护，且，移动管理实体在未从目标接入网设备收到用户面安全策略时，移动管理实体向该目标接入网设备发送用户面安全策略，而造成目标接入网设备即使收到该用户面安全策略也无法为该终端设备开启用户面安全按需保护的情况。因此，有利于减少移动管理实体向目标接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。

前述图 2 对应实施例所介绍的安全策略处理方法可以应用于切换（Handover）、RRC 连接恢复（RRC Connection Resume）以及 RRC 连接重建（RRC Connection Reestablishment）中任何一种流程中。下面以如图 3 所示的切换流程为例进行进一步介绍。其中，目标 eNB 为前述目标接入网设备的一种实现方式，源 eNB 为前述源接入网设备的一种实现方式、MME 为前述移动管理实体的一种实现方式、HSS 为前述归属用户服务器的

一种实现方式。并且，假设目标 eNB 为升级的 eNB（即支持用户面安全按需保护的 eNB），源 eNB 为未升级的 eNB（即不支持用户面安全按需保护的 eNB）。前述各个设备将执行如下步骤：

5 步骤 301、源 eNB 向目标 eNB 发送切换请求（handover request）。相应的，目标 eNB 从源 eNB 接收切换请求。

其中，切换请求为消息 001 在切换场景下的一种实现方式。

其中，该切换请求携带指示信息 011，未携带用户面安全策略。其中，指示信息 011 用于指示 UE 是否支持用户面安全按需保护。具体地，该指示信息 011 用于指示 UE 是否支持用户面加密保护和/或是否支持用户面完整性保护。前述 UE 为待从源 eNB 切换至目标
10 eNB 的 UE。此外，该指示信息 011 携带于 UE 演进分组系统安全能力（UE EPS security capabilities）中，由 UE 演进分组系统安全能力中一个预留的比特位来指示，例如 EEA7 或者 EIA7。具体地，关于指示信息 011 的介绍可以参阅前述步骤 201 中的描述，具体此处不再赘述。

15 步骤 302、目标 eNB 确定用户面安全激活状态，所述用户面安全激活状态用于指示是否开启用户面加密保护和/或用户面完整性保护。

其中，该用户面安全激活状态包含加密激活状态和/或完整性激活状态，加密激活状态用于指示是否开启用户面加密保护，完整性激活状态用于指示是否开启用户面完整性保护。

此外，该用户面安全激活状态是数据无线承载（data radio bearer，DRB）粒度的。一般地，一个 UE 对应一个或多个 E-RAB，而一个 E-RAB 可能映射一个或多个 DRB。因此，
20 该目标 eNB 需要为该 UE 对应的每一个 DRB 确定是否开启用户面加密保护和/或是否开启用户面完整性保护。

由于，目标 eNB 收到的切换请求中不携带用户安全策略，因此，该目标接入网设备可以使用以下任一方式为 UE 确定用户面安全激活状态。

方式一、目标 eNB 可以用默认的方式（也可以理解为，未升级的方式）为 UE 确定用
25 户面安全激活状态，即总是开启用户面加密保护，但不开启用户面完整性保护。具体的，对于该 UE 的所有 DRB，其对应的加密激活状态都为开启，其对应的完整性激活状态都为不开启。

方式二、目标 eNB 中预配置了用户面安全策略，该预配置的用户面安全策略可以是适用于所有 UE 的策略。若目标 eNB 根据指示信息 011 确定 UE 支持用户面安全按需保护，
30 则目标 eNB 根据预配置的用户面安全策略确定用户面安全激活状态。

具体的，若用户面加密保护策略是 required，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的加密激活状态都为开启。若用户面加密保护策略是 preferred，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的加密激活状态可以为开启或不开启。目标 eNB 可以根据本地策略（例如，自身运行状态、控制策略、法规要求等）进行判断。若用户面加密保
35 护策略是 not needed，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的加密激活状态都为不开启。

相应的，若用户面完整性保护策略是 required，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的完整性激活状态都为开启。若用户面完整性保护策略是 preferred，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的完整性激活状态可以为开启或不开启。目标 eNB 可以根据本地策略（例如，自身运行状态、控制策略、法规要求等）进行判断。若用户面完整性保护策略是 not needed，则对于该 UE 的所有 DRB，目标 eNB 确定其对应的完整性激活状态都为不开启。

步骤 303、目标 eNB 向源 eNB 发送切换请求响应（handover request acknowledge）。相应的，源 eNB 从目标 eNB 接收切换请求响应。

其中，切换请求响应中包含前述需要发送至 UE 的用户面安全激活状态。具体地，该切换请求响应中包含无线资源控制 RRC 重配置（RRC connection reconfiguration），该 RRC 重配置由目标 eNB 构造。前述 UE 的用户面安全激活状态包含于前述 RRC 重配置中。也就是说，目标 eNB 将用户面安全激活状态封装于 RRC 重配置中，通过切换请求响应发送至源 eNB，再由源 eNB 将封装了用户面安全激活状态的 RRC 重配置转发至 UE。

该 RRC 重配置包含了 DRB 配置信息。该 DRB 配置信息用于指示 UE 是否开启某个 DRB 的用户面加密保护和/或用户面完整性保护。一般地，若 DRB 配置信息中封装了禁用加密（ciphering disabled）字段，则 UE 不开启 DRB 的加密保护；若 DRB 配置信息中未封装禁用加密（ciphering disabled）字段，则 UE 开启 DRB 的加密保护。若 DRB 配置信息中封装了完整性保护（integrity protection）字段，则 UE 开启 DRB 的完整性保护；若 DRB 配置信息中未封装完整性保护（integrity protection）字段，则 UE 不开启 DRB 的完整性保护。

示例性的，在目标 eNB 确定对于该 UE 的所有 DRB，其对应的加密激活状态都为开启，其对应的完整性激活状态都为不开启时，该 RRC 重配置不包含 DRB 配置信息。

步骤 304、源 eNB 向 UE 发送 RRC 重配置。相应的，UE 从源 eNB 接收 RRC 重配置。

也就是说，该源 eNB 将从目标 eNB 中收到的 RRC 重配置转发至 UE，以使得该 UE 根据 RRC 重配置中携带的内容进行 RRC 重配置。

在一种可选的实施方式中，该 RRC 重配置中包含目标 eNB 指示给 UE 的用户面安全激活状态。可以理解为，该 RRC 重配置中包含目标 eNB 确定的 DRB 配置信息。此时，该目标 eNB 通过显示的方式指示 UE 不开启用户面加密保护和/或开启用户面完整性保护。

例如，当该 RRC 重配置中携带的 DRB 配置信息为禁用加密（ciphering disabled）字段和完整性保护（integrity protection）字段时，可以理解为，目标 eNB 通过显示的方式向 UE 发送用户面安全激活状态。

在另一种可选的实施方式中，该 RRC 重配置中不包含 DRB 配置信息。此时，该目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护和/或不开启用户面完整性保护。可以理解为，目标 eNB 通过隐式的方式向 UE 发送用户面安全激活状态。

例如，当该 RRC 重配置中未携带禁用加密（ciphering disabled）字段，也未携带完整性保护（integrity protection）字段时，可以理解为，目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护且不开启用户面完整性保护。

此外，还可能其他的实现方式，例如，当该 RRC 重配置中携带的 DRB 配置信息仅

包含禁用加密 (ciphering disabled) 字段时, 可以理解为, 目标 eNB 通过显示的方式指示 UE 不开启用户面加密保护, 并且, 通过隐式的方式指示 UE 不开启用户面完整性保护。又例如, 当该 RRC 重配置中携带的 DRB 配置信息仅包含完整性保护 (integrity protection) 字段时, 可以理解为, 目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护, 并且, 通过显示的方式指示 UE 开启用户面完整性保护。

应当理解的是, 前述步骤 303 和步骤 304 还可能携带其他的需要传输给 UE 的配置信息, 例如, DRB ID 等, 本实施例不再一一举例介绍。

步骤 305、UE 向目标 eNB 发送 RRC 重配置完成。相应的, 目标 eNB 从 UE 接收 RRC 重配置完成。

其中, 该 RRC 重配置完成用于指示目标 eNB 该 UE 已完成 RRC 重配置, 该 UE 成功从源 eNB 切换至目标 eNB。此后, 该 UE 可以与直接目标 eNB 进行信令交互。

步骤 306、目标 eNB 判断 UE 是否支持用户面安全按需保护。

应当注意的是, 步骤 302 至步骤 305 与步骤 306 无时间先后顺序的限定, 步骤 306 在步骤 301 之后便可以执行。也就是说, 目标 eNB 从源 eNB 中收到切换请求之后, 该目标 eNB 便可以基于该切换请求的内容确定 UE 的用户面安全激活状态, 与此同时, 该目标 eNB 也将基于前述切换请求中携带的指示信息 011 判断 UE 是否支持用户面安全按需保护。

具体地, 该目标 eNB 根据指示信息 011 判断该 UE 是否支持用户面安全按需保护。

可选的, 该目标 eNB 还可以判断目标 eNB 是否支持用户面安全按需保护。具体请参阅前述步骤 202 中的相关介绍, 此处不再赘述。

当目标 eNB 确定 UE 支持用户面安全按需保护时, 该目标 eNB 将依次执行步骤 307a 和步骤 307b; 当目标 eNB 确定 UE 不支持用户面安全按需保护, 或, 目标 eNB 不支持用户面安全按需保护时, 该目标 eNB 将执行步骤 307c 或 307d。

步骤 307a、目标 eNB 获取用户面安全策略 021。

具体地, 该目标 eNB 可以通过如下几种方式获取用户面安全策略 021。

方式一、当该目标 eNB 未从该源 eNB 收到用户面安全策略时, 该用户面安全策略 021 可以是目标接入网设备构建的用户面安全策略 021-1。也可以理解为, 该目标 eNB 构建该用户面安全策略 021-1。

本实施方式中, 由于目标 eNB 未从源 eNB 收到用户面安全策略, 因此, 目标 eNB 可以用默认的方式 (可以理解为, 未升级的方式) 为 UE 开启用户面安全按需保护, 即开启用户面加密保护不开启用户面完整性保护。该目标 eNB 构建的用户面安全策略 021-1 需要匹配 UE 当前的用户面安全激活状态。例如, 用户面加密保护开启、用户面完整性保护不开启的状态。例如, 该目标 eNB 构建的用户面安全策略 021-1 为匹配用户面加密保护开启且用户面完整性保护不开启的用户面安全激活状态的策略。具体地, 该用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略, 其中, 该用户面加密保护策略为需要开启 (required) 或推荐开启 (preferred), 该用户面完整性保护策略为不需要开启 (not needed) 或推荐开启 (preferred)。

示例性的, 若用户面安全策略表示为 {用户面加密保护策略, 用户面完整性保护策略},

则用户面安全策略 021-1 具体可以为如下任意一种实现方式：{需要开启（required），不需要开启（not needed）}；{需要开启（required），推荐开启（preferred）}；{推荐开启（preferred），不需要开启（not needed）}；{推荐开启（preferred），推荐开启（preferred）}。

此外，前述用户面安全策略 021-1 为 E-RAB 粒度的安全策略。具体地，该目标 eNB 将
5 获取 E-RAB 的标识，在后续过程中，将 E-RAB 的标识和用户面安全策略 021 一起发送至 MME。具体地，请参阅前述步骤 203a 和步骤 203b 中的相关介绍，此处不再赘述。

方式二、当该目标 eNB 未从该源 eNB 收到用户面安全策略时，该用户面安全策略 021 可以是预配置在目标接入网设备中的用户面安全策略 021-2。可以理解为，该目标 eNB 根据预配置的安全策略确定该用户面安全策略 021-2。

10 本实施方式中，目标 eNB 中预配置了用户面安全策略，该预配置的用户面安全策略可以是适用于所有 UE 的策略。该预配置的用户面安全策略可以包含加密保护策略和/或完整性保护策略，其中，加密保护策略可以是需要开启（required）或推荐开启（preferred）或不开启（not needed）中的任意一种，完整性保护策略也可以是需要开启（required）或推荐开启（preferred）或不开启（not needed）中的任意一种。

15 示例性的，若用户面安全策略表示为{用户面加密保护策略，用户面完整性保护策略}，则用户面安全策略 021-2 具体可以为如下任意一种实现方式：{需要开启（required），需要开启（required）}；{需要开启（required），推荐开启（preferred）}；{需要开启（required），不需要开启（not needed）}；{推荐开启（preferred），需要开启（required）}；{推荐开启（preferred），推荐开启（preferred）}；{推荐开启（preferred），不需要开启（not needed）}；
20 {不需要开启（not needed），需要开启（required）}；{不需要开启（not needed），推荐开启（preferred）}；{不需要开启（not needed），不需要开启（not needed）}。

具体地，请参阅前述步骤 203a 和步骤 203b 中的相关介绍，此处不再赘述。

步骤 307b、目标 eNB 向 MME 发送携带该用户面安全策略 021 的路径切换请求（path switch request）031。相应的，MME 从目标 eNB 接收携带该用户面安全策略 021 的路径切
25 换请求 031。

其中，该用户面安全策略 021 可以是步骤 307a 中任意一种实施方式所确定的用户安全策略，例如，可以是用户面安全策略 021-1 或用户面安全策略 021-2。

具体地，请参阅前文步骤 203b 中的相关描述，此处不再赘述。

步骤 307c、目标 eNB 向 MME 发送未携带用户面安全策略的路径切换请求 032。相应的，MME 从目标 eNB 接收未携带用户面安全策略的路径切换请求 032。
30

其中，路径切换请求 032 中未携带指示信息 011。

步骤 307d、目标 eNB 向 MME 发送未携带用户面安全策略的路径切换请求 033。相应的，MME 从目标 eNB 接收未携带用户面安全策略的路径切换请求 033。

其中，路径切换请求 033 中携带了指示信息 011。该指示信息 011 可以目标 eNB 从源
35 eNB 获得的指示信息 011。

步骤 308、MME 判断路径切换请求中是否携带用户面安全策略。

其中，该路径切换请求可以是前述路径切换请求 031、路径切换请求 032 以及路径切

换请求 033 中任意一项。

在一种可选的实施方式中，若路径切换请求中未携带用户面安全策略，例如，路径切换请求为路径切换请求 032，则该 MME 执行步骤 309a；若路径切换请求中携带了用户面安全策略，例如，路径切换请求为路径切换请求 031，则该 MME 执行步骤 309b。

5 在另一种可选的实施方式中，若路径切换请求中未携带用户面安全策略，但是，前述未携带用户面安全策略的切换请求携带指示信息011。也就是说，该MME收到的是路径切换请求033。此时，该MME还将对比指示信息011和MME中的指示信息012。若MME中的指示信息012指示UE支持用户面安全按需保护，则MME向目标eNB发送携带指示信息012和用户面安全策略023的路径切换响应043（图未示）。若指示信息011和MME中的指示信息012
10 一致，则该MME向目标eNB发送未携带用户面安全策略和指示信息的路径切换响应045（图未示）。本实施方式中，若源eNB是恶意的，它可以对指示信息011进行恶意篡改，使指示信息011指示UE不支持用户面安全按需保护，这将导致目标eNB无法向MME发送用户面安全策略，也无法为UE开启用户面安全按需保护，从而导致降质攻击。因此，可以使目标eNB在判断不向移动管理设备发送用户面安全策略后，额外发送指示信息011，以使得MME可以判断指示信息011是否被篡改，在MME判断该指示信息011被篡改后，便会向目标eNB发
15 送用户面安全策略。这样，可以避免上述降质攻击。

其中，指示信息012来自于UE，可以由UE在初始附着到网络时提供给MME的。

此外，该目标eNB还将该用户面安全策略023存储于该UE的上下文中。应当理解的是，若该UE的上下文中存储有用户面安全策略（例如，用户面安全策略023'），则该目标eNB
20 将采用用户面安全策略023更新存储于UE的上下文中的用户面安全策略023'。若该UE的上下文中未存储有用户面安全策略，则该目标eNB将直接存储用户面安全策略023。

步骤309a、该MME向目标eNB发送未携带用户面安全策略的路径切换响应（path switchover request acknowledge）042。相应的，目标eNB从MME接收未携带用户面安全策略的路径切换响应042。

25 相比于传统技术中，MME在收到未携带用户面安全策略的路径切换请求之后，该MME为了尽可能让4G网络中的eNB和UE能够开启用户面完整性保护，便会向目标eNB发送用户面安全策略。此时，目标eNB和UE很可能无法使用该用户面安全策略。而本实施例中，当指示信息011指示UE支持用户面安全按需保护时，该目标eNB会将构造或预配置的用户面安全策略021发送至MME。由此可知，若指示信息011指示UE不支持用户面安全按需保护，
30 则该目标eNB不会向MME发送用户面安全策略，相应的MME也无法从目标eNB收到用户面安全策略。此时，可以推断出UE不支持用户面安全按需保护，即使向该目标eNB提供了用户面安全策略，该目标eNB也无法使用该用户面安全策略为该UE开启用户面完整性保护。因此，设置MME在收到未携带用户面安全策略的路径切换请求时，向目标eNB发送未携带用户面安全策略的路径切换响应，即不向目标eNB提供用户面安全策略。因此，降低了目标eNB收到不能使用的信元的几率，降低了目标eNB与MME之间的数据传输复杂度。
35

步骤309b、MME判断用户面安全策略021与MME中的用户面安全策略是否一致。

若用户面安全策略021与MME中的用户面安全策略不一致，则该MME将执行步骤310。

若用户面安全策略021与MME中的用户面安全策略一致，则该MME向目标eNB发送未携带用户面安全策略的路径切换响应。

其中，用户面安全策略022可以根据归属用户服务器HSS获得的用户面安全策略获得，也可以根据移动管理实体预配置的用户面安全策略获得。

5 示例性的，在UE接入网络的过程中，UE会向MME发送附着请求（attach request），其中，该附着请求中携带了UE的标识，例如，国际移动用户识别码（international mobile subscriber identity, IMSI）。然后，该MME通过位置更新请求（update location request）将UE的标识发送至HSS，该HSS向MME发送位置更新响应（update location request acknowledge），其中，该位置更新响应携带该UE的签约数据，该签约数据中可能包含前述
10 用户面安全策略。

在一种可选的实施方式中，若步骤307b中的路径切换请求031携带一个用户面安全策略021，该用户面安全策略021为UE粒度的安全策略，则该MME将该MME中的UE粒度的用户面安全策略与该用户面安全策略021对比。此时，若用户面安全策略021与MME中的UE粒度的用户安全策略是一致的，则该MME向目标eNB发送未携带用户面安全策略的路径切换
15 响应。若用户面安全策略021与MME中的UE粒度的用户安全策略不一致，则该MME执行步骤310。

在另一种可选的实施方式中，若步骤307b中路径切换请求031携带一个或多个用户面安全策略021，其中，每个用户面安全策略021为E-RAB粒度的策略。此时，MME分别对比每个E-RAB对应的用户面安全策略，若每个E-RAB对应的用户面安全策略021与MME中的对
20 应E-RAB对应的用户安全策略均一致，则该MME向目标eNB发送未携带用户面安全策略的路径切换响应；若存在至少一个E-RAB对应的用户面安全策略021与MME中的对应E-RAB对应的用户安全策略不一致，则该MME执行步骤310。

示例性的，若步骤307b中的路径切换请求031携带3个用户面安全策略021，例如，用户面安全策略021a、用户面安全策略021b和用户面安全策略021c。其中，用户面安全策略021a
25 对应E-RAB1，用户面安全策略021b对应E-RAB2，用户面安全策略021c对应E-RAB3。若MME内部存储的用户面安全策略为：与E-RAB1对应的用户面安全策略021d，与E-RAB2对应的用户面安全策略021b，与E-RAB3对应的用户面安全策略021c。此时，由于路径切换请求携带的E-RAB1对应的用户面安全策略021a与MME中存储的E-RAB1对应的用户面安全策略021d不一致，因此，该MME将向目标eNB回复携带用户面安全策略021d的路径切换响
30 应，该路径切换响应中还将携带前述E-RAB1的标识。

步骤310、MME向目标eNB发送携带用户面安全策略022的路径切换响应041。相应的，目标eNB从MME接收携带用户面安全策略022的路径切换响应041。

可选的，若步骤307d中MME接收的路径切换请求033未携带用户面安全策略，但是，该未携带用户面安全策略的路径切换请求033携带指示信息011，并且，该指示信息012指示
35 UE支持用户面安全按需保护，则MME将向目标eNB发送携带指示信息012和用户面安全策略023的路径切换响应043。

步骤311、目标eNB将该用户面安全策略022存储于该UE的上下文中。

应当理解的是，若该UE的上下文中存储有用户面安全策略（例如，用户面安全策略021），则该目标eNB将采用用户面安全策略022更新存储于UE的上下文中的用户面安全策略021。若该UE的上下文中未存储有用户面安全策略，则该目标eNB将直接存储用户面安全策略022。

5 步骤312、当UE当前的用户面安全激活状态与用户面安全策略022不匹配，则该目标eNB根据该用户面安全策略022开启或不开启该UE的用户面加密保护和/或用户面完整性保护。

其中，用户面安全策略022包括用户面加密保护策略和用户面完整性保护策略。

当满足如下任意一项时，UE当前的用户面安全激活状态与用户面安全策略022不匹配：

10 UE的用户面安全激活状态为加密保护未开启，且，该用户面加密保护策略指示需要开启（required）；

或者，UE的用户面安全激活状态为加密保护开启，且，该用户面加密保护策略指示不需要开启（not needed）；

或者，UE的用户面安全激活状态为完整性保护未开启，且，该用户面完整性保护策略指示需要开启（required）；

15 或者，UE的用户面安全激活状态为完整性保护开启，且，该用户面完整性保护策略指示不需要开启（not needed）。

具体地，该目标eNB根据该用户面安全策略022开启或关闭该UE的加密保护和/或完整性保护状态的过程可以是：

20 当该用户面加密保护策略指示需要开启（required），且，该UE的加密保护未开启，则该目标eNB指示该UE开启用户面加密保护。

当该用户面加密保护策略指示不需要开启（not needed），且，该UE的加密保护开启，则该目标eNB指示该UE关闭用户面保护。

当该用户面完整性保护策略指示需要开启（required），且，该UE的完整性保护未开启，则该目标eNB指示该UE开启用户面完整性保护。

25 当该用户面完整性保护策略指示不需要开启（not needed），且，该UE的完整性保护开启，则该目标eNB指示该UE关闭用户面保护。

应当理解的是，在如下两种情况下，该目标eNB可以根据自身情况调整UE的用户面安全激活状态：

30 当该用户面加密保护策略指示推荐开启（preferred），且，该UE的加密保护未开启，则该目标eNB指示该UE开启用户面加密保护或不开启用户面加密保护。

当该用户面完整性保护策略指示推荐开启（preferred），且，该UE的完整性保护未开启，则该目标eNB指示该UE开启用户面完整性保护或不开启用户面完整性保护。

本实施例中，由于目标eNB能够根据指示信息011确定UE是否支持用户面安全按需保护，若该UE支持用户面安全按需保护，该目标eNB才向MME发送用户面安全策略。避免了
35 当UE不支持用户面安全按需保护，且，MME在未从目标eNB收到用户面安全策略时，MME向该目标eNB发送用户面安全策略，而造成目标eNB即使收到该用户面安全策略也无法为该UE开启用户面安全按需保护的情况。因此，有利于减少MME向目标eNB发送该eNB不需要

的信元，进而有利于简化传输复杂度。

如图 4 所示，为本申请提出的安全策略处理方法的另一种实施方式，该接入网设备和移动管理实体将执行如下步骤：

5 步骤 401、移动管理实体获取指示信息 013。

该移动管理实体可以通过如下多种实现方式获取前述指示信息 013：

在一种可能的实施方式中，该移动管理实体通过附着流程从终端设备获取前述指示信息 013。示例性的，在终端设备接入网络的过程中，终端设备会向移动管理实体发送附着请求（attach request），该附着请求中携带前述指示信息 013。

10 在另一种可能的实施方式中，该移动管理实体通过跟踪区更新流程从终端设备获取前述指示信息 013。示例性的，终端设备会向移动管理实体发送跟踪区更新请求（tracking area update request），该跟踪区更新请求中携带前述指示信息 013。

在另一种可能的实施方式中，该移动管理实体通过分组数据网连接建立流程从终端设备获取前述指示信息 013。示例性的，终端设备会向移动管理实体发送分组数据网连接请求（PDN connectivity request），该分组数据网连接请求中携带前述指示信息 013。或者，该移动管理实体通过附着流程或者跟踪区更新流程从终端设备获取前述指示信息 013 后，在终端设备的上下文中保存指示信息 013。该移动管理实体通过承载分组数据网连接请求的 S1 消息中的终端设备的标识（例如，eNB UE S1AP ID 或 MME UE S1AP ID）获得终端设备的上下文后，获得该终端设备的上下文中保存的指示信息 013。

20 在另一种可能的实施方式中，该移动管理实体通过路径切换请求从目标接入网设备获取前述指示信息 013。示例性的，在终端设备变更接入网设备时，即终端设备在切换、恢复或重建等场景下从源接入网设备变更至目标接入网设备时，目标接入网设备会向移动管理实体发送路径切换请求，该路径切换请求中携带前述指示信息 013。或者，该移动管理实体通过附着流程或者跟踪区更新流程或者分组数据网连接建立流程从终端设备获取前述指示信息 013 后，在终端设备的上下文中保存指示信息 013。该移动管理实体通过路径切换请求中的终端设备的标识（例如，eNB UE S1AP ID 或 MME UE S1AP ID）获得终端设备的上下文后，获得该终端设备的上下文中保存的指示信息 013。

本实施例中的，指示信息 013 可以由移动管理实体通过前述任意一种实施方式获取，具体此处不做限定。

30 其中，该指示信息 013 用于指示终端设备是否支持用户面安全按需保护。或者进一步的，指示信息 013 用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护。所述终端设备是否支持用户面安全按需保护，可以理解为，所述终端设备是否支持开启用户面加密保护和/或是否支持开启用户面完整性保护，即终端设备的用户面加密保护和/或用户面完整性保护不是固定的。终端设备是否支持与接入网设备之间的用户面安全按需保护，可以理解为，所述终端设备是否支持在接入网设备的指示下开启/不开启用户面加密保护和/或用户面完整性保护。这里的接入网设备可以是 eNB，例如，后文提及的源 eNB 或目标 eNB。应当理解的是，关于指示信息 013 的多种表述之间可以相互替换，在后续实施例中，

采用“指示信息 013 用于指示终端设备是否支持用户面安全按需保护”这种表述为例进行介绍。

具体地，该指示信息 013 可以由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。示例性的，前述终端设备的演进分组系统安全能力为 UE 演进分组系统安全能力（UE EPS security capabilities），该指示信息 013 可以用 UE 的安全能力中一个预留的比特位来指示，例如 EEA7 或者 EIA7。其中，EEA7 代表 UE 演进分组系统安全能力中为第八个加密算法预留的比特位，EIA7 代表 UE 演进分组系统安全能力中为第八个完整性算法预留的比特位，而本实施例将该比特位用于携带终端设备是否支持用户面安全按需保护的指示。

应当注意的是，本实施方式中的指示信息 013 与前述实施方式中的指示信息 011 可能是同一个指示信息，也可能是不同的指示信息。但是，指示信息 011 和指示信息 013 都用于指示终端设备是否支持用户面安全按需保护。

由于，无论接入网设备是否升级（即接入网设备是否支持用户面安全按需保护），该接入网设备均能够识别并转发终端设备的演进分组系统安全能力（例如，UE 演进分组系统安全能力）；类似的，无论终端设备是否升级（即终端设备是否支持用户面安全按需保护），该终端设备均能够发送终端设备的演进分组系统安全能力（例如，UE 演进分组系统安全能力）。因此，将指示信息 013 携带于终端设备的演进分组系统安全能力中能够保证指示信息 013 在传输时不丢失。而传统技术中，重新定义的一个指示信息用于指示终端设备是否支持用户面安全按需保护，该重新定义的指示信息不能够被未升级的接入网设备（或未升级的终端设备）识别。也就是说，不支持用户面安全按需保护的接入网设备无法识别该重新定义的指示信息，若该不支持用户面安全按需保护的接入网设备收到前述重新定义的指示信息，则该不支持用户面安全按需保护的接入网设备将丢弃前述重新定义的指示信息而无法发送给移动管理实体等。同样的，不支持用户面安全按需保护的终端设备无法识别前述重新定义的指示信息，若该不支持用户面安全按需保护的接入网设备收到前述重新定义的指示信息，则该不支持用户面安全按需保护的接入网设备将丢弃前述重新定义的指示信息而无法发送给移动管理实体等。

步骤 402、移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024。

在一种可选的实施方式中，该指示信息 013 携带于路径切换请求 034 中，为该终端设备提供服务的接入网设备为目标接入网设备。此时，该移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，具体可以为：当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该路径切换请求 034 未携带用户面安全策略时，该移动管理实体向该目标接入网设备发送携带该用户面安全策略 024 的路径切换响应 044。

在另一种可选的实施方式中，该指示信息 013 携带于非接入层（non-access stratum，NAS）消息中，其中，该非接入层消息包括附着请求（attach request）、位置更新请求（update location request）等。为该终端设备提供服务的接入网设备为源接入网设备。此时，移动管

理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，具体可以为：当该指示信息 013 指示该终端设备支持用户面安全按需保护时，该移动管理实体向该源接入网设备发送该用户面安全策略 024。

在另一种可选的实施方式中，该移动管理实体通过附着流程或者跟踪区更新流程从终端设备获取前述指示信息 013 后，在终端设备的上下文中保存指示信息 013。该移动管理实体通过承载分组数据网连接请求的 S1 消息中的终端设备的标识（例如，eNB UE S1AP ID 或 MME UE S1AP ID）获得终端设备的上下文后，获得该终端设备的上下文中保存的指示信息 013。此时，为该终端设备提供服务的接入网设备为源接入网设备。此时，移动管理实体根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024，具体可以为：当 MME 中保存的指示信息 013 指示该终端设备支持用户面安全按需保护时，该移动管理实体向该源接入网设备发送该用户面安全策略 024。

应当注意的是，前几种实施方式中，移动管理实体向接入网设备发送的用户面安全策略 024 可以来自于归属用户服务器 HSS，也可以是由该移动管理实体预配置的。

具体地，该移动管理实体在获取前述指示信息 013 之后，向接入网设备发送用户面安全策略 024 之前，该移动管理实体将从归属用户服务器接收该终端设备的签约数据。其中，该签约数据是该终端设备在签约时存储至归属用户服务器的数据，该签约数据可能包括该终端设备的用户面安全策略。应理解，该用户面安全策略可以在签约时确定，也就是说，该终端设备在签约时便签订了需要使用用户面安全按需保护的服务；该签约数据也可能不包括用户面安全策略，可以理解为，该终端设备在签约时没有签订需要使用用户面安全按需保护的服务。

在一种可能的实施方式中，该签约数据包括该用户面安全策略 024，并且，前述指示信息 013 指示该终端设备支持用户面安全按需保护，则该移动管理实体存储该用户面安全策略 024。此时，步骤 402 中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略可以是该移动管理实体存储在该移动管理实体中的来自归属用户服务器的用户面安全策略 024。

在另一种可能的实施方式中，该移动管理实体预配置了用户面安全策略，且该签约数据不包括用户面安全策略，但是，前述指示信息 013 指示该终端设备支持用户面安全按需保护，此时，该移动管理实体将预配置的用户面安全策略作为该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。此时，步骤 402 中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略可以是该移动管理实体存储在该移动管理实体中的由移动管理实体配置的用户面安全策略 024。

可选的，移动管理实体从 HSS 获得或者预配置的用户面安全策略是接入点名称（access point name, APN）粒度的，移动管理实体将 APN 粒度的用户面安全策略映射为 E-RAB 粒度的用户面安全策略后，获得 E-RAB 粒度的用户面安全策略 024。此时，步骤 402 中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略是一个或多个用户面安全策略 024，其中，每个用户面安全策略 024 对应着一个 E-RAB，即每个用户面安全策略 024 是 E-RAB 粒度的安全策略。具体地，该移动管理实体将用户面安全策略 024 和

该用户面安全策略024对应的E-RAB的标识一起发送至接入网设备（源接入网设备或目标接入网设备）。

本实施例中，由于移动管理实体能够根据指示信息013确定终端设备是否支持用户面安全按需保护，并在该终端设备支持用户面安全按需保护时才进一步考虑向为该终端设备提供服务的接入网设备发送用户面安全策略。因此，也有利于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。

如图5所示，为本申请提出的安全策略处理方法的另一种实施方式，该接入网设备和移动管理实体将执行如下步骤：

10 步骤501、移动管理实体获取指示信息013。

其中，该指示信息013用于指示终端设备是否支持用户面安全按需保护。具体地，该指示信息013用于指示终端设备是否支持用户面加密保护和/或是否支持用户面完整性保护。该指示信息013由该终端设备的演进分组系统安全能力的部分比特位表征，该终端设备的演进分组系统安全能力用于指示该终端设备支持使用的至少一个安全算法。

15 本实施例中，步骤501与前述步骤401类似，具体请参阅前述步骤401中的相关介绍。步骤502、移动管理实体获取指示信息051。

其中，该指示信息051用于指示为该终端设备提供服务的接入网设备是否支持用户面安全按需保护。或者进一步的，指示信息051用于指示接入网设备是否支持与终端设备之间的用户面安全按需保护。所述接入网设备是否支持用户面安全按需保护，可以理解为，
20 所述接入网设备是否支持开启用户面加密保护和/或是否支持开启用户面完整性保护，即接入网设备的用户面加密保护和/或用户面完整性保护不是固定的。接入网设备是否支持与终端设备之间的用户面安全按需保护，可以理解为，所述接入网设备是否能够指示终端设备开启/不开启用户面加密保护和/或用户面完整性保护。应当理解的是，关于指示信息051的多种表述之间可以相互替换，在后续实施例中，采用“指示信息051用于指示接入网设备
25 是否支持用户面安全按需保护”这种表述为例进行介绍。

具体地，该移动管理实体可以通过多种方式获取前述指示信息051，具体包括如下几种实施方式：

在一种可选的实施方式中，该指示信息051为该移动管理实体从该接入网设备接收的指示信息051-1，也可以理解为，该移动管理实体从该接入网设备接收该指示信息051-1。
30 示例性的，该若该接入网设备为目标接入网设备，则该目标接入网设备可以在向移动管理实体发送的路径切换请求中携带前述指示信息051-1。当然，该接入网设备还可以通过其他与该移动管理实体之间的信令向该移动管理实体发送指示信息051-1。具体本申请不做限定。

在另一种可选的实施方式中，该指示信息051为该移动管理实体从网络管理设备获取的指示信息051-2，可以理解为，该移动管理实体从网络管理设备获取指示信息051-2。其中，前述网络管理设备是能够管理前述接入网设备的相关信息的设备。例如，该网络管理设备可以是操作、管理和维护（operation administration and maintenance, OAM）网元。

应当注意的是，步骤 501 与步骤 502 无时间先后顺序的限定，也就是说，移动管理实体可以先获取指示信息 013 再获取指示信息 051，移动管理实体可以先获取指示信息 051 再获取指示信息 013，移动管理实体也可以同时获取指示信息 013 和指示信息 051。具体此处不做限定。

5 步骤 503、移动管理实体根据该指示信息 013 和该指示信息 051 确定是否向为该终端设备提供服务的接入网设备发送该用户面安全策略 024。

具体地，当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该指示信息 051 指示为该终端设备提供服务的接入网设备支持用户面安全按需保护时，该移动管理实体向该接入网设备发送该终端设备的用户面安全策略 024。也就是说，当该移动管理实体确定该接入网设备和终端设备均支持用户面安全按需保护的时候，不管该移动管理实体是否收到用户面安全策略，该移动管理实体均会向接入网设备发送用户面安全策略 024。此时，该移动管理实体发送给接入网设备的用户面安全策略 024 是该接入网设备能够识别的，并且，该接入网设备有能力根据该用户面安全策略 024 决策是否为终端设备开启用户面加密保护和/或用户面完整性保护。因此，在这种情况下，移动管理实体向接入网设备发送用户面安全策略 024 不会造成信元浪费。

具体地，该移动管理实体在获取前述指示信息 051 之后，向接入网设备发送用户面安全策略 024 之前，该移动管理实体将从归属用户服务器接收该终端设备的签约数据。其中，该签约数据可以是在签约时确定。关于该签约数据的介绍具体可以参阅前述步骤 402 中的描述，此处不再赘述。

20 在一种可能的实施方式中，该签约数据包括该用户面安全策略 024，并且，指示信息 013 指示该终端设备支持用户面安全按需保护，且，指示信息 051 指示该接入网设备支持用户面安全按需保护。此时，该移动管理实体存储该用户面安全策略 024。此时，步骤 503 中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略可以是该移动管理实体存储在该移动管理实体中的来自归属用户服务器的用户面安全策略 25 024。

在另一种可能的实施方式中，该移动管理实体预配置了用户面安全策略，且签约数据不包括用户面安全策略，但是，前述指示信息 013 指示终端设备支持用户面安全按需保护且前述指示信息 051 指示该接入网设备支持用户面安全按需保护。此时，移动管理实体将预配置的用户面安全策略作为该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。此时，步骤 503 中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略可以是该移动管理实体存储在该移动管理实体中的由移动管理实体配置的用户面安全策略 024。

30 可选的，移动管理实体从HSS获得或者预配置的用户面安全策略是接入点名称（access point name, APN）粒度的，移动管理实体将APN粒度的用户面安全策略映射为E-RAB粒度的用户面安全策略后，获得E-RAB粒度的用户面安全策略024。此时，步骤402中移动管理实体发送给接入网设备（源接入网设备或目标接入网设备）的用户面安全策略是一个或多个用户面安全策略024，其中，每个用户面安全策略024对应着一个E-RAB，即每个用户面

安全策略024是E-RAB粒度的安全策略。具体地，该移动管理实体将用户面安全策略024和该用户面安全策略024对应的E-RAB的标识一起发送至接入网设备（源接入网设备或目标接入网设备）。

5 本实施例中，由于移动管理实体能够根据指示信息013确定终端设备是否支持用户面安全按需保护，并且，能够根据指示信息051确定接入网设备是否支持用户面安全按需保护。当前述终端设备和接入网设备均支持用户面安全按需保护时，该移动管理实体才向接入网设备发送用户面安全策略024，以保证该接入网设备有能力使用该用户面安全策略024为终端设备开启用户面加密保护和/或用户面完整性保护。因此，可以避免移动管理实体向不支持用户面安全按需保护的接入网设备发送用户面安全策略，有利于减少移动管理实体向接入网设备发送该接入网设备不需要的信元，进而有利于简化传输复杂度。

前述图4或图5对应实施例所介绍的安全策略处理方法可以应用于切换（Handover）、RRC连接恢复（RRC Connection Resume）以及RRC连接重建（RRC Connection Reestablishment）中任何一种流程中。下面以如图6所示的RRC连接恢复流程为例进行进一步介绍。其中，目标eNB为前述目标接入网设备的一种实现方式，源eNB为前述源接入网设备的一种实现方式、MME为前述移动管理实体的一种实现方式、HSS为前述归属用户服务器的一种实现方式。并且，假设目标eNB为升级的eNB（即支持用户面安全按需保护的eNB），源eNB为未升级的eNB（即不支持用户面安全按需保护的eNB）。前述各个设备将执行如下步骤：

20 步骤601、UE向目标eNB发送RRC连接恢复请求（RRC connection resume request）。相应的，目标eNB从UE接收RRC连接恢复请求。

其中，该RRC连接恢复请求携带UE的标识（例如：I-RNTI或resume ID），该RRC连接恢复请求用于指示该UE需要恢复与目标eNB的连接。

25 步骤602、目标eNB向源eNB发送上下文检索请求（context retrieve request）。相应的，源eNB从目标eNB接收上下文检索请求。

其中，该上下文检索请求携带UE的标识，该上下文检索请求用于向源eNB获取UE的上下文。

步骤603、源eNB向目标eNB发送上下文检索响应（context retrieve response）。相应的，目标eNB从源eNB接收上下文检索响应。

30 其中，该上下文检索响应携带指示信息013，未携带用户面安全策略。其中，指示信息013用于指示UE是否支持用户面安全按需保护。或者进一步的，指示信息013用于指示UE是否支持与eNB之间的用户面安全按需保护。所述UE是否支持用户面安全按需保护，可以理解为，所述UE是否支持开启用户面加密保护和/或是否支持开启用户面完整性保护，即UE的用户面加密保护和/或用户面完整性保护不是固定的。UE是否支持与eNB之间的用户面安全按需保护，可以理解为，所述UE是否支持在eNB的指示下开启/不开启用户面加密保护和/或用户面完整性保护。应当理解的是，关于指示信息013的多种表述之间可以相互替换，在后续实施例中，采用“指示信息013用于指示UE是否支持用户面安

全按需保护”这种表述为例进行介绍。

此外，该指示信息 013 携带于 UE 演进分组系统安全能力 (UE EPS security capabilities) 中，由 UE 的安全能力中一个预留的比特位来指示，例如 EEA7 或者 EIA7。其中，EEA7 代表 UE 演进分组系统安全能力中为第八个加密算法预留的比特位，EIA7 代表 UE 演进分组系统安全能力中为第八个完整性算法预留的比特位，而本实施例将该比特位用于携带终端设备是否支持用户面安全按需保护的指示。其中，关于指示信息 013 的介绍可以参阅前述步骤 201 或步骤 401 中的描述，具体此处不再赘述。

步骤 604、目标 eNB 确定开启用户面加密保护、不开启用户面完整性保护。

由于，目标 eNB 收到的上下文检索响应中不携带用户安全策略，因此，该目标 eNB 可以用默认的（可以理解为，未升级）的方式为 UE 开启安全保护，即总是使用 RRC 保护相同的算法开启用户面加密保护，但不开启用户面完整性保护。一般地，可以将目标 eNB 确定的开启用户面加密保护不开启用户面完整性保护称为用户面安全激活状态，该用户面安全激活状态是目标 eNB 的关于是否为 UE 开启用户面加密保护和/或用户面完整性保护的决策结果。该目标 eNB 需要将该决策结果传输至 UE，以使得该 UE 根据该用户面安全激活状态开启用户面加密保护而不开启用户面完整性保护。因此，该目标 eNB 将执行步骤 605。

步骤 605、目标 eNB 向 UE 发送 RRC 连接恢复 (RRC connection resume)。相应的，UE 从目标 eNB 接收 RRC 连接恢复。

其中，该 RRC 连接恢复用于指示 UE 该目标 eNB 同意该 UE 的 RRC 连接恢复请求。该 RRC 连接恢复携带前述用户面安全激活状态，即开启用户面加密保护不开启用户面完整性保护的状态。

其中，该 RRC 连接恢复包含了 DRB 配置信息。该 DRB 配置信息用于指示 UE 是否开启某个 DRB 的加密保护和/或完整性保护。一般地，若 DRB 配置信息中封装了禁用加密 (ciphering disabled) 字段，则 UE 不开启 DRB 的加密保护；若 DRB 配置信息中未封装禁用加密 (ciphering disabled) 字段，则 UE 开启 DRB 的加密保护。若 DRB 配置信息中封装了完整性保护 (integrity protection) 字段，则 UE 开启 DRB 的完整性保护；若 DRB 配置信息中未封装完整性保护 (integrity protection) 字段，则 UE 不开启 DRB 的完整性保护。

示例性的，在目标 eNB 确定对于该 UE 的所有 DRB，其对应的加密激活状态都为开启，其对应的完整性激活状态都为不开启时，该 RRC 连接恢复不包含 DRB 配置信息。

在一种可选的实施方式中，该 RRC 连接恢复中包含目标 eNB 指示给 UE 的用户面安全激活状态。可以理解为，该 RRC 连接恢复中包含目标 eNB 确定的 DRB 配置信息。此时，该目标 eNB 通过显示的方式指示 UE 不开启用户面加密保护和/或开启用户面完整性保护。

例如，当该 RRC 连接恢复中携带的 DRB 配置信息为禁用加密 (ciphering disabled) 字段和完整性保护 (integrity protection) 字段时，可以理解为，目标 eNB 通过显示的方式向 UE 发送用户面安全激活状态。

在另一种可选的实施方式中，该 RRC 连接恢复中不包含 DRB 配置信息。此时，该目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护和/或不开启用户面完整性保护。可以理解为，目标 eNB 通过隐式的方式向 UE 发送用户面安全激活状态。

例如，当该 RRC 连接恢复中未携带禁用加密（ciphering disabled）字段，也未携带完整性保护（integrity protection）字段时，可以理解为，目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护且不开启用户面完整性保护。

此外，还可能其他的实现方式，例如，当该 RRC 连接恢复中携带的 DRB 配置信息仅包含禁用加密（ciphering disabled）字段时，可以理解为，目标 eNB 通过显示的方式指示 UE 不开启用户面加密保护，并且，通过隐式的方式指示 UE 不开启用户面完整性保护。又例如，当该 RRC 连接恢复中携带的 DRB 配置信息仅包含完整性保护（integrity protection）字段时，可以理解为，目标 eNB 通过隐式的方式指示 UE 开启用户面加密保护，并且，通过显示的方式指示 UE 开启用户面完整性保护。

步骤 606、UE 向目标 eNB 发送 RRC 连接恢复完成（RRC connection resume complete）。相应的，目标 eNB 从 UE 接收 RRC 连接恢复完成。

当 UE 收到前述 RRC 连接恢复之后，该 UE 将根据该 RRC 连接恢复中携带的用户面安全激活状态开启或关闭用户面加密保护和/或用户面完整性保护。待配置完成之后，该 UE 将向目标 eNB 发送 RRC 连接恢复完成。其中，该 RRC 连接恢复完成用于指示该 UE 已经按照 RRC 连接恢复中的指示进行配置并完成 RRC 连接恢复流程。

步骤 607、目标 eNB 向 MME 发送未携带用户面安全策略的路径切换请求 034。相应的，MME 从目标 eNB 接收未携带用户面安全策略的路径切换请求 034。

可选的，路径切换请求 034 携带指示信息 013，该指示信息 013 为该目标 eNB 在步骤 603 中从源 eNB 接收的。由于，该目标 eNB 未从源 eNB 接收到用户面安全策略，即步骤 603 所介绍的上下文检索响应中未携带用户面安全策略，因此，该路径切换请求 034 中也不携带用户面安全策略。具体地，关于指示信息 013 的介绍可以参阅前述步骤 401。

可选的，该路径切换请求 034 还包括指示信息 051，该指示信息 051 用于指示为该 UE 提供服务的目标 eNB 是否支持用户面安全按需保护。具体地，关于指示信息 051 的介绍可以参阅前述步骤 502。

步骤 608、MME 判断路径切换请求中是否携带用户面安全策略。

若该路径切换请求中未携带用户面安全策略，例如，该路径切换请求为路径切换请求 034，该 MME 将执行步骤 609；若该路径切换请求中携带了用户面安全策略，该 MME 将判断该 MME 中的用户面安全策略与该路径切换请求中携带的用户面安全策略是否一致，并基于判断结果确定是否在发送给目标 eNB 的路径切换响应中携带用户面安全策略。具体请参阅图 3 对应实施例中的步骤 309b 至步骤 312 中的相关描述，此处不再赘述。

步骤 609、MME 判断 UE（和目标 eNB）是否支持用户面安全按需保护。

具体地，该 MME 将根据前述指示信息 013（和指示信息 051）判断 UE（和目标 eNB）是否支持用户面安全按需保护。

在一种可选的实施方式中，该 MME 可以仅判断 UE 是否支持用户面安全按需保护，即 MME 根据步骤 607 中接收的指示信息 013 确定该 UE 是否支持用户面安全按需保护。此时，若 UE 支持用户面安全按需保护，则该 MME 执行步骤 610a；若 UE 不支持用户面安全按需保护，则该 MME 执行步骤 610b。

在一另种可选的实施方式中，该 MME 需要判断 UE 和目标 eNB 是否均支持用户面安全按需保护，即 MME 根据指示信息 013 确定该 UE 是否支持用户面安全按需保护，并且，根据指示信息 051 确定目标 eNB 是否支持用户面安全按需保护。此时，若 UE 和目标 eNB 支持用户面安全按需保护，则该 MME 执行步骤 610a；若 UE 不支持用户面安全按需保护，或，目标 eNB 不支持用户面安全按需保护，则该 MME 执行步骤 610b。

步骤 610a、MME 向目标 eNB 发送携带用户面安全策略 024 的路径切换响应 044。相应的，目标 eNB 从 MME 接收携带用户面安全策略 024 的路径切换响应 044。

步骤 610b、MME 向目标 eNB 发送未携带用户面安全策略的路径切换响应 045。相应的，目标 eNB 从 MME 接收未携带用户面安全策略的路径切换响应 045。

本实施方式中，提出在 MME 侧增加判断逻辑，即 MME 在决策是否向 eNB 发送用户面安全策略时，该 MME 根据指示信息 013 进行决策。而传统技术中，MME 仅根据是否收到了来自 eNB 的用户面安全策略进行决策。若没有收到来自 eNB 的用户面安全策略，则该 MME 便向 eNB 发送用户面安全策略。在传统技术方案中，可能是由于 UE 不支持用户面安全按需保护而造成 eNB 无法向 MME 发送用户面安全策略，在这种情况下，MME 向 eNB 发送用户面安全策略，会导致该 eNB 无法利用该用户面安全策略为该 UE 开启用户面完整性保护，造成降低 MME 与 eNB 之间信令的传输效率。而本申请的方案中，MME 仅在 UE 支持用户面安全按需保护时，才向 eNB 发送用户面安全策略。因此，有利于减少 MME 向 eNB 发送该 eNB 不需要的信元，进而有利于简化传输复杂度。

还应理解的是，目标 eNB 在接收来自 MME 的用户面安全策略 024 之后，该目标 eNB 将该用户面安全策略 024 存储于该 UE 的上下文中。此外，当用户面安全策略 024 指示的用户面安全激活状态与该 UE 当前的用户面安全激活状态不匹配，则该目标 eNB 根据该用户面安全策略 024 开启或关闭该 UE 的加密保护和/或完整性保护。具体地，请参阅前文步骤 311 至步骤 312 中的相关描述，具体此处不再赘述。

此外，前述图 4 或图 5 对应实施例所介绍的安全策略处理方法还可以应用于初始接入流程。下面以如图 7 为例进行进一步介绍。其中，源 eNB 为前述源接入网设备的一种实现方式、MME 为前述移动管理实体的一种实现方式、HSS 为前述归属用户服务器的一种实现方式。前述各个设备将执行如下步骤：

步骤 701、UE 向 MME 发送附着请求（attach request）。

其中，附着请求携带指示信息 013 和 UE 的标识。具体地，该指示信息 013 用于指示 UE 是否支持用户面加密保护和/或是否支持用户面完整性保护。该指示信息 013 由该 UE 的演进分组系统安全能力的部分比特位表征，该 UE 的演进分组系统安全能力用于指示该 UE 支持使用的至少一个安全算法。具体请参阅前述步骤 401 中的相关介绍。

步骤 702、MME 向 HSS 发送位置更新请求。

其中，该位置更新请求携带 UE 的标识。该位置更新请求用于请求该 HSS 中存储的 UE 的签约数据。该签约数据可能包括该终端设备的用户面安全策略。应理解，该用户面安全策略可以在签约时确定，也就是说，该终端设备在签约时便签订了需要使用用户面安全按

需保护的服务；该签约数据也可能不包括用户面安全策略，可以理解为，该终端设备在签约时没有签订需要使用用户面安全按需保护的服务。

可选的，HSS 中的用户面安全策略是 APN 粒度的。一个用户面安全策略与一个 APN 的标识对应。

5 步骤 703、HSS 向 MME 发送位置更新响应。

其中，该位置更新响应携带该 UE 的签约数据，该签约数据包括 UE 的用户面安全策略 024。当然，该签约数据还包括其他的关于 UE 的信息，具体地此处不再赘述。

步骤 704、MME 判断 UE（和源 eNB）是否支持用户面安全按需保护。

应当理解的是，步骤 702 至步骤 703 与步骤 704 无时间先后顺序的限定，该步骤 704
10 在步骤 701 之后执行即可。也就是说，该 MME 在收到附着请求中携带的指示信息 013 和 UE ID 之后，一方面，MME 会基于该指示信息 013 判断 UE 是否支持用户面安全按需保护；另一方面，该 MME 会向 HSS 发送携带 UE 的标识的位置更新请求以获取该 UE 的签约数据。

在一种可选的实施方式中，该 MME 可以仅判断 UE 是否支持用户面安全按需保护，
15 即 MME 根据步骤 701 中接收的指示信息 013 确定该 UE 是否支持用户面安全按需保护。

在本实施方式中，当 UE 支持用户面安全按需保护时，该 MME 将依次执行步骤 705a 和步骤 705b；当 UE 不支持用户面安全按需保护时，该 MME 将执行步骤 705c。

在一另种可选的实施方式中，该 MME 需要判断 UE 和目标 eNB 是否均支持用户面安全按需保护，即 MME 根据指示信息 013 确定该 UE 是否支持用户面安全按需保护，并且，
20 根据指示信息 051 确定目标 eNB 是否支持用户面安全按需保护。其中，指示信息 051 可以由该 MME 从与该源 eNB 之间的信令交互中获取，也可以由该 MME 从网络管理设备中获取，具体此处不做限定。

在本实施方式中，当 UE 和源 eNB 均支持用户面安全按需保护时，该 MME 将依次执行步骤 705a 和步骤 705b，或者，该 MME 仅执行步骤 705a；当 UE 不支持用户面安全按需
25 保护或源 eNB 不支持用户面安全按需保护时，该 MME 将执行步骤 705c。

步骤 705a、MME 向源 eNB 发送携带用户面安全策略 024 的 S1 消息。

其中，该 S1 消息携带指示信息 013 和 UE 的用户面安全策略 024。其中，S1 消息可以是初始上下文建立请求（initial context setup request）消息。

可选的，MME 从 HSS 获得 APN 粒度的用户面安全策略，并且，该 MME 将 APN 粒度的用户面安全策略映射为 E-RAB 粒度的用户面安全策略 024 之后，获得一个或多个 E-RAB 粒度的
30 用户面安全策略 024。

此时，步骤 705a 中 MME 发送给源 eNB 的用户面安全策略是一个或多个用户面安全策略 024，其中，每个用户面安全策略 024 对应着一个 E-RAB，即每个用户面安全策略 024 是 E-RAB 粒度的安全策略。具体地，该 MME 将用户面安全策略 024 和该用户面安全策略 024 对应的
35 E-RAB 的标识一起发送至源 eNB。

步骤 705b、MME 存储 UE 的用户面安全策略 024。

本实施例中，步骤 705b 是可选的步骤。

当该 MME 执行步骤 705b 时，步骤 705a 与步骤 705b 之间无时间先后顺序的限定。也就是说，该 MME 可以先执行步骤 705a 再执行步骤 705b，该 MME 也可以先执行 705b 再执行 705a，该 MME 还可以同时执行步骤 705a 和 705b。

步骤 705c、MME 向源 eNB 发送未携带用户面安全策略的 S1 消息。

5 步骤 706、MME 向 UE 发送附着接受（attach accept）。

该附着接受用于指示该 UE 完成附着流程。

本实施方式中，提出在 MME 侧增加判断逻辑，即 MME 在决策是否向源 eNB 发送用户面安全策略时，该 MME 根据指示信息 013（和指示信息 051）进行决策。而传统技术中，MME 仅根据是否从 HSS 中查询到用户面安全策略进行决策。若 HSS 返回的位置更新响应
10 中携带用户面安全策略，则该 MME 才向源 eNB 发送用户面安全策略，否则该 MME 不向源 eNB 发送用户面安全策略。

如图 8 所示，为本申请提供的一种通信设备 80 的结构示意图。前述图 2 对应的方法实施例中的目标接入网设备，以及图 3 对应的方法实施例中的目标 eNB 均可以基于本实施例
15 中图 8 所示的通信设备 80 的结构。

该通信设备 80 包括至少一个处理器 801、至少一个存储器 802 和至少一个收发器 803。可选的，该通信设备 80 还可以包括至少一个网络接口 805 和一个或多个天线 804。其中，处理器 801、存储器 802、收发器 803 和网络接口 805 通过连接装置相连，天线 804 与收发器 803 相连。其中，前述连接装置可包括各类接口、传输线或总线等，本实施例对此不做
20 限定。

其中，前述处理器 801 主要用于对通信协议以及通信数据进行处理，以及对整个网络设备进行控制，执行软件程序，处理软件程序的数据，例如用于支持该通信设备 80 执行前述实施例中所描述的动作。通信设备 80 可以包括基带处理器和中央处理器，其中，基带处理器主要用于对通信协议以及通信数据进行处理，中央处理器主要用于对整个通信设备 80
25 进行控制，执行软件程序，处理软件程序的数据。如图 8 中的处理器 801 可以集成基带处理器和中央处理器的功能。应当理解的是，前述基带处理器和前述中央处理器也可以是各自独立的处理器，通过总线等技术互联。还应理解的是，通信设备 80 可以包括多个基带处理器以适应不同的网络制式，通信设备 80 可以包括多个中央处理器以增强其处理能力，通信设备 80 的各个部件可以通过各种总线连接。所述基带处理器也可以表述为基带处理电路或者基带处理芯片。所述中央处理器也可以表述为中央处理电路或者中央处理芯片。对通信协议以及通信数据进行处理的功能可以内置在处理器中，也可以以软件程序的形式存储在存储器中，由处理器执行软件程序以实现基带处理功能。

此外，前述存储器 802 主要用于存储软件程序和数据。存储器 802 可以是独立存在，与处理器 801 相连。可选的，该存储器 802 可以和该处理器 801 集成于一体，例如，集成
35 于一个或多个芯片之内。其中，该存储器 802 能够存储执行本申请实施例的技术方案的程序代码，并由处理器 801 来控制执行，被执行的各类计算机程序代码也可被视为是处理器 801 的驱动程序。应当理解的是，本实施例中的图 8 仅示出了一个存储器和一个处理器，

但是，在实际应用中，该通信设备 80 可以存在多个处理器或多个存储器，具体此处不做限定。此外，该存储器 802 也可以称为存储介质或者存储设备等。该存储器 802 可以为与处理器处于同一芯片上的存储元件（即片内存储元件），或者为独立的存储元件，本申请实施例对此不做限定。

5 本实施例中，该收发器 803 可以用于支持该通信设备 80 与终端设备（或其他网络设备）之间射频信号的接收或者发送，收发器 803 可以与天线 804 相连。收发器 803 包括发射机 Tx 和接收机 Rx。具体地，一个或多个天线 804 可以接收射频信号，该收发器 803 的接收机 Rx 用于从天线 804 接收所述射频信号，并将射频信号转换为数字基带信号或数字中频信号，并将该数字基带信号或数字中频信号提供给所述处理器 801，以便处理器 801 对该数字基带信号或数字中频信号做进一步的处理，例如解调处理和译码处理。此外，收发器 803 10 中的发射机 Tx 还用于从处理器 801 接收经过调制的数字基带信号或数字中频信号，并将该经过调制的数字基带信号或数字中频信号转换为射频信号，并通过一个或多个天线 804 发送所述射频信号。具体地，接收机 Rx 可以选择性地对射频信号进行一级或多级下混频处理和模数转换处理以得到数字基带信号或数字中频信号，前述下混频处理和模数转换处理的先后顺序是可调整的。发射机 Tx 可以选择性地对经过调制的数字基带信号或数字中频信号 15 时进行一级或多级上混频处理和数模转换处理以得到射频信号，所述上混频处理和数模转换处理的先后顺序是可调整的。数字基带信号和数字中频信号可以统称为数字信号。

应当理解的是，前述收发器 803 也可以称为收发单元、收发机、收发装置等。可选的，可以将收发单元中用于实现接收功能的器件视为接收单元，将收发单元中用于实现发送功能的器件视为发送单元，即收发单元包括接收单元和发送单元，接收单元也可以称为接收机、输入口、接收电路等，发送单元可以称为发射机、发射器或者发射电路等。 20

此外，前述网络接口 805 用于使该通信设备 80 通过通信链路，与其它通信设备相连。具体地，该网络接口 805 可以包括该通信设备 80 与核心网网元之间的网络接口，例如，与 MME 之间的 S1-U 接口、与 S-GW 之间的 S1-MME 接口等；该网络接口 805 也可以包括该 25 通信设备 80 和终端设备之间的网络接口，例如，LTE-Uu 接口。

具体地，处理器 801 控制该收发器 803 接收来自源接入网设备的消息 001，其中，该消息 001 包括指示信息 011。并且，该处理器 801 在该指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，控制该收发器 803 向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，该用户面安全策略 021 用于指示是否 30 开启用户面加密保护和/或是否开启用户面完整性保护。

在一种可选的实施方式中，该处理器 801 用于确定与该终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；以及，构建匹配该用户面安全激活状态的该用户面安全策略 021-1。

在一种可选的实施方式中，该处理器 801 还用于控制该收发器 803 从该移动管理实体接收路径切换响应 041，其中，该路径切换响应 041 携带用户面安全策略 022；将该用户面安全策略 022 存储于该终端设备的上下文中。 35

在一种可选的实施方式中，该处理器 801 还用于当该终端设备当前的用户面安全激活状

态与该用户面安全策略022不匹配时, 根据该用户面安全策略022开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护, 其中, 该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

5 在一种可选的实施方式中, 该处理器 801 还用于在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下, 控制该收发器 803 向该移动管理实体发送未携带用户面安全策略的路径切换请求 032; 以及, 控制该收发器 803 从该移动管理实体接收未携带用户面安全策略的路径切换响应 042。

10 在一种可选的实施方式中, 该处理器 801 还用于在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下, 控制该收发器 803 向该移动管理实体发送未携带用户面安全策略的路径切换请求 033, 该路径切换请求 033 携带该指示信息 011。

15 在一种可选的实施方式中, 该处理器 801 还用于控制该收发器 803 从该移动管理实体接收携带用户面安全策略 023 的路径切换响应 043; 以及, 将该用户面安全策略 023 存储于该终端设备的上下文中。

20 在一种可选的实施方式中, 该处理器801还用于当该终端设备当前的用户面安全激活状态与该用户面安全策略023不匹配时, 根据该用户面安全策略023开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护, 该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

其余可以参考上述图 2 或图 3 实施例中目标接入网设备或目标 eNB 的方法, 此处不再赘述。

25 如图 9 所示, 为本申请提供的另一种通信设备 90 的结构示意图。前述图 4 或图 5 对应的方法实施例中的移动管理实体, 以及图 6 或图 7 对应的方法实施例中的 MME 均可以基于本实施例中图 9 所示的通信设备 90 的结构。

如图 9 所示, 通信设备 90 可以包括处理器 910、存储器 920 和收发器 930。其中, 该处理器 910 与该存储器 920 耦合连接, 该处理器 910 与该收发器 930 耦合连接。

30 其中, 前述收发器 930 也可以称为收发单元、收发机、收发装置等。可选的, 可以将收发单元中用于实现接收功能的器件视为接收单元, 将收发单元中用于实现发送功能的器件视为发送单元, 即收发单元包括接收单元和发送单元, 接收单元也可以称为接收机、输入口、接收电路等, 发送单元可以称为发射机、发射器或者发射电路等。

35 其中, 前述处理器 910 可以是中央处理器、网络处理器 (network processor, NP) 或者 CPU 和 NP 的组合。处理器还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。处理器 910 可以是指一个处理器，也可以包括多个处理器。

此外，前述该存储器 920 主要用于存储软件程序和数据。存储器 920 可以是独立存在，与处理器 910 相连。可选的，该存储器 920 可以和该处理器 910 集成于一体，例如集成于一个或多个芯片之内。其中，该存储器 920 能够存储执行本申请实施例的技术方案的程序代码，并由处理器 910 来控制执行，被执行的各类计算机程序代码也可被视为是处理器 910 的驱动程序。存储器 920 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如只读存储器（read-only memory，ROM），快闪存储器（flash memory），硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）；存储器 920 还可以包括上述种类的存储器的组合。存储器 920 可以是指一个存储器，也可以包括多个存储器。

在一个实现方式中，存储器 920 中存储有计算机可读指令，所述计算机可读指令包括多个软件模块，例如发送模块 921，处理模块 922 和接收模块 923。处理器 910 执行各个软件模块后可以按照各个软件模块的指示进行相应的操作。在本实施例中，一个软件模块所执行的操作实际上是指处理器 910 根据所述软件模块的指示而执行的操作。

具体地，处理模块 922 用于获取指示信息 013，以及根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024。其中，该用户面安全策略 024 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。该指示信息 013 用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护；

在一种可选的实施方式中，该发送模块 921 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该路径切换请求 034 未携带用户面安全策略时，向该目标接入网设备发送携带该用户面安全策略 024 的路径切换响应 044。

在一种可选的实施方式中，该发送模块 921 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护时，向该源接入网设备发送该用户面安全策略 024。

在一种可选的实施方式中，该处理模块 922 用于获取指示信息 051，该指示信息 051 用于指示为该终端设备提供服务的接入网设备是否支持与终端设备之间的用户面安全按需保护，以及根据该指示信息 013 和该指示信息 051 确定是否向为该终端设备提供服务的接入网设备发送该用户面安全策略 024。

在一种可选的实施方式中，该发送模块 921 用于当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该指示信息 051 指示为该终端设备提供服务的接入网设备支持与该终端设备之间的用户面安全按需保护时，向该接入网设备发送该用户面安全策略 024。

在一种可选的实施方式中，该接收模块 923 用于从归属用户服务器接收该终端设备的签约数据；该处理模块 922 用于当该指示信息 013 指示该终端设备支持用户面安全按需保护，且，该签约数据包括该用户面安全策略 024 时，存储该用户面安全策略 024。

在一种可选的实施方式中，该接收模块 923 用于从归属用户服务器接收该终端设备的签约数据；该处理模块 922 用于当该指示信息 013 指示该终端设备支持与接入网设备之间

的用户面安全按需保护，且，该签约数据不包括用户面安全策略时，根据预配置的用户面安全策略 024-1 确定该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。

5 在一种可选的实施方式中，该接收模块 923 用于从归属用户服务器接收该终端设备的签约数据；该处理模块 922 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护，且，该签约数据包括该用户面安全策略 024 时，存储该用户面安全策略 024。

10 在一种可选的实施方式中，该接收模块 923 用于从归属用户服务器接收该终端设备的签约数据；该处理模块 922 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该指示信息 051 指示该接入网设备支持与终端设备之间的用户面安全按需保护，且，该签约数据不包括用户面安全策略时，根据预配置的用户面安全策略 024-2 确定该用户面安全策略 024，并将该用户面安全策略 024 存储于该终端设备的上下文中。

15 其余可以参考上述图 4、图 5、图 6 或图 7 实施例中移动管理实体或 MME 的方法，此处不再赘述。

如图 10 所示，本实施例还提供了一种通信设备 100，该通信设备 100 可以为接入网设备或接入网设备中的芯片。该通信设备 100 包括收发单元 1001、处理单元 1002。

20 如图 11 所示，本实施例还提供了一种通信设备 110，该通信设备 110 可以为移动管理实体或移动管理实体中的芯片。该通信设备 110 包括收发单元 1101、处理单元 1102。

其中，当该通信设备 100 为接入网设备或者 eNB 时，当通信设备 110 为移动管理实体或 MME 时，收发单元 1001 以及收发单元 1101 在发送信息时可以为发送单元或发射器，收发单元 1001 以及收发单元 1101 在接收信息时可以为接收单元或接收器。前述收发单元 25 可以为收发器，或者，集成了发射器和接收器的射频电路。当通信设备 100 或通信设备 110 包含存储单元时，该存储单元用于存储计算机指令，该处理器与存储器通信连接，处理器执行存储器存储的计算机指令，以使得接入网设备以及移动管理实体执行如图 2、图 4、以及图 5 对应的方法实施例涉及的方法，使 eNB 以及 MME 执行图 3、图 6 以及图 7 对应的实施例涉及的方法。此外，前述处理单元 1002 以及处理单元 1102 可以是一个通用中央 30 处理器、微处理器、数字信号处理器（digital signal processor，DSP）、微控制器（micro controller unit，MCU）。该处理器可以是个单独的半导体芯片，也可以跟其他电路一起集成为一个半导体芯片，例如，可以跟其他电路（如编解码电路、硬件加速电路或各种总线 and 接口电路）构成一个片上系统（system-on-a-chip，SoC），或者也可以作为一个特殊应用集成电路 ASIC 的内置处理器集成在所述 ASIC 当中。

35 当该通信设备 100 为接入网设备中的芯片，当该通信设备 110 为移动管理实体中的芯片时，收发单元 1001 以及收发单元 1101 可以是输入和/或输出接口、管脚或电路等。此外，前述处理单元 1002 可以为该接入网设备中的芯片的处理器，该处理单元 1102 可以为

该移动管理实体中的芯片中的处理器。该处理器可执行存储单元存储的计算机执行指令，以使接入网设备内的芯片和移动管理实体内的芯片执行图 2 至 7 对应的实施例涉及的方法。可选地，该存储单元为所述芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是接入网设备或移动管理实体内的位于该芯片外部的存储单元。例如，只读存储器 ROM 或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器 RAM 等。

5 示例性的，对于前述通信设备 100，该收发单元 1001，用于接收来自源接入网设备的消息 001，以及向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031。处理单元 1002，用于控制该收发单元 1001 接收来自源接入网设备的消息 001，其中，该消息 001 包括指示信息 011。并且，该处理器 801 在该指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，控制该收发单元 1001 向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，该用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

10 示例性的，该处理单元 1002 还用于在该指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，控制该收发单元 1001 向该移动管理实体发送未携带用户面安全策略的路径切换请求 033，该路径切换请求 033 携带该指示信息 011。

示例性的，该处理单元 1002 还用于当该终端设备当前的用户面安全激活状态与该用户面安全策略 022 不匹配时，根据该用户面安全策略 022 开启或不开启该终端设备的用户面加密保护和/或用户面完整性保护，其中，该当前的用户面安全激活状态是指该目标接入网设备与该终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

20 其余可以参考上述图 2 或图 3 实施例中目标接入网设备或目标 eNB 的方法，此处不再赘述。

示例性的，对于前述通信设备 110，该处理单元 1102 用于获取指示信息 013，以及根据该指示信息 013 确定是否向为该终端设备提供服务的接入网设备发送用户面安全策略 024。其中，该用户面安全策略 024 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。该指示信息 013 用于指示终端设备是否支持与接入网设备之间的用户面安全按需保护。

25 示例性的，该收发单元 1101 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护，且，该路径切换请求 034 未携带用户面安全策略时，向该目标接入网设备发送携带该用户面安全策略 024 的路径切换响应 044。

30 示例性的，该收发单元 1101 用于当该指示信息 013 指示该终端设备支持与接入网设备之间的用户面安全按需保护时，向该源接入网设备发送该用户面安全策略 024。

其余可以参考上述图 4、图 5、图 6 或图 7 实施例中移动管理实体或 MME 的方法，此处不再赘述。

应当理解的是，前述接入网设备可以存在与接入网设备的方法或者流程的步骤对应的功能单元 (means)，前述移动管理实体可以存在与移动管理实体的方法或者流程的步骤对应的功能单元。以上模块或单元的一个或多个可以软件、硬件或二者结合来实现。当以上任一模块或单元以软件实现的时候，所述软件以计算机程序指令的方式存在，并被存储在

存储器中，处理器可以用于执行所述程序指令以实现以上方法流程。

根据本申请实施例提供的方法，本申请实施例还提供一种通信系统，该通信系统包括终端设备、接入网设备和移动管理实体。其中，接入网设备的结构可以参阅前述图 8 对应实施例中的通信设备 80；移动管理实体的结构可以参阅前述图 9 对应实施例中的通信设备 90。此外，当前述接入网设备为芯片时，该接入网设备可以参阅前述图 10 对应实施例中的通信设备 100；当前述移动管理实体为芯片时，该移动管理实体可以参阅前述图 11 对应实施例中的通信设备 110。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。还应理解，本文中涉及的第一、第二、第三、第四以及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实施例的范围。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权 利 要 求

1、一种安全策略处理方法，其特征在于，包括：

目标接入网设备接收来自源接入网设备的消息 001，所述消息 001 包括指示信息 011；

5 在所述指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，所述目标接入网设备向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，所述用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

2、根据权利要求 1 所述的方法，其特征在于，所述接入网设备为演进型基站 eNB。

3、根据权利要求 1 或 2 所述的方法，其特征在于，当所述目标接入网设备未从所述源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为所述目标接入网设备构建的用户面安全策略 021-1。

4、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

所述目标接入网设备确定与所述终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；

15 所述目标接入网设备构建匹配所述用户面安全激活状态的所述用户面安全策略 021-1。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，所述用户面加密保护策略为需要开启或推荐开启，所述用户面完整性保护策略为不需要开启或推荐开启。

6、根据权利要求 1 或 2 所述的方法，其特征在于，当所述目标接入网设备未从所述源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为预配置在所述目标接入网设备中的用户面安全策略 021-2。

7、根据权利要求 6 所述的方法，其特征在于，所述消息 001 还包括所述终端设备的 N 个演进无线接入承载的标识，所述 N 为大于等于 1 的整数；

所述路径切换请求 031 中还包括所述 N 个演进无线接入承载的标识。

25 8、根据权利要求 7 所述的方法，其特征在于，所述路径切换请求 031 包括 N 个所述用户面安全策略 021-2，其中，所述 N 个演进无线接入承载的标识中每个无线接入承载的标识分别与一个用户面安全策略 021-2 对应。

9、根据权利要求 1 至 8 中任意一项所述的方法，其特征在于，所述目标接入网设备向所述移动管理实体发送携带所述用户面安全策略 021 的路径切换请求 031 之后，所述方法还包括：

30 所述目标接入网设备从所述移动管理实体接收路径切换响应 041，其中，所述路径切换响应 041 携带用户面安全策略 022；

所述目标接入网设备将所述用户面安全策略 022 存储于所述终端设备的上下文中。

10、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

35 如果所述终端设备当前的用户面安全激活状态与所述用户面安全策略 022 不匹配，则所述目标接入网设备根据所述用户面安全策略 022 开启或不开启所述终端设备的用户面加密保护和/或用户面完整性保护，所述当前的用户面安全激活状态是指所述目标接入网设备与

所述终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

11、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，所述目标接入网设备向所述移动管理实体发送未携带用户面安全策略的路径切换请求 032；

所述目标接入网设备从所述移动管理实体接收未携带用户面安全策略的路径切换响应 042。

12、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，所述目标接入网设备向所述移动管理实体发送未携带用户面安全策略的路径切换请求 033，所述路径切换请求 033 携带所述指示信息 011；

所述目标接入网设备从所述移动管理实体接收携带用户面安全策略 023 的路径切换响应 043；

所述目标接入网设备将所述用户面安全策略 023 存储于所述终端设备的上下文中。

13、根据权利要求 12 所述的方法，其特征在于，所述携带用户面安全策略 023 的路径切换响应 043 还携带指示信息 012，其中，所述指示信息 012 用于指示终端设备支持与接入网设备之间的用户面安全按需保护。

14、根据权利要求 12 或 13 所述的方法，其特征在于，所述方法还包括：

如果所述终端设备当前的用户面安全激活状态与所述用户面安全策略 023 不匹配，则所述目标接入网设备根据所述用户面安全策略 023 开启或不开启所述终端设备的用户面加密保护和/或用户面完整性保护，所述当前的用户面安全激活状态是指所述目标接入网设备与所述终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

15、根据权利要求 1 至 14 中任意一项所述的方法，其特征在于，所述指示信息 011 由所述终端设备的演进分组系统安全能力的部分比特位表征，所述终端设备的演进分组系统安全能力用于指示所述终端设备支持使用的至少一个安全算法。

16、根据权利要求 1 至 15 中任意一项所述的方法，其特征在于，所述消息 001 为切换请求或上下文检索响应。

17、一种通信设备，其特征在于，包括：

接收模块，用于接收来自源接入网设备的消息 001，所述消息 001 包括指示信息 011；

处理模块，用于在所述指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，控制发送模块向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，所述用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

18、根据权利要求 17 所述的通信设备，其特征在于，所述接入网设备为演进型基站 eNB。

19、根据权利要求 17 或 18 所述的通信设备，其特征在于，当所述通信设备未从所述源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为所述通信设备构建的用户面安全策略 021-1。

20、根据权利要求 19 所述的通信设备，其特征在于，所述处理模块，还用于：

确定与所述终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；

构建匹配所述用户面安全激活状态的所述用户面安全策略 021-1。

5 21、根据权利要求 19 或 20 所述的通信设备，其特征在于，所述用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，所述用户面加密保护策略为需要开启或推荐开启，所述用户面完整性保护策略为不需要开启或推荐开启。

22、根据权利要求 17 或 18 所述的通信设备，其特征在于，当所述通信设备未从所述源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为预配置在所述通信设备
10 中的用户面安全策略 021-2。

23、根据权利要求 22 所述的通信设备，其特征在于，所述消息 001 还包括所述终端设备的 N 个演进无线接入承载的标识，所述 N 为大于等于 1 的整数；

所述路径切换请求 031 中还包括所述 N 个演进无线接入承载的标识。

24、根据权利要求 23 所述的通信设备，其特征在于，所述路径切换请求 031 包括 N
15 个所述用户面安全策略 021-2，其中，所述 N 个演进无线接入承载的标识中每个无线接入承载的标识分别与一个用户面安全策略 021-2 对应。

25、根据权利要求 17 至 24 中任意一项所述的通信设备，其特征在于，

所述接收模块，还用于从所述移动管理实体接收路径切换响应 041，其中，所述路径切换响应 041 携带用户面安全策略 022；

20 所述通信设备还包括存储模块；

所述存储模块，用于将所述用户面安全策略 022 存储于所述终端设备的上下文中。

26、根据权利要求 25 所述的通信设备，其特征在于，所述处理模块，还用于：

当所述终端设备当前的用户面安全激活状态与所述用户面安全策略 022 不匹配时，根据所述用户面安全策略 022 开启或不开启所述终端设备的用户面加密保护和/或用户面完整性
25 保护，所述当前的用户面安全激活状态是指所述目标接入网设备与所述终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

27、根据权利要求 17 所述的通信设备，其特征在于，

所述发送模块，还用于：

在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的
30 情况下，向所述移动管理实体发送未携带用户面安全策略的路径切换请求 032；

所述接收模块，还用于从所述移动管理实体接收未携带用户面安全策略的路径切换响应 042。

28、根据权利要求 17 所述的通信设备，其特征在于，

所述发送模块，还用于：

35 在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，向所述移动管理实体发送未携带用户面安全策略的路径切换请求 033，所述路径切换请求 033 携带所述指示信息 011；

所述接收模块，还用于从所述移动管理实体接收携带用户面安全策略 023 的路径切换响应 043；

所述通信设备还包括存储模块；

所述存储模块，用于将所述用户面安全策略023存储于所述终端设备的上下文中。

- 5 29、根据权利要求 28 所述的通信设备，其特征在于，所述携带用户面安全策略 023 的路径切换响应 043 还携带指示信息 012，其中，所述指示信息 012 用于指示终端设备支持与接入网设备之间的用户面安全按需保护。

30、根据权利要求28或29所述的通信设备，其特征在于，所述处理模块，还用于：

- 10 当所述终端设备当前的用户面安全激活状态与所述用户面安全策略023不匹配时，所述用户面安全策略023开启或不开启所述终端设备的用户面加密保护和/或用户面完整性保护，所述当前的用户面安全激活状态是指所述目标接入网设备与所述终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

- 31、根据权利要求 17 至 30 中任意一项所述的通信设备，其特征在于，所述指示信息 011 由所述终端设备的演进分组系统安全能力的部分比特位表征，所述终端设备的演进分组系统安全能力用于指示所述终端设备支持使用的至少一个安全算法。

32、根据权利要求 17 至 31 中任意一项所述的通信设备，其特征在于，所述消息 001 为切换请求或上下文检索响应。

- 20 33、一种通信设备，其特征在于，所述通信设备包括处理器、存储器以及收发器，其中，所述存储器中存储有程序代码，所述处理器用于调用存储器中存储的程序代码，用于执行以下操作：

控制所述收发器接收来自源接入网设备的消息 001，所述消息 001 包括指示信息 011；

- 25 在所述指示信息 011 指示终端设备支持与接入网设备之间的用户面安全按需保护的情况下，控制所述收发器向移动管理实体发送携带用户面安全策略 021 的路径切换请求 031，其中，所述用户面安全策略 021 用于指示是否开启用户面加密保护和/或是否开启用户面完整性保护。

34、根据权利要求33所述的通信设备，其特征在于，所述接入网设备为演进型基站 eNB。

35、根据权利要求 33 或 34 所述的通信设备，其特征在于，当所述通信设备未从所述源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为所述通信设备构建的用户面安全策略 021-1。

- 30 36、根据权利要求 35 所述的通信设备，其特征在于，所述处理器，还用于：

确定与所述终端设备之间的用户面安全激活状态为用户面加密保护开启且用户面完整性保护不开启；

构建匹配所述用户面安全激活状态的所述用户面安全策略 021-1。

- 35 37、根据权利要求 35 或 36 所述的通信设备，其特征在于，所述用户面安全策略 021-1 包括用户面加密保护策略和用户面完整性保护策略，其中，所述用户面加密保护策略为需要开启或推荐开启，所述用户面完整性保护策略为不需要开启或推荐开启。

38、根据权利要求 33 或 34 所述的通信设备，其特征在于，当所述通信设备未从所述

源接入网设备收到用户面安全策略时，所述用户面安全策略 021 为预配置在所述通信设备中的用户面安全策略 021-2。

39、根据权利要求 38 所述的通信设备，其特征在于，所述消息 001 还包括所述终端设备的 N 个演进无线接入承载的标识，所述 N 为大于等于 1 的整数；

5 所述路径切换请求 031 中还包括所述 N 个演进无线接入承载的标识。

40、根据权利要求 39 所述的通信设备，其特征在于，所述路径切换请求 031 包括 N 个所述用户面安全策略 021-2，其中，所述 N 个演进无线接入承载的标识中每个无线接入承载的标识分别与一个用户面安全策略 021-2 对应。

41、根据权利要求 33 至 40 中任意一项所述的通信设备，其特征在于，所述处理器，还用于：10

控制所述收发器从所述移动管理实体接收路径切换响应 041，其中，所述路径切换响应 041 携带用户面安全策略 022；

将所述用户面安全策略 022 存储于所述终端设备的上下文中。

42、根据权利要求 41 所述的通信设备，其特征在于，所述处理器，还用于：

15 当所述终端设备当前的用户面安全激活状态与所述用户面安全策略 022 不匹配时，根据所述用户面安全策略 022 开启或不开启所述终端设备的用户面加密保护和/或用户面完整性保护，所述当前的用户面安全激活状态是指所述目标接入网设备与所述终端设备之间当前的用户面加密保护和/或用户面完整性保护的是否开启的状态。

43、根据权利要求 33 所述的通信设备，其特征在于，所述处理器，还用于：

20 在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，控制所述收发器向所述移动管理实体发送未携带用户面安全策略的路径切换请求 032；

控制所述收发器从所述移动管理实体接收未携带用户面安全策略的路径切换响应 042。

44、根据权利要求 33 所述的通信设备，其特征在于，所述处理器，还用于：

25 在所述指示信息 011 指示终端设备不支持与接入网设备之间的用户面安全按需保护的情况下，控制所述收发器向所述移动管理实体发送未携带用户面安全策略的路径切换请求 033，所述路径切换请求 033 携带所述指示信息 011；

控制所述收发器从所述移动管理实体接收携带用户面安全策略 023 的路径切换响应 043；

30 将所述用户面安全策略 023 存储于所述终端设备的上下文中。

45、根据权利要求 44 所述的通信设备，其特征在于，所述携带用户面安全策略 023 的路径切换响应 043 还携带指示信息 012，其中，所述指示信息 012 用于指示终端设备支持与接入网设备之间的用户面安全按需保护。

46、根据权利要求 44 或 45 所述的通信设备，其特征在于，所述处理器，还用于：

35 当所述终端设备当前的用户面安全激活状态与所述用户面安全策略 023 不匹配时，根据所述用户面安全策略 023 开启或不开启所述终端设备的用户面加密保护和/或用户面完整性保护，所述当前的用户面安全激活状态是指所述目标接入网设备与所述终端设备之间当前

的用户面加密保护和/或用户面完整性保护的是否开启的状态。

47、根据权利要求 33 至 46 中任意一项所述的通信设备，其特征在于，所述指示信息 011 由所述终端设备的演进分组系统安全能力的部分比特位表征，所述终端设备的演进分组系统安全能力用于指示所述终端设备支持使用的至少一个安全算法。

5 48、根据权利要求 33 至 47 中任意一项所述的通信设备，其特征在于，所述消息 001 为切换请求或上下文检索响应。

49、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有指令，当所述指令在计算机上运行时，以使得计算机执行如权利要求 1 至 16 中任意一项所述的方法。

10 50、一种包含指令的计算机程序产品，其特征在于，当所述指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 16 中任意一项所述的方法。

51、一种通信系统，其特征在于，包括：

移动管理实体和如权利要求 17 至 32 中任意一项所述的通信设备。

15 52、根据权利要求 51 所述的通信系统，其特征在于，所述通信系统还包括源接入网设备和/或终端设备。