

通信方法和通信装置

本申请要求在 2023 年 04 月 07 日提交中国国家知识产权局、申请号为 202310385227.1 的中国专利申请优先权，发明名称为“通信方法和通信装置”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

本申请涉及通信领域，并且更具体地，涉及一种通信方法和通信装置。

背景技术

在通信系统，例如第五代（5th generation, 5G）通信系统中，随着移动通信的高速发展，新业务类型，如视频聊天、虚拟现实（Virtual Reality, VR）、增强现实（Augmented Reality, AR）等数据业务的普遍使用提高了用户对通信的需求。示例性的，设备到设备通信允许用户设备（user equipment, UE）之间直接进行通信，特别是针对一对多的场景，能够有效的提高通信效率。

然而，当前设备之间的通信可能因为攻击者的恶意篡改信息，导致网络安全无法得到保障。因此，亟需采取额外的措施来应对，以减少潜在的安全风险。

发明内容

本申请提供一种通信方法和通信装置，能够减少潜在的安全风险，提高网络通信安全。

第一方面，提供了一种通信方法，该方法可以由第一通信装置（例如发送者 UE）执行，或者，也可以由用于第一通信装置的芯片或电路执行，本申请对此不作限定。为了便于描述，下面以由第一通信装置执行为例进行说明。

可选地，本申请实施例中的第一通信装置和第二通信装置可以是终端设备，例如手机、汽车、无人机、可穿戴设备等，也可以是终端设备中的芯片。另外，终端设备也可以称为用户设备，因此通信装置也可以是用户设备，或者用户设备中的芯片。本申请对此不作具体限定。

该方法包括：第一通信装置获取邻近服务组对应的安全策略，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，第一通信装置向第二通信装置发送第一消息。其中，安全策略包括机密性安全策略和/或完整性安全策略，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，完整性安全策略用于指示针对邻近服务组的消息是否开启完整性安全保护，邻近服务组包括至少两个成员，且第一通信装置是至少两个成员中的一个，其他字段包括以下一项或者多项：邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、完整性指示信息或者消息认证码（message authentication code, MAC），机密性指示信息用于指示机密性安全保护是否开启，完整性指示信息用于指示完整性安全保护是否开启，安全保护包括机密性安全保护和/或完整性安全保护。

根据本申请提供的方案，通过重新定义第一消息的格式，包括载荷字段和其他字段，并根据邻近服务组对应的安全策略确定是否对载荷字段进行安全保护，以及对其他字段进行赋值，同时，将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息解耦，能够避免安全策略为机密性不需要但完整性需要的场景下完整性校验失败的情况，提高网络通信安全，减少潜在的安全风险。

结合第一方面，在第一方面的某些实现方式中，对第一消息中除载荷字段外的其他字段进行赋值，包括：在机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启的情况下，第一通信装置将 MAC 设置为非零，且将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零。

基于上述方案，针对机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启，将 MAC 设置为非零，将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零，能够避免后续接收者 UE 无法进行完整性校验或者导致完整性校验失败的情况。

发生，能够避免接收者 UE 被欺骗，保障通信安全，降低网络潜在的安全风险。

结合第一方面，在第一方面的某些实现方式中，对第一消息中除载荷字段外的其他字段进行赋值，包括：在机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启的情况下，第一通信装置将机密性指示信息设置为零。

基于上述方案，针对机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启，将 MAC 设置为非零，将机密性指示信息设置为零，能够避免后续接收者 UE 无法进行完整性校验或者导致完整性校验失败的情况发生，能够避免接收者 UE 被欺骗，保障通信安全，降低网络潜在的安全风险。

在本申请实施例中，第一消息中的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数是否取值为 0 不再与机密性安全保护是否开启完全绑定。换句话说，当机密性安全保护不开启（或关闭）时，可以通过该机密性指示信息来指示或确定，对应的，邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数的取值可以为 0，也可以为非 0，本申请对此不作具体限定。当机密性安全保护开启时，也可以通过该机密性指示信息来指示或确定，此时邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数的取值可以为非 0。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，包括：在机密性安全策略指示机密性安全保护开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段进行机密性安全保护，以及将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为非零。

基于上述方案，针对机密性安全策略指示机密性安全保护开启，第一通信装置将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为非零。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，包括：在完整性安全策略指示完整性安全保护开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段进行完整性安全保护，以及将第一消息中携带的 MAC 的取值设置为非零。

基于上述方案，针对完整性安全策略指示完整性安全保护开启，第一通信装置将第一消息中携带的 MAC 的取值设置为非零。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，包括：在机密性安全策略指示机密性安全保护不开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段不进行机密性安全保护，以及将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为零。

基于上述方案，针对机密性安全策略指示机密性安全保护不开启，第一通信装置将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为零。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，包括：在完整性安全策略指示完整性安全保护不开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段不进行完整性安全保护，以及将第一消息中携带的 MAC 的取值设置为零。

基于上述方案，针对完整性安全策略指示完整性安全保护不开启，第一通信装置将第一消息中携带的 MAC 的取值设置为零。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，包括：第一通信装置根据本地策略和安全策略，确定对第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，本地策略指示第一通信装置对载荷字段进行安全保护的触发条件。

结合第一方面，在第一方面的某些实现方式中，第一通信装置根据本地策略和安全策略，确定对载

荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在安全策略指示可选开启安全保护的情况下,第一通信装置根据本地策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值。

基于上述方案,针对安全策略指示可选开启安全保护,第一通信装置根据本地策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值。

结合第一方面,在第一方面的某些实现方式中,第一通信装置根据本地策略和安全策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在机密性安全策略指示可选开启机密性安全保护,且第一通信装置的类型为路边单元的情况下,第一通信装置确定对载荷字段不进行机密性安全保护,以及将其他字段中携带的机密性指示信息的取值设置为零,或者将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为零。

基于上述方案,针对机密性安全策略指示可选开启机密性安全保护,且第一通信装置的类型为路边单元,第一通信装置将其他字段中携带的机密性指示信息的取值设置为零,或者将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为零。

结合第一方面,在第一方面的某些实现方式中,第一通信装置根据本地策略和安全策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在机密性安全策略指示可选开启机密性安全保护,且第一通信装置的类型为汽车的情况下,第一通信装置确定对载荷字段进行机密性安全保护,以及将其他字段中携带的机密性指示信息的取值设置为非零,或者,第一通信装置将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零。

基于上述方案,针对机密性安全策略指示可选开启机密性安全保护,且第一通信装置的类型为汽车,第一通信装置将其他字段中携带的机密性指示信息的取值设置为非零,或者,第一通信装置将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零。

结合第一方面,在第一方面的某些实现方式中,第一通信装置根据本地策略和安全策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在完整性安全策略指示可选开启完整性安全保护,且邻近服务组中的至少两个成员的类型为路边单元的情况下,第一通信装置确定对载荷字段不进行完整性安全保护,以及将其他字段中携带的MAC的取值设置为零。

基于上述方案,针对完整性安全策略指示可选开启完整性安全保护,且邻近服务组中的至少两个成员的类型为路边单元,第一通信装置确定对载荷字段不进行完整性安全保护,以及将其他字段中携带的MAC的取值设置为零。

结合第一方面,在第一方面的某些实现方式中,第一通信装置根据本地策略和安全策略,确定对载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在完整性安全策略指示可选开启完整性安全保护,且邻近服务组中的至少两个成员的类型为汽车的情况下,第一通信装置确定对载荷字段进行完整性安全保护,以及第一通信装置将其他字段中携带的MAC的取值设置为非零。

基于上述方案,针对完整性安全策略指示可选开启完整性安全保护,且邻近服务组中的至少两个成员的类型为汽车,第一通信装置确定对载荷字段进行完整性安全保护,以及第一通信装置将其他字段中携带的MAC的取值设置为非零。

结合第一方面,在第一方面的某些实现方式中,第一通信装置根据安全策略,确定是否对待发送的第一消息中携带的载荷字段进行安全保护,以及对第一消息中除载荷字段外的其他字段进行赋值,包括:在机密性安全策略指示机密性安全保护不开启,且完整性安全策略指示完整性安全保护不开启的情况下,第一通信装置将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零。

结合第一方面,在第一方面的某些实现方式中,机密性指示信息携带在第一通信装置的分组数据汇聚协议(packet data convergence protocol, PDCP)数据包的信息头中。

结合第一方面,在第一方面的某些实现方式中,第一通信装置获取邻近服务组对应的安全策略,包括:第一通信装置向密钥管理功能网元发送请求消息,请求消息包括邻近服务组的组标识和第一通信装置的安全能力,请求消息用于请求获取与组标识关联的安全策略;第一通信装置接收来自密钥管理功能网元的安全策略。

可选的,安全策略是预配置的。

第二方面,提供了一种通信方法,该方法可以由第二通信装置(例如接收者UE)执行,或者,也可

以由用于第二通信装置的芯片或电路执行，本申请对此不限定。为了便于描述，下面以由第二通信装置执行为例进行说明。

该方法包括：第二通信装置接收来自第一通信装置的第一消息，第一消息包括载荷字段和其他字段，第二通信装置根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护。其中，其他字段包括以下一项或者多项：邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、完整性指示信息或者消息认证码 MAC，机密性指示信息用于指示机密性安全保护是否开启，完整性指示信息用于指示完整性安全保护是否开启，安全策略包括机密性安全策略和/或完整性安全策略，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，完整性安全策略用于指示针对邻近服务组的消息是否开启完整性安全保护，邻近服务组包括至少两个成员，且第二通信装置是至少两个成员中的一个，解安全保护包括解密和/或完整性校验。

根据本申请提供的方案，通过重新定义第一消息的格式，包括载荷字段和其他字段，并根据邻近服务组对应的安全策略确定是否对载荷字段进行安全保护，以及对其他字段进行赋值，同时，将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息解耦，能够避免安全策略为机密性不需要但完整性需要的场景下完整性校验失败的情况，提高网络通信安全，减少潜在的安全风险。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护开启的情况下，第二通信装置确定对载荷字段进行解密；和/或，在完整性安全策略指示完整性安全保护开启的情况下，第二通信装置确定对载荷字段进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行解密；和/或，在完整性安全策略指示完整性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护，包括：第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示完整性安全保护开启，且其他字段中未携带 MAC 或者其他字段中携带的 MAC 的取值为零的情况下，第二通信装置确定载荷字段的完整性校验失败，或者第二通信装置丢弃第一消息。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示完整性安全保护开启，且其他字段中携带的 MAC 的取值为非零的情况下，第二通信装置确定对载荷字段进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示完整性安全保护不开启，且其他字段中携带的 MAC 的取值不为零的情况下，第二通信装置确定对载荷字段不进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示完整性安全保护不开启，且其他字段中未携带 MAC 或者其他字段中携带的 MAC 的取值为零的情况下，第二通信装置确定对载荷字段不进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示可选开启完整性安全保护的情况下，且其他字段中携带的 MAC 的取值为非零的情况下，第二通信装置确定对载荷字段进行完整性校验。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在完整性安全策略指示可选开启完整性安全保护的情况下，且其他字段中未携带 MAC 或者其他字段中携带的 MAC 的取值为零的情况下，第二通信装置确定对载荷字段不进行安全保护。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护不开启，且其他字段中携带

的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个的取值为非零的情况下，第二通信装置确定对载荷字段不进行解密。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护不开启，且其他字段中携带的机密性指示信息指示机密性安全保护开启的情况下，第二通信装置确定对载荷字段不进行解密。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护开启，且机密性指示信息指示机密性安全保护不开启的情况下，第二通信装置确定对载荷字段进行解密。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护可选开启，且机密性指示信息指示机密性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行解密。

结合第二方面，在第二方面的某些实现方式中，第二通信装置根据安全策略和其他字段，确定是否对载荷字段进行解安全保护，包括：在机密性安全策略指示机密性安全保护可选开启，且机密性指示信息指示机密性安全保护开启的情况下，第二通信装置确定对载荷字段进行解密。

结合第二方面，在第二方面的某些实现方式中，机密性指示信息携带在第一通信装置的 PDCP 数据包的信息头中。

结合第二方面，在第二方面的某些实现方式中，第二通信装置获取邻近服务组对应的安全策略，具体为：第二通信装置向密钥管理功能网元发送请求消息，请求消息包括邻近服务组的组标识和第二通信装置的安全能力，请求消息用于请求获取与组标识关联的安全策略；第二通信装置接收来自密钥管理功能网元的安全策略。

可选的，安全策略是预配置的。

上述第二方面及第二方面的某些实现方式的有益效果可以对应参考第一方面相关的描述，在此不予赘述。

第三方面，提供了一种第一通信装置，例如发送者 UE。该装置包括：获取单元，用于获取邻近服务组对应的安全策略。例如，获取单元可以是收发单元，用于从网络侧接收该安全策略。处理单元，用于根据安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值，第一通信装置向第二通信装置发送第一消息。其中，安全策略包括机密性安全策略和/或完整性安全策略，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，邻近服务组包括至少两个成员，且第一通信装置是至少两个成员中的一个，其他字段包括以下一项或者多项：邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、或者消息认证码 MAC，机密性指示信息用于指示机密性安全保护是否开启，安全保护包括机密性安全保护和/或完整性安全保护。

该收发单元可以执行前述第一方面中的接收和发送的处理，处理单元可以执行前述第一方面中除了接收和发送之外的其他处理。

第四方面，提供了一种第二通信装置，例如接收者 UE。该装置包括：收发单元，用于接收来自第一通信装置的第一消息，第一消息包括载荷字段和其他字段。处理单元，用于根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护。其中，其他字段包括以下一项或者多项：邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、或者消息认证码 MAC，机密性指示信息用于指示机密性安全保护是否开启，安全策略包括机密性安全策略和/或完整性安全策略，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，邻近服务组包括至少两个成员，且第二通信装置是至少两个成员中的一个，解安全保护包括解密和/或完整性校验。

该收发单元可以执行前述第二方面中的接收和发送的处理，处理单元可以执行前述第二方面中除了接收和发送之外的其他处理。

第五方面，提供了一种通信装置，包括收发器、处理器和存储器，该处理器用于控制收发器收发信号，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得该通信装置执行上述第一方面或第二方面及其任一种可能实现方式中的方法。

可选地，所述处理器为一个或多个，所述存储器为一个或多个。

可选地，所述存储器可以与所述处理器集成在一起，或者所述存储器与处理器分离设置。

可选地，该通信装置还包括发射机（发射器）和接收机（接收器）。

第六方面，提供了一种通信系统，包括：前述的第一通信装置、第二通信装置、密钥管理功能网元中的一个或多个。

第七方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序或代码，所述计算机程序或代码在计算机上运行时，使得所述计算机执行上述第一方面或第二方面及其任一种可能实现方式中的方法。

第八方面，提供了一种芯片，包括至少一个处理器，所述至少一个处理器与存储器耦合，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得安装有该芯片系统的通信装置执行上述第一方面或第二方面及其任一种可能实现方式中的方法。

其中，该芯片可以包括用于发送信息或数据的输入电路或者接口，以及用于接收信息或数据的输出电路或者接口。

第九方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码被通信装置运行时，使得所述通信装置执行上述第一方面或第二方面及其任一种可能实现方式中的方法。

附图说明

图1是本申请实施例适用的网络架构100的示意图。

图2是本申请实施例提供的通信方法200的流程示意图。

图3是本申请实施例提供的通信方法300的流程示意图。

图4是本申请实施例提供的通信方法400的流程示意图。

图5是本申请实施例提供的通信方法500的流程示意图。

图6是本申请实施例提供的通信方法600的流程示意图。

图7是本申请实施例提供的通信方法700的流程示意图。

图8是本申请实施例提供的通信装置1000的结构示意图。

图9是本申请实施例提供的通信装置2000的结构示意图。

图10是本申请实施例提供的芯片系统3000的结构示意图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

本申请提供的技术方案可以应用于各种通信系统，例如：新无线（new radio, NR）系统、长期演进（long term evolution, LTE）系统、LTE频分双工（frequency division duplex, FDD）系统、LTE时分双工（time division duplex, TDD）系统等。本申请提供的技术方案还可以应用于设备到设备（device to device, D2D）通信，车到万物（vehicle-to-everything, V2X）通信，机器到机器（machine to machine, M2M）通信，机器类型通信（machine type communication, MTC），以及物联网（internet of things, IoT）通信系统或者其他通信系统。

在通信系统中，由运营者运营的部分可称为公共陆地移动网络（public land mobile network, PLMN），也可以称为运营商网络等。PLMN是由政府或其所批准的经营者为公众提供陆地移动通信业务目的而建立和经营的网络，主要是移动网络运营商（mobile network operator, MNO）为用户提供移动宽带接入服务的公共网络。本申请实施例中所描述的PLMN，具体可为符合3GPP标准要求的网络，简称3GPP网络。3GPP网络通常包括但不限于5G网络、第四代移动通信（4th-generation, 4G）网络，以及未来的其他通信系统，例如（6th-generation, 6G）网络等。

为了方便描述，本申请实施例中将以5G网络为例进行说明。

图1是本申请实施例适用的网络架构100的示意图。如图1所示，该网络架构具体可以包括下列网元：

1、用户设备（user equipment, UE）：可以称为终端设备、终端、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、无线通信设备、用户代理或用户装置。终端设备还可以是蜂窝电话、无绳电话、会话启动协议（session initiation protocol, SIP）电话、无线本地环路（wireless local loop, WLL）站、个人数字处理（personal digital assistant, PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、无人机、可穿戴设备，5G

网络中的终端设备或演进的 PLMN 中的终端设备等，本申请实施例对此并不限定。UE 可以通过 Uu 接口与下一代无线接入网（next generation radio access network, NG-RAN）设备相连，例如图 1 所示的 UE#A 和 UE#D 通过 Uu 接口与 NG-RAN 相连。

在与传统蜂窝网络通信相比，可以用于 ProSe 通信的 UE 需要有邻近业务应用（proximity-based services application, ProSe application）功能。两个具有邻近业务应用 ProSe application 功能的 UE 之间也可以通过 PC5 接口相连，例如图 1 所示的 UE#A 与 UE#B 通过 PC5 接口相连，UE#B 与 UE#C 通过 PC5 接口相连，UE#A 与 UE#D 通过 PC5 接口相连。对于同一群组中的多个终端设备（例如 UE#A、UE#B、UE#C 和 UE#D）来说，在进行消息交互时，为了保证网络通信安全，发送者 UE 通常会对该消息进行安全保护，对应的，接收者 UE 在接收到该消息后也会对该消息进行解密安全保护，避免恶意攻击者的篡改。例如，UE#A 与 UE#D 可以分别向运营商网络请求获取该邻近业务组对应的安全参数，UE#A 根据该安全参数对待发送的消息进行安全保护，并向 UE#D 发送经过安全保护的消息，对应的，UE#D 在接收到该消息后，根据该安全参数对该消息进行解密安全保护，从而有效保证通信安全。

2、接入网（access network, AN）：为特定区域的授权用户提供接入网功能，并能够根据用户的级别、业务的需求等使用不同质量的传输隧道。接入网络可以为采用不同接入技术的接入网络。目前的接入网络技术包括：第三代（3rd generation, 3G）系统中采用的无线接入网技术、4G 系统中采用的无线接入网技术、或图 1 所示的 NG-RAN 技术（如 5G 系统中采用的无线接入网技术）等。

基于无线通信技术实现接入网功能的接入网可以称为无线接入网络（radio access network, RAN）。无线接入网能够管理无线资源，为终端提供接入服务，进而完成控制信号和用户数据在终端和核心网之间的转发。

无线接入网设备例如可以是基站（NodeB）、演进型基站（evolved NodeB, eNB 或 eNodeB）、5G 移动通信系统中的下一代基站节点（next generation Node Base station, gNB）、为例移动通信系统中的基站或 wifi 无线热点（WiFi）系统中的接入点（access point, AP）等，还可以是云无线接入网络（cloud radio access network, CRAN）场景下的无线控制器，或者该无线接入网设备可以为中继站、接入点、车载设备、无人机、可穿戴设备以及 5G 网络中的网络设备或者演进的 PLMN 中的网络设备等。本申请实施例对无线接入网设备所采用的具体技术和具体设备形态不做限定。

3、接入管理网元：主要用于移动性管理和接入管理、负责在用户设备与策略控制功能（policy control function, PCF）网元间传递用户策略等，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他功能。接入授权（或鉴权）的功能。

接入和移动管理功能（access and mobility management function, AMF）网元与 UE 进行 NAS 连接。拥有与 UE 相同的 5G NAS 安全上下文。5G NAS 安全上下文包括 NAS 层级密钥与其相同的密钥标识信息，UE 安全能力，上下行 NAS COUNT 值。NAS 层级密钥包括 NAS 加密密钥和 NAS 完整性安全保护密钥，分别用于 NAS 消息的机密性安全保护和完整性安全保护。

在 5G 通信系统中，接入管理网元可以是 AMF 网元。在未来通信系统中，接入管理网元仍可以是 AMF 网元，或者，还可以有其他的名称，本申请不做限定。

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

在 5G 通信系统中，会话管理网元可以是会话管理功能（session management function, SMF）网元。在未来通信系统中，会话管理网元仍可以是 SMF 网元，或者，还可以有其他的名称，本申请不做限定。

5、用户面网元：用于分组路由和转发、用户面数据的服务质量（quality of services, QoS）处理、完成用户面数据转发、基于会话/流级的计费统计，带宽限制等功能等。

在 5G 通信系统中，用户面网元可以是用户面功能（user plane function, UPF）网元。在未来通信系统中，用户面网元仍可以是 UPF 网元，或者，还可以有其他名称，本申请不做限定。

6、数据网络网元：用于提供传输数据的网络。

在 5G 通信系统中，数据网络网元可以是 DN 网元。在未来通信系统中，数据网络网元仍可以是 DN 网元，或者，还可以有其他名称，本申请不做限定。

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

在 4G 通信系统中，该策略控制网元可以是策略和计费规则功能（policy and charging rules function,

PCRF) 网元。在 5G 通信系统中, 该策略控制网元可以是策略控制功能 (policy control function, PCF) 网元。在未来通信系统中, 该策略控制网元仍可以是 PCF 网元, 或者, 还可以有其他名称, 本申请不做限定。

8、数据管理网元: 用于处理用户设备标识, 接入鉴权, 注册以及移动性管理等。

在 5G 通信系统中, 该数据管理网元可以是统一数据管理 (unified data management, UDM) 网元; 在 4G 通信系统中, 该数据管理网元可以是归属用户服务器 (home subscriber serve, HSS) 网元。在未来通信系统中, 数据管理网元仍可以是 UDM 网元, 或者, 还可以有其他的名称, 本申请不做限定。

9、数据存储库网元: 用于负责签约数据、策略数据、应用数据等类型数据的存取功能。

在 5G 通信系统中, 该数据存储库网元可以是统一数据存储库 (unified data repository, UDR) 网元。在未来通信系统中, 数据存储库网元仍可以是 UDR 网元, 或者, 还可以有其他的名称, 本申请不做限定。

10、网络开放功能 (network exposure function, NEF) 实体: 用于安全地向外部开放由 3GPP 网络功能提供的业务和能力等。

11、ProSe 应用服务器 (application server, AS): 可以是 DN 的应用功能 (application function, AF), 也可以是提供 ProSe 服务的 AS 本身。具有 ProSe 应用服务器功能的 AF 具有 23.501 R-15 版本中定义的 AF 的所有功能, 以及具有用于 ProSe 业务的相关功能。也就是说, 在用户面架构中, ProSe 应用服务器与 UE 是通过 UE-RAN-UPF-AF 的路径进行用户面通信。ProSe 应用服务器还可以在控制面架构中, 通过 NEF 与 5G 核心网 (5G core network, 5GC) 中的其他网络功能 (network function, NF) 进行通信。比如通过 NEF 与 PCF 通信。如果 ProSe 应用服务器是 DN 的 AF, 且该 AF 为 5GC 的运营商布置, 则 ProSe 应用服务器还可在控制面架构中, 不通过 NEF 与 5GC 中的其他 NF 进行直接通信, 比如直接与 PCF 通信。

12、5G 直连通信发现名称管理功能 (direct discovery name management function, DDNMF): 具有为开放邻近业务发现 (open ProSe discovery) 分配和处理邻近业务应用标识 (ProSe application identifier) 和邻近业务应用代码 (ProSe application code) 之间映射关系的作用。在受限邻近业务发现 (restricted ProSe direct discovery) 中, 5G DDNMF 可以通过 PC2 接口与邻近业务应用服务器通信, 用于处理发现请求 (discovery request) 的授权, 也具有未分配和处理应用标识 (application identifier) 和受限邻近业务中使用的代码之间映射关系的作用, 其中受限邻近业务中使用的代码包括受限邻近业务代码 (ProSe restricted code)、邻近业务请求代码 (ProSe query code) 和邻近业务回复代码 (ProSe response code)。

目前标准定义中, 5G DDNMF 是 PLMN 粒度的, 即一个 PLMN 只有一个 5G DDNMF。通过移动国家码 (mobile country code, MCC) 和移动网络码 (mobile network code, MNC) 可以唯一确定一个 5G DDNMF。

13、认证服务器功能 (authentication server function, AUSF): AUSF 接收到签约用户发起的认证请求之后, 可通过 UDM 中存储的认证信息和/或授权信息对签约用户进行认证和/或授权, 或者通过 UDM 生成签约用户的认证和/或授权信息。AUSF 可向签约用户反馈认证信息和/或授权信息。

14、邻近业务密钥管理功能 (ProSe key management function, PKMF): 可以负责为使用邻近业务的 UE 生成和分发 PC5 接口连接使用的密钥, UE 需要通过控制面与密钥管理功能 (key management function, KMF) 进行交互以获取 PC5 接口使用的密钥。为便于描述, 本申请实施例中可以将 PKMF 替换为 KMF。

15、邻近业务锚点功能网元 (Prose Anchor Function, PAnF): 用于存储 UE 的 ProSe 安全上下文, 以及 5GPRUK 密钥, 便于后续 PAnF 在接收到 AUSF 的密钥获取请求后, 会基于 5GPRUK ID 检索关联的 5GPRUK。

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

应理解, 上述应用于本申请实施例的网络架构仅是举例说明的从服务化架构的角度描述的网络架构, 适用本申请实施例的网络架构并不局限于此, 任何能够实现上述各个网元的功能的网络架构都适用于本

申请实施例。例如，在某些网络架构中，AMF、SMF 网元、PCF 网元以及 UDM 网元等网络功能网元实体都称为网络功能 NF 网元；或者，在另一些网络架构中，AMF，SMF 网元，PCF 网元，UDM 网元等网元的集合都可以称为控制面功能网元。因为 UE 需要通过用户面与 KMF 和 DDNMF 交互，因此 KMF 和 DDNMF 等网元可以称为用户面网元。

还应理解，图 1 中所示的 AMF、SMF、UPF、NEF、AUSF、NRF、PCF、UDM 等可以理解为核心网中用于实现不同功能的网元，例如可以按需组合成网络切片。这些核心网网元可以各自独立的设备，也可以集成于同一设备中实现不同的功能，本申请对于上述网元的具体形态不作限定。

还应理解，上述命名仅为便于区分不同的功能而定义，不应对本申请构成任何限定。本申请并不排除在 5G 网络以及未来其它的网络中采用其他命名的可能。例如，在 6G 网络中，上述各个网元中的部分或全部可以沿用 5G 中的术语，也可能采用其他名称等。图 1 中的各个网元之间的接口名称只是一个示例，具体实现中接口的名称可能为其他的名称，本申请对此不作具体限定。此外，上述各个网元之间的所传输的消息（或信令）的名称也仅仅是一个示例，对消息本身的功能不构成任何限定。

随着移动通信的高速发展，新业务类型，如视频业务、虚拟现实（virtual reality，VR）/增强现实（augmented reality，AR）等数据业务的普遍使用提高了用户对带宽的需求。本申请技术方案主要适用于 D2D 通信场景，该场景可以是 ProSe 业务，也可以是 v2x 业务，还可以是测角测距业务（即 ranging 业务），本申请提供的网元和密钥名称对业务场景无限制作用。其中，D2D 通信允许 UE 之间直接进行通信，可以在小区网络的控制下与小区用户共享频谱资源，有效地提高频谱资源的利用率。D2D 通信包括一对多通信（One to many communication）以及一对一通信（One to one communication）。一对多通信对应于组播和广播通信，一对一通信对应于单播通信，为了实现一对多通信安全，UE 侧保存多个密钥，部分密钥的具体说明如下所示。

在与传统蜂窝网络通信相比，可以用于 ProSe 通信的 UE 需要有 ProSe Application（临近业务应用）功能。具有 ProSe Application 功能的 UE 之间通过 PC5 口通信，可用于数据面和信令面的信息传输。与 ProSe Application 相对应的是临近业务应用服务器（ProSe Application Server），ProSe Application Server 可以是 DN 的应用功能 AF。具有 ProSe Application server 功能的 AF 具有 23.501 R-15 版本中定义的 AF 的所有功能，以及用于 ProSe 业务的相关功能。

下面对本申请涉及的部分网元和密钥进行简单说明。

（1）密钥管理功能 KMF：KMF 根据本地配置存储有组粒度的安全算法和组成员信息。KMF 用于管理组密钥，UE 可以通过用户面通道与 KMF 进行交互。示例性的，KMF 可以是一个逻辑网元，与其他网元合设。示例性的，KMF 也可以是定位管理网元。

（2）网络管理功能：存储 KMF 的地址信息，并用于管理组标识，网络管理功能存储有组成员信息，用于进行授权。网络管理功能和 KMF 可以是合设的网元，也可以是独立的网元，本申请对此不作限定。

（3）邻近服务多媒体因特网密钥（ProSe MIKEY Key，PMK）：PMK 用于保护 MIKEY 消息的安全。为便于描述，本申请实施例中可以将 PMK 替换为 KMF。该密钥为 UE 粒度的密钥，可以通过预先配置的方式，存储于 UE 和 KMF 中，也可以通过安全传输通道，由密钥管理功能 KMF 发送给 UE。KMF 由 KMF ID 进行标识，例如 KMF ID 为 64bit。

（4）邻近服务组密钥（ProSe Group Key，PGK）：PGK 为群组粒度的密钥，与特定的群组绑定。组标识用于标识 UE 所在的群组信息。PGK 由组标识和 PGK ID 进行关联。示例性的，组标识可以是层 2 的组标识，也可以是分组数据汇聚协议 PDCP 层中携带的组标识，本申请对此不作限定；例如 PGK ID 可以是 8bit 的标识信息。PGK 由密钥管理功能 KMF 发送给 UE，KMF 保护携带有 PGK 消息的安全性。

（5）邻近服务传输密钥（ProSe Traffic Key，PTK）：PTK 为 UE 粒度的密钥，PTK 由组标识、PGK ID、组成员标识（组成员 ID）和 PTK 标识（PTK ID）唯一标识。推演 PTK 的输入密钥为 PGK，输入参数包括 UE 的组成员 ID 和 PTK 标识。组成员 ID 为用于标记 UE 的组内唯一标识，例如，组成员 ID 可以为 24bit 大小。例如 PTK ID 可以是 16bit 的计数器，每次生成新的 PTK 时，PTK ID 单调递增。

示例性的，从 PGK 计算 PTK 时，应使用以下参数来形成 TS 33.220 中指定的密钥导出函数（key derivation function，KDF）的输入 S：

- FC = 0x4A。
- P0 = 组成员身份（例如，可以是发送者 UE 的第 2 层源地址）。
- L0 = 组成员标识的长度（例如，可以是 0x00 0x03）。

- P1 = PTK 标识。
 - L1 = PTK 身份的长度（例如，可以是 0x00 0x02）。
 - P2 = 组标识。
 - L2 = 组标识的长度（例如，可以是 0x00 0x03）。
- 输入密钥应为 256 位 PGK。

(6) 邻近服务加密密钥 (ProSe Encryption Key, PEK) : PEK 用来对广播数据进行机密性安全保护。PTK 为 UE 粒度的密钥，推演 PEK 的输入密钥为 PTK，输入参数包括标记用于计算 PEK 的常数和机密性算法 ID。

(7) 邻近服务完整性密钥 (Prose Integrity Key, PIK) : PIK 用来对广播数据进行完整性安全保护。PIK 为 UE 粒度的密钥，推演 PIK 的输入密钥为 PTK，输入参数包括标记用于计算 PIK 的常数和完整性算法 ID。

示例性的，从 PTK 或 KD-sess 计算 PEK 或 PIK 时，应使用以下参数来形成 TS 33.220 中规定的 KDF 的输入 S：

- FC = 0x4B
- P0 = 0x00 用于派生 PEK，0x01 用于派生 PIK
- L0 = P0 的长度（即 0x00 0x01）
- P1 = 算法标识，算法标识应按照 TS 33.401 [21] 中所述进行设置。
- L1 = 算法标识的长度（即 0x00 0x01）

输入密钥应为 256 位 PTK 或 256 位 KD-sess。

对于长度为 n 位的算法密钥，其中 n 为小于或等于 256，KDF 输出的 256 位中的 n 个最低有效位应用作算法密钥。

图 2 是本申请实施例提供的通信方法 200 的流程示意图。该方法 200 可应用于图 1 的给出的网络架构，主要针对一对多通信安全（广播或者多播场景）。其中，发送者 UE 和接收者 UE 可以是网络覆盖内的 UE，也可以是网络覆盖外的 UE，KMF 可以是指密钥管理网元。如图 2 所示，该方法包括如下多个步骤，未详尽说明的部分可参考现有协议。

S210，发送者 UE 配置签约信息。发送者 UE 发起服务授权流程。

可选的，签约信息中包括密钥管理网元的地址。发送者 UE 配置密钥管理网元的地址，该地址用于发送者 UE 建立到密钥管理网元的用户面传输通道。

可选的，签约信息中包括安全参数。发送者 UE 配置用于接入密钥管理网元的安全参数，例如证书、（预）共享密钥等，该安全参数用于保护发送者 UE 和密钥管理网元之间的传输安全。

针对发送者 UE 发起服务授权流程。在一种实现方式中，发送者 UE 与网络管理功能网元之间建立连接，并且发送者 UE 向网络管理功能网元请求用于一对多通信所需要的参数#1。对应的，网络管理功能网元在接收到来自发送者 UE 的请求后，确定是否对发送者 UE 的请求进行授权，进而确定是否向发送者 UE 提供参数#1。

其中，参数#1 包括以下一项或者多项：组标识、安全策略、KMF 地址。

(1) 组标识：用于标识发送者 UE 所在的群组信息；

(2) 安全策略：主要包括机密性安全策略和完整性安全策略，安全策略的取值包括需要或者不需要，用于指示传输层是否需要安全保护。例如，安全策略用于指示传输层是否需要机密性安全保护和/或完整性安全保护。

可选地，安全策略可以在步骤 S210 预配置的，也可以是从网络侧接收的，例如从 KMF（例如携带在步骤 S240 的密钥响应消息中）接收该安全策略，或者从网络管理功能网元接收该安全策略。可选的，该安全策略与组标识是对应的，即通过组标识可以唯一缺的适用于该群组的安全策略。

其中，安全策略可以是显式指示的，即使用独立的信息元素（information element, IE）来表示，例如，通过 1 比特的指示信息来指示，“1”表示安全策略为需要，“0”表示安全策略为不需要；或者，“true”表示安全策略为需要，“false”表示安全策略为不需要；或者，安全策略也可以是隐式指示的，即根据安全算法来表示。例如，在安全算法为空算法时，表示安全策略为不需要；在安全算法为非空算法时，表示安全策略为需要，本申请对此不作限定。

(3) KMF 地址：用于指示发送者 UE 获取群组密钥的 KMF 的地址信息。

示例性的，在组播场景下，网络管理功能网元可以根据群组信息，确定是否对发送者 UE 的请求进行授权。例如，在发送者 UE 为群组成员的情况下，网络管理功能网元确定对发送者 UE 的请求进行授权，并向发送者 UE 发送参数#1；或者，在发送者 UE 不为群组成员的情况下，网络管理功能网元确定不对发送者 UE 的请求进行授权，并拒绝向发送者 UE 发送参数#1。

示例性的，在广播场景下，网络管理功能网元不对发送者 UE 的请求进行授权，在发送者 UE 请求一对多通信所需要参数#1 的情况下，网络管理功能网元向发送者 UE 发送该参数#1。

S220，发送者 UE 向 KMF 发送密钥请求消息。对应的，KMF 接收来自发送者 UE 的密钥请求消息。

其中，该密钥请求消息用于请求组密钥，该密钥请求消息包括发送者 UE 的安全能力和组标识（例如组 ID）。

示例性的，组标识用于指示发送者 UE 期望获取的组密钥。发送者 UE 的安全能力包括发送者 UE 支持的机密性算法和完整性算法。例如，发送者 UE 支持的机密性算法可以包括但不限于：空加密算法、AES-128 算法、SNOW-3G-128 算法、ZUC-128 算法等，对应的，其算法标识符分别为 NEA0、NEA1、NEA2、NEA3。再例如，完整性安全保护算法可以包括但不限于：空完保算法、AES-128 算法、SNOW-3G-128 算法、ZUC-128 算法等，对应的，其算法标识符分别为 NIA0、NIA1、NIA2、NIA3。

示例性的，密钥请求消息可以是 Key Request 消息。

S230，KMF 校验发送者 UE 是否支持组安全算法。

换句话说，KMF 检查发送者 UE 的安全能力中是否包含组安全算法。

示例性的，若发送者 UE 的安全能力支持的安全算法是空加密算法和 AES-128 算法，组安全算法包括空完保算法，则 KMF 可以确定发送者 UE 不支持组安全算法；或者，若发送者 UE 的安全能力支持的安全算法是空加密算法、空完保算法和 AES-128 算法，组安全算法包括 AES-128 算法，则 KMF 可以确定发送者 UE 支持组安全算法；或者，若发送者 UE 的安全能力支持的安全算法是 AES-128 算法和 SNOW-3G-128 算法，组安全算法包括 SNOW-3G-128 算法和 ZUC-128 算法，则 KMF 可以确定发送者 UE 支持组安全算法。

可选地，组安全算法可以是 KMF 根据本地配置确定的。

S240，KMF 向发送者 UE 发送密钥响应消息。对应的，发送者 UE 接收来自 KMF 的密钥响应消息。

示例性的，在上述步骤 S230 中，若 KMF 确定发送者 UE 支持组安全算法，则 KMF 可以接受步骤 S220 中发送者 UE 的密钥请求，即可以向发送者 UE 提供组密钥。其中，密钥响应消息包括以下一项或者多项：发送者 UE 组成员标识（例如，发送者 UE 组成员 ID）、组安全算法标识（例如，机密性算法 ID 和/或完整性算法 ID）、PGK、PGK ID 等参数。

(1) 组成员 ID：用于标记发送者 UE 在组内的标识；

(2) 组安全算法标识：用来指示发送者 UE 在群组中进行一对多通信时用到的安全算法，组安全算法标识包括机密性算法标识和完整性算法标识。

(3) PGK 和 PGK ID：具体说明可参见上述相关描述，这里不作赘述。可选的，PGK 和 PGK ID 可以携带在步骤 S240 的密钥响应消息中，也可以携带在其他独立的消息中。

可选地，在上述步骤 S230 中，若 KMF 确定发送者 UE 不支持组安全算法，则 KMF 可以拒绝步骤 S220 中发送者 UE 的密钥请求，即拒绝向发送者 UE 提供上述组成员 ID、组安全算法标识、PGK、PGK ID 等参数。例如，KMF 可以通过向发送者 UE 发送密钥响应消息，该密钥响应消息用于指示拒绝提供该组密钥，或者该密钥响应消息用于指示密钥请求失败。可选地，该密钥响应消息包括拒绝原因，例如，拒绝原因可以是发送者 UE 不支持组安全算法。

示例性的，密钥响应消息可以是 Key Response 消息。

S251，接收者 UE 配置签约信息。接收者 UE 发起服务授权流程。

S252，接收者 UE 向 KMF 发送密钥请求消息。对应的，KMF 接收来自接收者 UE 的密钥请求消息。进一步地，KMF 向接收者 UE 发送密钥响应消息。对应的，接收者 UE 接收来自 KMF 的密钥响应消息。

基于上述步骤 S251 和 S252，接收者 UE 可以与网络管理功能网元之间建立连接，并且从网络管理功能网元获取组标识、安全策略（例如，需要或不需要进行安全保护）和 KMF 地址等。同时，在接收者 UE 支持组安全算法的情况下，接收者 UE 也可以从 KMF 获取接收者 UE 的组成员标识、组安全算法标识（例如，机密性算法 ID 和/或完整性算法 ID）、PGK、PGK ID 等参数中的一项或者多项。

其中，上述步骤 S251 和 S252 的具体实现方式，可参考上述步骤 S210 至 S240 中的相关描述，为了

简洁，此处不再过多赘述。

S260，发送者 UE 推演安全密钥。

示例性的，发送者 UE 推演以下一项或多项安全密钥：PTK、PIK 或 PEK，用于保护后续发送者 UE 在群组中进行一对多通信时所发送的消息。其中，PTK、PIK 和 PEK 的具体推演方法可参见上述相关描述，为了简洁，此处不再赘述。

S270，发送者 UE 对消息#1 进行安全保护，例如机密性安全保护和完整性安全保护。

其中，消息#1 包括以下一项或者多项：组标识（例如组 ID）、发送者 UE 的组成员标识（例如发送者 UE ID）、PGK ID、PTK ID、counter、payload、MAC。可选的，密文 enc 可以作为 payload 的一部分，一同发送给接收者 UE。可选地，PGK ID 可以是 8 比特，PTK ID 可以是 16 比特，MAC 可以是 32 比特。

示例性的，在网络侧配置的安全策略指示消息#1 不需要加密，即消息#1 不需要机密性安全保护时，发送者 UE 可以将 PGK ID、PTK ID、counter 都设置为 0；在安全策略指示消息#1 不需要完整性安全保护时，发送者 UE 可以将 MAC 设置为 0。

在一种实现方式中，对消息#1 进行安全保护的输入参数可以包括：PEK/PIK、PTK ID、counter。具体地，算法（见 TS 33.401）与以下修改一起使用：

- direction 始终设置为 0；
- bearer[0]到 bearer [4]设置为 LCID；
- count[0]到 count [15]设置为 PTK ID；
- counter 被输入到 COUNT[16]到 COUNT[31]。

与 PDCP/RLC 实体关联的逻辑信道 ID（LCID），用作加密的输入，以避免密钥流重复。

其中，机密性安全保护是指根据所选的加密算法和加密密钥对消息进行加密。示例性的，加密密钥为 PEK。完整性安全保护（Integrity protection）是指根据所选的完整性算法和完整性保护密钥对消息进行完整性保护。示例性的，完整性保护密钥为 PIK。具体的，通过物理手段或密码学方法来确保信息在生成、传输、存储过程中，以及之后没有被篡改或没有被未经授权的修改。其中，通过密码学方法对信息进行完整性安全保护可以有多种方式，例如使用单向函数（如哈希函数 Hash），以对称密钥（完整性保护密钥）及消息#1 作为输入参数，用来生成 MAC，以实现消息#1 的完整性安全保护。

可选地，在发送者 UE 对消息#1 进行安全保护后，可以将机密性安全保护的密文记作 enc，完整性安全保护的计算结果记作 MAC，counter 作为新鲜性（freshness）参数。应理解，新鲜性参数是指为了防止重放攻击（replay attack）而在输入参数中新添加的参数，输入参数增加了新鲜性参数，可以确保输出参数是新生成的（fresh）。例如，常用的新鲜性参数包括：随机数（Nonce）、时间戳（timestamp）、计数器值（counter 或 index）等。

S280，发送者 UE 发送消息#1。对应的，接收者 UE 接收来自发送者 UE 的消息#1。

示例性的，发送者 UE 通过广播或者组播的方式发送该消息#1。

S290，接收者 UE 推演安全密钥，对消息#1 进行解安全保护。

基于上述步骤和 S252 和 S270，接收者 UE 从 KMF 获取下述参数中的部分或者全部：接收者 UE 组成员标识（例如，接收者 UE 组成员 ID）、组安全算法标识（例如，机密性算法 ID 和/或完整性算法 ID）、PGK、PGK ID；接收者 UE 从发送者 UE 获取的消息#1 包括下述参数中的部分或全部：组标识（例如组 ID）、发送者 UE 的组成员标识（例如发送者 UE ID）、PGK ID、PTK ID、counter、payload、MAC。

示例性的，接收者 UE 可以根据消息#1 中携带的组 ID 和 PGK ID 推演 PGK；根据 PGK、发送者 UE ID 和 PTK ID 推演 PTK；根据 PTK、用于计算 PEK 的常数和机密性算法 ID 推演 PEK；根据 PTK、用于计算 PIK 的常数和完整性安全保护算法 ID 推演 PIK。其中，PGK、PTK 和 PIK 的具体推演过程可参考上述步骤 S260 中的相关描述，为了简洁，此处不再赘述。

可选地，在 PGK ID、PTK ID、counter 不全为 0 的情况下，说明发送者 UE 对消息#1 进行了加密，则接收者 UE 可以根据 PEK 对消息#1 中携带的 payload 的密文进行解密，得到明文；同时，在 MAC 不全为 0 的情况下，说明发送者 UE 对消息#1 进行了完整性安全保护，则接收者 UE 可以根据 PIK 对消息#1 进行完整性安全保护校验。

在一种示例中，根据 PEK 对消息#1 中的密文进行解密，包括：根据所选的加密算法进行解密计算或解密操作。

在一种示例中, 根据 PIK 对消息#1 进行完整性安全保护校验, 包括: 根据所选的完整性算法计算 MAC 值, 并与消息#1 中携带的 MAC 值进行比较, 若二者相同, 则可以认为完整性校验通过; 反之, 则完整性校验失败。具体的, 接收者 UE 可以计算共享密钥 (完整性保护密钥), 并对消息#1 的完整性安全保护进行验证。其中, 共享密钥 (完整性保护密钥) 可以用于接收者 UE 校验接收到的消息#1 所携带的 MAC 是否由发送者 UE 生成, 即校验由发送者 UE 进行完整性安全保护的 message#1 的真实性。如果或者 MAC 是由发送者 UE 的共享密钥 (完整性保护密钥) 生成, 当接收者 UE 使用共享密钥 (完整性保护密钥) 成功地验证该数字签名或 MAC, 说明该消息#1 未被篡改过, 否则验证失败。

针对上述提供的方案, 对于发送者 UE 发送的消息#1, 如果攻击者将消息#1 中取值为非 0 的 MAC, 改为全为 0, 则接收者 UE 将不进行完整性安全保护校验, 因此, 攻击者可以对消息#1 进行篡改, 欺骗接收者 UE, 无法保障通信安全。另外, 在安全策略指示不需要机密性安全保护, 但需要完整性安全保护的情况下, 消息#1 中的 PGK ID、PTK ID、counter 都将被置为 0, 则接收者 UE 无法根据接收到的消息#1 中的参数推演 PIK, 导致完整性安全保护校验失败。

有鉴于此, 本申请提供一种通信方法和通信装置, 通过重新定义第一消息的格式, 包括载荷字段和其他字段, 并根据邻近服务组对应的安全策略确定是否对载荷字段进行安全保护, 以及对其他字段进行赋值, 同时, 将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息解耦, 能够避免安全策略为机密性不需要但完整性需要的场景下完整性校验失败的情况, 提高网络通信安全, 减少潜在的安全风险。

为了便于理解本申请实施例, 作出以下几点说明:

第一, 在本申请中, 如果没有特殊说明以及逻辑冲突, 不同的实施例之间的术语和/或描述具有一致性、且可以相互引用, 不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。

第二, 在本申请中, “至少一个”是指一个或者多个, “多个”是指两个或两个以上。“和/或”, 描述关联对象的关联关系, 表示可以存在三种关系, 例如, A 和/或 B, 可以表示: 单独存在 A, 同时存在 A 和 B, 单独存在 B 的情况, 其中 A, B 可以是单数或者复数。在本申请的文字描述中, 字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达, 是指的这些项中的任意组合, 包括单项(个)或复数项(个)的任意组合。例如, a、b 和 c 中的至少一项(个), 可以表示: a, 或, b, 或, c, 或, a 和 b, 或, a 和 c, 或, b 和 c, 或, a、b 和 c。其中 a、b 和 c 分别可以是单个, 也可以是多个。

第三, 在本申请中, “第一”、“第二”以及各种数字编号 (例如, #1、#2 等) 指示为了描述方便进行的区分, 并不用来限制本申请实施例的范围。例如, 区分不同的消息等, 而不是用于描述特定的顺序或先后次序。应理解, 这样描述的对象在适当情况下可以互换, 以便能够描述本申请的实施例以外的方案。需要说明的是, 本申请实施例中每个步骤的数字仅是一种编号, 不代表执行的先后顺序, 具体执行先后顺序以用文字说明。

第四, 在本申请中, “当……时”、“在……的情况下”以及“如果”等描述均指在某种客观情况下设备会做出相应的处理, 并非限定时间, 且也不要求设备在实现时一定要有所判断的动作, 也不意味着存在其它限定。

第五, 在本申请中, 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。

第六, 在本申请中, “用于指示”可以包括用于直接指示和用于间接指示。当描述某一指示信息用于指示 A 时, 可以包括该指示信息直接指示 A 或间接指示 A, 而并不代表该指示信息中一定携带有 A。本申请中的“指示信息”可以是显式指示, 即通过信令直接指示, 或者根据信令指示的参数, 结合其他规则或结合其他参数或通过推导获取。也可以是隐式指示, 即根据规则或关系, 或根据其他参数, 或推导获取。本申请对此不作具体限定。

第七, 在本申请中, “协议”可以是指通信领域的标准协议, 例如可以包括 5G 协议、NR 协议以及应用于未来的通信系统中的相关协议, 本申请对此不做限定。“预配置”可以包括预先定义。例如, 协议定义。其中, “预先定义”可以通过在设备中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现, 本申请对于其具体的实现方式不做限定。

第八, 在本申请中, “存储”可以是指保存在一个或者多个存储器中。所述一个或者多个存储器可以是单独的设置, 也可以是集成在编码器或者译码器、处理器、或通信装置中。所述一个或者多个存储器,

也可以是一部分单独设置，一部分集成在译码器、处理器、或通信装置中。存储器的类型可以是任意形式的存储介质，本申请并不对此限定。

第九，在本申请中，“通信”还可以描述为“数据传输”、“信息传输”、“数据处理”等，本申请对此不作限定。

下面将结合附图详细说明本申请实施例提供的通信方法。本申请提供的实施例可以适用于发送端设备和接收端设备通信的任何通信场景，如可以应用于上述图 1 和图 2 所示的通信系统中。

在本申请实施例中，消息验证码 MAC 设置为零，表示完整性保护不开启；或者，也可以将 MAC 设置为 false，用于表示完整性保护不开启。反之，MAC 设置为非零，则表示完整性保护开启。例如，若第一消息中的 MAC 取值为零，则说明第一消息中的载荷字段是没有经过完整性安全保护的，若第一消息中的 MAC 取值为非零，则说明第一消息中的载荷字段经过安全保护。

类似的，邻近服务组密钥的标识、邻近服务组传输密钥的标识中的至少一个设置为零，表示机密性保护不开启；或者，也可以将邻近服务组密钥的标识、邻近服务组传输密钥的标识中的至少一个设置为 false，用于表示机密性保护不开启。例如，若第一消息中的邻近服务组密钥的标识、邻近服务组传输密钥的标识的至少一个取值为零，则说明第一消息中的载荷字段没有被加密的。

需要指出的是，上述将第一消息中的除载荷字段外的其他字段（即，邻近服务组密钥的标识、邻近服务组传输密钥的标识、MAC）赋值为零或非零仅是一种示例，可选的，还可以按照布尔型或者字符串的形式对其他字段进行赋值，本申请对此不作限定，为便于理解，本申请实施例中以对其他字段（即，邻近服务组密钥的标识、邻近服务组传输密钥的标识、MAC）赋值为零或非零来表示对应载荷字段是否开启机密性安全保护和/或完整性安全保护。

图 3 是本申请实施例提供的通信方法 300 的流程示意图。该方法 300 可以由通信装置（例如，第一通信装置和第二通信装置）执行，或者，也可以由通信装置的芯片或电路执行，或者还可以由能实现全部或部分通信装置功能的逻辑模块或软件实现，本申请对此不作限制。下面以执行主体为第一通信装置（例如发送者 UE）和第二通信装置（例如接收者 UE）为例进行说明，如图 3 所示，该方法包括如下多个步骤，未详尽说明的部分可参考上述方法 200 或现有协议。

S310，第一通信装置获取邻近服务组对应的安全策略。

其中，安全策略包括机密性安全策略和/或完整性安全策略，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，完整性安全策略用于指示针对邻近服务组的消息是否开启完整性安全保护。示例性的，安全策略的取值可以包括 1 或 0，或者，安全策略的取值可以包括 true 或 false，其中取值为 1 或 true 用于指示第一通信装置对待发送的第一消息进行安全保护，取值为 0 或 false 用于指示第一通信装置对待发送的第一消息不进行安全保护。为了便于描述，下文中以安全策略的取值分别为 1 或 0 进行示例。其中，邻近服务组包括至少两个成员，且第一通信装置是至少两个成员中的一个。

可选地，安全策略可以在步骤 S310 预配置的，也可以是从网络侧接收的，例如从 KMF 接收该安全策略，或者从网络管理功能网元接收该安全策略。可选的，该安全策略与组标识是对应的，即通过组标识可以唯一缺的适用于该群组的安全策略。

可选地，本申请实施例中的第一通信装置和第二通信装置可以是终端设备，例如手机、汽车、无人机、可穿戴设备等，也可以是终端设备中的芯片。另外，终端设备也可以称为用户设备，因此通信装置也可以是用户设备，或者用户设备中的芯片。本申请对此不作具体限定。

应理解，这里的成员是指终端设备，本申请技术方案主要适用于终端设备之间的一对多安全通信场景。其中，邻近服务组对应的安全策略可以理解为：属于同一组内的所有成员在传递信息的过程中使用相同的安全策略，例如网络设备为组内的所有成员配置相同的安全策略，如机密性安全保护开启且完整性安全保护不开启。例如，某一组内包括 5 个 UE，分别是 UE1 至 UE5，该 5 个 UE 中的任意多个 UE 在相互收发消息时，则对该消息进行机密性安全保护，且不进行完整性保护。另外，机密性安全策略用于指示针对邻近服务组的消息是否开启机密性安全保护，完整性安全策略用于指示针对邻近服务组的消息是否开启完整性安全保护，可以理解为该 5 个 UE 中的任意多个 UE 在相互收发消息时，例如 UE1（即，第一通信装置）向 UE2（即，第二通信装置）发送消息时，UE1 根据机密性安全策略确定是否对该消息进行机密性安全保护，对应的，UE2 在接收到该消息后，根据机密性安全策略确定是否对该消息进行解密等，类似的，UE1 根据完整性安全策略确定是否对该消息进行完整性安全保护，对应的，UE2 在接收到该消息后，根据完整性安全策略确定是否对该消息进行完整性校验等。

示例性的，第一通信装置获取安全策略的方式可以是：第一通信装置向密钥管理功能网元发送请求消息，该请求消息包括邻近服务组的组标识和第一通信装置的安全能力，该请求消息用于请求获取与组标识关联的安全策略，对应的，向密钥管理功能网元接收来自第一通信装置的请求消息，并向第一通信装置发送安全策略，对应的，第一通信装置接收来自密钥管理功能网元的安全策略。

可选的，该安全策略是预配置在第一通信装置上的。

S320，第一通信装置根据安全策略，确定是否对待发送的第一消息中携带的载荷字段（payload）进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值。

其中，其他字段包括第一安全参数和/或第二安全参数，第一安全参数也可用于指示是否进行机密性安全保护，第二安全参数也可用于指示是否进行完整性安全保护。其中，第一安全参数包括以下一项或者多项：邻近服务组密钥的标识（例如 PGK ID）、邻近服务组传输密钥的标识（例如 PTK ID）、新鲜性参数（例如计数器值 counter）、或者机密性指示信息，第二安全参数包括完整性指示信息、或者 MAC。其中，机密性指示信息用于指示机密性安全保护是否开启，完整性指示信息用于指示完整性安全保护是否开启，安全保护包括机密性安全保护和/或完整性安全保护。应理解，以上第一安全参数和/或第二安全参数中包含的具体内容仅是示例，其他用于对第一消息进行机密性安全保护的参数同样属于该第一安全参数，其他用于对第一消息进行完整性安全保护的参数同样属于该第二安全参数，本申请对此不作限定。为了便于理解和描述，下文中以第一安全参数为 PGK ID、PTK ID、counter、或者机密性指示信息中的至少一个，第二安全参数为 MAC、完整性指示信息中的至少一个为例进行说明。

示例性的，第一消息包括组标识（group ID）、组成员标识（group member ID）、PGK ID、PTK ID、counter、payload 和 MAC，第一消息的格式如下所示：

组标识	组成员标识	PGK ID	PTK ID	counter	payload	MAC
-----	-------	--------	--------	---------	---------	-----

可选的，机密性指示信息和/或完整性指示信息携带在第一通信装置的 PDCP 数据包的信息头中。例如，该机密性指示信息或完整性指示信息的大小可以是 1 比特。示例性的，在机密性安全保护开启的情况下，该机密性指示信息的取值可以为 1；在机密性安全保护不开启的情况下，该机密性指示信息的取值可以为 0。在完整性安全保护开启的情况下，该完整性指示信息的取值可以为 1；在完整性安全保护不开启的情况下，该完整性指示信息的取值可以为 0。该机密性指示信息可以与邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的一个或多个同时携带在第一消息中，该完整性指示信息可以与 MAC 同时携带在第一消息中，本申请对此不做限定。

下面，针对安全策略用于指示需要（例如，安全策略的取值为 1）或不需要（例如，安全策略的取值为 0）对第一消息进行安全保护的情况下，第一通信装置确定是否对第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值的实现方式进行具体说明。

在本申请实施例中，在第一通信装置根据机密性安全策略，确定对第一消息的载荷字段进行机密性保护的情况下，该载荷字段携带的是所述待发送的消息内容的密文；在第一通信装置根据机密性安全策略，确定对第一消息的载荷字段不进行机密性保护的情况下，该载荷字段携带的是所述待发送的消息内容的明文。

示例性的，在机密性安全策略指示机密性安全保护开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段进行机密性安全保护，以及将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为非零。

示例性的，在机密性安全策略指示机密性安全保护不开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段不进行机密性安全保护，以及将第一消息中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息中的至少一个的取值设置为零。

例如，如果网络配置要使用机密性保护，则第一通信装置根据所选的加密算法为第一消息中的 PGK ID、PTK ID、counter 设置为非零，并且对第一消息中的 payload 加密。如果网络配置不使用机密性保护，则第一通信装置将第一消息中的 PGK ID、PTK ID 和 counter 设置为 0 或非零。

示例性的，在完整性安全策略指示完整性安全保护开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段进行完整性安全保护，以及将第一消息中携带的 MAC 的取值设置为非零，即将 MAC 的取值不设置为全 0，或者，参考图 2 中所述的计算方法或使用规则对 MAC 进行赋值。

示例性的，在完整性安全策略指示完整性安全保护不开启的情况下，第一通信装置确定对待发送的第一消息中携带的载荷字段不进行完整性安全保护，以及将第一消息中携带的 MAC 的取值设置为全 0。

例如，如果网络配置要使用完整性保护，则第一通信装置根据所选的完整性算法计算携带在第一消息中的 MAC。如果网络配置不使用完整性保护，则第一通信装置将第一消息中的 MAC 的取值设置为全 0，或者在待发送的第一消息中不携带 MAC。

示例性的，在机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启的情况下，第一通信装置将 MAC 设置为非零，且将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零，即不设置为 0。

示例性的，在机密性安全策略指示机密性安全保护不开启，且完整性安全策略指示完整性安全保护开启的情况下，第一通信装置将机密性指示信息设置为零。

例如，如果网络配置不使用机密性保护且使用完整性保护，则第一通信装置在第一消息中将安全信息（例如，PGK ID、PTK ID、counter）的值设置为非零，或者将机密性指示信息的值设置为 0，且将第一消息中的 MAC 设置为非 0。

例如，如果网络配置不使用机密性保护和完整性保护，则第一通信装置在第一消息中将安全信息（例如，PGK ID、PTK ID、counter）的值设置为 0，或者将机密性指示信息的值设置为 0，且将第一消息中的 MAC 的取值设置为全 0。

S330，第一通信装置向第二通信装置发送第一消息，对应的，第二通信装置接收来自第一通信装置的第一消息。

S340，第二通信装置根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护。

其中，解安全保护包括解密和/或完整性校验。针对解密和完整性校验的具体实现方式可参考上述方法 200 的相关描述，为了简洁，此处不作赘述。

下面，针对安全策略用于指示需要（例如，安全策略的取值为 1）或不需要（例如，安全策略的取值为 0）对第一消息进行安全保护的情况下，第二通信装置可以根据邻近服务组对应的安全策略，确定是否对载荷字段进行解安全保护的实现方式进行具体说明。

示例性的，在机密性安全策略指示机密性安全保护开启的情况下，第二通信装置确定对载荷字段进行解密。

示例性的，在机密性安全策略指示机密性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行解密。

例如，如果网络配置要使用机密性保护，则第二通信装置根据所选的加密算法进行解密操作。如果网络配置不使用机密性保护，则第二通信装置不对第一消息进行解密。

示例性的，在完整性安全策略指示完整性安全保护开启的情况下，第二通信装置确定对载荷字段进行完整性校验。

示例性的，在完整性安全策略指示完整性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行完整性校验。

例如，如果网络配置要使用完整性保护，则第二通信装置根据所选的完整性算法对第一消息进行完整性校验。如果网络配置不使用完整性保护，则第二通信装置不对第一消息进行完整性校验。

针对安全策略用于指示需要（例如，安全策略的取值为 1）或不需要（例如，安全策略的取值为 0）对第一消息进行安全保护的情况下，第二通信装置还可以根据邻近服务组对应的安全策略和第一消息中携带的除载荷字段外的其他字段的取值，确定是否对载荷字段进行解安全保护。

例如，第二通信装置比较网络设备配置的邻近服务组对应的安全策略和接收到的第一消息中携带的除载荷字段外的其他字段取值是否匹配，若二者不匹配，则可以丢弃该第一消息；反之，若二者匹配，则第二通信装置可以根据安全策略或者字段取值，进一步判断是否解安全保护。

示例性的，在完整性安全策略指示完整性安全保护开启，且第一消息中携带的除载荷字段外的其他字段中未携带 MAC，或者第一消息中携带的除载荷字段外的其他字段中携带的 MAC 的取值为全零的情况下，则说明第一消息中携带的完整性安全保护指示（例如 MAC）与网络侧配置的完整性安全策略不匹配，则第二通信装置可以确定载荷字段的完整性校验失败，或者第二通信装置丢弃第一消息。

示例性的，在完整性安全策略指示完整性安全保护开启，且第一消息中携带的除载荷字段外的其他字段中的 MAC 的取值为非零的情况下，第二通信装置确定对载荷字段进行完整性校验。

例如，当网络侧配置的完整性安全策略指示需要完整性安全保护（例如，取值为 1）时，如果第一消息中携带的 MAC 取值为全 0 或者未携带 MAC，则说明第一消息中携带的完整性安全保护指示与网络侧

配置的完整性安全策略不匹配,则第二通信装置丢弃该第一消息。如果第一消息中携带的 MAC 取值为非全 0,则说明第一消息中携带的完整性安全保护指示(例如 MAC)与网络侧配置的完整性安全策略匹配,则第二通信装置对该第一消息进行完整性校验,例如根据所选的完整性算法计算 MAC 值,并与第一消息携带的 MAC 值进行比较确定是否相同,来验证接收的第一消息的完整性。如果相同则说明完整性保护校验通过,如果不同则说明完整性保护校验失败。

示例性的,在完整性安全策略指示完整性安全保护不开启,且第一消息中携带的除载荷字段外的其他字段中携带的 MAC 的取值不为零的情况下,第二通信装置确定对载荷字段不进行完整性校验。

示例性的,在完整性安全策略指示完整性安全保护不开启,且第一消息中携带的除载荷字段外的其他字段中未携带 MAC,或者第一消息中携带的除载荷字段外的其他字段中携带的 MAC 的取值为全零的情况下,第二通信装置确定对载荷字段不进行完整性校验。

例如,当网络侧配置的完整性安全策略指示不需要完整性安全保护(例如,取值为 0)时,如果第一消息中携带的 MAC 取值为 0 或者未携带 MAC,则说明第一消息中携带的完整性安全保护指示(例如 MAC)与网络侧配置的完整性安全策略匹配,则第二通信装置不对该第一消息进行完整性校验。如果第一消息中携带的 MAC 取值为非 0,则说明第一消息中携带的完整性安全保护指示与网络侧配置的完整性安全策略不匹配,则第二通信装置丢弃该第一消息,或者第二通信装置对该第一消息不进行完整性校验。

可选地,如果网络配置不使用完整性保护,则第二通信装置可以忽略第一消息中携带的 MAC 的取值,对该第一消息不进行完整性校验,或者认为该第一消息完整性校验通过。

示例性的,在机密性安全策略指示机密性安全保护不开启,且第一消息中携带的除载荷字段外的其他字段中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个的取值为非零的情况下,第二通信装置确定对载荷字段不进行解密。

示例性的,在机密性安全策略指示机密性安全保护不开启,且第一消息中携带的除载荷字段外的其他字段中携带的机密性指示信息指示机密性安全保护开启的情况下,第二通信装置确定该其他字段中携带的机密性指示信息指示机密性安全保护开启对载荷字段不进行解密。

例如,当网络侧配置的机密性安全策略指示不需要机密性安全保护(例如,取值为 0)时,如果第一消息中携带的 PGK ID、PTK ID、counter 的取值均为 0,和/或第一消息中携带的机密性指示信息的取值为 0,则说明第一消息中携带的机密性安全保护指示(例如 PGK ID、PTK ID、counter、机密性指示信息)与网络侧配置的机密性安全策略匹配,则第二通信装置不对该第一消息进行解密。如果第一消息中携带的 PGK ID、PTK ID、counter 取值均非 0,和/或第一消息中携带的机密性指示信息的取值为 1,则说明第一消息中携带的机密性安全保护指示与网络侧配置的机密性安全策略不匹配,则第二通信装置丢弃该第一消息,或者第二通信装置对该第一消息不进行解密。

示例性的,在机密性安全策略指示机密性安全保护开启,且机密性指示信息指示机密性安全保护不开启(例如,其他字段中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个的取值为非零,或者其他字段中携带的机密性指示信息指示机密性安全保护不开启)的情况下,第二通信装置确定对载荷字段进行解密。

示例性的,在机密性安全策略指示机密性安全保护开启,且机密性指示信息指示机密性安全保护开启(例如,其他字段中携带的邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个的取值为非零,或者其他字段中携带的机密性指示信息指示机密性安全保护开启)的情况下,第二通信装置确定对载荷字段进行解密。

例如,当网络侧配置的机密性安全策略指示需要机密性安全保护(例如,取值为 1)时,如果第一消息中携带的 PGK ID、PTK ID、counter 的取值均为非零,和/或第一消息中携带的机密性指示信息的取值为 1,则说明第一消息中携带的机密性安全保护指示(例如 PGK ID、PTK ID、counter、机密性指示信息)与网络侧配置的机密性安全策略不匹配,则第二通信装置丢弃该第一消息,或者对该第一消息进行解密。如果第一消息中携带的 PGK ID、PTK ID、counter 取值均为非零,和/或第一消息中携带的机密性指示信息的取值为 0,则说明第一消息中携带的机密性安全保护指示与网络侧配置的机密性安全策略匹配,则第二通信装置对该第一消息进行解密。

根据本申请提供的方案,通过重新定义第一消息的格式,即第一消息包括载荷字段和其他字段,并根据邻近服务组对应的安全策略确定是否对载荷字段进行安全保护,以及对其他字段进行赋值,同时,将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息解耦,能够避免

安全策略为机密性不需要但完整性需要的场景下完整性校验失败的情况，提高网络通信安全，减少潜在的安全风险。

基于上述图 2 所示的方案，当前网络侧配置的安全策略以群组为粒度，指示消息#1 需要安全保护或者不需要安全保护，无法满足群组中不同 UE 的安全需求，适应性、灵活性较弱。例如，当群组中的接收者 UE 为路边单元（roadside unit）时，该消息#1 无机密性安全保护的需求；当群组中的 UE 为汽车时，该消息#1 有机密性安全保护的需求。如果安全策略指示消息#1 需要安全保护时，则路边单元在向汽车广播消息时，始终需要进行加密计算，进而汽车在接收到消息#1 时，始终需要进行解密计算，这将增加计算复杂度、信令开销和通信时延。因此，提出以下方法 400，通过增加安全策略的取值，来满足群组中不同 UE 的安全需求，适应性、灵活性更好。对应的，接收者 UE 可以根据安全策略和消息#1 中携带的其他字段的取值，进一步确定是否对消息#1 进行解安全保护。

图 4 是本申请实施例提供的通信方法 400 的流程示意图。该方法 400 可以由通信装置（例如，第一通信装置和第二通信装置）执行，或者，也可以由通信装置的芯片或电路执行，或者还可以由能实现全部或部分通信装置功能的逻辑模块或软件实现，本申请对此不作限制。下面以执行主体为第一通信装置（例如发送者 UE）和第二通信装置（例如接收者 UE）为例进行说明，如图 4 所示，该方法包括如下多个步骤，未详尽说明的部分可参考上述方法 200、300 或现有协议。

S410，第一通信装置获取邻近服务组对应的安全策略。

其中，安全策略的取值包括 preferred，用于指示对待发送的第一消息可选进行安全保护。

S420，第一通信装置根据安全策略和本地策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值。

下面，针对安全策略用于指示对第一消息可选进行安全保护（例如，安全策略的取值为 preferred）的情况下，第一通信装置确定是否对第一消息中携带的载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值的实现方式进行具体说明。

示例性的，在安全策略指示可选开启安全保护的情况下，第一通信装置根据本地策略，确定对载荷字段进行安全保护，以及对第一消息中除载荷字段外的其他字段进行赋值。

其中，该本地策略指示第一通信装置对载荷字段进行安全保护的触发条件。例如，当第一通信装置的终端类型为路边单元时，不进行机密性安全保护，可选地进行完整性安全保护；当第一通信装置的终端类型为汽车时，进行机密性安全保护，可选地进行完整性安全保护。再例如，当第一通信装置处于封闭的环境中，不进行机密性安全保护和/或完整性安全保护。又例如，当第一通信装置的性能或终端能力不足以支持开启安全保护时，不进行机密性安全保护和/或完整性安全保护。又例如，针对特定业务场景（会话建立、请求注册服务等），第一通信装置需要进行机密性安全保护和/或完整性安全保护。

示例性的，在机密性安全策略指示可选开启机密性安全保护，且第一通信装置的类型为路边单元的情况下，第一通信装置确定对载荷字段不进行机密性安全保护，例如将其他字段中携带的机密性指示信息的取值设置为零，或者将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为零。

示例性的，在机密性安全策略指示可选开启机密性安全保护，且第一通信装置的类型为汽车的情况下，第一通信装置确定对载荷字段进行机密性安全保护，例如将其他字段中携带的机密性指示信息的取值设置为非零，或者，第一通信装置将邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数中的至少一个设置为非零。

例如，如果网络配置可选使用机密性保护，机密性安全策略的取值为 preferred，则第一通信装置根据自身终端类型，例如路边单元，确定对第一消息不进行机密性安全保护，则将第一消息中的 PGK ID、PTK ID、counter 的值设置为零，或者将机密性指示信息的值设置为 0。可选地，将第一消息中的 MAC 设置为 0 或非 0。

S430，第一通信装置向第二通信装置发送第一消息，对应的，第二通信装置接收来自第一通信装置的第一消息。

S440，第二通信装置根据邻近服务组对应的安全策略和其他字段，确定是否对载荷字段进行解安全保护。

其中，解安全保护包括解密和/或完整性校验。

下面，针对安全策略用于指示对第一消息可选进行安全保护（例如，安全策略的取值为 preferred）

的情况下，第二通信装置根据邻近服务组对应的安全策略和其他字段，确定是否对载荷字段进行解安全保护的实现方式进行具体说明。

例如，第二通信装置比较网络设备配置的邻近服务组对应的安全策略和接收到的第一消息中携带的其他字段是否匹配，由于安全策略的取值为 preferred，则无论第一消息中其他字段的取值为 0 或非零，第二通信装置都可以认为二者匹配，进而第二通信装置可以根据其他字段（例如 PTK ID、PGK ID、counter、机密性指示信息、MAC）的取值，进一步判断是否解安全保护。

示例性的，在完整性安全策略指示可选开启完整性安全保护的情况下，且其他字段中携带的 MAC 的取值为非零的情况下，第二通信装置确定对载荷字段进行完整性校验。

示例性的，在完整性安全策略指示可选开启完整性安全保护的情况下，且其他字段中未携带 MAC 或者其他字段中携带的 MAC 的取值为零的情况下，第二通信装置确定对载荷字段不进行安全保护。

例如，当网络侧配置的完整性安全策略指示可选开启完整性安全保护（例如，取值为 preferred）时，如果第一消息中携带的 MAC 取值为 0 或者未携带 MAC，第二通信装置不对该第一消息进行完整性校验，或者认为该第一消息的完整性校验通过。如果第一消息中携带的 MAC 取值为非全 0，则第二通信装置对该第一消息进行完整性校验，例如根据所选的完整性算法计算 MAC 值，并与第一消息携带的 MAC 值进行比较确定是否相同，来验证接收的第一消息的完整性。如果相同则说明完整性保护校验通过，如果不同则说明完整性保护检验失败。

示例性的，在机密性安全策略指示机密性安全保护可选开启，且机密性指示信息指示机密性安全保护不开启的情况下，第二通信装置确定对载荷字段不进行解密。

示例性的，在机密性安全策略指示机密性安全保护可选开启，且机密性指示信息指示机密性安全保护开启的情况下，第二通信装置确定对载荷字段进行解密。

例如，当网络侧配置的机密性安全策略指示可选开启完整性安全保护（例如，取值为 preferred）时，如果第一消息中携带的机密性指示信息的取值为 0，第二通信装置不对该第一消息进行解密，或者认为该第一消息的解密成功。如果第一消息中携带的机密性指示信息的取值为 1，则第二通信装置对该第一消息进行解密，例如根据所选的机密性算法对第一消息中的载荷字段进行解密操作。

需要说明的是，上述方法 300 和 400 分别是第一消息的格式、第一消息中其他字段包含的参数的取值，以及增加网络设备配置的安全策略的取值进行说明，能够避免第二通信装置在接收到第一消息后无法进行完整性校验或者校验失败，同时灵活性、适应性更强。二者可以独立实现，也可以组合实现，本申请对此不作具体限定。

图 5 是本申请实施例提供的通信方法 500 的流程示意图，适用于一对多通信安全（广播或者多播场景），该实现方式中对消息#a 是否进行机密性安全保护和完整性安全保护是由发送者 UE 根据网络侧配置的机密性安全策略#a 和本地策略#a 共同确定的。如图 5 所示，该方法包括如下多个步骤，未详尽说明的部分可参考上述方法 200 至 400 或者现有协议。

S510，发送者 UE 配置签约信息。发送者 UE 发起服务授权流程。

示例性的，发送者 UE 获取用于一对多通信所需要的参数#a，参数#a 包括组标识、安全策略#a、KMF 地址中的一项或者多项。其中，安全策略#a 主要包括机密性安全策略#a 和完整性安全策略#a，安全策略#a 的取值可以包括需要、不需要或者 preferred，用于指示传输层是否需要安全保护。例如，在安全策略#a 的取值为 preferred 的情况下，表示发送者 UE 对待发送的消息#a 可选进行安全保护，即发送者 UE 可以对消息#a 进行安全保护，也可以对消息#a 不进行安全保护，这里安全保护包括机密性安全保护和完整性安全保护。

在本申请实施例中，发送者 UE 和接收者 UE 属于同一个群组（例如，邻近服务组），具有相同的组标识（例如，邻近服务组的组 ID）。可选地，安全策略#a 的粒度为群组粒度，与组 ID 关联。也就是说，同一个群组的多个 UE 对应相同的安全策略，即多个 UE 之间在收发消息#a 的情况下都是采用相同的安全策略。

S520，发送者 UE 向 KMF 发送密钥请求消息#a（即，请求消息）。对应的，KMF 接收来自发送者 UE 的密钥请求消息#a。

其中，请求消息包括组标识和发送者 UE 的安全能力，请求消息用于请求获取与组标识关联的安全策略。

S530，KMF 校验发送者 UE 是否支持组安全算法。

其中，安全策略#a和组安全算法可以是一致的。示例性的，当安全策略#a指示不需要安全保护时，组安全算法为空算法；当安全策略#a指示需要安全保护时，组安全算法为非空算法，例如组加密算法和组完整性保护算法；当安全策略#a的取值为preferred时，组安全算法为空算法和非空算法。

S540，KMF向发送者UE发送密钥响应消息#a。对应的，发送者UE接收来自KMF的密钥响应消息#a。

其中，密钥响应消息#a包括与组标识关联的所述安全策略，例如安全策略#a。

S551，接收者UE配置和服务授权。

S552，接收者UE向KMF发送密钥请求消息#b。对应的，KMF接收来自接收者UE的密钥请求消息#b。进一步地，KMF向接收者UE发送密钥响应消息#b。对应的，接收者UE接收来自KMF的密钥响应消息#b。

基于步骤S551和S552，接收者UE可以与网络管理功能网元之间建立连接，并且从网络管理功能网元获取组标识、安全策略#a和KMF地址等。可选地，安全策略#a与组ID关联。同时，在接收者UE支持组安全算法的情况下，接收者UE也可以从KMF获取接收者UE的组成员标识、组安全算法标识（例如，机密性算法ID和/或完整性算法ID）、PGK、PGK ID等参数中的一项或者多项。

S560，发送者UE推演安全密钥，例如PTK、PIK、PEK中的一个或多个，又或者是其他的用于进行机密性保护和/或完整性保护的密钥，本申请对此不作具体限定。

其中，上述步骤S510至S560的具体实现方式，交互的消息内容或释义，可参考上述方法200的步骤S210至S260的相关描述，为了简洁，此处不再赘述。

S570，发送者UE根据安全策略#a，确定是否对消息#a进行安全保护。

其中，安全策略#a包括机密性安全策略#a和/或完整性安全策略#a，安全保护包括机密性安全保护和/或完整性安全保护。

示例性的，用于广播或组播的消息#a包括以下一项或者多项：组标识（例如，组ID）、发送者UE的组成员标识（例如发送者UE ID）、PGK ID、PTK ID、counter（例如，第一安全参数）、payload、MAC（例如，第二安全参数）等参数。为了便于描述，可以将与机密性安全保护相关的参数PGK ID、PTK ID、counter统称为机密性安全保护指示，将与完整性安全保护相关的参数MAC称为完整性安全保护指示，下文相关部分不再重复说明。需要说明的是，以上机密性安全指示和完整性安全指示包含的参数仅是为便于理解方案给出的示例，不应构成对本申请技术方案的任何限定，其他与机密性安全保护相关的参数和完整性安全保护相关的参数也可以包含于机密性安全指示和完整性安全指示，也属于本申请的保护范围，本申请不作限定。

可选的，为了便于理解和描述，下文中以第一安全参数（或机密性安全保护指示）为PGK ID、PTK ID、counter、或者机密性指示信息中的至少一个，第二安全参数（或完整性安全保护指示）为MAC为例进行说明。

可选地，PGK ID、PTK ID、counter可以携带在发送者UE的PDCP数据包的头部(header)。

可选地，上述消息#a可以携带指示信息#a（即，机密性指示信息），用于指示机密性安全保护是否开启。例如，该指示信息#a的大小可以是1比特。示例性的，在机密性安全保护开启的情况下，该指示信息#a的取值可以为1；在机密性安全保护不开启的情况下，该指示信息#a的取值可以为0。为便于描述或理解，可以将该指示信息#a作为上述机密性安全保护指示的一部分。

可选地，该指示信息#a可以与PGK ID、PTK ID、counter一同携带在发送者UE的PDCP数据包的头部。

在该实现方式中，通过在消息#a中增加指示信息#a，使得接收者UE可以根据指示信息#a和MAC的取值，确定发送者UE是否对消息#a进行安全保护，避免了当机密性安全保护未开启，且完整性安全保护开启时，由于消息#a中的PGK ID、PTK ID、counter均被置为0，而导致接收者UE对消息#a的完整性安全保护校验失败的情况。

在一种实现方式中，在网络侧配置的安全策略#a为需要或者不需要的情况下，发送者UE可以根据该安全策略#a确定是否对消息#a进行安全保护。

示例性的，当安全策略#a为不需要时，发送者UE对消息#a不进行机密性安全保护，且不进行完整性安全保护，对应的，消息#a中的PGK ID、PTK ID、counter、MAC均被置为0；当安全策略#a为需要时，发送者UE对消息#a进行机密性安全保护，且进行完整性安全保护，对应的，消息#a中的PGK ID、

PTK ID、counter、MAC 均不为 0。其中，发送者 UE 对消息#a 进行安全保护的具体实现方式可参考上述方法 200 的步骤 S270 的相关描述，为了简洁，此处不再赘述。

可选地，上述消息#a 不携带指示信息#a，此时与机密性安全保护关联的参数 PGK ID、PTK ID、counter 是否取值为 0，由机密性安全保护和完整性安全保护是否开启共同决定，具体实现可参考表 1 的示例。对应的，接收者 UE 可以根据网络侧配置的安全策略#a 确定发送者 UE 是否对消息#a 进行安全保护。

具体地，当机密性安全保护关闭时，将关联的参数 PGK ID、PTK ID、counter 的取值设置为非 0，使得接收者 UE 可以根据网络侧配置的安全策略#a，确定发送者 UE 是否对消息#a 进行安全保护，进而确定是否需要消息#a 进行解密或者进行完整性安全保护校验，避免了现有方案中，当机密性安全保护未开启，且完整性安全保护开启时，由于消息#a 中的 PGK ID、PTK ID、counter 均被置为 0，而导致接收者 UE 对消息#a 的完整性安全保护校验失败的情况。

表 1 是发送者 UE 针对机密性安全保护和完整性安全保护是否开启，在广播或组播的消息#a 中携带的参数的具体取值的示例。应理解，表 1 仅是为便于理解给出的示例，表 1 可以有其他的变换，本申请实施例对消息#a 的内容和表述方式不作限制。

表 1

机密性安全保护	完整性安全保护	PGK ID	PTK ID	counter	MAC
开启	开启	非 0	非 0	非 0	非 0
开启	关闭	非 0	非 0	非 0	0
关闭	开启	非 0	非 0	非 0	非 0
关闭	关闭	0	0	0	0

如表 1 所示，若发送者 UE 根据网络侧配置的安全策略#a 和本地策略#a 确定完整性安全保护开启，则 MAC 的取值为非 0；反之，MAC 的取值为 0；若发送者 UE 根据网络侧配置的安全策略#a 和本地策略#a 确定机密性安全保护开启，无论完整性安全保护是否开启，则 PGK ID、PTK ID 和 counter 的取值为非 0；若发送者 UE 根据网络侧配置的安全策略#a 和本地策略#a 确定机密性安全保护和完整性安全保护均关闭，则 PGK ID、PTK ID 和 counter 的取值为 0；若发送者 UE 根据网络侧配置的安全策略#a 和本地策略#a 确定机密性安全保护关闭且完整性安全保护开启，则将 PGK ID、PTK ID 和 counter 的取值设置为非 0。也就是说，在该实现方式中，与机密性安全保护关联的参数 PGK ID、PTK ID 和 counter 是否取值为 0，与机密性安全保护和完整性安全保护是否开启共同决定。

在另一种实现方式中，在网络侧配置的安全策略#a 为 preferred 的情况下，发送者 UE 可以根据安全策略#a 和本地策略#a，确定是否对消息#a 进行安全保护。

其中，本地策略#a 可以指示发送者 UE 对消息#a 进行安全保护的触发条件。例如，当 UE1 的 type 为路边单元时，不进行机密性安全保护；当 UE1 的 type 为汽车时，进行机密性安全保护。或者，当 UE1 处于封闭的环境中，不进行机密性安全保护和/或完整性安全保护；当 UE1 处于开放或不安全的环境中，进行机密性安全保护和/或完整性安全保护。又例如，当 UE1 的性能或终端能力不足以支持开启安全保护时，不进行机密性安全保护和/或完整性安全保护。又例如，针对特定业务场景（会话建立、请求注册服务等），UE1 进行机密性安全保护和/或完整性安全保护等，以上仅是为便于理解方案给出的示例，不构成本申请技术方案的任何限定。

可选地，本地策略#a 可以在步骤 S410 预配置的，也可以是从网络侧接收的，例如从 KMF 或者网络管理功能网元获取。

示例性的，在网络侧配置的安全策略#a 为 preferred 的情况下，说明发送者 UE 对消息#a 进行可选安全保护。因此，进一步地，发送者 UE 可以根据本地策略#a 确定是否进行安全保护。例如，当群组中的 UE type 为路边单元时，广播或组播的消息#a 无机密性安全保护需求，则不进行机密性安全保护；当群组中的 UE type 为汽车时，广播或组播的消息#a 有机密性安全保护需求，则进行机密性安全保护。

在本申请实施例中，消息#a 中的 PGK ID、PTK ID、counter 是否取值为 0 不再与机密性安全保护是否开启完全绑定。换句话说，当机密性安全保护不开启（或关闭）时，可以通过该指示信息#a（即，机密性指示信息）来指示或确定，对应的，PGK ID、PTK ID 和 counter 的取值可以为 0，也可以为非 0，本申请对此不作具体限定。当机密性安全保护开启时，也可以通过该指示信息#a 来指示或确定，对应的，PGK ID、PTK ID 和 counter 的取值为非 0。类似的，当完整性安全保护不开启（或关闭）时，可以通过

该指示信息#b（即，完整性指示信息）来指示或确定，例如指示信息#b的取值为0，对应的，MAC的取值也为0。当完整性安全保护开启时，也可以通过该指示信息#b来指示或确定，例如指示信息#b的取值为1，对应的，MAC的取值为非0。

表2是发送者UE针对机密性安全保护和完整性安全保护是否开启，在广播或组播的消息#a中携带的参数的具体取值的示例。其中，表2示例的消息#a的各项参数可以是具体的参数值，也可以是发送者UE和接收者UE提前约定的编码值。应理解，表2仅是为便于理解给出的示例，表2可以有其他的变换，本申请实施例对消息#a的内容和表述方式不作限制。

表 2

机密性安全保护	完整性安全保护	PGK ID	PTK ID	counter	指示信息#a	指示信息#b	MAC
开启	开启	非0	非0	非0	1	1	非0
开启	关闭	非0	非0	非0	1	0	0
关闭	开启	非0	非0	非0	0	1	非0
关闭	关闭	0或非0	0或非0	0或非0	0	0	0

如表1所示，若发送者UE根据网络侧配置的安全策略#a和本地策略#a确定完整性安全保护开启，则MAC的取值为非0；反之，MAC的取值为0；若发送者UE根据网络侧配置的安全策略#a和本地策略#a确定机密性安全保护开启，则指示信息#a的取值为1，对应的PGK ID、PTK ID和counter的取值为非0；反之，指示信息#a的取值为0，此时，PGK ID、PTK ID和counter的取值可以为非0，也可以为非0，本申请对此不作限定。也就是说，在该实现方式中，机密性安全保护是否开启可以通过指示信息#a的取值来确定，与机密性安全保护关联的参数PGK ID、PTK ID和counter的取值不是判断机密性安全保护是否开启的唯一评判依据。

S580，发送者UE发送消息#a。对应的，接收者UE接收来自发送者UE的消息#a。

示例性的，发送者UE通过广播或者组播的方式发送该消息#a。

S590，接收者UE推算安全密钥，根据安全策略#a确定是否对消息#a进行解安全保护。

其中，接收者UE推算安全密钥（例如PTK、PIK、PEK中的一个或多个）的具体实现方式，可参考上述方法200的步骤S290的相关描述，为了简洁，此处不再赘述。

示例性的，安全策略#a包括机密性安全策略#a和完整性安全策略#a。例如，接收者UE根据接收到的消息#a中携带的组ID，以及上述步骤S551和S552中接收到的密钥响应消息#b，本地查找对应的安全策略#a。可选地，接收者UE在未找到组ID对应的安全策略#a的情况下，可选地，接收者UE可以向网络侧（例如PKM）发送请求消息，用于获取该组ID对应的安全策略#a，或者，接收者UE也可以选择丢弃接收到的消息#a，本申请不作具体限定。

在一种实现方式中，在网络侧配置的安全策略#a的取值为需要时，接收者UE确定对消息#a进行解安全保护；在网络侧配置的安全策略#a的取值为不需要时，接收者UE确定对消息#a不进行解安全保护。即该实现方式忽略消息#a中携带的指示信息#a（例如，指示信息#a参见表1）。

示例性的，在网络侧配置的机密性安全策略#a为需要时，接收者UE对消息#a中payload的密文进行解密；在网络侧配置的机密性安全策略#a为不需要时，接收者UE对消息#a中的payload不进行解密；在网络侧配置的完整性安全策略#a为需要时，接收者UE对消息#a进行完整性安全保护校验，即校验接收者UE计算得到的MAC和接收到的消息#a中携带的MAC是否相同；在网络侧配置的完整性安全策略#a为不需要时，接收者UE对消息#a不进行完整性安全保护校验。

在另一种实现方式中，接收者UE根据安全策略#a、消息#a中携带的机密性安全保护指示和完整性安全保护指示，确定是否对消息#a进行解安全保护。

示例性的，接收者UE可以检查消息#a中携带的机密性安全保护（例如PGK ID、PTK ID、counter、指示信息#a）和完整性安全保护指示（例如MAC）是否与网络侧配置的安全策略#a匹配，即接收者UE检查消息#a中携带的PGK ID、PTK ID、counter的取值指示的是否进行机密性安全保护，与配置的机密性安全策略#a指示的是否进行机密性安全保护是否匹配，以及消息#a中携带的MAC的取值指示的是否进行完整性安全保护，与配置的完整性安全策略#a指示的是否进行完整性安全保护是否匹配。

例如，当网络侧配置的完整性安全策略#a指示需要完整性安全保护（例如，取值为1）时，则说明

发送者 UE 对消息#a 进行完整性安全保护, 如果消息#a 中携带的 MAC 取值为非 0, 则说明消息#a 中携带的完整性安全保护指示 (例如 MAC), 与网络侧配置的完整性安全策略#a 匹配; 反之, 如果消息#a 中携带的 MAC 取值为 0, 则说明消息#a 中携带的完整性安全保护指示, 与网络侧配置的完整性安全策略#a 不匹配。

例如, 当网络侧配置的完整性安全策略#a 指示不需要完整性安全保护 (例如, 取值为 0) 时, 则说明发送者 UE 对消息#a 不进行完整性安全保护, 如果消息#a 中携带的 MAC 取值为 0, 则说明消息#a 中携带的完整性安全保护指示 (例如 MAC), 与网络侧配置的完整性安全策略#a 匹配; 反之, 如果消息#a 中携带的 MAC 取值为非 0, 则说明消息#a 中携带的完整性安全保护指示, 与网络侧配置的完整性安全策略#a 不匹配。或者, 此时接收者 UE 可以不考虑 MAC 的取值, 根据完整性安全策略#a, 确定是否对消息#a 进行解安全保护即可。

例如, 当网络侧配置的机密性安全策略#a 指示需要机密性安全保护 (例如, 取值为 1) 时, 则说明发送者 UE 对消息#a 进行机密性安全保护, 如果消息#a 中携带的 PGK ID、PTK ID、counter 取值均为非 0, 和/或消息#a 中携带的指示信息#a 的取值为 1, 则说明消息#a 中携带的机密性安全保护指示 (例如 PGK ID、PTK ID、counter), 与网络侧配置的机密性安全策略#a 匹配; 反之, 如果消息#a 中携带的 PGK ID、PTK ID、counter 取值均为 0, 和/或消息#a 中携带的指示信息#a 的取值为 0, 则说明消息#a 中携带的机密性安全保护指示, 与网络侧配置的机密性安全策略#a 不匹配。

例如, 当网络侧配置的机密性安全策略#a 指示不需要机密性安全保护 (例如, 取值为 0) 时, 则说明发送者 UE 对消息#a 不进行机密性安全保护, 如果消息#a 中携带的 PGK ID、PTK ID、counter 取值均为 0, 和/或消息#a 中携带的指示信息#a 的取值为 0, 则说明消息#a 中携带的机密性安全保护指示 (例如 PGK ID、PTK ID、counter), 与网络侧配置的机密性安全策略#a 匹配; 反之, 如果消息#a 中携带的 PGK ID、PTK ID、counter 取值均非为 0, 和/或消息#a 中携带的指示信息#a 的取值为 1, 则说明消息#a 中携带的机密性安全保护指示, 与网络侧配置的机密性安全策略#a 不匹配。或者, 此时接收者 UE 可以不考虑机密性安全保护指示的取值, 根据机密性安全策略#a, 确定是否对消息#a 进行解安全保护即可。

例如, 当网络侧配置的安全策略#a 指示可选进行安全保护 (例如, 取值为 preferred) 时, 则说明发送者 UE 对消息#a 可选进行安全保护, 此时消息#a 中携带的机密性安全保护指示 (例如 PGK ID、PTK ID、counter) 和完整性安全保护指示 (例如 MAC) 的取值无论是多少, 接收者 UE 都可以认为该消息#a 中携带的机密性安全保护指示和完整性安全保护指示, 与网络侧配置的安全策略#a 匹配。

基于上述消息#a 中携带的机密性安全保护指示和完整性安全保护指示, 与网络侧配置的安全策略#a 是否匹配的判断, 接收者 UE 可以确定对消息#a 是否进行解安全保护。

示例性的, 在消息#a 中携带的机密性安全保护指示和完整性安全保护指示, 与网络侧配置的安全策略#a 匹配的情况下, 如果二者不匹配, 则接收者 UE 可以丢弃该消息#a。如果二者匹配, 则接收者 UE 可以根据网络侧配置的安全策略#a, 或者根据消息#a 中携带的机密性安全保护指示和完整性安全保护指示, 确定是否对消息#a 进行解安全保护。

例如, 当机密性安全策略#a 的取值为需要, 消息#a 中携带的机密性安全保护指示, 例如 PGK ID、PTK ID、counter 的取值全为非 0 和/或指示信息#a 的取值为 1, 则接收者 UE 确定对消息#a 中的 payload 进行解密。当机密性安全策略#a 的取值为不需要, 消息#a 中携带的机密性安全保护指示, 例如 PGK ID、PTK ID、counter 的取值全为 0 和/或指示信息#a 的取值为 0, 则接收者 UE 确定对消息#a 中的 payload 不进行解密。当机密性安全策略#a 的取值为 preferred, 消息#a 中携带的机密性安全保护指示, 例如指示信息#a 的取值为 1, 则接收者 UE 确定对消息#a 中的 payload 进行解密。当完整性安全策略#a 的取值为需要, 消息#a 中携带的完整性安全保护指示, 例如 MAC 的取值全为非 0, 则接收者 UE 确定对消息#a 中的 payload 进行完整性校验。当完整性安全策略#a 的取值为不需要, 消息#a 中携带的完整性安全保护指示, 例如 MAC 的取值全为非 0, 则接收者 UE 确定对消息#a 中的 payload 进行完整性校验。当完整性安全策略#a 的取值为 preferred, 消息#a 中携带的完整性安全保护指示, 例如 MAC 的取值全为 0, 则接收者 UE 确定对消息#a 中的 payload 不进行完整性校验。其中, 解密和完整性安全保护校验的具体实现方式, 可参考上述方法 200 的步骤 S290 的相关描述, 为了简洁, 此处不再赘述。

本申请所揭示的方法, 接收者 UE 根据网络侧配置的安全策略确定是否需要消息#a 进行解安全保护, 而不是单纯依据消息#a 中携带的参数取值, 避免了攻击者对消息#a 的篡改; 通过定义消息#a 中不同参数的取值, 避免了在安全策略指示不需要机密性安全保护但需要完整性安全保护的场景下, 完整性安

全保护校验失败的情况发生；通过增加安全策略的取值，使得消息#a的安全保护是否开启更加灵活。

图 6 是本申请实施例提供的通信方法 600 的流程示意图，适用于一对多通信安全（广播或者多播场景）。相比于方法 500，该方法 600 中对消息#A 是否进行完整性安全保护是由网络侧配置的完整性安全策略#A 确定的，对消息#A 是否进行机密性安全保护则由发送者 UE 根据网络侧配置的机密性安全策略#A 和本地策略#A 共同确定的。如图 6 所示，该方法包括如下多个步骤，未详尽说明的部分可参考上述方法 200 至 500 或者现有协议。

S610，发送者 UE 配置签约信息。发送者 UE 发起服务授权流程。

示例性的，发送者 UE 获取用于一对多通信所需要的参数#A，参数#A 包括组标识、安全策略#A、KMF 地址中的一项或者多项。其中，安全策略#A 主要包括机密性安全策略#A 和完整性安全策略#A，用于指示传输层是否需要安全保护。例如，机密性安全策略#A 的取值可以包括需要、不需要或者 preferred，完整性安全策略#A 的取值可以包括需要或者不需要。也就是说，在机密性安全策略#A 的取值为 preferred 的情况下，发送者 UE 对待发送的消息#A 可选进行机密性安全保护，即发送者 UE 可以对消息#A 进行机密性安全保护，也可以对消息#A 不进行机密性安全保护，用于满足不同的发送者 UE 的灵活性需求。

S620，发送者 UE 向 KMF 发送密钥请求消息#A。对应的，KMF 接收来自发送者 UE 的密钥请求消息#A。

S630，KMF 校验发送者 UE 是否支持组安全算法。

S640，KMF 向发送者 UE 发送密钥响应消息#A。对应的，发送者 UE 接收来自 KMF 的密钥响应消息#A。

S651，接收者 UE 配置和服务授权。

S652，接收者 UE 向 KMF 发送密钥请求消息#B。对应的，KMF 接收来自接收者 UE 的密钥请求消息#B。进一步地，KMF 向接收者 UE 发送密钥响应消息#B。对应的，接收者 UE 接收来自 KMF 的密钥响应消息#B。

S660，发送者 UE 推演安全密钥，例如 PTK、PIK、PEK 中的一个或多个，又或者是其他的用于进行机密性保护和/或完整性保护的密钥，本申请对此不作具体限定。

其中，上述步骤 S610 至 S660 的具体实现方式，交互的消息的内容或释义，可参考上述方法 600 的步骤 S510 至 S560 的相关描述，为了简洁，此处不再赘述。区别之处在于，该方法 700 中的机密性安全策略#A 的取值可以包括需要、不需要或者 preferred，完整性安全策略#A 的取值可以包括需要或者不需要。

S670，发送者 UE 根据机密性安全策略#A，确定是否对消息#A 进行机密性安全保护。

在一种实现方式中，在网络侧配置的机密性安全策略#A 为需要或者不需要的情况下，发送者 UE 可以根据该机密性安全策略#A 确定对消息#A 进行加密或不进行加密。

示例性的，当机密性安全策略#A 为不需要时，发送者 UE 对消息#A 不进行机密性安全保护，对应的，消息#A 中的 PGK ID、PTK ID、counter 或者机密性指示信息均被置为 0；当机密性安全策略#A 为需要时，发送者 UE 对消息#A 进行机密性安全保护，对应的，消息#A 中的 PGK ID、PTK ID、counter 均为非零，将机密性指示信息设置为 1。其中，发送者 UE 对消息#A 进行机密性安全保护的具体实现方式可参考上述方法 200 的步骤 S270 的相关描述，为了简洁，此处不再赘述。

在本申请实施例中，消息#A 中的 PGK ID、PTK ID、counter 是否取值为 0 不再与机密性安全保护是否开启完全绑定。换句话说，当机密性安全保护不开启（或关闭）时，可以通过该机密性指示信息来指示或确定，对应的，PGK ID、PTK ID 和 counter 的取值可以为 0，也可以为非 0，本申请对此不作具体限定。当机密性安全保护开启时，也可以通过该机密性指示信息来指示或确定，此时 PGK ID、PTK ID 和 counter 的取值可以为非 0。

在另一种实现方式中，发送者 UE 根据机密性安全策略#A 和本地策略#A，确定是否对消息#A 进行机密性安全保护。

其中，本地策略#A 可以指示发送者 UE 对消息#A 进行安全保护的触发条件。具体示例可参考上述方法 600 的相关描述，这里不作赘述。可选地，本地策略#A 可以是在步骤 S610 预配置的，也可以是从网络侧接收的，例如从 KMF 或者网络管理功能网元获取。

示例性的，在网络侧配置的机密性安全策略#A 为 preferred 的情况下，说明发送者 UE 对消息#A 进行可选机密性安全保护。进一步地，发送者 UE 可以根据本地策略#A 确定是否进行机密性安全保护。例如，当群组中的 UE type 为路边单元时，广播或组播的消息#A 无机密性安全保护需求，则不进行机密性安全

保护；当群组中的 UE type 为汽车时，广播或组播的消息#A 有机密性安全保护需求，则进行机密性安全保护。

基于上述两种实现方式，发送者 UE 可以根据机密性安全策略#A 和本地策略#A，确定是否对消息#A 进行机密性安全保护。进一步的，发送者 UE 可以根据网络侧配置的完整性安全策略#A，确定是否对消息#A 进行完整性安全保护。其中，完整性安全策略#A 的取值为需要或不需要。

示例性的，在网络侧配置的完整性安全策略#A 为需要或者不需要的情况下，发送者 UE 可以根据该完整性安全策略#A 确定是否对消息#A 进行完整性安全保护。例如，当完整性安全策略#A 为不需要时，发送者 UE 对消息#A 不进行完整性安全保护，对应的，消息#A 中的 MAC 取值为非 0；当完整性安全策略#A 为需要时，发送者 UE 对消息#A 进行完整性安全保护，对应的，消息#A 中的 MAC 的取值为全 0，或者待发送的消息#A 中不携带 MAC 部分。其中，发送者 UE 对消息#A 进行安全保护的具体实现方式可参考上述方法 600 的步骤 S570 的相关描述，为了简洁，此处不再赘述。

S680，发送者 UE 发送消息#A。对应的，接收者 UE 接收来自发送者 UE 的消息#A。

示例性的，发送者 UE 通过广播或者组播的方式发送该消息#A。

S691，接收者 UE 推算安全密钥，根据完整性安全策略#A 确定是否对消息#A 进行完整性保护校验。

其中，接收者 UE 推算安全密钥（例如 PTK、PIK、PEK）的具体实现方式可参考上述方法 600 的步骤 S590 的相关描述，为了简洁，此处不再赘述。

示例性的，接收者 UE 根据接收到的消息#A 中携带的组 ID，以及上述步骤 S651 和 S652 中接收到的密钥响应消息#B，本地查找对应的安全策略#A。可选地，接收者 UE 在未找到组 ID 对应的安全策略#A 的情况下，可选地，接收者 UE 可以向网络侧（例如 PKM）发送请求消息，用于获取该组 ID 对应的安全策略#A，或者，接收者 UE 也可以选择丢弃接收到的消息#A，本申请不作具体限定。

示例性的，在网络侧配置的完整性安全策略#A 为需要的情况下，接收者 UE 对消息#A 进行完整性保护校验，即校验 MAC 是否正确。其中，解密和完整性安全保护校验的具体实现方式，可参考上述方法 200 的步骤 S290 的相关描述，为了简洁，此处不再赘述。在网络侧配置的完整性安全策略#A 为不需要时，接收者 UE 对消息#A 不进行完整性保护校验。

S692，在完整性保护校验通过的情况下，接收者 UE 根据机密性安全策略#A 确定是否对消息#A 进行解密。

在一种实现方式中，在网络侧配置的机密性安全策略#A 为需要时，接收者 UE 对消息#A 中 payload 的密文进行解密；在网络侧配置的机密性安全策略#A 的取值为不需要时，接收者 UE 对消息#A 中 payload 的密文不进行解密；在网络侧配置的机密性安全策略#A 的取值为 preferred 时，接收者 UE 对消息#A 中 payload 的密文进行可选解密。

在另一种实现方式中，接收者 UE 根据机密性安全策略#A 和消息#A 中携带的机密性安全保护指示，确定是否对消息#A 进行解密。

具体的，接收者 UE 可以先判断消息#A 中携带的机密性安全保护（例如 PGK ID、PTK ID、counter、机密性指示信息）是否与网络侧配置的机密性安全策略#A 匹配，即接收者 UE 检查消息#A 中携带的 PGK ID、PTK ID、counter、或者机密性指示信息的取值所指示的是否进行机密性安全保护，与配置的机密性安全策略#A 指示的是否进行机密性安全保护是否匹配。其中，判断是否匹配的的实现方式可参考上述方法 600 的步骤 S590 中的相关描述，为了简洁，此处不再赘述。

进一步的，若上述判断匹配，接收者 UE 再根据消息#A 中携带的 PTK ID、PGK ID 和 counter、或者机密性指示信息的取值，确定是否对消息#A 中的载荷字段进行解密。

示例性的，在消息#A 中携带的机密性安全保护指示包括 PTK ID、PGK ID 和 counter，但不包括机密性指示信息时，若 PTK ID、PGK ID 和 counter 的取值均为 0，则说明发送者 UE 对消息#A 进行机密性安全保护，接收者 UE 对消息#A 中 payload 的密文不进行解密，反之，若 PTK ID、PGK ID 和 counter 的取值均不为 0，则接收者 UE 可以对消息#A 中 payload 的密文进行解密。

示例性的，在消息#A 中携带的机密性安全保护指示包括 PTK ID、PGK ID、counter、机密性指示信息时，无论 PTK ID、PGK ID 和 counter 的取值是否为 0，接收者 UE 可以根据该机密性指示信息确定是否对消息#A 中 payload 的密文进行解密。如果机密性指示信息的取值为 0，则接收者 UE 可以对消息#A 中 payload 的密文不进行解密；反之，如果机密性指示信息的取值为 1，则接收者 UE 可以对消息#A 中 payload 的密文进行解密。

本申请所揭示的方法，发送者 UE 根据机密性安全策略#A 和本地策略#A 决定是否开启机密性安全保护，使得机密性安全机制更加灵活，降低了收发端的开销。

图 7 是本申请实施例提供的通信方法 700 的流程示意图，适用于一对多通信安全（广播或者多播场景）。相比于方法 600，该方法 700 中对消息#A 是否进行机密性安全保护是由网络侧配置的机密性安全策略#A 确定的，对消息#A 是否进行完整性安全保护则由发送者 UE 根据网络侧配置的完整性安全策略#A 和本地策略#A 共同确定的。如图 7 所示，该方法包括如下多个步骤，未详尽说明的部分可参考上述方法 200 至 600，或者现有协议。

S710，发送者 UE 配置签约信息。发送者 UE 发起服务授权流程。

示例性的，发送者 UE 获取用于一对多通信所需要的参数# α ，参数# α 包括组标识、安全策略# α 、KMF 地址中的一项或者多项。其中，安全策略# α 主要包括机密性安全策略# α 和完整性安全策略# α ，用于指示传输层是否需要安全保护。例如，机密性安全策略# α 的取值可以包括需要或者不需要，完整性安全策略# α 的取值可以包括需要、不需要或者 preferred。也就是说，在完整性安全策略# α 的取值为 preferred 的情况下，发送者 UE 对待发送的消息# α 可选进行完整性安全保护，即发送者 UE 可以对消息# α 进行完整性安全保护，也可以对消息# α 不进行完整性安全保护，用于满足不同的发送者 UE 的灵活性需求。

S720，发送者 UE 向 KMF 发送密钥请求消息# α 。对应的，KMF 接收来自发送者 UE 的密钥请求消息# α 。

S730，KMF 校验发送者 UE 是否支持组安全算法。

S740，KMF 向发送者 UE 发送密钥响应消息# α 。对应的，发送者 UE 接收来自 KMF 的密钥响应消息# α 。

S751，接收者 UE 配置和服务授权。

S752，接收者 UE 向 KMF 发送密钥请求消息# β 。对应的，KMF 接收来自接收者 UE 的密钥请求消息# β 。进一步地，KMF 向接收者 UE 发送密钥响应消息# β 。对应的，接收者 UE 接收来自 KMF 的密钥响应消息# β 。

S760，发送者 UE 推演安全密钥，例如 PTK、PIK、PEK 中的一个或多个，又或者是其他的用于进行机密性保护和/或完整性保护的密钥，本申请对此不作具体限定。

其中，上述步骤 S710 至 S760 的具体实现方式，交互的消息的内容或释义，可参考上述方法 600 的步骤 S610 至 S660 的相关描述，为了简洁，此处不再赘述。区别之处在于，该方法 700 中的完整性安全策略# α 的取值可以包括需要、不需要或者 preferred，机密性安全策略# α 的取值可以包括需要或者不需要。

S770，发送者 UE 根据完整性安全策略# α ，确定是否对消息# α 进行完整性安全保护。

在一种实现方式中，在网络侧配置的完整性安全策略# α 为需要或者不需要的情况下，发送者 UE 可以根据该完整性安全策略# α 确定对消息# α 进行完整性校验或不进行完整性校验。

示例性的，当完整性安全策略# α 为不需要时，发送者 UE 对消息# α 不进行完整性安全保护，对应的，消息# α 中的 MAC 被置为全 0；当完整性安全策略# α 为需要时，发送者 UE 对消息# α 进行完整性安全保护，对应的，消息# α 中的 MAC 为非零。其中，发送者 UE 对消息# α 进行完整性安全保护的具体实现方式可参考上述方法 200 的步骤 S270 的相关描述，为了简洁，此处不再赘述。

在另一种实现方式中，发送者 UE 根据完整性安全策略# α 和本地策略# α ，确定是否对消息# α 进行完整性安全保护。

其中，本地策略# α 可以指示发送者 UE 对消息# α 进行安全保护的触发条件。具体示例可参考上述方法 500 的相关描述，这里不作赘述。可选地，本地策略# α 可以是在步骤 S710 预配置的，也可以是从网络侧接收的，例如从 KMF 或者网络管理功能网元获取。

示例性的，在网络侧配置的完整性安全策略# α 为 preferred 的情况下，说明发送者 UE 对消息# α 进行可选完整性安全保护。进一步地，发送者 UE 可以根据本地策略# α 确定是否进行完整性安全保护。例如，当群组中的 UE type 为路边单元时，广播或组播的消息# α 无完整性安全保护需求，则不进行完整性安全保护；当群组中的 UE type 为汽车时，广播或组播的消息# α 有完整性安全保护需求，则进行完整性安全保护。

基于上述两种实现方式，发送者 UE 可以根据完整性安全策略# α 和本地策略# α ，确定是否对消息# α 进行完整性安全保护。

另外，发送者 UE 可以根据网络侧配置的机密性安全策略# α ，确定是否对消息# α 进行完整性安全保

护。其中，机密性安全策略# α 的取值为需要或不需要。示例性的，在网络侧配置的机密性安全策略# α 为需要或者不需要的情况下，发送者 UE 可以根据该机密性安全策略# α 确定是否对消息# α 进行机密性安全保护。例如，当机密性安全策略# α 为不需要时，发送者 UE 对消息# α 不进行机密性安全保护，对应的，消息# α 中的 MAC 取值为非 0；当机密性安全策略# α 为需要时，发送者 UE 对消息# α 进行机密性安全保护，对应的，消息# α 中的 MAC 的取值为全 0。其中，发送者 UE 对消息# α 进行安全保护的具体实现方式可参考上述方法 500 的步骤 S570 的相关描述，为了简洁，此处不再赘述。

S780，发送者 UE 发送消息# α 。对应的，接收者 UE 接收来自发送者 UE 的消息# α 。

示例性的，发送者 UE 通过广播或者组播的方式发送该消息# α 。

S790，接收者 UE 推演安全密钥，根据安全策略# α 确定是否对消息# α 进行解安全保护。

其中，解安全保护包括解密和完整性安全保护校验，具体实现方式可参考上述方法 200 的步骤 S290 的相关描述，为了简洁，此处不再赘述。接收者 UE 推演安全密钥（例如 PTK、PIK、PEK）的具体实现方式可参考上述方法 500 的步骤 S590 的相关描述，为了简洁，此处不再赘述。

示例性的，接收者 UE 根据接收到的消息# α 中携带的组 ID，以及上述步骤 S751 和 S752 中接收到的密钥响应消息# β ，本地查找对应的安全策略# α 。可选地，接收者 UE 在未找到组 ID 对应的安全策略# α 的情况下，可选地，接收者 UE 可以向网络侧（例如 PKM）发送请求消息，用于获取该组 ID 对应的安全策略# α ，或者，接收者 UE 也可以选择丢弃接收到的消息# α ，本申请不作具体限定。

示例性的，在网络侧配置的机密性安全策略# α 为需要的情况下，接收者 UE 对消息# α 中 payload 的密文进行解密。在网络侧配置的机密性安全策略# α 的取值为不需要时，接收者 UE 对消息# α 中 payload 的密文不进行解密。

示例性的，在网络侧配置的机密性安全策略# α 为不需要的情况下，若消息# α 中携带的 PTK ID、PGK ID、counter 或者机密性指示信息的取值均为 0，则接收者 UE 对消息# α 中 payload 的密文不进行解密；若消息# α 中携带的机密性指示信息的取值为 1，则接收者 UE 可以丢弃该消息# α ，或者认为该消息# α 中 payload 的密文解密失败。

示例性的，在网络侧配置的机密性安全策略# α 为需要的情况下，若消息# α 中携带的机密性安全保护指示包括 PTK ID、PGK ID、counter、机密性指示信息时，无论 PTK ID、PGK ID 和 counter 的取值是否为 0，接收者 UE 可以根据该机密性指示信息确定是否对消息# α 中 payload 的密文进行解密。

示例性的，在网络侧配置的完整性安全策略# α 为需要的情况下，接收者 UE 对消息# α 进行完整性保护校验，即校验 MAC 是否正确。在网络侧配置的完整性安全策略# α 为不需要时，接收者 UE 对消息# α 不进行完整性保护校验。在网络侧配置的完整性安全策略# α 为 preferred 时，接收者 UE 对消息# α 可选进行完整性保护校验，例如接收者 UE 根据消息# α 中携带的 MAC 的取值确定是否进行完整性保护校验。

具体的，接收者 UE 首先可以先判断消息# α 中携带的完整性安全保护（例如 PGK ID、PTK ID、counter、机密性指示信息）的取值所指示的完整性安全保护，与网络侧配置的完整性安全策略# α 是否匹配，即接收者 UE 检查消息# α 中携带的 MAC 的取值是否与配置的完整性算法计算得到的 MAC 的取值相同。如果相同则说明完整性校验通过，反之，完整性校验失败。其中，判断是否匹配的实现方式可参考上述方法 500 的步骤 S590 中的相关描述，为了简洁，此处不再赘述。

本申请所揭示的方法，接收者 UE 根据网络侧配置的安全策略确定是否需要消息# α 进行解安全保护，而不是单纯依据消息# α 中携带的参数取值，避免了攻击者对消息# α 的篡改；通过定义消息# α 中不同参数的取值，避免了在安全策略指示不需要机密性安全保护但需要完整性安全保护的场景下，完整性安全保护校验失败的情况发生；通过增加安全策略的取值，使得消息# α 的安全保护是否开启更加灵活。

上文结合图 1 至图 7，详细描述了本申请的通信方法侧实施例，下面将结合图 8 和图 9，详细描述本申请的通信装置侧实施例。应理解，装置实施例的描述与方法实施例的描述相互对应，因此，未详细描述的部分可以参见前面方法实施例。

图 8 是本申请实施例提供的通信装置 1000 的示意性框图。如图 8 所示，该设备 1000 可以包括收发单元 1010 和处理单元 1020。收发单元 1010 可以与外部进行通信，处理单元 1020 用于进行数据处理。收发单元 1010 还可以称为通信接口或收发单元。

在一种可能的设计中，该设备 1000 可实现对应于上文方法实施例中的第一通信装置执行的步骤或者流程，其中，处理单元 1020 用于执行上文方法实施例中第一通信装置的处理相关的操作，收发单元 1010 用于执行上文方法实施例中第一通信装置的收发相关的操作。

在另一种可能的设计中，该设备 1000 可实现对应于上文方法实施例中的第二通信装置执行的步骤或者流程，其中，处理单元 1020 用于执行上文方法实施例中第二通信装置的处理相关的操作，收发单元 1010 用于执行上文方法实施例中第二通信装置的收发相关的操作。

应理解，这里的设备 1000 以功能单元的形式体现。这里的术语“单元”可以指应用特有集成电路（application specific integrated circuit, ASIC）、电子电路、用于执行一个或多个软件或固件程序的处理器（例如共享处理器、专有处理器或组处理器等）和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。在一个可选例子中，本领域技术人员可以理解，设备 1000 可以具体为上述实施例中的发送端，可以用于执行上述方法实施例中与发送端对应的各个流程和/或步骤，或者，设备 1000 可以具体为上述实施例中的接收端，可以用于执行上述方法实施例中与接收端对应的各个流程和/或步骤，为避免重复，在此不再赘述。

上述各个方案的设备 1000 具有实现上述方法中发送端所执行的相应步骤的功能，或者，上述各个方案的设备 1000 具有实现上述方法中接收端所执行的相应步骤的功能。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。硬件或软件包括一个或多个与上述功能相对应的模块；例如收发单元可以由收发机替代（例如，收发单元中的发送单元可以由发送机替代，收发单元中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

此外，上述收发单元还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。在本申请的实施例，图 8 中的装置可以是前述实施例中的接收端或发送端，也可以是芯片或者芯片系统，例如：片上系统（system on chip, SoC）。其中，收发单元可以是输入输出电路、通信接口。处理单元为该芯片上集成的处理器或者微处理器或者集成电路。在此不做限定。

图 9 是本申请实施例提供的通信装置 2000 的示意性框图。如图 9 所示，该设备 2000 包括处理器 2010 和收发器 2020。其中，处理器 2010 和收发器 2020 通过内部连接通路互相通信，该处理器 2010 用于执行指令，以控制该收发器 2020 发送信号和/或接收信号。

可选地，该设备 2000 还可以包括存储器 2030，该存储器 2030 与处理器 2010、收发器 2020 通过内部连接通路互相通信。该存储器 2030 用于存储指令，该处理器 2010 可以执行该存储器 2030 中存储的指令。

在一种可能的实现方式中，设备 2000 用于实现上述方法实施例中的第一通信装置对应的各个流程和步骤。

在另一种可能的实现方式中，设备 2000 用于实现上述方法实施例中的第二通信装置对应的各个流程和步骤。

应理解，设备 2000 可以具体为上述实施例中的发送端或接收端，也可以是芯片或者芯片系统。对应的，该收发器 2020 可以是该芯片的收发电路，在此不做限定。具体地，该设备 2000 可以用于执行上述方法实施例中与发送端或接收端对应的各个步骤和/或流程。

可选地，该存储器 2030 可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。存储器的一部分还可以包括非易失性随机存取存储器。例如，存储器还可以存储设备类型的信息。该处理器 2010 可以用于执行存储器中存储的指令，并且当该处理器 2010 执行存储器中存储的指令时，该处理器 2010 用于执行上述与发送端或接收端对应的方法实施例的各个步骤和/或流程。

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。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例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。上述的处理器可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。本申请实施例中的处理器可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。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译码处理器执行完成，或者用译码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。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory, ROM）、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、电可擦除可编程只读存储器（electrically EPROM, EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory, RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器、动态随机存取存储器、同步动态随机存取存储器、双倍数据速率同步动态随机存取存储器、增强型同步动态随机存取存储器、同步连接动态随机存取存储器和直接内存总线随机存取存储器。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

图10是本申请实施例提供一种芯片系统3000的示意图。如图10所示，该芯片系统3000（或者也可以称为处理系统）包括逻辑电路3010以及输入/输出接口（input/output interface）3020。

其中，逻辑电路3010可以为芯片系统3000中的处理电路。逻辑电路3010可以耦合连接存储单元，调用存储单元中的指令，使得芯片系统3000可以实现本申请各实施例的方法和功能。输入/输出接口3020，可以为芯片系统3000中的输入输出电路，将芯片系统3000处理好的信息输出，或将待处理的数据或信令信息输入芯片系统3000进行处理。

作为一种方案，该芯片系统3000用于实现上文各个方法实施例中由第一通信装置执行的操作。

作为另一种方案，该芯片系统3000用于实现上文各个方法实施例中由第二通信装置执行的操作。

本申请实施例还提供一种计算机可读存储介质，其上存储有用于实现上述各方法实施例中由设备（例如，第一通信装置、第二通信装置、密钥管理网元）执行的方法的计算机指令。

本申请实施例还提供一种计算机程序产品，包含指令，该指令被计算机执行时以实现上述各方法实施例中由设备（例如，第一通信装置、第二通信装置、密钥管理网元）执行的方法。

本申请实施例还提供一种通信的系统，包括前述的第一通信装置、第二通信装置、密钥管理网元中的一个或多个。

上述提供的任一种装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例，此处不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

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。

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是示意性的，例如，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，机械或其它的形式。

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单元上。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，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。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或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器、随机存取存储器、磁碟

或者光盘等各种可以存储程序代码的介质。

以上，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，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，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权利要求的保护范围为准。

权 利 要 求 书

1. 一种通信方法，其特征在于，包括：

第一通信装置获取邻近服务组对应的安全策略，所述安全策略包括机密性安全策略和/或完整性安全策略，所述机密性安全策略用于指示针对所述邻近服务组的消息是否开启机密性安全保护，所述完整性安全策略用于指示针对所述邻近服务组的消息是否开启完整性安全保护，其中，所述邻近服务组包括至少两个成员，且所述第一通信装置是所述至少两个成员中的一个；

所述第一通信装置根据所述安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对所述第一消息中除所述载荷字段外的其他字段进行赋值，其中，所述其他字段包括以下一项或者多项：邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、完整性指示信息、或者消息认证码 MAC，所述机密性指示信息用于指示所述机密性安全保护是否开启，所述完整性指示信息用于指示所述完整性安全保护是否开启，所述安全保护包括所述机密性安全保护和/或所述完整性安全保护；

所述第一通信装置向第二通信装置发送所述第一消息。

2. 根据权利要求 1 所述的方法，其特征在于，所述对所述第一消息中除所述载荷字段外的其他字段进行赋值，包括：

在所述机密性安全策略指示所述机密性安全保护不开启，且所述完整性安全策略指示所述完整性安全保护开启的情况下，所述第一通信装置将所述 MAC 设置为非零，且将所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数中的至少一个设置为非零。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述对所述第一消息中除所述载荷字段外的其他字段进行赋值，包括：

在所述机密性安全策略指示所述机密性安全保护不开启，且所述完整性安全策略指示所述完整性安全保护开启的情况下，所述第一通信装置将所述机密性指示信息设置为零。

4. 根据权利要求 1 所述的方法，其特征在于，所述第一通信装置根据所述安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对所述第一消息中除所述载荷字段外的其他字段进行赋值，包括以下一种或者多种：

在所述机密性安全策略指示所述机密性安全保护开启的情况下，所述第一通信装置确定对待发送的第一消息中携带的载荷字段进行所述机密性安全保护，以及将所述第一消息中携带的所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数、所述机密性指示信息中的至少一个的取值设置为非零；

在所述完整性安全策略指示所述完整性安全保护开启的情况下，所述第一通信装置确定对待发送的第一消息中携带的载荷字段进行所述完整性安全保护，以及将所述第一消息中携带的所述 MAC 的取值设置为非零；

在所述机密性安全策略指示所述机密性安全保护不开启的情况下，所述第一通信装置确定对待发送的第一消息中携带的载荷字段不进行所述机密性安全保护，以及将所述第一消息中携带的所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数、所述机密性指示信息中的至少一个的取值设置为零；

在所述完整性安全策略指示所述完整性安全保护不开启的情况下，所述第一通信装置确定对待发送的第一消息中携带的载荷字段不进行所述完整性安全保护，以及将所述第一消息中携带的所述 MAC 的取值设置为零。

5. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述第一通信装置根据所述安全策略，确定是否对待发送的第一消息中携带的载荷字段进行安全保护，以及对所述第一消息中除所述载荷字段外的其他字段进行赋值，包括：

所述第一通信装置根据本地策略和所述安全策略，确定对所述第一消息中携带的载荷字段进行安全保护，以及对所述第一消息中除所述载荷字段外的其他字段进行赋值，所述本地策略指示所述第一通信装置对所述载荷字段进行安全保护的触发条件。

6. 根据权利要求 5 所述的方法，其特征在于，所述第一通信装置根据本地策略和所述安全策略，确

定对所述载荷字段进行安全保护,以及对所述第一消息中除所述载荷字段外的其他字段进行赋值,包括:

在所述安全策略指示可选开启安全保护的情况下,所述第一通信装置根据所述本地策略,确定对所述载荷字段进行安全保护,以及对所述第一消息中除所述载荷字段外的其他字段进行赋值。

7. 根据权利要求 5 或 6 所述的方法,其特征在于,所述第一通信装置根据本地策略和所述安全策略,确定对所述载荷字段进行安全保护,以及对所述第一消息中除所述载荷字段外的其他字段进行赋值,包括以下一种或者多种:

在所述机密性安全策略指示可选开启所述机密性安全保护,且所述第一通信装置的类型为路边单元的情况下,所述第一通信装置确定对所述载荷字段不进行所述机密性安全保护,以及将所述其他字段中携带的所述机密性指示信息的取值设置为零,或者将所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数中的至少一个设置为零;

在所述机密性安全策略指示可选开启所述机密性安全保护,且所述第一通信装置的类型为汽车的情况下,所述第一通信装置确定对所述载荷字段进行所述机密性安全保护,以及将所述其他字段中携带的所述机密性指示信息的取值设置为非零,或者,所述第一通信装置将所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数中的至少一个设置为非零。

8. 根据权利要求 1 所述的方法,其特征在于,所述第一通信装置根据所述安全策略,确定是否对待发送的第一消息中携带的载荷字段进行安全保护,以及对所述第一消息中除所述载荷字段外的其他字段进行赋值,包括:

在所述机密性安全策略指示所述机密性安全保护不开启,且所述完整性安全策略指示所述完整性安全保护不开启的情况下,所述第一通信装置将所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数中的至少一个设置为非零。

9. 根据权利要求 1 至 8 中任一项所述的方法,其特征在于,所述机密性指示信息携带在所述第一通信装置的分组数据汇聚协议 PDCP 数据包的信息头中。

10. 根据权利要求 1 至 9 中任一项所述的方法,其特征在于,所述第一通信装置获取邻近服务组对应的安全策略,包括:

所述第一通信装置向密钥管理功能网元发送请求消息,所述请求消息包括所述邻近服务组的组标识和所述第一通信装置的安全能力,所述请求消息用于请求获取与所述组标识关联的所述安全策略;

所述第一通信装置接收来自所述密钥管理功能网元的所述安全策略。

11. 一种通信方法,其特征在于,包括:

第二通信装置接收来自第一通信装置的第一消息,所述第一消息包括载荷字段和其他字段,其中,所述其他字段包括以下一项或者多项:邻近服务组密钥的标识、邻近服务组传输密钥的标识、新鲜性参数、机密性指示信息、完整性指示信息或者消息认证码 MAC,所述机密性指示信息用于指示机密性安全保护是否开启,所述完整性指示信息用于指示所述完整性安全保护是否开启;

所述第二通信装置根据邻近服务组对应的安全策略,确定是否对所述载荷字段进行解安全保护,所述安全策略包括机密性安全策略和/或完整性安全策略,所述机密性安全策略用于指示针对所述邻近服务组的消息是否开启所述机密性安全保护,所述完整性安全策略用于指示针对所述邻近服务组的消息是否开启完整性安全保护,其中,所述邻近服务组包括至少两个成员,且所述第二通信装置是所述至少两个成员中的一个,所述解安全保护包括解密和/或完整性校验。

12. 根据权利要求 11 所述的方法,其特征在于,所述第二通信装置根据邻近服务组对应的安全策略,确定是否对所述载荷字段进行解安全保护,包括以下一种或者多种:

在所述机密性安全策略指示所述机密性安全保护开启的情况下,所述第二通信装置确定对所述载荷字段进行解密;

在所述完整性安全策略指示所述完整性安全保护开启的情况下,所述第二通信装置确定对所述载荷字段进行完整性校验;

在所述机密性安全策略指示所述机密性安全保护不开启的情况下,所述第二通信装置确定对所述载荷字段不进行解密;

在所述完整性安全策略指示所述完整性安全保护不开启的情况下,所述第二通信装置确定对所述载荷字段不进行完整性校验。

13. 根据权利要求 11 或 12 所述的方法,其特征在于,所述第二通信装置根据邻近服务组对应的安

全策略，确定是否对所述载荷字段进行解安全保护，包括：

所述第二通信装置根据所述安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护。

14. 根据权利要求 13 所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示所述完整性安全保护开启，且所述其他字段中未携带所述 MAC 或者所述其他字段中携带的所述 MAC 的取值为零的情况下，所述第二通信装置确定所述载荷字段的完整性校验失败，或者所述第二通信装置丢弃所述第一消息。

15. 根据权利要求 13 或 14 所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示所述完整性安全保护开启，且所述其他字段中携带的所述 MAC 的取值为非零的情况下，所述第二通信装置确定对所述载荷字段进行完整性校验。

16. 根据权利要求 13 至 15 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示所述完整性安全保护不开启，且所述其他字段中携带的所述 MAC 的取值不为零的情况下，所述第二通信装置确定对所述载荷字段不进行完整性校验。

17. 根据权利要求 13 至 16 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示所述完整性安全保护不开启，且所述其他字段中未携带所述 MAC 或者所述其他字段中携带的所述 MAC 的取值为零的情况下，所述第二通信装置确定对所述载荷字段不进行完整性校验。

18. 根据权利要求 13 至 17 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示可选开启所述完整性安全保护的情况下，且所述其他字段中携带的所述 MAC 的取值为非零的情况下，所述第二通信装置确定对所述载荷字段进行完整性校验。

19. 根据权利要求 13 至 18 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述完整性安全策略指示可选开启所述完整性安全保护的情况下，且所述其他字段中未携带所述 MAC 或者所述其他字段中携带的所述 MAC 的取值为零的情况下，所述第二通信装置确定对所述载荷字段不进行安全保护。

20. 根据权利要求 13 至 19 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述机密性安全策略指示所述机密性安全保护不开启，且所述其他字段中携带的所述邻近服务组密钥的标识、所述邻近服务组传输密钥的标识、所述新鲜性参数中的至少一个的取值为非零的情况下，所述第二通信装置确定对所述载荷字段不进行解密。

21. 根据权利要求 13 至 20 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述机密性安全策略指示所述机密性安全保护不开启，且所述其他字段中携带的所述机密性指示信息指示所述机密性安全保护开启的情况下，所述第二通信装置确定对所述载荷字段不进行解密。

22. 根据权利要求 13 至 21 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述机密性安全策略指示所述机密性安全保护开启，且所述机密性指示信息指示所述机密性安全保护不开启的情况下，所述第二通信装置确定对所述载荷字段进行解密。

23. 根据权利要求 13 至 22 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述机密性安全策略指示所述机密性安全保护可选开启，且所述机密性指示信息指示所述机密性安全保护不开启的情况下，所述第二通信装置确定对所述载荷字段不进行解密。

24. 根据权利要求 13 至 23 中任一项所述的方法，其特征在于，所述第二通信装置根据安全策略和所述其他字段，确定是否对所述载荷字段进行解安全保护，包括：

在所述机密性安全策略指示所述机密性安全保护可选开启，且所述机密性指示信息指示所述机密性安全保护开启的情况下，所述第二通信装置确定对所述载荷字段进行解密。

25. 根据权利要求 13 至 24 中任一项所述的方法，其特征在于，所述机密性指示信息携带在所述第一通信装置的分组数据汇聚协议 PDCP 数据包的信息头中。

26. 根据权利要求 13 至 25 中任一项所述的方法，其特征在于，所述方法还包括：

所述第二通信装置获取所述邻近服务组对应的安全策略，具体为：

所述第二通信装置向密钥管理功能网元发送请求消息，所述请求消息包括所述邻近服务组的组标识和所述第二通信装置的安全能力，所述请求消息用于请求获取与所述组标识关联的所述安全策略；

所述第二通信装置接收来自所述密钥管理功能网元的所述安全策略。

27. 一种通信装置，其特征在于，包括：一个或多个功能模块，所述一个或多个功能模块用于执行如权利要求 1 至 10 中任一项所述的方法，或者，所述一个或多个功能模块用于执行如权利要求 11 至 26 中任一项所述的方法。

28. 一种通信装置，其特征在于，包括：处理器，所述处理器与存储器耦合；所述处理器，用于执行所述存储器中存储的计算机程序，以使得所述装置执行如权利要求 1 至 10 中任一项所述的方法，或者，用于执行所述存储器中存储的计算机程序，以使得所述装置执行如权利要求 10 至 26 中任一项所述的方法。

29. 一种计算机可读存储介质，其特征在于，包括：所述计算机可读存储介质上存储有计算机程序，当所述计算机程序运行时，使得所述计算机执行如权利要求 1 至 26 中任一项所述的方法。