(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109640324 A
(43)申请公布日 2019.04.16

(21)申请号 201910028368.1

(22)申请日 2017.07.31

(66)本国优先权数据
PCT/CN2017/083362 2017.05.05 CN

(62)分案原申请数据
201780031003.3 2017.07.31

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 李赫 陈璟 胡力

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04W 12/10(2009.01)

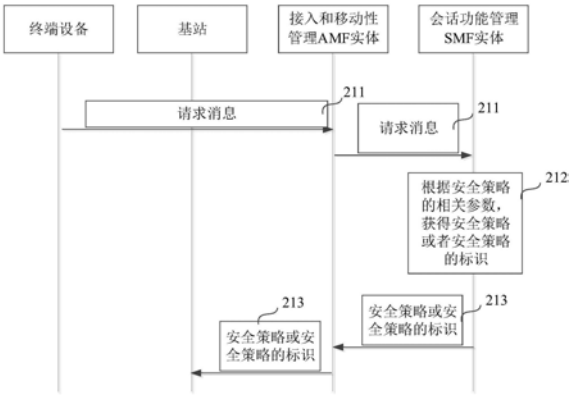
权利要求书3页 说明书52页 附图5页

(54)发明名称

一种通信方法及相关装置

(57)摘要

一种通信方法以及相关装置，基站获取安全策略，所述安全策略包括完整性保护指示信息，所述完整性保护指示信息用于指示所述基站是否对终端设备开启完整性保护；当所述完整性保护指示信息指示所述基站对所述终端设备开启完整性保护时，所述基站向所述终端设备发送目标用户面完整性保护算法。



CN 109640324 A

1.一种通信方法,其特征在于,所述方法包括:

终端设备接收到来自基站的接入层安全模式命令AS SMC之后,开启信令面保护;和

所述终端设备接收到无线资源控制RRC重配置消息后,使用用户面密钥进行用户面安全保护。

2.根据权利要求1所述的方法,其特征在于,所述用户面密钥包括用户面完整性保护密钥;

所述使用用户面密钥进行用户面安全保护,包括:

若所述RRC重配置消息中包括完整性保护指示信息且所述完整性保护指示信息用于指示开启用户面完整性保护,所述终端设备使用所述用户面完整性保护密钥进行完整性保护。

3.根据权利要求1所述的方法,其特征在于,所述用户面密钥包括用户面加密保护密钥;

所述使用用户面密钥进行用户面安全保护,包括:

若所述RRC重配置消息中包括加密保护指示信息且所述加密保护指示信息用于指示开启用户面加密保护,所述终端设备使用所述用户面加密保护密钥进行加密保护。

4.根据权利要求1所述的方法,其特征在于,所述用户面密钥包括用户面完整性保护密钥和用户面加密保护密钥;

所述使用用户面密钥进行用户面安全保护,包括:

若所述RRC重配置消息中包括完整性保护指示信息和加密指示信息,且所述完整性保护指示信息用于指示开启用户面完整性保护,以及所述加密保护指示信息用于指示开启用户面加密保护,所述终端设备使用所述用户面完整性保护密钥进行完整性保护以及使用所述用户面加密保护密钥进行加密保护。

5.根据权利要求1所述的方法,其特征在于,所述开启信令面保护,包括:

生成信令面密钥,并利用所述信令面密钥进行信令面保护;以及

生成所述用户面密钥。

6.根据权利要求1至5任一所述的方法,其特征在于,所述开启信令面保护之后,所述方法包括:

所述终端设备向所述基站发送接入层安全模式完成命令AS SMP。

7.一种终端设备,其特征在于,所述终端设备包括处理器;

所述处理器,用于在接收到基站发送的接入层安全模式命令AS SMC之后,开启信令面保护;

所述处理器,还用于在接收到无线资源控制RRC重配置消息后,使用用户面密钥进行用户面安全保护。

8.根据权利要求7所述的终端设备,其特征在于,所述用户面密钥包括用户面完整性保护密钥;

所述处理器,用于若所述RRC重配置消息中包括完整性保护指示信息且所述完整性保护指示信息用于指示开启用户面完整性保护,使用所述用户面完整性保护密钥进行完整性保护。

9.根据权利要求7所述的终端设备,其特征在于,所述用户面密钥包括用户面加密保护

密钥；

所述处理器，用于若所述RRC重配置消息中包括加密保护指示信息且所述加密保护指示信息用于指示开启用户面加密保护，使用所述用户面加密保护密钥进行加密保护。

10.根据权利要求7所述的终端设备，其特征在于，所述用户面密钥包括用户面完整性保护密钥和用户面加密保护密钥；

所述处理器，用于若所述RRC重配置消息中包括完整性保护指示信息和加密指示信息，且所述完整性保护指示信息用于指示开启用户面完整性保护，以及所述加密保护指示信息用于指示开启用户面加密保护，使用所述用户面完整性保护密钥进行完整性保护以及使用所述用户面加密保护密钥进行加密保护。

11.根据权利要求7所述的终端设备，其特征在于，

所述处理器，具体用于生成信令面密钥，并利用所述信令面密钥进行信令面保护；以及生成所述用户面密钥。

12.根据权利要求7至11任一所述的终端设备，其特征在于，所述终端设备还包括收发器；

所述收发器，用于向所述基站发送接入层安全模式完成命令AS SMP。

13.一种终端设备，其特征在于，所述终端设备包括处理单元；

所述处理单元，用于在接收到基站发送的接入层安全模式命令AS SMC之后，开启信令面保护；和

所述处理单元，还用于在接收到无线资源控制RRC重配置消息后，使用用户面密钥进行用户面安全保护。

14.根据权利要求13所述的终端设备，其特征在于，所述用户面密钥包括用户面完整性保护密钥；

所述处理单元，用于若所述RRC重配置消息中包括完整性保护指示信息且所述完整性保护指示信息用于指示开启用户面完整性保护，则使用所述用户面完整性保护密钥进行完整性保护。

15.根据权利要求13所述的终端设备，其特征在于，所述用户面密钥包括用户面加密保护密钥；

所述处理单元，用于若所述RRC重配置消息中包括加密保护指示信息且所述加密保护指示信息用于指示开启用户面加密保护，使用所述用户面加密保护密钥进行加密保护。

16.根据权利要求13所述的终端设备，其特征在于，所述用户面密钥包括用户面完整性保护密钥和用户面加密保护密钥；

所述处理单元，用于若所述RRC重配置消息中包括完整性保护指示信息和加密指示信息，且所述完整性保护指示信息用于指示开启用户面完整性保护，以及所述加密保护指示信息用于指示开启用户面加密保护，使用所述用户面完整性保护密钥进行完整性保护以及使用所述用户面加密保护密钥进行加密保护。

17.根据权利要求13所述的终端设备，其特征在于，

所述处理单元，具体用于生成信令面密钥，并利用所述信令面密钥进行信令面保护；以及

生成所述用户面密钥。

18.根据权利要求13至17任一所述的终端设备,其特征在于,所述终端设备还包括发送单元;

所述发送单元,还用于向所述基站发送接入层安全模式完成命令AS SMP。

19.一种计算机存储介质,其特征在于,所述计算机存储介质中存储有计算机软件指令,当所述计算机指令被执行时,所述权利要求1至6任一所述的方法会被运行。

一种通信方法及相关装置

技术领域

[0001] 本申请涉及无线通信技术领域,尤其涉及一种通信方法及相关装置。

背景技术

[0002] 在长期演进(Long Term Evolution,LTE)系统中,终端设备和基站之间执行加密/解密和完整性保护的安全操作,对信令提供加密保护和完整性保护。由于不同终端设备的安全能力不同,例如,所支持的加密算法或完整性保护算法不同,因此在接入层(Access Stratum,AS)进行加密保护和完整性保护之前,需要在终端设备和基站间协商一套安全算法。协商安全算法的过程包括以下步骤:

[0003] 1、终端设备通过基站向移动性管理实体(Mobility Management Entity,MME)发送附着请求;其中,附着请求中携带终端设备支持的算法。

[0004] 2、基站根据预配置的服务网络允许使用的算法,并结合MME转发的终端设备支持的算法,选择服务网络所支持的安全算法。该安全算法包括加密算法和完整性保护算法。基站根据选择的加密算法生成AS的加密秘钥,根据完整性保护算法生成完整性保护密钥。其中,基站选择出的服务网络所支持的安全算法既是用户面的安全算法,也是应用于信令面的安全算法。

[0005] 3、基站和终端设备通过AS安全模式命令(Security mode command,SMC)的流程使终端设备将基站选择出的安全算法应用于用户面和信令面。比如,将基站选择的加密算法和完整性保护算法携带在AS SMC中发送给终端设备。

[0006] 现有技术中通过AS SMC流程确定出同时应用于用户面和信令面的一种安全算法,且安全算法包括加密算法和完整性保护算法,这种安全算法的协商方案较为固定,比如用户面和信令面适用同一套安全算法,不能拆分,再比如加密算法和完整性保护算法必须同时确定出,也不能拆分,可见这种安全协商算法较为固定,并不能适应现在灵活多变的应用场景。

发明内容

[0007] 本申请实施例提供一种通信方法、相关装置及存储介质,用于能够灵活的单独协商用户面完整性保护算法的方案。

[0008] 第一方面,本申请实施例提供一种通信方法,包括:基站获取安全策略,安全策略包括完整性保护指示信息,完整性保护指示信息用于指示基站是否对终端设备开启完整性保护;当完整性保护指示信息指示基站对终端设备开启完整性保护时,基站向终端设备发送目标用户面完整性保护算法。如此,可根据安全策略灵活的为终端设备选择是否开启完整性保护,且仅在对终端设备开启完整性保护时,基站向终端设备发送目标用户面完整性保护算法,一方面,由于单独协商用户面的安全算法,提高了用户面安全算法和信令面安全算法分开确定的灵活性,另一方面,由于增加了完整性保护指示信息,提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0009] 可选地，所述完整性保护指示信息为用户面完整性保护算法的标识。也就是说若确定安全策略中携带用户面完整性保护算法的标识，则可确定基站对终端设备开启完整性保护。该实施例中安全策略中携带的用户面完整性保护算法的标识可以为一个或多个(可以称为算法列表)，该实施例中安全策略中携带的用户面完整性保护算法可以是根据服务网络允许的用户面完整性保护算法、终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法中的至少一项确定的；也可以说安全策略中携带的的用户面完整性保护算法是服务网络允许的用户面完整性保护算法。

[0010] 可选地，基站获取安全策略可以是基站从其它网元接收安全策略，也可以是基站从预先存储在基站的至少一个安全策略中确定出安全策略。预先存储在基站侧的安全策略也可以成为预先配置在基站侧的安全策略。基站从预先存储在基站的至少一个安全策略中获取安全策略的方式有多种，比如可根据终端标识与预存储在基站的安全策略的对应关系，确定出终端设备的标识对应的且存储在基站的安全策略；再比如，可以根据会话标识与预存储在基站的安全策略的对应关系，确定出会话标识对应的且存储在基站的安全策略；方案可以与SMF实体获取安全策略的方案类似，在此不再赘述。

[0011] 可选地，基站向终端设备发送目标用户面完整性保护算法，包括：基站通过RRC信令向终端设备发送目标用户面完整性保护算法。通过复用现有技术中的RRC信令的方式实现本申请实施例提供的方案，从而更好的兼容现有技术，且对现有技术改动较小。

[0012] 一种可选地实现基站向终端设备发送目标用户面完整性保护算法的方式中，基站向终端设备发送目标信令面完整性保护算法，终端设备将接收到的目标信令面完整性保护算法也确定为目标用户面完整性保护算法，也就是说基站向终端设备发送完整性保护算法，该完整性保护算法既是信令面完整性保护算法也是用户面完整性保护算法。

[0013] 可选地，在基站向终端设备发送目标用户面完整性保护算法之前，方法还包括：基站根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法，确定目标用户面完整性保护算法。如此可既考虑终端设备的安全能力也考虑基站的安全能力，从而使确定出的目标用户面完整性保护算法同时与终端设备的安全能力和基站的安全能力匹配。

[0014] 可选地，基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，如此可以选择出在基站侧更优的目标用户面完整性保护算法。或者，可选地，终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，如此可以选择出在终端设备侧更优的目标用户面完整性保护算法。

[0015] 可选地，安全策略还包括服务网络允许的用户面完整性保护算法；基站根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法，确定目标用户面完整性保护算法，包括：基站根据基站允许的用户面完整性保护算法，终端设备支持的用户面完整性保护算法，以及服务网络允许的用户面完整性保护算法，确定目标用户面完整性保护算法，如此可既考虑终端设备的安全能力也考虑基站的安全能力，同时还考虑到服务网络的实际状态，从而使确定出的目标用户面完整性保护算法一方面可与终端设备的安全能力和基站的安全能力匹配，另一方面与服务网络的实际状态更加匹配。

[0016] 可选地，在安全策略还包括服务网络允许的用户面完整性保护算法的情况下，基站也可以将安全策略中所包括的服务网络允许的用户面完整性保护算法之外的算法确定

为目标用户面完整性保护算法。比如可以从基站允许的用户面完整性保护算法中确定出一个算法作为目标用户面完整性保护算法。

[0017] 可选地，服务网络允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，如此可以选择出基于服务网络的更优的目标用户面完整性保护算法。

[0018] 可选地，方法还包括：当安全策略还包括加密指示信息，且加密指示信息用于指示基站对终端设备开启加密保护时，基站向终端设备发送目标用户面加密算法；或者，当安全策略还包括密钥长度时，基站向终端设备发送密钥长度；或者，当安全策略还包括D-H指示信息，且D-H指示信息用于指示基站对终端设备开启D-H时，基站向终端设备发送D-H相关密钥。如此，可以更加灵活的对安全策略中的任一个信息进行指示，使最终确定的安全策略更加适应复杂的应用场景。

[0019] 可选地，在基站向终端设备发送目标用户面完整性保护算法之前，还包括：基站从SMF实体接收终端设备的当前会话的服务质量；基站根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载。

[0020] 为了节省资源，可选地，基站根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载，包括：当基站上存在至少一个历史的无线数据承载满足第一条件时，基站将满足第一条件的至少一个历史的无线数据承载中的一个确定为目标无线数据承载；其中，满足所述第一条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的服务质量与所述当前会话的所述服务质量相同，且所述安全策略与所述每个无线数据承载支持的安全策略相同。

[0021] 可选地，第一条件包括：两个无线数据承载的服务质量相同，且两个无线数据承载的安全策略相同。

[0022] 为了节省资源，另一种可选地方案中，基站根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载，包括：当基站上不存在历史的无线数据承载满足第一条件，但存在至少一个历史的无线数据承载满足第二条件时，基站将满足第二条件的至少一个历史的无线数据承载中的一个进行更新后确定为目标无线数据承载；其中，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的与所述当前会话的所述服务质量相同，且所述安全策略与所述每个无线数据承载支持的安全策略匹配；或者，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的与所述当前会话的所述服务质量匹配，且所述安全策略与所述每个无线数据承载支持的安全策略相同；或者，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的与所述当前会话的所述服务质量匹配，且所述安全策略与所述每个无线数据承载支持的安全策略匹配。

[0023] 可选地，第二条件包括：两个无线数据承载的服务质量匹配，且两个无线数据承载的安全策略相同。或者，可选地，第二条件包括：两个无线数据承载的服务质量相同，且两个无线数据承载的安全策略匹配。或者，可选地，第二条件包括：两个无线数据承载的服务质量匹配，且两个无线数据承载的安全策略匹配。

[0024] 为了选择出合适的目标无线数据承载，另一种可选地方案中，基站根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载，包括：当基站上不存在历史的无线数据承载满足第一条件，且不存在至少一个历史的无线数据承载满足第二条件时，

基站根据安全策略和服务质量中的至少一种,为终端设备创建目标无线数据承载。

[0025] 为了选择出合适的目标无线数据承载,另一种可选地方案中,基站根据安全策略和服务质量中的至少一种,为终端设备分配目标无线数据承载,包括:当基站上不存在历史的无线数据承载满足第一条件时,基站根据安全策略和服务质量中的至少一种,为终端设备创建目标无线数据承载。

[0026] 为了选择出合适的目标无线数据承载,另一种可选地方案中,基站根据安全策略和服务质量中的至少一种,为终端设备分配目标无线数据承载,包括:基站根据安全策略和服务质量中的至少一种,为终端设备创建目标无线数据承载。

[0027] 可选地,基站获取安全策略,包括:基站从SMF实体接收安全策略;或者;基站从SMF实体接收安全策略的标识,并根据安全策略的标识,获取安全策略。

[0028] 可选地,本申请实施例中还包括:基站获取终端设备支持的信令面安全算法;基站根据终端设备支持的信令面安全算法,以及基站允许的信令面安全算法,确定目标信令面安全算法;基站将目标信令面安全算法携带在接入层AS安全模式命令SMC中发送给终端设备,如此可实现信令面的算法与用户面安全算法的解耦合,从而使用户面安全算法和信令面安全算法单独协商,从而为更加灵活的确定用户面安全算法提供了基础。

[0029] 可选地,基站在确定开启用户面完整性保护的情况下,开启用户面完整性保护。

[0030] 可选地,基站在确定开启用户面加密保护的情况下,开启用户面加密保护。

[0031] 可选地,基站在确定暂时不开启用户面完整性保护的情况下或者当前无法确定是否开启用户面完整性保护的情况下,不开启用户面完整性保护。

[0032] 可选地,基站在确定暂时不开启用户面加密保护的情况下或者当前无法确定是否需要开启用户面加密保护的情况下,不开启用户面加密保护。

[0033] 其中,暂时的意思是指具有一个时间段,暂时不开启用户面完整性保护是指一个时间段内不开启用户面完整性保护,在另一个时间段内开启用户面完整性保护。暂时不开启用户面加密保护是指一个时间段内不开启用户面加密保护,在另一个时间段内开启用户面加密保护。

[0034] 一种可选地实施方式中,网络规定的在接收到AS安全模式命令后可以开启用户面加密保护,而用户面完整性保护是否开启由RRC重配置消息来通知终端设备,这种情况下终端设备无法确定是否开启用户面完整性保护。

[0035] 另一种可选地实施方式中,网络规定的在接收到AS安全模式命令后,只开启信令面安全(开启信令面完整性保护和/或信令面加密保护),而用户面完整性保护是否开启以及用户面加密保护是否开启都由RRC重配置消息来通知终端设备,在这种情况下无法确定是否开启用户面完整性保护,也无法确定是否开启用户面加密保护。

[0036] 可选地,不开启用户面完整性保护包括:在无法确定是否开启用户面完整性保护或者确定暂时不开启用户面完整性保护的情况下,生成用户面完整性保护密钥,但是不使用用户面完整性保护密钥进行用户面完整性保护,在确定开启用户面完整性保护的情况下使用用户面完整性保护密钥进行用户面完整性保护。这种实施方式中,在生成用户面完整性保护密钥之前获取用户面完整性保护算法,比如可以将信令面完整性保护算法也作为用户面完整性保护算法。

[0037] 可选地,不开启用户面完整性保护包括:在确定开启用户面完整性保护的情况下

生成用户面完整性保护密钥,并使用用户面完整性保护密钥进行用户面完整性保护;也就是说,在无法确定是否开启用户面完整性保护或者确定暂时不开启用户面完整性保护的情况下,用户面完整性保护的情况下可以不生成用户面完整性保护密钥。相对应的,比如针对终端设备和基站,若确定终端设备和基站永久不开启用户面完整性保护(比如可以是预设的条件等等),则可以不生成用户面完整性保护密钥。

[0038] 可选地,不开启用户面加密保护包括:在无法确定是否开启用户面加密保护或者确定暂时不开启用户面加密保护的情况下,生成用户面加密密钥,但是不使用用户面加密密钥进行用户面加密保护,在确定开启用户面加密保护的情况下使用用户面加密密钥进行用户面加密保护。这种实施方式中,在生成用户面加密密钥之前获取用户面加密算法,比如可以将信令面加密算法也作为用户面加密算法。可选地,不开启用户面加密保护包括:在确定开启用户面加密保护的情况下生成用户面加密密钥,并使用用户面加密密钥进行用户面加密保护;也就是说,在无法确定是否开启用户面加密保护或者确定暂时不开启用户面加密保护的情况下,可以不生成用户面加密密钥。相对应的,比如针对终端设备和基站,若确定终端设备和基站永久不开启用户面加密保护(比如可以是预设的条件等等),则可以不生成用户面加密密钥。

[0039] 可选地,基站获取完整性保护指示信息和/或加密指示信息,根据获取的完整性保护指示信息确定是否开启完整性保护;或者,根据加密指示信息确定是否开启用户面加密保护。其中,完整性保护指示信息用于指示是否开启用户面完整性保护,加密指示信息用于指示是否开启用户面加密保护。

[0040] 可选地,基站获取完整性保护指示信息和/或加密指示信息的方式有多种,比如是基站判断后生成或者是接收到其它网元发送的完整性保护指示信息和加密指示信息中的至少一项。其它网元可以是SMF实体。

[0041] 可选地,基站可以向终端设备发送完整性保护指示信息和加密指示信息中的至少一项,以使终端设备确定是否开启用户面完整性保护和/或是否开启用户面加密保护。或者终端设备自己判断并确定是否开启用户面完整性保护和/或是否开启用户面加密保护。

[0042] 可选地,完整性保护指示信息和/或加密指示信息可以是比特信息或算法的标识。比如,完整性保护指示信息为目标用户面完整性保护算法的标识;再比如加密指示信息为目标用户面加密保护算法的标识,再比如,用1比特信息指示完整性保护指示信息或加密指示信息,再比如,用2比特信息指示完整性保护指示信息和加密指示信息。第二方面,本申请实施例提供一种通信方法,包括:SMF实体接收请求消息,请求消息包括安全策略的相关参数;SMF实体根据安全策略的相关参数,获得安全策略或者安全策略的标识;SMF实体向基站发送安全策略或安全策略的标识;其中,安全策略包括完整性保护指示信息,完整性保护指示信息用于指示基站是否对终端设备开启完整性保护。一方面,由于单独协商用户面的安全算法,提高了用户面安全算法和信令面安全算法分开确定的灵活性,另一方面,由于增加了完整性保护指示信息,提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0043] 可选地,所述完整性保护指示信息为用户面完整性保护算法的标识。也就是说若确定安全策略中携带用户面完整性保护算法的标识,则可确定基站对终端设备开启完整性保护。该实施例中安全策略中携带的用户面完整性保护算法的标识可以为一个或多个(可以称为算法列表),该实施例中安全策略中携带的用户面完整性保护算法可以是根据服务

网络允许的用户面完整性保护算法、终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法中的至少一项确定的;也可以说安全策略中携带的的用户面完整性保护算法是服务网络允许的用户面完整性保护算法。

[0044] 可选地,安全策略的相关参数包括终端设备的标识,终端设备的数据服务网络名称DNN,终端设备的切片的标识,终端设备的服务质量和终端设备的会话标识中的至少一种。如此,可根据不同的标识从不同的角度或粒度实现安全策略的制定,更加灵活。

[0045] 可选地,SMF实体根据安全策略的相关参数,获得安全策略或者安全策略的标识,包括:安全策略的相关参数包括终端设备的标识,SMF实体根据终端设备的标识与安全策略的关联关系以及终端设备的标识,获得安全策略,如此可实现在终端设备的粒度上的安全策略的确定,实现不同的终端设备可对应不同的安全策略的目的。

[0046] 另一种可选地实施方式中,SMF实体根据安全策略的相关参数,获得安全策略或者安全策略的标识,包括:安全策略的相关参数包括终端设备的切片的标识,SMF实体根据切片的标识和安全策略的关联关系以及终端设备的切片的标识,获得安全策略,如此可实现在切片的粒度上的安全策略的确定,实现接入不同的切片的终端设备可对应不同的安全策略的目的。

[0047] 另一种可选地实施方式中,SMF实体根据安全策略的相关参数,获得安全策略或者安全策略的标识,包括:安全策略的相关参数包括终端设备的会话标识,SMF实体根据会话标识和安全策略的关联关系以及终端设备的会话标识,获得安全策略,如此可实现在会话的粒度上的安全策略的确定,实现发起不同会话的终端设备可对应不同的安全策略的目的。

[0048] 另一种可选地实施方式中,SMF实体根据安全策略的相关参数,获得安全策略或者安全策略的标识,包括:安全策略的相关参数包括终端设备的服务质量;SMF实体根据终端设备的服务质量,获得安全策略,如此可实现在服务质量的粒度上的安全策略的确定,实现发起不同服务质量的终端设备可对应不同的安全策略的目的。

[0049] 可选地,安全策略还包括以下内容中至少一种:加密指示信息,加密指示信息用于指示基站对终端设备开启加密保护;密钥长度;D-H指示信息,D-H指示信息用于指示基站对终端设备开启D-H;和,服务网络允许的用户面完整性保护算法。如此,可以更加灵活的对安全策略中的任一个信息进行指示,使最终确定的安全策略更加适应复杂的应用场景。

[0050] 可选地,SMF实体向基站发送完整性保护指示信息和/或加密指示信息。完整性保护指示信息用于指示是否开启用户面完整性保护,加密指示信息用于指示是否开启加密保护。可选地,SMF实体判断是否开启用户面完整性保护和/或是否开启用户面加密保护有多种实施方式,可以参见后续实施例,也可以参见基站判断是否开启用户面完整性保护和/或是否开启用户面加密保护的实施方式,在此不再赘述。

[0051] 第三方面,本申请实施例提供一种基站,基站包括存储器、收发器和处理器,其中:存储器用于存储指令;处理器用于根据执行存储器存储的指令,并控制收发器进行信号接收和信号发送,当处理器执行存储器存储的指令时,基站用于执行上述第一方面或第一方面中任一种方法。

[0052] 第四方面,本申请实施例提供一种SMF实体,SMF实体包括存储器、收发器和处理器,其中:存储器用于存储指令;处理器用于根据执行存储器存储的指令,并控制收发器进

行信号接收和信号发送，当处理器执行存储器存储的指令时，SMF实体用于执行上述第二方面或第二方面中任一种方法。

[0053] 第五方面，本申请实施例提供一种基站，用于实现上述第一方面或第一方面中的任意一种方法，包括相应的功能模块，分别用于实现以上方法中的步骤。

[0054] 第六方面，本申请实施例提供一种SMF实体，用于实现上述第二方面或第二方面中的任意一种的方法，包括相应的功能模块，分别用于实现以上方法中的步骤。

[0055] 第七方面，本申请实施例提供一种计算机存储介质，计算机存储介质中存储有指令，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法。

[0056] 第八方面，本申请实施例提供一种计算机存储介质，计算机存储介质中存储有指令，当其在计算机上运行时，使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法。

[0057] 第九方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法。

[0058] 第十方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法。

[0059] 本申请实施例中，安全策略包括完整性保护指示信息，完整性保护指示信息用于指示基站是否对终端设备开启完整性保护，基站获取安全策略，当完整性保护指示信息指示基站对终端设备开启完整性保护时，基站向终端设备发送目标用户面完整性保护算法。如此，可根据安全策略灵活的为终端设备选择是否开启完整性保护，且仅在对终端设备开启完整性保护时，基站向终端设备发送目标用户面完整性保护算法，一方面，由于单独协商用户面的安全算法，提高了用户面安全算法和信令面安全算法分开确定的灵活性，另一方面，由于增加了完整性保护指示信息，提高了终端设备的目标用户面完整性保护算法确定的灵活性。

附图说明

[0060] 图1为本申请实施例适用的一种系统架构示意图；

[0061] 图2为本申请实施例提供的一种通信方法流程示意图；

[0062] 图2a为本申请实施例提供的另一种通信方法流程示意图；

[0063] 图2b为本申请实施例提供的另一种通信方法流程示意图；

[0064] 图3为本申请实施例提供的一种基站的结构示意图；

[0065] 图4为本申请实施例提供的一种终端设备的结构示意图；

[0066] 图5为本申请实施例提供的另一种基站的结构示意图；

[0067] 图6为本申请实施例提供的另一种终端设备的结构示意图。

具体实施方式

[0068] 图1示例性示出了本申请实施例适用的一种系统架构示意图，如图1所示，在5G系统架构中，包括终端设备101。终端设备101可以经无线接入网(Radio Access Network，简称RAN)与一个或多个核心网进行通信，终端设备可以指用户设备(User Equipment，简称终

端设备)、接入终端设备、用户单元、用户站、移动站、移动台、远方站、远程终端设备、移动设备、用户终端设备、终端设备、无线通信设备、用户代理或用户装置。接入终端设备可以是蜂窝电话、无绳电话、会话启动协议(Session Initiation Protocol,简称SIP)电话、无线本地环路(Wireless Local Loop,简称WLL)站、个人数字处理(Personal Digital Assistant,简称PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备,未来5G网络中的终端设备等。

[0069] 与终端设备101连接的基站102。可选地,基站102可为5G基站(generation Node B,gNB),可为演进的eNB,也可以为LTE基站eNB,3G基站NB,或者演进的5G基站等新型基站,英文也可写为(R)AN。基站102可以是用于与终端设备进行通信的设备,例如,可以是GSM系统或CDMA中的基站(Base Transceiver Station,BTS),也可以是WCDMA系统中的基站(NodeB,NB),还可以是LTE系统中的演进型基站(Evolutional Node B,eNB或eNodeB),还可以是5G基站或者该网络设备可以为中继站、接入点、车载设备、可穿戴设备以及未来5G网络中的网络侧设备或未来演进的PLMN网络中的网络设备等。

[0070] 会话管理功能(Session Management Function,SMF)实体103,可以是LTE中移动性管理模块(Mobility Management Entity,MME)的功能拆分,可主要负责用户的会话建立,用户的会话建立后,才可以收发数据。LTE系统中的MME是核心网侧负责安全、移动性管理和会话管理的网元。安全,即终端设备101在初始入网的时候,需要和网络进行相互认证。在互相认证之后,终端设备101和核心网会生成密钥。生成密钥后,终端设备101和MME会进行算法协商,也就是安全能力协商。移动性管理就是记录终端设备101的位置信息,根据终端设备101的位置信息为终端设备101选择合适的用户面网元设备。会话管理就是负责建立终端设备101的用户面链路,在建立好用户的数据面联络后,终端设备101才可以上网。

[0071] 用户面功能(User Plane Function,UPF)实体104可以是LTE系统中中服务网关(Serving GateWay,S-GW)和公用数据网网关(Public Data Network GateWay,P-GW)的合体,是终端设备101用户面的功能网元,主要负责连接外部网络。

[0072] 专用网络(Dedicated Network,DN)105可为终端设备101提供服务的网络,比如有些DN可以为终端设备101提供上网功能,有些DN可以为终端设备101提供短信功能。还包括策略控制功能(Policy Control Funtion,PCF)106。

[0073] 鉴权服务器功能(Authentication Server Function,AUSF)实体107与认证凭证存储和处理功能(Authentication Credential Repository and Processing Function,ARPF)交互,并且终结来自SEAF的鉴权请求。也是从LTE系统的归属签约用户服务器(Home Subscriber Server,HSS)拆分出来的功能。AUSF107可以是独立的网元。LTE系统中的HSS可以存储用户的签约信息,以及用户的长期密钥。

[0074] ARPF可以合并到用户数据管理(User Data Management,UDM)实体108中作为UDM的一部分。ARPF是从LTE的HSS中拆分出来的。主要用于存储长期密钥。与长期密钥相关的处理也在这里完成。

[0075] 接入和移动性管理(Access and Mobility Management Function,AMF)实体109的功能是管理终端设备101的接入问题,还管理终端设备101的移动性。可以是LTE中MME中的移动性管理模块(Mobility Management,MM)功能,同时加入了接入管理的功能。还可包括切片选择功能(Slice select Function,SSF)110。

[0076] 安全锚点功能(Security anchor function,SEAF)实体111负责终端设备101和网络侧的鉴权功能,会在鉴权成功后存储锚点密钥(anchor key)。

[0077] 安全上下文管理功能(Security Context Management Function,SCMF)实体112,从SEAF111获得密钥,进一步衍生其他密钥。是从MME拆分出来的功能。在实际情况中,SEAF111和SCMF112可能进一步独立成为一个单独的鉴权功能(Authentication function,AUF)实体。如图1所示,SEAF111和SCMF112合并到AMF109中组成一个网元。

[0078] 图1中还示出了各个网元中的接口的可能实现方式,比如基站102和AMF实体109之间的NG2接口,基站102与UPF实体104之间的NG9接口等等,在此不再一一赘述。

[0079] 图2示例性示出了本申请实施例提供的一种通信方法流程示意图。

[0080] 基于上述内容,本申请实施例提供的一种通信方法,如图2所示,该方法包括:

[0081] 步骤201,基站获取终端设备支持的信令面安全算法;可选地,有多种方式获取终端设备支持的信令面安全算法,终端设备支持的信令面安全算法至少包括至少一种信令面加密算法和至少一种信令面完整性保护算法,比如从AMF处接收,再比如通过信令消息直接从终端设备处获得,或者预配置在基站上。

[0082] 本申请实施例中提供一种方案用于实现上述步骤201,具体来说,终端设备向基站发送非接入层(Non-Access Stratum,NAS)消息。NAS消息是终端设备和核心网交互的信令面消息,如LTE的附着请求(attach request),或者5G的注册请求(Registration Request)。本实施例以5G的注册请求消息为例进行说明,其他NAS消息遇到类似的步骤可做相同处理。终端设备向基站发送注册请求(Registration Request),在该注册请求种携带终端设备支持的信令面安全算法。

[0083] 上述示例中可选地,注册请求中也可携带终端设备支持的用户面安全算法。终端设备支持的用户面安全算法可包括终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法。终端设备支持的信令面加密算法、终端设备支持的信令面完整性保护算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法中的任两种算法可相同或不同。一种可选地方案中,终端设备可以将终端设备支持的信令面完整性保护算法、终端设备支持的信令面加密算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法这四者可以分别上报,或者,若这四个算法中存在至少两个算法相同,则对于相同的两个算法可以进上报一个算法,比如,若终端设备支持的信令面完整性保护算法和终端设备支持的用户面完整性保护算法相同,则终端设备仅上报终端设备支持的信令面完整性保护算法和终端设备支持的用户面完整性保护算法对应的相同的一个算法;若终端设备支持的信令面加密算法和终端设备支持的用户面加密算法相同,则终端设备仅上报终端设备支持的信令面加密算法和终端设备支持的用户面加密算法对应的相同的一个算法。

[0084] 另一种可选地实施方式中,终端设备支持的信令面加密算法、终端设备支持的信令面完整性保护算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法都相同,则终端设备可仅上报一种算法用于指示该四种算法即可。比如,终端设备上报的算法分别为EEA1,EEA2,EIA1,EIA2;那么EEA1和EEA2可以既用于信令面加密算法选择,又用于用户面加密算法选择,同理EIA1和EIA2可以既用于信令面完整性保护算法选择,又可以用于用户面完整性保护算法选择。

[0085] 再比如,终端设备上报的算法分别为EEA11,EEA12,EIA11,EIA12,EEA21,EEA23,EIA21,EIA22,那么EEA11和EEA12可以用于信令面加密算法选择,EEA21和EEA23用于用户面加密算法选择,EIA11和EIA12用于信令面完整性保护算法选择,EIA21和EIA22用于用户面完整性保护算法选择。再比如,终端设备上报的算法分别为EEA11,EEA12,EIA1,EIA2,EEA21,EEA23,EIA21,EIA22,那么EEA11和EEA12可以用于信令面加密算法选择,EEA21和EEA23用于用户面加密算法选择,EIA1和EIA2可以既用于信令面完整性保护算法选择,又可以用于用户面完整性保护算法选择。再比如,终端设备上报的算法分别为EEA1,EEA1,EIA11,EIA12,EIA21,EIA22,那么EEA1和EEA2可以既用于信令面加密算法选择,又用于用户面加密算法选择,EIA11和EIA12用于信令面完整性保护算法选择,EIA21和EIA22用于用户面完整性保护算法选择。

[0086] 另一方面,一种可选地实施方案中,终端设备可以通过多条信令来上报终端设备支持的信令面安全算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法,其中一条信令中包括一种算法。另一种可选地方案中,通过一条或多条信令来上报终端设备支持的信令面安全算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法,其中一条信令中包括一种或多种算法,当一条信令中包括多种算法时,可在该条信令中预定义一些字段,这些字段用于承载对应算法,比如依次设置第一字段、第二字段和第三字段,第一字段预定义用于放置终端设备支持的信令面安全算法,第二字段预定义用于放置终端设备支持的用户面完整性保护算法,第三字段预定义用于放置终端设备支持的用户面加密算法。或者,当三种算法都相同时,仅在一条信令中上报一个算法,其它网元默认该一个算法同时为终端设备支持的信令面安全算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法。比如,终端设备上报的安全能力为EEA1,EEA2,EIA1,EIA2,那么EEA1和EEA2可以既用于信令面加密算法选择,又用于用户面加密算法选择,同理EIA1和EIA2可以既用于信令面完整性保护算法选择,又可以用于用户面完整性保护算法选择。再比如,UE上报的安全能力为EEA11,EEA12,EIA11,EIA12,EEA21,EEA23,EIA21,EIA22那么EEA11和EEA12可以用于信令面加密算法选择,EEA21和EEA23用于用户面加密算法选择,EIA11和EIA12用于信令面完整性保护算法选择,EIA21和EIA22用于用户面完整性保护算法选择。再比如,UE上报的安全能力为EEA11,EEA12,EIA1,EIA2,EEA21,EEA23,EIA21,EIA22那么EEA11和EEA12可以用于信令面加密算法选择,EEA21和EEA23用于用户面加密算法选择,EIA1和EIA2可以既用于信令面完整性保护算法选择,又可以用于用户面完整性保护算法选择。

[0087] 可选地,基站将注册请求转发给AMF,可选地,在AMF与基站之间进行双向鉴权并与其它核心网网元,比如SEAF、AUSF、SMF、PCF或UDM等进行其它注册流程之后,AMF发送第一注册接受消息(Registration Accept)给基站,基站将接收到的该第一注册接受信息转发给终端设备,转发的意思是不对消息本身进行改变,但由于承载消息的接口功能不同,会有额外参数添加到消息外,以实现消息传输功能,比如第一注册接受消息是通过N2接口发给基站,N2接口除了第一注册接受消息外,还有基站需要知道的信息。基站转发第一注册消息给UE是通过RRC消息,RRC消息中除了第一注册消息外,至少还会有其他UE需要知道的信息,或者能够找到UE的信息;或者将第一注册接受消息进行一定的转换,比如根据接口的不同进行格式转换等,将转换后的第一注册接受消息转发给终端设备。在此步骤中,若AMF和基站

之间的接口为NG2,则第一注册接受消息用NG2消息承载。第一注册接受消息中还携带有AMF或SEAF为基站生成的基础密钥(Kan)和终端设备上报的终端设备支持的信令面安全算法。可选地,注册请求消息可以放到NAS容器中,基础密钥(Kan)和终端设备的安全能力,可能放到NAS容器中,也可能放到NAS容器外。

[0088] 步骤202,基站根据终端设备支持的信令面安全算法,以及基站允许的信令面安全算法,确定目标信令面安全算法。

[0089] 在步骤202中,可选地,基站可预配置基站允许的信令面安全算法,可选地,该基站允许的信令面安全算法中包括的算法为进行优先级排序的,比如根据运营商的偏好进行优先级排序,根据本地现实环境配置的优先级排序。可选地,该基站允许的信令面安全算法可以是通过网络管理设备配置给基站的,也可以在基站建立之初在安装软件环境的过程中配置完成,也可以通过其他方式进行配置。

[0090] 步骤202中,一种可能的实现方式为,基站根据终端设备支持的信令面安全算法和具有优先级排序的基站允许的信令面安全算法,选择出具有优先级最高的同时又是终端设备支持的信令面安全算法作为目标信令面安全算法,目标信令面安全算法可包括一个加密算法和/或一个完整性保护算法。

[0091] 其中一种可能的具体实现方式为,基站选出既存在于终端设备支持的信令面安全算法,且存在于基站允许的信令面安全算法中所有算法的集合,并从该算法的集合中选择出在基站允许的信令面安全算法中优先级较高的算法作为目标信令面安全算法。

[0092] 这里需要说明的是,基站会至少根据运营商的喜好被配置或预配置有基站允许的信令面安全算法和基站允许的用户面安全算法。基站允许的信令面安全算法包括至少一个基站允许的信令面加密算法和/或至少一个基站允许的信令面完整性保护算法。基站允许的用户面安全算法包括至少一个基站允许的用户面加密算法和/或至少一个基站允许的用户面完整性保护算法。并且基站允许的信令面安全算法的至少一个基站允许的信令面加密算法和/或至少一个基站允许的信令面完整性保护算法是有优先级排序的,优先级排序可以由运营商决定。基站允许的用户面安全算法可以有优先级排序,也可以没有优先级排序。当基站允许的用户面安全算法和基站允许的信令面安全算法相同,并且基站允许的用户面安全算法的优先级排序和基站允许的信令面安全算法的优先级排序相同时,则基站可以只存一套有优先级排序的算法,即存储基站允许的且有优先级排序的用户面安全算法或存储基站允许的且有优先级排序的信令面安全算法。

[0093] 可选地,基站基于该目标信令面安全算法仅仅生成信令面的相关密钥,比如信令面完整性保护密钥和信令面加密密钥。信令面的相关密钥比如为无线资源控制(Radio Resource Control,RRC)相关密钥,具体来说可为RRC完整性保护密钥(Krrc-int)和RRC加密密钥(Krrc-enc)。基站生成密钥时可以基于基础密钥(Kan)来生成。Kan是基站从核心网网元获得的,比如接入和移动性管理功能(Access and mobility management Function,AMF),AUSF。

[0094] 步骤203,基站将目标信令面安全算法携带在接入层(Access Stratum,AS)安全模式命令(Security mode command,SMC)中发送给终端设备。

[0095] 可选地,在步骤203中有多种实现方式,基站可以向终端设备发送AS SMC,其中AS SMC中包括目标信令面安全算法的指示信息,比如目标信令面安全算法的标识。

[0096] 进一步，基站还可在AS SMC中携带终端设备支持的信令面安全算法。可选地，AS SMC可以用基站生成的信令面完整性保护密钥进行完整性保护。

[0097] 可选地，终端设备接收到AS SMC之后，基于目标信令面安全算法的指示信息确定目标信令面安全算法，并且生成信令面的相关密钥(终端设备生成信令面的相关密钥的方法与基站的生成信令面的相关密钥的方法相同)，并根据信令面完整性加密密钥对AS SMC的完整性保护进行检查。如果确定AS SMC完整性保护合格，即确定终端设备侧的信令面完整性保护密钥与基站用于对AS SMC的信令面完整性保护密钥相同。则可选地，在步骤203之后，还包括步骤204，终端设备向基站发送AS安全模式命令完成(Security mode command complete,SMP)。

[0098] 可选地，终端设备可以用生成的信令面的相关密钥对AS SMP进行加密和/或完整性保护。可选地，基站检查AS SMP消息的加密保护和/或完整性保护正确后。可选地，基站检查AS SMP消息的加密保护和完整性保护正确后，基站将接收到的该第一注册接受信息转发给终端设备，或者将第一注册接受消息进行一定的转换，比如根据接口的不同进行格式转换等，得到第二注册接受消息(Registration Accept)消息，将第二注册接受消息发送给终端设备。之后可选的，终端设备回复注册完成(Registration Complete)给AMF。

[0099] 基于上述示例可见，本申请实施例中通过AS SMC流程仅仅实现基站与终端设备协商目标信令面安全算法的目的，实现了信令面安全算法和用户面安全算法的解耦，由于可以分开确定信令面安全算法和用户面安全算法，因此提高了通信的灵活性。

[0100] 进一步，在上述示例中，一种可选地方案为终端设备通过发送注册请求上报终端设备支持的信令面安全算法，可选地，终端设备也可将终端设备支持的用户面完整性保护算法、终端设备支持的用户面加密算法携带在注册请求中上报。具体上报的可选方案可参照上述实施例，在此不再赘述。

[0101] 可选地，终端设备支持的信令面安全算法也可分为NAS层的终端设备支持的信令面安全算法和AS层的终端设备支持的信令面安全算法，其中，AS层的终端设备支持的信令面安全算法也可称为RRC层的终端设备支持的信令面安全算法。终端设备将上述终端设备支持的信令面安全算法、终端设备支持的用户面完整性保护算法、终端设备支持的用户面加密算法上报的时候可以为每个安全算法增加指示信息，也可以通过预定义一些字段，并在相应字段中放置相应算法的方式标识出每个安全算法是属于信令面还是用户面，或者是NAS层还是AS层的，举个例子，比如预定义一个字段用于放置信令面的安全算法，预定义另一个字段用于放置用户面安全算法，再比如，预定义一个字段用于放置NAS层的安全算法，预定义另一个字段用于放置AS层安全算法。或者终端设备将终端设备支持的所有安全算法全部上报给AMF，终端设备并不对这些安全算法是信令面还是用户面的进行区分，而由AMF做区分。或者由AMF转发给基站后，由基站做区分。

[0102] 相应地，在上述AMF向基站发送第一注册接受消息给基站时，可以将终端设备上报的所有安全算法均发送给基站，比如信令面安全算法、终端设备支持的用户面完整性保护算法和终端设备支持的用户面加密算法。或者仅仅将基站协商目标信令面安全算法需要的终端设备支持的信令面安全算法发送给基站。或者仅仅传递RRC层的终端设备支持的信令面安全算法。

[0103] 为了与现有技术兼容，可选地，基站在AS SMC消息中可以增加一个仅协商目标信

令面安全算法的指示信息，当终端设备解析AS SMC信息后发现存在仅协商目标信令面安全算法的指示信息，则仅仅根据确定的目标信令面安全算法生成信令面相关密钥。如此，终端设备和基站之间仍然只协商出来一套目标信令面安全算法。若终端设备解析AS SMC信息后发现不存在仅协商目标信令面安全算法的指示信息，则根据确定的目标信令面安全算法就变成目标安全算法，用于生成信令面相关密钥和用户面的相关密钥，用户面的相关密钥包括用户面加密密钥和用户面完整性保护密钥。信令面相关密钥包括信令面加密密钥和信令面完整性保护密钥。如此，终端设备和基站之间协商出来一套目标信令面安全算法，一套目标用户面安全算法。

[0104] 可选地，为了与现有技术兼容，基站可在在AS SMC信息中增加用于指示协商目标信令面安全算法的指示信息和/或协商用户面的相关密钥的指示信息的信息，比如增加一个比特位，该比特位可以为新增的也可复用目前的比特位，比如该比特位为0，则表示仅协商目标信令面安全算法，若该比特位为1，则表示同时协商目标信令面安全算法和用户面的相关密钥。

[0105] 本申请实施例中目标信令面安全算法包括目标信令面整性保护算法和目标信令面加密算法。可选地，可通过AS SMC流程协商出两个不同的目标信令面整性保护算法和目标信令面加密算法，或者协商出一个目标信令面安全算法，既作为目标信令面整性保护算法，也作为目标信令面加密算法。

[0106] 另一种可选地实施方案中，可通过AS SMC流程至少协商出目标信令面整性保护算法和目标信令面加密算法中的至少一种算法，另一种目标信令面安全算法可通过其它流程协商。

[0107] 可选地，基站和终端设备协商出的目标信令面安全算法可以用算法的标识来表示，一种可选地实施方案中，无论目标信令面整性保护算法和目标信令面加密算法相同或不同，则均用两个算法的标识分别表示，另一种可选地实施方案中，若目标信令面完整性保护算法和目标信令面加密算法相同，则可用一个算法的标识表示该目标信令面整性保护算法和目标信令面加密算法，若目标信令面整性保护算法和目标信令面加密算法不同，则用两个算法的标识表示该目标信令面整性保护算法和目标信令面加密算法。

[0108] 另一种可选地方案中，本申请实施例中包括目标信令面安全算法和目标用户面安全算法，一种可选地实施方案中，无论目标信令面安全算法和目标用户面安全算法相同或不同，则均用两套算法的标识分别表示，另一种可选地实施方案中，若目标信令面安全算法和目标用户面安全算法相同，则可用一套算法的标识表示该目标信令面安全算法和目标用户面安全算法，若目标信令面安全算法和目标用户面安全算法不同，则用两套算法的标识表示目标信令面安全算法和目标用户面安全算法。其中，目标信令面安全算法对应的一套算法的标识包括至少一个目标信令面整性保护算法的标识和至少一个目标信令面加密算法的标识，目标信令面安全算法对应的一套算法的标识依据上述示例中所示，可以用一个算法的标识也可分别用两个算法的标识来表示目标信令面整性保护算法和目标信令面加密算法。相应地，其中，目标用户面安全算法对应的一套算法的标识包括至少一个目标信令面整性保护算法的标识和至少一个目标用户面加密算法的标识，目标用户面安全算法对应的一套算法的标识依据上述示例中所示，可以用一个算法的标识也可分别用两个算法的标识来表示目标信令面整性保护算法和目标用户面加密算法。

[0109] 图2a示例性示出了本申请实施例提供的另一种通信方法流程示意图。

[0110] 基于上述论述，本申请实施例提供另一种通信方法，如图2a所示，该方法包括：

[0111] 可选地，步骤211，SMF实体接收请求消息，请求消息可包括终端设备的标识。可选地，SMF实体接收请求消息可以包括多种，比如注册请求(Registration Request)、服务请求(Service Request)或会话建立请求(Session Establishment Request)，其中，会话建立请求也可称为PDU会话建立请求。

[0112] 可选地，若请求消息消息为服务请求，则该服务请求可以首先由终端设备发送给基站，由基站转发给AMF，之后AMF直接转发，转发即不改变原消息的内容将消息发送给AMF，发送给AMF的时候可能会根据接口等因素增加其他参数，或者根据接口信息对其进行转换后，再发送给SMF。若基站和AMF之间的之间的接口为N2接口，AMF与SMF之间的接口为N11，则基站向AMF转发的服务请求为与N2接口匹配的请求，AMF向SMF转发的服务请求为与N11接口匹配的请求。服务请求为NAS层的请求。可选地，请求消息也可为注册请求。

[0113] 可选地，若请求消息为会话建立请求，则该会话建立请求可以首先由终端设备发送给AMF，之后AMF直接转发，转发即不改变原消息的内容将消息发送给AMF，发送给AMF的时候可能会或根据接口等因素增加其他参数，或者根据接口信息对其进行转换后再发送给SMF。

[0114] 可选地，在终端设备发送会话建立请求之前，终端设备可能处于会话连接断开的状态，可选地，终端设备与基站之间可以再次进行上述步骤的注册流程，即终端设备可以向基站发送注册请求，从而实现终端设备的注册，在注册流程中的AS SMC和AS SMP中重新协商终端设备和基站之间的目标信令面安全算法。

[0115] 在上述步骤中，终端设备的标识可包括：IMSI、IMEI和临时身份标识中的任一项或任多项等。

[0116] 步骤212，SMF实体根据安全策略的相关参数，获得安全策略或者安全策略的标识；

[0117] 步骤213，SMF实体向基站发送安全策略或安全策略的标识；其中，安全策略包括完整性保护指示信息，完整性保护指示信息用于指示基站是否对终端设备开启完整性保护。

[0118] 可选地，SMF或其他与SMF连接的网元上存储安全策略和安全策略标识的对应关系。此时安全策略已经完全预配置在SMF、基站、UE、或者其他与SMF连接的网元上。比如根据具体的业务配置，如VoIP话音业务的安全策略。比如根据服务的厂商配置，如水表厂。配置方式依据有多种，在此不一一列举。当SMF通过终端设备的标识或者其他参数，为终端设备确定安全策略后，就可以得带与安全策略对应的安全策略标识。SMF将安全策略标识传递给基站，基站就可以根据安全策略标识对应的安全策略，进行用户面安全保护。比如，SMF预配置有安全策略和安全策略标识的对应关系，SMF根据服务请求消息中的内容，比如终端设备的标识，确定安全策略标识。再比如，PCF有预配置的安全策略和安全策略标识对应的关系，则SMF需要从PDC处获得安全策略标识。再比如，SMF和PCF处都与预配置的安全策略标识，则PCF处预配置的安全策略标识可以覆盖SMF处配置的安全策略标识，即SMF将从PCF处获得的安全策略标识传递给基站。

[0119] 一种可选地实施方式中，SMF实体直接向基站发送安全策略或安全策略的标识，比如根据终端设备的标识以及预设的终端设备和安全策略的标识的预设关系，将终端设备标识对应的安全策略发给基站。预设的安全策略，可以预设在SMF上，也可以与设在PCF上或其

他网元上。预设的安全策略和安全策略的标识，可以预设在SMF上，也可以与设在PCF上或其他网元上。另一种可选地实施方式中，SMF实体接收请求消息之后，根据请求消息，向基站发送安全策略或安全策略的标识之前，还包括：SMF实体根据请求消息，获得安全策略。另一种可选地实施方式中，SMF实体接收请求消息之后，根据请求消息，向基站发送安全策略或安全策略的标识之前，还包括：SMF根据安全策略，获得安全策略标识。

[0120] 另一个方面，可选地，SMF实体向基站发送的安全策略或安全策略的标识所标识的安全策略可以是以前生成的安全策略，也可以是此次新生成的安全策略。

[0121] 上述步骤213中，SMF实体向基站发送安全策略或安全策略的标识有多种形式，比如，SMF实体可以根据安全策略的相关参数去生成安全策略。比如根据终端设备标识或者会话标识生成安全策略，也可以预设一些生成规则，也可以预配置好所有安全策略。

[0122] 可选地，基站可根据请求消息中携带的一些信息，将终端设备适用的或者终端设备此次的请求消息所适用的安全策略或安全策略的标识发送过去。可选地，安全策略的相关参数包括终端设备的标识，终端设备的数据网络名称(Data network name，DNN)，终端设备的切片的标识，终端设备的服务质量和终端设备的会话标识中的至少一种。可选地，安全策略的相关参数包括终端设备的标识，终端设备的DNN，终端设备的切片的标识，终端设备的服务质量，终端设备的会话标识和流标识中的至少一种。

[0123] 本申请实施例中的关联关系可以包括对应关系，也可包括一些规则，或者也可包括一些相关性的关系。举个例子，比如可以预设相关参数和安全策略的对应关系，之后找到相关参数对应的安全策略，比如，根据切片的标识确定切片标识对应的安全策略，再比如根据会话标识确定会话标识对应的安全策略，再比如根据会话标识、切片标识和安全策略这三者之间的关联关系确定会话标识和切片标识对应的安全策略。

[0124] 另一种可选地实施方式中，安全策略的相关参数包括终端设备的标识，SMF实体根据终端设备的标识与安全策略的关联关系以及终端设备的标识，获得安全策略。举例来说，可在SMF或其它与SMF连接的网元上存储终端设备与安全策略的对应关系，如终端设备与安全策略有对应关系，比如，用户签约数据中有IMSI和安全策略的对应关系，如此，可以针对不同的终端设备比如终端设备的一些服务性能要求等等设置不同的安全策略。

[0125] 再比如，可以预设终端设备的标识与安全策略的关联关系，比如终端设备的标识关联了多个安全策略，之后可以从终端设备的标识所关联的多个安全策略中选择一个安全策略，也可再根据相关参数中除终端设备的标识之外的其它参数进一步确定安全策略，比如结合会话标识从终端设备的标识关联的多个安全策略中选择出一个于该会话标识相关联的安全策略。再比如，根据服务质量确定服务质量流标识，再根据服务质量流标识确定对应的服务质量的安全策略。

[0126] 举个例子，比如一个物联网的终端设备，只负责抄送水表，即每月定期将水表数据发送给水厂。那么这个终端设备的安全策略是固定的，可以设置终端设备的标识对应一个安全策略，可选地，可以从UDM中保存的用户的签约数据获取。

[0127] 为了更清楚的介绍本申请实施例，下面再详细介绍几种根据根据相关参数发送安全策略或安全策略的标识的例子，详见下述实施方式a1、实施方式a2、实施方式a3和实施方式a4。

[0128] 实施方式a1

[0129] 终端设备的切片的标识为5G应用场景中终端设备所接入的切片的信息,用于表示终端设备会接入哪个切片。

[0130] 安全策略的相关参数包括终端设备的切片的标识,SMF实体根据切片的标识和安全策略的关联关系以及终端设备的切片的标识,获得安全策略。具体来说,一个终端设备可以对应至少一个切片的标识,比如终端设备可以接入不同的切片,终端设备用户面数据在不同的切片下可以对应不同的安全策略。

[0131] 终端设备在SR消息中,或者PDU会话建立请求(session establishement request)中,携带切片选择辅助信息(network slice selection assistance information,NSSAI)。SMF会获得NSSAI对应的安全策略,如果这个NSSAI对应的切片的安全策略是唯一的,那么终端设备接入该切片时获取的安全策略唯一。如果NSSAI信息中包含至少一个切片,则需要根据终端设备当前接入的切片的安全策略进行选择(不同切片的安全策略可不同)。如果在确定了接入的切片后,当前切片的安全策略唯一,那么终端设备接入该切片时获取的安全策略唯一。如果当前切片的安全策略不唯一,那么终端设备需要根据其他信息进一步确定安全策略,终端设备需要根据其他信息进一步确定安全策略的实施方式有多种,比如根据相关参数中除了切片标识之外的其它至少一种标识进行选择,比如通过终端设备标识或会话标识等等。

[0132] 实施方式a2

[0133] 终端设备的会话标识为终端设备此次请求消息所对应的会话所对应的会话标识。会话,英文可称为session,比如终端设备进行因特网(internet)业务(如,浏览网页、看视频、微信聊天),是一个会话。终端设备接入了终端设备所在公司的内网,使用公司特定的业务(如,公司会议),这又是一个会话。终端设备接入拨打VoIP电话的网络,这个又是一个会话。这里我们可以设置接入因特网(internet)业务的会话标识为1;公司内网的会话标识为2;VoIP电话的会话标识为3。

[0134] 安全策略的相关参数包括终端设备的会话标识,SMF实体根据会话标识和安全策略的关联关系以及终端设备的会话标识,获得安全策略。如此,针对同一个终端设备,当终端设备发起不同的会话时,可以为不同的会话选择不同的安全策略。

[0135] 举个例子,比如一个正常的终端设备,这个终端设备只开通了打电话和发短信的业务。这2种业务分部属于2个会话。那么服务质量和安全策略就是根据会话的不同而不同。对于打电话业务,不需要开启用户面完整性保护,不需要密钥混合,用户面加密算法用128比特的即可,用户面加密密钥长度128bit。而对于短信息业务,需要开启用户面完整性保护,需要密钥混合,用户面加密算法用128bit,用户面加密密钥用128bit(比特),用户面完整性保护算法用256bit,用户面完整性保护密钥用256bit。

[0136] 举个例子,比如会话标识所对应的业务是超低时延业务,则可能为了保证时延低,安全策略中就要使用安全级别较低的用户面完整性保护算法和用户面加密算法,比如128bit用户面完整性保护算法和用户面加密算法,以及128bit的用户面完整性保护密钥和用户面加密密钥;或不启用用户面完整性保护算法和用户面加密算法。再比如会话标识所对应的业务是可靠性要求高的业务,则不仅需要用户面加密密钥进行加密保护,还需要用户面完整性保护密钥进行完整性保护,而且要选择安全级别较高的用户面完整性保护算法和用户面加密算法,比如256bit的用户面完整性保护算法和用户面加密算法,以及256bit

的用户面加密密钥和用户面加密密钥。再比如会话标识所对应的业务是一般普通的业务，如话音业务，可能只需要用户面加密密钥保护，而不需要用户面完整性保护，并且可能需要256bit的用户面加密算法，但密钥用128bit用户面加密密钥就够了。可见，本申请实施例中基于不同的业务可以选择出不同的安全策略，满足用户面安全的动态需求。

[0137] 实施方式a3

[0138] 终端设备接入一个切片后可能发起多个会话，因此一个切片标识可能对应多个会话标识，这里所说的对应关系是逻辑上的对应关系，实际应用中，并不代表一定可以明确说明会话标识与切片标识的对应关系。

[0139] SMF实体根据终端设备的标识、切片的标识、会话标识和安全策略四者之间的关联关系，获得切片的标识和会话标识对应的安全策略。如此，可以得到更细粒度的划分，为同一个终端设备，接入同一个切片中发起的不同的会话分别选择安全策略。

[0140] 实施方式a4

[0141] 可选地，SMF实体根据流标识和安全策略的关联关系，获得终端设备的安全策略。如此，可以得到更细粒度的划分，为同一个终端设备，接入同一个网络中发起相同的会话，却根据会话的具体内容分别选择安全策略。

[0142] 举个例子，比如终端设备支持上网业务，那么上网的数据流可以是浏览网页，可以是看视频。对于这个终端设备，上网业务都属于会话1，那么浏览网页是流1，看视频是流2。SMF会在发现没有支持流1的服务质量的时候，为流1创建服务质量。对于流2的同理。如果SMF发现流1和流2的服务质量都有了，那么就会直接将这些服务质量发给基站。

[0143] 实施方式a4

[0144] 安全策略的相关参数包括终端设备的服务质量;SMF实体根据终端设备的服务质量，获得安全策略。可选地，可根据请求消息中包括的终端设备标识，获取该终端设备标识对应的一些服务质量，该服务质量比如为该终端设备要求时延低，安全性好等等，之后根据服务质量为终端设备设置一套安全策略。本申请实施例中，安全策略可以预配置在SMF或PCF上，也可以从UPF和、或UDM中获取到DNN对应的服务质量，之后根据服务质量得到一个安全策略。默认的服务质量UDM是在签约的时候录入的。UPF可以从外部的处理电话或短信的网络中了解到动态服务质量，也可以从PCF处了解到，也可以预配置。

[0145] 可选地，安全策略的相关参数包括终端设备的DNN，根据DNN对应设置一套安全策略，比如DNN为优酷，优酷网络中视频业务较多，则为终端设备设置的安全策略中时延可以低一些，再比如，DNN为与财务相关的网站，则为终端设备设置的安全策略中安全性要高一些。

[0146] 进一步，可以根据DNN从核心网网元，比如PCF/UPF或UDM中获取该DNN对应的服务质量，服务质量中携带有安全策略，或者之后根据服务质量设置安全策略。其中，从PCF获得的是动态的服务质量信息，从UDM中获得是用户签约时默认的服务质量信息。

[0147] 可选地，SMF从UDM获取信息可以通过向UDM发送签约数据请求(Subscription Data Request)，以及从UDM接收签约数据响应(Subscription Data Response)来获取。SMF与PCF之间可以通过PDU-CAN会话修改(PDU-CAN session modification)信息进行获取。SMF与UPF之间可以通过向UPF发送会话建立/修改请求(Session Establishment/Modification Request)，以及从UDM接收会话建立/修改响应(Session Establishment/

Modification Response)来获取。

[0148] 在实施方式a4中,服务质量可被服务质量流(Quality of Service flow,QoS flow),用标识(Identification,ID)标识,可称为QoS Flow ID,简称QFI。在本申请实施例中,服务质量内容(QoS Profile)用QFI进行标识。

[0149] 服务质量中可包括多个参数,比如5GQoS指示(QoS Indicator,5QI)。5QI用于标识性能特征(Performance characteristics),可包括:资源类型((Guaranteed flow bit rate,GBR)还是Non-GBR的)、数据包延迟度和误码率中的任一项或任多项,可能还包括其它参数。5QI是网元为服务质量分配资源的基础参数。

[0150] 服务质量中还可包括分配和保留优先级(allocation and retention Priority,ARP)。可用1到15标识优先级。表示为服务质量请求资源的优先级,是否可以因为资源限制而拒绝建立无线数据承载。

[0151] 服务质量中还可包括2个参数,用于定义是否可以抢占其他服务质量对应的资源(比如无线数据承载)或者该服务质量建立的无线数据承载是否可以被其他服务质量抢占。

[0152] 可选地,对于有GBR的数据内容,服务质量中还可包括:GBR保证数据传输速率(Guaranteed flow bit rate),可用于上下行。其中,GBR的数据内容GBR可以是一种会话或者是一种流,GBR数据拥有对应的服务级别,不同的服务级别也会对应不同的服务质量。Non-GBR数据对应的都是默认的服务级别。比如说,对于运营商,通话一定是要保障的,所以打电话就有GBR的保证。而对于普通的短消息业务,就是non-GBR,稍微延迟一会也不会有什么问题。还有一种情况,举例来说,就是如果腾讯游戏买了运营商的服务,那么原来腾讯游戏non-GBR的业务流就会变成GBR的。

[0153] 可选地,服务质量中还包括最大传输速率(Maximum Flow Bit Rate,MFBR),一个会话的所有流(flow)加起来不可以超过这个速率。一旦超过了,可能就需要参考ARP要不要拒绝建立或者抢占其他资源了。

[0154] 可选地,服务质量中还包括通知控制(Notification control)。这个设定为开或关,如果出现了无法为该服务质量建立无线数据承载的情况,要根据这个开关判断是否要通知终端设备。

[0155] 可选地,安全策略还包括以下内容中至少一种:加密指示信息,加密指示信息用于指示基站对终端设备开启加密保护;密钥长度;D-H指示信息,D-H指示信息用于指示基站对终端设备开启D-H;服务网络允许的用户面完整性保护算法。也就是说,安全策略还可包括是否开启用户面加密,是否开启用户面完整性保护,加解密算法是128bit还是256bit,密钥长度是128bit还是256bit,是否开启密钥混合中的一种或多种等等这些内容的任一项或任多项。举一些具体例子,比如用比特位来指示安全策略中包括的内容,比如比特序列0000000,代表不开启用户面加密保护且不开启用户面完整性保护,因为都没开启,所以后面都是0。再比如比特序列1010100,即指示开启用户面加密保护但不开启用户面完整性保护,使用128比特的加密算法,不开启密钥混合。请注意给出的只是示例,符合此原则的示例都被此专利覆盖。本申请实施例中密钥混合即是指D-H,D-H为一种密钥混合算法。

[0156] 可选地,SMF实体在确定该终端设备的安全策略中需要开启加密指示信息时,安全策略中还可包括服务网络允许的用户面加密算法。或者,安全策略中出现允许的用户面加密算法,就代表用户面加密是需要开启的。可选地,服务网络是为终端设备提供服务的网

络。

[0157] 可选地，安全策略中可包括用户面完整性保护算法的密钥长度，也可包括用户面加密算法的密钥长度。或者，安全策略中出现允许的用户面加密算法，算法是256bite，就代表使用256bite的密钥长度。

[0158] 可选地，在基站获取安全策略之前，方法还包括：基站向接入和移动性管理AMF实体发送第一优先级指示信息，第一优先级指示信息用于指示基站允许的用户面完整性保护算法未按照优先级排序。

[0159] 可选地，AMF将第一优先级指示信息转发给SMF，如此，SMF在获取该第一优先级指示信息后，知道基站允许的用户面完整性保护算法未按照优先级排序，因此SMF会对服务网络允许的用户面完整性保护算法进行优先级排序或者对该终端设备支持的用户面完整性保护算法并进行优先级排序，该终端设备支持的用户面完整性保护算法从AMF处获得。

[0160] 另一种可选地实施方式中，如果SMF未获取该第一优先级指示信息，或者SMF根据其它方式知道基站允许的用户面完整性保护算法按照优先级排序，则SMF可选的不对服务网络允许的用户面完整性保护算法进行优先级排序。可选地，对服务网络允许的用户面完整性保护算法进行优先级排序可以根据很多元素，比如可根据当前运营商的喜好、当地的服务网络环境等因素。

[0161] 可选地，在基站获取安全策略之前，方法还包括：基站向接入和移动性管理AMF实体发送第二优先级指示信息，第二优先级指示信息用于指示基站允许的用户面加密是否未按照优先级排序。

[0162] 可选地，AMF将第二优先级指示信息转发给SMF，如此，SMF在获取该第二优先级指示信息后，知道基站允许的用户面加密算法未按照优先级排序，因此SMF会对服务网络允许的用户面加密算法进行优先级排序或者对该终端设备支持的用户面加密算法并进行优先级排序，该终端设备支持的用户面加密算法从AMF处获得。

[0163] 另一种可选地实施方式中，如果SMF未获取该第二优先级指示信息，或者SMF根据其它方式知道基站允许的用户面加密算法按照优先级排序，则SMF可选的不对服务网络允许的用户面加密算法进行优先级排序。可选地，对服务网络允许的用户面加密算法进行优先级排序可以根据很多元素，比如可根据当前运营商的喜好、当地的服务网络环境等因素。

[0164] 上述示例中，对用户面加密算法和用户面完整性保护算法的优先级进行了分别介绍，另一种可选地实施方式中，用户一个指示信息同时指示用户面加密算法和用户面完整性保护算法的优先级问题。

[0165] 可选地，在基站获取安全策略之前，方法还包括：基站向接入和移动性管理AMF实体发送第三优先级指示信息，第三优先级指示信息用于指示基站允许的用户面加密算法和用户面的完整性保护算法均未按照优先级排序。用户面加密算法和用户面的完整性保护算法可以相同也可不同。

[0166] 可选地，AMF将第三优先级指示信息转发给SMF，如此，SMF在获取该第三优先级指示信息后，知道基站允许的用户面加密算法和用户面的完整性保护算法未按照优先级排序，因此SMF会对服务网络允许的用户面加密算法和用户面的完整性保护算法进行优先级排序或者对该终端设备支持的用户面加密算法和用户面的完整性保护算法并进行优先级排序，该终端设备支持的用户面加密算法和用户面的完整性保护算法从AMF处获得。

[0167] 另一种可选地实施方式中，如果SMF未获取该第三优先级指示信息，或者SMF根据其它方式知道基站允许的用户面加密算法和用户面的完整性保护算法按照优先级排序，则SMF可选的不对服务网络允许的用户面加密算法进行优先级排序。可选地，对服务网络允许的用户面加密算法和用户面的完整性保护算法进行优先级排序可以根据很多元素，比如可根据当前运营商的喜好、当地的网络环境等因素。

[0168] 图2b示例性示出了本申请实施例提供的另一种通信方法流程示意图。

[0169] 基于上述内容，本申请实施例提供的一种通信方法，如图2b所示，该方法包括：

[0170] 步骤221，基站获取安全策略，安全策略包括完整性保护指示信息，完整性保护指示信息用于指示基站是否对终端设备开启完整性保护。

[0171] 与前述内容类似，可选地，安全策略，还可以包括允许的用户面加密算法、服务网络允许的用户面完整性保护算法，以及是否开启密钥混合的指示信息。可选地，服务网络允许的用户面加密算法可包括开启用户面加密保护和密钥长度信息。比如用户面加密算法是256比特的，就使用256比特的密钥。可选地，如果服务网络允许的用户面加密算法出现了空加密算法，则允许基站不开启用户面加密保护。可选地，如果安全策略中出现了服务网络允许的用户面完整性保护算法，则基站开启用户面完整性保护。可选地，根据完整性算法的比特信息确定密钥长度，即256比特的完整性算法就使用256比特的密钥。可选地，允许的用户面完整性保护算法不会出现空算法，如果安全策略中没有出现完整性保护算法，则就是不开启完整性保护。可选地，也可以用其他信息告知基站密钥长度信息，如通过比特位信息。

[0172] 步骤222，当完整性保护指示信息指示基站对终端设备开启完整性保护时，基站确定目标用户面完整性保护算法；

[0173] 步骤223，基站向终端设备发送目标用户面完整性保护算法。基站如何向终端设备发送目标用户面完整性保护算法参考上述内容，在此不再赘述。

[0174] 可选地，在上述步骤221和步骤223之间还可包括上述AS SMC和AS SMP流程，用于重新协商基站和终端设备之间的目标信令面安全算法。具体来说，可以再上述步骤221和步骤223之间增加上述步骤201至步骤204。

[0175] 可选地，基站获取安全策略包括：基站从SMF实体接收安全策略。或者，可选地，在基站预先存储安全策略，之后当基站从SMF实体接收安全策略的标识，并根据安全策略的标识，获取安全策略。

[0176] 可选地，在基站可定义(Directory System Protocol，SDAP)层，用于将服务质量映射到分组数据汇聚协议(Packet Data Convergence Protocol，PDCP)层。每个PDCP层对应一个DRB。因此，之前我们定义的安全级别，需要在RAN侧更进一步细分。如果安全依然是在PDCP层做，即用户面的加解密和完整性保护依然在PDCP层完成。因为一个PDCP层对应一个DRB，因此在RAN侧只能做到DRB级别的安全处理。如果安全或者部分安全处理可以上移到SDAP层做，则可以做到QoS flow级别的安全处理。部分安全是指如果只有用户面完整性保护基于流粒度，则只需要将完整性保护相关的安全处理放到SDAP层。如果用户面加解密和完整性保护处理都是基于流粒度，则都需要在SDAP层完成。所以基于流粒度的级别的安全处理的前提是，安全或部分安全放到SDAP层做。

[0177] 比如一个会话中中有4个业务流(IP-flow)，3个QoS flow。NAS-level mapping表示第一次QoS处理。是将IP flow映射成为QoS flow。用QFI(QoS flow ID)表示。可以看到IP

lfow1和IP flow4放到了QFI1中,其他的都是单独的一个QFI。在SDAP层,SDAP层会将不同给的QFI映射到不同的PDCP层。可以看到QFI1和QFI2被放到了一个PDCPEntity(PDCP实体),就说明这QFI1和QFI2通过一个DRB传输。(一个PDCP实体对应一个DRB承载)QFI-3放到了另一个PDCP Entity-2,就是另一个DRB承载。

[0178] 可选地,基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。或者,终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。基站允许的用户面完整性保护算法可根据当地运营商喜好,或者当地环境等内容进行优先级排序,可预先配置在基站上。终端设备支持的用户面完整性保护算法可根据终端设备入网签约内容,或/和终端设备的喜好等内容进行优先级排序,可以由终端设备在签约时或者购买更多服务的时候进行排序。可选地,安全策略中可包括终端设备支持的用户面完整性保护算法。

[0179] 可选地,在上述步骤222中,一种可选地实施方案中,安全策略中包括至少一个用户面完整性保护算法,基站直接将安全策略中包括的至少一个用户面完整性保护算法中的一个用户面完整性保护算法确定为目标用户面完整性保护算法。另一种可选地方案中,所述基站确定所述目标用户面完整性保护算法,包括:基站根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法,确定目标用户面完整性保护算法。

[0180] 基站确定目标用户面完整性保护算法可存在几种可选地实施方式,比如基站确定既属于终端设备支持的用户面完整性保护算法,也属于基站允许的用户面完整性保护算法的至少一个算法,从该至少一个算法中确定目标用户面完整性保护算法。可选地,若基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法,则从至少一个算法中确定在基站允许的用户面完整性保护算法中优先级排序较高或者最高的算法作为目标用户面完整性保护算法。可选地,若终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法,则基站从至少一个算法中确定在终端设备支持的用户面完整性保护算法中优先级排序较高或者最高的算法作为目标用户面完整性保护算法。

[0181] 可选地,安全策略还包括服务网络允许的用户面完整性保护算法,可选地,服务网络允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。可选地,服务网络允许的用户面完整性保护算法可为预先配置在SMF上的。服务网络允许的用户面完整性保护算法的优先级可以根据运营商喜好,和\或当地环境等因素进行排序。可选地,基站根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法,确定目标用户面完整性保护算法,包括:基站根据基站允许的用户面完整性保护算法,终端设备支持的用户面完整性保护算法,以及服务网络允许的用户面完整性保护算法,确定目标用户面完整性保护算法。具体的,服务网络允许的用户面完整性保护算法有优先级排序的时候,以服务网络允许的优先级排序为首要条件或以基站允许的优先级排序为首要条件进行选择,究竟根据哪个优先级排序由当地运营商的策略决定,也可以根据其他信息决定,比如当前基站允许的用户面完整性保护算法是近期更新的,而服务网络允许的用户面完整性保护算法的是很久之前更新的,则以基站允许的用户面完整性保护算法的优先级排序为首要条件;再比如,默认的就是以基站允许的用户面完整性保护算法的优先级排序为首要条件;如果服务网络允许的用户面完整性保护算法没有优先级排序的时候,则以基站允许的用户面完整性保护算法的优先级排序为首要条件。

[0182] 基站确定目标用户面完整性保护算法可存在几种可选地实施方式，比如基站确定既属于终端设备支持的用户面完整性保护算法，也属于基站允许的用户面完整性保护算法，且还属于服务网络允许的用户面完整性保护算法的至少一个算法，从该至少一个算法中确定目标用户面完整性保护算法。可选地，若基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，则从至少一个算法中确定在基站允许的用户面完整性保护算法中优先级排序较高或者最高的算法作为目标用户面完整性保护算法。可选地，若终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，则基站从至少一个算法中确定在终端设备支持的用户面完整性保护算法中优先级排序较高或者最高的算法作为目标用户面完整性保护算法。可选地，若服务网络允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法，则基站从至少一个算法中确定在服务网络允许的用户面完整性保护算法中优先级排序较高或者最高的算法作为目标用户面完整性保护算法。可选地，本申请实施例中网络可包括5G网络或由5G网络演进的网络。

[0183] 可选地，方法还包括：当安全策略还包括加密指示信息，且加密指示信息用于指示基站对终端设备开启加密保护时，基站向终端设备发送目标用户面加密算法。

[0184] 基于上述内容，下面介绍基站和终端设备还需协商目标用户面加密算法方法流程。

[0185] 可选地，基站允许的用户面加密算法为按照优先级排序的用户面加密算法。或者，终端设备支持的用户面加密算法为按照优先级排序的用户面加密算法。基站允许的用户面加密算法可至少根据运营商喜好进行优先级排序，可以由运营商在建网时进行排序，可预先配置在基站上。终端设备支持的用户面加密算法可根据运营商喜好进行优先级排序，可以由用户在入网签约时进行排序。可选地，安全策略中可包括终端设备支持的用户面加密算法。

[0186] 可选地，还包括一种可选地实施方案，安全策略中包括至少一个用户面加密算法，基站直接将安全策略中包括的至少一个用户面加密算法中的一个用户面加密算法确定为目标用户面加密算法。另一种可选地方案中，基站根据终端设备支持的用户面加密算法和基站允许的用户面加密算法，确定目标用户面加密算法。

[0187] 基站确定目标用户面加密算法可存在几种可选地实施方式，比如基站确定既属于终端设备支持的用户面加密算法，也属于基站允许的用户面加密算法的至少一个算法，从该至少一个算法中确定目标用户面加密算法。可选地，若基站允许的用户面加密算法为按照优先级排序的用户面加密算法，则从至少一个既属于终端设备支持的用户面加密算法也属于基站允许的用户面加密算法中确定在基站允许的用户面加密算法中优先级排序较高或者最高的一个算法作为目标用户面加密算法。可选地，若终端设备支持的用户面加密算法为按照优先级排序的用户面加密算法，则基站从至少一个既属于终端设备支持的用户面加密算法也属于基站允许的用户面加密算法中确定在终端设备支持的用户面加密算法中优先级排序较高或者最高的算法作为目标用户面加密算法。

[0188] 可选地，安全策略还包括服务网络允许的用户面加密算法，可选地，服务网络允许的用户面加密算法为按照优先级排序的用户面加密算法。可选地，服务网络允许的用户面加密算法可为预先配置在SMF上的。服务网络允许的用户面加密算法的优先级可以至少根据运营商喜好进行排序。可选地，基站根据终端设备支持的用户面加密算法和基站允许的

用户面加密算法,确定目标用户面加密算法,包括:基站根据基站允许的用户面加密算法,终端设备支持的用户面加密算法,以及服务网络允许的用户面加密算法,确定目标用户面加密算法。具体的,服务网络允许的用户面加密算法有优先级排序的时候,以服务网络允许的优先级排序为首要条件进行选择;如果服务网络允许的用户面加密算法没有优先级排序的时候,则以基站允许的用户面安全算法的优先级为首要条件.

[0189] 基站确定目标用户面加密算法可存在几种可选地实施方式,比如基站确定既属于终端设备支持的用户面加密算法,也属于基站允许的用户面加密算法,且还属于服务网络允许的用户面加密算法的至少一个算法,从该至少一个既属于终端设备支持的用户面加密算法,也属于基站允许的用户面加密算法,且还属于服务网络允许的用户面加密算法中确定目标用户面加密算法。可选地,若基站允许的用户面加密算法为按照优先级排序的用户面加密算法,则从至少一个既属于终端设备支持的用户面加密算法,也属于基站允许的用户面加密算法,且还属于服务网络允许的用户面加密算法中确定在基站允许的用户面加密算法中优先级排序较高或者最高的算法作为目标用户面加密算法。可选地,若终端设备支持的用户面加密算法为按照优先级排序的用户面加密算法,则基站从至少一个既属于终端设备支持的用户面加密算法,也属于基站允许的用户面加密算法,且还属于服务网络允许的用户面加密算法中确定在终端设备支持的用户面加密算法中优先级排序较高或者最高的算法作为目标用户面加密算法。可选地,若服务网络允许的用户面加密算法为按照优先级排序的用户面加密算法,则基站从至少一个既属于终端设备支持的用户面加密算法,也属于基站允许的用户面加密算法,且还属于服务网络允许的用户面加密算法中确定在服务网络允许的用户面加密算法中优先级排序较高或者最高的算法作为目标用户面加密算法。

[0190] 可选地,当安全策略还包括密钥长度时,基站向终端设备发送密钥长度。密钥长度包括用户面完整性保护密钥长度和用户面加密密钥密钥长度。可选地,本申请实施例中基站向终端设备发送目标用户面完整性保护算法、目标用户面加密算法、密钥长度等信息时,可以通过一条信令,比如RRC重配置请求发送,或者通过多条信息发送。

[0191] 一种可选地实施方式中,若使用RRC重配置请求发送的时候,则发送方式可以有多种,比如可以采用RRC重配置消息,该RRC重配置消息种可包括:目前用户面加密算法、目标用户面完整性保护算法、用户面加密密钥长度、用户面完整性保护密钥长度、密钥混合策略(也可称为D-H是否开启指示信息、DRB-1(QoS信息)、DRB-2(QoS信息)和其他参数中的至少一种。

[0192] 一种可选地实施方式中,若用户面完整性不开启的时候,则不会传递目标用户面完整性保护算法,当算法本身可以指示密钥长度的时候,则密钥长度的指示信息是可以不携带的,当密钥混合策略基站不支持,或者不需要启用的时候,则也不需要传递。此方法因为没有在每个DRB中传递安全策略,所以适用于所有DRB都使用相同的安全能力的时候使用,并且可以通过一次选择过程为所有的DRB配置目标安全策略。

[0193] 另一种可选地实施方式中,RRC重配置消息中可包括:

[0194] 重配置参数;

[0195] DRB-1(目标用户面安加密算法-1,[目标用户面完整性保护算法-1],[用户面加密密钥长度-1],[用户面完整性保护密钥长度-1],[密钥混合策略],QoS参数,其他参数);

[0196] DRB-2(目标用户面安加密算法-2,[目标用户面完整性保护算法-2],[用户面加密

密钥长度-2],[用户面完整性保护密钥长度-2],[密钥混合策略],QoS参数,其他参数),其他参数)。

[0197] 该RRC重配置消息中仅仅示意性示出了DRB-1和DRB-2两种情况,RRC重配置消息中携带的格式可类似上述示例,其中的参数项可全部携带也可部分携带,比如上述示例中用[]标出的参数可以携带也可不携带。如此,可针对每个DRB配置目标安全策略,可以做到每个DRB的目标安全策略相同,也可以做到每个DRB的目标安全策略不同。

[0198] 上面两种方法也可以结合使用,即某些目标安全策略可以所有DRB公用,某种安全策略针对DRB不同而不同,如RRC重配置消息包括:

[0199] 目标用户面安加密算法;

[0200] DRB-1(,[目标用户面完整性保护算法-1],[用户面加密密钥长度-1],[用户面完整性保护密钥长度-1],[密钥混合策略],QoS参数,其他参数);

[0201] DRB-2([目标用户面完整性保护算法-2],[用户面加密密钥长度-2],[用户面完整性保护密钥长度-2],[密钥混合策略],QoS参数,其他参数);

[0202] 其他参数等。

[0203] 可选地,在基站向终端设备发送目标用户面完整性保护算法之前,还包括:基站从SMF实体接收终端设备的当前会话的服务质量。可选地,当前会话的服务质量可以和安全策略通过一条消息发送,也可通过多条消息分别发送。可选地,基站还从AMF接收一些用于生成密钥的基本信息,比如用于生成用户面完整性保护密钥的基础密钥,用于生成用户面加密密钥的基础密钥等等。

[0204] 可选地,基站根据安全策略和服务质量中的至少一种,为终端设备分配无线数据承载(Data Radio Bearer,DRB),无线数据承载由基站分配的。基站至少根据服务质量,为传递给终端设备的数据分配无线数据承载。在5G中,一个无线数据承载中,可能有多种服务质量对应的数据流。

[0205] 可选地,一个DRB可以对应多个服务质量。根据安全策略和服务质量中的至少一种为终端设备分配目标无线数据承载。

[0206] 可选地,当所述基站上不存在历史的无线数据承载满足所述第一条件,且不存在至少一个历史的无线数据承载满足所述第二条件时,所述基站根据所述安全策略和所述服务质量中的至少一种,为所述终端设备创建所述目标无线数据承载。

[0207] 可选地,当所述基站上不存在历史的无线数据承载满足所述第一条件时,所述基站根据所述安全策略和所述服务质量中的至少一种,为所述终端设备创建所述目标无线数据承载。

[0208] 可选地,所述基站根据所述安全策略和所述服务质量中的至少一种,为所述终端设备创建所述目标无线数据承载。

[0209] 可选地,可以为终端设备选择历史的以前建立的DRB作为目标无线数据承载,也可以新建一个DRB作为目标无线数据承载。

[0210] 一种可选地实施方式中,可以直接先从历史的无线数据承载中为终端设备选择一个作为目标无线数据承载,若从历史的无线数据承载中选择不出,则为终端设备创建一个新的无线数据承载直接作为目标无线数据承载。

[0211] 或者根据一些预设的规则,先确定是否允许该终端设备使用历史的无线数据承

载，若允许，则可以先从历史的无线数据承载中为终端设备选择一个作为目标无线数据承载，若从历史的无线数据承载中选择不出，则为终端设备创建一个新的无线数据承载直接作为目标无线数据承载。为了更详细的介绍上述方案，下面通过以下几种详细的示例进行介绍。

[0212] 实施方式b1

[0213] 当基站上存在至少一个历史的无线数据承载满足第一条件时，目标无线数据承载为满足第一条件的至少一个历史的无线数据承载中的一个；其中，满足所述第一条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的服务质量与所述当前会话的所述服务质量相同，且所述安全策略与所述每个无线数据承载支持的安全策略相同。

[0214] 可选地，第一条件包括：支持的服务质量和当前会话的服务质量相同，且步骤221获取的安全策略和支持的安全策略相同。

[0215] 复用DRB的信息可以通过发送消息来实现，举个例子，比如第一次传递给终端设备：RRC重配置消息(目标用户面加密算法-1，DRB-1(QoS信息-1)，DRB-2(QoS信息-2)，其他参数))；第二次传递给终端设备：RRC重配置消息(目前用户面加密算法-1，DRB-1(QoS信息-1)，DRB-2(QoS信息-2)，DRB-3(目前用户面加密算法-2，QoS信息-2/3/4)其他参数))，则实现了修改DRB-2的安全策略，达到重用QoS的目的。通过该示例可以看到，通过发送信令实现了将历史的无线数据承载作为目标无线数据承载的目的。

[0216] 再举一个例子，用于实现复用历史的DRB的目的，第一次传递给终端设备：RRC重配置消息(目标用户面加密算法-1，DRB-1(QoS信息-1)，DRB-2(QoS信息-2)，其他参数))；第二次传递给终端设备：RRC重配置消息(目前用户面加密算法-1，DRB-1(QoS信息-1)，DRB-2(目前用户面加密算法-2，QoS信息-2)，其他参数))，则实现了修改DRB-2的安全策略，重用QoS的目的。

[0217] 实施方式b2

[0218] 当基站上不存在历史的无线数据承载满足第一条件，但存在至少一个历史的无线数据承载满足第二条件时，目标无线数据承载为根据安全策略对满足第二条件的至少一个历史的无线数据承载中的一个进行更新后的无线数据承载，其中，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的服务质量与所述当前会话的所述服务质量相同，且所述安全策略与所述每个无线数据承载支持的安全策略匹配；或者，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的服务质量与所述当前会话的所述服务质量匹配，且所述安全策略与所述每个无线数据承载支持的安全策略相同；或者，满足所述第二条件的所述至少一个历史的无线数据承载中的每个无线数据承载支持的服务质量与所述当前会话的所述服务质量匹配，且所述安全策略与所述每个无线数据承载支持的安全策略匹配。

[0219] 可选地，第二条件包括：支持的服务质量的当前会话的服务质量匹配，获取的安全策略和支持的安全策略相同。或者，可选地，第二条件包括支持的服务质量的当前会话的服务质量相同，获取的安全策略和支持的安全策略匹配。或者，可选地，第二条件包括：支持的服务质量的当前会话的服务质量匹配，获取的安全策略和支持的安全策略匹配。

[0220] 也就是说，找到历史的无线数据承载与目的无线数据承载对应的安全策略和服务质量的内容不完全相同，但是差别很小，比如带宽要求的差值在预设范围内，如此可以使用

历史的无线数据承载做最小幅度的修改。比如，满足第二条件的无线数据承载与目标无线数据承载之间的关系可以满足：满足第二条件的无线数据承载开启用户面加密保护，但没有开启用户面完整性保护；而目标无线数据承载开启用户面加密保护，且开启用户面完整性保护，且满足第二条件的无线数据承载和目标无线数据承载的目标用户面加密算法相同。在该种情况下，由于基站资源受限了，无法创建新的，或者基站的设置就是想办法重用历史的无线数据承载，则基站利用多次发送RRC重配置消息，开启完整性保护就可以了。

[0221] 本申请实施例提供一种可能的实现方式：基站在第一次传给终端设备的消息如：RRC重配置消息(目标用户面加密算法，DRB-1(QoS信息-1)，DRB-2(QoS信息-2)，其他参数))；第二次这样传递则为RRC重配置消息(目前用户面加密算法，DRB-1(QoS信息-1)，DRB-2(目标用户面完整性保护算法，QoS信息-2，QoS信息-3)，其他参数))，如此，可重用DRB-2的资源。当然具体实现有多种方式，这里只是举例。

[0222] 实施方式b3

[0223] 直接根据安全策略或服务质量中的至少一种，新建一个无线数据承载。

[0224] 实施方式b4

[0225] 基站会预先配置无线数据承载跟服务质量和安全策略这三者之间的关联关系，并且将每个关联关系设置对应的标识，比如无线接入/频率优先的用户配置文件标识(Subscriber Profile ID for RAT/Frequency Priority，SPID)。也就是说SMF不管根据session ID，IMSI，DNN，NSSAI中的任何一个或多个，也不管是否去了UDM，UPF和PCF查找，总之会得到一个SPID。那么SMF将SPID下发给RAN，RAN通过SPID就可以找到预置的QoS策略和安全策略。这个时候SMF不需要下发任何安全策略，只需要下发SPID。然后RAN就可以根据SPID确定使用的DRB，使用的DRB会满足QoS策略和安全策略。

[0226] 可选地，基站向终端设备发送目标用户面完整性保护算法，包括：基站通过无线资源控制(Radio Resource Control，RRC)信令向终端设备发送目标用户面完整性保护算法。可选地，RRC信令包括RRC重配置请求(RRC Connection reconfiguration request)。

[0227] 可选地，若安全策略中指示基站和终端设备需要协商出目标用户面加密算法，则基站还需向终端设备发送目标用户面加密算法。可选地，基站还需向终端设备发送密钥长度，若安全策略中指示基站和终端设备需要协商出目标用户面加密算法，则密钥长度可包括用户面加密密钥长度，若完整性保护指示信息指示基站对终端设备开启完整性保护时，则密钥长度可包括用户面完整性保护密钥长度。目标用户面加密算法、目标用户面加密算法、密钥长度和服务质量中的一项或任多项可通过一条信令发送给终端设备。，比如RRC重配置请求。

[0228] 可选地，当安全策略还包括D-H指示信息，且D-H指示信息用于指示基站对终端设备开启D-H时，基站向终端设备发送D-H相关密钥。下面举个例子，详细描述若D-H指示信息用于指示基站对终端设备开启D-H时，基站和终端设备之间的信令交互流程。

[0229] 如果密钥混合策略开启，则基站会根据UE上报的D-H能力和基站允许的D-H能力进行选择，选择基站允许的优先级最高的D-H能力。并且基站根据选择出来的D-H能力，生成公钥P1和私钥B1，基站将公钥p1和选择出来的D-H能力发送给终端设备，比如可通过RRC重配置消息。终端设备基于选择的D-H能力，生成公钥P2和私钥B2，并利用私钥B2和公钥P1生成密钥Kdh。然后使用Kdh与Kan进行密钥混合，混合方法可以为New-Kan＝KDF(Kdh，Kan，其他

参数)，其中，KDF(key derive function)为密钥生成函数，比如哈希256算法，其他参数可以为新鲜性参数，比如PDCP COUNT。也可以不使用其他参数，直接使用Kdh和Kan做密钥混合。密钥混合后，再根据New-Kan和目标用户面安全算法生成新用户面密钥。并使用新用户面密钥，对RRC重配置消息进行保护后发送给基站，RRC重配置消息中，含有公钥P2。基站在得到公钥P2后，根据公钥P2和私钥B1，采用与终端设备相同的方法生成New-Kan，并进一步使用与终端设备相同的方法得到新用户面密钥。并使用新用户面密钥研制RRC重配置消息。如果验证成功，则基站开始启用新用户面密钥。

[0230] 在图2a或图2b所示实施例的一种可选地实施方式中，在上述图2b的步骤213之后还包括基站接收到安全策略或安全策略的标识，则基站可以根据安全策略中提供的信息选择安全策略中的一个用户面完整性保护算法作为目标用户面完整性保护算法，其中，安全策略中可以包括一个或多个用户面完整性保护算法；或者，基站也可以不使用安全策略中的用户面完整性保护算法作为目标用户面完整性保护算法；或者，基站在安全策略中的用户面完整性保护算法不在基站允许的用户面完整性保护算法列表中的情况下，不使用安全策略中的用户面完整性保护算法作为目标用户面完整性保护算法。进一步可选地，当不使用安全策略中的用户面完整性保护算法作为目标用户面完整性保护算法的情况下，若基站开启用户面完整性保护，则可以在除安全策略中的用户面完整性保护算法之外的用户面完整性保护算法中选择一个作为目标用户面完整性保护算法，比如可以从基站允许的用户面完整性保护算法中选择一个作为目标用户面完整性保护算法；再比如，若基站中预配置安全策略，则基站在未收到其它网元下发的安全策略的情况下，基站可以根据基站中预配置的安全策略选择目标用户面完整性保护算法等，比如预配置的安全策略中可以包括一个或多个用户面完整性保护算法，基站从预配置的安全策略中选择一个作为目标用户面完整性保护算法。其它更多实施方式可参见前述内容。

[0231] 可选地，上述安全策略中的用户面完整性保护算法可以是前述内容中所述的安全策略中所包括的服务网络允许的用户面完整性保护算法，也可以是SMF实体根据服务网络允许的用户面完整性保护算法、终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法中的至少一项确定的。比如，SMF实体可以将既属于终端设备支持的用户面完整性保护算法，也属于基站允许的用户面完整性保护算法的一个算法中确定为目标用户面完整性保护算法。再比如，SMF实体可以将既属于终端设备支持的用户面完整性保护算法，也属于基站允许的用户面完整性保护算法，且还属于服务网络允许的用户面完整性保护算法的一个算法确定为目标用户面完整性保护算法。

[0232] 其中，上述安全策略中可以包括信令面完整性保护算法，也就是说，安全策略中可以包括信令面完整性保护算法和/或用户面完整性保护算法。比如，安全策略中包括的用户面完整性保护算法，也是信令面完整性保护算法，也就是说，安全策略中包括的完整性保护算法，即同时用于用户面完整性保护和信令面完整性保护。

[0233] 本领域技术人员可知，基站选择目标用户面加密算法、目标信令面完整性保护算法和目标信令面加密算法的实施方式有多种，可以参见上述选择目标用户面完整性保护算法的方案描述，下面简单列举几种实施方式。

[0234] 在图2a或图2b所示实施例的一种可选地实施方式中，在上述图2b的步骤213之后还包括基站接收到安全策略或安全策略的标识，则基站可以根据安全策略中提供的信息选

择安全策略中的一个用户面加密算法作为目标用户面加密算法，其中，安全策略中可以包括一个或多个用户面加密算法；或者，基站也可以不使用安全策略中的用户面加密算法作为目标用户面加密算法；或者，基站在安全策略中的用户面加密算法不在基站允许的用户面加密算法列表中的情况下，不使用安全策略中的用户面加密算法作为目标用户面加密算法。进一步可选地，当不使用安全策略中的用户面加密算法作为目标用户面加密算法的情况下，若基站开启用户面加密保护，则可以在除安全策略中的用户面加密算法之外的用户面加密算法中选择一个作为目标用户面加密算法，比如可以从基站允许的用户面加密算法中选择一个作为目标用户面加密算法，其它更多实施方式可参见前述内容。

[0235] 可选地，上述安全策略中的用户面加密算法可以是前述内容中所述的安全策略中所包括的服务网络允许的用户面加密算法，也可以是SMF实体根据服务网络允许的用户面加密算法、终端设备支持的用户面加密算法和基站允许的用户面加密算法中的至少一项确定的。比如，SMF实体可以将既属于终端设备支持的用户面加密算法，也属于基站允许的用户面加密算法的一个算法中确定为目标用户面加密算法。再比如，SMF实体可以将既属于终端设备支持的用户面加密算法，也属于基站允许的用户面加密算法，且还属于服务网络允许的用户面加密算法的一个算法确定为目标用户面加密算法。

[0236] 其中，上述安全策略中可以包括信令面加密算法，也就是说，安全策略中可以包括信令面加密算法和/或用户面加密算法。比如，安全策略中包括的用户面加密算法，也是信令面加密算法，也就是说，安全策略中包括的加密算法，即同时用于用户面加密保护和信令面加密保护。

[0237] 可选地，在图2a所示实施例的一种实施方式中，图2a所示的方法还包括：终端设备获取目标用户面完整性保护算法。具体可以采用如下两种方式：

[0238] 方式一、终端设备接收基站发送的目标用户面完整性保护算法。例如，图2b中步骤223基站向终端设备发送的目标用户面完整性保护算法，相应地，终端设备接收该基站发送的目标用户面完整性保护算法。

[0239] 方式二、终端设备确定目标用户面完整性保护算法。比如，终端设备沿用之前使用的目标用户面完整性保护算法；再比如，终端设备将目标信令面完整性保护算法(其中，该目标信令面完整性保护算法可以由基站发送给该终端设备)确定为目标用户面完整性保护算法。如此可提高终端设备确定目标用户面完整性保护算法的灵活性。

[0240] 此外，终端设备还可以确定目标用户面加密算法，比如，终端设备沿用之前使用的目标用户面加密算法；再比如，终端设备将目标信令面加密算法确定为目标用户面加密算法。

[0241] 在上述图2所示实施例的一种实施方式中，图2所示的方法还包括：基站确定目标用户面完整性保护算法和/或目标用户面加密算法。比如，可以将步骤202中确定的目标信令面保护算法中的目标信令面完整性保护算法也作为目标用户面完整性保护算法，可以将步骤202中确定的目标信令面保护算法中的目标信令面加密算法也作为目标用户面加密算法。

[0242] 可选地，在上述图2、图2a和图2b所示的实施例中的一种实现方式中，还包括：

[0243] 基站开启用户面完整性保护；或者，终端设备和基站开启用户面完整性保护；或者，终端设备开启用户面完整性保护。

[0244] 下面以基站为例对开启用户面完整性保护或开启用户面加密保护进行说明：

[0245] 示例性地，当满足基站开启用户面完整性保护的条件时，基站开启用户面完整性保护。

[0246] 其中，上述基站开启用户面完整性保护的条件可以是基站收到第一预设用户面消息，例如，会话建立接受消息；还可以是基站收到用户面信息，例如，会话ID或Qos Profile，其中，该用户面信息可以指预设的用户面信息，例如，预设的会话ID或预设的Qos Profile，该预设的会话ID可以指特定的会话ID；也可以是基站当前为终端设备分配用户面资源或者为终端设备重新分配用户面资源，例如，基站接收到请求为终端设备分配用户面资源的消息；若基站当前在为终端设备重新分配用户面资源，且网络运行参数满足预设网络允许条件，则可以开启用户面完整性保护；也可以是基站接收到的安全策略中包含完整性保护指示信息，且该完整性保护指示信息指示开启用户面完整性保护；也可以是预设的会话的业务类型，例如预配置的安全策略中可以包括预设的会话的业务类型与开启用户面完整性保护的关联关系，在收到预设的会话的业务类型时则可以开启用户面完整性保护。

[0247] 当满足基站开启用户面完整性保护的条件时，基站开启用户面完整性保护的几种可选地具体实施方式可以参见下述实施方式c1-a1至实施方式c1-a7。

[0248] 实施方式c1-a1

[0249] 例如，基站在在预设时间段内收到第一预设用户面消息时可以开启用户面完整性保护；第一预设用户面消息可以是会话建立接受消息。

[0250] 举个例子，如果基站在预设时间段内收到会话建立接受消息(也可以称之为会话建立完成)，则说明基站当前处于会话建立流程中，则为了提高用户面信令安全性，可以开启用户面完整性保护。

[0251] 实施方式c1-a2

[0252] 基站在在预设时间段内收到用户面信息时，可以开启用户面完整性保护，其中，用户面信息可以是会话ID或预设的Qos Profile。

[0253] 举个例子，基站若在预设时间段内收到任一会话ID或任一QoS profile(可选地，可以从N2口接收，也可以直接从终端设备侧获得)，则基站当前处于会话建立流程，则开启用户面完整性保护。可选地，还可以开启信令面保护。

[0254] 可选地，开启信令面保护可以是开启信令面完整性保护和开启信令面加密保护中的至少一项。本段说明适用于本申请所有实施例，下述内容中不再重述。

[0255] 实施方式c1-a3

[0256] 基站在预设时间段内收到预设用户面信息时，可以开启用户面完整性保护。其中，预设用户面信息可以是预设的会话ID或预设的Qos Profile。基站中预设用户面信息和是否开启用户面完整性保护的关联关系，该预设用户面信息和是否开启用户面完整性保护的关联关系可以作为基站中预配置的安全策略中的一部分。

[0257] 举个例子，设置是否开启用户面完整性保护和会话ID二者之间的关联关系，如此，基站在预设时间段内若接收到预设的会话ID，则开启用户面完整性保护。其中，预设的会话ID在是否开启用户面完整性保护和会话ID二者之间的关联关系中所对应的是开启用户面完整性保护。

[0258] 再举个例子，设置是否开启用户面完整性保护和Qos Profile二者之间的关联关

系，如此，基站在预设时间段内若接收到预设的Qos Profile，则开启用户面完整性保护。其中，预设的会话ID在是否开启用户面完整性保护和会话ID二者之间的关联关系中所对应的是开启用户面完整性保护。

[0259] 进一步，是否开启用户面完整性保护和会话ID二者之间的关联关系可以是预设在基站中的，也可以有基站接收到的其它网元发送的更新后的关联关系。可选的，基站可以根据预设的关联关系和更新后的关联关系，决定是否开启用户完整性保护。比如，在首次开启用户面完整性保护的时候，可以依据预设的关联关系决定是否开启用户完整性保护；当后续有更新的关联关系时，也可以仅依据最新的关联关系确定是否开启用户面完整性保护。还可以结合具体的预设的关联关系、更新的关联关系和网络负荷情况进行综合判定，比如，如基站因为过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面完整性保护。

[0260] 实施方式c1-a4

[0261] 若基站当前在为终端设备分配用户面资源或者为终端设备重新分配用户面资源，则可以开启用户面完整性保护。例如，基站在预设时间段内接收到请求为终端设备分配用户面资源的消息，则基站为终端设备分配用户面资源或为终端设备重新分配用户面资源，该流程中涉及到用户面信令，为了提高用户面信令的安全性，则可以开启用户面完整性保护。

[0262] 实施方式c1-a5

[0263] 若基站当前在为终端设备重新分配用户面资源，且网络运行参数满足预设网络允许条件，则可以开启用户面完整性保护；其中，网络运行参数包括网络负荷量和/或丢包率。

[0264] 需要指出的是，在基站重新为一个会话分配资源的过程中，可以采用如下两种可选的实施方式：

[0265] 方式一，沿用终端设备的该会话之前所分配的资源对应的用户面安全方案，比如终端设备的会话之前所分配的资源对应的是开启用户面完整性保护，则终端设备的该会话对应的重新分配的资源对应的也是开启用户面完整性保护。

[0266] 方式二，根据基站的状态重新确定该会话对应的重新分配的资源对应的用户面安全方案。比如，基站的状态显示某个会话丢包率过高，因为用户面完整性保护是附升高丢包率的，因此在为这个会话重新分配资源的过程中，关掉用户面完整性保护。再比如，如基站因为过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面完整性保护。

[0267] 显然上述两种可选地实施方式可以结合，比如，如果基站重新为一个会话分配资源，那么若基站的状态正常，则维持开启用户面完整性保护；或者，若基站的状态异常，如基站因为过载再为这个会话重新分配资源，那么如果这个会话原来开启了用户面完整性保护，则关掉用户面完整性保护，再比如某个会话丢包率过高，因此为这个会话重新分配资源，因为用户面完整性保护是附升高丢包率的，因此关掉用户面完整性保护。可选的，这种情况可作为安全策略的一部分预配置在基站内(预配置在基站内的安全策略也可如上述内容所述为预配置在基站内的安全策略)。

[0268] 实施方式c1-a6

[0269] 若基站接收到的安全策略中包括完整性保护指示信息，且该完整性保护指示信息

指示开启用户面完整性保护，则基站可以开启用户面完整性保护。可选地，完整性保护指示信息可以是完整性保护算法的标识、比特位指示信息、也可以是预设的信息。该完整性保护指示信息可以是比如SMF实体发送的。SMF实体在确定满足SMF实体用户面完整性保护条件时发送指示开启用户面完整性保护的完整性保护指示信息，其中，SMF实体在确定满足SMF实体用户面完整性保护条件的方式有多种实施方式，也可以参见实施方式c1-a1至实施方式c1-a5中所描述的基站的实施方式。

[0270] 实施方式c1-a7

[0271] 基站中可以预配置安全策略，预配置的安全策略中可以包括预设的会话的业务类型与开启用户面完整性保护的关联关系。基站开启用户面完整性保护的条件可以是基站预配置的安全策略中包含的预设的会话的业务类型。例如预配置的安全策略中可以包括预设的会话的业务类型与开启用户面完整性保护的关联关系，在收到预设的会话的业务类型时则可以开启用户面完整性保护。可选地，若基站没有收到网元发送的安全策略，那么可以使用基站中预配置的安全策略。

[0272] 举个例子，基站中预配置的安全策略可以是以用户面数据(比如业务类型)为维度去规定的，比如基站中预配置的安全策略中规定:VoIP业务对应的流程不开启用户面完整性保护，则基站在判断当前会话对应VoIP业务时，不开启用户面完整性保护。

[0273] 进一步，安全策略可以是预设预配置在基站中的，也可以有基站接收到的其它网元发送的更新后的安全策略。可选的，基站可以根据预配置的安全策略和更新后的安全策略，决定是否开启用户完整性保护。比如，在首次开启用户面完整性保护的时候，可以依据预配置的安全策略决定是否开启用户完整性保护;当后续有更新的安全策略时，也可以仅依据最新的安全策略确定是否开启用户面完整性保护。还可以结合具体的预配置的安全策略、更新的安全策略和网络负荷情况进行综合判定，比如，如基站因为过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面完整性保护。

[0274] 进一步可选地，上述方法还包括:基站向终端设备发送完整性保护指示信息，该加密指示信息用于指示开启用户面完整性保护。其中，该完整性指示信息可以是基站接收的安全策略中包含的完整性保护指示信息。

[0275] 可选地，在上述图2、图2a和图2b所示的实施例中的另一种实现方式中，还包括:

[0276] 基站开启用户面加密保护;或者，终端设备和基站开启用户面加密保护;或者，终端设备开启用户面加密保护。

[0277] 示例性地，当满足基站开启用户面加密保护的条件时，基站开启用户面加密保护。

[0278] 其中，上述基站开启用户面加密保护的条件可以是基站收到第一预设用户面消息，例如，会话建立接受消息;还可以是基站收到用户面信息，例如，会话ID或Qos Profile，其中，该用户面信息可以指预设的用户面信息，例如，预设的会话ID或预设的Qos Profile，该预设的会话ID可以指特定的会话ID;也可以是基站当前为终端设备分配用户面资源或者为终端设备重新分配用户面资源，例如，基站接收到请求为终端设备分配用户面资源的消息;也可以是基站接收到的安全策略中包含加密指示信息，且该加密指示信息指示开启用户面加密保护;也可以是预设的会话的业务类型，例如预配置的安全策略中可以包括预设的会话的业务类型与开启用户面加密保护的关联关系，在收到预设的会话的业务类型时则

可以开启用户面加密保护;也可以是开启信令面保护时则可以开启用户面加密保护。

[0279] 进一步可选地,上述方法还包括:基站向终端设备发送加密指示信息,该加密指示信息用于指示开启用户面加密保护。其中,该加密指示信息可以是基站接收的安全策略中包含的加密指示信息。

[0280] 基站开启用户面加密保护的条件时,基站开启用户面加密保护的几种可选地具体实施方式可以参见下述实施方式c1-b1至实施方式c1-b8。

[0281] 实施方式c1-b1

[0282] 例如,基站在在预设时间段内收到第一预设用户面消息时可以开启用户面加密保护;第一预设用户面消息可以是会话建立接受消息。

[0283] 举个例子,如果基站在预设时间段内收到会话建立接受消息(也可以称之为会话建立完成),则说明基站当前处于会话建立流程中,则为了提高用户面信令安全性,可以开启用户面加密保护。

[0284] 实施方式c1-b2

[0285] 基站在在预设时间段内收到用户面信息时,可以开启用户面加密保护,其中,用户面信息可以是会话ID或预设的Qos Profile。

[0286] 举个例子,基站若在预设时间段内收到任一会话ID或任一QoS profile(可选地,可以从N2口接收,也可以直接从终端设备侧获得),则基站当前处于会话建立流程,则开启用户面加密保护。可选地,还可以开启信令面保护。

[0287] 可选地,开启信令面保护可以是开启信令面加密保护和开启信令面加密保护中的至少一项。本段说明适用于本申请所有实施例,下述内容中不再重述。

[0288] 实施方式c1-b3

[0289] 基站在预设时间段内收到预设用户面信息时,可以开启用户面加密保护。其中,预设用户面信息可以是预设的会话ID或预设的Qos Profile。基站中预设用户面信息和是否开启用户面加密保护的关联关系,该预设用户面信息和是否开启用户面加密保护的关联关系可以作为基站中预配置的安全策略中的一部分。

[0290] 举个例子,设置是否开启用户面加密保护和会话ID二者之间的关联关系,如此,基站在预设时间段内若接收到预设的会话ID,则开启用户面加密保护。其中,预设的会话ID在是否开启用户面加密保护和会话ID二者之间的关联关系中所对应的是开启用户面加密保护。

[0291] 再举个例子,设置是否开启用户面加密保护和Qos Profile二者之间的关联关系,如此,基站在预设时间段内若接收到预设的Qos Profile,则开启用户面加密保护。其中,预设的会话ID在是否开启用户面加密保护和会话ID二者之间的关联关系中所对应的是开启用户面加密保护。

[0292] 进一步,是否开启用户面加密保护和会话ID二者之间的关联关系可以是预设在基站中的,也可以有基站接收到的其它网元发送的更新后的关联关系。可选的,基站可以根据预设的关联关系和更新后的关联关系,决定是否开启用户加密保护。比如,在首次开启用户面加密保护的时候,可以依据预设的关联关系决定是否开启用户加密保护;当后续有更新的关联关系时,也可以仅依据最新的关联关系确定是否开启用户面加密保护。还可以结合具体的预设的关联关系、更新的关联关系和网络负荷情况进行综合判定,比如,如基站因为

过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面加密保护。

[0293] 实施方式c1-b4

[0294] 若基站当前在为终端设备分配用户面资源或者为终端设备重新分配用户面资源，则可以开启用户面加密保护。例如，基站在预设时间段内接收到请求为终端设备分配用户面资源的消息，则基站为终端设备分配用户面资源或为终端设备重新分配用户面资源，该流程中涉及到用户面信令，为了提高用户面信令的安全性，则可以开启用户面加密保护。

[0295] 实施方式c1-b5

[0296] 若基站当前在为终端设备重新分配用户面资源，且网络运行参数满足预设网络允许条件，则可以开启用户面加密保护；其中，网络运行参数包括网络负荷量和/或丢包率。

[0297] 需要指出的是，在基站重新为一个会话分配资源的过程中，可以采用如下两种可选的实施方式：

[0298] 方式一，沿用终端设备的该会话之前所分配的资源对应的用户面安全方案，比如终端设备的会话之前所分配的资源对应的是开启用户面加密保护，则终端设备的该会话对应的重新分配的资源对应的也是开启用户面加密保护。

[0299] 方式二，根据基站的状态重新确定该会话对应的重新分配的资源对应的用户面安全方案。比如，基站的状态显示某个会话丢包率过高，因为用户面加密保护是附升高丢包率的，因此在为这个会话重新分配资源的过程中，关掉用户面加密保护。再比如，如基站因为过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面加密保护。

[0300] 显然上述两种可选地实施方式可以结合，比如，如果基站重新为一个会话分配资源，那么若基站的状态正常，则维持开启用户面加密保护；或者，若基站的状态异常，如基站因为过载再为这个会话重新分配资源，那么如果这个会话原来开启了用户面加密保护，则关掉用户面加密保护，再比如某个会话丢包率过高，因此为这个会话重新分配资源，因为用户面加密保护是附升高丢包率的，因此关掉用户面加密保护。可选的，这种情况可作为安全策略的一部分预配置在基站内(预配置在基站内的安全策略也可如上述内容所述为预配置在基站内的安全策略)。

[0301] 实施方式c1-b6

[0302] 若基站接收到的安全策略中包括加密保护指示信息，且该加密保护指示信息指示开启用户面加密保护，则基站可以开启用户面加密保护。可选地，加密保护指示信息可以是加密算法的标识、比特位指示信息、也可以是预设的信息。该加密保护指示信息可以是比如SMF实体发送的。SMF实体在确定满足SMF实体用户面加密保护条件时发送指示开启用户面加密保护的加密保护指示信息，其中，SMF实体在确定满足SMF实体用户面加密保护条件的方式有多种实施方式，也可以参见实施方式c1-b1至实施方式c1-b5中所描述的基站的实施方式。

[0303] 实施方式c1-b7

[0304] 基站中可以预配置安全策略，预配置的安全策略中可以包括预设的会话的业务类型与开启用户面加密保护的关联关系。基站开启用户面加密保护的条件可以是基站预配置的安全策略中包含的预设的会话的业务类型。例如预配置的安全策略中可以包括预设的会

话的业务类型与开启用户面加密保护的关联关系，在收到预设的会话的业务类型时则可以开启用户面加密保护。可选地，若基站没有收到网元发送的安全策略，那么可以使用基站中预配置的安全策略。

[0305] 举个例子，基站中预配置的安全策略可以是以用户面数据(比如业务类型)为维度去规定的，比如基站中预配置的安全策略中规定：VoIP业务对应的流程不开启用户面加密保护，则基站在判断当前会话对应VoIP业务时，不开启用户面加密保护。

[0306] 进一步，安全策略可以是预设预配置在基站中的，也可以有基站接收到的其它网元发送的更新后的安全策略。可选的，基站可以根据预配置的安全策略和更新后的安全策略，决定是否开启用户加密保护。比如，在首次开启用户面加密保护的时候，可以依据预配置的安全策略决定是否开启用户加密保护；当后续有更新的安全策略时，也可以仅依据最新的安全策略确定是否开启用户面加密保护。还可以结合具体的预配置的安全策略、更新的安全策略和网络负荷情况进行综合判定，比如，如基站因为过载再为会话重新分配资源，那么在重新为该会话分配资源的过程中，关闭该会话原来开启的用户面加密保护。

[0307] 实施方式c1-b8

[0308] 基站在开启信令面保护(开启信令面完整性保护和/或信令面加密保护)时可以也开启用户面加密保护。比如在上述图2所示的实施方式中，在步骤202之后还包括一种可选地实施方式，基站在开启信令面保护时，也开启用户面加密保护。

[0309] 在这种实施方式下，若终端设备和基站开启了信令面保护，但是未开启用户面完整性保护且未开启用户面加密保护，在开启用户面完整性保护且开启用户面加密保护时，可以继续维持开启信令面保护的状态，这种实施方式下，基站可以向终端设备发送完整性保护指示信息和加密指示信息，如此，终端设备一方面可以维持当前信令面保护的开启状态(比如若终端设备之前开启了信令面完整性保护未开启信令面加密保护，则继续维持信令面完整性保护且不开启信令面加密保护的状态)，另一方面根据用于完整保护指示信息开启用户面完整性保护，且根据加密指示信息开启用户面加密保护。

[0310] 另一种可选地实施方案中，若终端设备和基站开启了信令面保护，且已经开启用户面加密保护，但是未开启用户面完整性保护，在开启用户面完整性保护时，基站可以只向终端设备发送用于开启用户面完整性保护的完整性保护指示信息，终端设备一方面可以维持当前信令面保护的开启状态(比如若终端设备之前开启了信令面完整性保护未开启信令面加密保护，则继续维持信令面完整性保护且不开启信令面加密保护的状态)，另一方面根据完整保护指示信息开启用户面完整性保护，加密保护持续开启。另一种可选地实施方式中，可以再次传输加密指示信息，用于指示用户面加密保护持续开启。

[0311] 下面以终端设备为例对开启用户面完整性保护或开启用户面完整性保护进行说明：

[0312] 当满足终端设备开启用户面完整性保护的条件时，终端设备开启用户面完整性保护。

[0313] 其中，终端设备开启用户面完整性保护的条件可以终端设备接收基站发送的完整性保护指示信息，且该完整性保护指示信息指示开启用户面完整性保护；还可以是终端设备发送第二预设用户面消息，例如，会话建立请求消息。

[0314] 当满足终端设备开启用户面完整性保护的条件时，终端设备开启用户面完整性保

护的几种可选地具体实施方式可以参见下述实施方式c1-c1至实施方式c1-c2。

[0315] 实施方式c1-c1

[0316] 在上述图2a和图2b所示的实施例中的一种可选地实施方式中，在步骤211之后还包括：基站向终端设备发送完整性保护指示信息，该完整性保护指示信息用于指示是否开启用户面完整性保护。其中，该完整性保护指示信息可以是基站在上述图2b的布置221中获取的安全策略中包含的完整性保护指示信息，也可以是基站在通过上述实施方式c1-a1至c1-a7中的任一种实施方式确定的。

[0317] 终端设备在接收到完整性保护指示信息，且该完整性保护指示信息指示开启用户面完整性保护，则终端设备可以开启用户面完整性保护。

[0318] 实施方式c1-c2

[0319] 举个例子，终端设备在预设时间段内发送了会话建立请求消息，终端设备当前则处于会话建立流程中，在这种情况下，为了提高用户面安全性，终端设备可以开启用户面完整性保护。

[0320] 进一步可选地，若终端设备采用实施方式c1-c2，且终端设备还收到了完整性保护指示信息，若二者出现矛盾，则终端设备以收到的完整性保护指示信息为依据去确定是否开启用户面完整性保护。

[0321] 在上述图2a和图2b所示的实施例中的一种可选地实施方式中，在步骤211之后还包括：基站向终端设备发送加密指示信息，该加密指示信息用于指示是否开启用户面加密保护。其中，该加密指示信息可以是基站在上述图2b的布置221中获取的安全策略中包含的加密指示信息，也可以是基站在通过上述实施方式c1-a1至c1-a7中的任一种实施方式确定的。

[0322] 例如，终端设备在接收到加密指示信息，且该加密指示信息指示开启用户面加密保护，则终端设备可以开启用户面加密保护。

[0323] 例如，终端设备在预设时间段内发送第二预设用户面消息，则可以开启用户面加密保护。举个例子，终端设备在预设时间段内发送了会话建立请求消息，终端设备当前则处于会话建立流程中，在这种情况下，为了提高用户面安全性，终端设备可以开启用户面加密保护。

[0324] 进一步可选地，若终端设备采用实施方式c1-c2，且终端设备还收到了加密指示信息，若二者出现矛盾，则终端设备以收到的加密指示信息为依据去确定是否开启用户面加密保护。

[0325] 再例如，终端设备在开启信令面保护(开启信令面加密保护和/或信令面加密保护)时可以也开启用户面加密保护。比如在上述图2所示的实施方式中，在步骤203和步骤204之间，还包括基站在开启信令面保护时，也可以开启用户面加密保护。

[0326] 终端设备可以根据预设时间段内是否发送第二预设用户面消息判断是否开启信令面保护(信令面完整性保护和/或信令面加密保护)。第二预设信令面消息可以包括注册请求或服务请求。具体来说，当前所处的流程确定终端设备当前发起的是注册请求(或服务请求)，则确定当前所处的流程为注册流程(或服务流程)，由于该流程中还未收到用户面资源分配信息，终端设备可以开启信令面保护。

[0327] 进一步可选地，终端设备可以根据接收到的信令面完整性保护指示信息确定是否

开启信令面的完整性保护，可以根据接收到的信令面加密指示信息确定是否开启信令面的加密保护。其中，终端设备接收到的信令面完整性保护指示信息和信令面加密指示信息中的至少一项也可以是由其它网元发送给基站，并由基站转发给终端设备的。其它网元比如可以是SMF实体等。

[0328] 可选地，在上述图2、图2a和图2b所示的实施例中的一种实现方式中，还包括：

[0329] 基站不开启用户面完整性保护；或者，终端设备和基站不开启用户面完整性保护。

[0330] 下面以基站不开启用户面完整性保护为例进行说明：

[0331] 当满足基站不开启用户面完整性保护的条件时，基站不开启用户面完整性保护。

[0332] 其中，上述基站不开启用户面完整性保护的条件可以是基站接收到第一预设的信令面消息，例如，注册请求完整消息或服务请求完成消息；还可以基站在预设时间段内未收到用户面信息或预设的用户面信息，例如，会话ID，QoS profile，或者，预设的会话ID，预设的QoS profile；也可以是基站在预设时间段内未收到为终端设备分配用户面资源或为终端设备重新分配用户面资源的请求消息，例如，资源分配请求消息；也可以是基站接收的安全策略包含的完整性保护指示信息指示不开启用户面完整性保护；也可以是会话的业务类型不是预设的会话的业务类型，例如预配置的安全策略中可以包括预设的话的业务类型与开启用户面完整性保护的关联关系，在未收到预设的会话的业务类型时则可以不开启用户面完整性保护。

[0333] 例如，当预设的默认条件指示基站是永久不开启时，不生成用户面完整性保护密钥。

[0334] 可选地，在上述图2、图2a和图2b所示的实施例中的一种实现方式中，还包括：

[0335] 基站不开启用户面加密保护；或者，终端设备和基站不开启用户面加密保护。

[0336] 下面以基站不开启用户面加密保护为例进行说明：

[0337] 当满足基站不开启用户面加密保护的条件时，基站不开启用户面加密保护。

[0338] 其中，上述基站不开启用户面加密保护的条件可以是基站接收到第一预设的信令面消息，例如，注册请求完整消息或服务请求完成消息；还可以基站在预设时间段内未收到用户面信息或预设的用户面信息，例如，会话ID，QoS profile，或者，预设的会话ID，预设的QoS profile；也可以是基站在预设时间段内未收到为终端设备分配用户面资源或为终端设备重新分配用户面资源的请求消息，例如，资源分配请求消息；也可以是基站接收的安全策略包含的完整性保护指示信息指示不开启用户面加密保护；也可以是会话的业务类型不是预设的会话的业务类型，例如预配置的安全策略中可以包括预设的话的业务类型与开启用户面加密保护的关联关系。

[0339] 例如，当预设的默认条件指示基站是永久不开启时，不生成用户面加密密钥。

[0340] 下面以终端设备不开启用户面完整性保护为例进行说明：

[0341] 当满足终端设备不开启用户面完整性保护的条件时，终端设备不开启用户面完整性保护。

[0342] 其中，上述终端设备不开启用户面完整性保护的条件可以是在预设时间段内终端设备未发送第二预设用户面消息，例如，会话建立请求消息；还可以是终端设备接收基站发送的完整性保护指示信息，且该完整性保护指示信息指示开启用户面完整性保护；还可以是终端设备在预设时间段内接收到第一预设的信令面消息，例如，注册请求完整消息或服

务请求完成消息。

[0343] 例如，当预设的默认条件指示终端设备是永久不开启时，不生成用户面完整性保护密钥。

[0344] 例如，当预设的默认条件指示基站是永久不开启时，不生成用户面加密密钥。

[0345] 下面以终端设备不开启用户面加密保护为例进行说明：

[0346] 当满足终端设备不开启用户面加密保护的条件时，终端设备不开启用户面加密保护。

[0347] 其中，上述终端设备不开启用户面加密保护的条件可以是在预设时间段内终端设备未发送第二预设用户面消息，例如，会话建立请求消息；还可以是终端设备接收基站发送的加密保护指示信息，且该加密保护指示信息指示不开启用户面加密保护。

[0348] 例如，当预设的默认条件指示终端设备是永久不开启时，不生成用户面加密密钥。

[0349] 其中，终端设备或基站不开启用户面的完整性保护有多种实施方式，如下：

[0350] 不开启用户面的完整性保护方式一，终端设备或基站不开启用户面完整性保护可以为：生成用户面完整性保护密钥，但是不使用用户面完整性保护密钥进行用户面完整性保护。也就是说，在不开启用户面完整性保护时可以先生成用户面完整性保护密钥，但是不使用用户面完整性保护密钥，然后在开启用户面完整性保护的情况下，使用用户面完整性保护密钥进行用户面完整性保护。

[0351] 在上述不开启用户面的完整性保护方式一中，在终端设备生成用户面完整性保护密钥之前获取用户面完整性保护算法，比如可以将信令面完整性保护算法作为用户面完整性保护算法。

[0352] 不开启用户面的完整性保护方式二，终端设备或基站不开启用户面完整性保护可以为：生成用户面完整性保护密钥，并使用用户面完整性保护密钥进行用户面完整性保护。也就是说，在无法确定是否开启用户面完整性保护或者确定不开启用户面完整性保护时，可以不生成用户面完整性保护密钥，在开启用户面完整性保护时再生成用户面完整性密钥。

[0353] 相对应的，比如针对终端设备和基站，若确定终端设备和基站始终不开启用户面完整性保护(比如可以是预设的条件等等)，则可以不生成用户面完整性保护密钥。

[0354] 其中，基站和终端设备不开启用户面的完整性保护的实施方式可以相同，也可以不同，比如都使用不开启用户面的完整性保护方式一，或者终端设备使用不开启用户面的完整性保护方式一，基站使用不开启用户面的完整性保护方式二。

[0355] 终端设备或基站不开启用户面的加密保护有多种实施方式，如下：

[0356] 不开启用户面的加密保护方式一，终端设备或基站不开启用户面加密保护包括：生成用户面加密保护密钥，但是不使用用户面加密保护密钥进行用户面加密保护。也就是说，在不开启用户面加密保护时可以先生成用户面加密保护密钥，但是不使用，在开启用户面加密保护的情况下，使用用户面加密保护密钥进行用户面加密保护。

[0357] 在不开启用户面的加密保护方式一种，在终端设备生成用户面加密保护密钥之前获取用户面加密算法，比如可以将信令面加密算法作为用户面加密算法。

[0358] 不开启用户面的加密保护方式二，终端设备或基站不开启用户面加密保护包括：在开启用户面加密保护时生成用户面加密保护密钥，并使用用户面加密保护密钥进行用户

面加密保护。也就是说，在无法确定是否开启用户面加密保护或者确定不开启用户面加密保护时，可以不生成用户面加密保护密钥，在开启用户面加密保护时再生成用户面完整性密钥。

[0359] 相对应的，比如针对终端设备和基站，若确定终端设备和基站始终不开启用户面加密保护(比如可以是预设的条件等等)，则可以不生成用户面加密保护密钥。

[0360] 其中，基站和终端设备不开启用户面的加密保护的实施方式可以相同，也可以不同，比如都使用不开启用户面的加密保护方式一，或者终端设备使用不开启用户面的加密保护方式一，基站使用不开启用户面的加密保护方式二。

[0361] 此外，基站和终端设备开启用户面加密保护有多种实施方式，比如可以根据预设的规定确定是否开启用户面加密保护，预设的规定可以是终端设备在接收到AS安全模式命令后开启用户面加密保护，也就是说满足基站用户面加密保护条件包括接收到AS安全模式命令。基于该示例，举个例子，比如满足终端设备用户面完整性保护条件包括终端设备接收到指示开启用户面完整性保护的完整性保护指示信息，也就是说，终端设备在接收到AS安全模式命令后开启用户面加密保护，而用户面完整性保护是否开启需要基站通过发送完整性保护指示信息通知终端设备，这种情况下终端设备在没有收到完整性保护指示信息的情况下，不开启用户面完整性保护。进一步，当终端设备接收到指示开启用户面完整性保护的完整性保护指示信息的情况下，开启用户面完整性保护。换言之，终端设备在一个时间段内不开启用户面完整性保护，但是在另一个时间段内有可能开启用户面完整性保护，也就是说终端设备不开启用户面完整性保护是暂时的，这与终端设备始终不开启用户面完整性保护有区别。基站和终端设备还可以根据预设的规定确定是否开启信令面保护(包括信令面完整性保护和/或信令面加密保护)，预设的规定可以是终端设备在接收到AS安全模式命令后开启信令面保护。

[0362] 再比如，终端设备或基站在开启信令面保护(开启信令面完整性保护和/或信令面加密保护)时，开启用户面加密保护。也就是说，满足基站用户面加密保护条件包括开启信令面保护。换言之，用户面加密保护可以和信令面保护一起开启，而开启或不开启用户面完整性保护可以根据是否满足基站用户面完整性保护条件来确定。比如，在基站收到注册接受或服务请求接受后可以开启信令面保护(开启信令面完整性保护和/或信令面加密保护)且开启用户面加密保护，不开启用户面完整性保护。进一步，在这种实施方式中，也可以不设置上述加密指示信息。

[0363] 举个例子，上述图2中的步骤203之后，即终端设备在基站向终端设备发送AS安全模式命令之后，终端设备开启信令面保护不开启用户面保护，可以生成信令面密钥(信令面完整性保护密钥和/或信令面加密保护密钥)、用户面密钥(用户面完整性保护密钥和/或用户面加密保护密钥)。但是仅使用信令面密钥进行保护，可以保存用户面密钥。在开启用户面保护的情况下再使用用户面密钥。

[0364] 再比如，上述图2中的步骤203之后，即终端设备在基站向终端设备发送AS安全模式命令之后，终端设备开启信令面保护、开启用户面加密保护且不开启用户面完整性保护，可以生成信令面密钥(信令面完整性保护密钥和/或信令面加密保护密钥)、用户面加密密钥和用户面完整性保护密钥。但是仅使用信令面密钥进行保护，使用用户面加密密钥进行保护，可以保存用户面完整性保护密钥。在开启用户面完整性保护的情况下再使用用户面

完整性保护密钥进行完整性保护。

[0365] 再比如，上述图2中的步骤203之后，即终端设备在基站向终端设备发送AS安全模式命令之后，终端设备开启信令面保护不开启用户面保护，可以生成信令面密钥(信令面完整性保护密钥和/或信令面加密保护密钥)且使用信令面密钥进行保护，不生成用户面密钥(用户面完整性保护密钥和/或用户面加密保护密钥)。再比如，上述图2b中的步骤211中的请求消息是会话建立请求时，在步骤211之后，基站再向终端设备发送AS安全模式命令或RRC重配置消息，终端设备在接收到AS安全模式命令或RRC重配置消息后使用用户面密钥进行用户面安全保护。

[0366] 再比如，上述图2中的步骤203之后，即终端设备在基站向终端设备发送AS安全模式命令之后，终端设备开启信令面保护、开启用户面加密保护，且不开启用户面完整性保护，可以生成信令面密钥(信令面完整性保护密钥和/或信令面加密保护密钥)且使用信令面密钥进行保护，生成用户面加密密钥，且使用用户面加密密钥进行保护，但不生成用户面完整性保护密钥。再比如，上述图2b中的步骤211中的请求消息是会话建立请求时，在步骤211之后，基站再向终端设备发送AS安全模式命令或RRC重配置消息，终端设备在接收到AS安全模式命令或RRC重配置消息后，生成用户面完整性保护密钥，且使用用户面完整性保护密钥进行用户面安全保护。

[0367] 终端设备可以根据接收到的基站发送的完整性保护指示信息确定是否开启用户面的完整性保护，终端设备也可以判断后开启用户面完整性保护或不开启用户面完整性保护，下面通过实施方式c1和实施方式c2进行介绍。进一步，可选地，为了节省资源，若终端设备确定不开启用户面的完整性保护，则可以不发送用户面的完整性保护算法，也就是说，在这种可选地实施方式中，不能发送空的用户面完整性保护算法，但是若终端设备不开启用户面的加密保护，则发送空的用户面加密算法。

[0368] 需要说明的是，上述各实施例及其各种可选的实施方式中，基站向终端设备发送的完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项可以承载在预设消息中，比如在预设消息中预定义一个字段，在该预定义字段承载完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项。预设消息可以是AS安全模式命令或者RRC重配置请求。例如，采用用下述实施方式c1-1(b7)的方式所示的算法的标识的形式向终端设备发送完整性保护指示信息。

[0369] 需要说明的是，上述各实施例及其各种可选的实施方式中，基站接收的完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项可以携带在安全策略中，具体可以采用c1-1(b2)-c1-1(b7)。

[0370] 下面介绍了完整性保护指示信息和/或加密指示信息的各种表现方式。

[0371] 实施方式c1-1(b1)

[0372] 完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项可以通过在预定义字段设置会话ID来表示。比如当基站没有收到会话ID的时候，将发送给终端设备的预设消息中的预定义字段中的会话ID设置为0，则表示只开启信令面保护，不开启用户面完整性保护指示信息，不开启用户面加密指示信息。终端设备接收到的预设消息中的预定义字段中的会话ID为0的信息时，可以确定只开启信令面保

护(开启信令面完整性保护和/或开启信令面加密保护),不开启用户面完整性保护指示信息,不开启用户面加密指示信息。

[0373] 进一步,开启信令面保护可以是开启信令面完整性保护和开启信令面加密保护中的至少一种,具体开启信令面完整性保护,还是开启信令面加密保护,还是开启信令面完整性保护和信令面加密保护,可以根据预设的规则等确定,比如预设规则中默认开启信令面完整性保护和信令面加密保护。下述内容中与此段解释类似,下面不再重复。

[0374] 再比如,基站在收到会话ID的情况下,比如可以将发送给终端设备的预设消息中的预定义字段中的会话ID设置为当前的会话ID。若终端设备接收到的基站发送的预设消息,预设消息中的预定义字段中包括会话ID,且会话ID为当前会话的ID,则终端设备会默认开启用户面加密保护和用户面完整性保护。可选地,可以将基站选择的信令面的加密算法也用于用户面,也就是基站选择出来的加密算法即为信令面加密算法也为用户面加密算法,类似地,将选择的信令面完整性保护算法作为用户面完整性保护算法。进一步,若终端设备接收到的基站发送的预设消息,预设消息中的预定义字段中包括会话ID,且会话ID不为空的情况下,终端设备可以开启用户面完整性保护和/或用户面加密保护,具体开启用户面加密保护还是开启用户面完整性保护,还是开启用户面加密保护和用户面完整性保护,可以参考预设规则,也可以根据本申请其它实施例中的描述。

[0375] 另一种可选地实施方式中,完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项可以通过在预设消息中的预定义字段中设置QoS的相关信息来指示,比如设置QFI值。QFI值的使用方式可以与上述会话ID的使用方式相类似,比如当基站没有收到QFI的时候,将发送给终端设备的预设消息中的预定义字段中的QFI设置为0,则表示只开启信令面保护,不开启用户面完整性保护指示信息,不开启用户面加密指示信息。终端设备在接收到预定义字段中的QFI为0的信息时,可以确定只开启信令面保护,不开启用户面完整性保护指示信息,不开启用户面加密指示信息。

[0376] 实施方式c1-1(b2)

[0377] 完整性保护指示信息和/或加密指示信息可以通过在预设消息或安全策略中的预定义字段中的比特信息来表示,比如预定义字段中可以包括1个比特信息。

[0378] 例如,在默认情况下,开启用户面加密保护且不开启用户面完整性保护,则预定义字段中的1个比特信息就是完整性保护指示信息,该预定义字段中比特位置1,可以表示开启用户面完整性保护;该预定义字段中比特位置0,可以表示不开启用户面完整性保护。

[0379] 再比如,在默认情况下,不开启用户面加密保护且开启用户面完整性保护,则预定义字段中的1个比特信息就是加密指示信息,具体地,该预定义字段中的比特位置1,可以表示开启用户面加密保护,该预定义字段中的比特位置0,可以表示不开启用户面加密保护。

[0380] 再比如,在默认情况下,开启用户面加密保护且开启用户面完整性保护,则预定义字段中的1个比特信息就是完整性保护指示信息和加密指示信息。该预定义字段中的比特位置1可以表示开启用户面完整性保护且开启用户面加密保护,预定义字段中的比特位置0可以表示不开启用户面完整性保护且不开启用户面加密保护。

[0381] 实施方式c1-1(b3)

[0382] 完整性保护指示信息和加密指示信息可以通过在预设消息中或安全策略的预定义字段中的比特信息来表示,比如预定义字段中可以包括2个比特信息,其中一个比特信息

代表用户面加密是否需要开启或关闭，另一比特信息代表用户面完整性保护是否需要开启或关闭，即其中一个比特信息是加密指示信息，另一个比特信息是完整性保护指示信息，比如，将预定义字段中加密指示信息对应的比特信息置1表示开启用户面加密保护；将预定义字段中完整性保护指示信息对应的比特信息置1表示终端设备开启用户面完整性保护；将预定义字段中加密指示信息对应的比特信息置0表示不开启用户面加密保护；将预定义字段中完整性保护指示信息对应的比特信息置0表示终端设备不开启用户面完整性保护。

[0383] 实施方式c1-1(b4)

[0384] 完整性保护指示信息和加密指示信息可以通过在预设消息或安全策略中的预定义字段中的比特信息来表示，比如预定义字段中可以包括4个比特信息，其中，预定义字段中一个比特信息指示用户面加密保护是否开启，比如，该比特信息置1，表示开启用户面加密保护，置0表示不开启用户面加密保护；预定义字段中一个比特信息指示用户面加密保护的秘钥长度是128比特还是256比特，比如，该比特信息置1，表示用户面加密保护的秘钥长度是128比特，置0表示用户面加密保护的秘钥长度是256比特；预定义字段中一个比特信息指示用户面完整性保护的秘钥长度是128比特还是256比特，该比特信息置1，表示用户面完整性保护的秘钥长度是128比特，即生成32bit的MAC值，置0表示用户面完整性保护的秘钥长度是256比特，即生成64bit的MAC值；预定义字段中一个比特信息指示用户面完整性保护是否开启，比如，该比特信息置1，表示开启用户面完整性保护，置0表示不开启用户面完整性保护。

[0385] 完整性保护指示信息和/或加密指示信息可以为上述实施方式c1-1(b2)、实施方式c1-1(b3)和实施方式c1-1(b4)中所示的例子，为比特信息，也可以称完整性保护指示信息和/或加密指示信息为开关信息。

[0386] 进一步，开关信息的具体内容，可以结合具体方法。比如，若开启用户面加密保护和用户面完整性保护；进一步，如果预设规则定义用户面加密保护默认开启，而用户面完整性保护则需要灵活确定，则可以在预设字段只携带1比特指示信息，该1比特指示信息用于指示是否需要开启用户面完整性保护；进一步，如果预设规则定义在没有收到完整性保护指示信息和加密指示信息前，不开启用户面加密保护，也不开启用户面完整性保护，则可以在预设字段携带2比特指示信息，分别用于指示是否开启用户加密保护，以及是否开启用户面完整性保护。

[0387] 实施方式c1-1(b5)

[0388] 完整性保护指示信息和/或加密指示信息可以是算法的标识。这种情况下完整性保护指示信息和/或加密指示信息可以承载在预设消息或安全策略中的预定义字段中，也可以承载在安全策略中。换言之，基站向终端设备发送算法的标识，该算法的标识用于指示算法，该算法的标识也是完整性保护指示信息和/或加密指示信息。

[0389] 一种可选地实施方式中，基站传递的AS SMC中，携带如LTE网络中的EIA和EEA的号码代表选择的完整性保护算法和加密算法。可以通过携带EIA和EEA的号码表示完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息，例如，EIA的号码表示开启完整性保护。

[0390] 另一种可选地实施方式中，可以将算法的标识扩充为4个预设字段，分别为EIA-RRC，EEA-RRC，EIA-UP，EEA-UP，并通过将选择的算法放到其相应位置，代表此次协商的方

法。比如，基站选择了EIA-RRC＝3，EEA-RRC＝2，则完整性保护指示信息、加密指示信息、信令面完整性保护指示信息和信令面加密指示信息可以是(EIA-RRC＝3，EEA-RRC＝2，EIA-UP＝0，EEA-UP＝0)；从而，终端设备接收到该信息后，由于EIA-RRC不是0，因此开启信令面完整性保护；由于EEA-RRC不是0，因此开启信令面加密保护；由于EIA-UP是0，因此不开启用户面完整性保护；或者，由于EEA-UP是0，因此不开启用户面加密保护。

[0391] 进一步，在该实施方式中，算法的标识不仅可以指示出完整性保护指示信息、加密指示信息，还可以指示出算法。也就是说，运用该实施例的情况下，发送算法的标识，即可以同时指示出算法(比如目标信令面完整性保护算法、目标信令面加密算法、目标用户面完整性保护算法和目标用户面加密算法)，以及完整性保护指示信息、加密指示信息。

[0392] 比如，EIA-RRC＝3还可以指示出信令面完整性保护算法，再比如EEA-RRC＝2还可以指示出信令面加密保护算法，再EIA-UP＝0还可以指示出用户面完整性保护算法，再比如EEA-UP＝0还可以指示出用户面加密保护算法，

[0393] 在图2a或图2b所示实施例的一种可选地实施方式中，完整性保护指示信息可以是算法的标识，比如当基站对终端设备开启用户面完整性保护的情况下，完整性保护指示信息可以是目标用户面完整性保护算法的标识。

[0394] 可选地，当基站对终端设备不开启用户面完整性保护的情况下，完整性保护指示信息可以为预设用户面完整性保护算法的标识；或者，不携带任何完整性保护算法的信息。也就是说，不发送任何完整性保护算法的标识或者发送预设用户面完整性保护算法的标识，即表示完整性保护指示信息指示不开启完整性保护。举个例子，假设预设用户面完整性保护算法的标识为X123，若终端设备接收到的完整性保护指示信息是X123的情况下，终端设备不开启用户面完整性保护。

[0395] 在图2a或图2b所示实施例的一种可选地实施方式中，基站还可以向终端设备发送加密指示信息，加密指示信息用于指示基站是否对终端设备开启用户面加密保护。在基站对终端设备开启用户面加密保护的情况下，加密指示信息可以是算法的标识，比如，加密指示信息是目标用户面加密算法的标识。

[0396] 可选地，当基站对终端设备不开启加密保护的情况下，加密指示信息可以预设用户面加密算法的标识，或者为空加密算法。也就是说，不发送任何加密算法的标识或者发送空加密算法或者发送预设用户面加密算法的标识，即表示加密指示信息指示不开启加密保护。举个例子，假设预设用户面加密算法算法的标识为X321，若终端设备接收到的加密保护指示信息是X321的情况下，终端设备不开启用户面加密保护。

[0397] 在图2，图2a或图2b所示实施例的另一种可选地实施方式中，基站还可以向终端设备发送信令面完整性保护指示信息，信令面完整性保护指示信息用于指示基站是否对终端设备开启信令面完整性保护。在基站对终端设备开启信令面完整性保护的情况下，信令面完整性保护指示信息可以是算法的标识，比如，信令面完整性保护指示信息是目标信令面完整性保护算法的标识。

[0398] 可选地，当基站对终端设备不开启信令面完整性保护的情况下，信令面完整性保护指示信息可以为预设信令面完整性保护算法的标识，或者为不携带任何完整性保护算法的信息。举个例子，假设预设信令面完整性保护算法的标识为X456，若终端设备接收到的信令面完整性保护指示信息是X456的情况下，终端设备不开启信令面完整性保护。

[0399] 在图2,图2a或图2b所示实施例的另一种可选地实施方式中,基站还可以向终端设备发送信令面加密指示信息,信令面加密指示信息用于指示基站是否对终端设备开启信令面加密保护。在基站对终端设备开启信令面加密保护的情况下,信令面加密指示信息可以是算法的标识,比如,信令面加密指示信息是目标信令面加密算法的标识。

[0400] 可选地,当基站对终端设备不开启信令面加密保护的情况下,信令面加密指示信息可以预设信令面加密算法的标识,或者为空加密算法。举个例子,假设预设信令面加密算法算法的标识为X654,若终端设备接收到的信令面加密保护指示信息是X654的情况下,终端设备不开启信令面加密保护。

[0401] 实施方式c1-1(b6)

[0402] 完整性保护指示信息和/或加密指示信息可以是预设消息或安全策略中的预定义字段中的会话ID和4比特信息,那么终端设备需要根据比特信息,开启这个会话ID下相应的用户面安全,举个例子,比如终端设备有多个会话ID,则每个会话ID对应的用户面安全方案可以是不同的,比如一个会话ID对应的是开启用户面完整性保护和开启用户面加密保护,另一个会话ID对应的可以是不开启用户面完整性保护和开启用户面加密保护。

[0403] 实施方式c1-1(b7)

[0404] 完整性保护指示信息和/或加密指示信息可以是预设消息或安全策略中的预定义字段中的会话ID和算法的标识。

[0405] 通过上述实施例可以看出,上述实施方式中,算法的标识和4比特位信息对应的实施方式是较为灵活的用方式,因为可以明确到用户面加密保护是否开启,以及用户名完整性保护是否开启。通过上述实施例可以看出比特位信息可以重用(复用)协商过的信令面算法(也就是说将适用于信令面的算法也适用于用户面,比如将确定出的目标信令面完整性保护算法也作为目标用户面完整性保护算法,将确定出的目标信令面加密算法也作为目标用户面加密算法),而算法的标识可以实现信令面算法和用户面安全算法不同,比如信令面加密算法和用户面加密算法不同,信令面完整性保护算法和用户面完整性保护算法不同。

[0406] 完整性保护指示信息和/或加密指示信息可以承载于RRC重配置请求消息中,由基站发送给终端设备。在这种情况下,若当前终端设备已经开启用户面加密保护,未开启用户面完整性保护,但是当前终端设备确定开启用户面完整性保护,可选地,RRC重配置请求消息中可以只传递完整性保护指示信息就够了。

[0407] 基站可以生成并将完整性保护指示信息发送给终端设备,另一种可选地实施方式中,基站接收到完整性保护指示信息和加密指示信息之后,生成新的指示信息(该新的指示信息中可以只包括完整性保护指示信息),进一步将该新的指示信息承载在RRC重配置请求中。由于完整性保护指示信息、加密指示信息可来自于N2接口,发出去的时候可能换了接口,所以基站还是需要根据RRC重配置请求消息中的格式,对将要承载的完整性保护指示信息和/或加密指示信息做一些相应处理。

[0408] 基站发送完整性保护指示信息和/或加密指示信息的一种方式中,基站也可以将完整性保护指示信息和/或加密指示信息直接转发给终端设备。

[0409] 基站发送完整性保护指示信息和/或加密指示信息的另一种方式中,基站根据完整性保护指示信息和/或加密指示信息是算法的标识,这种情况下,基站可以根据获取的(例如,基站接收或者是基站判断得到的)完整性保护指示信息和/或加密指示信息,确定对

应的目标算法的标识，并将对应的目标算法的标识发送给终端设备。举个例子，比如基站开启用户面完整性保护，则确定目标用户面完整性保护算法，并将目标用户面完整性保护算法的标识发送给终端设备，终端设备在接收到时可以开启用户面完整性保护算法，且使用目标用户面完整性保护算法进行用户面完整性保护。

[0410] 完整性保护指示信息和/或加密指示信息可以承载在RRC重配置请求消息中，由基站发送给终端设备。可选地，在完整性保护指示信息和/或加密指示信息为算法的标识的情况下，RRC消息中可以携带算法的标识。

[0411] 举个例子，比如当完整性保护指示信息和/或加密指示信息为算法的标识，则完整性保护指示信息和/或加密指示信息可以是一个算法列表。可选地，如果完整性保护指示信息和/或加密指示信息对应的算法列表中的算法是完整性保护算法，并且完整性保护算法不是空算法，且基站若确定终端设备支持的用户面完整性保护算法、基站允许的用户面完整性保护算法以及完整性保护指示信息和/或加密指示信息对应的算法列表中的算法，这三者没有交集；则基站可以选择一个既是终端设备支持的用户面完整性保护算法，又是基站允许的用户面完整性保护算法作为目标用户面完整性保护算法。如果完整性保护指示信息和/或加密指示信息对应的算法列表中的算法是是空算法，则基站不选择目标用户面完整性保护算法，可以理解为不开启用户面完整性保护。

[0412] 进一步，可选地，如果完整性保护指示信息和/或加密指示信息对应的算法列表中的算法是加密算法，并且加密算法不是空加密算法，且基站若确定终端设备支持的用户面加密算法、基站允许的用户面加密算法以及完整性保护指示信息和/或加密指示信息对应的算法列表中的算法，这三者没有交集；则基站可以选择一个既是终端设备支持的用户面加密算法，又是基站允许的用户面加密算法作为目标用户面加密算法。如果完整性保护指示信息和/或加密指示信息对应的算法列表中的算法是是空加密算法，则基站可以选择一个空加密算法作为目标用户面加密算法，可以理解为不开启用户面加密保护。

[0413] 再举个例子，当完整性保护指示信息和/或加密指示信息为算法的标识，则完整性保护指示信息和/或加密指示信息可以是一个算法列表，可以从该算法列表中选择一个算法，若选择出的算法为完整性保护算法，且该选择出的完整性保护算法是预设完整性保护算法，则可选的，基站在转发选择出的完整性保护算法给终端设备之前，检查选择出的完整性保护算法是否既是终端设备支持的用户面完整性保护算法，又是基站允许的用户面完整性保护算法；若是，则该选择出的完整性保护算法即作为目标用户面完整性保护算法发送给终端设备。

[0414] 另一方面，若选择出的完整性保护算法不满足既是终端设备支持的用户面完整性保护算法，又是基站允许的用户面完整性保护算法的条件，且选择出的完整性保护算法不是空算法，则基站要选择一个既是终端设备支持的用户面完整性保护算法，又是基站允许的用户面完整性保护算法的算法作为目标用户面完整性保护算法发送给终端设备。另一方面，若选择出的完整性保护算法不满足既是终端设备支持的用户面完整性保护算法，又是基站允许的用户面完整性保护算法的条件，且选择出的完整性保护算法是空算法，则则基站不选择目标用户面完整性保护算法，可以理解为不开启用户面完整性保护。

[0415] 进一步，另一方面，可选地，若选择出的算法为加密算法，且该选择出的加密算法是预设加密算法，则可选的，基站在转发选择出的加密算法给终端设备之前，检查选择出的

加密算法是否既是终端设备支持的用户面加密算法，又是基站允许的用户面加密算法；若是，则该选择出的加密算法即作为目标用户面加密算法发送给终端设备。

[0416] 另一方面，若选择出的加密算法不满足既是终端设备支持的用户面加密算法，又是基站允许的用户面加密算法的条件，且选择出的加密算法不是空算法，则基站要选择一个既是终端设备支持的用户面加密算法，又是基站允许的用户面加密算法的算法作为目标用户面加密算法发送给终端设备。另一方面，若选择出的加密算法不满足既是终端设备支持的用户面加密算法，又是基站允许的用户面加密算法的条件，且选择出的加密算法是空算法，则则基站不选择目标用户面加密算法，可以理解为不开启用户面加密保护。

[0417] 本申请实施例中完整性保护指示信息和/或加密指示信息可以承载在AS安全模式命令中，并通过基站发送给终端设备。可选地，也可以将信令面完整性保护指示信息和/或信令面加密指示信息承载在AS安全模式命令中，并通过基站发送给终端设备。

[0418] 一种可选地实施方式中，在终端设备在开启用户面完整性保护前，终端设备可以验证AS安全模式命令的完整性保护。可选的，基站使用用户面完整性保护算法对AS安全模式命令进行完整性保护。可选的，基站可以根据安全策略判断用户面完整性保护开启后，使用用户面完整性保护算法对AS安全模式命令进行完整性保护。可选的，终端设备使用用户面完整性保护算法验证AS安全模式命令的完整性保护是否正确。比如，终端设备是在发现用户面完整性保护激活后，使用用户面完整性保护算法验证AS安全模式命令的完整性保护是否正确；不排除用户面完整性保护算法为当前使用的AS信令面完整性保护算法。进一步，基站接收到终端设备回复的AS安全模式结束消息。可选的，基站使用用户面完整性保护算法，验证AS安全模式结束消息的完整性保护。可选的，基站是在发现AS安全模式结束消息中携带了完整性保护参数MAC-I后，对AS安全模式结束消息进行完整性保护验证；不排除，用户面完整性保护算法为当前使用的AS信令面完整性保护算法。可选地，基站在接收到安全模式结束消息之后，相应的开启用户面完整性保护(比如完整性指示信息和加密指示信息指示开启用户面完整性保护，不开启用户面加密保护，则基站可以在收到安全模式结束消息之后开启用户面完整性保护，不开启用户面加密保护)。进一步，可选地，基站在相应的开启用户面完整性保护之后可以向终端设备发送RRC重配置请求消息；进一步可选地终端设备向基站返回RRC重配置完成消息。

[0419] 另一种可选地实施方式中，开启用户面完整性保护的情况，完整性保护指示信息可以承载在AS安全模式命令中，再将AS安全模式命令承载在RRC重配置请求消息中，并通过基站发送给终端设备。可选地，加密指示信息、信令面完整性保护指示信息和信令面加密指示信息中的至少一项，也可以承载在AS安全模式命令中，再将AS安全模式命令承载在RRC重配置请求消息中，并通过基站发送给终端设备。

[0420] 图3示例性示出了本申请提供的一种基站的结构示意图。

[0421] 基于相同构思，本申请提供一种基站300，用于执行上述方法中的任一个方案。如图3所示，基站300包括处理器301、收发器302、存储器303和通信接口304；其中，处理器301、收发器302、存储器303和通信接口304通过总线305相互连接。

[0422] 总线305可以是外设部件互连标准(peripheral component interconnect，PCI)总线或扩展工业标准结构(extended industry standard architecture，EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图3中仅用一条粗线表示，但并

不表示仅有一根总线或一种类型的总线。

[0423] 存储器303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303还可以包括上述种类的存储器的组合。

[0424] 通信接口304可以为有线通信接入口,无线通信接口或其组合,其中,有线通信接口例如可以为以太网接口。以太网接口可以是光接口,电接口或其组合。无线通信接口可以为WLAN接口。

[0425] 处理器301可以是中央处理器(central processing unit,CPU),网络处理器(network processor,NP)或者CPU和NP的组合。处理器301还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit,ASIC),可编程逻辑器件(programmable logic device,PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(complex programmable logic device,CPLD),现场可编程逻辑门阵列(field-programmable gate array,FPGA),通用阵列逻辑(generic array logic,GAL)或其任意组合。

[0426] 可选地,存储器303还可以用于存储程序指令,处理器301调用该存储器303中存储的程序指令,可以执行上述方案中所示实施例中的一个或多个步骤,或其中可选的实施方式,使得基站300实现上述方法中基站的功能。

[0427] 处理器301用于根据执行存储器存储的指令,并控制收发器302进行信号接收和信号发送,当处理器301执行存储器存储的指令时,基站300可用于执行下述方案。

[0428] 处理器301,用于获取安全策略,安全策略包括完整性保护指示信息,完整性保护指示信息用于指示基站是否对终端设备开启完整性保护;当完整性保护指示信息指示基站对终端设备开启完整性保护时,确定目标用户面完整性保护算法;收发器302,用于向终端设备发送目标用户面完整性保护算法。如此,可根据安全策略灵活的为终端设备选择是否开启完整性保护,且仅在对终端设备开启完整性保护时,基站向终端设备发送目标用户面完整性保护算法,一方面,由于单独协商用户面的安全算法,提高了用户面安全算法和信令面安全算法分开确定的灵活性,另一方面,由于增加了完整性保护指示信息,提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0429] 可选地,收发器302,用于:通过无线资源控制RRC信令向终端设备发送目标用户面完整性保护算法。通过复用现有技术中的RRC信令的方式实现本申请实施例提供的方案,从而更好的兼容现有技术,且对现有技术改动较小。具体可选地实施方式可以参考上述内容,在此不再赘述。

[0430] 可选地,处理器301,具体用于:根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法,确定目标用户面完整性保护算法。

[0431] 可选地,基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法;或者,终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。

[0432] 可选地,安全策略还包括服务网络允许的用户面完整性保护算法;处理器301,用于:根据基站允许的用户面完整性保护算法,终端设备支持的用户面完整性保护算法,以及

服务网络允许的用户面完整性保护算法,确定目标用户面完整性保护算法。

[0433] 可选地,服务网络允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。

[0434] 可选地,处理器301,还用于:当安全策略还包括加密指示信息,且加密指示信息用于指示基站对终端设备开启加密保护时,通过收发器302向终端设备发送目标用户面加密算法;或者,当安全策略还包括密钥长度时,通过收发器302向终端设备发送密钥长度;或者,当安全策略还包括D-H指示信息,且D-H指示信息用于指示基站对终端设备开启D-H时,通过收发器302向终端设备发送D-H相关密钥。

[0435] 可选地,收发器302,具体用于:从会话管理功能SMF实体接收终端设备的当前会话的服务质量;处理器301,还用于:根据安全策略和服务质量中的至少一种,为终端设备分配目标无线数据承载。

[0436] 处理器301,还用于:根据安全策略和服务质量中的至少一种,为终端设备分配目标无线数据承载的具体方式参见上述方法实施例中的内容,在此不再赘述。

[0437] 一种可选地实施方案中,处理器301,用于:根据安全策略和服务质量中的至少一种,为终端设备创建目标无线数据承载。

[0438] 可选地,收发器302,用于:从SMF实体接收安全策略;或者;从SMF实体接收安全策略的标识,并根据安全策略的标识,获取安全策略。

[0439] 可选地,处理器301,还用于:获取终端设备支持的信令面安全算法;根据终端设备支持的信令面安全算法,以及基站允许的信令面安全算法,确定目标信令面安全算法;收发器302,还用于:将目标信令面安全算法携带在接入层AS安全模式命令SMC中发送给终端设备。

[0440] 图4示例性示出了本申请提供的一种SMF实体的结构示意图。

[0441] 基于相同构思,本申请提供一种SMF实体400,用于执行上述方法中的任一个方案。如图4所示,SMF实体400包括处理器401、收发器402、存储器403和通信接口404;其中,处理器401、收发器402、存储器403和通信接口404通过总线405相互连接。

[0442] 总线405可以是外设部件互连标准(peripheral component interconnect,PCI)总线或扩展工业标准结构(extended industry standard architecture,EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示,图4中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

[0443] 存储器403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403还可以包括上述种类的存储器的组合。

[0444] 通信接口404可以为有线通信接入口,无线通信接口或其组合,其中,有线通信接口例如可以为以太网接口。以太网接口可以是光接口,电接口或其组合。无线通信接口可以为WLAN接口。

[0445] 处理器401可以是中央处理器(central processing unit,CPU),网络处理器(network processor,NP)或者CPU和NP的组合。处理器401还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit,ASIC),可

编程逻辑器件(programmable logic device,PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(complex programmable logic device,CPLD),现场可编程逻辑门阵列(field-programmable gate array,FPGA),通用阵列逻辑(generic array logic,GAL)或其任意组合。

[0446] 可选地,存储器403还可以用于存储程序指令,处理器401调用该存储器403中存储的程序指令,可以执行上述方案中所示实施例中的一个或多个步骤,或其中可选的实施方式,使得SMF实体400实现上述方法中SMF实体的功能。

[0447] 处理器401用于根据执行存储器存储的指令,并控制收发器402进行信号接收和信号发送,当处理器401执行存储器存储的指令时,SMF实体400可用于执行下述方案。

[0448] 收发器402,用于接收请求消息,请求消息包括安全策略的相关参数;向基站发送安全策略或安全策略的标识;处理器401,用于根据安全策略的相关参数,获得安全策略或者安全策略的标识;其中,安全策略包括完整性保护指示信息,完整性保护指示信息用于指示基站是否对终端设备开启完整性保护。一方面,由于单独协商用户面的安全算法,提高了用户面安全算法和信令面安全算法分开确定的灵活性,另一方面,由于增加了完整性保护指示信息,提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0449] 一种可选地实施方案中,安全策略的相关参数包括终端设备的标识,终端设备的数据网络名称DNN,终端设备的切片的标识,终端设备的服务质量和终端设备的会话标识中的至少一种。如此,可根据不同的标识从不同的角度或粒度实现安全策略的制定,更加灵活。

[0450] 可选地,处理器401,用于:安全策略的相关参数包括终端设备的标识,SMF实体根据终端设备的标识与安全策略的关联关系以及终端设备的标识,获得安全策略,如此可实现在终端设备的粒度上的安全策略的确定,实现不同的终端设备可对应不同的安全策略的目的。

[0451] 另一种可选地实施方式中,处理器401,用于:安全策略的相关参数包括终端设备的切片的标识,SMF实体根据切片的标识和安全策略的关联关系以及终端设备的切片的标识,获得安全策略,如此可实现在切片的粒度上的安全策略的确定,实现接入不同的切片的终端设备可对应不同的安全策略的目的。

[0452] 另一种可选地实施方式中,处理器401,用于:安全策略的相关参数包括终端设备的会话标识,SMF实体根据会话标识和安全策略的关联关系以及终端设备的会话标识,获得安全策略,如此可实现在会话的粒度上的安全策略的确定,实现发起不同会话的终端设备可对应不同的安全策略的目的。

[0453] 另一种可选地实施方式中,处理器401,用于:安全策略的相关参数包括终端设备的服务质量;SMF实体根据终端设备的服务质量,获得安全策略,如此可实现在服务质量的粒度上的安全策略的确定,实现发起不同服务质量的终端设备可对应不同的安全策略的目的。

[0454] 可选地,安全策略还包括以下内容中至少一种:加密指示信息,加密指示信息用于指示基站对终端设备开启加密保护;密钥长度;D-H指示信息,D-H指示信息用于指示基站对终端设备开启D-H;和,服务网络允许的用户面完整性保护算法。如此,可以更加灵活的对安全策略中的任一个信息进行指示,使最终确定的安全策略更加适应复杂的应用场景。

[0455] 图5示例性示出了本申请实施例提供的一种基站的结构示意图。

[0456] 基于相同构思，本申请实施例提供一种基站，用于执行上述方法流程中的任一个方案。如图5所示，基站500包括接收单元501、处理单元502和发送单元503。

[0457] 处理单元502，用于获取安全策略，安全策略包括完整性保护指示信息，完整性保护指示信息用于指示基站是否对终端设备开启完整性保护；当完整性保护指示信息指示基站对终端设备开启完整性保护时，通过发送单元503向终端设备发送目标用户面完整性保护算法；发送单元503，用于向终端设备发送目标用户面完整性保护算法。如此，可根据安全策略灵活的为终端设备选择是否开启完整性保护，且仅在对终端设备开启完整性保护时，基站向终端设备发送目标用户面完整性保护算法，一方面，由于单独协商用户面的安全算法，提高了用户面安全算法和信令面安全算法分开确定的灵活性，另一方面，由于增加了完整性保护指示信息，提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0458] 可选地，发送单元503，用于：通过无线资源控制RRC信令向终端设备发送目标用户面完整性保护算法。通过复用现有技术中的RRC信令的方式实现本申请实施例提供的方案，从而更好的兼容现有技术，且对现有技术改动较小。具体可选地实施方式可以参考上述内容，在此不再赘述。

[0459] 可选地，处理单元502，在通过发送单元503向终端设备发送目标用户面完整性保护算法之前，还用于：根据终端设备支持的用户面完整性保护算法和基站允许的用户面完整性保护算法，确定目标用户面完整性保护算法。

[0460] 可选地，基站允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法；或者，终端设备支持的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。

[0461] 可选地，安全策略还包括服务网络允许的用户面完整性保护算法；处理单元502，用于：根据基站允许的用户面完整性保护算法，终端设备支持的用户面完整性保护算法，以及服务网络允许的用户面完整性保护算法，确定目标用户面完整性保护算法。

[0462] 可选地，服务网络允许的用户面完整性保护算法为按照优先级排序的用户面完整性保护算法。

[0463] 可选地，处理单元502，还用于：当安全策略还包括加密指示信息，且加密指示信息用于指示基站对终端设备开启加密保护时，通过发送单元503向终端设备发送目标用户面加密算法；或者，当安全策略还包括密钥长度时，通过发送单元503向终端设备发送密钥长度；或者，当安全策略还包括D-H指示信息，且D-H指示信息用于指示基站对终端设备开启D-H时，通过发送单元503向终端设备发送D-H相关密钥。

[0464] 可选地，还包括接收单元501，在通过发送单元503向终端设备发送目标用户面完整性保护算法之前，用于：从会话管理功能SMF实体接收终端设备的当前会话的服务质量；处理单元502，还用于：根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载。

[0465] 处理单元502，还用于：根据安全策略和服务质量中的至少一种，为终端设备分配目标无线数据承载的具体方式参见上述方法实施例中的内容，在此不再赘述。

[0466] 一种可选地实施方案中，处理单元502，用于：根据安全策略和服务质量中的至少一种，为终端设备创建目标无线数据承载。

[0467] 可选地，接收单元501，用于：从SMF实体接收安全策略；或者；从SMF实体接收安全策略的标识，并根据安全策略的标识，获取安全策略。

[0468] 可选地，处理单元502，还用于：获取终端设备支持的信令面安全算法；根据终端设备支持的信令面安全算法，以及基站允许的信令面安全算法，确定目标信令面安全算法；发送单元503，还用于：将目标信令面安全算法携带在接入层AS安全模式命令SMC中发送给终端设备。

[0469] 应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，接收单元501和发送单元503可以由收发器302实现，处理单元502可以由处理器301实现。如图3所示，基站300可以包括处理器301、收发器302和存储器303。其中，存储器303可以用于存储处理器301执行方案时的代码，该代码可为基站300出厂时预装的程序/代码。

[0470] 图6示例性示出了本申请实施例提供的一种SMF实体的结构示意图。

[0471] 基于相同构思，本申请实施例提供一种SMF实体，用于执行上述方法流程中的任一个方案。如图6所示，SMF实体600包括接收单元601、处理单元602，可选地，还包括发送单元603。

[0472] 接收单元601，用于接收请求消息，请求消息包括安全策略的相关参数；向基站发送安全策略或安全策略的标识；处理单元602，用于根据安全策略的相关参数，获得安全策略或者安全策略的标识；其中，安全策略包括完整性保护指示信息，完整性保护指示信息用于指示基站是否对终端设备开启完整性保护。一方面，由于单独协商用户面的安全算法，提高了用户面安全算法和信令面安全算法分开确定的灵活性，另一方面，由于增加了完整性保护指示信息，提高了终端设备的目标用户面完整性保护算法确定的灵活性。

[0473] 一种可选地实施方案中，安全策略的相关参数包括终端设备的标识，终端设备的数据网络名称DNN，终端设备的切片的标识，终端设备的服务质量和终端设备的会话标识中的至少一种。如此，可根据不同的标识从不同的角度或粒度实现安全策略的制定，更加灵活。

[0474] 可选地，处理单元602，用于：安全策略的相关参数包括终端设备的标识，SMF实体根据终端设备的标识与安全策略的关联关系以及终端设备的标识，获得安全策略，如此可实现在终端设备的粒度上的安全策略的确定，实现不同的终端设备可对应不同的安全策略的目的。

[0475] 另一种可选地实施方式中，处理单元602，用于：安全策略的相关参数包括终端设备的切片的标识，SMF实体根据切片的标识和安全策略的关联关系以及终端设备的切片的标识，获得安全策略，如此可实现在切片的粒度上的安全策略的确定，实现接入不同的切片的终端设备可对应不同的安全策略的目的。

[0476] 另一种可选地实施方式中，处理单元602，用于：安全策略的相关参数包括终端设备的会话标识，SMF实体根据会话标识和安全策略的关联关系以及终端设备的会话标识，获得安全策略，如此可实现在会话的粒度上的安全策略的确定，实现发起不同会话的终端设备可对应不同的安全策略的目的。

[0477] 另一种可选地实施方式中，处理单元602，用于：安全策略的相关参数包括终端设备的服务质量；SMF实体根据终端设备的服务质量，获得安全策略，如此可实现在服务质量

的粒度上的安全策略的确定，实现发起不同服务质量的终端设备可对应不同的安全策略的目的。

[0478] 可选地，安全策略还包括以下内容中至少一种：加密指示信息，加密指示信息用于指示基站对终端设备开启加密保护；密钥长度；D-H指示信息，D-H指示信息用于指示基站对终端设备开启D-H；和，服务网络允许的用户面完整性保护算法。如此，可以更加灵活的对安全策略中的任一个信息进行指示，使最终确定的安全策略更加适应复杂的应用场景。

[0479] 应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，接收单元601和发送单元603可以由收发器402实现，处理单元602可以由处理器401实现。如图4所示，SMF实体400可以包括处理器401、收发器402和存储器403。其中，存储器403可以用于存储处理器401执行方案时的代码，该代码可为SMF实体400出厂时预装的程序/代码。

[0480] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现、当使用软件程序实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个指令。在计算机上加载和执行计算机程序指令时，全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。指令可以存储在计算机存储介质中，或者从一个计算机存储介质向另一个计算机存储介质传输，例如，指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质，(例如，软盘、硬盘、磁带、磁光盘(MO)等)、光介质(例如，CD、DVD、BD、HVD等)、或者半导体介质(例如ROM、EPROM、EEPROM、非易失性存储器(NAND FLASH)、固态硬盘(Solid State Disk，SSD))等。

[0481] 本领域内的技术人员应明白，本申请实施例可提供为方法、系统、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0482] 本申请实施例是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0483] 这些指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0484] 这些指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他

可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0485] 显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

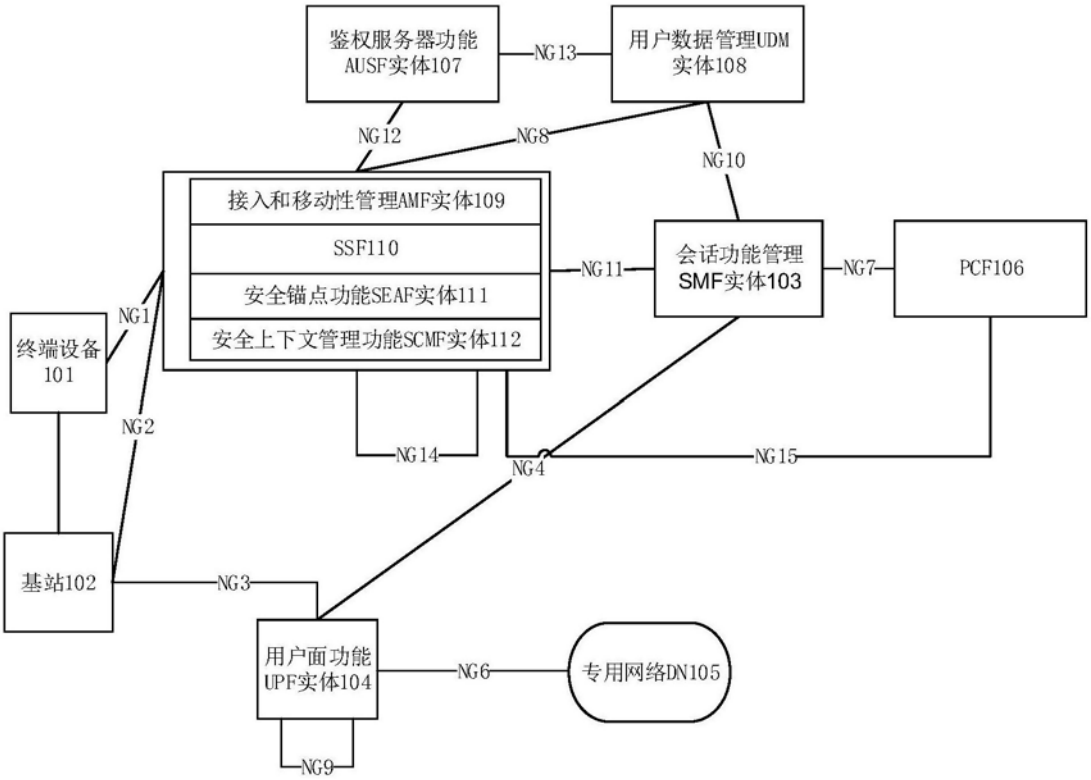

鉴权服务器功能
AUSF实体107
NG13
用户数据管理UDM
实体108
NG12
NG8
NG10
接入和移动性管理AMF实体109
SSF110
安全锚点功能SEAF实体111
安全上下文管理功能SCMF实体112
NG11
会话功能管理
SMF实体103
NG7
PCF106
NG1
终端设备
101
NG2
NG14
NG4
NG15
基站102
NG3
用户面功能
UPF实体104
NG6
专用网络DN105
NG9

图1

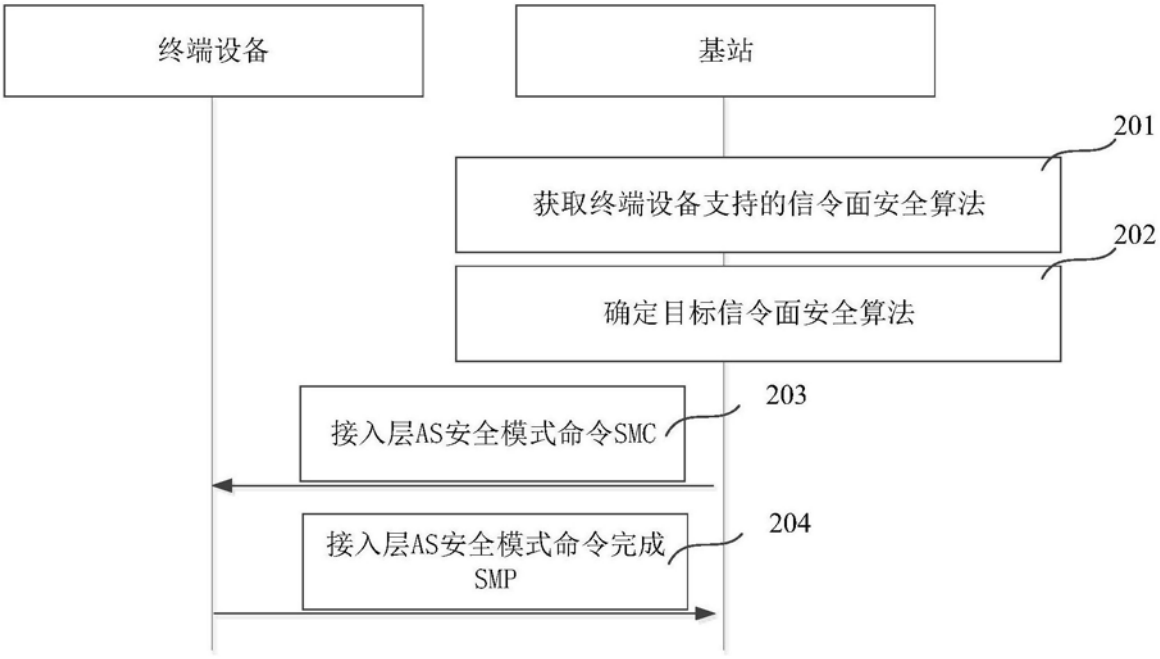

终端设备
基站
201
获取终端设备支持的信令面安全算法
202
确定目标信令面安全算法
203
接入层AS安全模式命令SMC
204
接入层AS安全模式命令完成
SMP

图2

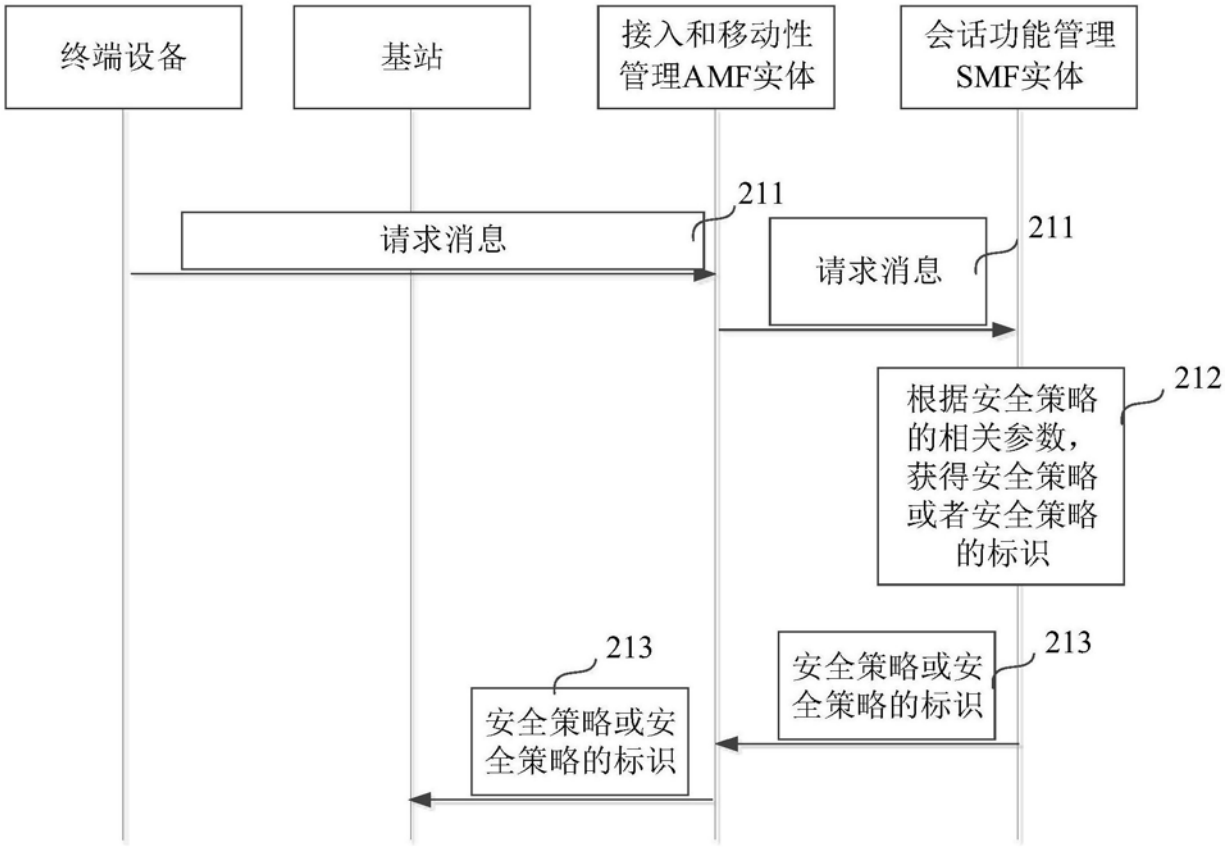

终端设备
基站
接入和移动性管理AMF实体
会话功能管理SMF实体
211
请求消息
211
请求消息
212
根据安全策略的相关参数，获得安全策略或者安全策略的标识
213
安全策略或安全策略的标识
213
安全策略或安全策略的标识

图2a

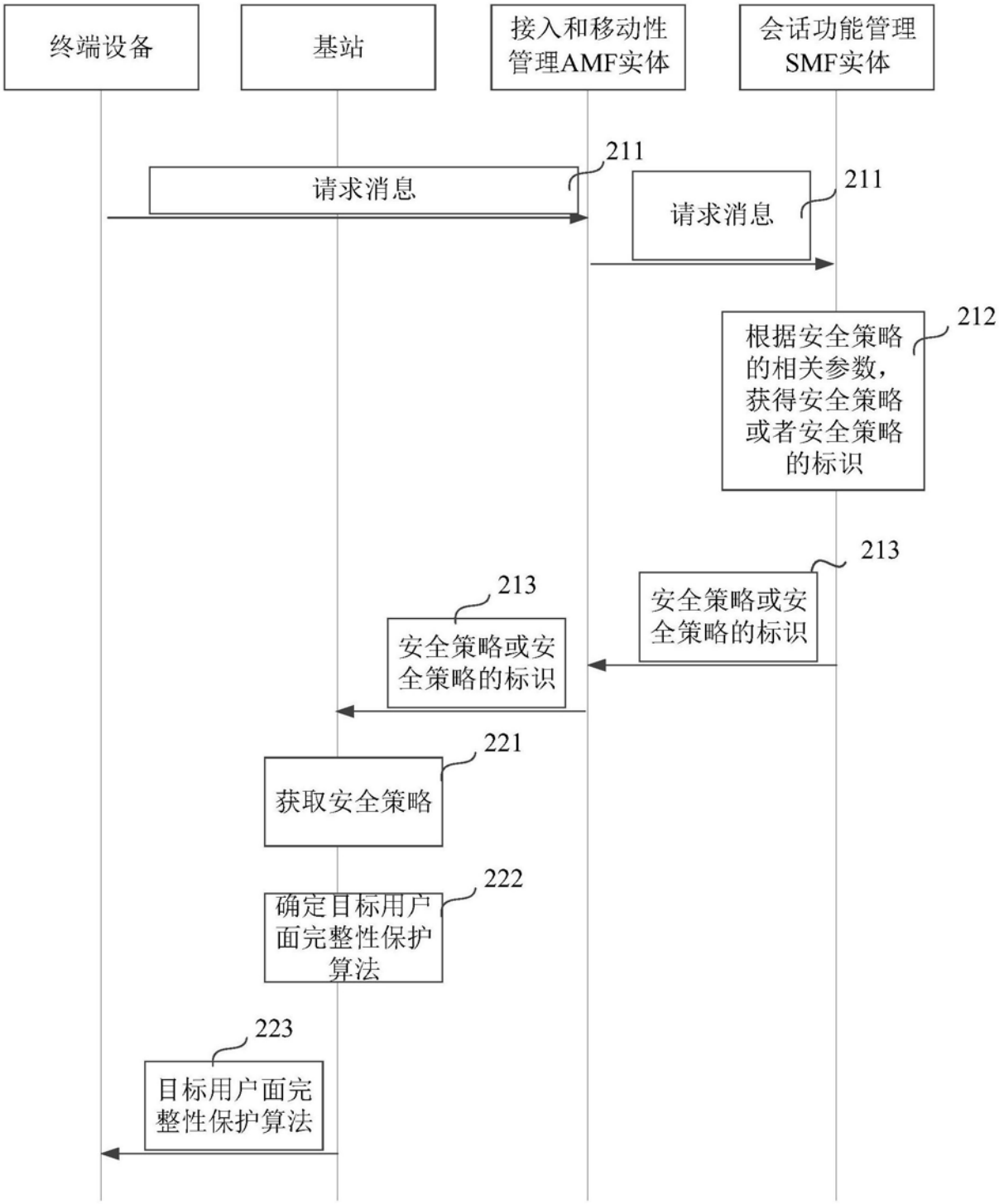

终端设备
基站
接入和移动性管理AMF实体
会话功能管理SMF实体
211
请求消息
211
请求消息
212
根据安全策略的相关参数，获得安全策略或者安全策略的标识
213
安全策略或安全策略的标识
213
安全策略或安全策略的标识
221
获取安全策略
222
确定目标用户面完整性保护算法
223
目标用户面完整性保护算法

图2b

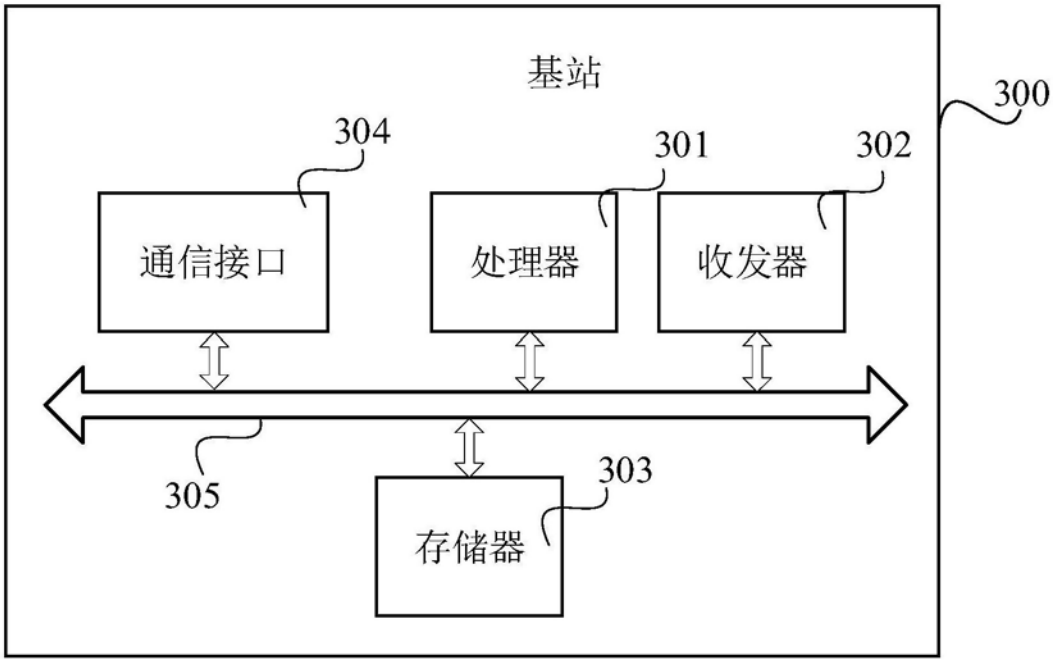

基站
300
304
301
302
通信接口
处理器
收发器
305
303
存储器

图3

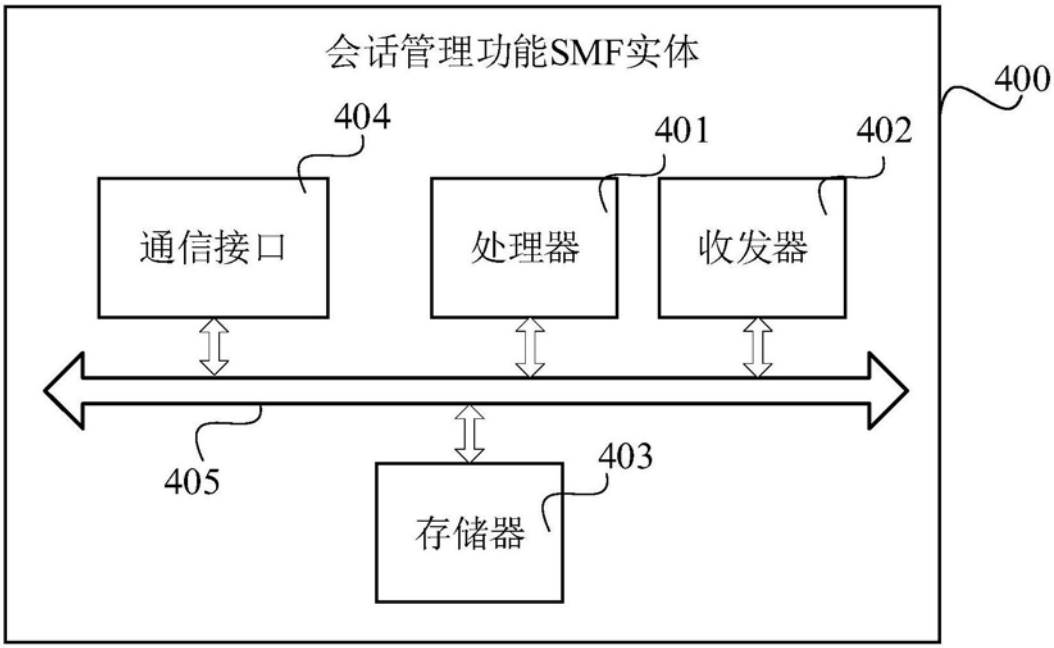

会话管理功能SMF实体
400
404
401
402
通信接口
处理器
收发器
405
403
存储器

图4

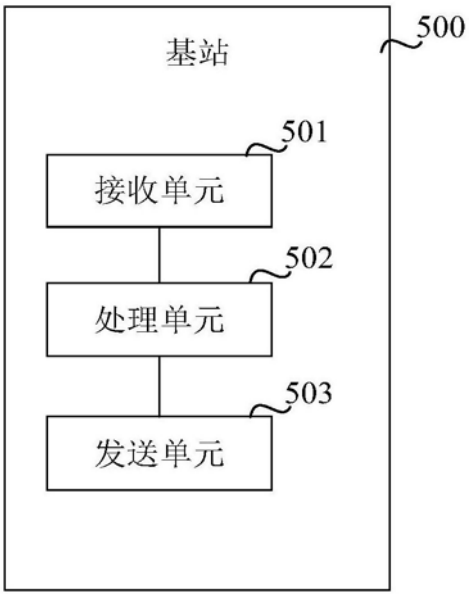

基站
500
501
接收单元
502
处理单元
503
发送单元

图5

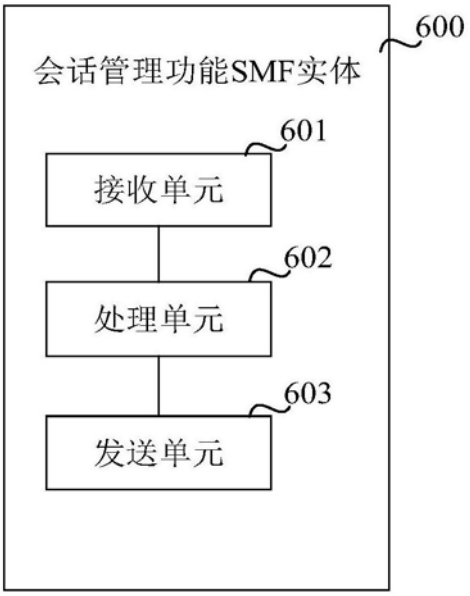

会话管理功能SMF实体
600
601
接收单元
602
处理单元
603
发送单元

图6