(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 109246692 A
(43)申请公布日 2019.01.18

(21)申请号 201710458181.6

(22)申请日 2017.06.16

(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 李秉肇 权威 王学龙

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 杨泽 刘芳

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/10(2009.01)
H04W 76/10(2018.01)
H04W 76/20(2018.01)

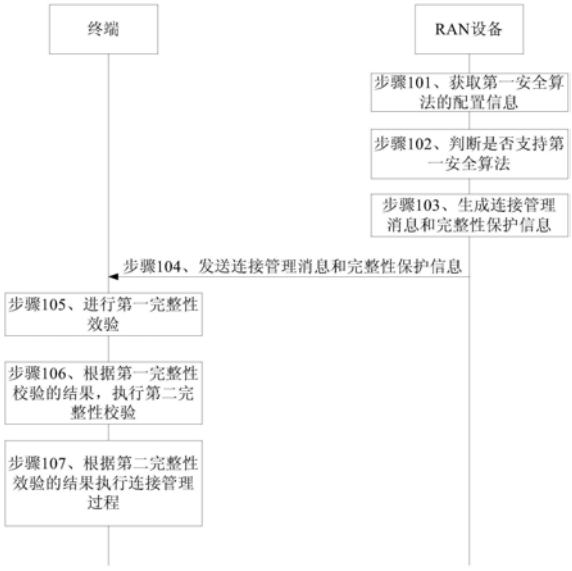
权利要求书4页 说明书16页 附图7页

(54)发明名称

连接管理方法、终端及无线接入网设备

(57)摘要

本申请实施例提供一种连接管理方法、终端及无线接入网设备。本申请连接管理方法，包括：终端接收连接管理消息及完整性保护信息，所述完整性保护信息是根据所述连接管理消息使用第一安全算法生成的；所述终端根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验；所述终端根据第一完整性校验的结果，执行第二完整性校验；所述终端根据第二完整性效验的结果执行连接管理过程。本申请实施例可以实现正确效验与解密，确保连接管理的正常执行。



CN 109246692 A

1.一种连接管理方法,其特征在于,包括:

终端接收连接管理消息及完整性保护信息,所述完整性保护信息是根据所述连接管理消息使用第一安全算法生成的;

所述终端根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验;

所述终端根据第一完整性校验的结果,执行第二完整性校验,所述终端根据第二完整性效验的结果执行连接管理过程。

2.根据权利要求1所述的方法,其特征在于,所述终端根据第一完整性校验的结果,执行第二完整性校验,包括:

当所述第一完整性效验的结果为未通过时,所述终端获取所述连接管理消息中包括的第二安全算法的配置信息;

所述终端根据所述第二安全算法的配置信息和所述完整性保护信息对所述连接管理消息进行第二完整性效验。

3.根据权利要求2所述的方法,其特征在于,所述终端根据所述第二完整性效验的结果执行连接管理过程,包括:

当所述第二完整性效验的结果为通过时,执行连接管理过程。

4.根据权利要求3所述的方法,其特征在于,所述当所述第二完整性效验的结果为通过时,执行连接管理过程,包括:

当所述第二完整性效验的结果为通过,且所述连接管理消息未携带第一类配置参数信息,执行连接管理过程,所述第一类配置参数信息为被允许在加密的消息中发送的配置信息。

5.一种连接管理方法,其特征在于,包括:

无线接入网RAN设备获取终端使用的第一安全算法的配置信息;

所述RAN设备根据所述配置信息判断所述RAN设备是否支持所述第一安全算法;

所述RAN设备根据判断结果生成连接管理消息和完整性保护信息;

所述RAN设备发送所述连接管理消息和所述完整性保护信息。

6.根据权利要求5所述的方法,其特征在于,所述RAN设备根据判断结果生成连接管理消息和完整性保护信息,包括:

当所述判断结果为所述RAN设备不支持所述第一安全算法时,所述RAN设备生成连接管理消息,并根据所述连接管理消息使用第二安全算法生成所述完整性保护信息,所述第二安全算法是所述RAN设备支持的;

其中,所述连接管理消息包括所述第二安全算法的配置信息。

7.根据权利要求6所述的方法,其特征在于,所述连接管理消息还包括第二类配置参数信息,所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。

8.根据权利要求5所述的方法,其特征在于,所述RAN设备根据判断结果生成连接管理消息和完整性保护信息,包括:

当所述RAN设备支持所述第一安全算法时,所述RAN设备使用所述第一安全算法加密生成所述连接管理消息,并根据所述连接管理消息使用第一安全算法生成所述完整性保护信息。

9.根据权利要求8所述的方法，其特征在于，所述连接管理消息携带第一类配置参数信息和第二类配置参数信息，所述第一类配置参数信息为被允许在加密的消息中发送的配置信息，所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。

10.一种连接管理方法，其特征在于，包括：

终端接收连接管理消息、完整性保护信息、以及安全算法的配置信息，所述连接管理消息为使用所述安全算法加密的，所述完整性保护信息为使用所述安全算法根据所述连接管理消息生成的，所述安全算法的配置信息未加密；

所述终端根据所述安全算法的配置信息对所述连接管理消息进行完整性校验，并且基于所述安全算法的配置信息对所述连接管理消息进行解密，并根据解密结果执行连接管理过程。

11.根据权利要求10所述的方法，其特征在于，所述连接管理消息、完整性保护信息、以及安全算法的配置信息是通过一个高层数据单元传输的。

12.根据权利要求11所述的方法，其特征在于，所述安全算法的配置信息在PDCP层数据单元的包头，或者在PDCP层数据单元的所述完整性保护信息之后。

13.一种连接管理方法，其特征在于，包括：

无线接入网RAN设备使用安全算法加密生成连接管理消息，使用所述安全算法根据所述连接管理消息生成完整性保护信息；

所述RAN设备发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

14.根据权利要求13所述的方法，其特征在于，所述安全算法的配置信息包括安全算法的标识、密钥和密钥输入参数中的至少一种。

15.根据权利要求13或14所述的方法，其特征在于，所述RAN设备发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息，包括：

所述RAN设备通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

16.根据权利要求15所述的方法，其特征在于，所述高层数据单元包括PDCP层数据单元；

所述RAN设备通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息，包括：

所述RAN设备将RRC层的所述连接管理消息设置为PDCP层数据单元的数据；

所述RAN设备将所述未加密的安全算法的配置信息设置在PDCP层数据单元的包头，或者设置在PDCP层数据单元的所述完整性保护信息之后。

17.一种终端，其特征在于，包括：

接收模块，用于接收连接管理消息及完整性保护信息，所述完整性保护信息是根据所述连接管理消息使用第一安全算法生成的；

处理模块，用于根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验；

所述处理模块，还用于根据第一完整性校验的结果，执行第二完整性校验，并根据第二完整性效验的结果执行连接管理过程。

18.根据权利要求17所述的终端，其特征在于，所述处理模块用于根据第一完整性校验的结果，执行第二完整性校验，包括：

当所述第一完整性效验的结果为未通过时，获取所述连接管理消息中包括的第二安全算法的配置信息；

根据所述第二安全算法的配置信息和所述完整性保护信息对所述连接管理消息进行第二完整性效验。

19.根据权利要求18所述的终端，其特征在于，所述处理模块用于根据所述第二完整性效验的结果执行连接管理过程，包括：

当所述第二完整性效验的结果为通过时，执行连接管理过程。

20.根据权利要求19所述的终端，其特征在于，所述处理模块用于当所述第二完整性效验的结果为通过时，执行连接管理过程，包括：

当所述第二完整性效验的结果为通过，且所述连接管理消息未携带第一类配置参数信息，执行连接管理过程，所述第一类配置参数信息为被允许在加密的消息中发送的配置信息。

21.一种无线接入网RAN设备，其特征在于，包括：

处理模块，用于确定终端使用的第一安全算法的配置信息；

所述处理模块，还用于根据所述配置信息判断所述RAN设备是否支持所述第一安全算法；

所述处理模块，还用于根据判断结果生成连接管理消息和完整性保护信息；

发送模块，用于发送所述连接管理消息和所述完整性保护信息。

22.根据权利要求21所述的RAN设备，其特征在于，所述处理模块用于根据判断结果生成连接管理消息和完整性保护信息，包括：

当所述判断结果为所述RAN设备不支持所述第一安全算法时，生成连接管理消息，并根据所述连接管理消息使用第二安全算法生成所述完整性保护信息，所述第二安全算法是所述RAN设备支持的；

其中，所述连接管理消息包括所述第二安全算法的配置信息。

23.根据权利要求22所述的RAN设备，其特征在于，所述连接管理消息还包括第二类配置参数信息，所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。

24.根据权利要求21所述的RAN设备，其特征在于，所述处理模块用于根据判断结果生成连接管理消息和完整性保护信息，包括：

当所述RAN设备支持所述第一安全算法时，使用所述第一安全算法加密生成所述连接管理消息，并根据所述连接管理消息使用第一安全算法生成所述完整性保护信息。

25.根据权利要求24所述的RAN设备，其特征在于，所述连接管理消息携带第一类配置参数信息和第二类配置参数信息，所述第一类配置参数信息为被允许在加密的消息中发送的配置信息，所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。

26.一种终端，其特征在于，包括：

接收模块，用于接收连接管理消息、完整性保护信息、以及安全算法的配置信息，所述

连接管理消息为使用所述安全算法加密的，所述完整性保护信息为使用所述安全算法根据所述连接管理消息生成的，所述安全算法的配置信息未加密；

处理模块，用于根据所述安全算法的配置信息对所述连接管理消息进行完整性校验，并且基于所述安全算法的配置信息对所述连接管理消息进行解密，并根据解密结果执行连接管理过程。

27.根据权利要求26所述的终端，其特征在于，所述连接管理消息、完整性保护信息、以及安全算法的配置信息是通过一个高层数据单元传输的。

28.根据权利要求27所述的终端，其特征在于，所述安全算法的配置信息在PDCP层数据单元的包头，或者在PDCP层数据单元的所述完整性保护信息之后。

29.一种无线接入网RAN设备，其特征在于，包括：

处理模块，用于使用安全算法加密生成连接管理消息，使用所述安全算法根据所述连接管理消息生成完整性保护信息；

发送模块，用于发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

30.根据权利要求29所述的RAN设备，其特征在于，所述安全算法的配置信息包括安全算法的标识、密钥和密钥输入参数中的至少一种。

31.根据权利要求29或30所述的RAN设备，其特征在于，所述发送模块用于通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

32.根据权利要求31所述的RAN设备，其特征在于，所述高层数据单元包括PDCP层数据单元；

所述处理模块还用于将RRC层的所述连接管理消息设置为PDCP层数据单元的数据；将所述未加密的安全算法的配置信息设置在PDCP层数据单元的包头，或者设置在PDCP层数据单元的所述完整性保护信息之后。

连接管理方法、终端及无线接入网设备

技术领域

[0001] 本申请实施例涉及通信技术，尤其涉及一种连接管理方法、终端及无线接入网设备。

背景技术

[0002] 随着无线通信技术的不断发展，非激活态被提出，该非激活态是有别于连接(Connected)态和空闲(Idle)态的另一种状态，终端处于非激活态时，会保存终端自身的上下文信息和与核心网连接的信息，还会保存锚点无线接入网(RAN)设备配置的位置管理区域信息。该位置管理区域信息对应一个位置管理区，终端在该位置管理区内移动时无需通知锚点RAN设备，超出该位置管理区时需要通过消息通知锚点RAN设备。

[0003] 处于非激活态的终端需要进行连接管理时，可以向服务RAN设备发送连接管理请求消息，该连接管理请求消息包括终端的上下文标识，服务RAN设备根据该终端的上下文标识从锚点RAN设备处获取终端的上下文信息，服务RAN设备根据该终端的上下文信息确定终端使用的安全算法，服务RAN若不支持该安全算法，则服务RAN采用自身支持的安全算法发送的连接管理消息，不能被终端正确效验和解密，从而导致连接管理失败。

发明内容

[0004] 本申请实施例提供一种连接管理方法、终端及无线接入网设备，可以完成连接管理过程。

[0005] 第一方面，本申请实施例提供一种连接管理方法，包括：

[0006] 终端接收连接管理消息及完整性保护信息，所述完整性保护信息是根据所述连接管理消息使用第一安全算法生成的；

[0007] 所述终端根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验；

[0008] 所述终端根据第一完整性校验的结果，执行第二完整性校验，所述终端根据第二完整性效验的结果执行连接管理过程。

[0009] 本实现方式，终端在接收到RAN设备发送的连接管理消息和完整性保护信息后，使用终端自身保存的第一安全算法对接收到的连接管理消息进行第一完整性效验，并根据第一完整性效验的结果确定使用第二安全算法执行第二完整性效验，进而执行连接管理过程，从而实现正确效验与解密，确保连接管理的正常执行，完成连接管理过程。

[0010] 结合第一方面，在第一方面的一种可能的实现方式中，所述终端根据第一完整性校验的结果，执行第二完整性校验，具体可以包括：当所述第一完整性效验的结果为未通过时，所述终端获取所述连接管理消息中包括的第二安全算法的配置信息；所述终端根据所述第二安全算法的配置信息和所述完整性保护信息对所述连接管理消息进行第二完整性效验。

[0011] 本实现方式，终端在第一完整性效验的结果为未通过时，可以获知RAN设备使用的

安全算法与其自身的安全算法不同，且其接收到的连接管理消息未加密，终端获取该连接管理消息中携带的RAN设备使用的第二安全算法的配置信息，使用该第二安全算法配置信息进行第二完整性效验，从而实现正确效验，完成连接恢复过程。

[0012] 结合第一方面或者第一方面的一种可能的实现方式，在第一方面的另一种可能的实现方式中，所述终端根据所述第二完整性效验的结果执行连接管理过程，包括：当所述第二完整性效验的结果为通过时，执行连接管理过程。

[0013] 结合第一方面或者第一方面的任一种可能的实现方式，在第一方面的另一种可能的实现方式中，所述当所述第二完整性效验的结果为通过时，执行连接管理过程，包括：当所述第二完整性效验的结果为通过，且所述连接管理消息未携带第一类配置参数信息，执行连接管理过程，所述第一类配置参数信息为仅在加密的消息中发送的配置信息。

[0014] 本实现方式，当第二完整性效验通过时，终端还可以检验连接管理消息中是否携带第一类配置参数信息，当其未携带第一类配置参数信息时，执行连接管理过程。当其携带第一类配置参数信息时，则可以确定该连接管理消息为非法消息，可以终止连接管理过程。从而可以进一步提升连接管理的安全性。

[0015] 结合第一方面或者第一方面的任一种可能的实现方式，在第一方面的另一种可能的实现方式中，所述方法还包括：当所述第一次完整性效验的结果为通过时，所述终端使用所述第一安全算法对所述连接恢复消息进行解密，并根据解密后的连接恢复消息进行连接恢复。

[0016] 第二方面，本发明实施例提供一种连接管理方法，包括：

[0017] 无线接入网RAN设备获取终端使用的第一安全算法的配置信息；

[0018] 所述RAN设备根据所述配置信息判断所述RAN设备是否支持所述第一安全算法；

[0019] 所述RAN设备根据判断结果生成连接管理消息和完整性保护信息；

[0020] 所述RAN设备发送所述连接管理消息和所述完整性保护信息。

[0021] 本实现方式，RAN设备通过判断该RAN设备是否支持终端使用的第一安全算法，并根据判断结果生成连接管理消息和完整性保护信息，将该连接管理消息和完整性保护信息发送给终端，从而确保终端可以对接收到的连接管理消息进行正确效验与解密，完成连接管理过程。

[0022] 结合第二方面，在第二方面的一种可能的实现方式中，所述RAN设备根据判断结果生成连接管理消息和完整性保护信息，包括：当所述判断结果为所述RAN设备不支持所述第一安全算法时，所述RAN设备生成连接管理消息，并根据所述连接管理消息使用第二安全算法生成所述完整性保护信息，所述第二安全算法是所述RAN设备支持的；其中，所述连接管理消息包括所述第二安全算法的配置信息。

[0023] 本实现方式，当所述判断结果为所述RAN设备不支持所述第一安全算法时，RAN设备生成连接管理消息，该连接管理消息包括RAN设备使用的第二安全算法的配置信息，并根据所述连接管理消息使用第二安全算法生成所述完整性保护信息，将该连接管理消息和完整性保护信息发送给终端，从而实现终端从未加密的连接管理消息中获取RAN设备使用的第二安全算法的配置信息，从而完成连接管理过程。

[0024] 结合第二方面或者第二方面的一种可能的实现方式，在第二方面的另一种可能的实现方式中，所述连接管理消息还包括第二类配置参数信息，所述第二类配置参数信息为

被允许在加密和未加密的消息中发送的配置信息。

[0025] 结合第二方面或者第二方面的任一种可能的实现方式，在第二方面的另一种可能的实现方式中，所述RAN设备根据判断结果生成连接管理消息和完整性保护信息，包括：当所述RAN设备支持所述第一安全算法时，所述RAN设备使用所述第一安全算法加密生成所述连接管理消息，并根据所述连接管理消息使用第一安全算法生成所述完整性保护信息。

[0026] 结合第二方面或者第二方面的任一种可能的实现方式，在第二方面的另一种可能的实现方式中，所述连接管理消息携带第一类配置参数信息和第二类配置参数信息，所述第一类配置参数信息为被允许在加密的消息中发送的配置信息，所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。

[0027] 第三方面，本发明实施例提供一种连接管理方法，包括：

[0028] 终端接收连接管理消息、完整性保护信息、以及安全算法的配置信息，所述连接管理消息为使用所述安全算法加密的，所述完整性保护信息为使用所述安全算法根据所述连接管理消息生成的，所述安全算法的配置信息未加密；

[0029] 所述终端根据所述安全算法的配置信息对所述连接管理消息进行完整性校验，并且基于所述安全算法的配置信息对所述连接管理消息进行解密，并根据解密结果执行连接管理过程。

[0030] 本实现方式，终端接收连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息，终端可以从未加密的安全算法的配置信息获知RAN设备使用的安全算法的配置信息，从而正确对连接管理消息进行解密，确保连接管理的正常执行。

[0031] 结合第三方面，在第三方面的一种可能的实现方式中，所述连接管理消息、完整性保护信息、以及安全算法的配置信息是通过一个高层数据单元传输的。

[0032] 结合第三方面或第三方面的一种可能的实现方式，在第三方面的另一种可能的实现方式中，所述安全算法的配置信息在PDCP层数据单元的包头，或者在PDCP层数据单元的所述完整性保护信息之后。

[0033] 第四方面，本发明实施例提供一种连接管理方法，包括：

[0034] 无线接入网RAN设备使用安全算法加密生成连接管理消息，使用所述安全算法根据所述连接管理消息生成完整性保护信息；

[0035] 所述RAN设备发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

[0036] 本实现方式，RAN设备使用安全算法加密生成连接管理消息，使用安全算法根据所述连接管理消息生成完整性保护信息，将加密的连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息发送给终端，使得终端可以获知RAN设备使用的安全算法的配置信息，从而正确对连接管理消息进行解密，确保连接管理的正常执行。

[0037] 结合第四方面，在第四方面的一种可能的实现方式中，所述安全算法的配置信息包括安全算法的标识、密钥和密钥输入参数中的至少一种。

[0038] 结合第四方面或者第四方面的一种可能的实现方式，在第四方面的另一种可能的实现方式中，所述RAN设备发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息，包括：所述RAN设备通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

[0039] 本实现方式，RAN设备使用安全算法加密生成连接管理消息，使用安全算法根据所述连接管理消息生成完整性保护信息，将加密的连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息通过一个高层数据单元发送给终端，使得终端可以获知RAN使用的安全算法的配置信息，从而正确对连接管理消息进行解密，确保连接管理的正常执行。

[0040] 结合第四方面或者第四方面的任一种可能的实现方式，在第四方面的另一种可能的实现方式中，所述高层数据单元包括PDCP层数据单元；

[0041] 所述RAN设备通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息，包括：所述RAN设备将RRC层的所述连接管理消息设置为PDCP层数据单元的数据；所述RAN设备将所述未加密的安全算法的配置信息设置在PDCP层数据单元的包头，或者设置在PDCP层数据单元的所述完整性保护信息之后。

[0042] 第五方面，本发明实施例提供一种终端，该终端具有实现上述方法实施例中终端行为的功能。该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。该硬件或软件包括一个或多个与上述功能相对应的模块。

[0043] 第六方面，本发明实施例提供一种终端，包括：处理器、存储器和通信接口；该存储器用于存储计算机执行指令，当该终端运行时，该处理器执行该存储器存储的该计算机执行指令，以使该终端执行如上述第一方面任意一项或者第三方面任意一项的连接管理方法。

[0044] 第七方面，本发明实施例提供了一种计算机可读存储介质，用于储存为上述终端所用的计算机软件指令，当其在计算机上运行时，使得计算机可以执行上述第一方面中任意一项或者第三方面任意一项的连接管理方法。

[0045] 第八方面，本发明实施例提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面中任意一项或者第三方面任意一项的连接管理方法。

[0046] 另外，第五方面至第八方面中任一种设计方式所带来的技术效果可参见第一方面或第三方面中不同设计方式所带来的技术效果，此处不再赘述。

[0047] 第九方面，本发明实施例提供一种无线接入网设备，该无线接入网设备具有实现上述方法实施例中无线接入网设备行为的功能。该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。该硬件或软件包括一个或多个与上述功能相对应的模块。

[0048] 第十方面，本发明实施例提供一种无线接入网设备，包括：处理器、存储器和通信接口；该存储器用于存储计算机执行指令，当无线接入网设备运行时，该处理器执行该存储器存储的该计算机执行指令，以使该无线接入网设备执行如上述第二方面任意一项或者第四方面任意一项的连接管理方法。

[0049] 第十一方面，本发明实施例提供了一种计算机可读存储介质，用于储存为上述无线接入网设备所用的计算机软件指令，当其在计算机上运行时，使得计算机可以执行上述第二方面中任意一项或者第四方面任意一项的连接管理方法。

[0050] 第十二方面，本发明实施例提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面中任意一项或者第三方面任意一项的连接管理方法。

[0051] 另外，第九方面至第十三方面中任一种设计方式所带来的技术效果可参见第二方

面或第四方面中不同设计方式所带来的技术效果，此处不再赘述。

[0052] 第十三方面，本发明实施例提供了一种运行指令的芯片，该芯片用于执行以下步骤：

[0053] 根据第一安全算法和完整性保护信息对连接管理消息进行第一完整性效验；根据第一完整性校验的结果，执行第二完整性校验，根据第二完整性效验的结果执行连接管理过程，其中，所述连接管理消息及所述完整性保护信息来自于无线接入网设备，所述完整性保护信息是无线接入网设备根据所述连接管理消息使用第一安全算法生成的。

[0054] 其技术效果可以参见上述第一方面或第二方面中不同设计方式所带来的技术效果，此处不再赘述。

[0055] 第十四方面，本发明实施例提供了一种运行指令的芯片，该芯片用于执行以下步骤：

[0056] 根据安全算法的配置信息对连接管理消息进行完整性校验，并且基于所述安全算法的配置信息对所述连接管理消息进行解密，并根据解密结果执行连接管理过程，所述连接管理消息、完整性保护信息、以及安全算法的配置信息来自于无线接入网设备，所述连接管理消息为使用所述安全算法加密的，所述完整性保护信息为使用所述安全算法根据所述连接管理消息生成的，所述安全算法的配置信息未加密。

[0057] 其技术效果可以参见上述第三方面或第四方面中不同设计方式所带来的技术效果，此处不再赘述。

[0058] 本文所涉及的连接管理消息指网络侧和终端之间进行连接管理的消息，其具体可以是连接恢复消息，连接挂起消息，连接继续消息，连接激活消息，连接重激活消息，连接建立消息，连接重建立消息，连接重配置消息等。

[0059] 本文所涉及的非激活态具体指，终端保存其自身的上下文信息，并且可以执行基于小区的重选操作。同时，终端的连接信息保存在锚点RAN设备，终端的连接信息包括终端的上下文信息以及核心网连接信息。

[0060] 通常，非激活态的终端会和空闲Idle态的终端一样进行小区重选。当终端处于非激活态时，终端保存锚点RAN设备配置的位置管理区域信息，终端移动出该位置管理区域信息对应的位置管理区域时，需要通知锚点RAN设备。

[0061] 本申请实施例连接管理方法、终端及无线接入网设备，通过RAN设备判断该RAN设备是否支持终端使用的第一安全算法，并根据判断结果生成连接管理消息和完整性保护信息，将该连接管理消息和完整性保护信息发送给终端，终端在接收到RAN设备发送的连接管理消息和完整性保护信息后，使用终端自身保存的第一安全算法对接收到的连接管理消息进行第一完整性效验，并根据第一完整性效验的结果，使用第二安全算法执行第二完整性效验，进而执行连接管理过程，从而实现正确效验与解密，确保连接管理的正常执行。其中，即使终端和RAN设备使用的加密算法不同，也可以实现终端的连接管理的正常执行。

附图说明

[0062] 图1为本申请实施例一种应用场景的示意图；

[0063] 图2为本申请实施例的一种连接管理方法的流程图；

[0064] 图3为本申请实施例的另一种连接管理方法的流程图；

[0065] 图4为本申请实施例另一种连接管理方法的流程图；

[0066] 图5为本申请实施例另一种连接管理方法的流程图；

[0067] 图6为本申请实施例一种PDCP数据单元的示意图。

[0068] 图7为本申请实施例一种终端的结构示意图；

[0069] 图8为本申请实施例一种无线接入网RAN设备的结构示意图；

[0070] 图9为本申请实施例另一种终端的结构示意图；

[0071] 图10为本申请实施例另一种无线接入网RAN设备的结构示意图。

具体实施方式

[0072] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述。

[0073] 图1为本申请实施例一种应用场景的示意图，如图1所示，本实施例的应用场景可以包括：核心网设备1、锚点无线接入网(Radio Access Network，RAN)设备2、RAN设备3以及终端4，其中，核心网设备用于负责无线资源的管理、无线连接的建立、业务服务质量(Quality of Service，简称QoS)保证和最终的资源释放等。该核心网设备可以为移动性管理实体(Mobility Management Entity，简称MME)、网关设备(Gateway，简称GW)等，也可以为5G核心网络侧(5G Core network)的功能实体，例如接入与移动性管理功能实体(Core Access and Mobility Management Function，AMF)、会话管理功能实体(Session Management Function，SMF)等，当然也可以是其他核心网设备，此处仅为示意性说明。上述锚点RAN设备2保留有终端4的上下文信息和核心网接口信息，终端4可以通过RAN设备3与锚点RAN设备2进行连接，并通过该锚点RAN设备2与核心网侧建立通信连接。上述锚点RAN设备2也可以称之为源RAN设备，上述RAN设备3也可以称之为新的RAN设备、服务RAN设备等。本申请实施例的终端4处于非激活态，处于非激活态的终端4需要进行连接管理时，可以通过本申请实施例的连接管理方法，实现终端4的连接管理，避免由于RAN设备3不支持终端4的安全算法而导致连接管理失败。本申请实施例的连接管理方法的具体实现方式可以参见下述实施例的解释说明。

[0074] 其中，连接管理具体可以包括：为空闲态终端建立连接，为非激活态终端恢复连接，或者为连接态终端更新连接使用等。当然可以理解的，还可以是其他具体操作，此处不一一举例说明。

[0075] 需要说明的是，本文所涉及的无线接入网(Radio Access Network，RAN)设备，是一种将终端接入到无线网络的设备，可以是全球移动通讯(Global System of Mobile communication，GSM)或码分多址(Code Division Multiple Access，CDMA)中的基站(Base Transceiver Station，BTS)，也可以是宽带码分多址(Wideband Code Division Multiple Access，WCDMA)中的基站(NodeB，NB)，还可以是长期演进(Long Term Evolution，LTE)中的演进型基站(Evolutional Node B，eNB或eNodeB)，或者中继站或接入点，或者未来5G网络中的基站等，在此并不限定。

[0076] 本文所涉及的终端，指向用户提供语音和/或数据连通性的设备(device)，包括无线终端或有线终端。无线终端可以是具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备，经无线接入网与一个或多个核心网进行通信的移动终端。例如，无

线终端可以是移动电话(或称为“蜂窝”电话)和具有移动终端的计算机。又如,无线终端也可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置。再如,无线终端可以为用户设备(User Equipment,简称UE)的一部分。

[0077] 本文所涉及的安全算法包括加密算法或完整性保护算法,也可以包括加密算法和完整性保护算法。该加密算法可以包括:EPS Encryption Algorithm 1(EEA1)、EEA2、EEA3等,该完整性保护算法可以包括EPS Integrity Algorithm 1(EIA1)、EIA2等。其中,EIA1是基于SNOW 3G算法。当所述安全算法包括加密算法和完整性保护算法时,所述加密算法和完整性保护算法可以存在对应关系。例如加密算法1对应于完整性保护算法1;加密算法2对应于完整性保护算法2。使用安全算法进行加密可以包括:使用安全算法中的加密算法进行加密。使用安全算法进行完整性保护可以包括:使用安全算法中的完整性保护算法进行完整性保护。

[0078] 本文所涉及的“第一安全算法”和“第二安全算法”仅用于区分不同的安全算法。即二者采用的加密算法和/或完整性保护算法不同。

[0079] 本文所涉及的“完整性效验”具体指终端根据接收到的消息和安全算法配置信息计算出X-MAC,将该X-MAC与接收到的完整性效验信息进行比较,如果相同,则完整性效验通过,否则,完整性效验不通过。

[0080] 本文所涉及的“第一完整性效验”和“第二完整性效验”仅用于区分使用不同的安全算法。

[0081] 本文所涉及的“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这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

[0082] 图2为本申请实施例的一种连接管理方法的流程图,如图2所示,本实施例涉及RAN设备和终端,该RAN设备具体可以是图1所示的RAN设备3,本实施例的方法可以包括:

[0083] 步骤101、RAN设备获取终端使用的第一安全算法的配置信息。

[0084] 其中,在步骤101之前,终端可以向RAN设备发送连接管理请求消息。所述连接恢复请求消息可以用于请求RAN设备为该终端管理连接。RAN设备接收该连接管理请求消息,该连接管理请求消息可以包括该终端的上下文标识,RAN设备根据该终端的上下文标识从锚点RAN设备处获取该终端的上下文信息,RAN设备从该终端的上下文信息中获取该终端使用的第一安全算法的配置信息。

[0085] 具体的一种可实现方式,该终端的上下文标识可以包括锚点RAN设备的标识和该终端的标识,RAN设备可以根据该锚点RAN设备的标识,确定向该锚点RAN设备请求该终端的标识对应的上下文信息,该锚点RAN设备将该终端的上下文信息发送给RAN设备,其中,该上下文信息可以包括终端使用的第一安全算法的配置信息,RAN设备从该终端的上下文信息中获取第一安全算法的配置信息,该第一安全算法的配置信息可以包括第一安全算法的标识、密钥和密钥输入参数中的至少一种。该第一安全算法的配置信息可以是锚点RAN设备配置给终端的。

[0086] 步骤102、所述RAN设备根据所述配置信息判断所述RAN设备是否支持所述第一安全算法。

[0087] 具体的,RAN设备可以根据步骤101中获取的配置信息确定该配置信息对应的第一

安全算法，进而判断其自身是否支持该第一安全算法。

[0088] 其中，RAN设备判断是否支持第一安全算法具体可以包括：RAN设备判断是否支持第一安全算法所包括的加密算法和/或完整性保护算法，即判断是否支持第一安全算法的加密算法、或者判断是否支持第一安全算法的完整性保护算法、或者判断是否支持第一安全算法的加密算法和完整性保护算法，其具体实现方式可以根据需求进行灵活设置。

[0089] 步骤103、所述RAN设备根据判断结果生成连接管理消息和完整性保护信息。

[0090] 其中，完整性保护信息为对连接管理消息进行完整性保护生成的。

[0091] 具体的，上述步骤102的判断结果包括两种：支持和不支持。

[0092] 当判断结果为不支持时，步骤103的具体实现方式可以为，RAN设备生成连接管理消息，该连接管理消息未加密，且该连接管理消息携带第二安全算法的配置信息，该第二安全算法为RAN设备支持的安全算法，并且RAN设备根据该连接管理消息使用第二安全算法进行完整性保护生成完整性保护信息。

[0093] 当判断结果为支持时，步骤103的具体实现方式可以为，RAN设备使用第一安全算法加密生成连接管理消息，即该连接管理消息为加密的消息，并根据该连接管理消息使用第一安全算法进行完整性保护生成完整性保护信息。

[0094] 步骤104、所述RAN设备发送所述连接管理消息和所述完整性保护信息。

[0095] 具体的，所述RAN设备向终端发送所述连接管理消息和所述完整性保护信息，终端接收RAN设备发送的所述连接管理消息和所述完整性保护信息。

[0096] 步骤105、所述终端根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验。

[0097] 其中，终端在接收到所述连接管理消息和所述完整性保护信息后，使用其自身支持的第一安全算法对该连接管理消息进行完整性效验，即根据接收到的完整性保护信息使用完整性保护算法来效验接收到的连接管理消息的完整性。

[0098] 步骤106、所述终端根据第一完整性校验的结果，执行第二完整性校验。

[0099] 具体的，第一完整性效验的结果包括通过和不通过。其中一种可实现方式为，当第一完整性效验的结果为通过时，则跳过执行第二完整性效验。当第一完整性效验的结果为不通过时，执行步骤106，即执行第二完整性效验。其中终端根据第一完整性效验的结果为不通过，可以获知RAN设备使用的安全算法与其自身的安全算法不同，进而执行第二完整性效验。

[0100] 步骤107、所述终端根据第二完整性效验的结果执行连接管理过程。

[0101] 其中，第一完整性效验的结果为通过时，终端根据该第一完整性效验的结果可以确定终端接收到的连接管理消息加密，并使用第一安全算法对该连接管理消息进行解密，根据解密后的连接管理消息进行连接管理。第一完整性效验的结果为不通过时，步骤106后，执行步骤107，终端根据该第一完整性效验的结果可以确定终端接收到的连接管理消息未加密，且RAN设备与终端使用的安全算法不同，终端从未加密的连接管理消息中获取RAN设备使用的第二安全算法的配置信息，并根据该第二安全算法的配置信息和完整性保护信息对连接管理消息进行第二完整性效验，在第二完整性效验的结果为通过时，根据连接管理消息执行连接管理过程。

[0102] 本实施例，通过RAN设备判断该RAN设备是否支持终端使用的第一安全算法，并根

据判断结果生成连接管理消息和完整性保护信息，将该连接管理消息和完整性保护信息发送给终端，终端在接收到RAN设备发送的连接管理消息和完整性保护信息后，使用终端自身保存的第一安全算法对接收到的连接管理消息进行第一完整性效验，并根据第一完整性效验的结果，使用第二安全算法执行第二完整性效验，进而执行连接管理过程，从而实现正确效验与解密，确保连接管理的正常执行。其中，即使终端和RAN设备使用的加密算法不同，也可以实现终端的连接管理的正常执行。

[0103] 下面采用一个具体的实施例，对图2所示方法实施例的技术方案进行详细说明。

[0104] 图3为本申请实施例的另一种连接管理方法的流程图，如图3所示，本实施例的方法可以包括：

[0105] 步骤201、锚点RAN设备向终端配置该终端使用的第一安全算法。

[0106] 具体的，锚点RAN设备可以通过向终端发送第一安全算法的配置信息，从而实现向终端配置该终端使用的第一安全算法。其中，第一安全算法的配置信息的具体解释说明可以参见上述图2所示实施例的解释说明，此处不再赘述。终端使用给第一安全算法对接收或发送的数据或者信令消息进行完整性保护效验、加解密操作。

[0107] 步骤202、锚点RAN设备控制终端进入非激活态。

[0108] 具体的，锚点RAN设备向终端发送状态控制命令，以指示该终端进入非激活(Inactive)态。其中，锚点RAN设备在实施步骤202之前或者同时，向终端发送终端的上下文信息，该终端的上下文信息包括终端的上下文标识。该终端的上下文标识的具体解释说明可以参见上述图2所示实施例的解说说明，此处不再赘述。

[0109] 步骤203、终端向RAN设备发送连接管理请求消息。

[0110] RAN设备接收终端发送的连接管理请求消息，该连接管理请求消息携带该终端的上下文标识。

[0111] 具体的，终端在有数据需要发送时，可以向RAN设备发送连接管理请求消息，以便RAN设备为该终端管理连接。

[0112] 步骤204、RAN设备根据该终端的上下文标识从锚点RAN设备获取该终端的上下文信息，并从该终端的上下文信息中获取该终端使用的第一安全算法的配置信息。

[0113] 步骤205、RAN设备根据第一安全算法的配置信息判断RAN设备是否支持第一安全算法，当RAN设备不支持第一安全算法时，执行步骤206，当RAN设备支持第一安全算法时，则执行步骤206’。

[0114] 步骤206、RAN设备生成连接管理消息，并根据连接管理消息使用第二安全算法生成完整性保护信息。

[0115] 其中，第二安全算法是RAN设备支持的。步骤206生成的连接管理消息未加密，且该连接管理消息携带RAN设备使用的第二安全算法的配置信息。

[0116] 其中，该连接管理消息还可以携带第二类配置参数，所述第二类配置参数信息为被允许在加密或者未加密的消息中发送的配置信息。举例而言，该第二类配置参数具体可以是物理资源配置信息。

[0117] 步骤206’、RAN设备使用第一安全算法加密生成连接管理消息，并根据连接管理消息使用第一安全算法生成完整性保护信息。

[0118] 其中，步骤206’生成的连接管理消息为加密的消息。

[0119] 其中，该连接管理消息可以携带第一类配置参数信息和第二类配置参数信息，所述第一类配置参数信息为被允许在加密的消息中发送的配置信息，所述第二类配置参数信息为被允许在加密和未加密的消息中发送的配置信息。其中，第二类配置参数信息的具体解释说明可以参见步骤206的解释，此处不再赘述，第一类配置参数信息具体可以是逻辑信道的配置信息。

[0120] 由此可见，本申请实施例将连接管理消息中携带的配置参数分为两类，一类是需要加密才可以发送的参数信息，即第一类配置参数信息，另一类是可以不加密发送的参数信息，即第二类配置参数信息。

[0121] 步骤207、RAN设备向终端发送连接管理消息和完整性保护信息。

[0122] 其中，该连接管理消息和完整性保护信息是步骤206或者步骤206’生成的。

[0123] 终端接收RAN设备发送的连接管理消息和完整性保护信息。

[0124] 步骤208、终端根据第一安全算法和完整性保护信息对接收到的连接管理消息进行第一完整性效验。

[0125] 当第一完整性效验未通过时，执行步骤209，当第一完整性效验通过时，执行步骤210。

[0126] 具体的，第一完整性效验的结果为不通过时，则执行步骤209，第一完整性效验的结果为通过时，执行步骤210。

[0127] 步骤209、终端获取连接管理消息中包括的第二安全算法的配置信息，根据第二安全算法的配置信息和完整性保护信息对连接管理消息进行第二完整性效验，所述终端根据所述第二完整性效验的结果执行连接管理过程。

[0128] 具体的，第一完整性效验的结果为不通过时，终端可以根据该结果确定接收到的连接管理消息未加密，则获取该连接管理消息中包括的第二安全算法的配置信息。使用该第二安全算法进行第二完整性效验，当第二完整性效验通过时，执行连接管理过程。其中，需要说明的是，连接管理消息未加密，其携带第二类配置参数信息，对于第一类参数配置信息，RAN设备可以使用另一条加密消息发送给终端，终端可以使用连接管理消息中包括的第二安全算法的配置信息解密获取第一类参数配置信息。

[0129] 可选的，当第二完整性效验通过时，终端还可以检验连接管理消息中是否携带第一类配置参数信息，当其未携带第一类配置参数信息时，执行连接管理过程。当其携带第一类配置参数信息时，则可以确定该连接管理消息为非法消息，可以终止连接管理过程。从而可以进一步提升连接管理的安全性。

[0130] 步骤210、所述终端使用所述第一安全算法对所述连接管理消息进行解密，并根据解密后的连接管理消息进行连接管理。

[0131] 本实施例，通过RAN设备判断该RAN设备是否支持终端使用的第一安全算法，并根据判断结果生成连接管理消息和完整性保护信息，将该连接管理消息和完整性保护信息发送给终端，终端在接收到RAN设备发送的连接管理消息和完整性保护信息后，使用终端自身保存的第一安全算法对接收到的连接管理消息进行第一完整性效验，并当第一完整性效验的结果为通过时，使用第二安全算法执行第二完整性效验，进而执行连接管理过程，从而实现正确效验与解密，确保连接管理的正常执行。其中，即使终端和RAN设备使用的加密算法不同，也可以实现终端的连接管理的正常执行。

[0132] 与上述实施例不同，本申请还提供另一种连接管理方法，以实现与上述实施例相同的技术效果，具体可以参见下述实施例的具体解释说明。

[0133] 图4为本申请实施例另一种连接管理方法的流程图，如图4所示，本实施例的方法可以包括：

[0134] 步骤301、RAN设备使用安全算法加密生成连接管理消息，使用安全算法根据连接管理消息生成完整性保护信息。

[0135] 步骤302、RAN设备发送连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息。

[0136] 终端接收RAN设备发送的连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息。

[0137] 步骤303、终端根据安全算法的配置信息对连接管理消息进行完整性校验，并且基于安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程。

[0138] 上述安全算法的配置信息可以包括安全算法的标识、密钥和密钥输入参数中的至少一种。

[0139] 可选的，上述连接管理消息、完整性保护信息、以及安全算法的配置信息是通过一个高层数据单元传输的。其中，高层包括物理层之外的层，例如可以包括以下任意一项：业务数据适配协议(Service Data Adaptation Protocol，SDAP)层、分组数据汇聚协议(Packet Data Convergence Protocol，PDCP)层、MAC层以及RLC层。

[0140] 可选的，高层数据单元为MAC层数据单元时，上述安全算法的配置信息可以通过MAC层包头、或者MAC层控制单元、或者MAC逻辑信道进行传输。

[0141] 可选的，高层数据单元为PDCP层数据单元时，上述安全算法的配置信息可以通过PDCP层包头、或者PDCP层控制单元、或者PDCP层包尾传输。

[0142] 本实施例，通过RAN设备使用安全算法加密生成连接管理消息，使用安全算法根据所述连接管理消息生成完整性保护信息，将加密的连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息发送给终端，使得终端可以获知RAN使用的安全算法的配置信息，从而正确对连接管理消息进行解密，确保连接管理的正常执行。其中，即使终端和RAN设备使用的加密算法不同，也可以实现终端的连接管理的正常执行。

[0143] 下面采用一个具体的实施例，对图4所示方法实施例的技术方案进行详细说明。

[0144] 图5为本申请实施例另一种连接管理方法的流程图，图6为本申请实施例一种PDCP数据单元的示意图，如图5所示，本实施例的方法可以包括：

[0145] 步骤401、锚点RAN设备向终端配置该终端使用的第一安全算法。

[0146] 步骤402、锚点RAN设备控制终端进入非激活态。

[0147] 步骤403、终端向RAN设备发送连接管理请求消息。

[0148] 步骤404、RAN设备根据该终端的上下文标识从锚点RAN设备获取该终端的上下文信息，并从该终端的上下文信息中获取该终端使用的第一安全算法的配置信息。

[0149] 上述步骤401至步骤404的具体解释说明可以参见图3所示实施例的步骤201至步骤204，此处不再赘述。

[0150] 步骤405、RAN设备根据第一安全算法的配置信息判断RAN设备是否支持第一安全算法，当RAN设备不支持第一安全算法时，则执行步骤406，当RAN设备支持第一安全算法时，

则执行步骤406’。

[0151] 步骤406、RAN设备使用第二安全算法加密生成连接管理消息，使用第二安全算法根据连接管理消息生成完整性保护信息。

[0152] 步骤407、RAN设备发送连接管理消息、完整性保护信息、以及未加密的第二安全算法的配置信息。

[0153] 终端接收RAN设备发送的连接管理消息、完整性保护信息、以及未加密的第二安全算法的配置信息。

[0154] 一种可实现方式，RAN设备在通过步骤405获知RAN设备不支持终端使用的第一安全算法时，该RAN设备确定需要更新终端的安全算法的配置信息，则RAN设备的RRC层生成连接管理消息，将该连接管理消息封装在PDCP层的负载中，并在PDCP层的完整性保护信息之后增加携带第二安全算法的配置信息的字段。该PDCP层数据单元具体可以如图6所示，通过该PDCP层数据单元向终端发送连接管理消息、完整性保护信息、以及未加密的第二安全算法的配置信息。

[0155] 步骤408、终端根据第二安全算法的配置信息对连接管理消息进行完整性校验，并且基于第二安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程。

[0156] 具体的，以上述PDCP层数据单元为例做进一步举例说明，终端接收到PDCP层数据单元后，提取其中的第二安全算法的配置信息，使用该第二安全算法对连接管理消息进行完整性效验和解密，进而执行连接管理过程。

[0157] 步骤406’、RAN设备使用第一安全算法加密生成连接管理消息，并根据连接管理消息使用第一安全算法生成完整性保护信息。

[0158] 步骤407’、RAN设备发送连接管理消息和完整性保护信息。

[0159] 终端接收RAN设备发送的连接管理消息和完整性保护信息。

[0160] 步骤408’、终端使用其自身的第一安全算法对连接管理消息进行完整性校验，并且基于第一安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程。

[0161] 本实施例，通过RAN设备使用第二安全算法加密生成连接管理消息，使用第二安全算法根据所述连接管理消息生成完整性保护信息，将加密的连接管理消息、完整性保护信息、以及未加密的第二安全算法的配置信息发送给终端，使得终端可以获知RAN使用的第二安全算法的配置信息，从而正确对连接管理消息进行解密，确保连接管理的正常执行。其中，即使终端和RAN设备使用的加密算法不同，也可以实现终端的连接管理的正常执行。

[0162] 图7为本申请实施例一种终端的结构示意图，如图7所示，本实施例的装置可以包括：接收模块11和处理模块12，其中，接收模块11用于接收连接管理消息及完整性保护信息，所述完整性保护信息是根据所述连接管理消息使用第一安全算法生成的，处理模块12用于根据所述第一安全算法和所述完整性保护信息对所述连接管理消息进行第一完整性效验，处理模块12还用于根据第一完整性校验的结果，执行第二完整性校验，根据第二完整性效验的结果执行连接管理过程。

[0163] 可选的，所述处理模块12用于根据第一完整性校验的结果，执行第二完整性校验，具体可以包括：当所述第一完整性效验的结果为未通过时，获取所述连接管理消息中包括

的第二安全算法的配置信息;根据所述第二安全算法的配置信息和所述完整性保护信息对所述连接管理消息进行第二完整性效验。

[0164] 可选的,所述处理模块12用于根据所述第二完整性效验的结果执行连接管理过程。

[0165] 可选的,所述处理模块12用于根据所述第二完整性效验的结果执行连接管理过程,具体可以包括:当所述第二完整性效验的结果为通过时,执行连接管理过程。

[0166] 可选的,所述处理模块12用于当所述第二完整性效验的结果为通过时,执行连接管理过程,具体可以包括:当所述第二完整性效验的结果为通过时,且所述连接管理消息未携带第一类配置参数信息,执行连接管理过程,所述第一类配置参数信息为仅在加密的消息中发送的配置信息。

[0167] 可选的,所述处理模块12还用于:当所述第一次完整性效验的结果为通过时,使用所述第一安全算法对所述连接管理消息进行解密,并根据解密后的连接管理消息进行连接管理。

[0168] 可选的,本申请实施例的终端还可以包括存储模块,该存储模块用于存储终端的程序代码和数据。

[0169] 可选的,本申请实施例的终端还可以包括发送模块,该发送模块用于发送消息、数据等。

[0170] 本实施例的装置,可以用于执行图2或图3所示方法实施例的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0171] 图8为本申请实施例一种无线接入网RAN设备的结构示意图,如图8所示,本实施例的装置可以包括:处理模块21和发送模块22,其中,处理模块21用于确定终端使用的第一安全算法的配置信息,处理模块21还用于根据所述配置信息判断所述RAN设备是否支持所述第一安全算法,处理模块12还用于根据判断结果生成连接管理消息和完整性保护信息,发送模块22用于发送所述连接管理消息和所述完整性保护信息。

[0172] 可选的,所述处理模块21用于根据判断结果生成连接管理消息和完整性保护信息,具体可以包括:当所述判断结果为所述RAN设备不支持所述第一安全算法时,生成连接管理消息,并根据所述连接管理消息使用第二安全算法生成所述完整性保护信息,所述第二安全算法是所述RAN设备支持的;其中,所述连接管理消息包括所述第二安全算法的配置信息。

[0173] 可选的,所述连接管理消息还包括第二类配置参数信息,所述第二类配置参数信息为允许在加密或者未加密的消息中发送的配置信息。

[0174] 可选的,所述处理模块21用于根据判断结果生成连接管理消息和完整性保护信息,具体可以包括:当所述RAN设备支持所述第一安全算法时,使用所述第一安全算法加密生成所述连接管理消息,并根据所述连接管理消息使用第一安全算法生成所述完整性保护信息。

[0175] 可选的,所述连接管理消息携带第一类配置参数信息和第二类配置参数信息,所述第一类配置参数信息为允许在加密的消息中发送的配置信息,所述第二类配置参数信息为允许在加密或者未加密的消息中发送的配置信息。

[0176] 可选的,本申请实施例的RAN设备还可以包括存储模块,该存储模块用于存储终端

的程序代码和数据。

[0177] 可选的，本申请实施例的RAN设备还可以包括接收模块，该接收模块用于接收消息、数据等。

[0178] 本实施例的装置，可以用于执行图2或图3所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0179] 图9为本申请实施例另一种终端的结构示意图，如图9所示，本实施例的装置可以包括：接收模块31和处理模块32，其中，接收模块31用于接收连接管理消息、完整性保护信息、以及安全算法的配置信息，所述连接管理消息为使用所述安全算法加密的，所述完整性保护信息为使用所述安全算法根据所述连接管理消息生成的，所述安全算法的配置信息未加密，处理模块32用于根据所述安全算法的配置信息对所述连接管理消息进行完整性校验，并且基于所述安全算法的配置信息对所述连接管理消息进行解密，并根据解密结果执行连接管理过程。

[0180] 可选的，所述连接管理消息、完整性保护信息、以及安全算法的配置信息是通过一个高层数据单元传输的。

[0181] 可选的，所述安全算法的配置信息在PDCP层数据单元的包头，或者在PDCP层数据单元的所述完整性保护信息之后。

[0182] 可选的，本申请实施例的终端还可以包括存储模块，该存储模块用于存储终端的程序代码和数据。

[0183] 可选的，本申请实施例的终端还可以包括发送模块，该发送模块用于发送消息、数据等。

[0184] 本实施例的装置，可以用于执行图4或图5所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0185] 图10为本申请实施例另一种无线接入网RAN设备的结构示意图，如图10所示，本实施例的装置可以包括：处理模块41和发送模块42，其中，处理模块41用于使用安全算法加密生成连接管理消息，使用所述安全算法根据所述连接管理消息生成完整性保护信息，发送模块42用于发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

[0186] 可选的，所述安全算法的配置信息包括安全算法的标识、密钥和密钥输入参数中的至少一种。

[0187] 可选的，所述发送模块用于通过一个高层数据单元发送所述连接管理消息、所述完整性保护信息、以及未加密的所述安全算法的配置信息。

[0188] 可选的，所述高层数据单元包括PDCP层数据单元；所述处理模块41还用于将RRC层的所述连接管理消息设置为PDCP层数据单元的数据；将所述未加密的安全算法的配置信息设置在PDCP层数据单元的包头，或者设置在PDCP层数据单元的所述完整性保护信息之后。

[0189] 可选的，本申请实施例的RAN设备还可以包括存储模块，该存储模块用于存储终端的程序代码和数据。

[0190] 可选的，本申请实施例的RAN设备还可以包括接收模块，该接收模块用于接收消息、数据等。

[0191] 本实施例的装置，可以用于执行图4或图5所示方法实施例的技术方案，其实现原

理和技术效果类似,此处不再赘述。

[0192] 需要说明的是,本申请实施例中的接收模块11可以与终端的接收器对应,也可以对应终端的收发器。该终端还可以包括发送模块,发送模块可以与终端的发送器对应,也可以对应终端的收发器。处理模块12可以与终端的处理器对应,这里处理器可以是一个中央处理器(Central Processing Unit,CPU),或者是特定集成电路(Application Specific Integrated Circuit,ASIC),或者完成实施本申请实施例的一个或多个集成电路。终端还可以包括存储器,存储器用于存储指令代码,处理器调用存储器的指令代码,控制本申请实施例中的接收模块11执行上述操作。

[0193] 需要说明的是,本申请实施例中的发送模块22可以与RAN设备的发送器对应,也可以对应RAN设备的收发器。该RAN设备还可以包括接收模块,接收模块可以与RAN设备的接收器对应,也可以对应RAN设备的收发器。处理模块21可以与RAN设备的处理器对应,这里处理器可以是一个CPU,或者是ASIC,或者完成实施本申请实施例的一个或多个集成电路。RAN设备还可以包括存储器,存储器用于存储指令代码,处理器调用存储器的指令代码,控制本申请实施例中的发送模块22执行上述操作。

[0194] 需要说明的是,本申请实施例中的接收模块31可以与终端的接收器对应,也可以对应终端的收发器。该终端还可以包括发送模块,发送模块可以与终端的发送器对应,也可以对应终端的收发器。处理模块32可以与终端的处理器对应,这里处理器可以是一个中央处理器(Central Processing Unit,CPU),或者是特定集成电路(Application Specific Integrated Circuit,ASIC),或者完成实施本申请实施例的一个或多个集成电路。终端还可以包括存储器,存储器用于存储指令代码,处理器调用存储器的指令代码,控制本申请实施例中的接收模块31执行上述操作。

[0195] 需要说明的是,本申请实施例中的发送模块42可以与RAN设备的发送器对应,也可以对应RAN设备的收发器。该RAN设备还可以包括接收模块,接收模块可以与RAN设备的接收器对应,也可以对应RAN设备的收发器。处理模块41可以与RAN设备的处理器对应,这里处理器可以是一个CPU,或者是ASIC,或者完成实施本申请实施例的一个或多个集成电路。RAN设备还可以包括存储器,存储器用于存储指令代码,处理器调用存储器的指令代码,控制本申请实施例中的发送模块42执行上述操作。

[0196] 当本发明实施例的连接管理方法的至少一部分功能通过软件实现时,本发明实施例还提供一种计算机可读存储介质,计算机可读存储介质用于储存为上述终端所用的计算机软件指令,当其在计算机上运行时,使得计算机可以执行上述方法实施例中各种可能的连接管理方法。在计算机上加载和执行所述计算机执行指令时,可全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,所述传输可以通过无线(例如蜂窝通信、红外、短距离无线、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。所述计算机可读存储介质可以是计算机能够存取的任何可用介质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。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

[0197] 当本发明实施例的连接管理方法的至少一部分功能通过软件实现时,本发明实施

例还提供一种计算机可读存储介质，计算机可读存储介质用于储存为上述RAN设备所用的计算机软件指令，当其在计算机上运行时，使得计算机可以执行上述方法实施例中各种可能的连接管理方法。在计算机上加载和执行所述计算机执行指令时，可全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，所述传输可以通过无线(例如蜂窝通信、红外、短距离无线、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。所述计算机可读存储介质可以是计算机能够存取的任何可用介质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。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如SSD)等。

[0198] 此外，本发明实施例还提供一种包含指令的计算机程序产品，即软件产品，当其在计算机上运行时，使得计算机执行上述方法实施例中各种可能的连接管理方法。其实现原理和技术效果类似，此处不再赘述。

[0199] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0200] 最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

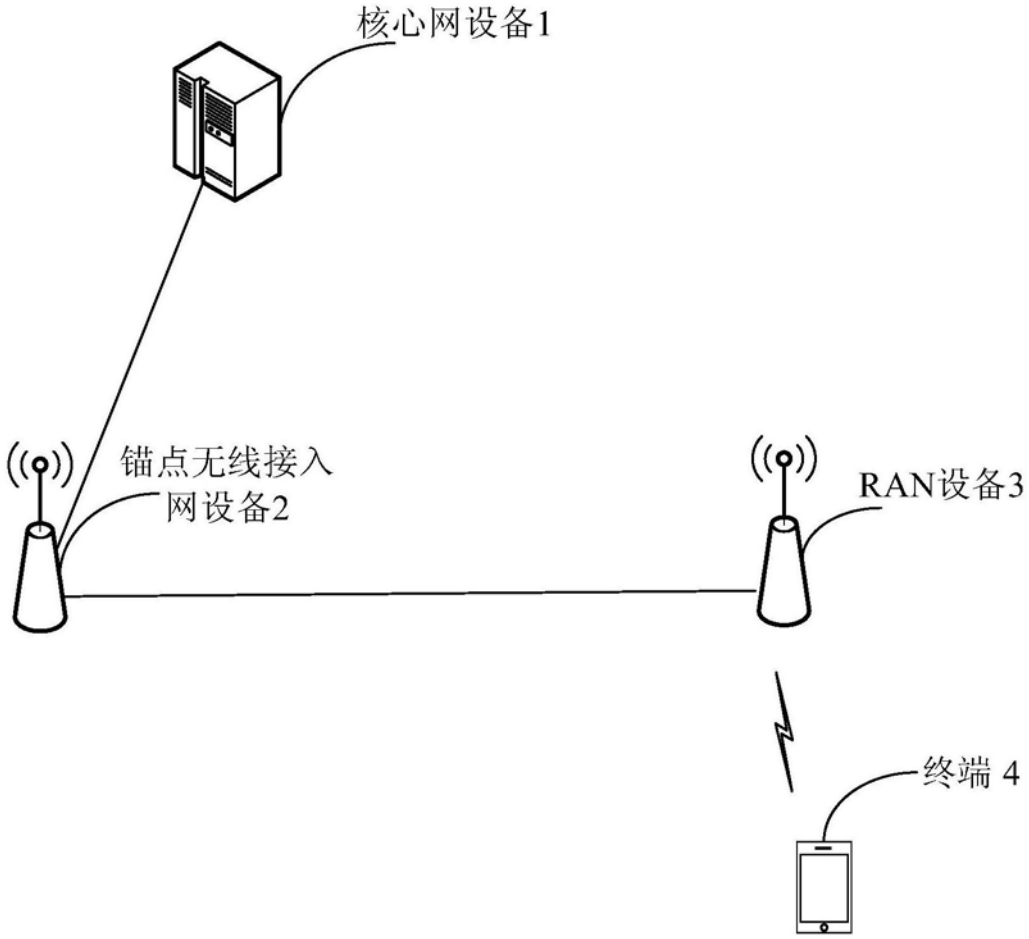


图1

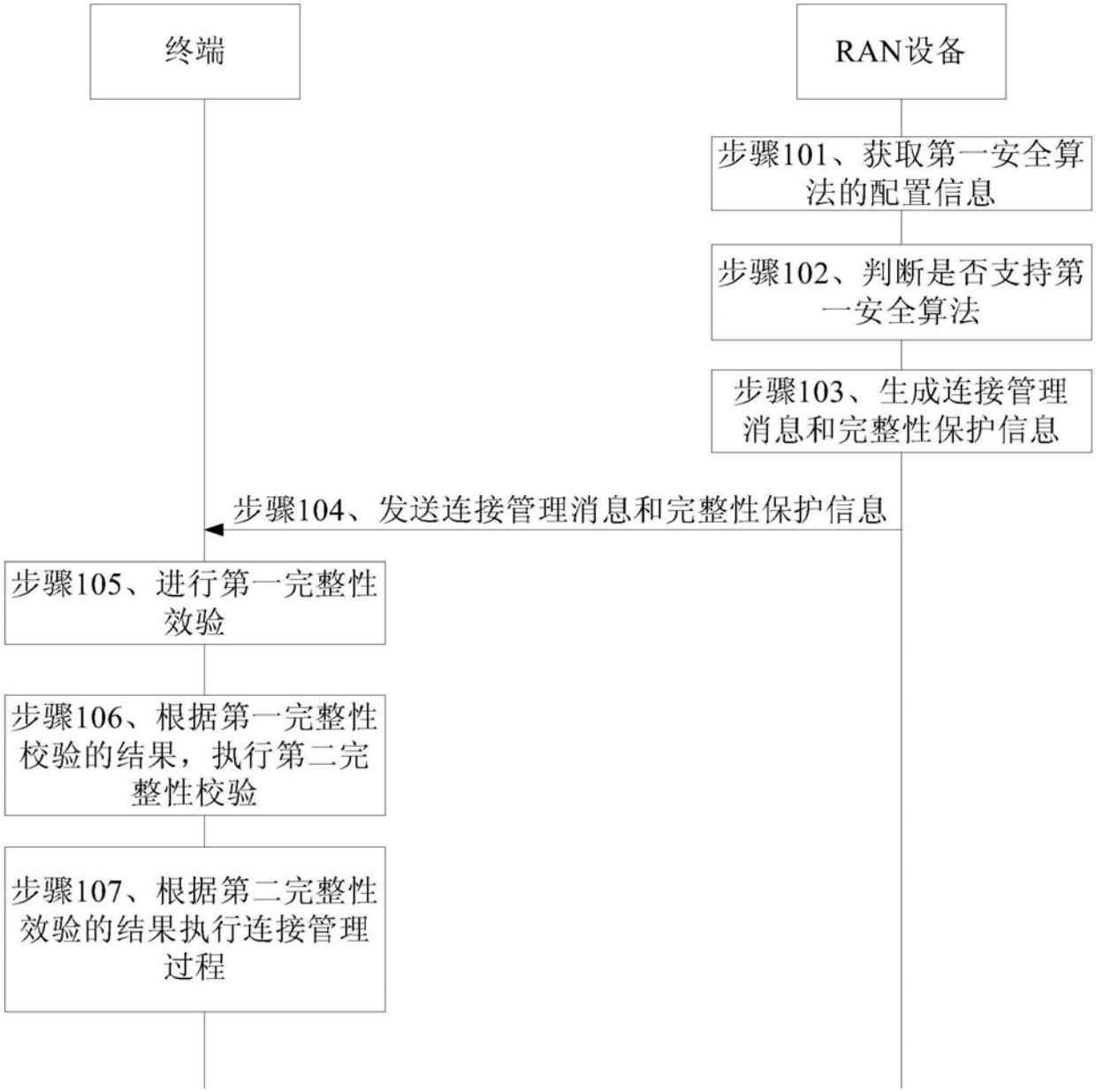

终端
RAN设备
步骤101、获取第一安全算法的配置信息
步骤102、判断是否支持第一安全算法
步骤103、生成连接管理消息和完整性保护信息
步骤104、发送连接管理消息和完整性保护信息
步骤105、进行第一完整性效验
步骤106、根据第一完整性校验的结果，执行第二完整性校验
步骤107、根据第二完整性效验的结果执行连接管理过程

图2

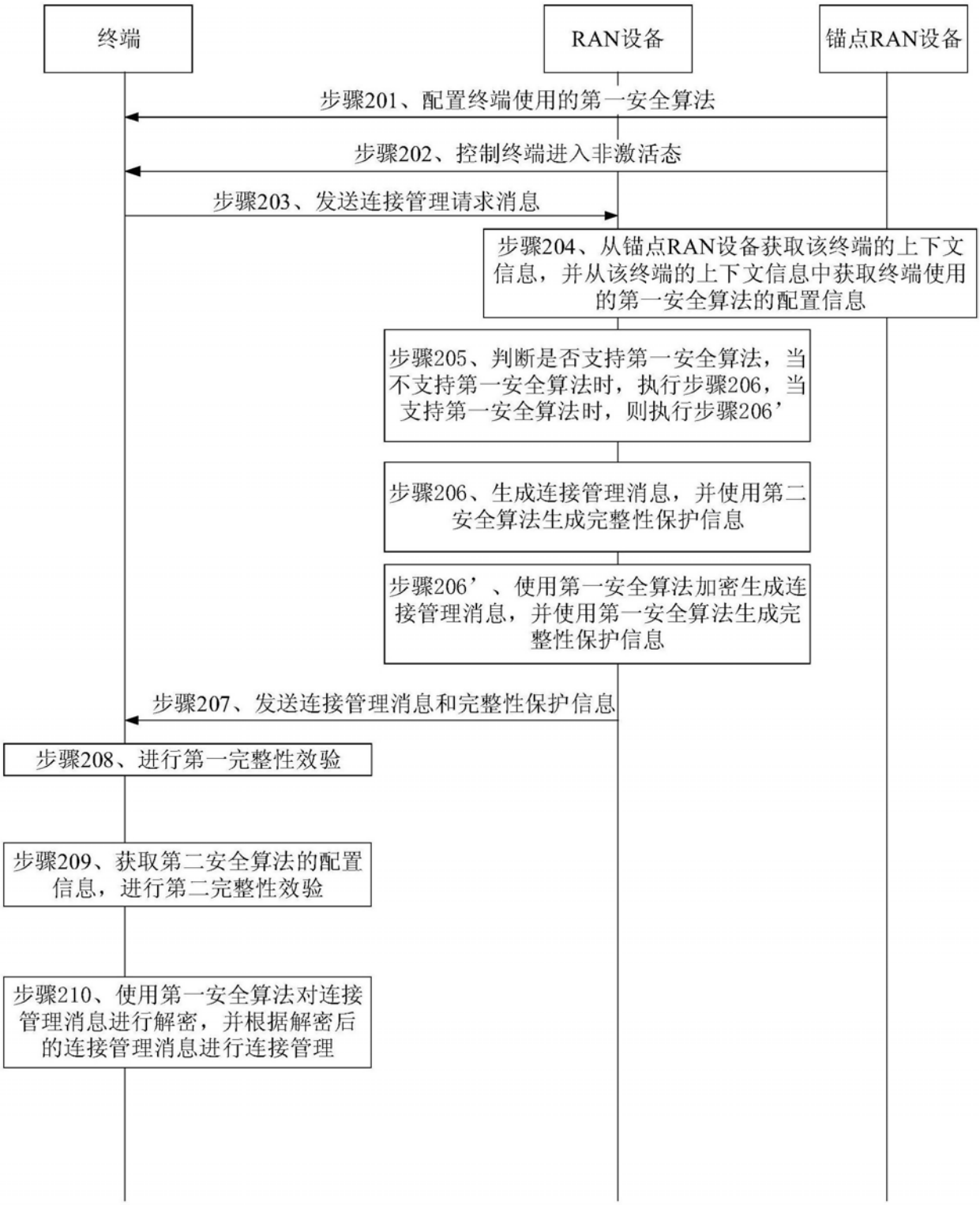

终端
RAN设备
锚点RAN设备
步骤201、配置终端使用的第一安全算法
步骤202、控制终端进入非激活态
步骤203、发送连接管理请求消息
步骤204、从锚点RAN设备获取该终端的上下文信息，并从该终端的上下文信息中获取终端使用的第一安全算法的配置信息
步骤205、判断是否支持第一安全算法，当不支持第一安全算法时，执行步骤206，当支持第一安全算法时，则执行步骤206’
步骤206、生成连接管理消息，并使用第二安全算法生成完整性保护信息
步骤206’、使用第一安全算法加密生成连接管理消息，并使用第一安全算法生成完整性保护信息
步骤207、发送连接管理消息和完整性保护信息
步骤208、进行第一完整性效验
步骤209、获取第二安全算法的配置信息，进行第二完整性效验
步骤210、使用第一安全算法对连接管理消息进行解密，并根据解密后的连接管理消息进行连接管理

图3

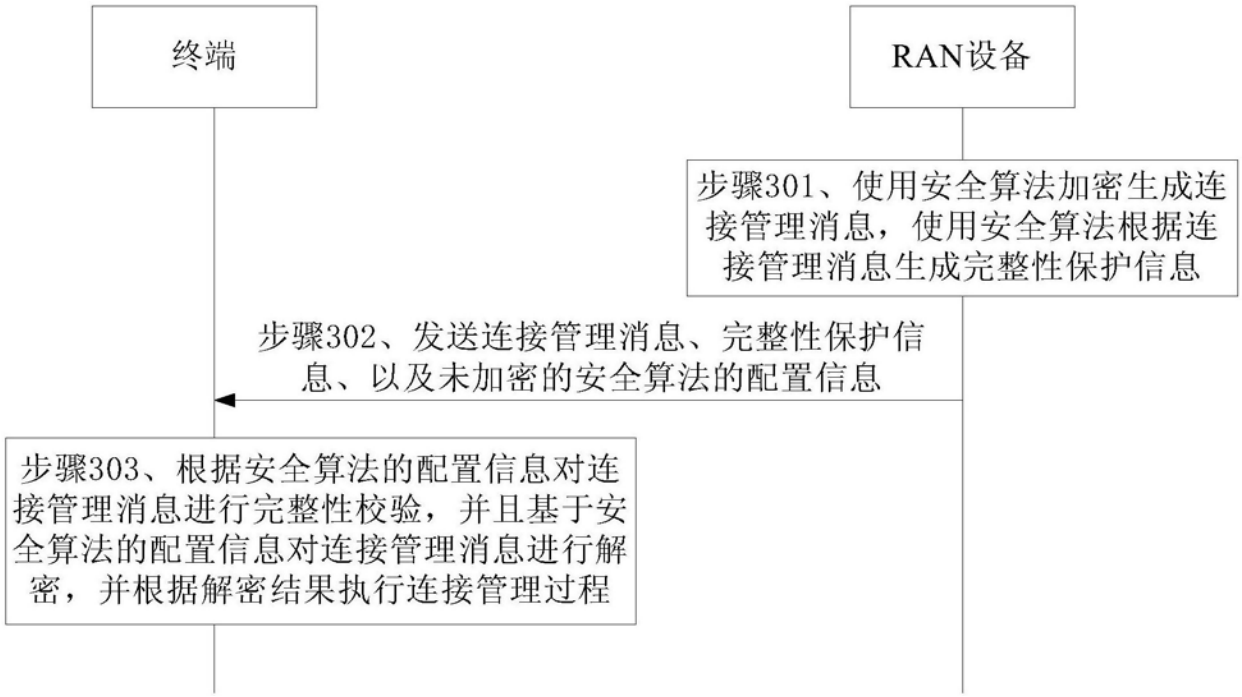

终端
RAN设备
步骤301、使用安全算法加密生成连接管理消息，使用安全算法根据连接管理消息生成完整性保护信息
步骤302、发送连接管理消息、完整性保护信息、以及未加密的安全算法的配置信息
步骤303、根据安全算法的配置信息对连接管理消息进行完整性校验，并且基于安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程

图4

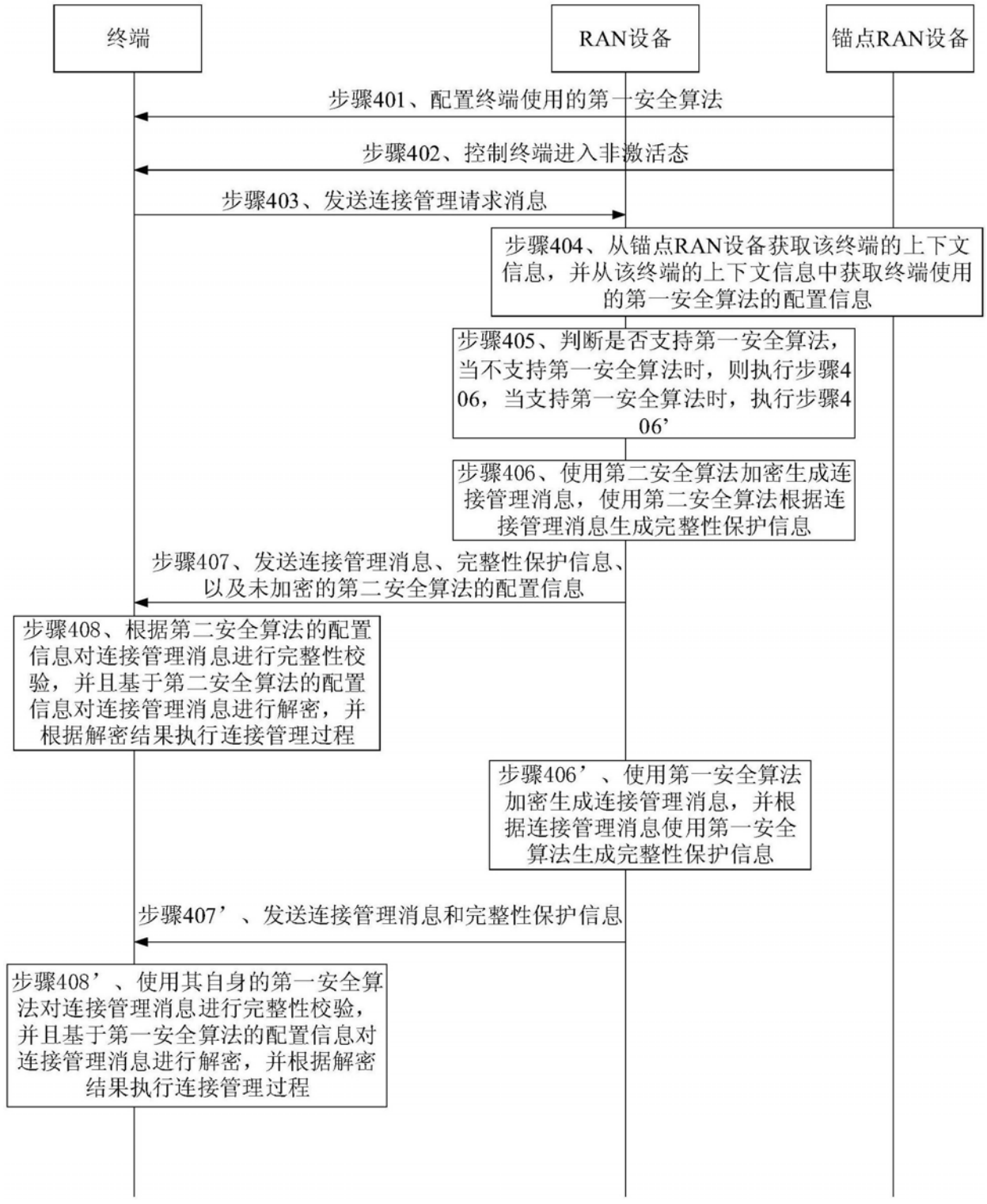

终端
RAN设备
锚点RAN设备
步骤401、配置终端使用的第一安全算法
步骤402、控制终端进入非激活态
步骤403、发送连接管理请求消息
步骤404、从锚点RAN设备获取该终端的上下文信息，并从该终端的上下文信息中获取终端使用的第一安全算法的配置信息
步骤405、判断是否支持第一安全算法，当不支持第一安全算法时，则执行步骤406，当支持第一安全算法时，执行步骤406’
步骤406、使用第二安全算法加密生成连接管理消息，使用第二安全算法根据连接管理消息生成完整性保护信息
步骤407、发送连接管理消息、完整性保护信息、以及未加密的第二安全算法的配置信息
步骤408、根据第二安全算法的配置信息对连接管理消息进行完整性校验，并且基于第二安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程
步骤406’、使用第一安全算法加密生成连接管理消息，并根据连接管理消息使用第一安全算法生成完整性保护信息
步骤407’、发送连接管理消息和完整性保护信息
步骤408’、使用其自身的第一安全算法对连接管理消息进行完整性校验，并且基于第一安全算法的配置信息对连接管理消息进行解密，并根据解密结果执行连接管理过程

图5

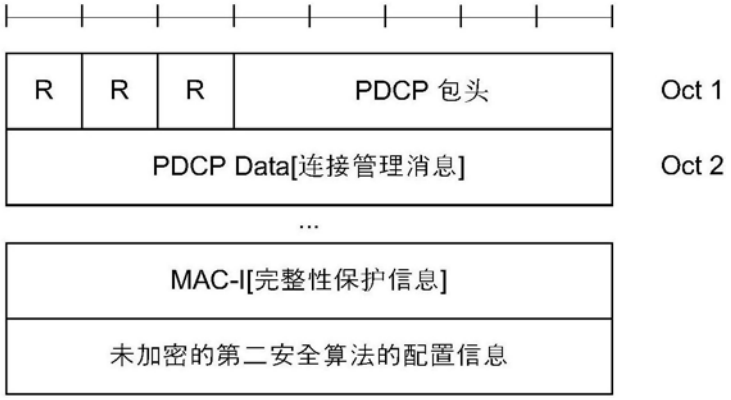

R
R
R
PDCP 包头
Oct 1
PDCP Data[连接管理消息]
Oct 2
...
MAC-I[完整性保护信息]
未加密的第二安全算法的配置信息

图6

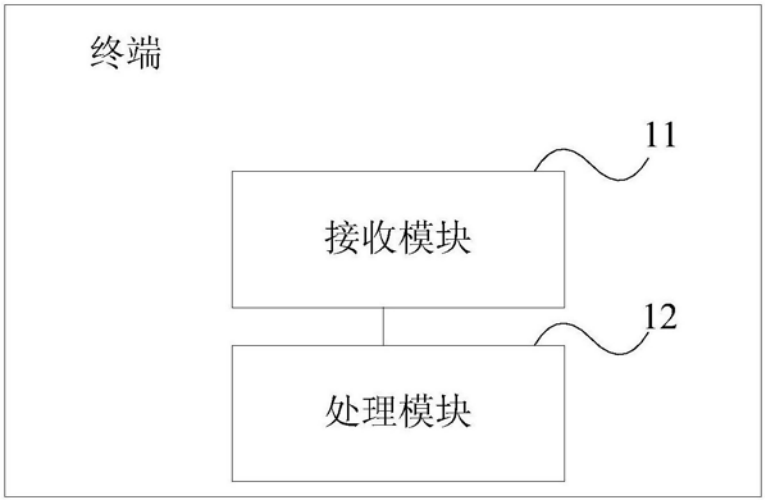

终端
11
接收模块
12
处理模块

图7

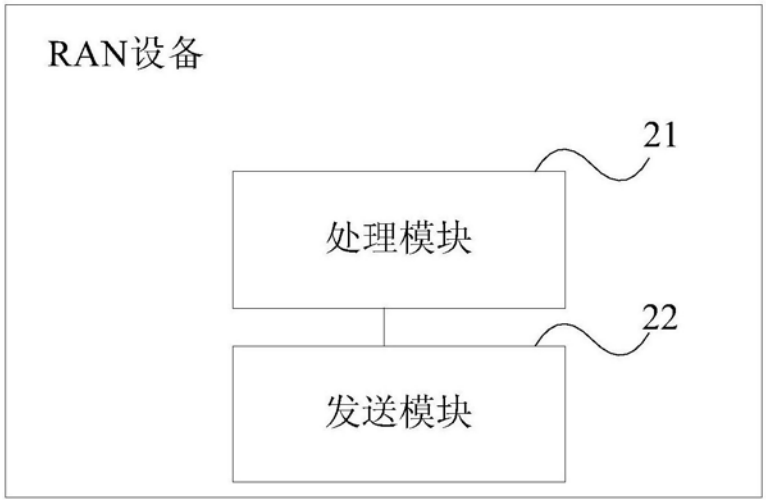

RAN设备
21
处理模块
22
发送模块

图8

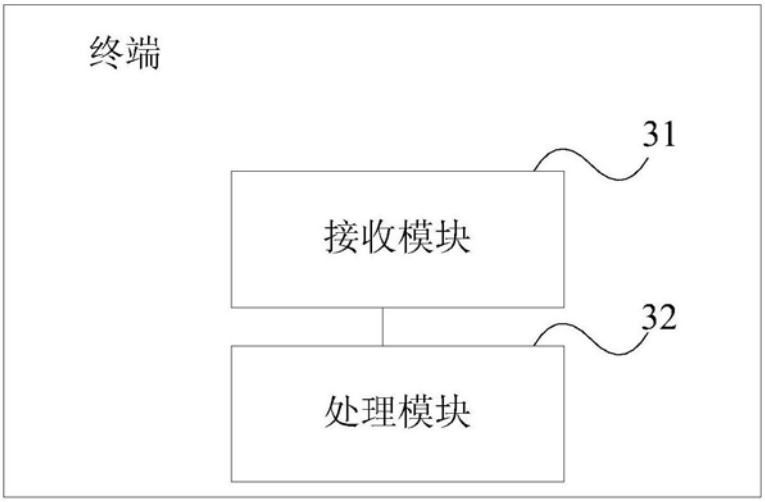


图9

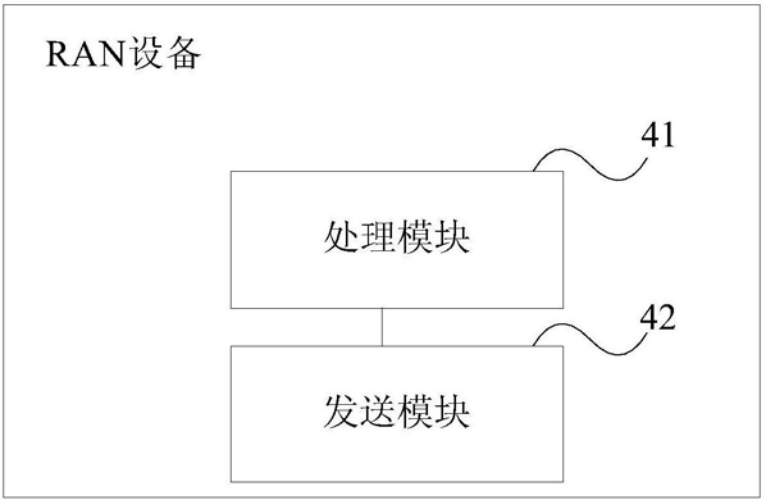


图10