(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110313164 B
(45)授权公告日 2022.07.26

(21)申请号 201780083603.4
(22)申请日 2017.03.19
(65)同一申请的已公布的文献号
申请公布号 CN 110313164 A
(43)申请公布日 2019.10.08
(85)PCT国际申请进入国家阶段日
2019.07.26
(86)PCT国际申请的申请数据
PCT/CN2017/077196 2017.03.19
(87)PCT国际申请的公布数据
WO2018/170645 ZH 2018.09.27
(73)专利权人 上海朗帛通信技术有限公司
地址 200240 上海市闵行区东川路555号乙楼A2117室

(72)发明人 张晓博
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 69/321(2022.01)
(56)对比文件
CN 106375992 A,2017.02.01
CN 102158901 A,2011.08.17
CN 101755469 A,2010.06.23
US 2016073265 A1,2016.03.10
审查员 何丹霞

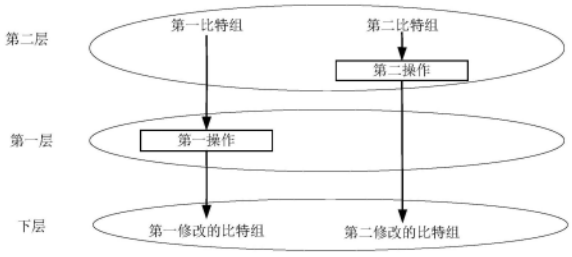
权利要求书4页 说明书19页 附图5页

(54)发明名称

一种用于上行传输的方法和装置

(57)摘要

本发明公开了一种用于上行传输的方法和装置。UE首先在第二层执行第二操作;然后在第一层执行第一操作。其中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。所述比特组中包括正整数个比特。所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一。本发明能满足不同业务的QoS需求以及安全性需求。此外,本发明降低了上行传输的接入网延迟,提高了上行传输的接入网保密性。



CN 110313164 B

1.一种被用于无线通信的用户设备中的方法,其特征在于,包括如下步骤:

-步骤A11.接收第二信息;

-步骤A.在第二层执行第二操作;

-步骤B.在第一层执行第一操作;

其中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出;所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述比特组中包括正整数个比特;所述第一操作包括压缩,所述第二操作包括{加密,完整性保护}中的至少之一;所述第一比特组是IP报头,所述第二层是PDCP层;所述第二信息被用于确定{所述第一层,所述第二层}是否相同;所述第二比特组是IP负载。

2.根据权利要求1所述的方法,其特征在于,

所述第一操作和第三操作分别在UE和核心网设备的对等的层中被执行;所述第三操作包括解压缩。

3.根据权利要求1所述的方法,其特征在于,

所述第一层和所述第二层之间通过S1接口连接;所述第一操作是压缩。

4.根据权利要求1所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A10.接收第一信息;

其中,所述第一信息被用于所述第一操作和所述第二操作;所述第一信息承载在NAS信息中。

5.根据权利要求1所述的方法,其特征在于,所述步骤A还包括如下步骤:

其中,所述第二信息被用于确定{所述第一层和所述第二层};所述第二信息承载在RRC信令中。

6.根据权利要求1所述的方法,其特征在于,所述步骤A还包括如下步骤:

其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;所述第二信息在网络侧设备的PDCP层生成。

7.根据权利要求1所述的方法,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务;所述业务对应的安全要求是独立配置的。

8.根据权利要求1所述的方法,其特征在于,所述第一操作包括{加密,完整性保护}中的至少加密。

9.一种被用于无线通信的基站设备中的方法,其特征在于,包括如下步骤:

-步骤A11.发送第二信息;

-步骤A.在第一层执行{第三操作,第四操作}中的所述第三操作;

其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出;所述第三操作包括解压缩,所述第四操作包括{解密,完整性验证}中的至少之一,所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述第一比特组是IP报头,所述第四操作在第二层中被执行,所述第二层是PDCP层;所述第二信息被用于确定{所述第一层,所述第二层}是否相同;所述第二比特组是IP负载。

10.根据权利要求9所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A1.从下层接收第一比特集合;传递第一比特组和所述第二修改的比特组给第二层;

其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。

11.根据权利要求9所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A10.通过S1接口接收第一信息;或者通过空中接口发送第一信息;

其中,所述第一信息被用于所述第三操作和所述第四操作。

12.根据权利要求11所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A11.通过S1接口接收第二信息;或者通过空中接口发送第二信息;

其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者。

13.根据权利要求9所述的方法,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

14.根据权利要求9所述的方法,其特征在于,所述第四操作不在所述第一层中被执行。

15.一种非接入网设备中的方法,其特征在于,包括如下步骤:

-步骤A.在第二层执行{第三操作,第四操作}中的所述第四操作;

-步骤A2.通过S1接口发送第二信息;

其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出;所述第三操作包括解压缩,所述第四操作包括{解密,完整性验证}中的至少之一,所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述第一比特组是IP报头,所述第二层是PDCP层;所述第二信息被用于确定所述第二层是否与第一层相同,所述第三操作是在第一层中执行;所述第二比特组是IP负载。

16.根据权利要求15所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A1.从第一层接收第一比特组和第二修改的比特组;

其中,所述第三操作是在所述第一层中被执行。

17.根据权利要求15所述的方法,其特征在于,所述步骤A还包括如下步骤:

-步骤A0.通过S1接口发送第一信息;

其中,所述第一信息被用于所述第三操作和所述第四操作。

18.根据权利要求15所述的方法,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

19.根据权利要求15所述的方法,其特征在于,所述第四操作不在所述第一层中被执行。

20.一种被用于无线通信的用户设备,其特征在于,包括如下模块:

-第一处理模块:用于在第二层执行第二操作;

-第二处理模块:用于在第一层执行第一操作;

-所述第一处理模块:用于接收第二信息;

其中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出;所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述比特组中

包括正整数个比特;所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一;所述第一比特组是IP报头,所述第二层是PDCP层,所述第一操作包括压缩;所述第二信息被用于确定{所述第一层,所述第二层}是否相同;所述第二比特组是IP负载。

21.根据权利要求20所述的用户设备,其特征在于,

第三操作包括解压缩,所述压缩和所述解压缩互为逆操作;所述第一操作和所述第三操作分别在UE和核心网设备的对等的层中被执行。

22.根据权利要求20所述的用户设备,其特征在于,

所述第一层和所述第二层之间通过S1接口连接;所述第一操作是压缩。

23.根据权利要求20所述的用户设备,其特征在于,所述第一处理模块还用于接收第一信息;其中,所述第一信息被用于所述第一操作和所述第二操作;所述第一信息承载在NAS信息中。

24.根据权利要求20所述的用户设备,其特征在于,所述第一处理模块还用于接收第二信息;其中,所述第二信息被用于确定{所述第一层和所述第二层};所述第二信息承载在RRC信令中。

25.根据权利要求20所述的用户设备,其特征在于,所述第一处理模块还用于接收第二信息;其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;所述第二信息在网络侧设备的PDCP层生成。

26.根据权利要求20所述的用户设备,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务,所述业务对应的安全要求是独立配置的。

27.根据权利要求20所述的用户设备,其特征在于,所述第一操作包括{加密,完整性保护}中的至少加密。

28.一种被用于无线通信的基站设备,其特征在于,包括如下模块:

-第三处理模块:用于在第一层执行{第三操作,第四操作}中的所述第三操作;

-所述第三处理模块:用于发送第二信息;

其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出;所述第三操作包括解压缩,所述第四操作包括{解密,完整性验证}中的至少之一,所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述第一比特组是IP报头,所述第四操作在第二层中被执行,所述第二层是PDCP层;所述第二信息被用于确定{所述第一层,所述第二层}是否相同;所述第二比特组是IP负载。

29.根据权利要求28所述的基站设备,其特征在于,所述第三处理模块还用于从下层接收第一比特集合;传递第一比特组和所述第二修改的比特组给第二层;其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组;所述第四操作是在所述第二层中被执行。

30.根据权利要求28所述的基站设备,其特征在于,所述第三处理模块还用于通过S1接口接收第一信息;或者通过空中接口发送第一信息;其中,所述第一信息被用于所述第三操作和所述第四操作。

31.根据权利要求28所述的基站设备,其特征在于,所述第三处理模块还用于通过S1接口接收第二信息;或者通过空中接口发送第二信息;其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者。

32.根据权利要求28所述的基站设备,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

33.根据权利要求28所述的基站设备,其特征在于,所述第四操作不在所述第一层中被执行。

34.一种非接入网设备,其特征在于,包括如下模块:

-第四处理模块:用于在第二层执行{第三操作,第四操作}中的所述第四操作;通过S1接口发送第二信息;

其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出;所述第三操作包括解压缩,所述第四操作包括{解密,完整性验证}中的至少之一,所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元;所述第一比特组是IP报头,所述第二层是PDCP层;所述第二信息被用于确定所述第二层是否与第一层相同所述第二比特组是IP负载;所述第三操作是在第一层中执行。

35.根据权利要求34所述的非接入网设备,其特征在于,所述第四处理模块还用于从第一层接收第一比特组和第二修改的比特组;其中,所述第三操作是在所述第一层中被执行。

36.根据权利要求34所述的非接入网设备,其特征在于,所述第四处理模块还用于通过S1接口发送第一信息,所述第一信息被用于所述第三操作和所述第四操作。

37.根据权利要求34所述的非接入网设备,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

38.根据权利要求34所述的非接入网设备,其特征在于,所述第四操作不在所述第一层中被执行。

一种用于上行传输的方法和装置

技术领域

[0001] 本申请涉及无线通信系统中的上行传输的方案,特别是涉及安全传输的方法和装置。

背景技术

[0002] LTE(Long Term Evolution)系统中,分组数据汇聚协议(PDCP,Packet Data Convergence Protocol)层位于无线链路控制(RLC,Radio Link Control)层之上,网际通信协议(IP,Internet Protocol)层之下,或者无线资源控制(RRC,Radio Resource Control)层之下。PDCP层支持报头压缩(Header Compression)功能,主要使用鲁棒性报头压缩(ROHC,Robust Header Compression)算法。报头压缩主要用于对IP包进行报头压缩。报头压缩主要针对数据无线承载(DRB,Data Radio Bearer)。PDCP层还支持安全功能,主要包括完整性保护(integrity protection)和加密(ciphering)。其中完整性保护主要针对信令无线承载(SRB,Signaling Radio Bearer),加密主要针对数据无线承载和信令无线承载。

[0003] NR(New Radio)系统中存在多种业务,不同业务的QoS不同,同时对安全功能的要求也不同。在NR系统中,不同的业务可能在不同的网络切片中传输。网络切片是一个逻辑网络,包括核心网和接入网。

发明内容

[0004] 申请人通过研究发现:如果类似于LTE系统那样,NR系统只在PDCP层对数据进行安全操作,则PDCP层需要针对每一个网络切片进行网络切片专属的安全操作,这样会增加PDCP层的复杂度。

[0005] 申请人通过进一步研究发现:对于时延敏感的业务,在接入网侧进行的安全操作可能增加接入网侧的时延;对于一些安全性要求较高的业务,在接入网侧进行的加密可能增大接入网侧泄密的可能性。

[0006] 根据上述申请人的研究,NR系统中的不同业务可能采用不同的加密和完整性保护操作的实体。这些实体可以分属于不同的网络切片,位于不同的协议实体中。对于上行传输,用户设备在非接入层对数据(报头+负载)进行加密,用户设备在PDCP发送端对上层下发的已加密的数据(报头+负载)进行报头压缩。基站侧PDCP接收端不能正确解压缩。

[0007] 针对上述问题,本申请提供了解决方案。需要说明的是,在不冲突的情况下,本申请的实施例和实施例中的特征可以任意相互组合。例如本申请的UE中的实施例和实施例中的特征可应用到基站中,反之亦然。

[0008] 本申请公开了一种被用于无线通信的用户设备中的方法,其中,包括如下步骤:

[0009] -步骤A.在第二层执行第二操作;

[0010] -步骤B.在第一层执行第一操作

[0011] 其中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操

作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。所述比特组中包括正整数个比特。所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一。

[0012] 作为一个实施例,所述第一比特组是网际通讯协议(IP,Internet Protocol)报头,所述第二比特组是网际通信协议(IP,Internet Protocol)包Payload(负载)。

[0013] 作为上述实施例的一个子实施例,所述第二修改的比特组是一个PDCP SDU(Service Data Unit,服务数据单元)。

[0014] 作为一个实施例,所述第二层是所述第一层的上层。

[0015] 作为一个实施例,所述第一层是PDCP层,所述第二层是非接入层(NAS,Non Access Stratum)。

[0016] 上述实施例中,所述第一操作和所述第二操作是在两个不同的层中完成的,上述实施例降低了接入网的延迟,同时提高了接入网的安全性。

[0017] 作为一个实施例,所述第一层包括PDCP层和RRC(Radio Resource Control,无线资源控制)层,所述第二层是非接入层。

[0018] 作为上述实施例的一个子实施例,所述第一修改的比特组和所述第二修改的比特组属于同一个PDCP PDU(Protocol Data Unit,协议数据单元)。

[0019] 作为一个实施例,所述第二层和所述第一层是否相同是可以配置的。

[0020] 作为一个实施例,对于所述压缩,输入的比特的数量大于输出的比特的数量。

[0021] 作为一个实施例,所述压缩是鲁棒性报头压缩(ROHC,Robust Header Compression)。

[0022] 作为一个实施例,所述压缩是TS36.323表5.5.1.1中示例的压缩算法。

[0023] 作为一个实施例,所述加密是保证数据在发端和收端之间保持机密。

[0024] 作为一个实施例,所述加密是原始数据和一串密钥加掩。

[0025] 作为一个子实施例,所述加掩是两个数据做抑或操作。

[0026] 作为一个子实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0027] 作为一个子实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0028] 作为一个子实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0029] 作为一个子实施例,所述一串密钥播包括第一安全密钥。

[0030] 作为一个实施例,所述加密是TS36.323描述的加密算法。

[0031] 作为一个实施例,所述完整性保护通过消息验证码-完整性(MAC-I,Message Authentication Code-Integrity)与数据加掩实现。

[0032] 作为一个子实施例,所述消息验证码-完整性是通过完整性保护算法实现。

[0033] 作为一个子实施例,所述完整性算法保护的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0034] 作为一个子实施例,所述完整性算法保护的输入参数包括无线承载标识(Radio Bearer ID)。

[0035] 作为一个子实施例,所述完整性算法保护的输入参数包括PDCP序列号(PDCP SN)。

[0036] 作为一个子实施例,所述完整性保护算法的输入参数包括第一安全密钥。

[0037] 作为一个子实施例,所述完整性保护算法的输入参数包括数据。

[0038] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤A1,所述步骤B还包括如下步骤B1:

[0039] -步骤A1.从所述第二层传递第一比特组和所述第二修改的比特组给所述第一层;

[0040] -步骤B1.从所述第一层传递第一比特集合给下层。

[0041] 其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。

[0042] 作为一个实施例,所述第一比特集合是一个PDCP PDU。

[0043] 作为一个实施例,所述第一比特集合是一个上行的高层PDU。

[0044] 作为一个实施例,所述第一比特集合是一个上行的PDCP PDU。

[0045] 作为一个实施例,所述第一比特集合包括{PDCP报头,所述第一修改的比特组,所述第二修改的比特组}。

[0046] 作为一个实施例,所述第一层是PDCP层,所述下层是RLC层。

[0047] 作为一个实施例,所述第一层包括PDCP层和RRC(Radio Resource Control,无线资源控制)层,所述第二层是非接入层,所述下层包括RLC层。

[0048] 作为一个实施例,所述第二层是非接入层(NAS,Non Access Stratum)。

[0049] 作为一个实施例,所述第二层是PDCP层。

[0050] 作为一个实施例,所述第二层是由支持3GPP Rel-15版本的网络测设备维护的。

[0051] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0052] -步骤A10.接收第一信息。

[0053] 其中,所述第一信息被用于所述第一操作和所述第二操作。

[0054] 作为一个实施例,所述第一信息承载在RRC信令中。

[0055] 作为一个实施例,所述第一信息承载在NAS信息中。

[0056] 作为一个实施例,所述第一信息承载在高层信令中。

[0057] 作为一个实施例,所述第一信息与S1信令相关。

[0058] 作为一个实施例,所述第一信息和第一业务组相关联。所述第一业务组包括一种或者多种业务。

[0059] 作为一个实施例,所述第一信息包含第一安全密钥,所述第一安全密钥由高层配置。

[0060] 作为一个实施例,所述第一安全密钥是KASME。

[0061] 作为一个实施例,所述加密被用于PDCP层的信号无线承载(SRB,Signaling Radio Bearer)和数据无线承载(DRB,Data Radio Bearer)。

[0062] 作为一个实施例,所述完整性保护被用于PDCP层的信号无线承载(SRB,Signaling Radio Bearer)。

[0063] 作为一个实施例,所述加密需要的第二安全密钥从第一安全密钥获得。

[0064] 作为一个实施例,所述第二安全密钥是KRRCenc。

[0065] 作为一个实施例,所述第二安全密钥是KUPenc。

[0066] 作为一个实施例,所述完整性保护需要的第三安全密钥从第一安全密钥获得。

[0067] 作为一个实施例,所述第三安全密钥是KRRCint。

[0068] 作为一个实施例,所述第一信息的发送者是支持3GPP Rel-15及之后版本的基站

设备。

[0069] 作为一个实施例,所述第一信息的发送者是基站设备。

[0070] 作为一个实施例,所述第一信息的发送者是用户分组系统(UPS,User Packet System)。

[0071] 作为一个实施例,所述第一信息在网络侧设备的NAS层中被生成。

[0072] 作为一个实施例,所述第一信息在网络侧设备的所述第二层中被生成。

[0073] 作为一个实施例,所述第一信息在用户分组系统(UPS,User Packet System)中生成。

[0074] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0075] -步骤A11.接收第二信息。

[0076] 其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0077] 作为一个实施例,所述第二信息承载在RRC信令中。

[0078] 作为一个实施例,所述第二信息承载在NAS信息中。

[0079] 作为一个实施例,所述第二信息和第一业务组相关联。所述第一业务组包括一种或者多种业务。

[0080] 作为一个实施例,所述第二信息被应用于第一无线承载。所述第一比特组和所述第二比特组在所述第一无线承载中传输。

[0081] 作为一个实施例,所述第二信息被基站设备生成。

[0082] 作为一个实施例,所述第二信息在网络侧设备的所述第二层生成。

[0083] 作为一个实施例,所述第二信息在网络侧设备的NAS层生成。

[0084] 作为一个实施例,所述第二信息在网络侧设备的PDCP层生成。

[0085] 作为一个实施例,所述第二信息指示所述第一层和所述第二层都是PDCP层。

[0086] 作为一个实施例,所述第二信息指示所述第一层和所述第二层都是NAS层。

[0087] 具体的,根据本申请的一个方面,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

[0088] 作为一个实施例,所述业务的QoS要求是独立配置的。

[0089] 作为一个实施例,所述业务对应的安全要求是独立配置的。

[0090] 作为一个实施例,所述第一业务组是一个网络切片。

[0091] 作为一个实施例,所述第一业务组中的所有业务共享相同的安全要求。

[0092] 作为一个实施例,所述第一业务组中的所有业务共享相同的QoS要求。

[0093] 具体的,根据本申请的一个方面,其特征在于,所述第一层是PDCP层,所述第二层是非接入层。

[0094] 本申请公开了一种被用于无线通信的基站设备中的方法,其中,包括如下步骤:

[0095] -步骤A.在第一层执行{第三操作,第四操作}中的所述第三操作。

[0096] 其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个协

议数据单元。

[0097] 作为一个实施例,上述方面中,第四操作不在所述第一层中被执行。

[0098] 作为一个实施例,所述第一层和所述第二层之间通过S1接口连接。

[0099] 作为一个实施例,所述第一比特组是网际通信协议(IP,Internet Protocol)报头,所述第二比特组是IP包Payload(负载)。

[0100] 作为上述实施例的一个子实施例,所述第二修改的比特组是一个PDCP SDU。

[0101] 作为一个实施例,所述第一比特集合是一个PDCP PDU。

[0102] 作为一个实施例,所述第一比特集合是一个上行的高层PDU。

[0103] 作为一个实施例,所述第一比特集合是一个上行的PDCP PDU。

[0104] 作为一个实施例,所述第一比特集合包括{PDCP报头,所述第一修改的比特组,所述第二修改的比特组}。

[0105] 作为一个实施例,对于所述解压缩,输出的比特的数量大于输入的比特的数量。

[0106] 作为一个实施例,所述解压缩是比较原始报头和压缩后的报头获得压缩前的报头。

[0107] 作为一个实施例,所述解压缩是对鲁棒性报头压缩(ROHC,Robust Header Compression)算法的逆操作。

[0108] 作为一个实施例,所述解压缩是对TS36.323表5.5.1.1中示例的压缩算法的逆操作。

[0109] 作为一个实施例,所述解密是原始数据和一串密钥去掩。

[0110] 作为一个子实施例,所述去掩是数据和掩码做抑或操作。

[0111] 作为一个子实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0112] 作为一个子实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0113] 作为一个子实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0114] 作为一个子实施例,所述一串密钥播包括第一安全密钥。

[0115] 作为一个实施例,所述解密是TS36.323描述的解密算法。

[0116] 作为一个实施例,所述完整性验证通过比较X消息验证码-完整性(XMAC-I,Message Authentication Code-Integrity)与消息验证码-完整性实现。

[0117] 作为一个子实施例,所述X消息验证码-完整性与消息验证码-完整性一致,则完整性验证通过,反之则不通过。

[0118] 作为一个子实施例,所述X消息验证码-完整性是通过完整性验证算法实现。

[0119] 作为一个子实施例,所述完整性验证算法的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0120] 作为一个子实施例,所述完整性验证算法的输入参数包括无线承载标识(Radio Bearer ID)。

[0121] 作为一个子实施例,所述完整性验证算法的输入参数包括PDCP序列号(PDCP SN)。

[0122] 作为一个子实施例,所述完整性验证算法的输入参数包括第一安全密钥。

[0123] 作为一个子实施例,所述完整性验证算法的输入参数包括数据。

[0124] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0125] -步骤A1.从下层接收第一比特集合;传递第一比特组和所述第二修改的比特组给

第二层。

[0126] 其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。所述第四操作是在所述第二层中被执行。

[0127] 作为一个实施例,所述第二层由所述基站设备之外的设备维护。

[0128] 作为一个实施例,所述第二层由核心网侧设备维护。

[0129] 作为一个子实施例,所述核心网侧设备是属于户分组系统(UPS,User Packet System)。

[0130] 作为一个实施例,所述第二层是所述第一层的上层。

[0131] 作为一个实施例,所述第一层是PDCP层,所述第二层是非接入层(NAS,Non Access Stratum)。

[0132] 作为上述实施例的一个子实施例,所述第一修改的比特组和所述第二修改的比特组属于同一个PDCP PDU。

[0133] 作为一个实施例,所述第二层和所述第一层是否相同是可以配置的。

[0134] 作为一个实施例,所述第一层是PDCP层,所述下层是RLC层。

[0135] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0136] -步骤A10.通过S1接口接收第一信息;或者通过空中接口发送第一信息。

[0137] 其中,所述第一信息被用于所述第三操作和所述第四操作。

[0138] 作为一个实施例,所述第一信息和第一业务组相关联。所述第一业务组包括一种或者多种业务。

[0139] 作为一个实施例,所述第一信息包含第一安全密钥,所述第一安全密钥由高层配置。

[0140] 作为一个实施例,所述第一安全密钥是KASME。

[0141] 作为一个实施例,所述加密被用于PDCP层的信号无线承载(SRB,Signaling Radio Bearer)和数据无线承载(DRB,Data Radio Bearer)。

[0142] 作为一个实施例,所述完整性保护被用于PDCP层的信号无线承载(SRB,Signaling Radio Bearer)。

[0143] 作为一个实施例,所述加密需要的第二安全密钥从第一安全密钥获得。

[0144] 作为一个实施例,所述第二安全密钥是KRRCenc。

[0145] 作为一个实施例,所述第二安全密钥是KUPenc。

[0146] 作为一个实施例,所述完整性保护需要的第三安全密钥从第一安全密钥获得。

[0147] 作为一个实施例,所述第三安全密钥是KRRCint。

[0148] 作为一个实施例,所述第一信息的发送者是支持3GPP Rel-15及之后版本的基站设备。

[0149] 作为一个实施例,所述第一信息的发送者是基站设备。

[0150] 作为一个实施例,所述第一信息承载在RRC信令中。

[0151] 作为一个实施例,所述第一信息的发送者是用户分组系统(UPS,User Packet System)。

[0152] 作为一个实施例,所述第一信息承载在高层信令中。

[0153] 作为一个实施例,所述第一信息和一个S1信令相关。

[0154] 作为一个实施例,所述S1信令的发送者是用户分组系统(UPS,User Packet System)。

[0155] 作为一个实施例,所述第一信息在网络侧设备的NAS层中被生成。

[0156] 作为一个实施例,所述第一信息在网络侧设备的所述第二层中被生成。

[0157] 作为一个实施例,所述第一信息在用户分组系统(UPS,User Packet System)中生成。

[0158] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0159] -步骤A11.通过S1接口接收第二信息;或者通过空中接口发送第二信息。

[0160] 其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0161] 作为一个实施例,上述方面确保基站能够对所述第一修改的比特组和所述第二修改的比特组采取正确的操作,避免了基站对所述第二修改的比特组执行所述第四操作。

[0162] 作为一个实施例,所述第二信息和第一业务组相关联。所述第一业务组包括一种或者多种业务。

[0163] 作为一个实施例,所述第二信息被应用于第一无线承载。所述第一比特组和所述第二比特组在所述第一无线承载中传输。

[0164] 作为一个实施例,所述第二信息承载在RRC信令中。

[0165] 作为一个实施例,所述第二信息被基站设备生成。

[0166] 作为一个实施例,所述第二信息在网络侧设备的所述第二层生成。

[0167] 作为一个实施例,所述第二信息在网络侧设备的NAS层生成。

[0168] 作为一个实施例,所述第二信息在网络侧设备的PDCP层生成。

[0169] 作为一个实施例,所述第二信息承载在高层信令中。

[0170] 作为一个实施例,所述第二信息与一个S1信令相关。

[0171] 作为一个实施例,所述第二信息指示所述第一层和所述第二层都是PDCP层。

[0172] 作为一个实施例,所述第二信息指示所述第一层和所述第二层都是NAS层。

[0173] 具体的,根据本申请的一个方面,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

[0174] 作为一个实施例,所述第一业务组是一个网络切片。

[0175] 具体的,根据本申请的一个方面,其特征在于,所述第一层是PDCP层,所述第二层是非接入层。

[0176] 本申请公开了一种非接入网设备中的方法,其中,包括如下步骤:

[0177] -步骤A.在第二层执行{第三操作,第四操作}中的所述第四操作。

[0178] 其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。

[0179] 作为一个实施例,所述第一层由所述非接入网设备之外的设备维护。

[0180] 作为一个实施例,所述第一层由基站维护。

[0181] 作为一个子实施例,所述基站支持3GPP Rel-15。

[0182] 作为一个实施例,所述第一层和所述第二层之间通过S1接口连接。

[0183] 作为一个实施例,所述第一比特组是网际通信协议(IP,Internet Protocol)报头,所述第二比特组是网际通信协议(IP,Internet Protocol)包Payload(负载)。

[0184] 作为上述实施例的一个子实施例,所述第二修改的比特组是一个PDCP SDU作为一个实施例,所述非接入网设备是核心网设备。

[0185] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0186] -步骤A1.从第一层接收第一比特组和第二修改的比特组。

[0187] 其中,所述第三操作是在所述第一层中被执行。

[0188] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0189] -步骤A0.通过S1接口发送第一信息。

[0190] 其中,所述第一信息被用于所述第三操作和所述第四操作。

[0191] 作为一个实施例,所述第一信息和一个S1信令相关。

[0192] 作为一个实施例,所述第一信息承载在非接入层(NAS,Non Access Stratum)信息中。

[0193] 具体的,根据本申请的一个方面,其特征在于,所述步骤A还包括如下步骤:

[0194] -步骤A2.通过S1接口发送第二信息。

[0195] 其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0196] 作为一个实施例,所述第二信息和一个S1信令相关。

[0197] 作为一个实施例,所述第二信息承载在非接入层(NAS,Non Access Stratum)信息中。

[0198] 具体的,根据本申请的一个方面,其特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

[0199] 作为一个实施例,针对不同业务,上述方面能满足可变的QoS要求以及安全要求

[0200] 具体的,根据本申请的一个方面,其特征在于,所述第一层是PDCP层,所述第二层是非接入层。

[0201] 本申请公开了一种被用于无线通信的用户设备,其中,包括如下模块:

[0202] -第一处理模块:用于在第二层执行第二操作;

[0203] -第二处理模块:用于在第一层执行第一操作

[0204] 其中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。所述比特组中包括正整数个比特。所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一。

[0205] 作为一个实施例,上述被用于无线通信的用户设备的特征在于:

[0206] -.所述第一处理模块还用于从所述第二层传递第一比特组和所述第二修改的比特组给所述第一层;

[0207] -.所述第二处理模块还用于从所述第一层传递第一比特集合给下层。

[0208] 其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。

[0209] 作为一个实施例,上述被用于无线通信的用户设备的特征在于,所述第一处理模块还用于接收第一信息。其中,所述第一信息被用于所述第一操作和所述第二操作。

[0210] 作为一个实施例,上述被用于无线通信的用户设备的特征在于:所述第一处理模块还用于接收第二信息。其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0211] 作为一个实施例,上述被用于无线通信的用户设备的特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

[0212] 具体的,根据本申请的一个方面,其特征在于,所述第一层是PDCP层,所述第二层是非接入层。

[0213] 本申请公开了一种被用于无线通信的基站设备,其中,包括如下模块:

[0214] -第三处理模块:用于在第一层执行{第三操作,第四操作}中的所述第三操作。

[0215] 其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。

[0216] 作为一个实施例,上述被用于无线通信的基站设备的特征在于,所述第三处理模块还用于从下层接收第一比特集合以及传递(Del iver)第一比特组和所述第二修改的比特组给第二层。其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。所述第四操作是在所述第二层中被执行。

[0217] 作为一个实施例,上述被用于无线通信的基站设备的特征在于,所述第三处理模块还用于通过S1接口接收第一信息;或者通过空中接口发送第一信息。其中,所述第一信息被用于所述第三操作和所述第四操作。

[0218] 作为一个实施例,上述被用于无线通信的基站设备的特征在于,所述第三处理模块还用于通过S1接口接收第二信息;或者通过空中接口发送第二信息。其中,所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0219] 作为一个实施例,上述被用于无线通信的基站设备的特征在于,所述第一比特组和所述第二比特组对应第一业务组,所述第一业务组包括一种或者多种业务。

[0220] 具体的,根据本申请的一个方面,其特征在于,所述第一层是PDCP层,所述第二层是非接入层。

[0221] 本申请公开了一种非接入网设备,其中,包括如下模块:

[0222] -第四处理模块:用于在第二层执行{第三操作,第四操作}中的所述第四操作。

[0223] 其中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。

[0224] 作为一个实施例，上述非接入网设备的特征在于，所述第四处理模块还用于从第一层接收第一比特组和第二修改的比特组。其中，所述第三操作是在所述第一层中被执行。

[0225] 作为一个实施例，上述非接入网设备的特征在于，所述第四处理模块还用于通过S1接口发送第一信息。其中，所述第一信息被用于所述第三操作和所述第四操作。

[0226] 作为一个实施例，上述非接入网设备的特征在于，所述第四处理模块还用于通过S1接口发送第二信息。其中，所述第二信息被用于确定{所述第一层，所述第二层}中的至少后者；或者所述第二信息被用于确定{所述第一层，所述第二层}是否相同。

[0227] 作为一个实施例，上述非接入网设备的特征在于，所述第一比特组和所述第二比特组对应第一业务组，所述第一业务组包括一种或者多种业务。

[0228] 具体的，根据本申请的一个方面，其特征在于，所述第一层是PDCP层，所述第二层是非接入层。

[0229] 作为一个实施例，相比现有公开技术，本申请具有如下技术优势：

[0230] -.通过将数据包的报头和负载在不同的实体进行加密满足了不同业务的QoS要求，同时满足了对不同业务的安全要求；

[0231] -.通过指示数据包的报头和负载在用户设备某个实体发送端加密，帮助基站侧实体接收端解压缩；

[0232] -.降低了接入网的延迟；

[0233] -.降低了接入网失密的风险，提高了传输的安全性。

附图说明

[0234] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更加明显：

[0235] 图1示出了根据本申请的一个实施例的第一操作的示意图；

[0236] 图2示出了根据本申请的一个实施例的第三操作的示意图；

[0237] 图3示出了根据本申请的一个实施例的第二操作的示意图；

[0238] 图4示出了根据本申请的一个实施例的第四操作的示意图；

[0239] 图5示出了根据本申请的一个实施例的第一操作和第三操作的示意图；

[0240] 图6示出了根据本申请的一个实施例的第二操作和第四操作的示意图；

[0241] 图7示出了根据本申请的一个实施例的上行数据的发送和接收的流程图；

[0242] 图8示出了根据本申请的一个实施例的上行数据的发送的流程图；

[0243] 图9示出了根据本申请的一个实施例的上行数据的接收的流程图；

[0244] 图10示出了根据本申请的一个实施例的第一比特集合的示意图；

[0245] 图11示出了根据本申请的一个实施例的网络切片的示意图；

[0246] 图12示出了根据本申请的一个实施例的UE中的处理装置的结构框图；

[0247] 图13示出了根据本申请的一个实施例的基站中的处理装置的结构框图；

[0248] 图14示出了根据本申请的一个实施例的核心网设备中的处理装置的结构框图。

具体实施方式

[0249] 下文将结合附图对本申请的技术方案作进一步详细说明，需要说明的是，在不冲

突的情况下,本申请的实施例和实施例中的特征可以任意相互组合。

[0250] 实施例1

[0251] 实施例1示例了第一操作的示意图,如附图1所示。

[0252] 实施例1中,第一比特组经过第一操作之后变成第一修改的比特组。所述第一比特组和所述第一修改的比特组分别包括正整数个比特。所述第一操作包括{压缩,加密,完整性保护}中的至少之一。

[0253] 作为一个实施例,所述第一比特组是IP报头。所述第一操作在UE中的PDCP层中被执行。

[0254] 作为一个实施例,所述第一操作包括{压缩,加密};或者所述第一操作包括{压缩,加密,完整性保护}。

[0255] 作为一个实施例,所述第一修改的比特组是所述第一比特组依次经过所述压缩,所述加密和所述完整性保护之后生成的。

[0256] 作为一个实施例,所述第一修改的比特组是所述第一比特组依次经过所述压缩和所述加密之后生成的。

[0257] 作为一个实施例,所述第一比特组经过压缩之后的比特的数量小于所述第一比特组中的比特的数量。

[0258] 作为一个实施例,所述压缩是鲁棒性报头压缩(ROHC,Robust Header Compression)。

[0259] 作为一个实施例,所述压缩采用3GPP TS36.323中的表5.5.1.1中示例的压缩算法。

[0260] 作为一个实施例,所述加密被用于保证数据在发端和收端之间保持机密。

[0261] 作为一个实施例,所述加密是采用一串密钥对原始数据加掩。

[0262] 作为一个实施例,所述加掩是两个数据做异或操作。

[0263] 作为一个实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0264] 作为一个实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0265] 作为一个实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0266] 作为一个实施例,所述一串密钥播包括第一安全密钥。

[0267] 作为一个实施例,所述加密采用TS36.323中描述的加密算法。

[0268] 作为一个实施例,所述完整性保护是指:通过消息验证码-完整性(MAC-I,Message Authentication Code-Integrity)与数据加掩实现。

[0269] 作为一个实施例,所述消息验证码-完整性是通过完整性保护算法实现。

[0270] 作为一个实施例,所述完整性算法保护的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0271] 作为一个实施例,所述完整性算法保护的输入参数包括无线承载标识(Radio Bearer ID)。

[0272] 作为一个实施例,所述完整性算法保护的输入参数包括PDCP序列号(PDCP SN)。

[0273] 作为一个实施例,所述完整性保护算法的输入参数包括第一安全密钥。

[0274] 作为一个实施例,所述完整性保护算法的输入参数包括数据。

[0275] 作为一个实施例,所述第一操作是在用户设备中被执行。

[0276] 作为一个实施例,所述第一操作是由用户设备中的软件程序实现。

[0277] 实施例2

[0278] 实施例2示例了第三操作的示意图,如附图2所示。

[0279] 实施例2中,第一修改的比特组经过第三操作之后变成第一比特组。所述第一比特组和所述第一修改的比特组分别包括正整数个比特。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一。

[0280] 作为一个实施例,所述第一比特组是IP报头。所述第三操作在基站中的PDCP层中被执行。

[0281] 作为一个实施例,所述第三操作包括{解压缩,解密};或者所述第三操作包括{解压缩,解密,完整性验证}。

[0282] 作为一个实施例,所述第一比特组是所述第一修改的比特组依次经过所述完整性验证,所述解密和所述解压缩之后生成的。

[0283] 作为一个实施例,所述第一比特组是所述第一修改的比特组依次经过所述解密和所述解压缩之后生成的。

[0284] 作为一个实施例,所述第一比特组在解压缩之前的比特的数量小于所述第一比特组中的比特的数量。

[0285] 作为一个实施例,对于所述解压缩,输出数据的比特数大于输入数据的比特数。

[0286] 作为一个实施例,所述解压缩是比较原始报头和压缩后的报头获得压缩前的报头。

[0287] 作为一个实施例,所述解压缩是对鲁棒性报头压缩(ROHC,Robust Header Compression)算法的逆操作。

[0288] 作为一个实施例,所述解压缩是对TS36.323表5.5.1.1中示例的压缩算法的逆操作。

[0289] 作为一个实施例,所述解密是原始数据和一串密钥去掩。

[0290] 作为一个子实施例,所述去掩是数据和掩码做抑或操作。

[0291] 作为一个子实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0292] 作为一个子实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0293] 作为一个子实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0294] 作为一个子实施例,所述一串密钥播包括第一安全密钥。

[0295] 作为一个实施例,所述解密是TS36.323描述的解密算法。

[0296] 作为一个实施例,所述完整性验证通过比较X消息验证码-完整性(XMAC-I,Message Authentication Code-Integrity)与消息验证码-完整性实现。

[0297] 作为一个子实施例,所述X消息验证码-完整性与消息验证码-完整性一致,则完整性验证通过,反之则不通过。

[0298] 作为一个子实施例,所述X消息验证码-完整性是通过完整性验证算法实现。

[0299] 作为一个子实施例,所述完整性验证算法的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0300] 作为一个子实施例,所述完整性验证算法的输入参数包括无线承载标识(Radio Bearer ID)。

[0301] 作为一个子实施例,所述完整性验证算法的输入参数包括PDCP序列号(PDCP SN)。

[0302] 作为一个子实施例,所述完整性验证算法的输入参数包括第一安全密钥。

[0303] 作为一个子实施例,所述完整性验证算法的输入参数包括数据。

[0304] 作为一个实施例,所述第三操作是在基站设备中被执行。

[0305] 作为一个实施例,所述第三操作是由基站设备中的软件程序实现。

[0306] 实施例3

[0307] 实施例3示例了第二操作的示意图,如附图3所示。

[0308] 实施例3中,第二比特组经过第二操作之后变成第二修改的比特组。所述第二比特组和所述第二修改的比特组分别包括正整数个比特。所述第二操作包括{加密,完整性保护}中的至少之一。

[0309] 作为一个实施例,所述第二比特组是IP负载。所述第二操作在UE中的NAS中被执行。

[0310] 作为一个实施例,所述第二操作包括加密;或者所述第二操作包括{加密,完整性保护}。

[0311] 作为一个实施例,所述第二修改的比特组是所述第二比特组依次经过所述加密和所述完整性保护之后生成的。

[0312] 作为一个实施例,所述第二修改的比特组是所述第二比特组经过所述加密之后生成的。

[0313] 作为一个实施例,所述加密被用于保证数据在发端和收端之间保持机密。

[0314] 作为一个实施例,所述加密是采用一串密钥对原始数据加掩。

[0315] 作为一个实施例,所述加掩是两个数据做异或操作。

[0316] 作为一个实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0317] 作为一个实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0318] 作为一个实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0319] 作为一个实施例,所述一串密钥播包括第一安全密钥。

[0320] 作为一个实施例,所述加密采用TS36.323中描述的加密算法。

[0321] 作为一个实施例,所述完整性保护是指:通过消息验证码-完整性(MAC-I,Message Authentication Code-Integrity)与数据加掩实现。

[0322] 作为一个实施例,所述消息验证码-完整性是通过完整性保护算法实现。

[0323] 作为一个实施例,所述完整性算法保护的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0324] 作为一个实施例,所述完整性算法保护的输入参数包括无线承载标识(Radio Bearer ID)。

[0325] 作为一个实施例,所述完整性算法保护的输入参数包括PDCP序列号(PDCP SN)。

[0326] 作为一个实施例,所述完整性保护算法的输入参数包括第一安全密钥。

[0327] 作为一个实施例,所述完整性保护算法的输入参数包括数据。

[0328] 作为一个实施例,所述第二操作是在用户设备中被执行。

[0329] 作为一个实施例,所述第二操作是由用户设备中的软件程序实现。

[0330] 实施例4

[0331] 实施例4示例了第四操作的示意图,如附图4所示。

[0332] 实施例4中,第二修改的比特组经过第四操作之后变成第二比特组。所述第二比特组和所述第二修改的比特组分别包括正整数个比特。所述第四操作包括{解密,完整性验证}中的至少之一。

[0333] 作为一个实施例,所述第二比特组是IP负载。所述第四操作在核心网设备中的NAS中被执行。

[0334] 作为一个实施例,所述第四操作包括解密;或者所述第四操作包括{解密,完整性验证}。

[0335] 作为一个实施例,所述第二比特组是所述第二修改的比特组依次经过所述完整性验证和所述解密之后生成的。

[0336] 作为一个实施例,所述第二比特组是所述第二修改的比特组经过所述解密之后生成的。

[0337] 作为一个实施例,所述解密是原始数据和一串密钥去掩。

[0338] 作为一个子实施例,所述去掩是数据和掩码做抑或操作。

[0339] 作为一个子实施例,所述一串密钥包括超帧号(HFN,Hyper Frame Number)。

[0340] 作为一个子实施例,所述一串密钥包括无线承载标识(Radio Bearer ID)。

[0341] 作为一个子实施例,所述一串密钥包括PDCP序列号(PDCP SN)。

[0342] 作为一个子实施例,所述一串密钥播包括第一安全密钥。

[0343] 作为一个实施例,所述解密是TS36.323描述的解密算法。

[0344] 作为一个实施例,所述完整性验证通过比较X消息验证码-完整性(XMAC-I,Message Authentication Code-Integrity)与消息验证码-完整性实现。

[0345] 作为一个子实施例,所述X消息验证码-完整性与消息验证码-完整性一致,则完整性验证通过,反之则不通过。

[0346] 作为一个子实施例,所述X消息验证码-完整性是通过完整性验证算法实现。

[0347] 作为一个子实施例,所述完整性验证算法的输入参数包括超帧号(HFN,Hyper Frame Number)。

[0348] 作为一个子实施例,所述完整性验证算法的输入参数包括无线承载标识(Radio Bearer ID)。

[0349] 作为一个子实施例,所述完整性验证算法的输入参数包括PDCP序列号(PDCP SN)。

[0350] 作为一个子实施例,所述完整性验证算法的输入参数包括第一安全密钥。

[0351] 作为一个子实施例,所述完整性验证算法的输入参数包括数据。

[0352] 作为一个实施例,所述第四操作是在非接入网设备即核心网设备中被执行。

[0353] 作为一个实施例,所述第四操作是由核心网设备中的软件程序实现。

[0354] 实施例5

[0355] 实施例5示例了第一操作和第三操作的示意图,如附图5所示。

[0356] 实施例5中,所述第一操作包括{压缩,加密,完整性保护}中的至少前两者,所述第三操作包括{完整性验证,解密,解压缩}中的至少后两者。

[0357] 实施例5中,所述压缩和所述解压缩互为逆操作,所述加密和所述解密互为逆操作,所述完整性保护和所述完整性验证互为逆操作。

[0358] 作为一个实施例,所述第一操作和所述第三操作分别在UE和基站中被执行。

[0359] 作为一个实施例,所述第一操作和所述第三操作分别在UE的PDCP层和基站的PDCP层中被执行。

[0360] 作为一个实施例,所述第一操作和所述第三操作分别在UE和基站的对等的层中被执行。

[0361] 实施例6

[0362] 实施例6示例了第二操作和第四操作的示意图,如附图6所示。

[0363] 实施例6中,所述第二操作包括{加密,完整性保护}中的至少前者,所述第四操作包括{完整性验证,解密}中的至少后者。

[0364] 实施例6中,所述加密和所述解密互为逆操作,所述完整性保护和所述完整性验证互为逆操作。

[0365] 作为一个实施例,所述第二操作和所述第四操作分别在UE和核心网设备中被执行。

[0366] 作为一个实施例,所述第二操作和所述第四操作分别在UE的NAS和核心网设备的NAS中被执行。

[0367] 作为一个实施例,所述第一操作和所述第三操作分别在UE和核心网设备的对等的层中被执行。

[0368] 实施例7

[0369] 实施例7示例了上行数据的发送和接收的流程图,如附图7所示。附图7中,步骤S31是可选的。

[0370] 实施例7中,UE维护下层C0,第一层C1,第二层C2;基站维护下层D0和第一层D1;核心网设备维护第二层D2。

[0371] 在步骤S10中,第二层C2执行第二操作,传递第一比特组和所述第二修改的比特组给所述第一层C1;在步骤S11中,第一层C1执行第一操作,传递第一比特集合给下层C0。

[0372] 在步骤S21中,第一层D1从下层D0接收第一比特集合,第一层D1执行第三操作;在步骤S20中,第一层D1传递第一比特组和所述第二修改的比特组给第二层D2,第二层D2执行第四操作。

[0373] 实施例7中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出。所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一。第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组属于同一个协议数据单元。所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。

[0374] 作为一个实施例,所述协议数据单元是PDCP PDU。

[0375] 作为一个实施例,在步骤S31中,第二层D2发送所述目标信息给第二层C2。

[0376] 作为上述实施例的一个子实施例,第二层D2和第二层C2之间的数据通道包括{第

一层D1,下层D0,无线信道,下层C0,第一层C1}。

[0377] 作为一个实施例,所述目标信息包括{本申请中的所述第一信息,本申请中的所述第二信息}中的至少之一。

[0378] 作为一个实施例,所述目标信息是通过RRC信令承载的。

[0379] 作为一个实施例,所述目标信息是通过NAS信息承载的。

[0380] 作为一个实施例,下层C0,第一层C1,第二层C2,下层D0和第一层D1和第二层D2分别包括RLC层,PDCP层,NAS,RLC层,PDCP层和NAS。

[0381] 作为上述实施例的一个子实施例,第一层C1还包括RRC(Radio Resource Control,无线资源控制)层,第一层D1还包括RRC层。

[0382] 作为上述实施例的一个子实施例,下层D0还包括MAC(Media Access Control,媒体介入控制)层和物理层,下层C0还包括MAC层和物理层。

[0383] 作为一个实施例,所述核心网设备和所述基站之间通过S1接口连接。

[0384] 作为一个实施例,所述第一修改的比特组和所述第二修改的比特组属于同一个PDCP PDU。

[0385] 实施例8

[0386] 实施例8示例了上行数据的发送的流程图,如附图8所示。附图8中,第二层,第一层和下层都是由UE维护的。

[0387] 实施例8中,第二层对来{第一比特组,第二比特组}中的后者执行第二操作后传递(Diliver)给下层;第一层对来自第二层的{第一比特组,第二修改的比特组}中的前者进行第一操作后传递给下层;第一层将来自第二层的第二修改的比特组透明的传递给下层。所述第一修改的比特组和所述第二修改的比特组属于一个高层PDU。

[0388] 作为一个实施例,所述下层是RLC层。

[0389] 作为一个实施例,所述第一层包括{PDCP层,RRC层}中的至少前者,所述第二层是NAS。

[0390] 作为一个实施例,本申请中的第二信息被用于确定:

[0391] -.所述第一层和所述第二层分别是PDCP层和NAS;或者

[0392] -.所述第一层和所述第二层都属于PDCP层;或者

[0393] -.所述第一层和所述第二层都属于NAS。

[0394] 实施例9

[0395] 实施例9示例了上行数据的接收的流程图,如附图9所示。附图9中,下层是由基站维护的。

[0396] 实施例9中,第一层接收来自下层的第一修改的比特组和第二修改的比特组;第一层对其中的第一修改的比特组执行第三操作,把其中的第二修改的比特组透明的传递给第二层;第二层对接收到的所述第二修改的比特组执行第四操作。所述第一修改的比特组和所述第二修改的比特组属于一个高层PDU。

[0397] 作为一个实施例,所述下层是RLC层。

[0398] 作为一个实施例,所述第一层和所述第二层分别是PDCP层和NAS,所述第一层和所述第二层分别被基站和UPS维护。

[0399] 作为一个实施例,本申请中的第二信息被用于确定:

[0400] -.所述第一层和所述第二层分别是PDCP层和NAS;或者

[0401] -.所述第一层和所述第二层都属于PDCP层;或者

[0402] -.所述第一层和所述第二层都属于NAS。

[0403] 实施例10

[0404] 实施例10示例了第一比特集合的示意图,如附图10所示。

[0405] 实施例10中,所述第一比特集合是由第三比特组,第一修改的比特组和第二修改的比特组依次级联而成。

[0406] 作为一个实施例,所述第一比特集合是一个PDCP PDU,所述第三比特组包括PDCP报头(Header)。

[0407] 实施例11

[0408] 实施例11示例了一个网络切片的示意图,如附图11所示。附图11中,给定RAT(Radio Access Technology,无线接入技术)包含三个所述网络切片,所示网络切片#1对应用户类型#1,所示网络切片#2对应用户类型#2,所示网络切片#3对应用户类型#3。所示网络切片#1对应业务组#1,所示网络切片#2对应业务组#2,所示网络切片#3对应业务组#3。

[0409] 作为一个实施例,所述用户类型#1针对移动宽带用户。

[0410] 作为一个实施例,所述用户类型#2针对一般IOT(Internet of Things,物联网)用户。

[0411] 作为一个实施例,所述用户类型#3针对特殊需求的IOT用户。

[0412] 作为一个实施例,所述特殊需求的IOT用户对应医疗类IOT用户。

[0413] 作为一个实施例,所述特殊需求的IOT用户对应车联网IOT用户。

[0414] 作为一个实施例,所述特殊需求的IOT用户对应工业机器人IOT用户。

[0415] 作为一个子实施例,所述业务组#1包括{无线通信,互联网}业务中的至少之一。

[0416] 作为一个子实施例,所述业务组#2包括{物流,农业,气象}业务中的至少之一。

[0417] 作为一个子实施例,所述业务组#3包括{自动驾驶,工业制造}业务中的至少之一。

[0418] 作为一个子实施例,所述给定RAT是基于5G技术的RAT。

[0419] 作为一个子实施例,所述给定RAT是基于NR(New Radio,新无线)技术的RAT。

[0420] 实施例12

[0421] 实施例12示例了一个UE中的处理装置的结构框图,如附图12所示。附图12中,UE处理装置100主要由第一处理模块101和第二处理模块102组成。

[0422] 第一处理模块101用于在第二层执行第二操作;第二处理模块102用于在第一层执行第一操作

[0423] 实施例12中,第一比特组被用于所述第一操作的输入,第一修改的比特组是所述第一操作的输出;第二比特组被用于所述第二操作的输入,第二修改的比特组是所述第二操作的输出。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。所述比特组中包括正整数个比特。所述第一操作包括{压缩,加密,完整性保护}中的至少之一,所述第二操作包括{加密,完整性保护}中的至少之一。

[0424] 作为一个实施例,所述第一处理模块101还用于以下至少之一:

[0425] -步骤A10.接收第一信息。

[0426] -步骤A11.接收第二信息。

[0427] 其中,所述第一信息被用于所述第一操作和所述第二操作。所述第二信息被用于确定所述第一操作和所述第二操作分别在所述第一层和所述第二层中被执行。所述第一层包括PDCP层,所述第二层是NAS。

[0428] 作为一个实施例,所述第一处理模块101还用于从所述第二层传递第一比特组和所述第二修改的比特组给所述第一层;所述第二处理模块102还用于从所述第一层传递第一比特集合给下层。其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。

[0429] 作为一个实施例,所述第一比特块是IP报头,所述第二比特块是IP负载。

[0430] 实施例13

[0431] 实施例13示例了一个基站中的处理装置的结构框图,如附图13所示。附图13中,基站处理装置200主要由第三处理模块201组成。

[0432] 所述第三处理模块201用于在第一层执行{第三操作,第四操作}中的所述第三操作。

[0433] 实施例13中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个协议数据单元。

[0434] 作为一个实施例,所述第三处理模块201还用于:

[0435] -.从下层接收第一比特集合

[0436] -.传递第一比特组和所述第二修改的比特组给第二层。

[0437] 其中,所述第一比特集合包括所述第一修改的比特组和所述第二修改的比特组。所述第四操作是在所述第二层中被执行。所述第二层是由核心网设备维护的。

[0438] 作为一个实施例,所述第三处理模块201还用于以下至少之一:

[0439] -步骤A10.通过S1接口接收第一信息;并且通过空中接口发送第一信息。

[0440] -步骤A11.通过S1接口接收第二信息;或者通过空中接口发送第二信息。

[0441] 其中,所述第一信息被用于所述第三操作和所述第四操作。所述第二信息被用于确定所述第一层和所述第二层;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。

[0442] 实施例14

[0443] 实施例14示例了一个核心王设备中的处理装置的结构框图,如附图14所示。附图14中,核心网设备的处理装置300主要由第四处理模块301组成。

[0444] 所述第四处理模块301用于在第二层执行{第三操作,第四操作}中的所述第四操作。

[0445] 实施例14中,第一修改的比特组被用于所述第三操作的输入,第一比特组是所述第三操作的输出;第二修改的比特组被用于第四操作的输入,第二比特组是所述第四操作的输出。所述第三操作包括{解压缩,解密,完整性验证}中的至少之一,所述第四操作包括{解密,完整性验证}中的至少之一。所述第一修改的比特组和所述第二修改的比特组对应同一个PDCP PDU。

[0446] 作为一个实施例,所述第四处理模块301还用于:

[0447] -.从第一层接收第一比特组和第二修改的比特组。

[0448] 其中,所述第三操作是在所述第一层中被执行。所述第一层是由基站设备维护的。

[0449] 作为一个实施例,所述第四处理模块301还用于以下至少之一:

[0450] -.通过S1接口发送第一信息;

[0451] -.通过S1接口发送第二信息。

[0452] 其中,所述第一信息被用于所述第三操作和所述第四操作。所述第二信息被用于确定{所述第一层,所述第二层}中的至少后者;或者所述第二信息被用于确定{所述第一层,所述第二层}是否相同。所述第二层是NAS,所述第一层是PDCP层。所述第一信息是网络切片(Slice)特定的。所述第二信息是网络切片(Slice)特定的。

[0453] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可以通过程序来指令相关硬件完成,所述程序可以存储于计算机可读存储介质中,如只读存储器,硬盘或者光盘等。可选的,上述实施例的全部或部分步骤也可以使用一个或者多个集成电路来实现。相应的,上述实施例中的各模块单元,可以采用硬件形式实现,也可以由软件功能模块的形式实现,本申请不限于任何特定形式的软件和硬件的结合。本申请中的UE和终端包括但不限于RFID,物联网终端设备,MTC(Machine Type Communication,机器类型通信)终端,车载通信设备,无线传感器,上网卡,手机,平板电脑,笔记本等无线通信设备。本申请中的基站,基站设备,和网络侧设备包括但不限于宏蜂窝基站,微蜂窝基站,家庭基站,中继基站等无线通信设备。

[0454] 以上所述,仅为本申请的较佳实施例而已,并非用于限定本申请的保护范围。凡在本申请的精神和原则之内,所做的任何修改,等同替换,改进等,均应包含在本申请的保护范围之内。

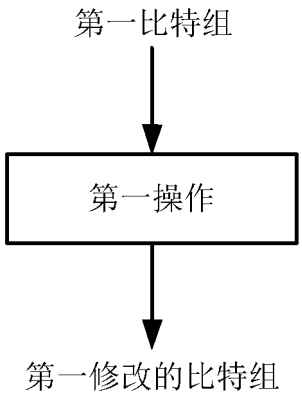

第一比特组
第一操作
第一修改的比特组

图1

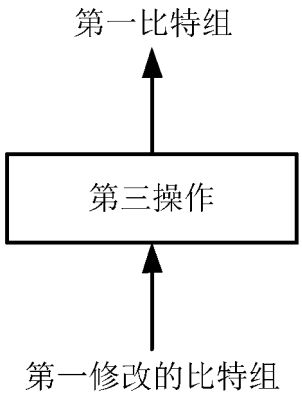

第一比特组
第三操作
第一修改的比特组

图2

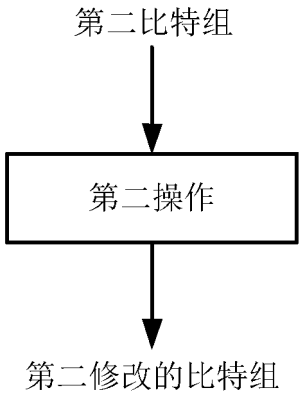

第二比特组
第二操作
第二修改的比特组

图3

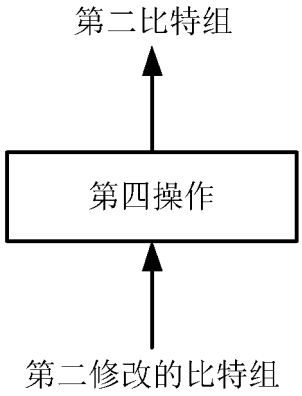

第二比特组
第四操作
第二修改的比特组

图4

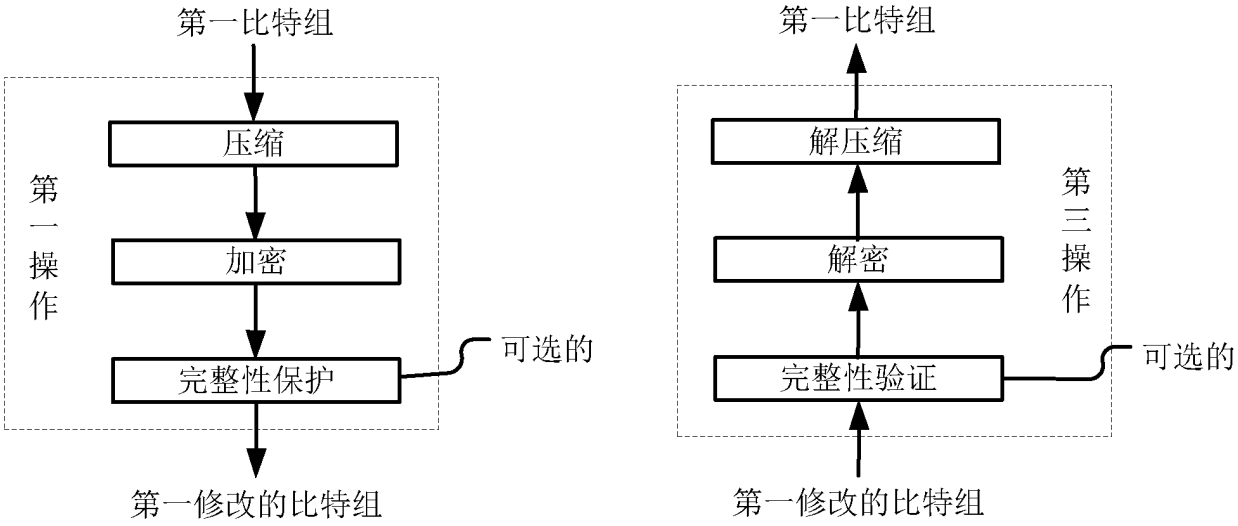

第一比特组
压缩
加密
完整性保护
第一操作
可选的
第一修改的比特组
第一比特组
解压缩
解密
完整性验证
第三操作
可选的
第一修改的比特组

图5

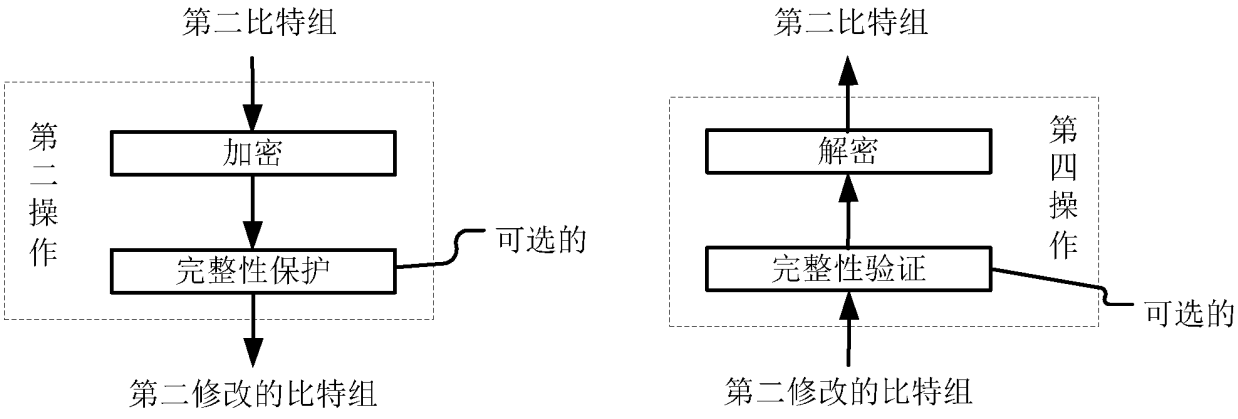

第二比特组
加密
完整性保护
第二操作
可选的
第二修改的比特组
第二比特组
解密
完整性验证
第四操作
可选的
第二修改的比特组

图6

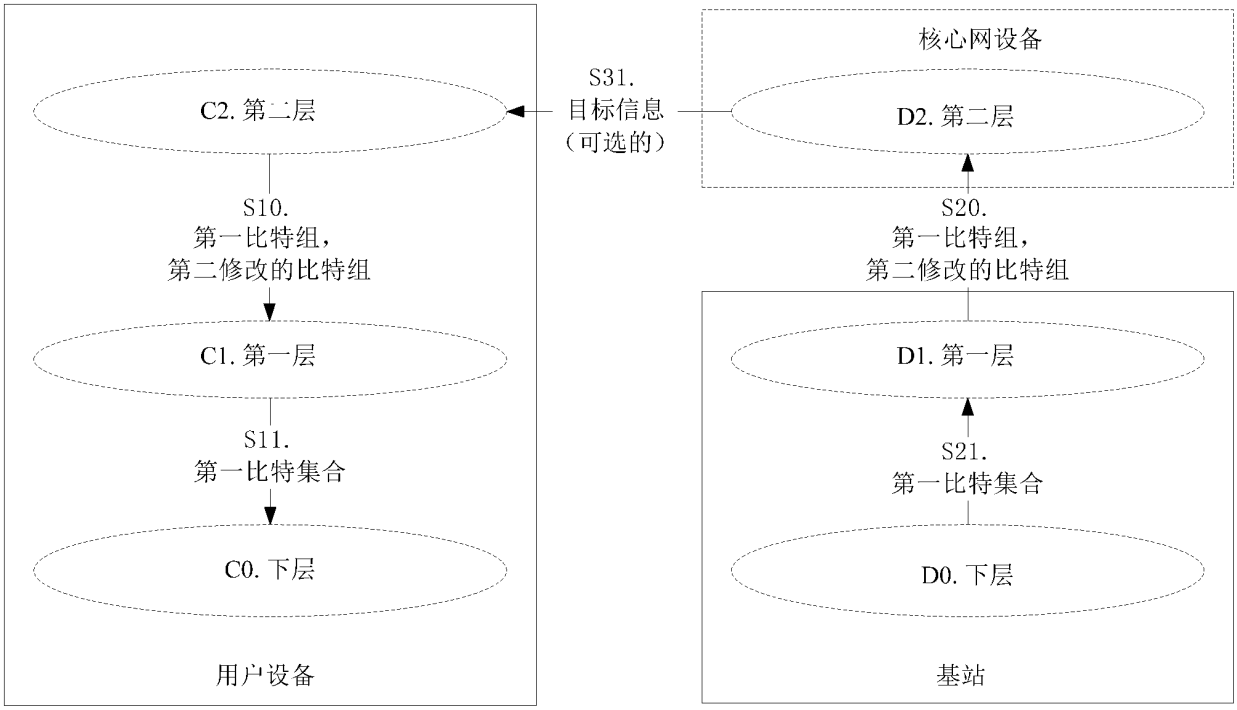

核心网设备
C2. 第二层
S31.
目标信息
（可选的）
D2. 第二层
S10.
第一比特组，
第二修改的比特组
S20.
第一比特组，
第二修改的比特组
C1. 第一层
D1. 第一层
S11.
第一比特集合
S21.
第一比特集合
C0. 下层
D0. 下层
用户设备
基站

图7

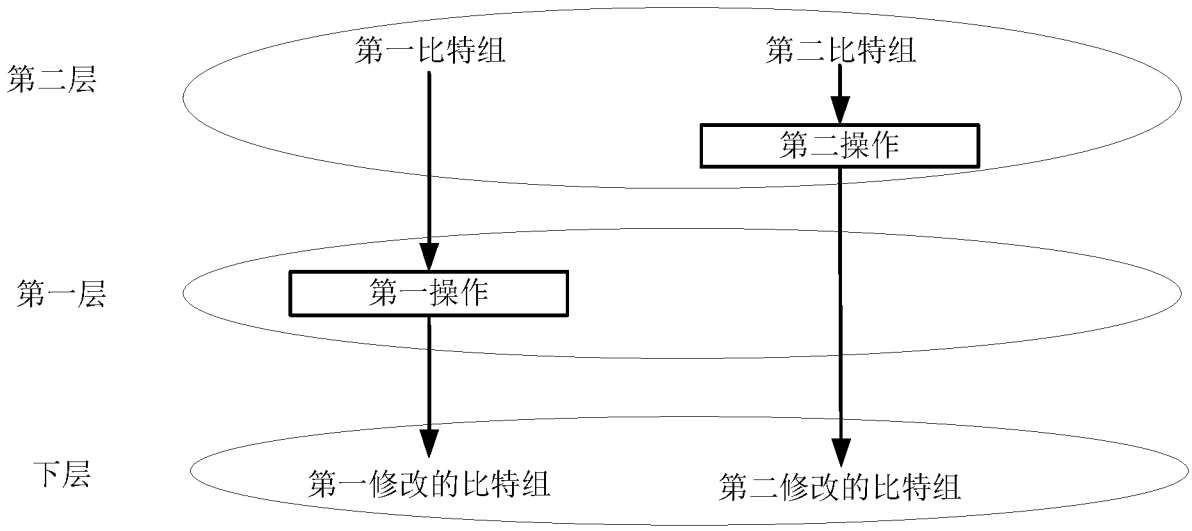

第二层
第一比特组
第二比特组
第二操作
第一层
第一操作
下层
第一修改的比特组
第二修改的比特组

图8

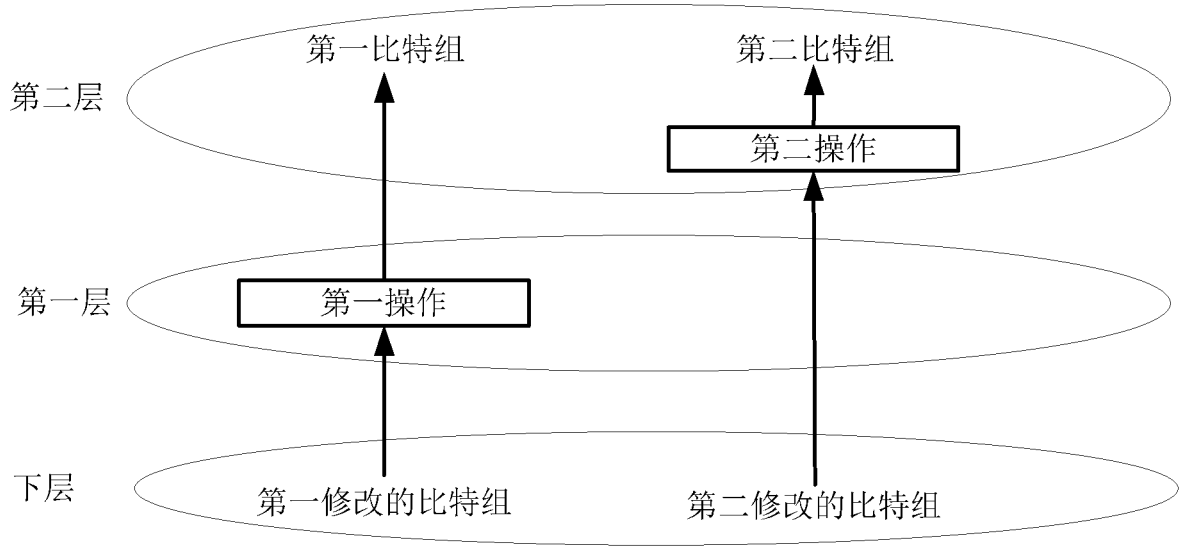

第一比特组
第二比特组
第二层
第二操作
第一层
第一操作
下层
第一修改的比特组
第二修改的比特组

图9

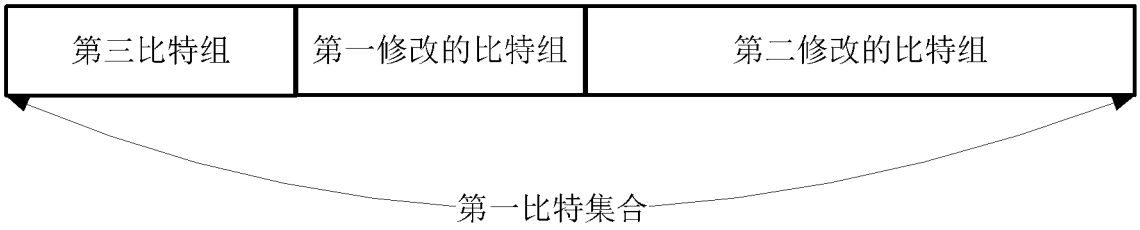

第三比特组
第一修改的比特组
第二修改的比特组
第一比特集合

图10

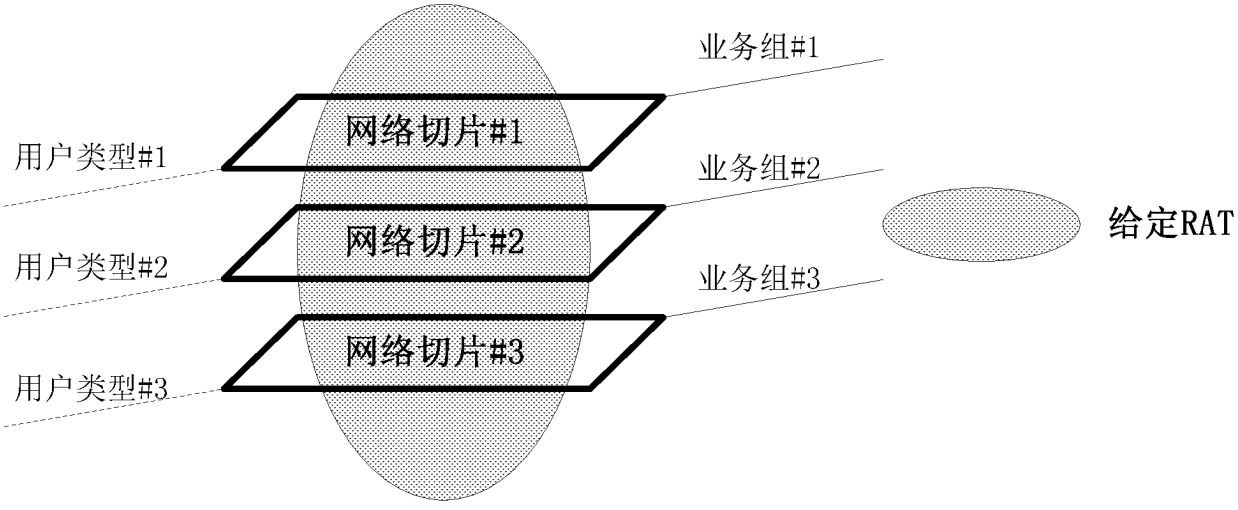

业务组#1
网络切片#1
用户类型#1
业务组#2
网络切片#2
给定RAT
用户类型#2
业务组#3
网络切片#3
用户类型#3

图11

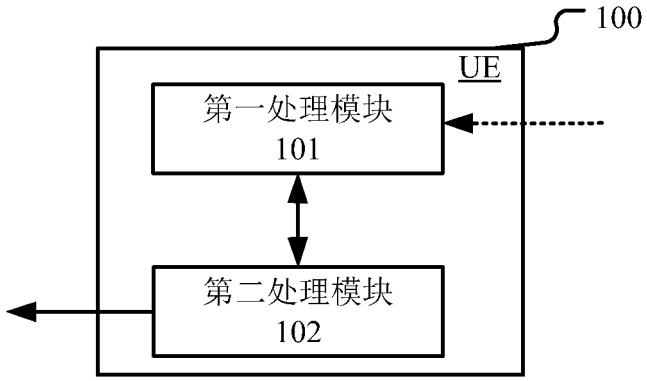

100
UE
第一处理模块
101
第二处理模块
102

图12


200
基站
第三处理模块
201

图13


300
核心网设备
第四处理模块
301

图14