(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107005410 B
(45)授权公告日 2020.06.26

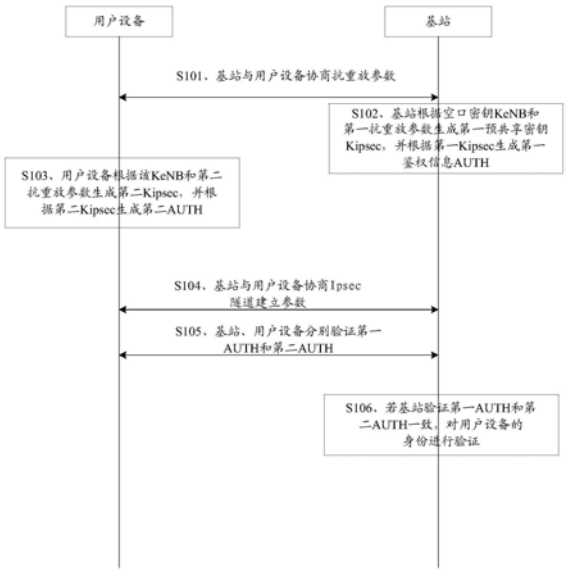
(21)申请号 201580035366.5
(22)申请日 2015.10.31
(65)同一申请的已公布的文献号
申请公布号 CN 107005410 A
(43)申请公布日 2017.08.01
(85)PCT国际申请进入国家阶段日
2017.01.03
(86)PCT国际申请的申请数据
PCT/CN2015/093536 2015.10.31
(87)PCT国际申请的公布数据
WO2017/070973 ZH 2017.05.04
(73)专利权人 大势至(北京)软件工程有限公司
地址 100080 北京市海淀区学清路甲18号中关村东升科技园学院园东配楼2层208室
专利权人 华为技术有限公司
(72)发明人 陈璟 李赫
(74)专利代理机构 北京同辉知识产权代理事务所(普通合伙) 11357
代理人 饶富春
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
CN 104969578 A,2015.10.07,
US 2015281254 A1,2015.10.01,
CN 103312668 A,2013.09.18,
CN 101272251 A,2008.09.24,
CN 104184675 A,2014.12.03,
CN 101945387 A,2011.01.12,
JP 5319575 B2,2013.10.16,
US 7159242 B2,2007.01.02,
审查员 刘旭
权利要求书8页 说明书17页 附图8页

(54)发明名称

因特网协议安全性隧道建立方法,用户设备及基站

(57)摘要

本发明实施例公开了一种因特网协议安全性IPsec隧道建立方法,用户设备及基站。在用户设备通过无线局域网请求接入核心网时,基站与用户设备协商抗重放参数及IPsec隧道建立参数,建立IPsec隧道,以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据,从而实现用户设备通过无线局域网安全地接入核心网,保证了数据传输的安全性。



CN 107005410 B

1.一种因特网协议安全性IPsec隧道建立方法,其特征在于,包括:

基站发送第一抗重放参数给用户设备;

所述基站确定所述用户设备的第二抗重放参数,所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同;

所述基站根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec,并根据所述第一Kipsec生成第一鉴权信息AUTH;

所述基站确定IPsec隧道建立参数,所述IPsec隧道建立参数包括第二AUTH,其中,所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec,并根据所述第二Kipsec生成所述第二AUTH;

若所述基站验证所述第一AUTH和所述第二AUTH一致,对所述用户设备的身份进行验证。

2.如权利要求1所述的方法,其特征在于,还包括:

所述基站将所述基站的互联网协议IP地址发送给所述用户设备;

所述基站接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址。

3.如权利要求1或2所述的方法,其特征在于,所述IPsec隧道建立参数还包括IPsec隧道传输参数,所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS,所述第一安全参数包括安全算法,以及所述第一Kipsec或所述第二Kipsec。

4.如权利要求3所述的方法,其特征在于,所述基站确定IPsec隧道建立参数,包括:

所述基站接收所述用户设备发送的第一因特网密钥交换协议版本2IKEv2消息,所述第一IKEv2消息包括第二安全参数;

所述基站发送所述第一IKEv2消息的响应消息给所述用户设备;

所述基站接收所述用户设备根据所述第二安全参数加密发送的第二IKEv2消息,所述第二IKEv2消息包括所述IPsec隧道建立参数;

所述基站发送所述第二IKEv2消息的响应消息给所述用户设备;

其中,所述IPsec隧道建立参数中还包括所述用户设备的身份标识,和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI;所述安全算法为设置有安全算法级别的安全算法。

5.如权利要求4所述的方法,其特征在于,所述基站验证所述用户设备的身份,包括:

所述基站验证所述用户设备的身份标识是否与核心网侧已获得的所述用户设备的身份一致。

6.如权利要求4所述的方法,其特征在于,所述基站确定IPsec隧道建立参数,包括:

所述基站接收所述用户设备发送的至少一个无线资源控制RRC消息;

其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

7.如权利要求3所述的方法,其特征在于,所述基站确定IPsec隧道建立参数,包括:

所述基站接收所述用户设备通过无线资源控制RRC消息发送的所述第二AUTH和所述用户设备所支持的安全算法列表;

所述基站根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,

确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

所述基站将所述IPsec隧道建立参数发送给所述用户设备。

8.如权利要求3所述的方法，其特征在于，所述基站确定IPsec隧道建立参数，包括：

所述基站通过RRC消息将所述第二AUTH和所述基站的安全算法级别列表发送给所述用户设备，以使所述用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

所述基站接收所述用户设备发送的所述IPsec隧道建立参数。

9.一种IPsec隧道建立方法，其特征在于，包括：

用户设备接收基站发送的第一抗重放参数；

所述用户设备确定所述用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

所述用户设备根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec，并根据所述第二Kipsec生成第二鉴权信息AUTH，并发送所述第二AUTH给所述基站；

所述用户设备接收所述基站发送的IPsec隧道建立参数，所述IPsec隧道建立参数包括第一AUTH，其中，所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec，所述基站根据第一Kipsec生成所述第一AUTH；

所述用户设备验证所述第一AUTH和所述第二AUTH。

10.如权利要求9所述的方法，其特征在于，还包括：

所述用户设备接收所述基站发送的所述基站的互联网协议IP地址；

所述用户设备将所述用户设备连接的无线局域网的IP地址发送给所述基站。

11.如权利要求9或10所述的方法，其特征在于，还包括：

所述用户设备发送第一IKEv2消息给所述基站，所述第一IKEv2消息包括第二安全参数；

所述用户设备接收所述基站发送的所述第一IKEv2消息的响应消息；

所述用户设备根据所述第二安全参数加密第二IKEv2消息，将加密后的所述第二IKEv2消息发送给所述基站，所述第二IKEv2消息包括所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec，所述安全算法为设置有安全算法级别的安全算法；

所述用户设备接收所述基站发送的所述第二IKEv2消息的响应消息。

12.如权利要求11所述的方法，其特征在于，还包括：

所述用户设备发送至少一个RRC消息给所述基站；

其中，所述至少一个RRC消息封装所述第一IKEv2消息，所述第一IKEv2消息的响应消息，所述第二IKEv2消息，以及所述第二IKEv2消息的响应消息。

13.如权利要求9或10所述的方法，其特征在于，还包括：

所述用户设备通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站，以使所述基站根据自身的安全算法级别列表，以及所述用户设备所支持的安全算法列表，确定第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

所述用户设备接收所述基站发送的所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

14.如权利要求9或10所述的方法，其特征在于，还包括：

所述用户设备接收所述基站通过RRC消息发送的所述基站的安全算法级别列表，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

所述用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定第一安全参数的安全算法的级别；

所述用户设备将所述IPsec隧道建立参数发送给所述基站，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

15.一种基站，其特征在于，包括：

发送单元，用于发送第一抗重放参数给用户设备；

确定单元，用于确定所述用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

生成单元，用于根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec，并根据所述第一Kipsec生成第一鉴权信息AUTH；

所述确定单元还用于确定IPsec隧道建立参数，所述IPsec隧道建立参数包括第二AUTH，其中，所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec，并根据所述第二Kipsec生成所述第二AUTH；

验证单元，用于若验证所述第一AUTH和所述第二AUTH一致，对所述用户设备的身份进行验证。

16.如权利要求15所述的基站，其特征在于：

所述发送单元还用于将所述基站的互联网协议IP地址发送给所述用户设备；

所述基站还包括：接收单元；

所述接收单元还用于接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址。

17.如权利要求16所述的基站，其特征在于，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec。

18.如权利要求17所述的基站，其特征在于：

所述接收单元还用于接收所述用户设备发送的第一因特网密钥交换协议版本2IKEv2

消息,所述第一IKEv2消息包括第二安全参数;

所述发送单元还用于发送所述第一IKEv2消息的响应消息给所述用户设备;

所述接收单元还用于接收所述用户设备根据所述第二安全参数加密发送的第二IKEv2消息,所述第二IKEv2消息包括所述IPsec隧道建立参数;

所述发送单元还用于发送所述第二IKEv2消息的响应消息给所述用户设备;

其中,所述IPsec隧道建立参数中还包括所述用户设备的身份标识,和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI;所述安全算法为设置有安全算法级别的安全算法。

19.如权利要求18所述的基站,其特征在于,所述验证单元具体用于:

验证所述用户设备的身份标识是否与核心网侧已获得的所述用户设备的身份一致。

20.如权利要求17所述的基站,其特征在于:

所述接收单元还用于接收所述用户设备发送的至少一个无线资源控制RRC消息;

其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

21.如权利要求17所述的基站,其特征在于:

所述接收单元还用于接收所述用户设备通过无线资源控制RRC消息发送的所述第二AUTH和所述用户设备所支持的安全算法列表;

所述确定单元还用于根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述发送单元还用于将所述IPsec隧道建立参数发送给所述用户设备。

22.如权利要求17所述的基站,其特征在于:

所述发送单元还用于通过RRC消息将所述第二AUTH和所述基站的安全算法级别列表发送给所述用户设备,以使所述用户设备根据自身所支持的安全算法列表,以及所述基站的安全算法级别列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述接收单元还用于接收所述用户设备发送的所述IPsec隧道建立参数。

23.一种用户设备,其特征在于,包括:

确定单元,用于确定用户设备的第二抗重放参数,第一抗重放参数和第二抗重放参数分别用于防止基站和所述用户设备每次生成的密钥相同;

生成单元,用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec,并根据所述第二Kipsec生成第二鉴权信息AUTH;

发送单元,用于发送所述第二AUTH给所述基站;

接收单元,用于接收所述基站发送的IPsec隧道建立参数,所述IPsec隧道建立参数包括第一AUTH,其中,所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec,所述基站根据第一Kipsec生成所述第一AUTH;

验证单元,用于验证所述第一AUTH和所述第二AUTH。

24.如权利要求23所述的用户设备,其特征在于:

所述接收单元还用于接收所述基站发送的所述基站的互联网协议IP地址;

所述发送单元还用于将所述用户设备连接的无线局域网的IP地址发送给所述基站。

25.如权利要求23或24所述的用户设备,其特征在于:

所述发送单元还用于发送第一IKEv2消息给所述基站,所述第一IKEv2消息包括第二安全参数;

所述接收单元还用于接收所述基站发送的所述第一IKEv2消息的响应消息;

所述发送单元还用于根据所述第二安全参数加密第二IKEv2消息,将加密后的所述第二IKEv2消息发送给所述基站,所述第二IKEv2消息包括所述IPsec 隧道建立参数,所述IPsec隧道建立参数还包括IPsec隧道传输参数,所述用户设备的身份标识,和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS,所述第一安全参数包括安全算法,以及所述第一Kipsec或所述第二Kipsec,所述安全算法为设置有安全算法级别的安全算法;

所述接收单元还用于接收所述基站发送的所述第二IKEv2消息的响应消息。

26.如权利要求25所述的用户设备,其特征在于:

所述发送单元还用于发送至少一个RRC消息给所述基站;

其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

27.如权利要求23或24所述的用户设备,其特征在于:

所述发送单元还用于通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站,以使所述基站根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述接收单元还用于接收所述基站发送的所述IPsec隧道建立参数,所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和TS,所述第一安全参数包括确定所述级别的安全算法,以及所述第一Kipsec或所述第二Kipsec。

28.如权利要求23或24所述的用户设备,其特征在于:

所述接收单元还用于接收所述基站通过RRC消息发送的所述基站的安全算法级别列表,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述确定单元还用于根据自身所支持的安全算法列表,以及所述基站的安全算法级别列表,确定第一安全参数的安全算法的级别;

所述发送单元还用于将所述IPsec隧道建立参数发送给所述基站,所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和TS,所述第一安全参数包括确定所述级别的安全算法,以及所述第一Kipsec或所述第二Kipsec。

29.一种基站,其特征在于,包括:发送器和处理器;

所述发送器,用于发送第一抗重放参数给用户设备;

所述处理器,用于确定所述用户设备的第二抗重放参数,所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同;

所述处理器还用于根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec,并根据所述第一Kipsec生成第一鉴权信息AUTH;

所述处理器还用于确定IPsec隧道建立参数,所述IPsec隧道建立参数包括第二AUTH,其中,所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec,并根据所述第二Kipsec生成所述第二AUTH;

所述处理器还用于若验证所述第一AUTH和所述第二AUTH一致,对所述用户设备的身份进行验证。

30.如权利要求29所述的基站,其特征在于:

所述发送器还用于将所述基站的互联网协议IP地址发送给所述用户设备;

所述基站还包括:接收器;

所述接收器还用于接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址。

31.如权利要求30所述的基站,其特征在于,所述IPsec隧道建立参数还包括IPsec隧道传输参数,所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS,所述第一安全参数包括安全算法,以及所述第一Kipsec或所述第二Kipsec。

32.如权利要求31所述的基站,其特征在于:

所述接收器还用于接收所述用户设备发送的第一因特网密钥交换协议版本2IKEv2消息,所述第一IKEv2消息包括第二安全参数;

所述发送器还用于发送所述第一IKEv2消息的响应消息给所述用户设备;

所述接收器还用于接收所述用户设备根据所述第二安全参数加密发送的第二IKEv2消息,所述第二IKEv2消息包括所述IPsec隧道建立参数;

所述发送器还用于发送所述第二IKEv2消息的响应消息给所述用户设备;

其中,所述IPsec隧道建立参数中还包括所述用户设备的身份标识,和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI;所述安全算法为设置有安全算法级别的安全算法。

33.如权利要求32所述的基站,其特征在于,所述处理器还用于:

验证所述用户设备的身份标识是否与核心网侧已获得的所述用户设备的身份一致。

34.如权利要求31所述的基站,其特征在于:

所述接收器还用于接收所述用户设备发送的至少一个无线资源控制RRC消息;

其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

35.如权利要求31所述的基站,其特征在于:

所述接收器还用于接收所述用户设备通过无线资源控制RRC消息发送的所述第二AUTH和所述用户设备所支持的安全算法列表;

所述处理器还用于根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述发送器还用于将所述IPsec隧道建立参数发送给所述用户设备。

36.如权利要求31所述的基站,其特征在于:

所述发送器还用于通过RRC消息将所述第二AUTH和所述基站的安全算法级别列表发送给所述用户设备,以使所述用户设备根据自身所支持的安全算法列表,以及所述基站的安全算法级别列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

所述接收器还用于接收所述用户设备发送的所述IPsec隧道建立参数。

37.一种用户设备,其特征在于,包括:处理器、发送器和接收器;其中,

所述处理器,用于确定用户设备的第二抗重放参数,第一抗重放参数和第二抗重放参数分别用于防止基站和所述用户设备每次生成的密钥相同;

所述处理器还用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec,并根据所述第二Kipsec生成第二鉴权信息AUTH;

发送器,用于发送所述第二AUTH给所述基站;

接收器,用于接收所述基站发送的IPsec隧道建立参数,所述IPsec隧道建立参数包括第一AUTH,其中,所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec,所述基站根据第一Kipsec生成所述第一AUTH;

所述处理器还用于验证所述第一AUTH和所述第二AUTH。

38.如权利要求37所述的用户设备,其特征在于:

所述接收器还用于接收所述基站发送的所述基站的互联网协议IP地址;

所述发送单元还用于将所述用户设备连接的无线局域网的IP地址发送给所述基站。

39.如权利要求37或38所述的用户设备,其特征在于:

所述发送器还用于发送第一IKEv2消息给所述基站,所述第一IKEv2消息包括第二安全参数;

所述接收器还用于接收所述基站发送的所述第一IKEv2消息的响应消息;

所述发送器还用于根据所述第二安全参数加密第二IKEv2消息,将加密后的所述第二IKEv2消息发送给所述基站,所述第二IKEv2消息包括所述IPsec隧道建立参数,所述IPsec隧道建立参数还包括IPsec隧道传输参数,所述用户设备的身份标识,和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS,所述第一安全参数包括安全算法,以及所述第一Kipsec或所述第二Kipsec,所述安全算法为设置有安全算法级别的安全算法;

所述接收器还用于接收所述基站发送的所述第二IKEv2消息的响应消息。

40.如权利要求39所述的用户设备,其特征在于:

所述发送器还用于发送至少一个RRC消息给所述基站;

其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

41.如权利要求37或38所述的用户设备,其特征在于:

所述发送器还用于通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站,以使所述基站根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安

全算法级别的对应关系；

所述接收器还用于接收所述基站发送的所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

42.如权利要求37或38所述的用户设备，其特征在于：

所述接收器还用于接收所述基站通过RRC消息发送的所述基站的安全算法级别列表，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

所述处理器还用于根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定第一安全参数的安全算法的级别；

所述发送器还用于将所述IPsec隧道建立参数发送给所述基站，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

因特网协议安全性隧道建立方法,用户设备及基站

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及一种因特网协议安全性(Internet Protocol security,简称IPsec)隧道建立方法,用户设备及基站。

背景技术

[0002] 长期演进系统-无线局域网络聚合(Long Term Evolution-Wireless Local Area Networks,简称LWA),是长期演进(Long Term Evolution,简称LTE)系统利用无线局域网(Wireless Local Area network,简称WLAN)的高数据传输效率特性进行下行传输数据,是数据分流的一种新型技术。其架构定义如图1所示。移动管理实体(Mobility Management Entity,简称MME)/服务网关(Serving Gateway,简称S-GW)为核心网侧节点,在架构中代表核心网侧,长期演进系统基站(Evolved Node B,简称eNB)与核心网侧之间通过S1接口连接,同时eNB与无线局域网络总站(WLAN Terminal,简称WT)通过Xw接口连接。这种架构下,WT和eNB是分开部署的。对于核心网侧来说,WT是透明的,不可见的,即核心网侧不知道WT的存在。一个WT可以连接多个无线局域网接入节点(Access Point,简称AP),用户设备(User Equipment,简称UE)通过与AP相连接入网络。当下行数据到来的时候,eNB通过WT,转发数据给UE,实现WLAN分流。

[0003] 图1所示是在新架构下的LWA技术,要求在新架构下兼容现有WLAN技术。现有WLAN的接入方式是采用图2的架构,通过S2a和S2b接口的方式接入。

[0004] S2a接入方式是UE接入可信的WLAN时所用的接口。可信的WLAN是指WLAN是运营商部署的。在S2a接入方式下,UE接入WLAN完成鉴权后,可以直接连接核心网侧的分组数据网关(Packet Data Network-Gateway,简称P-GW),进而实现使用WLAN上网,进行数据分流。

[0005] S2b接口是ePDG和P-GW之间的接口。UE在接入非可信的WLAN的情况下使用此接口。非可信的WLAN指不是运营商部署的WLAN节点。当用户通过这类非可信的WLAN接入的时候,要通过演进的分组数据域网关(Evloved Packet Data Gateway,简称ePDG)辅助。ePDG是运营商部署的网元,因此ePDG对于运营商来说是可信的,这样可以保证非可信的WLAN没有办法看到、修改UE和核心网侧之间传输的用户数据,进而保证只是利用WLAN传输数据,而不用WLAN提供其他服务。

[0006] 新需求要求兼容现有WLAN,就是指要求兼容S2b接入方式下的非可信的WLAN接入方式。根据图1的架构,可以看到WT和eNB之间没有部署ePDG,因此无法保证在非可信WLAN下保护用户的数据安全。

发明内容

[0007] 本发明实施例提供了一种IPsec隧道建立方法,用户设备及基站,以建立用户设备与基站之间的IPsec隧道,保证用户设备安全地接入核心网,保证数据传输的安全性。

[0008] 第一方面,提供了一种因特网协议安全性IPsec隧道建立方法,包括:

[0009] 基站发送第一抗重放参数给用户设备;

[0010] 所述基站确定所述用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

[0011] 所述基站根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec，并根据所述第一Kipsec生成第一鉴权信息AUTH；

[0012] 所述基站确定IPsec隧道建立参数，所述IPsec隧道建立参数包括第二AUTH，其中，所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec，并根据所述第二Kipsec生成所述第二AUTH；

[0013] 所述基站验证所述第一AUTH和所述第二AUTH、以及所述用户设备的身份。

[0014] 在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0015] 在第一方面的第一种可能的实现方式中，所述方法还包括：

[0016] 所述基站将所述基站的互联网协议IP地址发送给所述用户设备；

[0017] 所述基站接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址。

[0018] 结合第一方面或第一方面的第一种可能的实现方式，在第二种可能的实现方式中，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0019] 结合第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，所述基站确定IPsec隧道建立参数，包括：

[0020] 所述基站接收所述用户设备发送的第一因特网密钥交换协议版本2IKEv2消息，所述第一IKEv2消息包括第二安全参数；

[0021] 所述基站发送所述第一IKEv2消息的响应消息给所述用户设备；

[0022] 所述基站接收所述用户设备根据所述第二安全参数加密发送的第二IKEv2消息，所述第二IKEv2消息包括所述IPsec隧道建立参数；

[0023] 所述基站发送所述第二IKEv2消息的响应消息给所述用户设备；

[0024] 其中，所述IPsec隧道建立参数中还包括所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI；所述安全算法为设置有安全算法级别的安全算法。

[0025] 本实现方式基站与用户设备之间通过IP数据包，具体的是因特网密钥交换协议版本2消息，协商IPsec隧道建立参数。

[0026] 结合第一方面的第三种可能的实现方式，在第四种可能的实现方式中，所述基站验证所述用户设备的身份，包括：

[0027] 所述基站验证所述用户设备的身份标识是否与核心网侧已获得的所述用户设备的身份一致。

[0028] 结合第一方面的第三种可能的实现方式，在第五种可能的实现方式中，所述基站获取与所述用户设备协商后的IPsec隧道建立参数，包括：

[0029] 所述基站接收所述用户设备发送的至少一个无线资源控制RRC消息；

[0030] 其中，所述至少一个RRC消息封装所述第一IKEv2消息，所述第一IKEv2消息的响应

消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

[0031] 在本实现方式中,用户设备通过RRC消息发送IPsec隧道建立参数给基站,基站接收用户设备发送的IPsec隧道建立参数,即将建立IPsec隧道的整个IKEv2的消息封装在RRC消息中传递,RRC消息可以保证收发对端是认证过的。

[0032] 结合第一方面,在第一方面的第六种可能的实现方式中,所述基站确定IPsec隧道建立参数,包括:

[0033] 所述基站接收所述用户设备通过无线资源控制RRC消息发送的所述第二AUTH和所述用户设备所支持的安全算法列表;

[0034] 所述基站根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

[0035] 所述基站将所述IPsec隧道建立参数发送给所述用户设备。

[0036] 在本实现方式中,通过RRC消息来传输IPsec隧道建立必要参数,没有完全封装IKEv2消息。

[0037] 结合第一方面,在第一方面的第七种可能的实现方式中,所述基站确定IPsec隧道建立参数,包括:

[0038] 所述基站通过RRC消息将所述第二AUTH和所述基站的安全算法级别列表发送给所述用户设备,以使所述用户设备根据自身所支持的安全算法列表,以及所述基站的安全算法级别列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

[0039] 所述基站接收所述用户设备发送的所述IPsec隧道建立参数。

[0040] 在本实现方式中,通过RRC消息来传输IPsec隧道建立必要参数,没有完全封装IKEv2消息。

[0041] 第二方面,提供了一种IPsec隧道建立方法,包括:

[0042] 用户设备接收基站发送的第一抗重放参数;

[0043] 所述用户设备确定所述用户设备的第二抗重放参数,所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同;

[0044] 所述用户设备根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec,并根据所述第二Kipsec生成第二鉴权信息AUTH,并发送所述第二AUTH给所述基站;

[0045] 所述用户设备接收所述基站发送的IPsec隧道建立参数,所述IPsec隧道建立参数包括第一AUTH,其中,所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec,所述基站根据第一Kipsec生成所述第一AUTH;

[0046] 所述用户设备验证所述第一AUTH和所述第二AUTH。

[0047] 结合第一方面,在第一种可能的实现方式中,所述方法还包括:

[0048] 所述用户设备接收所述基站发送的所述基站的互联网协议IP地址;

[0049] 所述用户设备将所述用户设备连接的无线局域网的IP地址发送给所述基站。

[0050] 结合第二方面或第二方面的第一种可能的实现方式,在第二种可能的实现方式中,所述方法还包括:

[0051] 所述用户设备发送第一IKEv2消息给所述基站,所述第一IKEv2消息包括第二安全

参数；

[0052] 所述用户设备接收所述基站发送的所述第一IKEv2消息的响应消息；

[0053] 所述用户设备根据所述第二安全参数加密第二IKEv2消息，将加密后的所述第二IKEv2消息发送给所述基站，所述第二IKEv2消息包括所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec，所述安全算法为设置有安全算法级别的安全算法；

[0054] 所述用户设备接收所述基站发送的所述第二IKEv2消息的响应消息。

[0055] 结合第二方面的第二种可能的实现方式，在第三种可能的实现方式中，所述方法还包括：

[0056] 所述用户设备发送至少一个RRC消息给所述基站；

[0057] 其中，所述至少一个RRC消息封装所述第一IKEv2消息，所述第一IKEv2消息的响应消息，所述第二IKEv2消息，以及所述第二IKEv2消息的响应消息。

[0058] 结合第二方面，在第四种可能的实现方式中，所述方法还包括：

[0059] 所述用户设备通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站，以使所述基站根据自身的安全算法级别列表，以及所述用户设备所支持的安全算法列表，确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0060] 所述用户设备接收所述基站发送的所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0061] 结合第二方面，在第五种可能的实现方式中，所述方法还包括：

[0062] 所述用户设备接收所述基站通过RRC消息发送的所述基站的安全算法级别列表，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0063] 所述用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别；

[0064] 所述用户设备将所述IPsec隧道建立参数发送给所述基站，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0065] 第三方面，提供了一种基站，该基站具有实现上述方法中基站行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。

[0066] 一种可能的实现方式中，所述基站包括：发送器和处理器；其中，

[0067] 所述发送器，用于发送第一抗重放参数给用户设备；

[0068] 所述处理器，用于确定所述用户设备的第二抗重放参数，所述第一抗重放参数和

第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

[0069] 所述处理器，用于根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec，并根据所述第一Kipsec生成第一鉴权信息AUTH；

[0070] 所述处理器还用于确定IPsec隧道建立参数，所述IPsec隧道建立参数包括第二AUTH，其中，所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec，并根据所述第二Kipsec生成所述第二AUTH；

[0071] 所述处理器还用于验证所述第一AUTH和所述第二AUTH以及所述用户设备的身份。

[0072] 另一种可能的实现方式中，所述基站包括：

[0073] 发送单元，用于发送第一抗重放参数给用户设备；

[0074] 确定单元，用于确定所述用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

[0075] 生成单元，用于根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec，并根据所述第一Kipsec生成第一鉴权信息AUTH；

[0076] 所述确定单元还用于确定IPsec隧道建立参数，所述IPsec隧道建立参数包括第二AUTH，其中，所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec，并根据所述第二Kipsec生成所述第二AUTH；

[0077] 验证单元，用于验证所述第一AUTH和所述第二AUTH以及所述用户设备的身份。

[0078] 第四方面，提供了一种用户设备，该用户设备具有实现上述方法中用户设备行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。

[0079] 一种可能的实现方式中，所述用户设备包括：接收器、发送器和处理器；其中，

[0080] 所述接收器，用于接收基站发送的第一抗重放参数；

[0081] 所述处理器，用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec，并根据所述第二Kipsec生成第二鉴权信息AUTH；

[0082] 所述发送器还用于发送所述第二AUTH给所述基站；

[0083] 所述接收器还用于接收所述基站发送的IPsec隧道建立参数，所述IPsec隧道建立参数包括第一AUTH，其中，所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec，所述基站根据第一Kipsec生成所述第一AUTH；

[0084] 所述处理器还用于验证所述第一AUTH和所述第二AUTH。

[0085] 另一种可能的实现方式中，所述用户设备包括：

[0086] 接收单元，用于接收基站发送的第一抗重放参数；

[0087] 生成单元，用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec，并根据所述第二Kipsec生成第二鉴权信息AUTH；

[0088] 发送单元，用于发送所述第二AUTH给所述基站；

[0089] 所述接收单元还用于接收所述基站发送的IPsec隧道建立参数，所述IPsec隧道建立参数包括第一AUTH，其中，所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec，所述基站根据第一Kipsec生成所述第一AUTH；

[0090] 验证单元，用于验证所述第一AUTH和所述第二AUTH。

[0091] 根据本发明实施例提供的一种因特网协议安全性IPsec隧道建立方法，用户设备

及基站，在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

附图说明

[0092] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0093] 图1为长期演进系统-无线局域网络聚合LWA示意图；

[0094] 图2为现有无线局域网WLAN的接入方式示意图；

[0095] 图3为本发明实施例提供的一种IPsec隧道建立方法的流程示意图；

[0096] 图4为本发明实施例提供的另一种IPsec隧道建立方法的流程示意图；

[0097] 图5为本发明实施例提供的又一种IPsec隧道建立方法的流程示意图；

[0098] 图6为本发明实施例提供的一种基站的结构示意图；

[0099] 图7为本发明实施例提供的另一种基站的结构示意图；

[0100] 图8为本发明实施例提供的一种用户设备的结构示意图；

[0101] 图9为本发明实施例提供又一种基站的结构示意图；

[0102] 图10为本发明实施例提供另一种用户设备的结构示意图。

具体实施方式

[0103] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0104] 本发明要求图1所示的LWA新架构兼容现有的WLAN技术，即要求兼容S2b接入方式下的非可信的WLAN接入方式。本发明实施例要在用户设备和基站之间建立IPsec隧道，达到S2b接口下ePDG的作用。

[0105] 在实施本发明实施例的IPsec隧道建立方法之前，用户设备已经接入核心网，并且鉴权成功。此时，基站处已经有用户设备的身份标识，如小区无线网络临时标识(Cell Radio Network Temporary Identifier，简称C-RNTI)，并且基站可以通过此标识找到用户设备。鉴权成功带来的结果是用户设备和基站之间的空口安全已经建立，即用户设备和基站之间已经持有相同的机密性密钥和完整性密钥，这些密钥用来保证用户设备和基站之间在通过移动网络传输消息的安全性。

[0106] 本发明实施例在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0107] 图3为本发明实施例提供的一种IPsec隧道建立方法的流程示意图，该方法包括以

下步骤：

[0108] S101、基站与用户设备协商抗重放参数。

[0109] 抗重放参数是为了防止基站或用户设备每次生成的密钥是相同的，或者生成的消息是相同的，如果密钥或消息相同的话，攻击者可以截获以前的消息，再次重新发送。抗重放参数一般是随机数，时间戳，或者计数器的值。

[0110] 基站可以在发送基站的IP地址给用户设备的RRC消息中携带抗重放参数-1，用户设备则可以在回复基站的RRC消息时携带抗重放参数-2，也可以不携带抗重放参数-2，这由具体配置决定，例如，如果抗重放参数是随机数，抗重放参数-1和抗重放参数-2有可能是相同的，也可能是不同的，如果选择传递随机数的方式，则在回复消息中要携带抗重放参数-2；如果采用计数器的方式，基站可以设置计数器，而用户设备不设置计数器，所以需要基站把计数器的值作为抗重放参数-1传给用户设备，而用户设备由于没有计时器，所以回复消息中没有携带抗重放参数；如果用户设备中也设置有计数器，则用户设备也需要将其计数器的值作为抗重放参数-2传给基站；如果采用时间戳的方式，则双方都需要传送抗重放参数。相应地，回复基站的RRC消息可以包括：RRC重配置完成消息，RRC完成消息等。

[0111] S102、基站根据空口密钥KeNB和第一抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH。

[0112] S103、用户设备根据该KeNB和第二抗重放参数生成第二Kipsec，并根据第二Kipsec生成第二AUTH。

[0113] 用户设备和基站在建立空口安全的时候，会生成相同的空口密钥KeNB。然后，基站、用户设备分别利用设定的密钥生成函数，根据KeNB和协商后的抗重放参数生成第一Kipsec和第二Kipsec，再分别根据第一Kipsec和第二Kipsec生成第一AUTH(Authentication)和第二AUTH，由于采用的密钥生成函数相同，KeNB相同，且抗重放参数是经过协商过的，基站和用户设备知道对端的抗重放参数，因此，基站、用户设备能够分别根据自己的鉴权信息，验证对端的鉴权信息。

[0114] S104、基站与用户设备协商IPsec隧道建立参数。

[0115] 该IPsec隧道建立参数包括鉴权信息(AUTH)和IPsec隧道传输参数，该IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识(Traffic Selector，简称TS)，安全参数又称安全联盟参数(Security Association，简称SA)，此参数包含安全算法，以及第一Kipsec或第二Kipsec，该安全算法具有安全算法级别，安全算法级别用于表示哪种算法应该被优先考虑，第一Kipsec或第二Kipsec用于在安全算法中加密IPsec隧道中传输的数据流。IPsec隧道建立参数还可能包括用户设备的身份标识IDi，和基站的身份标识IDr。在此实施例中，为了使基站准确无误的判断用户设备的身份，可采用C-RNTI作为IDi。其中，IDi表示发起方身份，即Identification-Initiator，IDr表示接收方身份，即Identification-Responder。

[0116] S105、基站、用户设备分别验证第一AUTH和第二AUTH。

[0117] S106、若基站验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证。

[0118] 在获得协商后的IPsec隧道建立参数后，基站、用户设备分别验证对端的鉴权信息是否与自身的鉴权信息一致，如果验证通过，基站再对用户设备的身份进行验证。基站验证用户设备的身份，可以将空口连接时已经获取的用户设备的身份以及IPsec隧道建立参数

包含的用户设备的身份标识进行比较，而如果接收的是RRC消息，则用户设备的身份已经在接收RRC消息时进行验证。

[0119] 基站与用户设备协商了IPsec隧道传输参数，则建立IPsec隧道的工作已经完成，从而可以根据IPsec隧道传输参数在IPsec隧道中传输数据。

[0120] 根据本发明实施例提供的一种IPsec隧道建立方法，在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0121] 图4为本发明实施例提供的另一种IPsec隧道建立方法的流程示意图，该方法包括以下步骤：

[0122] S201、基站在RRC重配置消息中发送基站的IP地址给用户设备。

[0123] RRC重配置消息中携带抗重放参数-1。

[0124] S202、用户设备在收到基站的RRC重配置消息之后，回复RRC重配置完成消息。

[0125] RRC重配置完成消息中携带抗重放参数-2。

[0126] 在建立用户设备与基站之间的IPsec隧道时，需要完成两个操作：第一，双方需要知道对端的IP地址，第二，基站需要确定建立IPsec隧道的对端是本用户设备，而不是攻击者或其他人的用户设备，即用户设备的身份是正确的。

[0127] 首先，基站将基站的IP地址发送给用户设备。基站可以在多种无线资源控制(Radio Resource Control，简称RRC)消息中选择一个，用于发送基站的IP地址，该RRC消息包括：RRC重配置消息，RRC建立请求消息，RRC重建立消息等。选择通过RRC消息传送是基于已通过安全认证的移动网络，可以确保发送的消息的安全性。

[0128] 同时，用户设备发送用户设备连接的无线局域网的IP地址给基站，在用户设备发送IP之前，用户设备首先要通过AP接入无线局域网，然后获得无线局域网分发的IP地址。

[0129] S203、基站利用设定密钥生成函数，根据空口密钥KeNB和协商后的抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH。

[0130] S204、用户设备利用该设定密钥生成函数，根据该KeNB和协商后的抗重放参数生成第二Kipsec，并根据第二Kipsec生成第二AUTH。

[0131] S205、用户设备接入AP。

[0132] S206、用户设备获得AP分发的IP地址。

[0133] S207、用户设备将AP分发的IP地址发送给基站。

[0134] S208、基站与用户设备通过第一因特网密钥交换协议版本2消息协商第二安全参数。

[0135] 具体地，用户设备发送因特网密钥交换安全联盟参数协商初始消息IKE_SA_INIT消息给基站，该IKE_SA_INIT消息中包括因特网密钥交换协议头(IKE Header，简称HDR)，第二安全参数SAi1，发送方基本密钥KEi，随机数Ni，其中，HDR中包括安全参数索引(Security Parameter Indexes，简称SPI)，用于标识IPsec隧道建立过程；基站回复IKE_SA_INIT消息，回复的消息中包括HDR，SAr1，回复方基本密钥KEr，随机数Nr，从而完成基站与用户设备的第二安全参数的协商。第二安全参数也包括安全算法，安全算法级别和密钥。这里的SAi1和SAr1的安全算法级别是通过IKEv2消息确定的，SAi1和SAr1中包括多个安全算法，通过安全

算法级别来指定采用的安全算法。密钥是根据基本密钥(KEi和KEr),以及随机数(Ni,Nr)生成的。第二安全参数用于加密传输IPsec隧道建立参数的第二IKEv2消息。

[0136] S209、基站接收用户设备根据第二安全参数加密发送的第二IKEv2消息。

[0137] 具体地,用户设备发送IKE_AUTH消息给基站该IKE_AUTH消息由第二安全参数进行加密发送。该IKE_AUTH消息中包括HDR,SK{IDi,AUTH,SAi2,TSi,TSr},其中,SK{}表示{}中的参数用第二安全参数中的安全算法和密钥进行加密保护了;基站回复用户设备的IKR_AUTH消息,回复的消息中包括HDR,SK{IDr,AUTH,SAr2,TSi,TSr}。

[0138] 在本实施例中,基站与用户设备之间通过IP数据包,具体的是因特网密钥交换协议版本2消息,协商IPsec隧道建立参数,由于是通过IP数据包传输,尚未验证对端的身份,不能保证传输过程的安全性,因此,需要先协商用于传输IPsec隧道建立参数的消息的安全参数,然后通过协商好的安全参数对发送IPsec隧道建立参数的消息进行加密。

[0139] 作为S208-S209的一种替代方式,用户设备通过RRC消息发送IPsec隧道建立参数给基站,基站接收用户设备发送的IPsec隧道建立参数,即将建立IPsec隧道的整个IKEv2的消息封装在RRC消息中传递,由于RRC消息可以保证收发对端是认证过的,不需要强调鉴权信息AUTH和发起方的身份IDi。

[0140] S210、基站、用户设备分别验证第一AUTH和第二AUTH。

[0141] S211、若基站验证第一AUTH和第二AUTH一致,对用户设备的身份进行验证。

[0142] 图5为本发明实施例提供的又一种IPsec隧道建立方法的流程示意图,该方法包括以下步骤:

[0143] S301、用户设备接入AP。

[0144] S302、用户设备获得AP分发的IP地址。

[0145] S303、基站在RRC重配置消息中发送基站的IP地址给用户设备。

[0146] 此消息中携带抗重放参数-1。

[0147] S304、用户设备在收到基站的RRC重配置消息之后,回复RRC重配置完成消息。

[0148] 携带用户设备连接的AP的IP地址和抗重放参数-2。

[0149] S305、基站利用设定密钥生成函数,根据空口密钥KeNB和协商后的抗重放参数生成第一预共享密钥Kipsec,并根据第一Kipsec生成第一鉴权信息AUTH。

[0150] S306、用户设备利用该设定密钥生成函数,根据该KeNB和协商后的抗重放参数生成第二Kipsec,并根据第二Kipsec生成第二AUTH。

[0151] S307、基站接收用户设备通过RRC消息发送的第二AUTH和用户设备所支持的安全算法列表。

[0152] 用户设备通过RRC消息将IPsec隧道建立必要参数发送给基站,基站接收用户设备发送的IPsec隧道建立必要参数,该IPsec隧道建立必要参数包括:鉴权信息,以及用户设备所支持的安全算法列表,该安全算法可包括加密算法和完整性保护算法。

[0153] 可选地,也可以在用户设备附着到核心网的过程中即attach过程中,将用户设备所支持的安全算法列表事先传输给基站,即可以在S301之前,用户设备在Attach Request消息中携带用户设备所支持的安全算法列表给MME,MME在Attach Accept消息中,将用户设备所支持的安全算法列表传输给基站,之后完成用户设备的Attach流程,建立默认承载。

[0154] S308、基站根据自身的安全算法级别列表,以及用户设备所支持的安全算法列表,

确定第一安全参数的安全算法的级别。

[0155] 基站中设置有安全算法级别列表，该安全算法级别列表中包括多个安全算法与安全算法级别的对应关系。基站根据该安全算法级别列表和获取的用户设备所支持的安全算法列表，可以从用户设备所支持的安全算法确定第一安全参数的安全算法的级别，该安全算法作为保护IPsec隧道传输的安全算法，例如，可以选取用户设备所支持的安全算法列表中算法安全能力级别最高的安全算法。

[0156] 可选地，如果用户设备在attach过程中事先将用户设备所支持的安全算法列表传输给基站，则基站可以在RRC重配置消息中将基站的IP地址和确定的第一安全参数的安全算法的级别发送给用户设备。

[0157] S309、基站将IPsec隧道建立参数发送给用户设备。

[0158] 在确定了鉴权信息和第一安全算法后，基站将IPsec隧道建立参数发送给用户设备，该IPsec隧道建立参数包括第一安全参数和TS，该第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0159] 在本实施例中，通过RRC消息来传输IPsec隧道建立必要参数，没有完全封装IKEv2消息，由于RRC消息本身可以保证数据传输的安全性，无需协商第二安全参数。

[0160] 在本实施例中，是由用户设备发起IPsec隧道建立，作为S307-S309的一种替代方式，也可以由基站发起IPsec隧道建立，即基站通过RRC消息将IPsec隧道建立必要参数发送给用户设备，以使用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别，然后用户设备将IPsec隧道建立参数发送给基站，基站接收用户设备发送的IPsec隧道建立参数。

[0161] S310、基站、用户设备分别验证第一AUTH和第二AUTH。

[0162] S311、若基站验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证。

[0163] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为根据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0164] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0165] 本发明实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[0166] 图6为本发明实施例提供的一种基站的结构示意图，该基站1000包括发送单元11、确定单元12、生成单元13和验证单元14。其中：

[0167] 发送单元11，用于发送第一抗重放参数给用户设备。

[0168] 确定单元12，用于确定所述用户设备的第二抗重放参数基站可以在给用户设备的RRC消息中携带抗重放参数-1，用户设备则可以在回复基站的RRC消息时携带抗重放参数-2，也可以不携带抗重放参数-2，这由具体配置决定。相应地，回复基站的RRC消息可以包括：RRC重配置完成消息，RRC完成消息等。

[0169] 生成单元13，用于根据空口密钥KeNB和第一抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH。

[0170] 用户设备和基站在建立空口安全的时候，会生成相同的空口密钥KeNB。然后，基站、用户设备分别利用设定的密钥生成函数，根据KeNB和协商后的抗重放参数生成第一Kipsec和第二Kipsec，再分别根据第一Kipsec和第二Kipsec生成第一AUTH和第二AUTH，由于采用的密钥生成函数相同，KeNB相同，且抗重放参数是经过协商过的，基站和用户设备知道对端的抗重放参数，因此，基站、用户设备能够分别根据自己的鉴权信息，验证对端的鉴权信息。

[0171] 所述确定单元12还用于确定IPsec隧道建立参数。

[0172] 该IPsec隧道建立参数包括鉴权信息和IPsec隧道传输参数，该IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识，安全参数又称安全联盟参数(Security Association，简称SA)，此参数包含安全算法，以及第一Kipsec或第二Kipsec，该安全算法具有安全算法级别，安全算法级别用于表示哪种算法应该被优先考虑，第一Kipsec或第二Kipsec用于在安全算法中加密IPsec隧道中传输的数据流。IPsec隧道建立参数还可能包括用户设备的身份标识IDi，和基站的身份标识IDr。

[0173] 验证单元14，用于验证第一AUTH和第二AUTH以及用户设备的身份。

[0174] 在获得协商后的IPsec隧道建立参数后，基站、用户设备分别验证对端的鉴权信息是否与自身的鉴权信息一致，如果验证通过，基站再对用户设备的身份进行验证。基站验证用户设备的身份，可以将空口连接时已经获取的用户设备的身份以及IPsec隧道建立参数包含的用户设备的身份标识进行比较，而如果接收的是RRC消息，则用户设备的身份已经在接收RRC消息时进行验证。

[0175] 基站与用户设备协商了IPsec隧道传输参数，则建立IPsec隧道的工作已经完成。

[0176] 根据本发明实施例提供的一种基站，在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0177] 请继续参阅图6，基站还包括接收单元，下面提供接收单元的一种具体实现方式：

[0178] 接收单元具体用于获取与所述用户设备通过第一因特网密钥交换协议版本2消息协商的第二安全参数。

[0179] 具体地，用户设备发送因特网密钥交换安全联盟参数协商初始消息IKE_SA_INIT消息给基站，该IKE_SA_INIT消息中包括HDR，第二安全参数SAi1，发送方基本密钥KEi，随机数Ni，其中，HDR中包括SPI，用于标识IPsec隧道建立过程；基站回复IKE_SA_INIT消息，回复的消息中包括HDR，SAr1，回复方基本密钥KEr，随机数Nr，从而完成基站与用户设备的第二安全参数的协商。第二安全参数也包括安全算法，安全算法级别和密钥。这里的SAi1和SAr1的安全算法级别是通过IKEv2消息确定的，SAi1和SAr1中包括多个安全算法，通过安全算法级别来指定采用的安全算法。密钥是根据基本密钥(KEi和KEr)，以及随机数(Ni，Nr)生成的。第二安全参数用于加密传输IPsec隧道建立参数的第二IKEv2消息。

[0180] 接收单元还具体用于接收用户设备根据第二安全参数加密发送的第二IKEv2消息。

[0181] 具体地，用户设备发送IKE_AUTH消息给基站该IKE_AUTH消息由第二安全参数进行加密发送。该IKE_AUTH消息中包括HDR，SK{IDi，AUTH，SAi2，TSi，TSr}，其中，SK{}表示{}中

的参数用第二安全参数中的安全算法和密钥进行加密保护了;基站回复用户设备的IKR_AUTH消息,回复的消息中包括HDR,SK{IDr,AUTH,SAr2,TSi,TSr}。

[0182] 在本实施例中,基站与用户设备之间通过IP数据包,具体的是因特网密钥交换协议版本2消息,协商IPsec隧道建立参数,由于是通过IP数据包传输,尚未验证对端的身份,不能保证传输过程的安全性,因此,需要先协商用于传输IPsec隧道建立参数的消息的安全参数,然后通过协商好的安全参数对发送IPsec隧道建立参数的消息进行加密。

[0183] 作为接收单元的另一种替代的实现方式,用户设备通过RRC消息发送IPsec隧道建立参数给基站,接收单元接收用户设备发送的IPsec隧道建立参数,即将建立IPsec隧道的整个IKEv2的消息封装在RRC消息中传递,由于RRC消息可以保证收发对端是认证过的,不需要强调鉴权信息AUTH和发起方的身份IDi。

[0184] 图7为本发明实施例提供的另一种基站的结构示意图,该基站2000包括发送单元21、接收单元22、生成单元23、确定单元24和验证单元25。其中:

[0185] 发送单元21,用于在RRC重配置消息中将基站的互联网协议IP地址和抗重放参数发送给用户设备。

[0186] 接收单元22,用于接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址和抗重放参数。

[0187] 生成单元23,用于利用设定密钥生成函数,根据空口密钥KeNB和协商后的抗重放参数生成第一预共享密钥Kipsec,并根据第一Kipsec生成第一鉴权信息AUTH。

[0188] 接收单元22还用于接收用户设备通过RRC消息发送的第二AUTH和用户设备所支持的安全算法列表。

[0189] 用户设备通过RRC消息将IPsec隧道建立必要参数发送给基站,基站接收用户设备发送的IPsec隧道建立必要参数,该IPsec隧道建立必要参数包括:鉴权信息,以及用户设备所支持的安全算法列表,该安全算法可包括加密算法和完整性保护算法。

[0190] 可选地,也可以在用户设备附着到核心网的过程中即attach过程中,将用户设备所支持的安全算法列表事先传输给基站,即可以在S301之前,用户设备在Attach Request消息中携带用户设备所支持的安全算法列表给MME,MME在Attach Accept消息中,将用户设备所支持的安全算法列表传输给基站,之后完成用户设备的Attach流程,建立默认承载。

[0191] 确定单元24,用于根据自身的安全算法级别列表,以及用户设备所支持的安全算法列表,确定第一安全参数的安全算法的级别。

[0192] 基站中设置有安全算法级别列表,该安全算法级别列表中包括多个安全算法与安全算法级别的对应关系。基站根据该安全算法级别列表和获取的用户设备所支持的安全算法列表,可以从用户设备所支持的安全算法确定第一安全参数的安全算法的级别,该安全算法作为保护IPsec隧道传输的安全算法,例如,可以选取用户设备所支持的安全算法列表中算法安全能力级别最高的安全算法。

[0193] 可选地,如果用户设备在attach过程中事先将用户设备所支持的安全算法列表传输给基站,则基站可以在RRC重配置消息中将基站的IP地址和确定的第一安全参数的安全算法的级别发送给用户设备。

[0194] 发送单元21还用于将IPsec隧道建立参数发送给用户设备。

[0195] 在确定了鉴权信息和第一安全算法后,基站将IPsec隧道建立参数发送给用户设

备，该IPsec隧道建立参数包括第一安全参数和TS，该第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec。。

[0196] 在本实施例中，通过RRC消息来传输IPsec隧道建立必要参数，没有完全封装IKEv2消息，由于RRC消息本身可以保证数据传输的安全性，无需协商第二安全参数。

[0197] 在本实施例中，是由用户设备发起IPsec隧道建立，作为一种替代方式，也可以由基站发起IPsec隧道建立，即基站通过RRC消息将IPsec隧道建立必要参数发送给用户设备，以使用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别，然后用户设备将IPsec隧道建立参数发送给基站，基站接收用户设备发送的IPsec隧道建立参数。

[0198] 验证单元25，用于验证第一AUTH和第二AUTH。

[0199] 所述验证单元25还用于若验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证。

[0200] 图8为本发明实施例提供的一种用户设备的结构示意图，该用户设备3000包括确定单元31、生成单元32、发送单元33、接收单元34和验证单元35；其中：

[0201] 确定单元31，用于确定用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

[0202] 生成单元32，用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec，并根据所述第二Kipsec生成第二鉴权信息AUTH；

[0203] 发送单元33，用于发送所述第二AUTH给所述基站；

[0204] 接收单元34，用于接收所述基站发送的IPsec隧道建立参数，所述IPsec隧道建立参数包括第一AUTH，其中，所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec，所述基站根据第一Kipsec生成所述第一AUTH；

[0205] 验证单元35，用于验证所述第一AUTH和所述第二AUTH。

[0206] 进一步地，所述接收单元34还用于接收所述基站发送的所述基站的互联网协议IP地址；

[0207] 所述发送单元还用于将所述用户设备连接的无线局域网的IP地址发送给所述基站。

[0208] 作为一种实现方式，所述发送单元33还用于发送第一IKEv2消息给所述基站，所述第一IKEv2消息包括第二安全参数；

[0209] 所述接收单元34还用于接收所述基站发送的所述第一IKEv2消息的响应消息；

[0210] 所述发送单元33还用于根据所述第二安全参数加密第二IKEv2消息，将加密后的所述第二IKEv2消息发送给所述基站，所述第二IKEv2消息包括所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec，所述安全算法为设置有安全算法级别的安全算法；

[0211] 所述接收单元34还用于接收所述基站发送的所述第二IKEv2消息的响应消息。

[0212] 作为另一种实现方式，所述发送单元33还用于发送至少一个RRC消息给所述基站；

[0213] 其中,所述至少一个RRC消息封装所述第一IKEv2消息,所述第一IKEv2消息的响应消息,所述第二IKEv2消息,以及所述第二IKEv2消息的响应消息。

[0214] 作为又一种实现方式,所述发送单元33还用于通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站,以使所述基站根据自身的安全算法级别列表,以及所述用户设备所支持的安全算法列表,确定所述第一安全参数的安全算法的级别,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

[0215] 所述接收单元34还用于接收所述基站发送的所述IPsec隧道建立参数,所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和TS,所述第一安全参数包括确定所述级别的安全算法,以及所述第一Kipsec或所述第二Kipsec。

[0216] 作为又一种实现方式,所述接收单元34还用于接收所述基站通过RRC消息发送的所述基站的安全算法级别列表,所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系;

[0217] 所述确定单元31还用于根据自身所支持的安全算法列表,以及所述基站的安全算法级别列表,确定所述第一安全参数的安全算法的级别;

[0218] 所述发送单元33还用于将所述IPsec隧道建立参数发送给所述基站,所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR,所述HDR中包括用于标识IPsec隧道建立流程的标识SPI,所述IPsec隧道传输参数包括第一安全参数和TS,所述第一安全参数包括确定所述级别的安全算法,以及所述第一Kipsec或所述第二Kipsec。

[0219] 根据本发明实施例提供的一种用户设备,在用户设备通过无线局域网请求接入核心网时,基站与用户设备协商抗重放参数及IPsec隧道建立参数,建立IPsec隧道,以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据,从而实现用户设备通过无线局域网安全地接入核心网,保证了数据传输的安全性。

[0220] 如图9所示,为本发明实施例提供又一种基站的结构示意图,用于实现上述IPsec隧道建立的功能,如图9所示,基站4000包括发送器41和处理器42,其中,所述发送器41和处理器42之间通过总线43相互连接。其中:

[0221] 所述发送器,用于发送第一抗重放参数给用户设备;

[0222] 所述处理器,用于确定所述用户设备的第二抗重放参数,所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同;

[0223] 所述处理器还用于用于根据空口密钥KeNB和所述第一抗重放参数生成第一预共享密钥Kipsec,并根据所述第一Kipsec生成第一鉴权信息AUTH;

[0224] 所述处理器还用于确定IPsec隧道建立参数,所述IPsec隧道建立参数包括第二AUTH,其中,所述用户设备根据所述KeNB和所述第二抗重放参数生成第二Kipsec,并根据所述第二Kipsec生成所述第二AUTH;

[0225] 所述处理器还用于验证所述第一AUTH和所述第二AUTH、以及所述用户设备的身份。

[0226] 进一步地,所述发送器还用于将所述基站的互联网协议IP地址发送给所述用户设备;

[0227] 所述基站还包括:接收器;

[0228] 所述接收器还用于接收所述用户设备发送的所述用户设备连接的无线局域网的IP地址。

[0229] 进一步地，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0230] 进一步地，所述接收器还用于接收所述用户设备发送的第一因特网密钥交换协议版本2IKEv2消息，所述第一IKEv2消息包括第二安全参数；

[0231] 所述发送器还用于发送所述第一IKEv2消息的响应消息给所述用户设备；

[0232] 所述接收器还用于接收所述用户设备根据所述第二安全参数加密发送的第二IKEv2消息，所述第二IKEv2消息包括所述IPsec隧道建立参数；

[0233] 所述发送器还用于发送所述第二IKEv2消息的响应消息给所述用户设备；

[0234] 其中，所述IPsec隧道建立参数中还包括所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI；所述安全算法为设置有安全算法级别的安全算法。

[0235] 进一步地，所述处理器还用于：

[0236] 验证所述用户设备的身份标识是否与核心网侧已获得的所述用户设备的身份一致。

[0237] 进一步地，所述接收器还用于接收所述用户设备发送的至少一个无线资源控制RRC消息；

[0238] 其中，所述至少一个RRC消息封装所述第一IKEv2消息，所述第一IKEv2消息的响应消息，所述第二IKEv2消息，以及所述第二IKEv2消息的响应消息。

[0239] 进一步地，所述接收器还用于接收所述用户设备通过无线资源控制RRC消息发送的所述第二AUTH和所述用户设备所支持的安全算法列表；

[0240] 所述处理器还用于根据自身的安全算法级别列表，以及所述用户设备所支持的安全算法列表，确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0241] 所述发送器还用于将所述IPsec隧道建立参数发送给所述用户设备。

[0242] 进一步地，所述发送器还用于通过RRC消息将所述第二AUTH和所述基站的安全算法级别列表发送给所述用户设备，以使所述用户设备根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0243] 所述接收器还用于接收所述用户设备发送的所述IPsec隧道建立参数。

[0244] 根据本发明实施例提供的一种基站，在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0245] 如图10所示，为本发明实施例提供另一种用户设备的结构示意图，用于实现上述IPsec隧道建立的功能，如图10所示，用户设备5000包括接收器51，发送器52和处理器53，其中，所述接收器51，发送器52和处理器53之间通过总线54相互连接。其中：

[0246] 所述处理器，用于确定用户设备的第二抗重放参数，所述第一抗重放参数和第二抗重放参数分别用于防止所述基站和所述用户设备每次生成的密钥相同；

[0247] 所述处理器还用于根据空口密钥KeNB和所述第二抗重放参数生成第二预共享密钥Kipsec，并根据所述第二Kipsec生成第二鉴权信息AUTH；

[0248] 发送器，用于发送所述第二AUTH给所述基站；

[0249] 接收器，用于接收所述基站发送的IPsec隧道建立参数，所述IPsec隧道建立参数包括第一AUTH，其中，所述基站根据所述KeNB和所述第一抗重放参数生成第一Kipsec，所述基站根据第一Kipsec生成所述第一AUTH；

[0250] 所述处理器还用于验证所述第一AUTH和所述第二AUTH。

[0251] 进一步地，所述接收器还用于接收所述基站发送的所述基站的互联网协议IP地址；

[0252] 所述发送单元还用于将所述用户设备连接的无线局域网的IP地址发送给所述基站。

[0253] 进一步地，所述发送器还用于发送第一IKEv2消息给所述基站，所述第一IKEv2消息包括第二安全参数；

[0254] 所述接收器还用于接收所述基站发送的所述第一IKEv2消息的响应消息；

[0255] 所述发送器还用于根据所述第二安全参数加密第二IKEv2消息，将加密后的所述第二IKEv2消息发送给所述基站，所述第二IKEv2消息包括所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数，所述用户设备的身份标识，和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和用于标识IPsec保护的数据流的出/入端口的标识TS，所述第一安全参数包括安全算法，以及所述第一Kipsec或所述第二Kipsec，所述安全算法为设置有安全算法级别的安全算法；

[0256] 所述接收器还用于接收所述基站发送的所述第二IKEv2消息的响应消息。

[0257] 进一步地，所述发送器还用于发送至少一个RRC消息给所述基站；

[0258] 其中，所述至少一个RRC消息封装所述第一IKEv2消息，所述第一IKEv2消息的响应消息，所述第二IKEv2消息，以及所述第二IKEv2消息的响应消息。

[0259] 进一步地，所述发送器还用于通过RRC消息发送所述用户设备所支持的安全算法列表给所述基站，以使所述基站根据自身的安全算法级别列表，以及所述用户设备所支持的安全算法列表，确定所述第一安全参数的安全算法的级别，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0260] 所述接收器还用于接收所述基站发送的所述IPsec隧道建立参数，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0261] 进一步地，所述接收器还用于接收所述基站通过RRC消息发送的所述基站的安全算法级别列表，所述安全算法级别列表包括多个安全算法与安全算法级别的对应关系；

[0262] 所述处理器还用于根据自身所支持的安全算法列表，以及所述基站的安全算法级别列表，确定所述第一安全参数的安全算法的级别；

[0263] 所述发送器还用于将所述IPsec隧道建立参数发送给所述基站，所述IPsec隧道建立参数还包括IPsec隧道传输参数和因特网密钥交换协议头HDR，所述HDR中包括用于标识IPsec隧道建立流程的标识SPI，所述IPsec隧道传输参数包括第一安全参数和TS，所述第一安全参数包括确定所述级别的安全算法，以及所述第一Kipsec或所述第二Kipsec。

[0264] 根据本发明实施例提供的一种用户设备，在用户设备通过无线局域网请求接入核心网时，基站与用户设备协商抗重放参数及IPsec隧道建立参数，建立IPsec隧道，以及根据隧道建立参数中包括的IPsec隧道传输参数在IPsec隧道中传输数据，从而实现用户设备通过无线局域网安全地接入核心网，保证了数据传输的安全性。

[0265] 本发明实施例装置中的单元可以根据实际需要进行合并、划分和删减。本领域的技术人员可以将本说明书中描述的不同实施例以及不同实施例的特征进行结合或组合。

[0266] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可以用硬件实现，或固件实现，或它们的组合方式来实现。当使用软件实现时，可以将上述功能存储在计算机可读介质中或作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于：计算机可读介质可以包括随机存取存储器(Random Access Memory，RAM)、只读存储器(Read-Only Memory，ROM)、电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory，EEPROM)、只读光盘(Compact Disc Read-Only Memory，CD-ROM)或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。此外。任何连接可以适当的成为计算机可读介质。例如，如果软件是使用同轴电缆、光纤光缆、双绞线、数字用户线(Digital Subscriber Line，DSL)或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或者其他远程源传输的，那么同轴电缆、光纤光缆、双绞线、DSL或者诸如红外线、无线和微波之类的无线技术包括在所属介质的定影中。如本发明所使用的，盘(Disk)和碟(disc)包括压缩光碟(CD)、激光碟、光碟、数字通用光碟(DVD)、软盘和蓝光光碟，其中盘通常磁性的复制数据，而碟则用激光来光学的复制数据。上面的组合也应当包括在计算机可读介质的保护范围之内。

[0267] 总之，以上所述仅为本发明技术方案的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

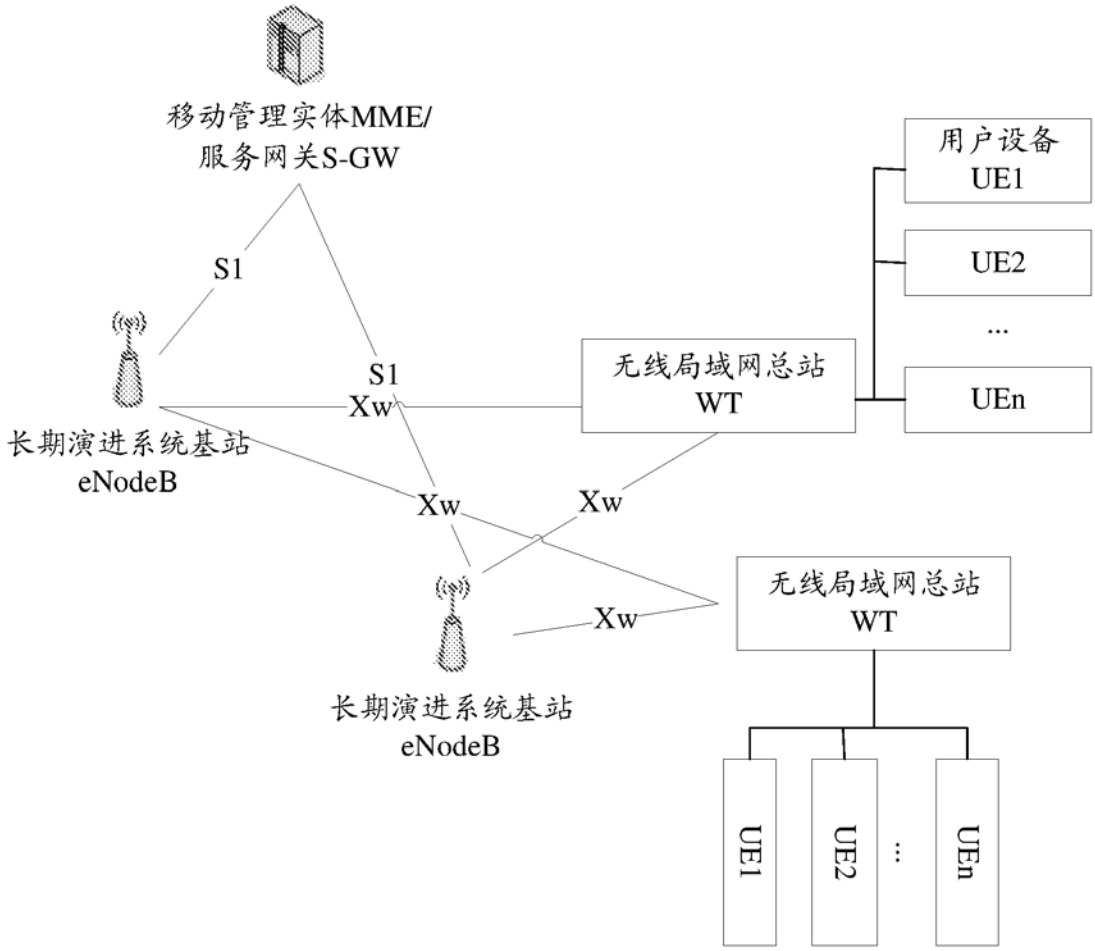

移动管理实体MME/
服务网关S-GW
S1
S1
Xw
长期演进系统基站
eNodeB
无线局域网总站
WT
用户设备
UE1
UE2
...
UEn
Xw
Xw
Xw
长期演进系统基站
eNodeB
无线局域网总站
WT
UE1
UE2
...
UEn

图1

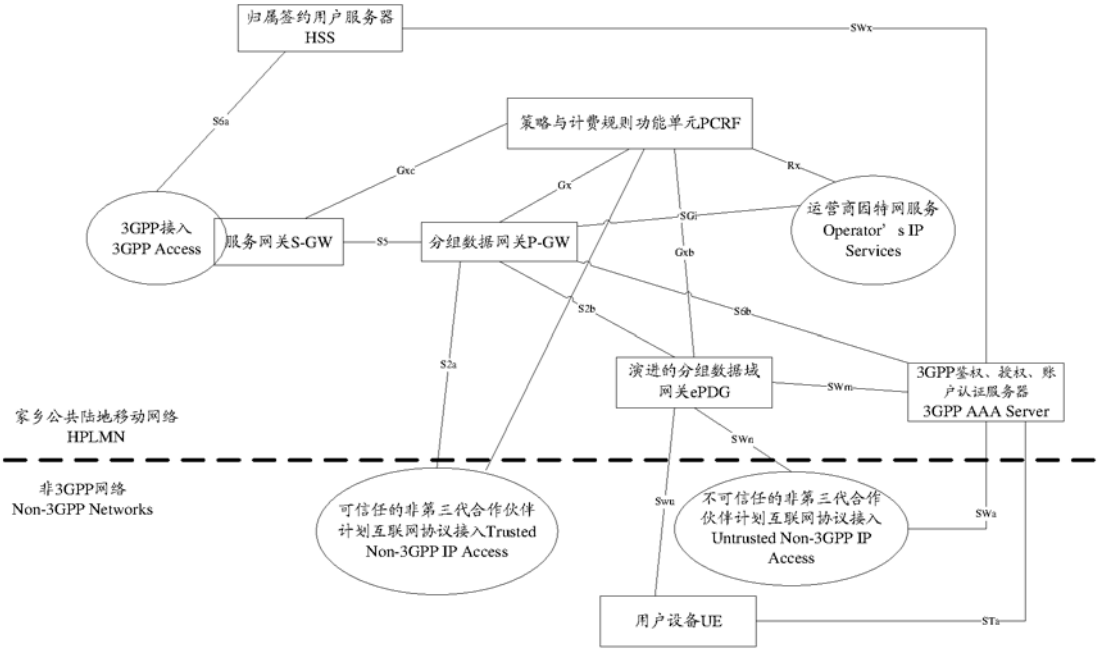

归属签约用户服务器
HSS
SWx
S6a
策略与计费规则功能单元PCRF
Gxc
Gx
Rx
3GPP接入
3GPP Access
服务网关S-GW
S5
分组数据网关P-GW
SGi
运营商因特网服务
Operator’s IP
Services
Gxb
S2b
S6b
S2a
演进的分组数据域
网关ePDG
SWm
3GPP鉴权、授权、账
户认证服务器
3GPP AAA Server
家乡公共陆地移动网络
HPLMN
SWn
非3GPP网络
Non-3GPP Networks
Swu
SWa
可信任的非第三代合作伙伴
计划互联网协议接入Trusted
Non-3GPP IP Access
不可信任的非第三代合作
伙伴计划互联网协议接入
Untrusted Non-3GPP IP
Access
用户设备UE
STa

图2

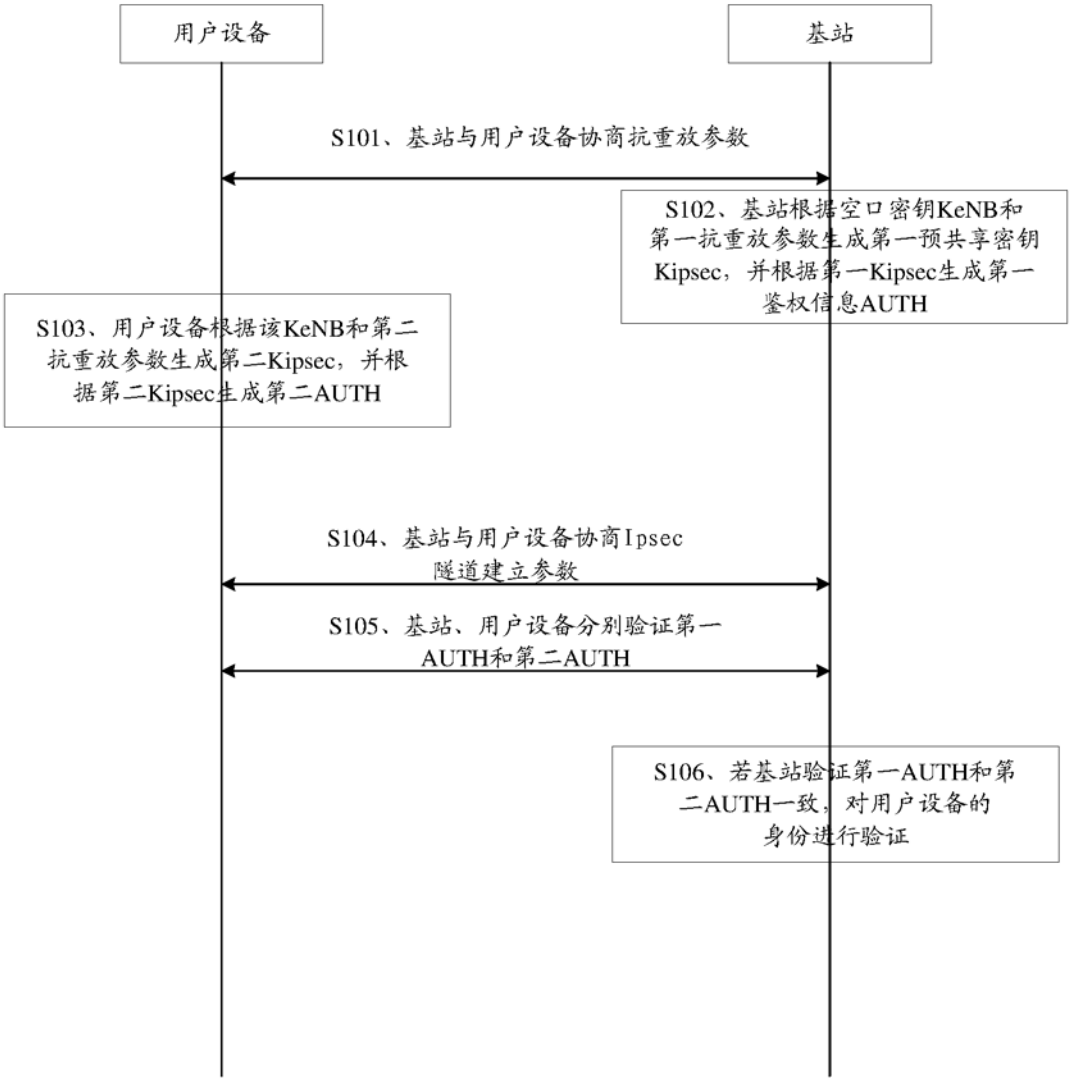

用户设备
基站
S101、基站与用户设备协商抗重放参数
S102、基站根据空口密钥KeNB和第一抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH
S103、用户设备根据该KeNB和第二抗重放参数生成第二Kipsec，并根据第二Kipsec生成第二AUTH
S104、基站与用户设备协商Ipsec隧道建立参数
S105、基站、用户设备分别验证第一AUTH和第二AUTH
S106、若基站验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证

图3

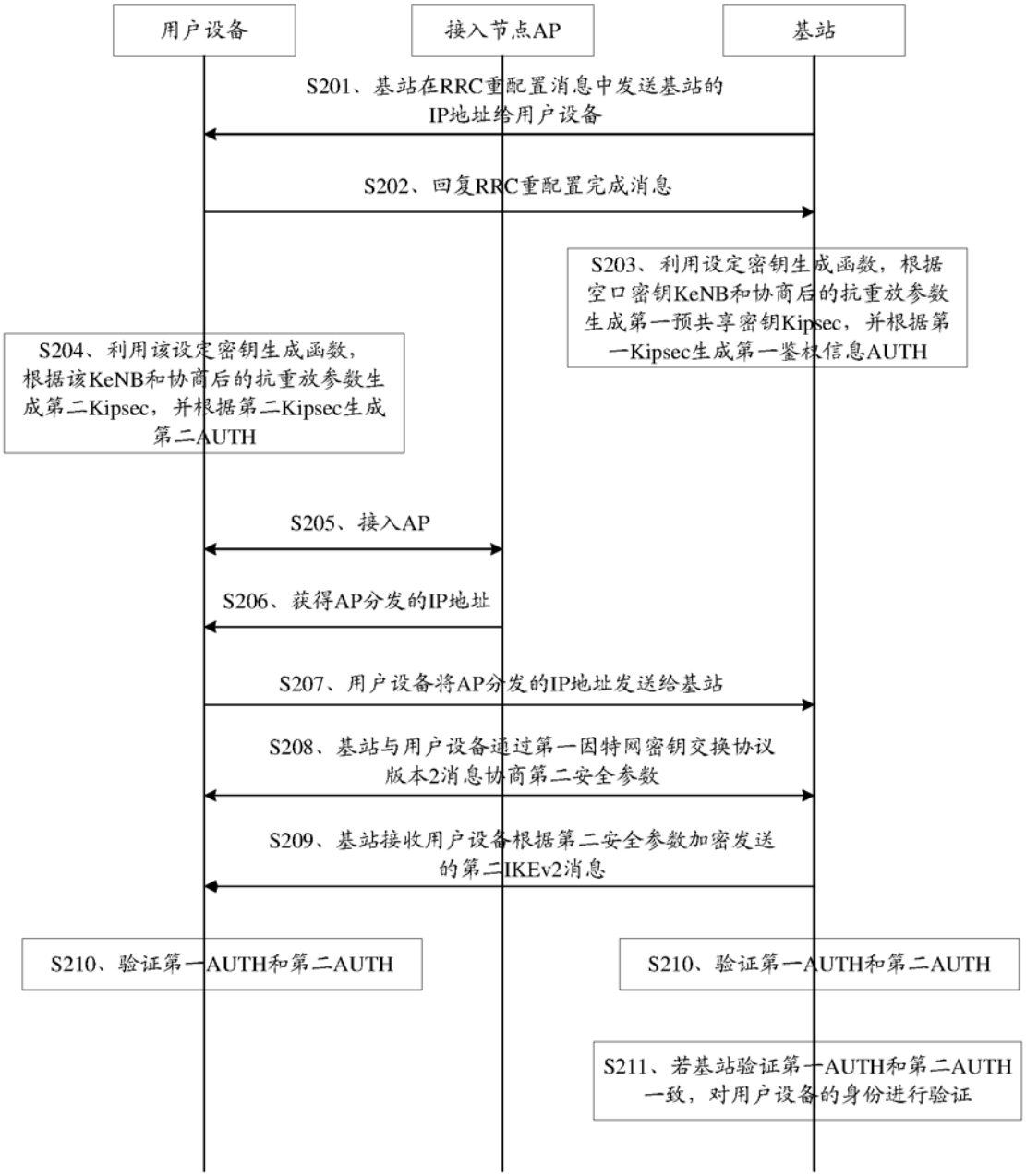

用户设备
接入节点AP
基站
S201、基站在RRC重配置消息中发送基站的IP地址给用户设备
S202、回复RRC重配置完成消息
S203、利用设定密钥生成函数，根据空口密钥KeNB和协商后的抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH
S204、利用该设定密钥生成函数，根据该KeNB和协商后的抗重放参数生成第二Kipsec，并根据第二Kipsec生成第二AUTH
S205、接入AP
S206、获得AP分发的IP地址
S207、用户设备将AP分发的IP地址发送给基站
S208、基站与用户设备通过第一因特网密钥交换协议版本2消息协商第二安全参数
S209、基站接收用户设备根据第二安全参数加密发送的第二IKEv2消息
S210、验证第一AUTH和第二AUTH
S210、验证第一AUTH和第二AUTH
S211、若基站验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证

图4

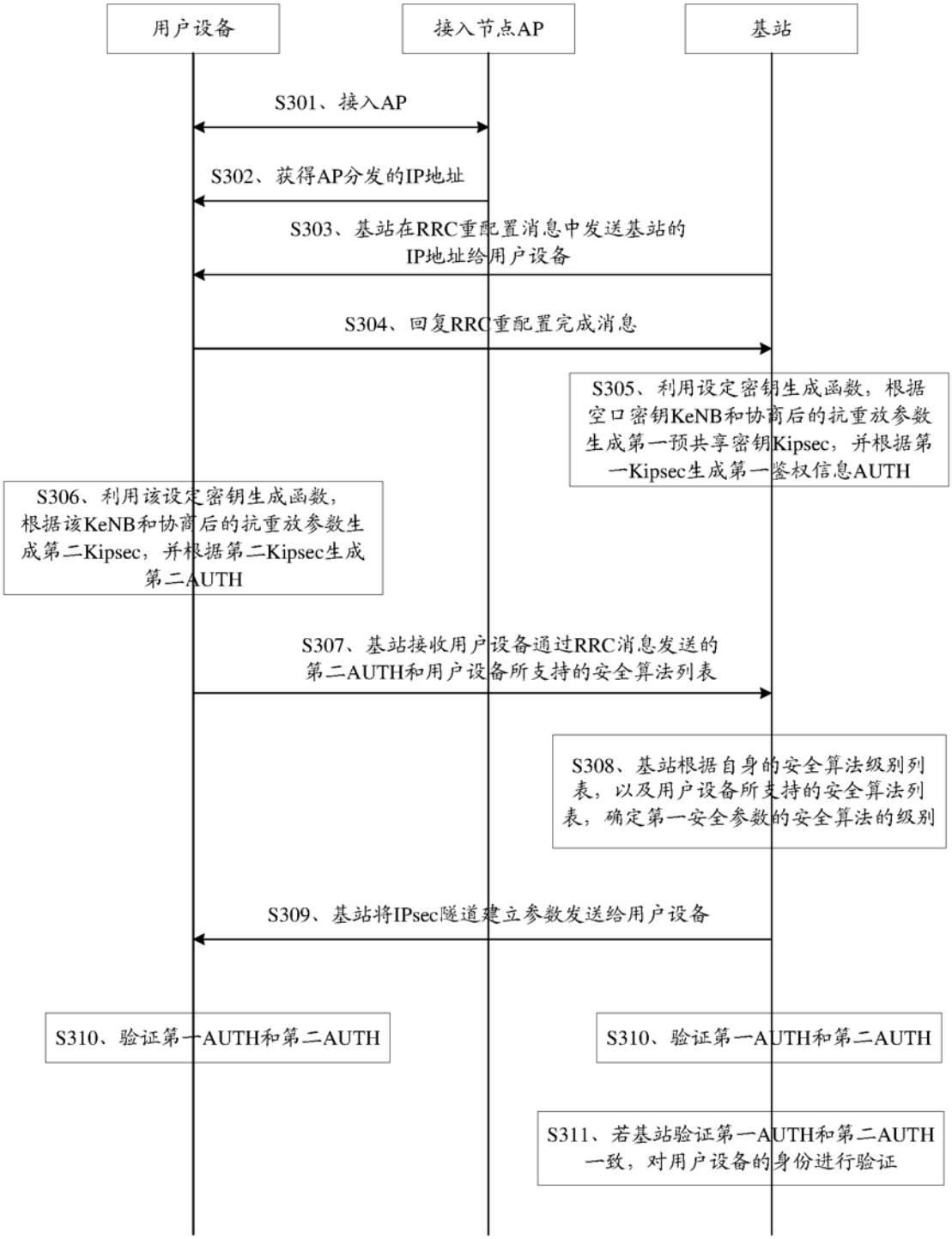

用户设备
接入节点AP
基站
S301、接入AP
S302、获得AP分发的IP地址
S303、基站在RRC重配置消息中发送基站的IP地址给用户设备
S304、回复RRC重配置完成消息
S305、利用设定密钥生成函数，根据空口密钥KeNB和协商后的抗重放参数生成第一预共享密钥Kipsec，并根据第一Kipsec生成第一鉴权信息AUTH
S306、利用该设定密钥生成函数，根据该KeNB和协商后的抗重放参数生成第二Kipsec，并根据第二Kipsec生成第二AUTH
S307、基站接收用户设备通过RRC消息发送的第二AUTH和用户设备所支持的安全算法列表
S308、基站根据自身的安全算法级别列表，以及用户设备所支持的安全算法列表，确定第一安全参数的安全算法的级别
S309、基站将IPsec隧道建立参数发送给用户设备
S310、验证第一AUTH和第二AUTH
S310、验证第一AUTH和第二AUTH
S311、若基站验证第一AUTH和第二AUTH一致，对用户设备的身份进行验证

图5

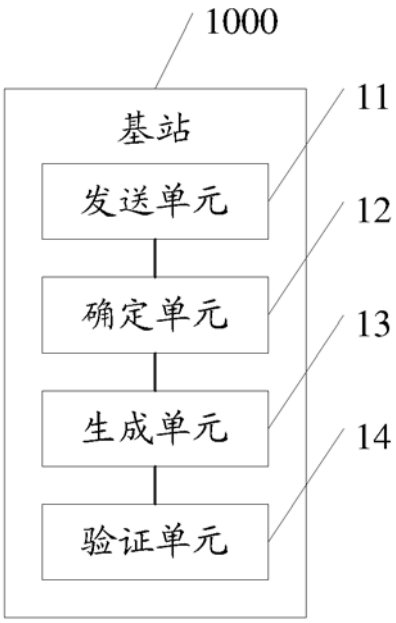

1000
基站
发送单元
确定单元
生成单元
验证单元
11
12
13
14

图6

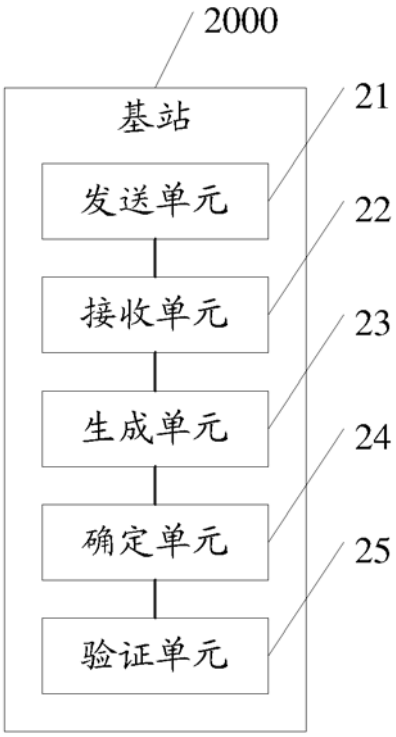

2000
基站
发送单元
接收单元
生成单元
确定单元
验证单元
21
22
23
24
25

图7

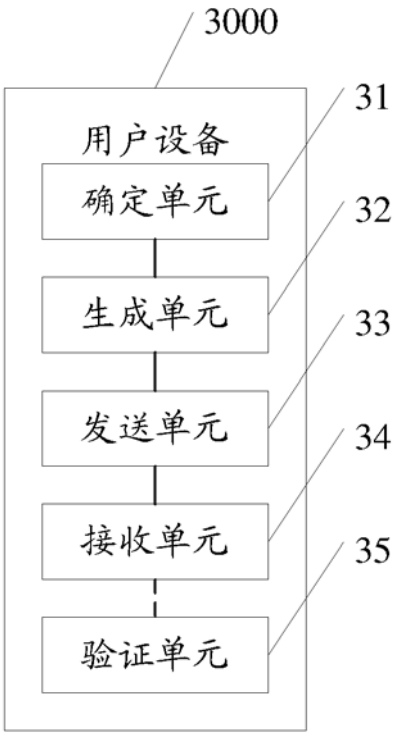

3000
用户设备
确定单元
生成单元
发送单元
接收单元
验证单元
31
32
33
34
35

图8

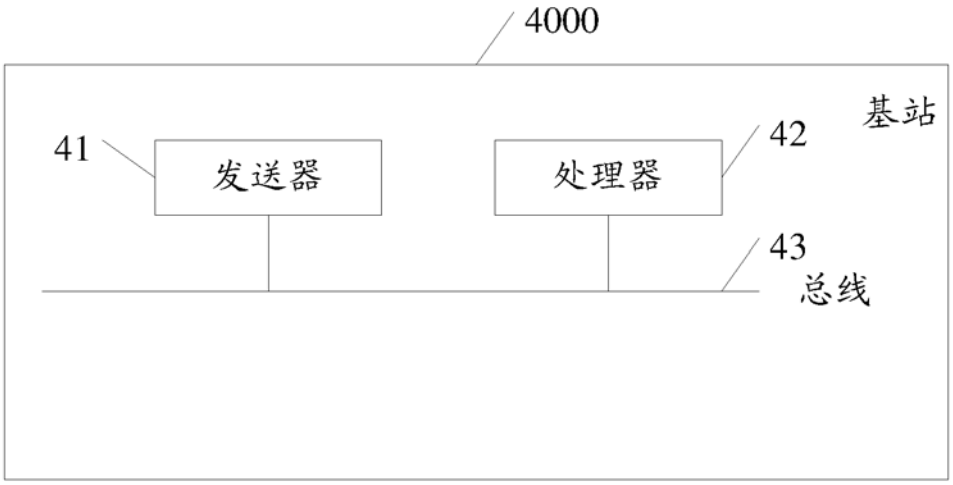

4000
基站
41
发送器
处理器
42
43
总线

图9

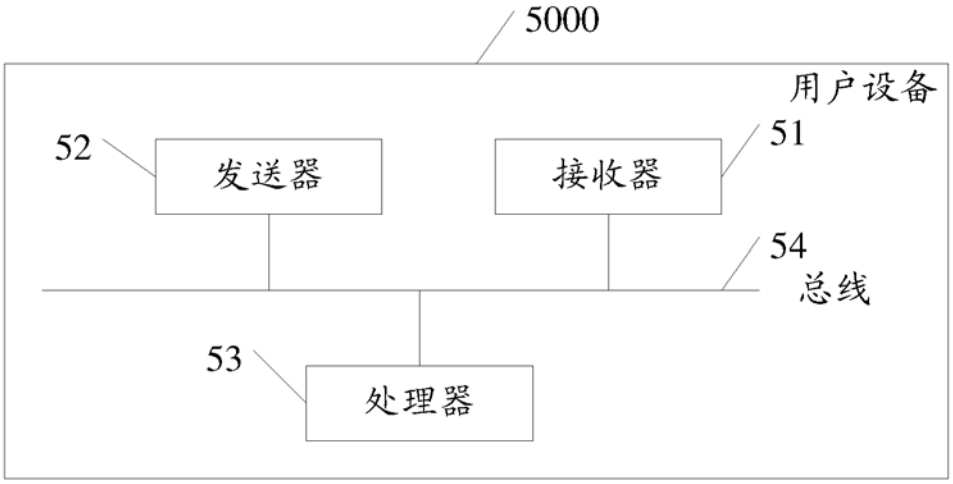


图10