(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 109691157 B
(45)授权公告日 2022.05.03

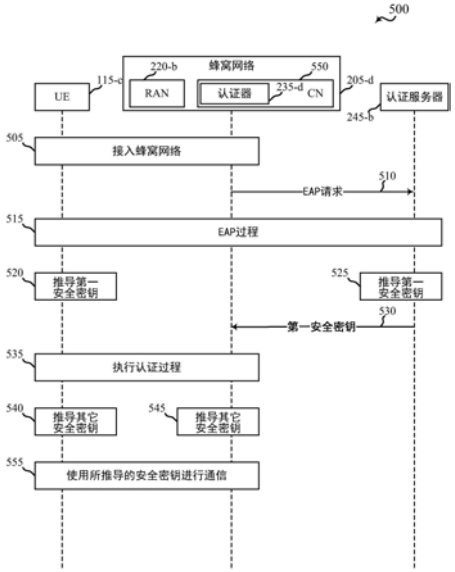
(21)申请号 201780056316.4
(22)申请日 2017.08.17
(65)同一申请的已公布的文献号
申请公布号 CN 109691157 A
(43)申请公布日 2019.04.26
(30)优先权数据
62/396,791 2016.09.19 US
15/489,670 2017.04.17 US
(85)PCT国际申请进入国家阶段日
2019.03.13
(86)PCT国际申请的申请数据
PCT/US2017/047355 2017.08.17
(87)PCT国际申请的公布数据
WO2018/052640 EN 2018.03.22
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 S·B·李 A·帕拉尼恭德尔
A·E·埃斯科特
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张立达 王英
(51)Int.Cl.
H04W 12/041(2021.01)
H04W 12/06(2021.01)
H04W 12/122(2021.01)
(56)对比文件
US 2016127903 A1,2016.05.05
CN 101656957 A,2010.02.24
CN 102045173 A,2011.05.04
WO 2009087006 A1,2009.07.16
US 2010281249 A1,2010.11.04
US 2016127897 A1,2016.05.05
审查员 孙铭君
权利要求书6页 说明书22页 附图18页

(54)发明名称

用于无线通信的方法、装置和非暂时性计算机可读介质

(57)摘要

描述了用于无线通信的技术。一种用于用户设备(UE)处的无线通信的方法包括经由认证器与认证服务器执行扩展认证协议(EAP)过程。该EAP过程至少部分基于在UE和认证服务器之间交换的一组认证凭证。该方法还包括:作为执行EAP过程的一部分,推导主会话密钥(MSK)和扩展主会话密钥(EMSK),所述MSK和所述EMSK至少部分基于认证凭证和第一组参数;确定与认证器相关联的网络类型;以及至少部分基于所确定的网络类型,与认证器执行至少一个认证过程。该至少一个认证过程基于MSK或EMSK与所确定的网络类型的关联。



CN 109691157 B

1.一种用于用户设备UE处的无线通信的方法,包括:

经由认证器与认证服务器执行扩展认证协议EAP过程,所述EAP过程至少部分基于在所述UE和所述认证服务器之间交换的一个或多个认证凭证;

作为执行所述EAP过程的一部分,推导主会话密钥MSK和扩展主会话密钥EMSK,所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

确定与所述认证器相关联的网络类型;以及

至少部分基于所确定的网络类型,与所述认证器执行至少一个认证过程,所述至少一个认证过程基于所述MSK或所述EMSK与所确定的网络类型的关联。

2.如权利要求1所述的方法,其中,所确定的网络类型包括蜂窝网络类型,并且与所述认证器执行所述至少一个认证过程包括:

推导蜂窝网络的第一安全密钥,所述第一安全密钥至少部分基于所述EMSK和一个或多个参数的第二集合。

3.如权利要求2所述的方法,其中,所述一个或多个参数的第二集合包括:所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

4.如权利要求2所述的方法,其中,与所述认证器执行所述至少一个认证过程包括:

推导所述蜂窝网络的网络节点的第二安全密钥,所述第二安全密钥至少部分基于所述第一安全密钥和一个或多个参数的第三集合;以及

至少部分基于所述第二安全密钥,经由所述网络节点与所述蜂窝网络通信。

5.如权利要求4所述的方法,其中,所述一个或多个参数的第三集合包括:所述网络节点的标识符、至少一个网络节点特定参数、所述UE和所述网络节点之间交换的至少一个参数或者它们的组合。

6.如权利要求1所述的方法,其中,所述一个或多个参数的第一集合包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

7.如权利要求2所述的方法,其中,所述蜂窝网络包括以下各项中的至少一项:第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

8.如权利要求1所述的方法,其中,所确定的网络类型是非蜂窝网络类型,并且与所述认证器执行所述至少一个认证过程包括:

推导非蜂窝网络的第一安全密钥,所述第一安全密钥至少部分基于所述MSK和一个或多个参数的第二集合。

9.一种用于用户设备UE处的无线通信的装置,包括:

处理器;以及

与所述处理器电子通信的存储器;

其中,所述处理器和所述存储器被配置为:

经由认证器与认证服务器执行扩展认证协议EAP过程,所述EAP过程至少部分基于在所述UE和所述认证服务器之间交换的一个或多个认证凭证;

作为执行所述EAP过程的一部分,推导主会话密钥MSK和扩展主会话密钥EMSK,所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

确定与所述认证器相关联的网络类型;以及

至少部分基于所确定的网络类型,与所述认证器执行至少一个认证过程,所述至少一个认证过程基于所述MSK或所述EMSK与所述网络类型的关联。

10.一种用于用户设备UE处的无线通信的装置,包括:

用于经由认证器与认证服务器执行扩展认证协议EAP过程的单元,所述EAP过程至少部分基于在所述UE和所述认证服务器之间交换的一个或多个认证凭证;

用于作为执行所述EAP过程的一部分,推导主会话密钥MSK和扩展主会话密钥EMSK的单元,所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

用于确定与所述认证器相关联的网络类型的单元;以及

用于至少部分基于所确定的网络类型,与所述认证器执行至少一个认证过程的单元,所述至少一个认证过程基于所述MSK或所述EMSK与所确定的网络类型的关联。

11.如权利要求10所述的装置,其中,所确定的网络类型包括蜂窝网络类型,并且所述用于执行所述至少一个认证过程的单元包括:

用于推导蜂窝网络的第一安全密钥的单元,所述第一安全密钥至少部分基于所述EMSK和一个或多个参数的第二集合。

12.如权利要求11所述的装置,其中,所述一个或多个参数的第二集合包括:所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

13.如权利要求11所述的装置,其中,所述用于执行所述至少一个认证过程的单元包括:

用于推导所述蜂窝网络的网络节点的第二安全密钥的单元,所述第二安全密钥至少部分基于所述第一安全密钥和一个或多个参数的第三集合;以及

用于至少部分基于所述第二安全密钥,经由所述网络节点与所述蜂窝网络通信的单元。

14.如权利要求13所述的装置,其中,所述一个或多个参数的第三集合包括:所述网络节点的标识符、至少一个网络节点特定参数、所述UE和所述网络节点之间交换的至少一个参数或者它们的组合。

15.如权利要求10所述的装置,其中,所述一个或多个参数的第一集合包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

16.如权利要求11所述的装置,其中,所述蜂窝网络包括以下各项中的至少一项:第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

17.如权利要求10所述的装置,其中,所确定的网络类型是非蜂窝网络类型,并且所述用于执行所述至少一个认证过程的单元包括:

用于推导非蜂窝网络的第一安全密钥的单元,所述第一安全密钥至少部分基于所述MSK和一个或多个参数的第二集合参数。

18.一种存储用于用户设备UE处的无线通信的计算机可执行代码的非暂时性计算机可读介质,所述代码可由处理器执行以进行以下操作:

经由认证器与认证服务器执行扩展认证协议EAP过程,所述EAP过程至少部分基于在所述UE和所述认证服务器之间交换的一个或多个认证凭证;

作为执行所述EAP过程的一部分,推导主会话密钥MSK和扩展主会话密钥EMSK,所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

确定与所述认证器相关联的网络类型;以及

至少部分基于所确定的网络类型,与所述认证器执行至少一个认证过程,所述至少一个认证过程基于所述MSK或所述EMSK与所确定的网络类型的关联。

19.一种用于认证服务器处的无线通信的方法,包括:

经由认证器与用户设备UE执行扩展认证协议EAP过程,所述EAP过程至少部分基于在所述认证服务器和所述UE之间交换的一个或多个认证凭证;

作为执行所述EAP过程的一部分,推导主会话密钥MSK和扩展主会话密钥EMSK,所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

确定与所述认证器相关联的网络类型;

至少部分基于所述MSK或所述EMSK与所述网络类型的关联,并且至少部分基于一个或多个参数的第二集合,推导所确定的网络类型的安全密钥;以及

经由安全信道将所述安全密钥发送给所述认证器。

20.如权利要求19所述的方法,其中,所述一个或多个参数的第一集合包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

21.如权利要求19所述的方法,其中,所确定的网络类型包括蜂窝网络类型,并且所述一个或多个参数的第二集合包括:蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述认证服务器和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

22.如权利要求21所述的方法,其中,所述蜂窝网络包括以下各项中的至少一项:第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

23.一种用于认证服务器处的无线通信的装置,包括:

处理器;以及

与所述处理器电子通信的存储器;

其中,所述处理器和所述存储器被配置为:

经由认证器与用户设备(UE)执行扩展认证协议(EAP)过程,所述EAP过程至少部分基于在所述认证服务器和所述UE之间交换的一个或多个认证凭证;

作为执行所述EAP过程的一部分,推导主会话密钥(MSK)和扩展主会话密钥(EMSK),所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合;

确定与所述认证器相关联的网络类型;

至少部分基于所述MSK或所述EMSK与所确定网络类型的关联,并且至少部分基于一个或多个参数的第二集合,推导所确定的网络类型的安全密钥;以及

经由安全信道将所述安全密钥发送给所述认证器。

24.一种用于认证服务器处的无线通信的装置,包括:

用于经由认证器与用户设备(UE)执行扩展认证协议(EAP)过程的单元,所述EAP过程至少部分基于在所述认证服务器和所述UE之间交换的一个或多个认证凭证;

用于作为执行所述EAP过程的一部分，推导主会话密钥(MSK)和扩展主会话密钥(EMSK)的单元，所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合；

用于确定与所述认证器相关联的网络类型的单元；

用于至少部分基于所述MSK或所述EMSK与所确定的网络类型的关联，并且至少部分基于一个或多个参数的第二集合，推导所确定的网络类型的安全密钥的单元；以及

用于经由安全信道将所述安全密钥发送给所述认证器的单元。

25.如权利要求24所述的装置，其中，所述一个或多个参数的第一集合包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

26.如权利要求24所述的装置，其中，所确定的网络类型包括蜂窝网络类型，并且所述一个或多个参数的第二集合包括：蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述认证服务器和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

27.如权利要求26所述的装置，其中，所述蜂窝网络包括以下各项中的至少一项：第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

28.一种存储用于认证服务器处的无线通信的计算机可执行代码的非暂时性计算机可读介质，所述代码可由处理器执行以进行以下操作：

经由认证器与用户设备UE执行扩展认证协议EAP过程，所述EAP过程至少部分基于在所述认证服务器和所述UE之间交换的一个或多个认证凭证；

作为执行所述EAP过程的一部分，推导主会话密钥MSK和扩展主会话密钥EMSK，所述MSK和所述EMSK至少部分基于所述一个或多个认证凭证和一个或多个参数的第一集合；

确定与所述认证器相关联的网络类型；

至少部分基于所述MSK或所述EMSK与所确定的网络类型的关联，并且至少部分基于一个或多个参数的第二集合，推导所确定的网络类型的安全密钥；以及

经由安全信道将所述安全密钥发送给所述认证器。

29.一种用于蜂窝网络处的无线通信的方法，包括：

在认证器处，从认证服务器接收第一安全密钥，

其中，所述第一安全密钥是所述认证服务器至少部分基于在主会话密钥MSK或扩展主会话密钥EMSK和所述认证服务器确定的、关联于所述认证器的网络类型之间的关联，以及至少部分基于一个或多个参数的第一集合，来推导的，并且

其中，所述MSK和所述EMSK至少部分基于一个或多个认证凭证和一个或多个参数的第二集合，所述一个或多个认证凭证是在扩展认证协议EAP过程期间在用户设备UE和所述认证服务器之间交换的；以及

由所述认证器至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程。

30.如权利要求29所述的方法，其中，与所述UE执行所述至少一个认证过程包括：

推导所述蜂窝网络的网络节点的第二安全密钥，所述第二安全密钥至少部分基于所述第一安全密钥和一个或多个参数的第三集合；以及

至少部分基于所述第二安全密钥，经由所述网络节点与所述UE通信。

31.如权利要求30所述的方法，其中，所述一个或多个参数的第三集合包括：所述网络

节点的标识符、至少一个网络节点特定参数、所述UE和所述网络节点之间交换的至少一个参数或者它们的组合。

32.如权利要求29所述的方法，其中，所述一个或多个参数的第一集合包括：所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

33.如权利要求29所述的方法，其中，所述一个或多个参数的第二集合包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

34.如权利要求29所述的方法，其中，所述蜂窝网络包括以下各项中的至少一项：第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

35.一种用于蜂窝网络处的无线通信的装置，包括：

处理器；以及

与所述处理器电子通信的存储器；

其中，所述处理器和所述存储器被配置为：

在认证器处，从认证服务器接收第一安全密钥，

其中，所述第一安全密钥是所述认证服务器至少部分基于在主会话密钥MSK或扩展主会话密钥EMSK和所述认证服务器确定的、关联于所述认证器的网络类型之间的关联，以及至少部分基于一个或多个参数的第一集合，来推导的并且

其中，所述MSK和所述EMSK至少部分基于一个或多个认证凭证和一个或多个参数的第二集合，所述一个或多个认证凭证是在扩展认证协议EAP过程期间在用户设备UE和所述认证服务器之间交换的；以及

通过所述认证器至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程。

36.一种用于蜂窝网络处的无线通信的装置，包括：

用于在认证器处，从认证服务器接收第一安全密钥的单元，

其中，所述第一安全密钥是所述认证服务器至少部分基于在主会话密钥MSK或扩展主会话密钥EMSK和所述认证服务器确定的、关联于所述认证器的网络类型之间的关联，以及至少部分基于一个或多个参数的第一集合，来推导的并且

其中，所述MSK和所述EMSK至少部分基于一个或多个认证凭证和一个或多个参数的第二集合，所述一个或多个认证凭证是在扩展认证协议EAP过程期间在用户设备UE和所述认证服务器之间交换的；以及

用于通过所述认证器至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程的单元。

37.如权利要求36所述的装置，其中，所述用于与所述UE执行所述至少一个认证过程的单元包括：

用于推导所述蜂窝网络的网络节点的第二安全密钥的单元，所述第二安全密钥至少部分基于所述第一安全密钥和一个或多个参数的第三集合；以及

用于至少部分基于所述第二安全密钥，经由所述网络节点与所述UE通信的单元。

38.如权利要求37所述的装置，其中，所述一个或多个参数的第三集合包括：所述网络节点的标识符、至少一个网络节点特定参数、所述UE和所述网络节点之间交换的至少一个

参数或者它们的组合。

39.如权利要求36所述的装置,其中,所述一个或多个参数的第一集合包括:所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

40.如权利要求36所述的装置,其中,所述一个或多个参数的第二集合包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

41.如权利要求36所述的装置,其中,所述蜂窝网络包括以下各项中的至少一项:第五代(5G)网络、第四代(4G)网络、长期演进(LTE)网络、高级LTE(LTE-A)网络、第三代(3G)网络或者它们的组合。

42.一种存储用于蜂窝网络处的无线通信的计算机可执行代码的非暂时性计算机可读介质,所述代码可由处理器执行以进行以下操作:

在认证器处,从认证服务器接收第一安全密钥,

其中,所述第一安全密钥是所述认证服务器至少部分基于在主会话密钥MSK或扩展主会话密钥EMSK和所述认证服务器确定的、关联于所述认证器的网络类型之间的关联,以及至少部分基于一个或多个参数的第一集合,来推导的并且

其中,所述MSK和所述EMSK至少部分基于一个或多个认证凭证和一个或多个参数的第二集合,所述一个或多个认证凭证是在扩展认证协议EAP过程期间在用户设备UE和所述认证服务器之间交换的;以及

由所述认证器至少部分基于所述第一安全密钥,与所述UE执行至少一个认证过程。

用于无线通信的方法、装置和非暂时性计算机可读介质

[0001] 交叉引用

[0002] 本专利申请要求享有由Lee等人于2017年4月17日递交的、名称为“Techniques For Deriving Security Keys For A Cellular Network Based On Performance of an Extensible Authentication Protocol(EAP)Procedure”的美国专利申请No.15/489,670;以及由Lee等人于2016年9月19日递交的、名称为“Techniques For Deriving Security Keys For A Cellular Network Based On Performance Of an Extensible Authentication Protocol(EAP)Procedure”的美国临时专利申请No.62/396,791的优先权;上述每个申请被转让给本申请的受让人。

技术领域

[0003] 本公开内容例如涉及无线通信系统,更具体地说,涉及用于基于扩展认证协议(EAP)过程的执行来推导蜂窝网络的安全密钥的技术。

背景技术

[0004] 无线通信系统被广泛地部署以提供各种类型的通信内容,例如语音、视频、分组数据、消息传送、广播等等。这些系统可以是能够通过共享可用系统资源(例如,时间、频率和功率)来支持与多个用户通信的多址系统。这些多址系统的示例包括码分多址(CDMA)系统、时分多址(TDMA)系统、频分多址(FDMA)系统和正交频分多址(OFDMA)系统。

[0005] 在一些示例中,无线多址通信系统可以是或包括蜂窝网络。蜂窝网络可以包括多个网络接入设备,每个网络接入设备同时支持多个通信设备(或者公知为用户设备(UE))的通信。在第四代(4G)网络、长期演进(LTE)网络或高级LTE(LTE-A)网络中,网络接入设备可以采取增强型节点B(eNB)的形式,每个eNB包括一个或多个基站的集合。在第五代(5G或下一代(NextGen))网络中,网络接入设备可以在与网络接入设备控制器(例如,接入节点控制器(ANC))的通信中采取智能无线电头端(SRH)或gNodeB(gNB)的形式,其中,与网络接入设备控制器通信的一个或多个网络接入设备的集合定义网络节点。eNB、gNB或网络节点可以在下行链路信道(例如,用于从eNB、gNB或网络节点到该UE的传输)和上行链路信道(例如,用于从UE到eNB、gNB或网络节点的传输)上与UE集合通信。

[0006] 当UE接入蜂窝网络时,UE或蜂窝网络可以发起使UE能够向蜂窝网络的认证器认证它自己,并且使认证器能够向UE认证蜂窝网络的一个或多个过程。在一些示例中,认证过程可以包括EAP过程,其中,具有与认证认证器的安全连接的认证服务器对UE进行认证;使UE能够推导一个或多个安全密钥用于向认证器认证它自己;以及推导在安全连接上发送给认证器的一个或多个安全密钥,以便使认证器能够向UE认证蜂窝网络。

发明内容

[0007] 在一些情况下,蜂窝网络可以允许经由不同类型的接入网络接入该蜂窝网络,其中的一些接入网络可能或多或少容易受到攻击,并且其中一些可能或多或少处于该蜂窝网

络的运营商的控制下。例如，蜂窝网络可以允许经由蜂窝接入网络或非蜂窝接入网络(例如，无线局域网(WLAN))接入该蜂窝网络。当与不同接入网络相关联的认证器支持相同的EAP过程时，作为经由与蜂窝接入网络相关联的认证器或与非蜂窝接入网络相关联的认证器执行该EAP过程的结果，可以推导相同的主会话密钥(MSK)。因此，该相同的MSK或从其推导的相同安全密钥可以被提供给与该蜂窝接入网络相关联的认证器或与该非蜂窝接入网络相关联的认证器。如果非蜂窝接入网络被攻击者损害，则该攻击者对MSK或从其推导的安全密钥的访问可以使该攻击者能够使用该非蜂窝接入网络向UE冒充该蜂窝接入网络，这会损害该UE和/或运行在该UE上的应用的安全性。本公开内容中描述的技术通过确定与认证器相关联的网络类型和基于与该网络类型相关联的EAP会话密钥(例如，MSK或扩展MSK(EMSK))的类型与该认证器执行认证过程(或推导该认证器的安全密钥)来帮助减轻这种威胁。在一些示例中，当认证器与非蜂窝接入网络相关联时，可以使用MSK，并且当认证器与蜂窝接入网络相关联时可以使用EMSK。

[0008] 在一个示例中，描述了一种用于UE处的无线通信的方法。所述方法可以包括经由认证器与认证服务器执行EAP过程。所述EAP过程至少部分基于在所述UE和所述认证服务器之间交换的认证凭证的集合。所述方法还可以包括作为执行所述EAP过程的一部分，推导MSK和EMSK，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；确定与所述认证器相关联的网络类型；以及至少部分基于所确定的网络类型与所述认证器执行至少一个认证过程。所述至少一个认证过程可以基于所述MSK或所述EMSK与所确定的网络类型的关联。

[0009] 在一个示例中，描述了一种用于UE处的无线通信的装置。所述装置可以包括用于经由认证器与认证服务器执行EAP过程的单元。所述EAP过程可以至少部分基于在所述UE和所述认证服务器之间交换的认证凭证的集合。所述装置还可以包括用于作为执行所述EAP过程的一部分，推导MSK和EMSK的单元，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；用于确定与所述认证器相关联的网络类型的单元；以及用于与所述认证器执行至少一个认证过程的单元。所述至少一个认证过程可以基于所述MSK或所述EMSK与所确定的网络类型的关联。

[0010] 在一个示例中，描述了一种用于UE处的无线通信的另一装置。所述装置可以包括处理器和与所述处理器电子通信的存储器。所述处理器和所述存储器可以被配置为经由认证器与认证服务器执行EAP过程。所述EAP过程可以至少部分基于在所述UE和所述认证服务器之间交换的认证凭证的集合。所述处理器和存储器还可以被配置为作为执行所述EAP过程的一部分，推导MSK和EMSK，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；确定与所述认证器相关联的网络类型；以及至少部分基于所确定的网络类型与所述认证器执行至少一个认证过程。所述至少一个认证过程可以基于所述MSK或所述EMSK与所确定的网络类型的关联。

[0011] 在一个示例中，描述了一种存储用于UE处的无线通信的计算机可执行代码的非暂时性计算机可读介质。所述代码可以由处理器执行以经由认证器与认证服务器执行EAP过程。所述EAP过程可以至少部分基于在所述UE和所述认证服务器之间交换的认证凭证的集合。所述代码还可以由所述处理器执行以作为执行所述EAP过程的一部分，推导MSK和EMSK，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；确定与所述认证器相

关联的网络类型;以及至少部分基于所确定的网络类型与所述认证器执行至少一个认证过程。所述至少一个认证过程可以基于所述MSK或所述EMSK与所确定的网络类型的关联。

[0012] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中,所确定的网络类型可以包括蜂窝网络类型,并且与所述认证器执行所述至少一个认证过程可以包括推导蜂窝网络的第一安全密钥。所述第一安全密钥可以至少部分基于所述EMSK和参数的第二集合。在一些示例中,所述参数的第二集合可以包括:所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

[0013] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中,与所述认证器执行所述至少一个认证过程可以包括推导所述蜂窝网络的网络节点的第二安全密钥,所述第二安全密钥至少部分基于所述第一安全密钥和参数的第三集合;以及至少部分基于所述第二安全密钥经由所述网络节点与所述蜂窝网络通信。在这些示例中的一些中,所述参数的第三集合可以包括:所述网络节点的标识符、至少一个网络节点特定参数、所述UE和所述网络节点之间交换的至少一个参数或者它们的组合。

[0014] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中,所述参数的第一集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0015] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中,所述蜂窝网络可以包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0016] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中,所确定的网络类型可以包括非蜂窝网络类型,并且与所述认证器执行所述至少一个认证过程可以包括推导非蜂窝网络的第一安全密钥。所述第一安全密钥可以至少部分基于所述MSK和参数的第二集合。

[0017] 在一个示例中,一种用于认证服务器处的无线通信的方法可以包括经由认证器与UE执行EAP过程。所述EAP过程可以至少部分基于在所述认证服务器和所述UE之间交换的认证凭证的集合。所述方法还可以包括作为执行所述EAP过程的一部分,推导MSK和EMSK,所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合;确定与所述认证器相关联的网络类型;至少部分基于所述MSK或所述EMSK与所述网络类型的关联,并且至少部分基于参数的第二集合推导所确定的网络类型的安全密钥;以及经由安全信道将所述安全密钥发送给所述认证器。

[0018] 在一个示例中,描述了一种用于认证服务器处的无线通信的装置。所述装置可以包括用于经由认证器与UE执行EAP过程的单元。所述EAP过程可以至少部分基于在所述认证服务器和所述UE之间交换的认证凭证的集合。所述装置还可以包括用于作为执行所述EAP过程的一部分,推导MSK和EMSK的单元,所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合;用于确定与所述认证器相关联的网络类型的单元;用于至少部分基于所述MSK或所述EMSK与所述网络类型的关联,并且至少部分基于参数的第二集合,推导所确定的网络类型的安全密钥的单元;以及用于经由安全信道将所述安全密钥发送给所述认证器的单元。

[0019] 在一个示例中,描述了另一种用于认证服务器处的无线通信的装置。所述装置可

以包括处理器和与所述处理器电子通信的存储器。所述处理器和存储器可以被配置为经由认证器与UE执行EAP过程。所述EAP过程可以至少部分基于在所述认证服务器和所述UE之间交换的认证凭证的集合。所述处理器和所述存储器还可以被配置为作为执行所述EAP过程的一部分，推导MSK和EMSK，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；确定与所述认证器相关联的网络类型；至少部分基于所述MSK或所述EMSK与所述网络类型的关联，并且至少部分基于参数的第二集合，推导所确定的网络类型的安全密钥；以及经由安全信道将所述安全密钥发送给所述认证器。

[0020] 在一个示例中，描述了一种存储用于认证服务器处的无线通信的计算机可执行代码的非暂时性计算机可读介质。所述代码可以由处理器执行以经由认证器与UE执行EAP过程。所述EAP过程可以至少部分基于在所述认证服务器和所述UE之间交换的认证凭证的集合。所述代码还可以由所述处理器执行以作为执行所述EAP过程的一部分，推导MSK和EMSK，所述MSK和所述EMSK至少部分基于所述认证凭证和参数的第一集合；确定与所述认证器相关联的网络类型；至少部分基于所述MSK或所述EMSK与所述网络类型的关联，并且至少部分基于参数的第二集合，推导所确定的网络类型的安全密钥；以及经由安全信道将所述安全密钥发送给所述认证器。

[0021] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所述参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0022] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所确定的网络类型可以包括蜂窝网络类型，并且所述参数的第二集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、所述认证服务器和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

[0023] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所述蜂窝网络可以包括以下各项中的至少一项：5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0024] 在一个示例中，描述了一种用于蜂窝网络处的无线通信的方法。所述方法可以包括从认证服务器接收第一安全密钥，所述第一安全密钥至少部分基于EMSK和参数的第一集合。所述EMSK可以至少部分基于认证凭证的集合和参数的第二集合。所述认证凭证可以在EAP过程期间在UE和所述认证服务器之间交换。所述方法还可以包括：至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程。

[0025] 在一个示例中，描述了一种用于蜂窝网络处的无线通信的装置。所述装置可以包括用于从认证服务器接收第一安全密钥的单元，所述第一安全密钥至少部分基于EMSK和参数的第一集合。所述EMSK可以至少部分基于认证凭证的集合和参数的第二集合。所述认证凭证可以在EAP过程期间在UE和所述认证服务器之间交换。所述装置还可以包括用于至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程的单元。

[0026] 在一个示例中，描述了另一种用于蜂窝网络处的无线通信的装置。所述装置可以包括处理器和与所述处理器电子通信的存储器。所述处理器和所述存储器可以被配置为从认证服务器接收第一安全密钥，所述第一安全密钥至少部分基于EMSK和参数的第一集合。所述EMSK至少部分基于认证凭证的集合和参数的第二集合。所述认证凭证可以在EAP过程

期间在UE和所述认证服务器之间交换。所述处理器和存储器还可以被配置为至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程。

[0027] 在一个示例中，描述了一种存储用于蜂窝网络处的无线通信的计算机可执行代码的非暂时性计算机可读介质。所述代码可由处理器执行以从认证服务器接收第一安全密钥，所述第一安全密钥至少部分基于EMSK和参数的第一集合。所述EMSK至少部分基于认证凭证的集合和参数的第二集合。所述认证凭证可以在EAP过程期间在UE和所述认证服务器之间交换。所述代码还可执行用于至少部分基于所述第一安全密钥，与所述UE执行至少一个认证过程。

[0028] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，与所述UE执行所述至少一个认证过程可以包括推导所述蜂窝网络的网络节点的第二安全密钥，所述第二安全密钥至少部分基于所述第一安全密钥和参数的第三集合；以及至少部分基于所述第二安全密钥经由所述网络节点与所述UE通信。在一些示例中，所述参数的第三集合可以包括：所述网络节点的标识符、至少一个网络节点特定参数、在所述UE和所述网络节点之间交换的至少一个参数或者它们的组合。

[0029] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所述参数的第二集合可以包括：所述蜂窝网络的标识符、至少一个蜂窝网络特定参数、在所述UE和所述蜂窝网络之间交换的至少一个参数或者它们的组合。

[0030] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所述参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0031] 在上面描述的方法、装置和非暂时性计算机可读介质的一些示例中，所述蜂窝网络可以包括以下各项中的至少一项：5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0032] 前面已经对根据本公开内容的示例的技术和技术优点进行了相当广泛的概述，以便可以更好地理解下面的详细描述。下文将描述另外的技术和优点。公开的构思和具体示例可以容易地被作为用于修改或设计用于执行本公开内容的相同目的的其它结构的基础。这样的等同构造没有脱离所附权利要求的范围。通过以下结合附图时考虑的描述，将更好地理解被认为在它们的组织上和在操作方法二者上是本申请公开的构思的特性以及关联的优点。各图都仅是被提供用于说明和描述的目的，并不旨在作为权利要求的限制的定义。

附图说明

[0033] 通过参照以下附图可以实现对本发明的本质和优点的进一步的理解。在附图中，类似的组件或功能可以具有相同的附图标记。此外，可以通过在附图标记后跟随破折号和在类似组件当中进行区分的第二标记来区分相同类型的各种组件。如果在本说明书中只使用了第一附图标记，则该描述可适用于具有相同的第一附图标记的类似组件中的任意一个，而不考虑第二附图标记。

[0034] 图1示出根据本公开内容的各个方面的无线通信系统的示例；

[0035] 图2示出根据本公开内容的各个方面的无线通信系统的示例；

[0036] 图3示出根据本公开内容的各个方面的无线通信系统的密钥层级的示例。

[0037] 图4示出根据本公开内容的各个方面的无线通信系统的示例；

[0038] 图5示出根据本公开内容的各个方面的在UE、蜂窝网络和认证服务器之间的示例消息流；

[0039] 图6示出根据本公开内容的各个方面的UE的框图；

[0040] 图7示出根据本公开内容的各个方面的无线通信管理器的框图；

[0041] 图8示出根据本公开内容的各个方面的无线通信系统的示意图；

[0042] 图9示出根据本公开内容的各个方面的认证服务器的框图；

[0043] 图10示出根据本公开内容的各个方面的认证服务器的框图；

[0044] 图11示出根据本公开内容的各个方面的网络节点的框图；

[0045] 图12示出根据本公开内容的各个方面的通信管理器的框图；

[0046] 图13示出根据本公开内容的各个方面的网络节点的示意图；以及

[0047] 图14-18示出说明根据本公开内容的各个方面的无线通信的方法的流程图。

具体实施方式

[0048] 本公开内容中描述的技术使UE能够经由与不同类型的接入网络相关联的认证器与认证服务器执行EAP过程。在成功地经由认证器执行了EAP过程时，UE和认证服务器可以至少部分基于与认证器相关联的网络类型来推导认证器的安全密钥。在一些示例中，UE和认证服务器可以在认证器与非蜂窝接入网络相关联时基于MSK来推导认证器的安全密钥，并且可以在认证器与蜂窝接入网络相关联时基于EMSK来推导认证器的安全密钥。

[0049] 以下描述提供了示例，但并不限制权利要求书中阐述的范围、适用性或示例。可以改变所论述的元素的功能和布置而不脱离本公开内容的精神和范围。各个示例可以酌情省略、替代或者添加各种过程或组件。例如，可以按照与所描述顺序不同的顺序来执行所描述的方法，并且可以添加、省略或组合各个步骤。另外，可以将针对一些示例描述的特征组合到一些其它的示例中。

[0050] 图1示出根据本公开内容的各个方面的无线通信系统100的示例。无线通信系统100可以包括网络接入设备(例如，分布式网络接入设备、分布式单元、gNB、无线电头端(RH)、SRH、传输/接收点(TRP)、边缘节点、边缘单元等等)105、UE 115、网络接入设备控制器(例如，集中式网络接入设备、中央节点、中央单元、接入节点控制器(ANC)等等)125和核心网络130。核心网络130可以提供用户认证、接入授权、跟踪、互联网协议(IP)连接和其它接入、路由或移动功能。网络接入设备控制器125可以通过回程链路132(例如，S1、S2等等)与核心网络130交互，并且可以执行针对与UE 115的通信的无线配置和调度。在各个示例中，网络接入设备控制器125可以直接地或间接地(例如，通过核心网络130)通过回程链路134(例如，X1、X2等等)相互通信，回程链路134可以是有线或无线通信链路。每个网络接入设备控制器125还可以通过多个网络接入设备(例如，RH)105与多个UE 115通信。在无线通信系统100的替代配置中，网络接入设备控制器125的功能可以由网络接入设备105提供或者跨越网络节点(例如，接入节点、新无线基站(NR BS)等等)135的网络接入设备105分布。在无线通信系统100的另一个替代配置中，网络节点135可以由eNB替代，网络接入设备105可以用基站替代，并且网络接入设备控制器125可以由基站控制器替代(或者链接到核心网络130)。

[0051] 网络接入设备控制器125可以经由一个或多个网络接入设备105与UE115通信，每个网络接入设备105具有用于与多个UE 115无线通信的一个或多个天线。每个网络节点135可以为相应地理覆盖区域110提供通信覆盖，并且可以提供与一个或多个网络接入设备105相关联的一个或多个远程收发机。网络接入设备105可以执行LTE/LTE-A基站的很多功能。在一些示例中，网络接入设备控制器125可以用分布式形式实现，在每个网络接入设备105中提供网络接入设备控制器125的一部分。网络节点135的地理覆盖区域110可以被划分为只构成该覆盖区域的一部分的扇区(未示出)，并且在一些示例中，网络节点135的地理覆盖区域110可以通过与网络节点135相关联的一组网络接入设备105的一组地理覆盖区域构成(未示出)。在一些示例中，网络接入设备105可以用另外的网络接入设备替代，例如基站收发机、无线基站、接入点、无线收发机、节点B、eNB、家庭节点B、家庭演进型节点B、gNB等等。无线通信系统100可以包括不同类型(例如，宏小区和/或小型小区网络接入设备)的网络接入设备105(或者基站或其它网络接入设备)。网络接入设备105和/或网络节点135的地理覆盖区域可以交迭。在一些示例中，不同网络接入设备105可以与不同无线接入技术相关联。

[0052] 在一些示例中，无线通信系统100可以包括5G网络。在其它示例中，无线通信系统100可以包括LTE/LTE-A网络。无线通信系统100可以在一些情况下是异构网络，其中，不同类型的网络接入设备105或网络节点135为各个地理区域提供覆盖。例如，每个网络接入设备105或网络节点135可以为宏小区、小型小区和/或其它类型的小区提供通信覆盖。根据上下文，术语“小区”可以用于描述基站、RH、与基站或RH相关联的载波或分量载波、或者载波或基站的覆盖区域(例如，扇区等等)。

[0053] 宏小区可以覆盖相对大的地理区域(例如，半径为若干千米)并且可以允许具有与网络供应商的服务订制的UE 115接入。小型小区可以包括与宏小区相比较更低功率的RH或基站，并且可以工作在与宏小区相同或不同的频带中。根据各个示例，小型小区可以包括微微小区、毫微微小区和微小区。微微小区可以覆盖相对较小的地理区域并且可以允许具有与网络供应商的服务订制的UE 115不受限制的接入。毫微微小区也可以覆盖相对小的地理区域(例如，家庭)并且可以提供具有与该毫微微小区的关联性的UE 115(例如，闭合用户组(CSG)中的UE、家庭中的用户的UE等等)的受限制的接入。宏小区的网络接入设备可以被称为宏网络接入设备。小型小区的网络接入设备可以被称为小型小区网络接入设备、微微网络接入设备、毫微微网络接入设备或家庭网络接入设备。网络接入设备可以支持一个或多个(例如，两个、三个、四个等等)小区(例如，分量载波)。

[0054] 无线通信系统100可以支持同步或异步操作。对于同步操作，网络节点135或网络接入设备105可以具有相似的帧定时，并且来自不同网络接入设备105的传输可以在时间上近似对齐。对于异步操作，网络节点135或网络接入设备105可以具有不同帧定时，并且来自不同网络接入设备105的传输可以在时间上不对齐。本申请中描述的技术可以用于同步操作或异步操作。

[0055] 可以容适各个公开的示例中的一些示例的通信网络可以是根据分层协议栈操作的基于分组的网络。在用户平面中，承载或分组数据汇聚协议(PDCP)层处的通信可以是基于IP的。无线链路控制(RLC)层可以在一些情况下执行分组分段和重组以通过逻辑信道进行通信。介质访问控制(MAC)层可以执行优先级处理和逻辑信道向传输信道中的复用。MAC层还可以使用混合ARQ(HARQ)来提供MAC层处的重传以提高链路效率。在控制平面中，无线

资源控制(RRC)协议层可以提供UE 115和网络接入设备105、网络接入设备控制器125或支持用户平面数据的无线承载的核心网络130之间的RRC连接的建立、配置和维护。在物理(PHY)层处,传输信道可以映射到物理信道。

[0056] UE 115可以遍布整个无线通信系统100,并且每个UE 115可以是静止的或移动的。UE 115还可以包括或由本领域技术人员称为移动站、订户站、移动单元、订户单元、无线单元、远程单元、移动设备、无线设备、无线通信设备、远程设备、移动订户站、接入终端、移动终端、无线终端、远程终端、手持机、用户代理、移动客户端、客户端或一些其它合适的术语。UE 115可以是蜂窝电话、个人数字助理(PDA)、无线调制解调器、无线通信设备、手持设备、平板计算机、膝上型计算机、无绳电话、无线本地环路(WLL)站、万物互联(IoE)设备、机动车、电器或其它具有无线通信接口的电子设备。UE可以能够与各种类型的网络节点135或网络接入设备105(包括小型小区节点、中继节点等等)通信。UE还可以能够直接与其它UE通信(例如,使用对等(P2P)协议)。

[0057] 无线通信系统100中示出的通信链路122可以包括从UE 115到网络接入设备105的上行链路(UL)信道,和/或从网络接入设备105到UE 115的下行链路(DL)信道。下行链路信道还可以被称为前向链路信道,而上行链路信道还可以被称为反向链路信道。

[0058] 每条通信链路122可以包括一个或多个载波,其中,每个载波可以是由根据一个或多个无线接入技术调制的多个子载波或频调(例如,不同频率的波形信号)组成的信号。每个经调制的信号可以在不同子载波上发送并且可以携带控制信息(例如,参考信号、控制信道等等)、开销信息、用户数据等。通信链路122可以使用频分双工(FDD)技术(例如,使用成对的频谱资源)或时分双工(TDD)技术(例如,使用未成对的频谱资源)来发送双向通信。可以定义FDD的帧结构(例如,帧结构类型1)和TDD的帧结构(例如,帧结构类型2)。

[0059] 在无线通信系统100的一些示例中,网络接入设备105和/或UE 115可以包括用于采用天线分集方案来提高网络接入设备105和UE 115之间的通信质量和可靠性的多个天线。另外地或作为替代,网络接入设备105和/或UE 115可以采用多输入多输出(MIMO)技术,其可以利用多路环境的优势来发送携带相同或不同编码数据的多个空间层。

[0060] 无线通信系统100可以支持多个小区或载波上的操作,一种可以被称为载波聚合(CA)或多载波操作的特征。载波还可以被称为分量载波(CC)、层、信道等等。术语“载波”、“分量载波”、“小区”和“信道”可以在本申请中互换使用。UE 115可以配置有多个下行链路CC和一个或多个上行链路CC用于载波聚合。载波聚合可以与FDD分量载波和TDD分量载波二者一起使用。

[0061] 一个或多个UE 115可以包括无线通信管理器140。在一些示例中,无线通信管理器140可以用于经由与核心网络130相关联的认证器与认证服务器执行EAP过程。如参考图2所描述的,可以经由核心网络130接入认证服务器。EAP过程可以至少部分基于在UE和认证服务器之间交换的认证凭证的集合。无线通信管理器140还可以用于推导至少部分基于认证凭证和参数的第一集合的MSK和EMSK(共同地被称为EAP方法或认证方法)(作为执行EAP过程的一部分);确定认证器与蜂窝网络相关联;以及至少部分基于EMSK,与蜂窝网络执行至少一个认证过程。在一些示例中,无线通信管理器140可以是参考图6-8描述的无线通信管理器的方面的示例。

[0062] 图2示出根据本公开内容的各个方面的无线通信系统200的示例。无线通信系统

200可以包括UE 115-a的归属蜂窝网络205和由UE 115-a访问的蜂窝网络(即,被访问的蜂窝网络205-a)。

[0063] 归属蜂窝网络205可以包括第一认证器235(例如,提供归属安全锚定功能(H-SEAF)的服务器或设备)和归属用户平面网关(H-UP-GW)210。本领域技术人员应当领会的是,归属蜂窝网络205还可以包括提供其它功能的其它服务器或设备(未示出)。被访问的蜂窝网络205-a可以包括第二认证器235-a(例如,提供访问SEAF(V-SEAF)的服务器或设备)、被访问的UP-GW(V-UP-GW)210-a、被访问的蜂窝网络控制平面核心网络功能单元(V-CP-CN)215和无线接入网络(RAN)220。在一些示例中,RAN220可以包括参考图1描述的网络节点135、网络接入设备105和网络接入设备控制器125中的一个或多个。第一认证器235、H-UP-GW 210、第二认证器235-a、V-UP-GW 210-a和V-CP-CN 215可以是参考图1描述的核心网络130的示例性组件。

[0064] 归属蜂窝网络205可以与认证服务器245通信(或可以提供认证服务器245)。认证服务器245可以提供认证服务器功能单元(AUSF)。认证服务器245可以接入和/或调用认证凭证库和处理功能单元(ARPF)240。

[0065] UE 115-a可以经由RAN 220的节点(例如,网络接入设备)连接到被访问的蜂窝网络205-a。图2假设UE 115-a在操作在漫游模式中的同时接入被访问的蜂窝网络205-a。在非漫游场景中,UE 115-a可以经由归属蜂窝网络205的RAN而不是被访问的蜂窝网络205-a接入归属蜂窝网络205(图2中未示出)。

[0066] V-CP-CN 215可以包括或管理UE 115-a的移动性管理(MM)功能和/或会话管理(SM)功能的一个或多个方面,以及维护相对应的安全性上下文。第二认证器235-a可以促进并管理由被访问的蜂窝网络205-a对UE115-a的认证,以及可以维护可以从其推导后续安全密钥的锚定会话密钥。当用户平面安全性终止于V-UP-GW 210-a处时,V-UP-GW 210-a可以维护UE 115-a的用户平面安全性上下文(例如,安全密钥)。用户平面安全性可以由RAN 220和/或V-UP-GW 210-a终止并且可以由网络配置。一般来讲,UE 115-a可以维护与被访问的蜂窝网络205-a的每个节点的安全性上下文。

[0067] 在接入了被访问的蜂窝网络205-a时,第二认证器235-a可以促进由UE 115-a和认证服务器245执行的EAP过程。第二认证器235-a可以经由(归属蜂窝网络205的)第一认证器235建立或维护用于与认证服务器245执行EAP过程的安全信道。

[0068] 由UE 115-a和认证服务器245执行的EAP过程可以至少部分基于在UE 115-a和认证服务器245之间交换的认证凭证的集合。作为执行EAP过程的一部分,UE 115-a和认证服务器245中的每一个可以推导MSK和EMSK。MSK和EMSK可以至少部分基于认证凭证和参数的第一集合。在一些示例中,参数的第一集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0069] 当EAP过程成功时(例如,当UE 115-a和认证服务器245成功地相互认证时),认证服务器245可以向第二认证器235-a发送会话锚定密钥(例如,第一安全密钥)。根据本公开内容中描述的技术,会话锚定密钥可以至少部分基于EMSK。会话锚定密钥还可以至少部分基于参数的第二集合。参数的第二集合可以包括被访问的蜂窝网络205-a的标识符、至少一个蜂窝网络特定参数、在UE 115-a和第二蜂窝网络205-a之间交换的至少一个参数或者它们的组合。

[0070] UE 115-a可以独立地推导会话锚定密钥。至少部分基于会话锚定密钥,UE 115-a和第二认证器235-a可以相互认证并推导另外的安全密钥(例如,第二蜂窝网络205-a的其它节点或功能单元的安全密钥),如图3中所示。

[0071] 作为对图2中示出的替代,提供H-SEAF和V-SEAF的服务器或设备可以不假设在UE 115-a和认证服务器245之间执行的EAP过程中的认证器的角色,相反,认证器可以与认证服务器245(例如,提供AUSF的服务器)搭配使用。在这些示例中,认证服务器245可以基于MSK或EMSK和参数的第二集合来推导H-SEAF或V-SEAF的会话锚定密钥,并且将会话锚定密钥发送给H-SEAF(在非漫游场景中)或V-SEAF(在漫游场景中)。

[0072] 图3示出根据本公开内容的各个方面的无线通信系统的密钥层级300的示例。这一解决方案通过使用EMSK推导从EAP服务器(例如,参考图2描述的认证服务器245)向下传递的密钥(例如,K_{SEAF}),来提供到针对一般EAP协议递送给3GPP服务网络的密钥的服务网络绑定。在一些示例中,密钥层级300可以由参考图1和2描述的无线通信系统100和200使用。例如,UE和/或网络节点可以使用密钥层级300来实现参考图1和2描述的认证或安全性功能的一个或多个方面。

[0073] 密钥层级300可以包括用作通用用户识别模块(USIM)和ARPF之间的安全性上下文的K根密钥305。K根密钥305可以用作执行EAP过程和推导密钥310(例如,MSK和EMSK)以提供认证服务器和UE之间(例如,参考图2描述的认证服务器245和UE 115-a之间)的安全性上下文的基础。K根密钥305可以用于执行基于共享密钥的EAP过程,但是在执行基于证书的EAP过程时可以使用一个或多个其它密钥(例如,基于证书推导的密钥)。EMSK可以被认证服务器(例如,AUSF)和UE用于推导针对认证器(例如,针对参考图2描述的第二认证器235-a)的K_{SEAF}锚定会话密钥315。由于EMSK(而不是MSK)被用于推导K_{SEAF},因此可以不需要将凭证的使用限制于3GPP接入。例如,当非3GPP实体基于EAP认证获取MSK时,非3GPP实体无法推导K_{SEAF},这是因为K_{SEAF}是从非3GPP实体所不知道的EMSK推导出的。K_{SEAF}锚定会话密钥315可以由认证器和UE维护。

[0074] K_{SEAF}锚定会话密钥315可以被认证器用于推导K_{CP-CN}密钥320和K_{UP-GW}密钥325。K_{CP-CN}密钥320可以由CP-CN功能单元(例如,参考图2描述的V-CP-CN 215)和UE维护。K_{UP-GW}密钥325可以由UP-GW功能单元(例如,参考图2描述的V-UP-GW 210-a)和UE维护。K_{UP-GW}密钥325可以被UP-GW用于确立$K_{UP-GWenc}$密钥340和$K_{UP-GWint}$密钥345。$K_{UP-GWenc}$密钥340和$K_{UP-GWint}$密钥345可以用于用户平面分组的完整性保护和编码。

[0075] K_{CP-CN}密钥320可以被CP-CN功能单元用于推导K_{NASenc}密钥330、K_{NASint}密钥335和K_{AN}/NH密钥350。K_{AN}/NH密钥350可以被接入点用于推导K_{UPint}密钥355、K_{UPenc}密钥360、K_{RRCint}密钥365和K_{RRCenc}密钥370,它们可以用于RRC和用户平面分组的完整性保护和编码。

[0076] 图4示出根据本公开内容的各个方面的无线通信系统400的示例。无线通信系统400可以包括UE 115-b的归属蜂窝网络205-b和由UE 115-b访问的蜂窝网络(即,被访问的蜂窝网络205-c)。

[0077] 归属蜂窝网络205-b可以包括第一认证器235-b(例如,提供H-SEAF的服务器或设备)和H-UP-GW 210-b。归属蜂窝网络205-b还可以包括提供其它功能的其它服务器或设备(未示出)。被访问的蜂窝网络205-c可以包括第二认证器235-c(例如,提供V-SEAF的服务器或设备)、V-UP-GW210-c、V-CP-CN 215-a和RAN 220-a。在一些示例中,RAN 220-a可以包括

参考图1描述的网络节点135、网络接入设备105和网络接入设备控制器125中的一个或多个。第一认证器235-b、H-UP-GW 210-b、第二认证器235-c、V-UP-GW 210-c和V-CP-CN 215-a可以是参考图1描述的核心网络130的示例性组件。

[0078] 归属蜂窝网络205-b可以与认证服务器245-a通信(或者可以提供认证服务器245-a)。认证服务器245-a可以提供AUSF。认证服务器245-a可以接入和/或调用ARPF 240-a。

[0079] 第一认证器235-b、H-UP-GW 210-b、第二认证器235-c、V-UP-GW210-c、V-CP-CN 215-a、RAN 220-a、认证服务器245-a和ARPF 240-a中的每一个可以是参考图2描述的类似编号的组件、功能单元或节点的示例。

[0080] 图4还示出包括非蜂窝接入节点410(例如,WALN接入点(AP)或无线LAN控制器(WLC))的非蜂窝网络405。如图所示,UE 115-b可以连接到RAN 220-a或非蜂窝接入节点410,并且在每种情况下,相同的认证服务器245-a可以与UE 115-b执行EAP过程。当UE 115-b连接到RAN 220-a时,第二认证器235-c可以用作由UE 115-b和认证服务器245-a执行的EAP过程中的认证器。当UE 115-b连接到非蜂窝接入节点410时,非蜂窝接入节点410可以用作由UE 115-b和认证服务器245-a执行的EAP过程中的认证器。

[0081] 如果UE 115-b和认证服务器245-a二者都能够执行相同的EAP过程并推导相同的会话锚定密钥(例如,用于在UE 115-b和第二认证器235-c之间执行认证过程,或者用于在UE 115-b和非蜂窝接入节点410之间执行认证过程),包括非蜂窝接入节点410的攻击者可以能够从非蜂窝接入节点410获得该会话锚定密钥并使用它来假扮被访问的蜂窝网络205-c或归属蜂窝网络205-b的节点。为了解决上面提到的问题,UE 115-b和认证服务器245-a可以确定与认证器相关联的网络类型(例如,与第二认证器235-c或非蜂窝接入节点410相关联的网络的类型),并且确定要使用哪个密钥(在MSK和EMSK之间)来推导会话锚定密钥(即,基于该网络类型推导会话锚定密钥)。在一些示例中,在认证器(例如,非蜂窝接入节点410)与非蜂窝接入网络(例如,非蜂窝网络405)相关联时可以使用MSK,并且在认证器(例如,第二认证器235-c)与蜂窝接入网络(例如,被访问的蜂窝网络205-c)相关联时可以使用EMSK。另外,针对与蜂窝网络相关联的认证器推导的会话锚定密钥可以至少部分基于与该蜂窝网络相关联的参数的集合来推导得到。例如,K_{SEAF}密钥可以由UE 115-b和认证服务器245-a基于密钥推导公式(KDF)来推导得到

[0082] K_{SEAF}=KDF(EMSK,PLMN ID,CTX)

[0083] 其中,PLMN ID是与服务(例如,被访问的)蜂窝网络205-b相关联的且在该EAP过程期间提供给认证服务器245-a的公共陆地移动网络标识符,并且CTX是描述接入技术(例如,蜂窝网络接入,例如5G(NextGen)、4G、LTE/LTE-A或3G网络接入)的上下文。本领域技术人员应当领会的是,K_{SEAF}还可以至少部分基于其它合适的参数来推导得到。

[0084] 通过基于与认证器相关联的网络类型来推导认证器的会话锚定密钥,一个网络类型的网络无法获得另一个类型的网络的会话锚定密钥并且假扮不同网络类型的节点。因此,相同的EAP过程(或认证方法)可以用于不同类型的网络而不影响所述不同类型网络的安全性。

[0085] 图5示出根据本公开内容的各个方面的UE 115-c、蜂窝网络205-d和认证服务器245-b之间的示例性消息流500。UE 115-c可以是参考图1、2和4描述的UE 115的方面的示例。蜂窝网络205-d可以是参考图2和4描述的蜂窝网络205的示例,并且在一些情况下可以

包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。认证服务器245-b可以是参考图2和4描述的认证服务器245的方面的示例。蜂窝网络205-d可以包括RAN 220-b和蜂窝CN 550。RAN 220-b和CN 550可以是参考图2和4描述的RAN 220和CN的示例。在一些示例中,RAN 220-b可以包括参考图1描述的网络节点135、网络接入设备105或网络接入设备控制器125中的一个或多个。CN 550可以包括认证器235-d(例如,CN 550的节点),其可以是参考图2和4描述的认证器235的方面的示例。

[0086] 在505处,UE 115-c可以接入蜂窝网络205-d,并且UE 115-c或蜂窝网络205-d可以发起EAP过程。在一些示例中,UE 115-c可以经由RAN220-b的网络接入设备(例如,网络节点)接入蜂窝网络205-d。RAN 220-b可以与CN 550通信。CN 550内的认证器235-d可以促进EAP过程的执行。在蜂窝网络的替代配置中,认证器235-d可以是RAN 220-b的一部分或者搭配认证服务器245-b一起使用。

[0087] 在510处,蜂窝网络205-d可以向认证服务器245-b发送用于执行EAP过程的请求。在一些示例中,在510处发送的请求可以通过认证器235-d和认证服务器245-b之间的安全信道进行发送(例如,该请求可以使用Diameter协议(例如,使用Diameter封装)在认证器235-d和认证服务器245-b之间进行发送)。

[0088] 在515处,UE 115-c和认证服务器245-b可以经由认证器235-d执行EAP过程,其中,认证器235-d提供在UE 115-c和认证服务器245-b之间发送的消息的传输。EAP过程可以至少部分基于在UE 115-c和认证服务器245-b之间交换的认证凭证的集合。作为执行该EAP过程的一部分,UE115-c和认证服务器245-b中的每一个可以推导MSK和EMSK。MSK和EMSK可以至少部分基于认证凭证和参数的第一集合来推导得到。在一些示例中,参数的第一集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0089] 在505、510或515处的操作之前、期间或之后,UE 115-c和认证服务器245-b中的每一个可以确定认证器235-d与蜂窝网络(即,与蜂窝网络205-d)相关联。

[0090] 在520和525处,UE 115-c和认证服务器245-b中的每一个可以独立地推导蜂窝网络205-d的第一安全密钥。由于UE 115-c和认证服务器245-b中的每一个确定认证器235-d与蜂窝网络205-d相关联,因此,UE 115-c和认证服务器245-b中的每一个可以至少部分基于该EMSK来推导第一安全密钥。第一安全密钥还可以至少部分基于参数的第二集合来推导得到。在一些示例中,参数的第二集合可以包括蜂窝网络205-d的标识符、至少一个蜂窝网络特定参数、在UE 115-c或认证服务器245-b和蜂窝网络205-c之间交换的至少一个参数或者它们的组合。

[0091] 在530处,认证服务器245-b可以经由认证器235-d和认证服务器245-b之间的安全信道向认证器235-d发送第一安全密钥(例如,第一安全密钥可以使用Diameter协议(例如,使用Diameter封装)在认证服务器245-b和认证器235-d之间进行发送)。

[0092] 在535处,UE 115-c和蜂窝网络205-d可以执行认证过程。在540和545处,在535处成功执行了认证过程时,UE 115-c和蜂窝网络205-d可以推导蜂窝网络205-d的一个或多个网络节点的一个或多个另外的安全密钥(例如,第二安全密钥)。在一些示例中,第二安全密钥可以至少部分基于第一安全密钥和参数的第三集合。在一些示例中,参数的第三集合可以包括该网络节点的标识符、至少一个网络节点特定参数、在UE 115-c和该网络节点之间

交换的至少一个参数或者它们的组合。

[0093] 在555处,UE 115-c可以至少部分基于所推导的安全密钥与蜂窝网络205-d通信。

[0094] 图6示出根据本公开内容的各个方面的UE 115-d的框图600。UE 115-d可以是参考图1、2、4和5描述的UE 115的方面的示例。UE 115-d可以包括接收机610、无线通信管理器620和发射机630。UE 115-d还可以包括处理器。这些组件中的每一个可以相互通信。

[0095] 接收机610可以接收信号或信息,例如与各种信道(例如,控制信道、数据信道、广播信道、多播信道、单播信道等等)相关联的参考信号、控制信息或用户数据。所接收的信号和信息可以由接收机610使用(例如,用于频率/时间跟踪)或者被传递给UE 115-d的其它组件,包括无线通信管理器620。接收机610可以是参考图8描述的收发机825的方面的示例。接收机610可以包括单个天线或多个天线或与之相关联。

[0096] 无线通信管理器620可以用于管理UE 115-d的无线通信的一个或多个方面。在一些示例中,无线通信管理器620的一部分可以合并到接收机610或发射机630中或与之共享。无线通信管理器620可以包括EAP管理器635、网络类型识别器640和网络认证器645。这些组件中的每一个可以直接地或间接地相互通信(例如,通过一个或多个总线)。

[0097] 如上参考图5所描述的,EAP管理器635可以用于经由认证器与认证服务器执行EAP过程。该EAP过程可以至少部分基于在UE和认证服务器之间交换的认证凭证的集合。如上参考图5所描述的,作为执行该EAP过程的一部分,EAP管理器635还可以用于推导MSK和EMSK,所述MSK和所述EMSK至少部分基于该认证凭证和参数的第一集合。在一些示例中,参数的第一集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0098] 如上参考图5所描述的,网络类型识别器640可以用于确定与该认证器相关联的网络类型。在一些示例中,所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如,WLAN类型)。

[0099] 网络认证器645可以用于至少部分基于所确定的网络类型与该认证器执行至少一个认证过程。如上参考图5所描述的,该至少一个认证过程可以基于该MSK或EMSK与所确定的网络类型的关联。

[0100] 发射机630可以发送从UE 115-d的其它组件(包括无线通信管理器620)接收的信号或信息。所述信号或信息可以包括例如与各种信道(例如,控制信道、数据信道、广播信道、多播信道、单播信道等等)相关联的参考信号、控制信息或用户数据。在一些示例中,发射机630可以搭配接收机610在收发机中一起使用。发射机630可以是参考图8描述的收发机825的方面的示例。发射机630可以包括单个天线或多个天线或与之相关联。

[0101] 图7示出根据本公开内容的各个方面的无线通信管理器720的框图700。无线通信管理器720可以是参考图6描述的无线通信管理器620的方面的示例。

[0102] 无线通信管理器720可以包括EAP管理器635-a、网络类型识别器640-a、网络认证器645-a和蜂窝网络通信管理器715。EAP管理器635-a、网络类型识别器640-a和网络认证器645-a可以是参考图6描述的EAP管理器635、网络类型识别器640和网络认证器645的示例。网络认证器645-a可以包括网络密钥推导器705和网络节点密钥推导器710。这些组件中的每一个可以直接地或间接地相互通信(例如,经由一个或多个总线)。

[0103] 如上参考图5所描述的,EAP管理器635-a可以用于经由认证器与认证服务器执行

EAP过程。该EAP过程可以至少部分基于在UE和认证服务器之间交换的认证凭证的集合。如上参考图5所描述的，作为执行EAP过程的一部分，EAP管理器635-a还可以用于推导MSK和EMSK，所述MSK和所述EMSK至少部分基于该认证凭证和参数的第一集合。在一些示例中，参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0104] 如上参考图5所描述的，网络类型识别器640-a可以用于确定与认证器相关联的网络类型。在一些示例中，所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如，WLAN类型)。

[0105] 网络认证器645-a至少部分基于所确定的网络类型与该认证器执行至少一个认证过程。该至少一个认证过程可以基于该MSK或EMSK与所确定的网络类型的关联。

[0106] 如上参考图5所描述的，当所确定的网络类型包括蜂窝网络类型时，网络密钥推导器705可以用于推导蜂窝网络的第一安全密钥。第一安全密钥可以至少部分基于该EMSK和参数的第二集合。在一些示例中，参数的第二集合可以包括该蜂窝网络的标识符、至少一个蜂窝网络特定参数、在该UE和蜂窝网络之间交换的至少一个参数或者它们的组合。当所确定的网络类型包括非蜂窝网络类型时，网络密钥推导器705可以用于推导非蜂窝网络的第一安全密钥。

[0107] 如上参考图5所描述的，当所确定的网络类型包括蜂窝网络类型时，网络节点密钥推导器710可以用于推导该蜂窝网络的网络节点的第二安全密钥。第二安全密钥可以至少部分基于第一安全密钥和参数的第三集合。在一些示例中，参数的第三集合可以包括该网络节点的标识符、至少一个网络节点特定参数、在UE和网络节点之间交换的至少一个参数或者它们的组合。

[0108] 如上参考图5所描述的，蜂窝网络通信管理器715可以用于至少部分基于第二安全密钥经由该网络节点与该蜂窝网络通信。

[0109] 图8示出根据本公开内容的各个方面的无线通信系统800的示意图。无线通信系统800可以包括UE 115-e，其可以是参考图1、2和4-6描述的UE 115的方面的示例。

[0110] UE 115-e可以包括无线通信管理器805、存储器810、处理器820、收发机825和天线830。这些组件中的每一个可以直接地或间接地相互通信(例如，经由一个或多个总线)。无线通信管理器805可以是参考图6和7描述的无线通信管理器620和720的方面的示例。

[0111] 存储器810可以包括随机存取存储器(RAM)或只读存储器(ROM)。存储器810可以存储计算机可读、计算机可执行软件815，其包括指令，所述指令在被执行时使处理器820执行本申请中描述的各种功能，包括与网络安全性和认证有关的功能。在一些情况下，软件815可以不由处理器820直接执行，但是可以使处理器820(例如，在被编译和执行时)执行本申请中描述的功能。处理器820可以包括智能硬件设备(例如，中央处理单元(CPU)、微控制器、专用集成电路(ASIC)等等)。

[0112] 如本申请中所描述的，收发机825可以经由一个或多个天线或有线链路与一个或多个网络双向通信。例如，收发机825可以与蜂窝网络205-e(或其一个或多个节点)或另一个UE 115-f双向通信。收发机825可以包括调制解调器，其用于调制分组并将经调制分组提供给天线用于传输，以及解调从天线接收的分组。在一些情况下，UE 115-e可以包括单个天线830。然而，在一些情况下，UE 115-e可以具有一个以上的天线830，它们可以能够同时发

送或接收多个无线传输。

[0113] 图9示出根据本公开内容的各个方面的认证服务器245-c的框图900。认证服务器245-c可以是参考图2、4和5描述的认证服务器245的方面的示例。认证服务器245-c可以包括接收机910、认证管理器920和发射机930。认证服务器245-c还可以包括处理器。这些组件中的每一个可以相互通信。

[0114] 接收机910可以从各个网络节点(包括蜂窝网络、WLAN等等的节点)接收认证请求。接收机910还可以经由网络节点从UE接收认证信息。所接收的认证请求和认证信息可以被传递给认证管理器920。接收机910可以是参考图10描述的认证接口1025的方面的示例。接收机910可以包括一个或多个有线和/或无线接口。

[0115] 认证管理器920可以用于管理认证服务器245-c的设备认证的一个或多个方面。在一些示例中,认证管理器920的一部分可以合并到接收机910或发射机930中或者与之共享。认证管理器920可以包括EAP管理器935、网络类型识别器940、网络密钥推导器945和网络密钥安装器950。这些组件中的每一个可以直接地或间接地相互通信(例如,经由一个或多个总线)。

[0116] 如上参考图5所描述的,EAP管理器935可以用于经由认证器与UE执行EAP过程。EAP过程可以至少部分基于在认证服务器和UE之间交换的认证凭证的集合。如上参考图5所描述的,作为执行EAP过程的一部分,EAP管理器935还可以用于推导MSK和EMSK,所述MSK和所述EMSK至少部分基于认证凭证和参数的第一集合。在一些示例中,参数的第一集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。

[0117] 如上参考图5所描述的,网络类型识别器940可以用于确定与认证器相关联的网络类型。在一些示例中,所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如,WLAN类型)。

[0118] 如上参考图5所描述的,网络密钥推导器945可以用于至少部分基于MSK或EMSK与该网络类型的关联,并且至少部分基于参数的第二集合,推导所确定的网络类型的安全密钥。当所确定的网络类型包括蜂窝网络类型时,并且在一些示例中,参数的第二集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在认证服务器和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中,蜂窝网络可以包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0119] 如上参考图5所描述的,网络密钥安装器950可以用于经由安全信道向认证器发送安全密钥。

[0120] 发射机930可以发送从认证服务器245-c的其它组件(包括认证管理器920)接收的认证反馈消息和安全密钥。发射机930可以是参考图10描述的认证接口1025的方面的示例。发射机930可以包括一个或多个有线和/或无线接口。

[0121] 图10示出根据本公开内容的各个方面的认证服务器245-d的框图1000。认证服务器245-d可以是参考图2、4、5和9描述的认证服务器245的方面的示例。

[0122] 认证服务器245-d可以包括认证管理器1005、存储器1010、处理器1020和认证接口1025。这些组件中的每一个可以直接地或间接地相互通信(例如,经由一个或多个总线)。认证管理器1005可以是参考图9描述的认证管理器920的方面的示例。

[0123] 存储器1010可以包括RAM或ROM。存储器1010可以存储计算机可读、计算机可执行软件1015，其包括指令，所述指令在被执行时使处理器1020执行本申请中描述的各种功能，包括与网络安全性和认证有关的功能。在一些情况下，软件1015可以不由处理器1020直接执行，但是可以使处理器1020(例如，在被编译和执行时)执行本申请中描述的功能。处理器1020可以包括智能硬件设备(例如，CPU、微控制器、ASIC等等)。

[0124] 如本申请中所描述的，认证接口1025可以经由一个或多个天线或有线链路与一个或多个网络、网络节点或UE双向通信。在一些示例中，认证接口1025可以用于与网络节点建立安全连接(例如，使用Radius或Diameter协议)并且经由该安全连接和网络节点与UE双向通信。

[0125] 图11示出根据本公开内容的各个方面的网络节点1105的框图1100。网络节点1105可以是参考图2、4和5描述的网络节点的方面的示例，并且在一些示例中，可以是参考图2、4和5描述的认证器235的示例。网络节点1105可以包括接收机1110、通信管理器1120和发射机1130。网络节点1105还可以包括处理器。这些组件中的每一个可以相互通信。

[0126] 接收机1110可以从其它网络节点、从UE、从认证服务器等接收信号或信息。所接收的信号和信息可以被传递给网络节点1105的其它组件，包括通信管理器1120。接收机1110可以是参考图13描述的认证接口1325的方面的示例。接收机1110可以包括一个或多个有线和/或无线接口。

[0127] 通信管理器1120可以用于管理网络节点1105的无线通信的一个或多个方面。在一些示例中，通信管理器1120的一部分可以合并到接收机1110或发射机1130中或者与之共享。通信管理器1120可以包括网络密钥管理器1135和UE认证器1140。这些组件中的每一个可以直接地或间接地相互通信(例如，经由一个或多个总线)。

[0128] 如上参考图5所描述的，网络密钥管理器1135可以用于从认证服务器接收第一安全密钥，所述第一安全密钥至少部分基于EMSK和参数的第一集合。EMSK可以至少部分基于认证凭证的集合和参数的第二集合。认证凭证可以在EAP过程期间在UE和认证服务器之间交换。在一些示例中，参数的第一集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在UE和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中，参数的第二集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在一些示例中，蜂窝网络可以包括以下各项中的至少一项：5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0129] 如上参考图5所描述的，UE认证器1140可以用于至少部分基于第一安全密钥与UE执行至少一个认证过程。

[0130] 发射机1130可以发送从网络节点1105的其它组件(包括通信管理器1120)接收的信号或信息。发射机1130可以是参考图13描述的认证接口1325的方面的示例。接收机1110可以包括一个或多个有线和/或无线接口。

[0131] 图12示出根据本公开内容的各个方面的通信管理器1220的框图1200。该通信管理器1220可以是参考图11描述的通信管理器1120的方面的示例。

[0132] 通信管理器1220可以包括网络密钥管理器1135-a、UE认证器1140-a和UE通信管理器1210。网络密钥管理器1135-a和UE认证器1140-a可以是参考图11描述的网络密钥管理器1135和UE认证器1140的示例。UE认证器1140-a可以包括网络节点密钥推导器1205。这些组

件中的每一个可以直接地或间接地相互通信(例如,经由一个或多个总线)。

[0133] 如上参考图5所描述的,网络密钥管理器1135-a可以用于从认证服务器接收第一安全密钥,所述第一安全密钥至少部分基于EMSK和参数的第一集合。EMSK可以至少部分基于认证凭证的集合和参数的第二集合。可以在EAP过程期间在UE和认证服务器之间交换认证凭证。在一些示例中,参数的第一集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在UE和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中,参数的第二集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在一些示例中,蜂窝网络可以包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0134] 如上参考图5所描述的,UE认证器140-a可以用于至少部分基于第一安全密钥与UE执行至少一个认证过程。网络节点密钥推导器1205可以用于与UE执行至少一个认证过程,可以包括推导蜂窝网络的网络节点的第二安全密钥。第二安全密钥可以至少部分基于第一安全密钥和参数的第三集合。在一些示例中,参数的第三集合可以包括网络节点的标识符、至少一个网络节点特定参数、在UE和网络节点之间交换的至少一个参数或者它们的组合。

[0135] 如上参考图5所描述的,UE通信管理器1210可以用于至少部分基于第二安全密钥经由网络节点与UE通信。

[0136] 图13示出根据本公开内容的各个方面的网络节点1105-a的示意图1300。网络节点1105-a可以是参考图2、4、5和11描述的网络节点的方面的示例。

[0137] 网络节点1105-a可以包括通信管理器1305、存储器1310、处理器1320和认证接口1325。这些组件中的每一个可以直接地或间接地相互通信(例如,经由一个或多个总线)。通信管理器1305可以是参考图11或12描述的通信管理器的方面的示例。

[0138] 存储器1310可以包括RAM或ROM。存储器1310可以存储计算机可读、计算机可执行软件1315,其包括指令,所述指令在被执行时使处理器1320执行本申请中描述的各种功能,包括与网络安全性和认证有关的功能。在一些情况下,软件1315可以不直接由处理器1320执行,但是可以使处理器1320(例如,在被编译和执行时)执行本申请中描述的功能。处理器1320可以包括智能硬件设备(例如,CPU、微控制器、ASIC等等)。

[0139] 如本申请中所描述的,认证接口1325可以经由一个或多个天线或有线链路与一个或多个网络、网络节点或UE双向通信。在一些示例中,认证接口1325可以用于与认证服务器建立安全连接(例如,使用Radius或Diameter协议)并且促进由UE和认证服务器执行的EAP过程。

[0140] 图14示出根据本公开内容的各个方面的用于无线通信的方法1400的流程图。如参考图1-8所描述的,方法1400的操作可以由UE 115或其组件执行。在一些示例中,方法1400的操作可以由参考图6-8描述的无线通信管理器执行。在一些示例中,UE可以执行用于控制该UE的功能元件执行下面描述的功能的代码集。另外地或者作为替代,UE可以使用专用硬件来执行下面描述的功能的方面。

[0141] 在框1405处,如上参考图5所描述的,UE可以经由认证器与认证服务器执行EAP过程。该EAP过程可以至少部分基于在UE和认证服务器之间交换的认证凭证的集合。在某些示例中,可以使用参考图6和7描述的EAP管理器635来执行框1405的操作。

[0142] 在框1410处,如上参考图5所描述的,作为执行EAP过程的一部分,UE可以推导MSK

和EMSK，所述MSK和所述EMSK至少部分基于认证凭证和参数的第一集合。在一些示例中，参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在某些示例中，可以使用参考图6和7描述的EAP管理器635来执行框1410的操作。

[0143] 在框1415处，如上参考图5所描述的，UE可以确定与认证器相关联的网络类型。在一些示例中，所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如，WLAN类型)。在某些示例中，可以使用参考图6和7描述的网络类型识别器640来执行框1415的操作。

[0144] 在框1420处，UE可以至少部分基于所确定的网络类型与认证器执行至少一个认证过程。如上参考图5所描述的，该至少一个认证过程可以至少部分基于MSK或EMSK与所确定的网络类型的关联。在某些示例中，可以使用参考图6和7描述的网络认证器645来执行框1420的操作。

[0145] 图15示出根据本公开内容的各个方面的用于无线通信的方法1500的流程图。如参考图1-8所描述的，方法1500的操作可以由UE 115或其组件执行。在一些示例中，方法1500的操作可以由参考图6-8描述的无线通信管理器执行。在一些示例中，UE可以执行用于控制该UE的功能元件执行下面描述的功能的代码集。另外地或者作为替代，UE可以使用专用硬件来执行下面描述的功能的方面。

[0146] 在框1505处，如上参考图5所描述的，UE可以经由认证器与认证服务器执行EAP过程。该EAP过程可以至少部分基于在UE和认证服务器之间交换的认证凭证的集合。在某些示例中，可以使用参考图6和7描述的EAP管理器635执行框1505的操作。

[0147] 在框1510处，如上参考图5所描述的，作为执行EAP过程的一部分，UE可以推导MSK和EMSK，所述MSK和所述EMSK至少部分基于认证凭证和参数的第一集合。在一些示例中，参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在某些示例中，可以使用参考图6和7描述的EAP管理器635执行框1510的操作。

[0148] 在框1515处，如上参考图5所描述的，UE可以确定与认证器相关联的网络类型。在一些示例中，所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如，WLAN类型)。在某些示例中，可以使用参考图6和7描述的网络类型识别器640执行框1515的操作。

[0149] 在框1520处，方法1500可以分支到框1525或1540，这取决于所确定的网络类型包括蜂窝网络类型还是非蜂窝网络类型。当所确定的网络类型包括蜂窝网络类型时，方法1500可以分支到框1525。当所确定的网络类型包括非蜂窝网络类型时，方法1500可以分支到框1540。在某些示例中，可以使用参考图6和7描述的网络类型识别器640来执行框1520的操作。在一些示例中，蜂窝网络可以包括以下各项中的至少一项：5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。

[0150] 如果UE确定网络类型包括蜂窝网络类型，则在框1525和1530处，UE可以至少部分基于所确定的网络类型与认证器执行至少一个认证过程。该至少一个认证过程可以基于MSK或EMSK与所确定的网络类型的关联。在框1525处，如上参考图5所描述的，UE可以推导蜂窝网络的第一安全密钥。第一安全密钥可以至少部分基于EMSK和参数的第二集合。在一些示例中，参数的第二集合可以包括该蜂窝网络的标识符、至少一个蜂窝网络特定参数、在UE和蜂窝网络之间交换的至少一个参数或者它们的组合。在某些示例中，可以使用参考图6和

7描述的网络认证器645，或参考图7所描述的网络密钥推导器705来执行框1525的操作。

[0151] 在框1530处，如上参考图5所描述的，UE可以推导蜂窝网络的网络节点的第二安全密钥。第二安全密钥可以至少部分基于第一安全密钥和参数的第三集合。在一些示例中，参数的第三集合可以包括网络节点的标识符、至少一个网络节点特定参数、在UE和网络节点之间交换的至少一个参数或者它们的组合。在某些示例中，可以使用参考图6和7描述的网络认证器645，或参考图7所描述的网络节点密钥推导器710来执行框1530的操作。

[0152] 在框1535处，如上参考图5所描述的，UE可以至少部分基于第二安全密钥，经由网络节点与蜂窝网络通信。在某些示例中，可以使用参考图7描述的蜂窝网络通信管理器715来执行框1530的操作。

[0153] 如果UE确定网络类型包括非蜂窝网络，则在框1540处，UE可以推导非蜂窝网络的第一安全密钥。第一安全密钥可以至少部分基于MSK和参数的第四集合。在某些示例中，可以使用参考图6和7描述的网络认证器645，或参考图7所描述的网络密钥推导器705来执行框1540的操作。

[0154] 图16示出根据本公开内容的各个方面的用于无线通信的方法1600的流程图。如参考图1-5、9和10所描述的，方法1600的操作可以由认证服务器或其组件执行。在一些示例中，方法1600的操作可以由参考图9和10描述的认证管理器执行。在一些示例中，认证服务器可以执行用于控制该认证服务器的功能元件执行下面描述的功能的代码集。另外地或者作为替代，认证服务器可以使用专用硬件执行下面描述的功能的方面。

[0155] 在框1605处，如上参考图5所描述的，认证服务器可以经由认证器与UE执行EAP过程。该EAP过程可以至少部分基于在认证服务器和UE之间交换的认证凭证的集合。在某些示例中，可以使用参考图9描述的EAP管理器935来执行框1605的操作。

[0156] 在框1610处，如上参考图5所描述的，作为执行EAP过程的一部分，认证服务器可以推导MSK和EMSK，所述MSK和所述EMSK至少部分基于认证凭证和参数的第一集合。在一些示例中，参数的第一集合可以包括：至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在某些示例中，可以使用参考图9描述的EAP管理器935来执行框1610的操作。

[0157] 在框1615处，如上参考图5所描述的，认证服务器可以确定与认证器相关联的网络类型。在一些示例中，所确定的网络类型可以包括蜂窝网络类型或非蜂窝网络类型(例如，WLAN类型)。在某些示例中，可以使用参考图9描述的网络类型识别器940来执行框1615的操作。

[0158] 在框1620处，如上参考图5所描述的，认证服务器可以至少部分基于MSK或EMSK与网络类型的关联，并且至少部分基于参数的第二集合，推导所确定的网络类型的安全密钥。当所确定的网络类型包括蜂窝网络类型时，并且在一些示例中，参数的第二集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在认证服务器和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中，蜂窝网络可以包括以下各项中的至少一项：5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。在某些示例中，可以使用参考图9描述的网络密钥推导器945来执行框1620的操作。

[0159] 在框1625处，如上参考图5所描述的，认证服务器可以经由安全信道向认证器发送安全密钥。在某些示例中，可以使用参考图9描述的网络密钥安装器950来执行框1625的操

作。

[0160] 图17示出根据本公开内容的各个方面的用于无线通信的方法1700的流程图。如参考图1-5和11-13所描述的,可以由蜂窝网络或其组件执行方法1700的操作。在一些示例中,可以由参考图11-13描述的通信管理器执行方法1700的操作。在一些示例中,蜂窝网络(或其一个或多个节点)可以执行用于控制该蜂窝网络的功能元件执行下面描述的功能的代码集。另外地或者作为替代,蜂窝网络(或其一个或多个节点)可以使用专用硬件执行下面描述的功能的方面。

[0161] 在框1705处,如上参考图5所描述的,蜂窝网络可以从认证服务器接收第一安全密钥,所述第一安全密钥至少部分基于EMSK和参数的第一集合。该EMSK可以至少部分基于认证凭证的集合和参数的第二集合。该认证凭证可以在EAP过程期间在UE和认证服务器之间交换。在一些示例中,参数的第一集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在UE和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中,参数的第二集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在一些示例中,蜂窝网络可以包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。在某些示例中,可以使用参考图11描述的网络密钥管理器1135来执行框1705的操作。

[0162] 在框1710处,如上参考图5所描述的,蜂窝网络可以至少部分基于第一安全密钥与UE执行至少一个认证过程。在某些示例中,可以使用参考图11描述的UE认证器140来执行框1710的操作。

[0163] 图18示出根据本公开内容的各个方面的用于无线通信的方法1800的流程图。如参考图1-5和11-13所描述的,可以由蜂窝网络或其组件执行方法1800的操作。在一些示例中,可以由参考图11-13描述的通信管理器执行方法1800的操作。在一些示例中,蜂窝网络(或其一个或多个节点)可以执行用于控制该蜂窝网络的功能元件执行下面描述的功能的代码集。另外地或者作为替代,蜂窝网络(或其一个或多个节点)可以使用专用硬件执行下面描述的功能的方面。

[0164] 在框1805处,如上参考图5所描述的,蜂窝网络可以从认证服务器接收第一安全密钥,所述第一安全密钥至少部分基于EMSK和参数的第一集合。该EMSK可以至少部分基于认证凭证的集合和参数的第二集合。该认证凭证可以在EAP过程期间在UE和认证服务器之间交换。在一些示例中,参数的第一集合可以包括蜂窝网络的标识符、至少一个蜂窝网络特定参数、在UE和蜂窝网络之间交换的至少一个参数或者它们的组合。在一些示例中,参数的第二集合可以包括:至少一个标识符、至少一个随机数、至少一个网络参数、至少一个UE参数或者它们的组合。在一些示例中,蜂窝网络可以包括以下各项中的至少一项:5G网络、4G网络、LTE网络、LTE-A网络、3G网络或者它们的组合。在某些示例中,可以使用参考图11描述的网络密钥管理器1135来执行框1805的操作。

[0165] 在框1810处,蜂窝网络可以至少部分基于第一安全密钥与UE执行至少一个认证过程。如上参考图5所描述的,与UE执行至少一个认证过程可以包括推导蜂窝网络的网络节点的第二安全密钥。第二安全密钥可以至少部分基于第一安全密钥和参数的第三集合。在一些示例中,参数的第三集合可以包括网络节点的标识符、至少一个网络节点特定参数、在UE和网络节点之间交换的至少一个参数或者它们的组合。在某些示例中,可以使用参考图11

描述的UE认证器140，或参考图12描述的网络节点密钥推导器1205来执行框1810的操作。

[0166] 在框1815处，如上参考图5所描述的，蜂窝网络可以至少部分基于第二安全密钥，经由网络节点与UE通信。在某些示例中，可以使用参考图12描述的UE通信管理器1210来执行框1815的操作。

[0167] 应当注意的是，上面描述的方法说明了本公开内容中描述的技术的可能实施方式。在一些示例中，方法的操作可以用不同顺序执行或者包括不同操作。

[0168] 本申请描述的技术可以用于各种无线通信系统，例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其它系统。术语“系统”和“网络”通常互换使用。CDMA系统可以实现诸如CDMA 2000、通用陆地无线接入(UTRA)等的无线技术。CDMA 2000涵盖IS-2000、IS-95和IS-856标准。IS-2000版本0和A可以被称为CDMA 2000 1X、1X等等。IS-856(TIA-856)可以被称为CDMA 2000 1xEV-DO、高速分组数据(HRPD)等。UTRA包括宽带CDMA(W-CDMA)和CDMA的其它变型。TDMA系统可以实现诸如全球移动通信系统(GSM)之类的无线技术。OFDMA系统可以实现例如超移动宽带(UMB)、演进型UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、闪速OFDM™等的无线技术。UTRA和E-UTRA是通用移动电信系统(UMTS)的一部分。3GPP LTE和LTE-A是使用E-UTRA的UMTS的新版本。在来自名为3GPP的组织的文档中描述了UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM。在来自名为“第3代合作伙伴项目2”(3GPP2)的组织的文档中描述了CDMA 2000和UMB。本申请中描述的技术可以用于上面提及的系统和无线技术以及其它系统和无线技术，包括非授权带宽或共享带宽上的蜂窝(例如，LTE)通信。然而，上面的描述以举例为目的描述了LTE/LTE-A系统，并且在上面大部分描述中使用了LTE术语，但是这些技术可应用于LTE/LTE-A应用以外。

[0169] 上面结合附图阐述的详细描述描述了示例，但是不表示可以被实现或在权利要求的范围内的所有例子。术语“示例性”在本说明书中使用时意指“用作示例、实例或说明”，而不是“优选的”或“比其它例子更具优势的”。出于提供对所描述技术的理解的目的，详细描述包括具体细节。然而，在没有这些具体细节的情况下，也可以实践这些技术。在一些实例中，公知的结构和装置以框图的形式示出，以便于避免使得所描述的示例的构思不清楚。

[0170] 信息和信号可以使用各种不同的技术和方法中的任意一种来表示。例如，在贯穿上面的描述中可能提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或粒子、光场或粒子或其任意组合来表示。

[0171] 利用被设计为执行本申请所描述的功能的通用处理器、数字信号处理器(DSP)、ASIC、FPGA或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件或者其任意组合可以实现或执行结合本申请公开内容所描述的各种说明性框和组件。通用处理器可以是微处理器，或者，该处理器可以是任何传统的处理器、控制器、微控制器或者状态机。处理器还可以被实现为计算设备的组合，例如，DSP和微处理器的组合、多个微处理器、结合DSP内核一个或多个微处理器或者任何其它这样的结构。

[0172] 本申请描述的功能可以用硬件、由处理器执行的软件、固件或其任意组合来实现。如果用由处理器执行的软件实现，则可以将这些功能作为一个或多个指令或代码存储在计算机可读介质上或者通过计算机可读介质来发送。其它示例和实施方式在本公开内容和所附权利要求的范围和精神内。例如，由于软件的本质，上面描述的功能可以使用由处理器执行的软件、硬件、固件、硬接线或其任意组合来实现。实现功能的组件还可以物理地位于各

种位置处，包括为分布式的，从而在不同的物理位置处实现部分功能。另外，如本申请所使用的，包括在权利要求书中，术语“或者”当用于两个或更多个项目的列表中时，意指其自身可以采用所列项目中的任何一个，或者可以采用所列项目的两个或更多个项目的任意组合。例如，如果组合被描述为包含分量A、B和/或C，则该组合可以只包含A；只包含B；只包含C；联合包含A和B；联合包含A和C；联合包含B和C或者联合包含A、B和C。另外，如本申请所使用的，包括在权利要求书中，项目列表(例如，以诸如“……中的至少一个”或“……中的一个或多个”之类的措词描述的项目列表)中所使用的“或者”指示分离的列表，从而例如“A、B或C中的至少一个”的列表指A或B或C或AB或AC或BC或ABC(即，A和B和C)。

[0173] 计算机可读介质包括计算机存储介质和通信介质二者，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。存储介质可以是通用计算机或专用计算机能够存取的任何可用介质。通过举例而非限制的方式，计算机可读介质可以包括RAM、ROM、EEPROM、闪存、CD-ROM或其它光盘存储设备、磁盘存储设备或其它磁存储设备、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单元并能够由通用计算机或专用计算机或通用处理器或专用处理器存取的任何其它介质。另外，可以将任何连接适当地称作计算机可读介质。例如，如果软件是使用同轴电缆、光纤光缆、双绞线、数字订户线(DSL)或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或其它远程源发送的，则所述同轴电缆、光纤光缆、双绞线、DSL或者诸如红外线、无线电和微波之类的无线技术包括在介质的定义中。如本申请所使用的，磁盘和光盘包括压缩光盘(CD)、激光光盘、光盘、数字多功能光盘(DVD)、软盘和蓝光光盘，其中，磁盘通常磁性地复制数据，而光盘则用激光来光学地复制数据。上面的组合也应当被包括在计算机可读介质的范围之内。

[0174] 提供前面对公开内容的描述以使本领域技术人员能够实施或使用本公开内容。对本领域技术人员而言，对本公开内容的各种修改将是显而易见的，并且可以将本申请所定义的一般性原理应用于其它变型而不脱离本公开内容的精神或范围。因此，本公开内容并不旨在要受限于本申请描述的示例和设计，而是要符合与本申请所公开的原理和新颖性特征相一致的最广泛的范围。

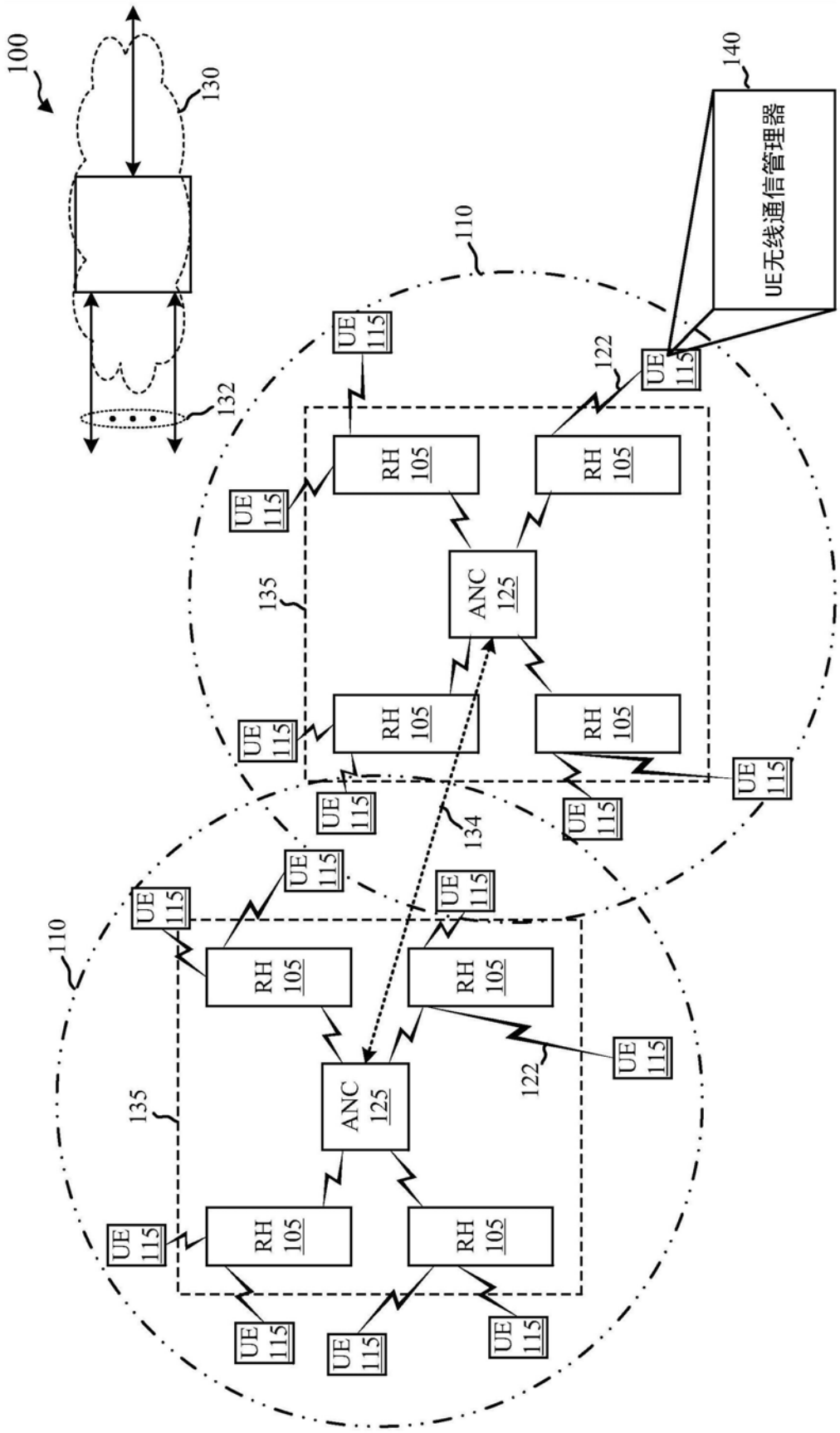

100
130
132
140
UE无线通信管理器
110
UE 115
122
RH 105
ANC 125
135
134
110
UE 115
122
RH 105
ANC 125
135

图1

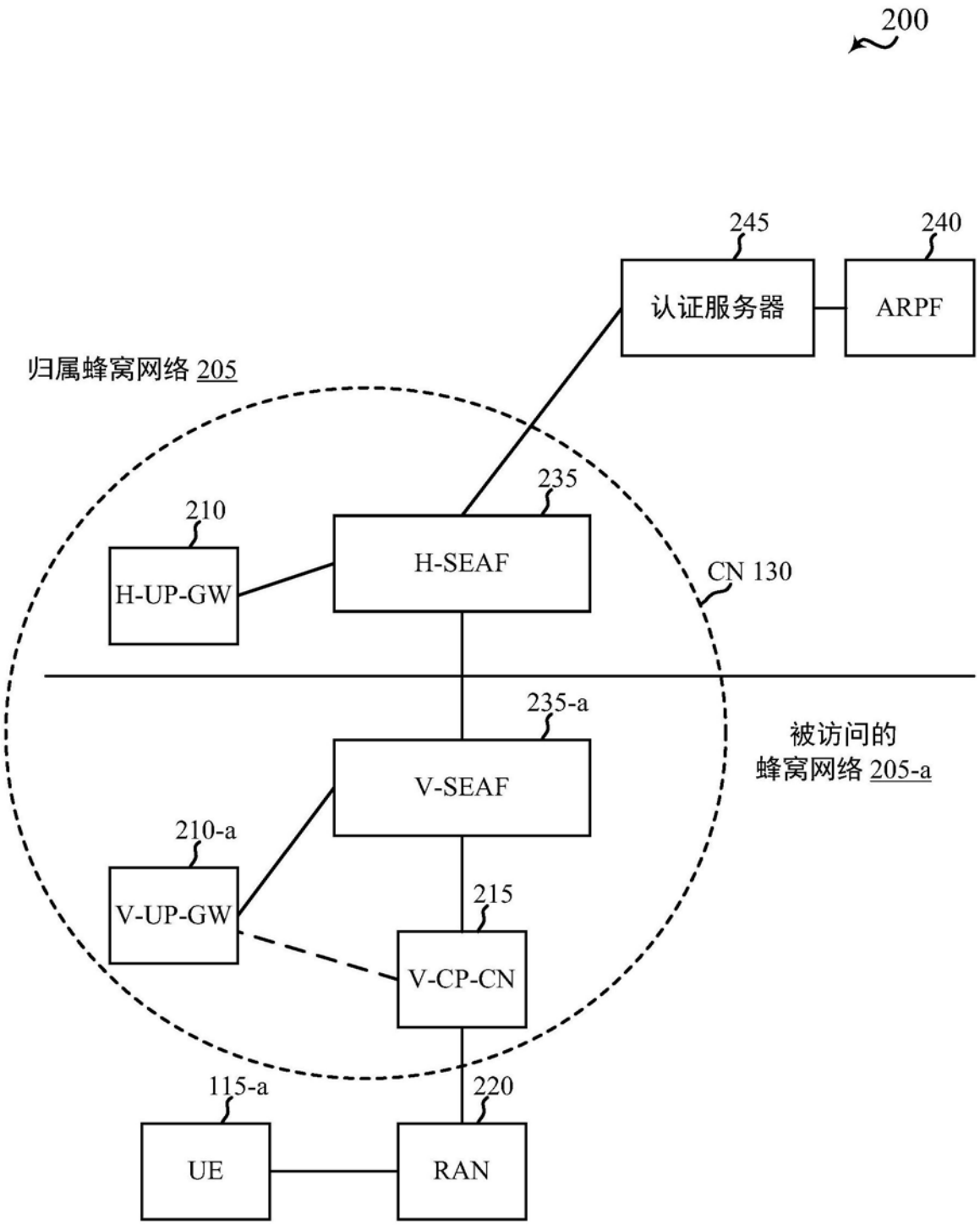

200
245
240
认证服务器
ARPF
归属蜂窝网络 205
235
210
H-SEAF
H-UP-GW
CN 130
235-a
被访问的
蜂窝网络 205-a
V-SEAF
210-a
V-UP-GW
215
V-CP-CN
115-a
220
UE
RAN

图2

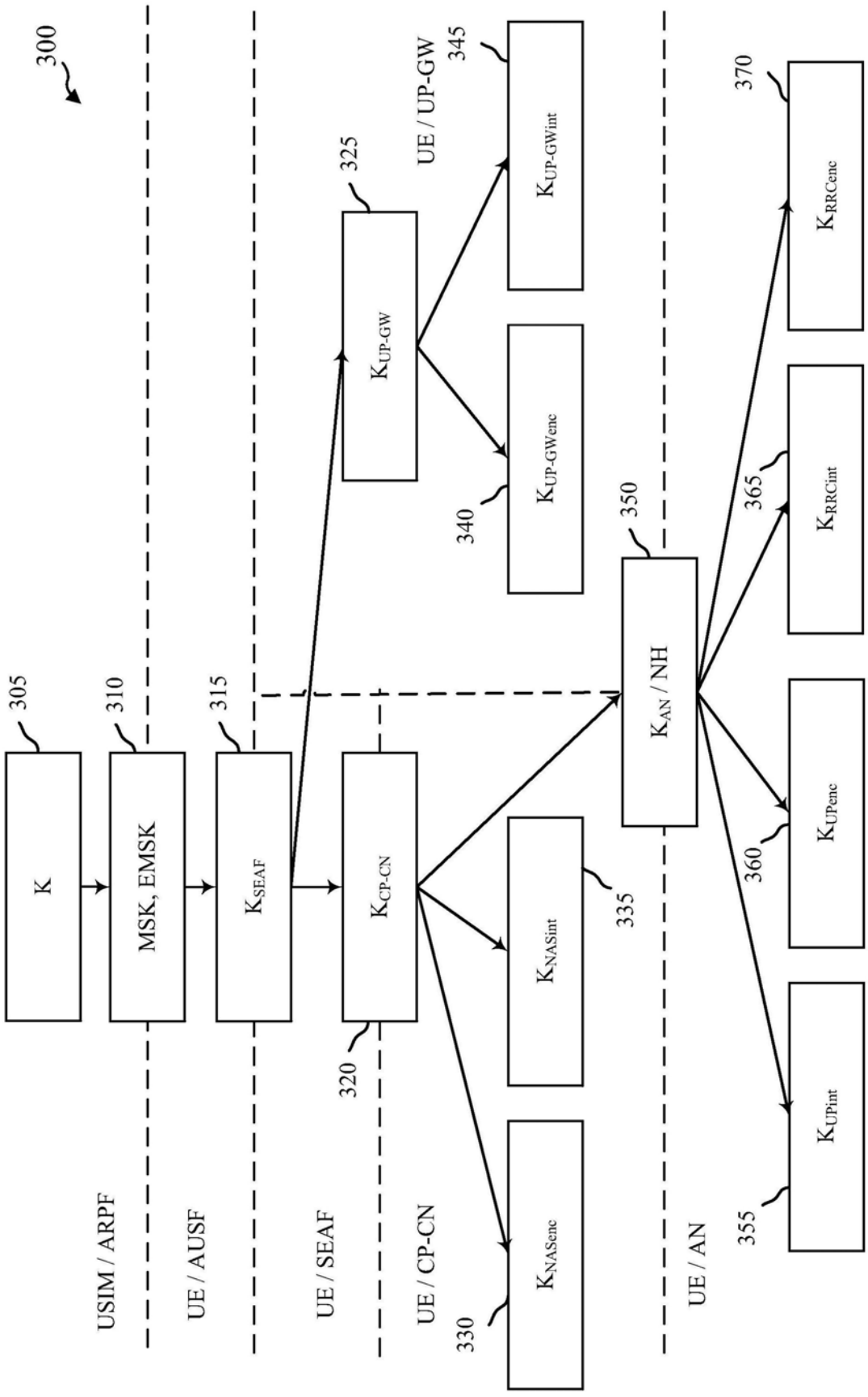

300
305
K
310
MSK, EMSK
315
K_{SEAF}
320
K_{CP-CN}
325
K_{UP-GW}
330
K_{NASenc}
335
K_{NASint}
340
$K_{UP-GWenc}$
345
$K_{UP-GWint}$
350
K_{AN} / NH
355
K_{UPint}
360
K_{UPenc}
365
K_{RRCint}
370
K_{RRCenc}
USIM / ARPF
UE / AUSF
UE / SEAF
UE / CP-CN
UE / UP-GW
UE / AN

图3

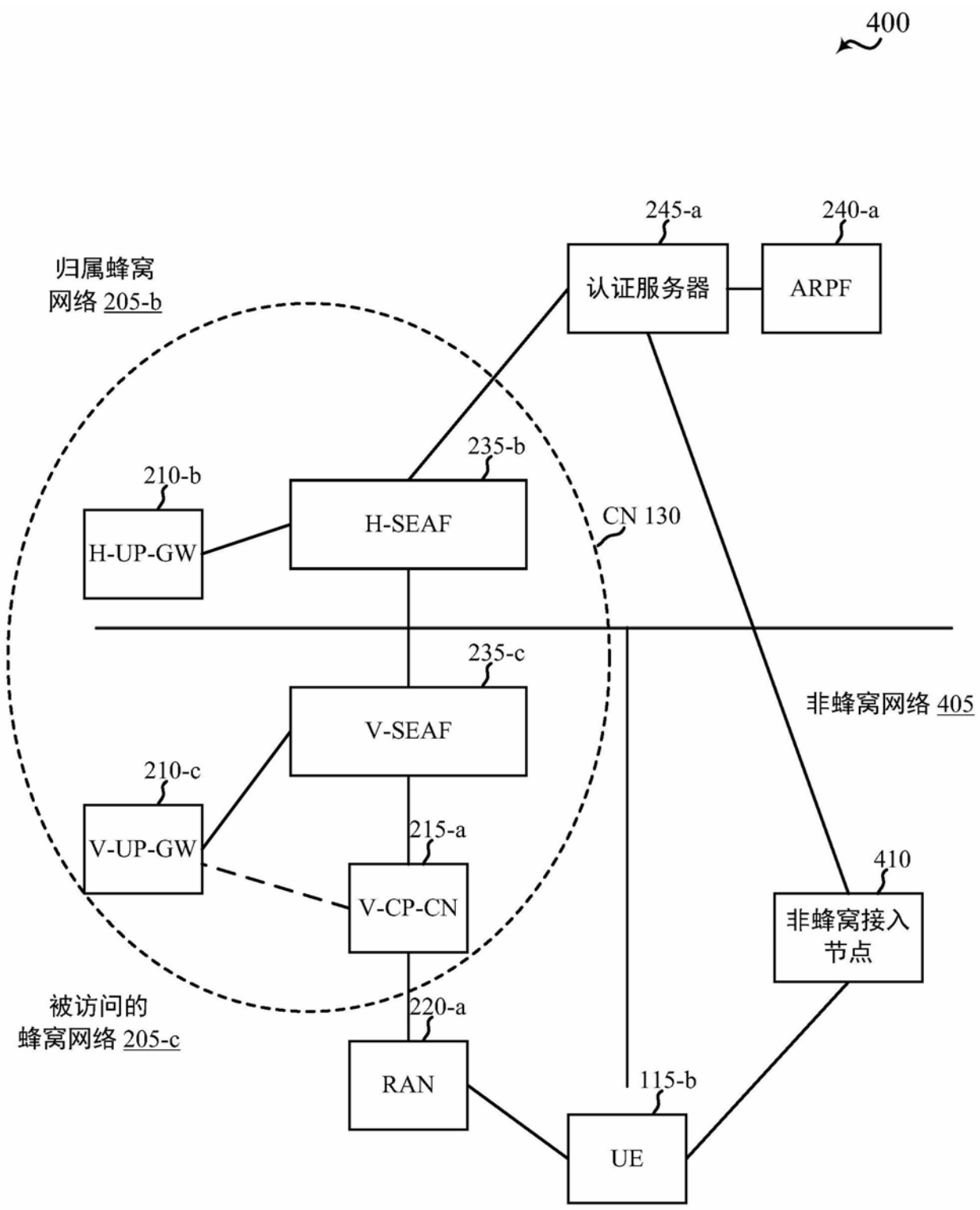

400
245-a
240-a
认证服务器
ARPF
归属蜂窝
网络 205-b
235-b
210-b
H-SEAF
H-UP-GW
CN 130
235-c
非蜂窝网络 405
V-SEAF
210-c
V-UP-GW
215-a
410
V-CP-CN
非蜂窝接入
节点
被访问的
蜂窝网络 205-c
220-a
RAN
115-b
UE

图4

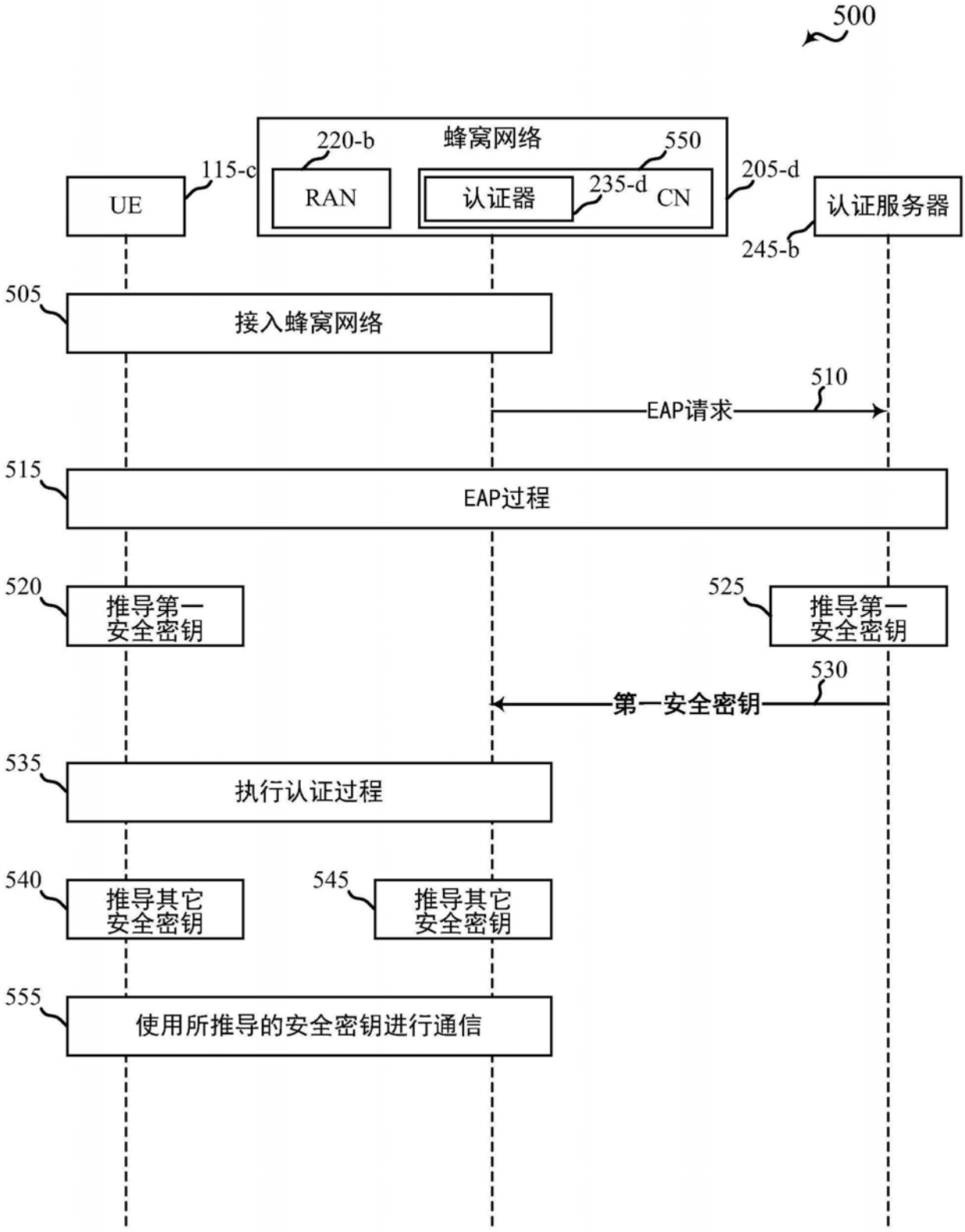

500
蜂窝网络
220-b
550
115-c
205-d
UE
RAN
认证器
235-d
CN
认证服务器
245-b
505
接入蜂窝网络
510
EAP请求
515
EAP过程
520
推导第一安全密钥
525
推导第一安全密钥
530
第一安全密钥
535
执行认证过程
540
推导其它安全密钥
545
推导其它安全密钥
555
使用所推导的安全密钥进行通信

图5

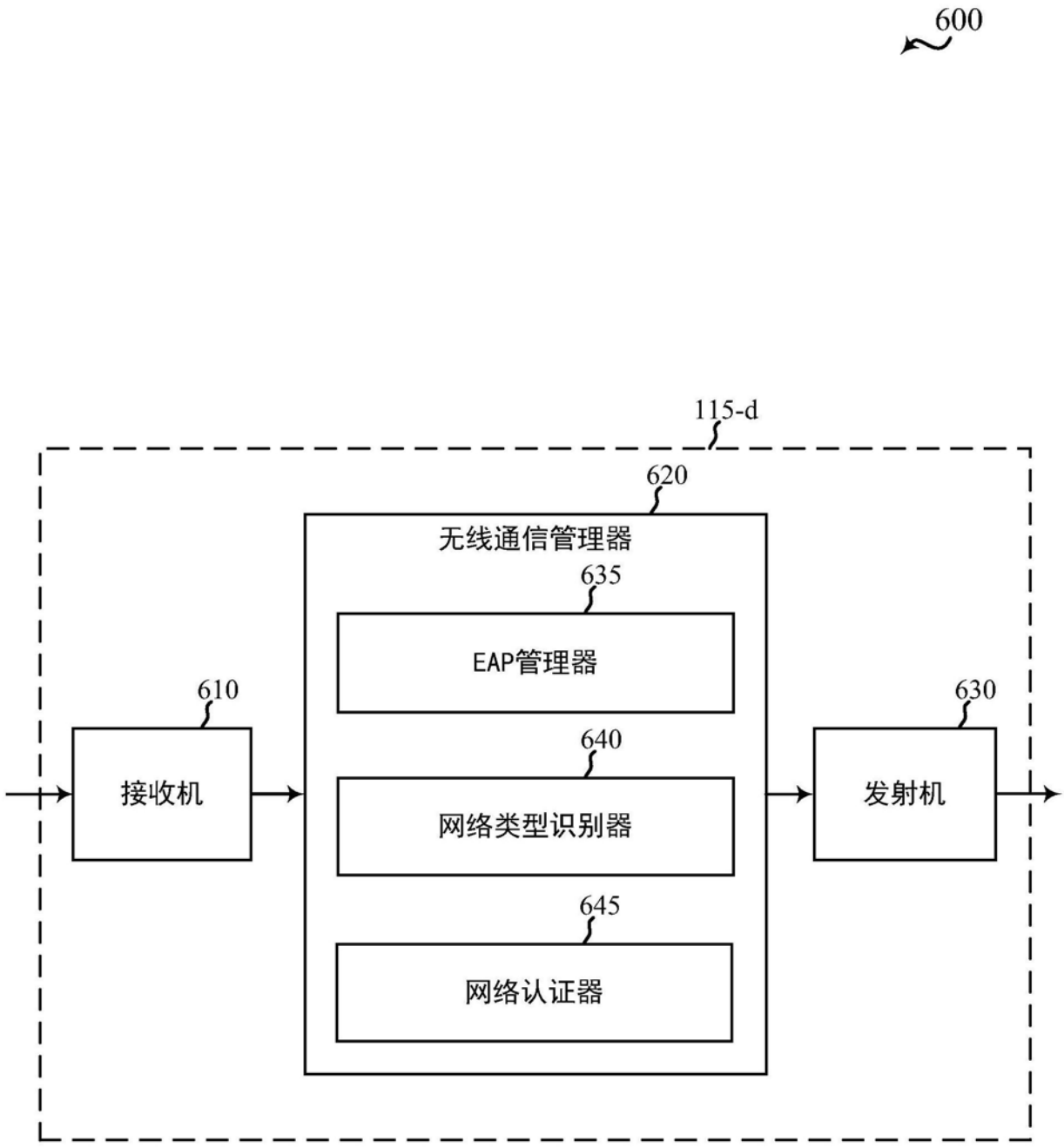

600
115-d
620
无线通信管理器
635
EAP管理器
610
接收机
640
网络类型识别器
630
发射机
645
网络认证器

图6

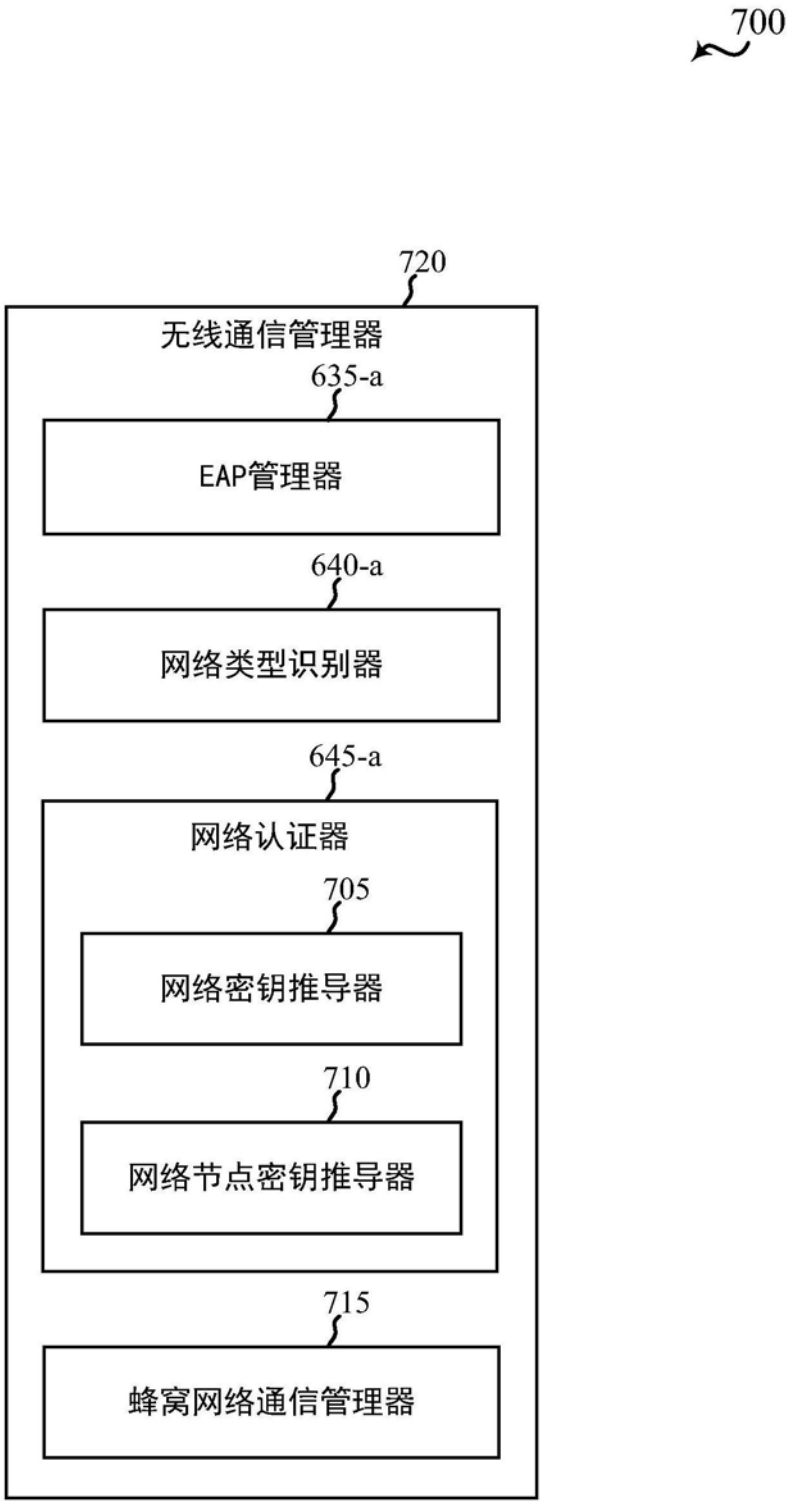

700
720
无线通信管理器
635-a
EAP管理器
640-a
网络类型识别器
645-a
网络认证器
705
网络密钥推导器
710
网络节点密钥推导器
715
蜂窝网络通信管理器

图7

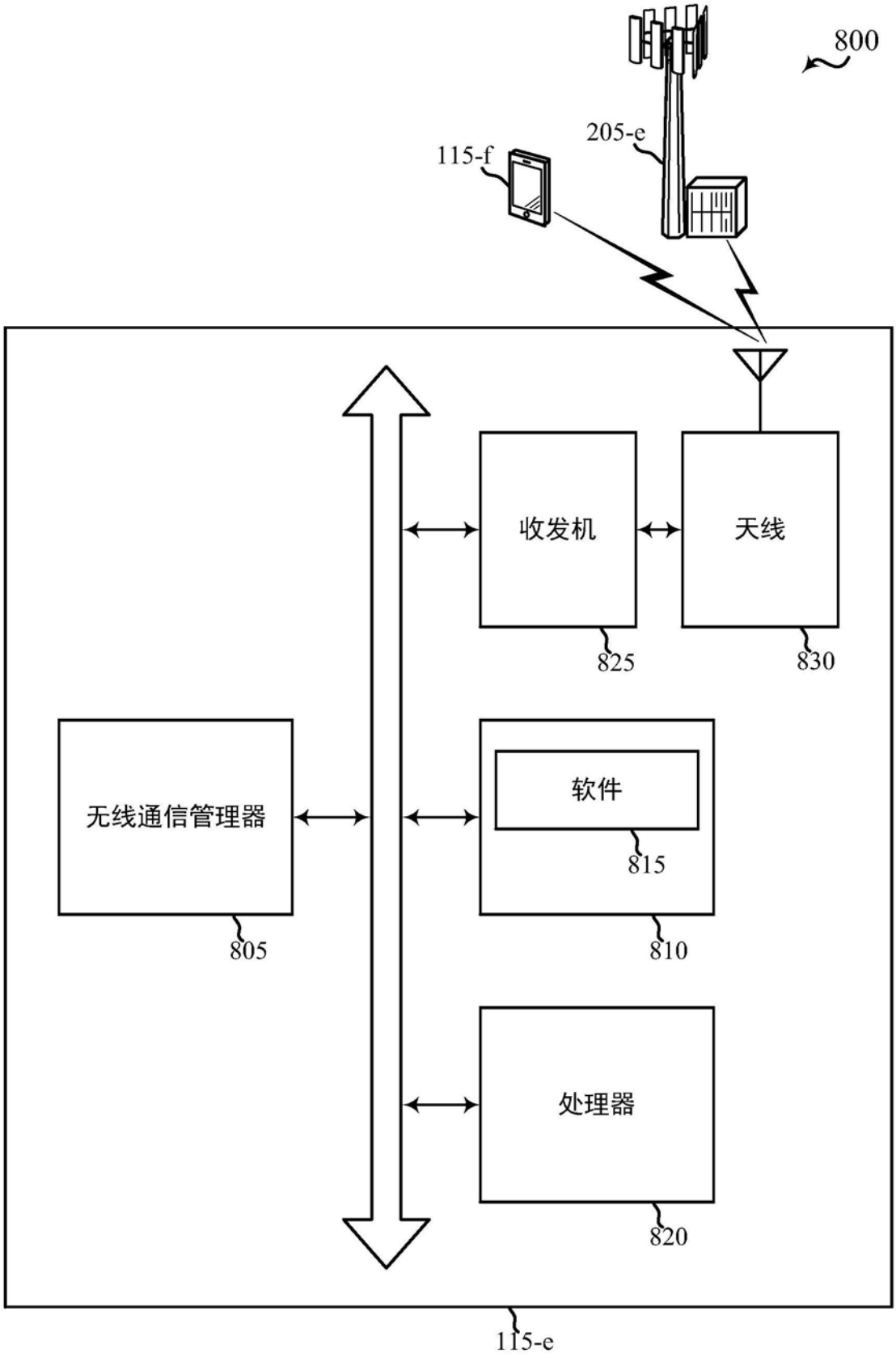

800
205-e
115-f
收发机
天线
825
830
无线通信管理器
软件
815
805
810
处理器
820
115-e

图8

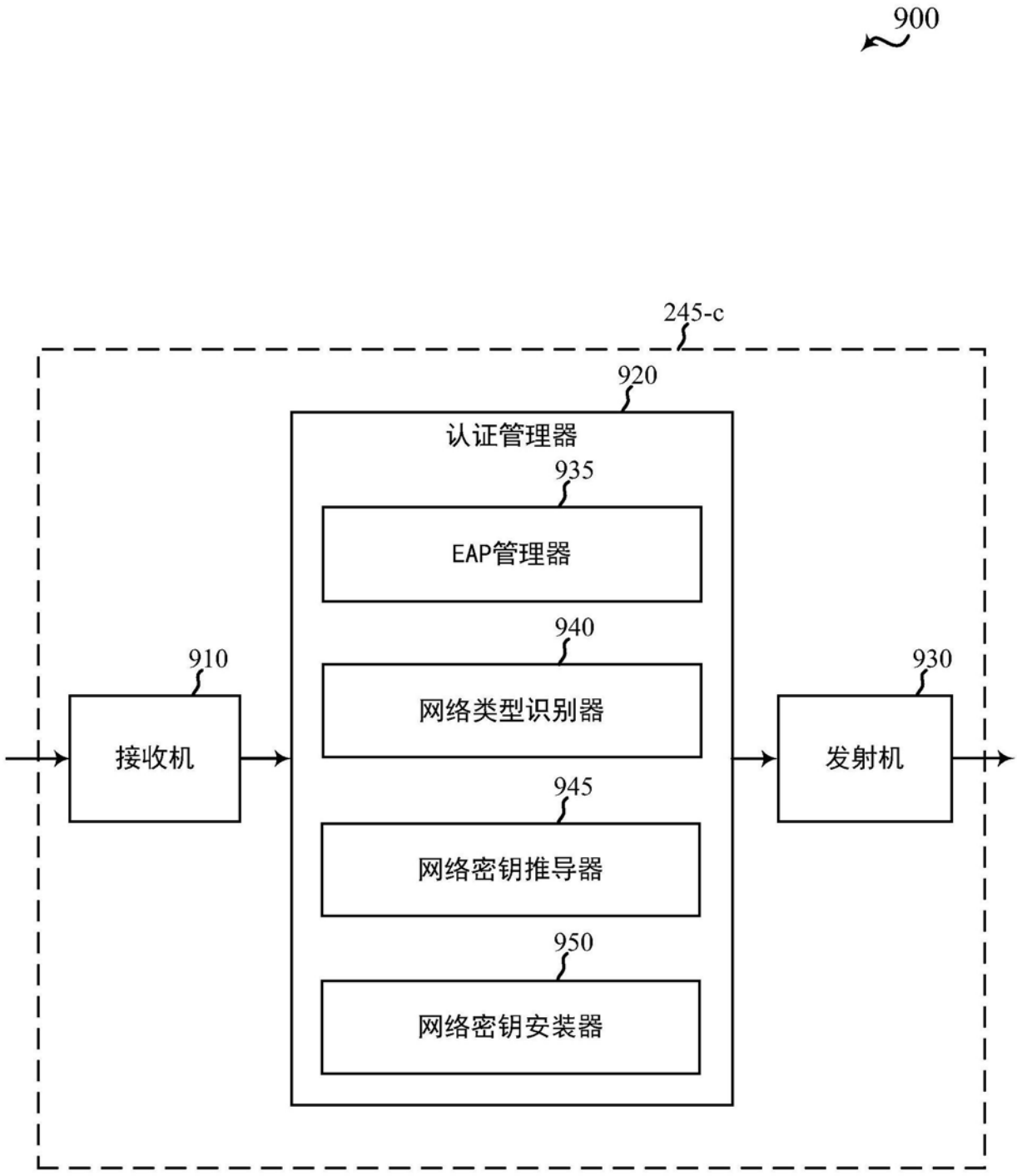

900
245-c
920
认证管理器
935
EAP管理器
940
网络类型识别器
945
网络密钥推导器
950
网络密钥安装器
910
接收机
930
发射机

图9

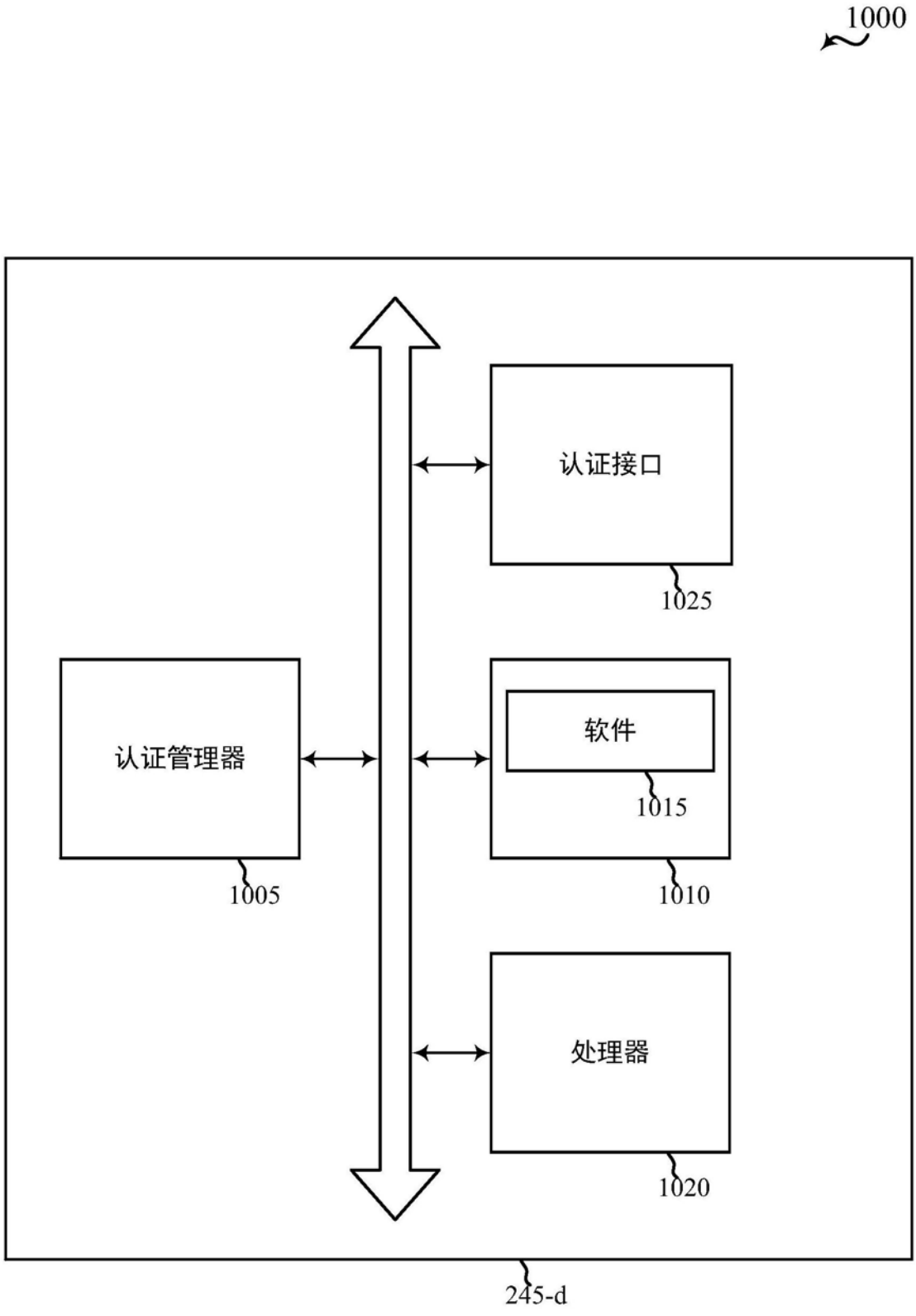


图10

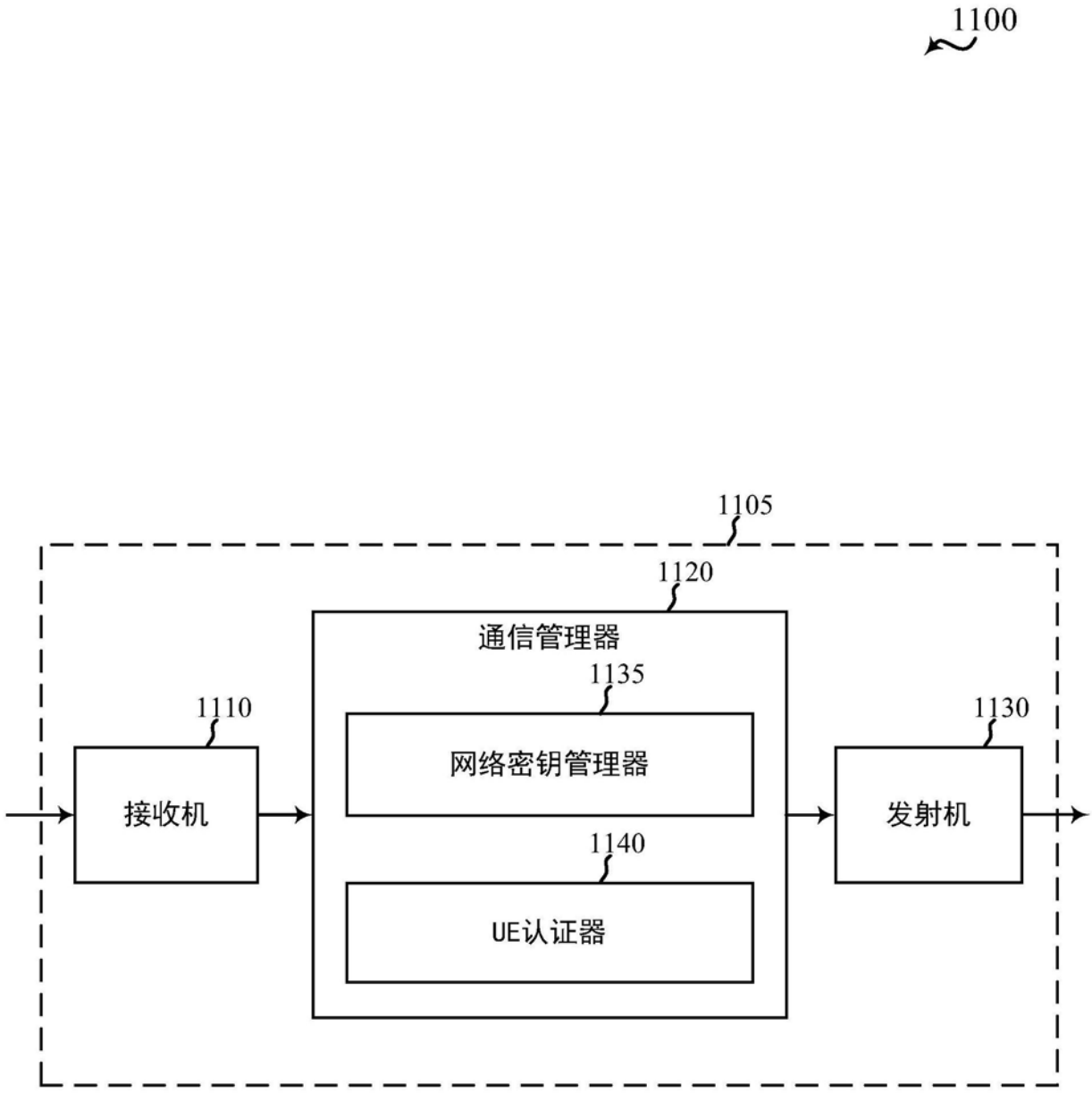

1100
1105
1120
通信管理器
1135
网络密钥管理器
1110
接收机
1130
发射机
1140
UE认证器

图11

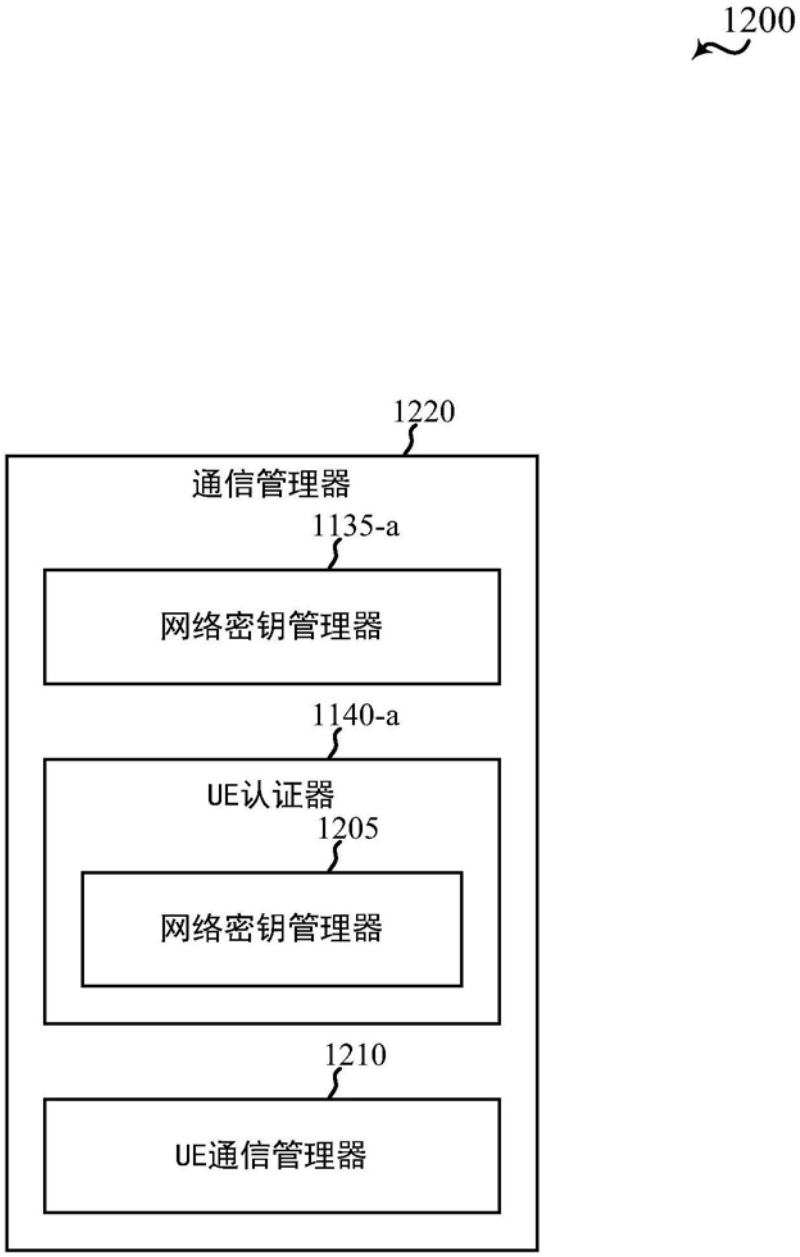

1200
1220
通信管理器
1135-a
网络密钥管理器
1140-a
UE认证器
1205
网络密钥管理器
1210
UE通信管理器

图12

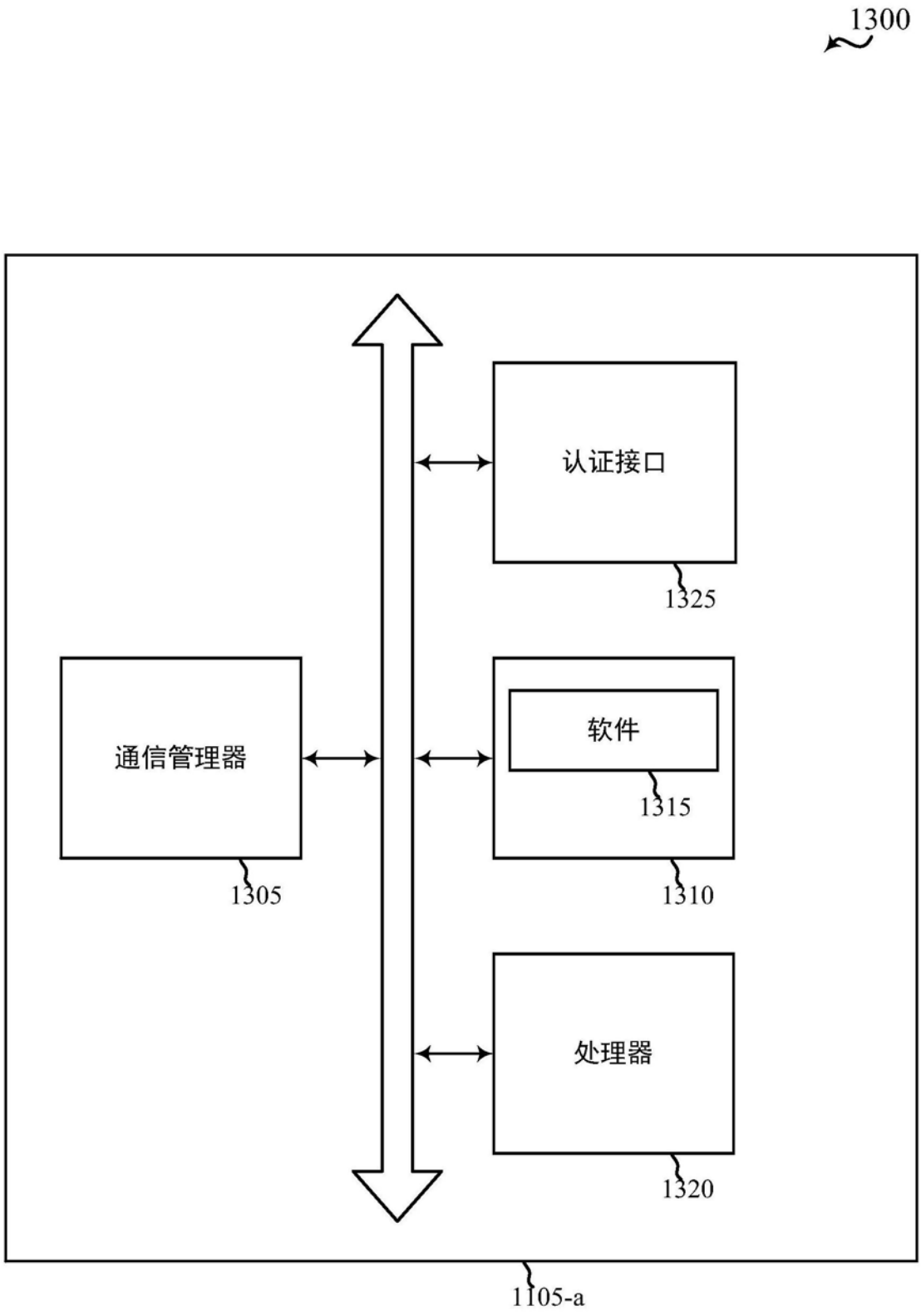


图13

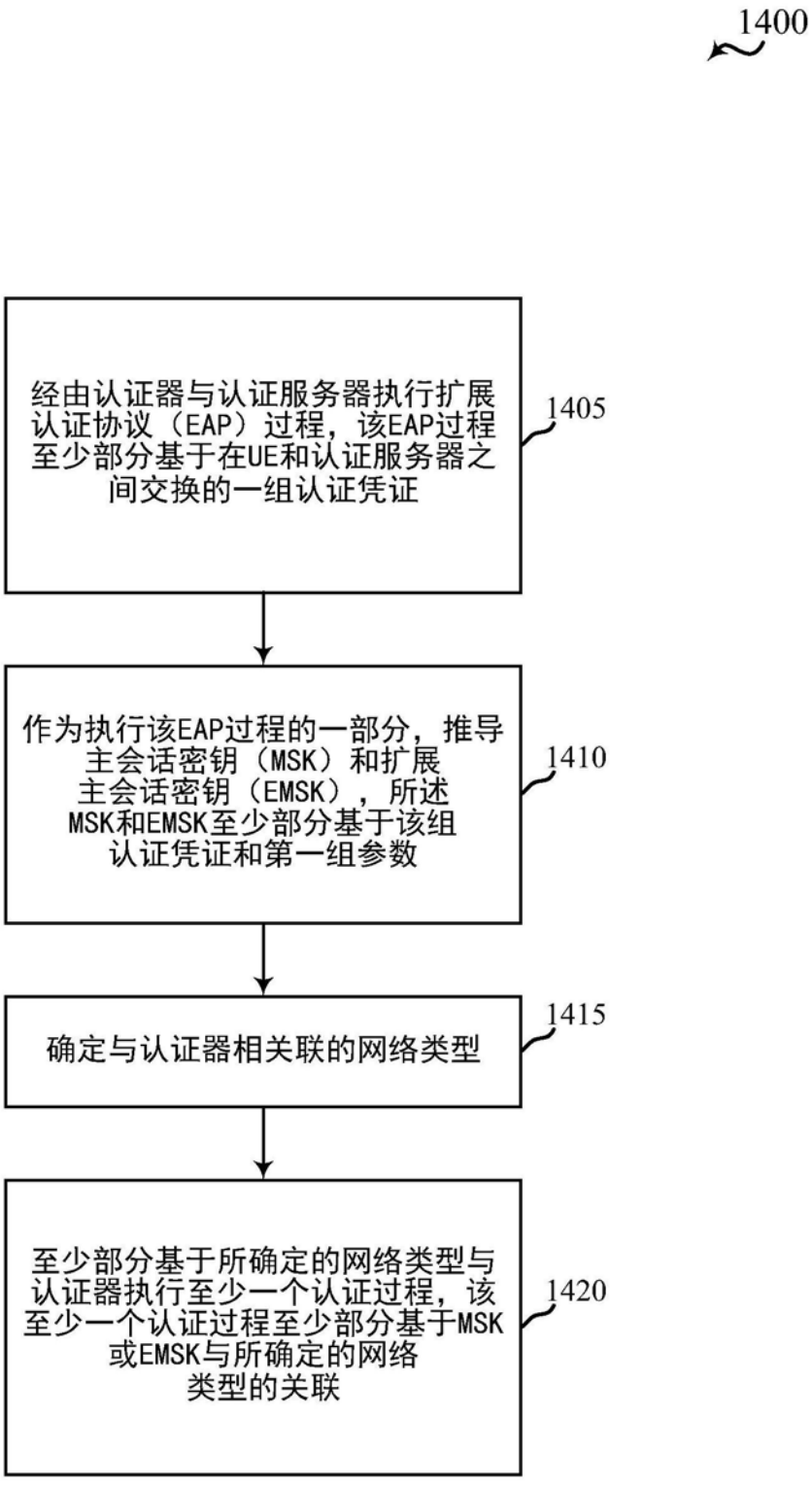

1400
经由认证器与认证服务器执行扩展认证协议（EAP）过程，该EAP过程至少部分基于在UE和认证服务器之间交换的一组认证凭证
1405
作为执行该EAP过程的一部分，推导主会话密钥（MSK）和扩展主会话密钥（EMSK），所述MSK和EMSK至少部分基于该组认证凭证和第一组参数
1410
确定与认证器相关联的网络类型
1415
至少部分基于所确定的网络类型与认证器执行至少一个认证过程，该至少一个认证过程至少部分基于MSK或EMSK与所确定的网络类型的关联
1420

图14

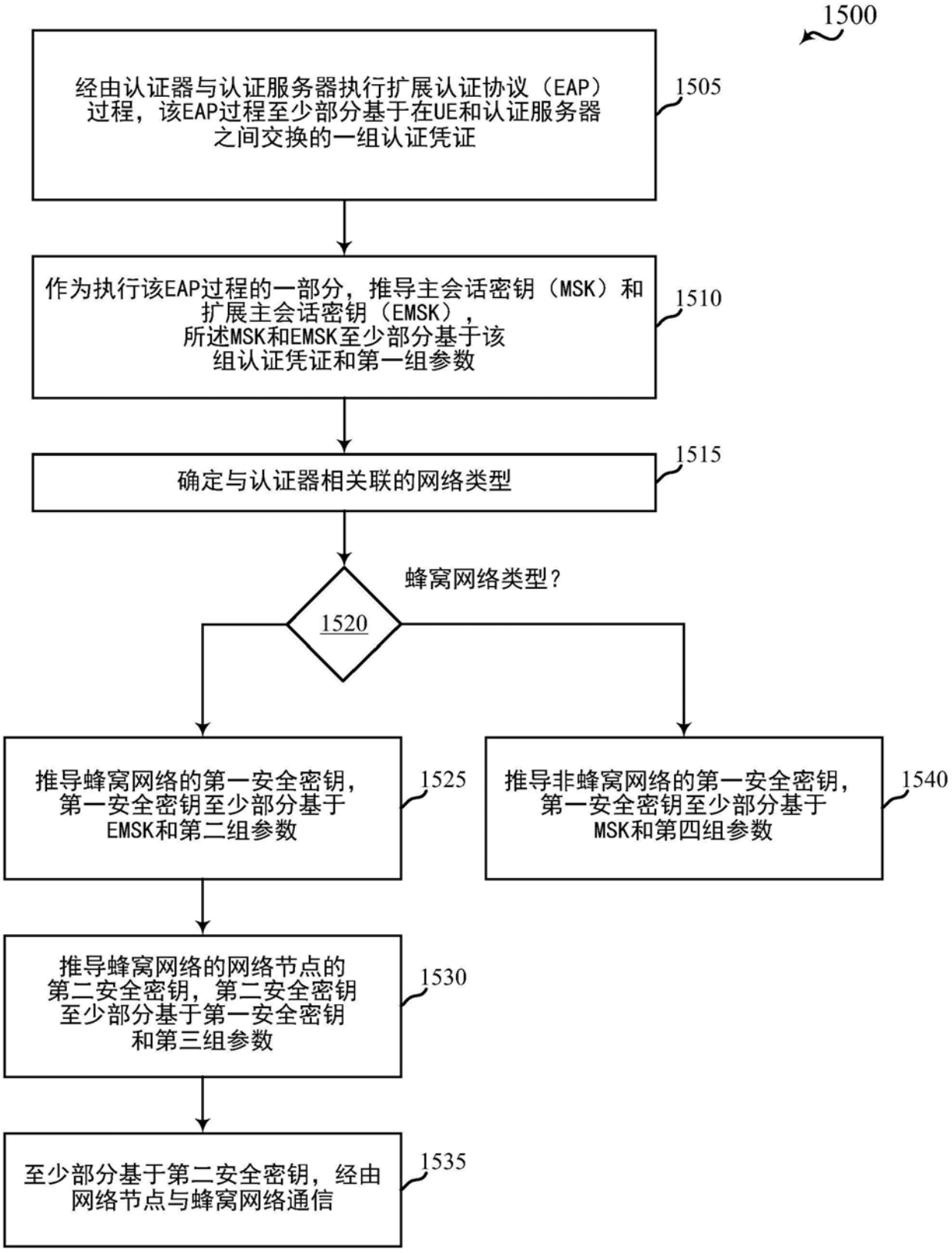

1500
经由认证器与认证服务器执行扩展认证协议（EAP）过程，该EAP过程至少部分基于在UE和认证服务器之间交换的一组认证凭证
1505
作为执行该EAP过程的一部分，推导主会话密钥（MSK）和扩展主会话密钥（EMSK），所述MSK和EMSK至少部分基于该组认证凭证和第一组参数
1510
确定与认证器相关联的网络类型
1515
蜂窝网络类型？
1520
推导蜂窝网络的第一安全密钥，第一安全密钥至少部分基于EMSK和第二组参数
1525
推导非蜂窝网络的第一安全密钥，第一安全密钥至少部分基于MSK和第四组参数
1540
推导蜂窝网络的网络节点的第二安全密钥，第二安全密钥至少部分基于第一安全密钥和第三组参数
1530
至少部分基于第二安全密钥，经由网络节点与蜂窝网络通信
1535

图15

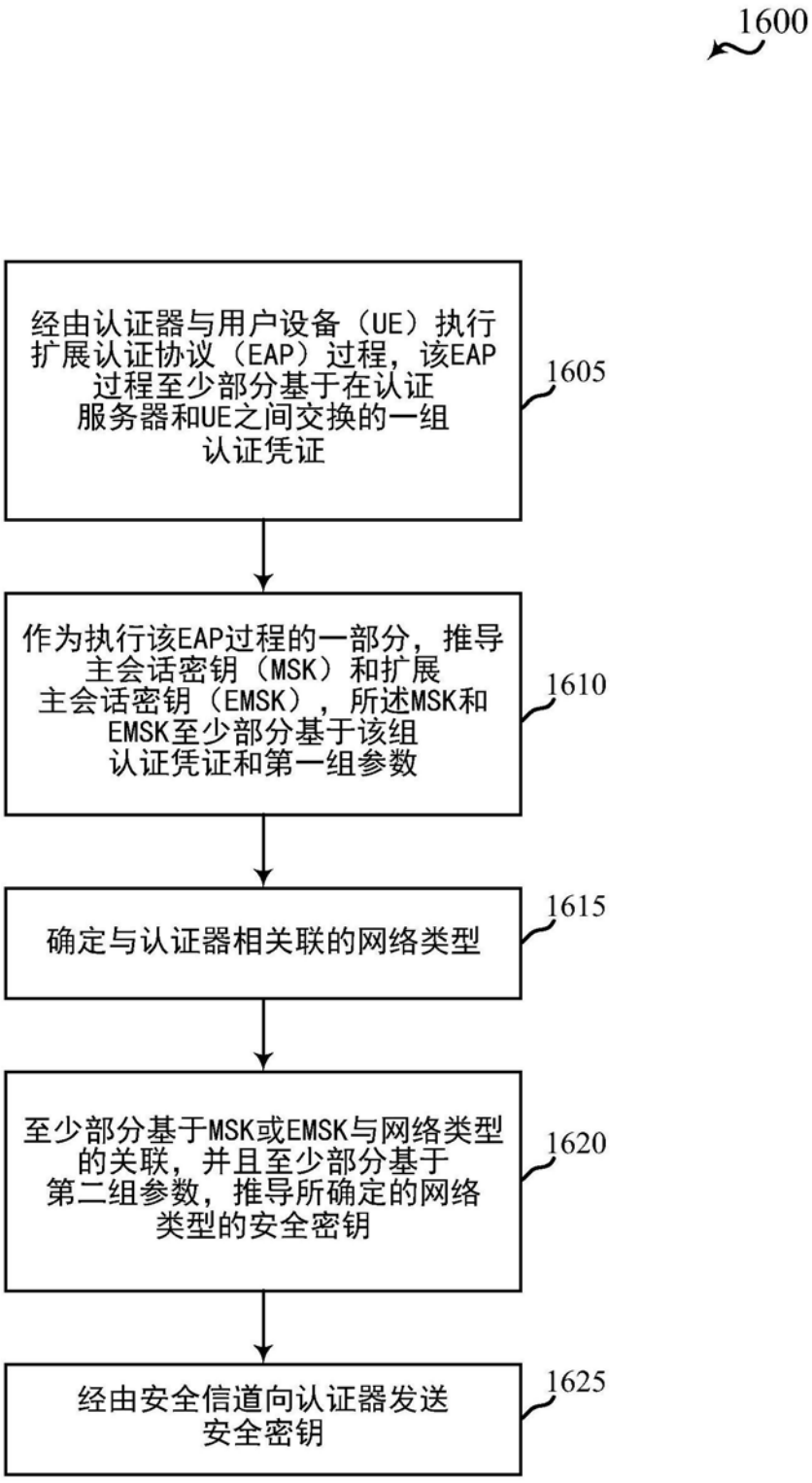

1600
经由认证器与用户设备（UE）执行扩展认证协议（EAP）过程，该EAP过程至少部分基于在认证服务器和UE之间交换的一组认证凭证
1605
作为执行该EAP过程的一部分，推导主会话密钥（MSK）和扩展主会话密钥（EMSK），所述MSK和EMSK至少部分基于该组认证凭证和第一组参数
1610
确定与认证器相关联的网络类型
1615
至少部分基于MSK或EMSK与网络类型的关联，并且至少部分基于第二组参数，推导所确定的网络类型的安全密钥
1620
经由安全信道向认证器发送安全密钥
1625

图16

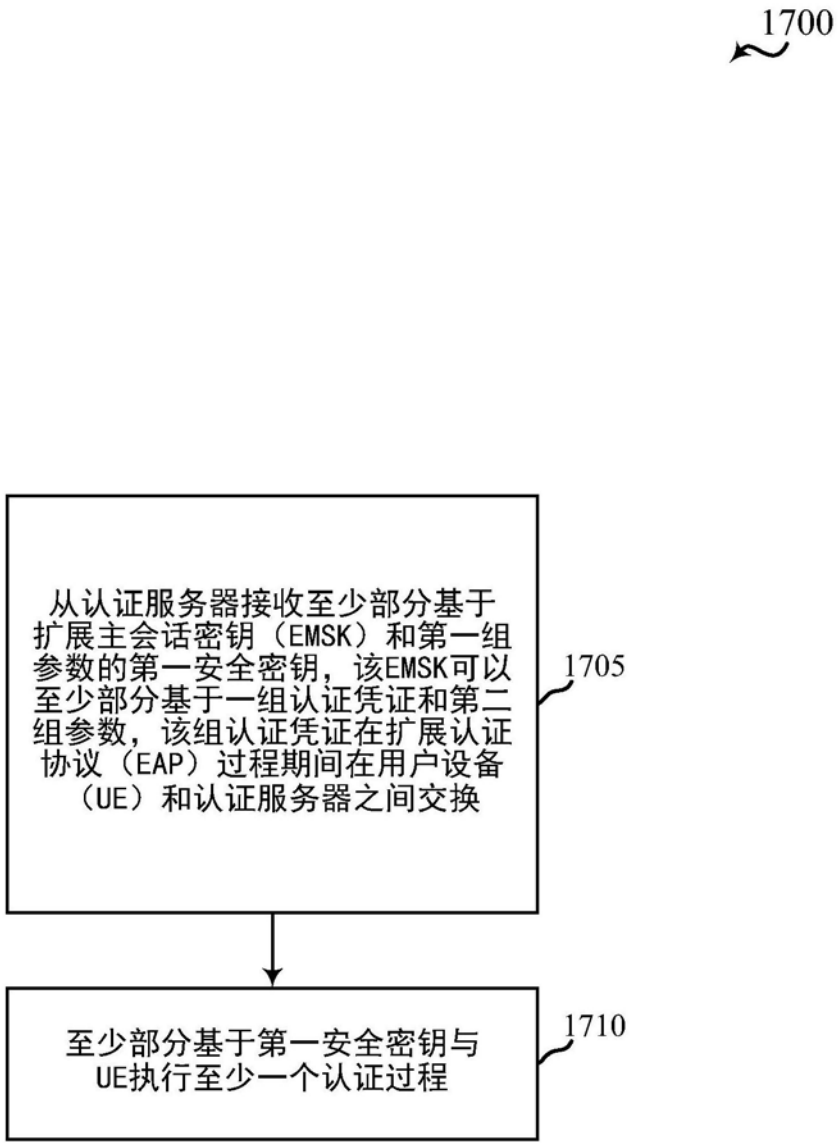

1700
从认证服务器接收至少部分基于扩展主会话密钥（EMSK）和第一组参数的第一安全密钥，该EMSK可以至少部分基于一组认证凭证和第二组参数，该组认证凭证在扩展认证协议（EAP）过程期间在用户设备（UE）和认证服务器之间交换
1705
至少部分基于第一安全密钥与UE执行至少一个认证过程
1710

图17

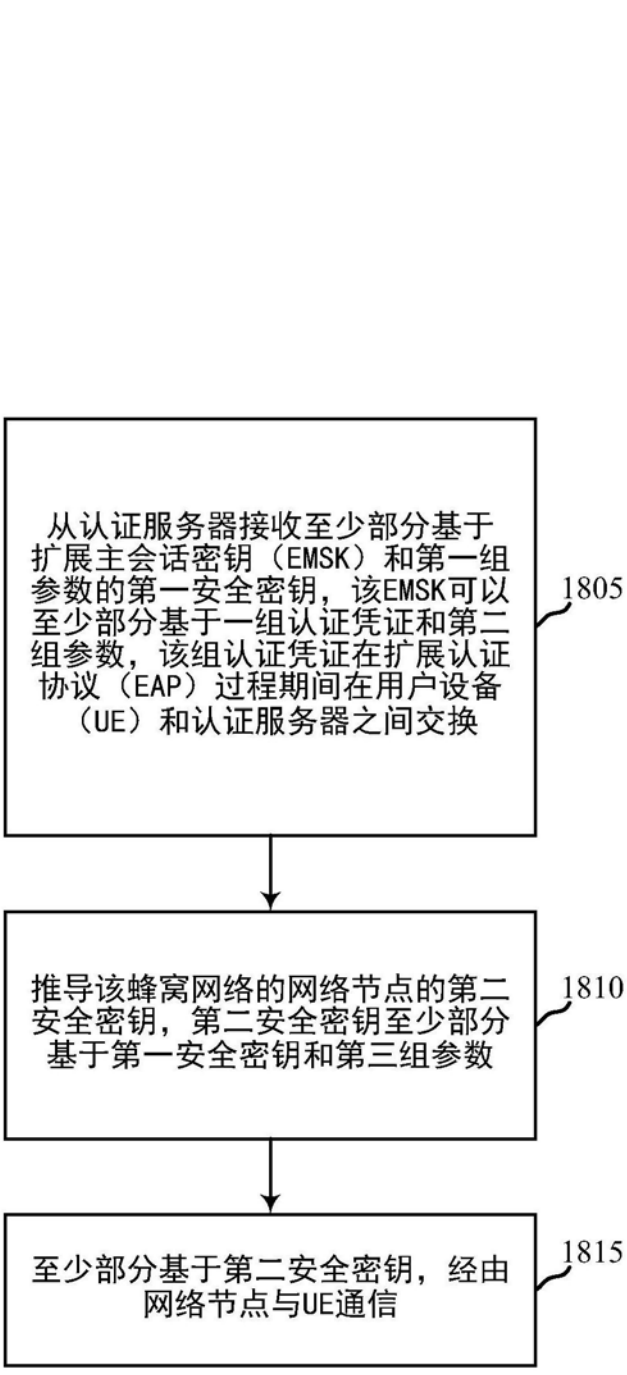

1800
从认证服务器接收至少部分基于扩展主会话密钥（EMSK）和第一组参数的第一安全密钥，该EMSK可以至少部分基于一组认证凭证和第二组参数，该组认证凭证在扩展认证协议（EAP）过程期间在用户设备（UE）和认证服务器之间交换
1805
推导该蜂窝网络的网络节点的第二安全密钥，第二安全密钥至少部分基于第一安全密钥和第三组参数
1810
至少部分基于第二安全密钥，经由网络节点与UE通信
1815

图18