(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115152257 B
(45)授权公告日 2025.03.28

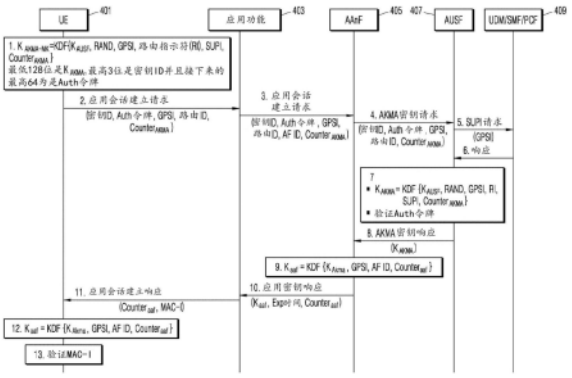
(21)申请号 202180015987.2
(22)申请日 2021.02.19
(65)同一申请的已公布的文献号
申请公布号 CN 115152257 A
(43)申请公布日 2022.10.04
(30)优先权数据
202041007160 2020.02.19 IN
202041007160 2021.02.17 IN
(85)PCT国际申请进入国家阶段日
2022.08.19
(86)PCT国际申请的申请数据
PCT/KR2021/002124 2021.02.19
(87)PCT国际申请的公布数据
WO2021/167399 EN 2021.08.26
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 N.P.萨西 R.拉贾杜赖 R.拉金德兰
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 邵亚丽
(51)Int.Cl.
H04W 12/041(2021.01)
H04W 12/0431(2021.01)
H04W 12/06(2021.01)
H04W 12/084(2021.01)
H04W 12/69(2021.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
(56)对比文件
Valbonne.Study on authentication and key management for applications based on 3GPP credential in 5G.3GPP specs\archive.2020,33,64,70-71.
审查员 肖乐义
权利要求书2页 说明书21页 附图11页

(54)发明名称

使用从网络接入认证导出的密钥生成应用特定密钥的装置和方法

(57)摘要

本发明大体上涉及3GPP中的应用认证和密钥管理(AKMA)服务,且更具体地,涉及一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的系统和方法。



CN 115152257 B

1.一种由无线通信系统中的用户设备UE执行的方法,所述方法包括:

获得与认证服务器功能AUSF实体相关的密钥;

基于与AUSF实体相关的密钥和所述UE的订阅永久标识符SUPI来生成与应用认证和密钥管理AKMA相关的密钥;

基于与AUSF实体相关的密钥生成对应于与AKMA相关的密钥的密钥标识符;

向应用功能AF实体发送包括所述密钥标识符的应用会话建立请求消息;和

从所述AF实体接收作为对所述应用会话建立请求消息的响应的应用会话建立响应消息。

2.根据权利要求1所述的方法,

其中所述密钥标识符、与AKMA相关的密钥和所述UE的SUPI被递送到AKMA锚功能AAnF实体。

3.根据权利要求1所述的方法,进一步包括:

基于与AKMA相关的密钥和AF实体的身份来生成针对AKMA的应用密钥。

4.根据权利要求3所述的方法,

其中AF实体的身份是基于所述AF实体的完全限定域名FQDN和Ua*安全协议标识符来识别的。

5.根据权利要求1所述的方法,

其中所述应用会话建立请求消息包括路由身份。

6.一种由无线通信系统中的应用功能AF实体执行的方法,所述方法包括:

从用户设备UE接收应用会话建立请求消息,所述应用会话建立请求消息包括对应于与应用认证和密钥管理AKMA相关的密钥的密钥标识符,其中与AKMA相关的密钥是基于与认证服务器功能AUSF实体相关的密钥和所述UE的订阅永久标识符SUPI来生成的,并且其中,所述密钥标识符是基于与AUSF实体相关的密钥来生成的;和

向所述UE发送应用会话建立响应消息作为对所述应用会话建立请求消息的响应。

7.根据权利要求6所述的方法,

其中所述密钥标识符、与AKMA相关的密钥和所述UE的SUPI被递送到AKMA锚功能AAnF实体。

8.根据权利要求6所述的方法,

其中所述应用会话建立请求消息包括路由身份。

9.根据权利要求6所述的方法,

向AKMA锚功能AAnF实体发送密钥请求消息,所述密钥请求消息包括对应于与AKMA相关的密钥的密钥标识符;以及

从AAnF实体接收作为对所述密钥请求消息的响应的密钥响应消息,所述密钥响应消息包括针对AKMA的应用密钥。

10.根据权利要求9所述的方法,

其中针对AKMA的应用密钥是基于与AKMA相关的密钥和AF实体的身份来生成的;和

其中AF实体的身份是基于所述AF实体的完全限定域名FQDN和Ua*安全协议标识符来识别的。

11.根据权利要求9所述的方法,

其中所述密钥请求消息还包括AF实体的身份。

12.一种在无线通信系统中执行的用户设备UE,所述UE包括:

收发器;和

至少一个处理器,耦合到所述收发器并且被配置为:

获得与认证服务器功能AUSF实体相关的密钥;

基于与AUSF实体相关的密钥和所述UE的订阅永久标识符SUPI来生成与应用认证和密钥管理AKMA相关的密钥;

基于与AUSF实体相关的密钥生成对应于与AKMA相关的密钥的密钥标识符;

向应用功能AF实体发送包括所述密钥标识符的应用会话建立请求消息;和

从所述AF实体接收作为对所述应用会话建立请求消息的响应的应用会话建立响应消息。

使用从网络接入认证导出的密钥生成应用特定密钥的装置和方法

技术领域

[0001] 本发明大体上涉及3GPP中的应用认证和密钥管理(Authentication and Key Management for Applications)(AKMA)服务,且更具体地,涉及一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的系统和方法。

背景技术

[0002] 为了满足对自部署第4代(4G)通信系统以来不断增加的无线数据业务的需求,已经努力开发了改进型第5代(5G)或准5G(pre-5G)通信系统。5G或准5G通信系统也被称作‘超4G网络’或‘后长期演进(LTE)系统’。5G通信系统被视为在更高的频率(毫米波)带(例如60千兆赫(GHz)的频带)中实施,以便实现更高的数据速率。为了减少无线电波的传播损耗并且增加传输距离,相对于5G通信系统论述了波束成形、大规模多输入多输出(MIMO)、全维MIMO(FD-MIMO)、阵列天线、模拟波束成形和大规模天线技术。此外,在5G通信系统中,针对系统网络改进的开发正基于先进的小小区、云无线电接入网(RAN)、超密集网络、设备到设备(D2D)通信、无线回程、移动网络、协同通信、协调多点(CoMP)、接收端干扰消除等进行。在5G系统中,已经开发了作为高级编码调制(ACM)的混合频移键控(FSK)和费赫正交振幅调制(FQAM)和滑动窗口叠加编码(SWSC)以及作为高级接入技术的滤波器组多载波(FBMC)、非正交多址(NOMA)和稀疏码多址(SCMA)。

[0003] 互联网(其为人类在其中生成并且消费信息的以人为中心的连接性网络)现在正朝向物联网(IoT)演进,在物联网中,诸如事物的分布式实体在无人工干预的情况下交换和处理信息。已经出现了万物互联(IoE),万物互联是通过与云服务器的连接的IoT技术与大数据处理技术的组合。随着诸如人类生成和消费信息的技术连接性网络的技术元件现在正朝向物联网(IoT)演进,在物联网中,云服务器具有最近已经进行了研究的IoT实施方式、传感器网络、机器对机器(M2M)通信、机器类型通信(MTC)等。这种IoT环境可以提供智能互联网技术服务,这些智能互联网技术服务通过收集和分析在所连接的事物之间生成的数据来为人类生活创造新价值。IoT可以通过现有信息技术(IT)与各种工业应用之间的融合和组合而应用于各种领域,包括智能家居、智能楼宇、智能城市、智能汽车或联网汽车、智能电网、医疗保健、智能家电和先进的医疗服务。

[0004] 据此,已经为将5G通信系统应用于IoT网络进行了各种尝试。例如,诸如传感器网络、MTC和M2M通信的技术可以通过波束成形、MIMO和阵列天线来实施。将云RAN作为上文所描述的大数据处理技术的应用也可以被视为是5G技术与IoT技术之间的融合的示例。

发明内容

[0005] 技术解决方案

[0006] 本发明内容的提供是为了以简化的格式介绍对于在本发明的详细说明中进一步

描述的构思的选择。本发明内容既不旨在标识本发明的关键或必要发明构思,也不旨在确定本发明的范围。

[0007] 本发明公开了一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的系统和方法。

[0008] 在本发明中,由于AKMA架构支持不同AKMA AF的密钥分离,因此,引入了从KAKMA导出的应用密钥(KAAF)来解决TS 33.535v020中规定的各种要求。特定地,本发明公开了一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的方法。该方法在网络侧包括:由应用功能(AF)从UE接收应用会话建立请求消息,其中应用会话建立请求消息包括UE侧认证令牌、UE侧的UE标识符(密钥ID)、UE的第一应用身份参数(GPSI)、路由标识符(RI)和新鲜度参数(CounterAKMA)。该方法然后标识由AF基于由网络供应的RI来标识第一网络元件(AAnF)。此后,第一网络元件(AAnF)基于由网络供应的RI来选择正确的对应的第二网络元件,该正确的对应的第二网络元件是所请求的UE的认证服务功能(AUSF)。AUSF然后从第三网络元件(统一数据管理(UDM))获得UE的第二应用身份参数(SUPI),其中第三网络元件(UDM)提供与第一应用身份参数(GPSI)对应的第二应用身份参数。所选择的AUSF然后基于第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI、RAND和新鲜度参数(CounterAKMA)以及用于在网络侧标识UE的订户相关上下文的AKMA服务的UE标识符(密钥ID)中的至少一者来导出网络侧协商密钥(KAKMA)。AUSF然后验证网络侧的UE标识符(密钥ID)与UE侧的接收到的UE标识符(密钥ID)类似。此后,第一网络元件(AAnF)基于网络侧协商密钥(KAKMA)、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID(RI)和新鲜度参数(CounterAKMA)中的至少一者来导出网络侧应用特定密钥(KAF)。第一网络元件(AAnF)向应用功能(AF)提供所导出的网络侧应用特定密钥(KAF)以及用于在UE处认证所导出的网络侧应用特定密钥(KAF)以便在UE与应用功能(AF)之间建立安全接口的预定时间段和CounterAF(AF)。

[0009] 为了进一步阐明本发明的优点和特征,将参考附图中所说明的具体实施例呈现对本发明的更具体描述。应了解,这些图式仅描绘了本发明的典型实施例,因此不应被视为限制其范围。本发明将与附图一起以附加特征和细节进行描述和解释。

附图说明

[0010] 当参考附图阅读以下详细说明时,将更好地理解本发明的这些和其他特征、方面和优点,其中贯穿图式,相同字符表示相同部分,在图式中:

[0011] 图1图示了AKMA的网络模型;

[0012] 图2图示了AKMA密钥层级结构;

[0013] 图3A图示了根据本公开的实施例的用于在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的流程图。

[0014] 图3B图示了根据本公开的实施例的用于在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的流程图。

[0015] 图4图示了根据本公开的实施例的用于将图3a和图3b的方法实施为替代1解决方

案的消息流;

[0016] 图5图示了根据本公开的实施例的作为替代2解决方案的在图4处实施的方法的替代实施例;

[0017] 图6图示了根据本公开的实施例的作为替代3解决方案的在图4处实施的方法的替代实施例;

[0018] 图7图示了根据本公开的实施例的作为替代4解决方案的在图4处实施的方法的替代实施例;

[0019] 图8图示了根据本公开的实施例的作为替代5解决方案的在图4处实施的方法的替代实施例;

[0020] 图9图示了根据本公开的实施例的作为替代6解决方案的在图4处实施的方法的替代实施例。

[0021] 图10图示了根据本公开的实施例的实施3GPP和5G技术的无线通信系统的实施方式,该3GPP和5G技术实施如图3至图9中所示出的方法。

[0022] 图11图示了根据本公开的实施例的网络实体。

[0023] 图12图示了根据本公开的实施例的用户设备(UE)。

[0024] 另外,熟练的技术人员应了解,图式中的元件是出于简单起见而图示的并且可能不一定按比例绘制。例如,流程图就帮助提高对本发明的各个方面的理解所涉及的最突出的步骤而言说明了方法。此外,就设备的构造而言,设备的一个或多个组件可能已经在图式中用常规符号进行了表示,并且图式可以仅示出与理解本发明的实施例相关的那些具体细节,以免用易于对受益于本文中的描述的本领域的普通技术人员而言显而易见的细节模糊图式。

具体实施方式

[0025] 最佳发明模式

[0026] 根据本公开的实施例,提供了一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务的应用特定密钥的方法,该方法在网络侧包括:由应用功能(AF)从UE接收应用会话建立请求消息,其中应用会话建立请求消息包括与K_{AKMA}相关联的AKMA密钥ID、用作外部标识符的第一UE身份参数(GPSI)、路由标识符(RI)和新鲜度参数($Counter_{AKMA}$);由AF基于由本地网络供应的RI来标识第一网络元件AKMA锚功能(AAnF);由第二网络元件(AUSF)基于网络侧密钥(K_{AUSF})、SUPI、GPSI和RI中的至少一者来导出网络侧AKMA密钥(K_{AKMA});以及由第一网络元件(AAnF)基于网络侧AKMA密钥(K_{AKMA})、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID(RI)和新鲜度参数($Counter_{AKMA}$)中的至少一者来导出网络侧应用特定密钥(K_{AF})。

[0027] 在实施例中,该方法进一步包括:由第一网络元件(AAnF)向应用功能(AF)提供所导出的网络侧应用特定密钥(K_{AF})以及用于在UE处认证所导出的网络侧应用特定密钥(K_{AF})的预定时间段和$Counter_{AF}$。

[0028] 在实施例中,网络侧协商密钥(K_{AKMA})是由所选择的AUSF基于第一应用身份参数(GPSI)、第二UE身份参数(SUPI)、RI、RAND和新鲜度参数($Counter_{AKMA}$)以及用于在网络侧标识UE的订户相关上下文的AKMA服务的AKMA密钥ID中的至少一者导出的。

[0029] 在实施例中,该方法进一步包括:由AUSF从第三网络元件(UDM)获得UE的第二UE身份参数(SUPI),其中第三网络元件(UDM)提供与第一UE(SUPI)身份参数(GPSI)对应的第二UE身份参数。

[0030] 在实施例中,该方法进一步包括:由第一网络元件(AAnF)基于由第一网络元件(AAnF)导出的K_{AF}来生成网络侧MAC-I;由第一网络元件(AAnF)向AF发送所生成的网络侧MAC-I。

[0031] 在实施例中,UE:基于第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧协商密钥(K_{AKMA});基于第一应用身份参数(GPSI)、RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧的UE标识符(密钥ID),其中UE侧的UE标识符(密钥ID)由UE在应用会话建立请求消息中向AF提供。

[0032] 在实施例中,在由AF向UE发送应用会话建立响应之后,UE:基于UE侧协商密钥(K_{AKMA})、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧应用特定密钥(K_{AF})。

[0033] 在实施例中,AF向UE发送应用会话建立响应以在UE与应用功能(AF)之间建立安全接口,其中UE:在接收到来自AF的应用会话建立响应之后导出UE侧MAC-I,验证UE侧MAC-I与网络侧MAC-I匹配并且基于验证的成功结果来在UE与应用功能(AF)之间建立安全接口。

[0034] 在实施例中,该方法进一步包括:由第一网络元件(AAnF)对所获得的第二应用身份参数(SUPI)执行UE的授权检查。

[0035] 在实施例中,该方法进一步包括:由第一网络元件(AAnF)基于应用会话建立请求消息中所包括的RI来标识所请求的UE的第三网络元件(UDM);以及由第一网络元件(AAnF)在从第三网络元件(UDM)接收到的订阅数据响应消息中获得来自UDM的第二应用身份参数(SUPI),其中第三网络元件(UDM)向第一网络元件(AAnF)提供与第一应用身份参数(GPSI)对应的第二应用身份参数(SUPI)。

[0036] 在实施例中,该方法进一步包括:由第一网络元件(AAnF)向AUSF发送AKMA密钥请求,该AKMA密钥请求包括UE侧认证令牌、第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和作为AKMA密钥ID的新鲜度参数($Counter_{AKMA}$)。

[0037] 在实施例中,UE或网络侧协商密钥(K_{AKMA})的格式由128位的最低有效位(LSB)定义,UE或UE标识符(密钥ID)的格式与$Counter_{AKMA}$相同,并且UE侧认证令牌由连续64位的最高有效位(MSB)按位格式定义。

[0038] 在实施例中,应用功能(AF)与第三方实体对应,第一网络元件与AKMA锚功能(AAnF)对应。

[0039] 在实施例中,应用ID(AF ID)标识AF的哪个应用正在发出应用会话建立请求。

[0040] 在实施例中,如果KAF密钥先前在AAnF中对UE可用,那么AAnF跳过向AUSF请求密钥(KAF)。

[0041] 在实施例中,该方法进一步包括:由第一网络元件AAnF向应用功能(内部)发送UE标识符SUPI和/或向应用功能(外部)发送GPSI,向应用功能提供UE标识符(SUPI或GPSI)以标识或认证UE。

[0042] 在实施例中,该方法进一步包括:由应用功能使用$Counter_{KAF}$或使用Ua*协议(如果其支持)刷新所导出的K_{AF}。

[0043] 在实施例中,UDM向AAnF提供与SUPI对应的GPSI和/或订阅数据。

[0044] 根据本公开的实施例,提供了一种在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务的应用特定密钥的系统,该系统在网络侧包括具有一个或多个网络元件的多个网络节点和应用功能(AF),一个或多个网络元件和AF与UE耦合,多个网络节点配置成:由应用功能(AF)从UE接收应用会话建立请求消息,其中应用会话建立请求消息包括与K_{AKMA}相关联的AKMA密钥ID、用作外部标识符的第一UE身份参数(GPSI)、路由标识符(RI)和新鲜度参数($Counter_{AKMA}$);由AF基于由本地网络供应的RI来标识第一网络元件AKMA锚功能(AAnF);由第二网络元件(AUSF)基于网络侧密钥(K_{AUSF})、SUPI、GPSI和RI中的至少一者来导出网络侧AKMA密钥(K_{AKMA});以及由第一网络元件(AAnF)基于网络侧AKMA密钥(K_{AKMA})、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID(RI)和新鲜度参数($Counter_{AKMA}$)中的至少一者来导出网络侧应用特定密钥(K_{AF})。

[0045] 在实施例中,多个网络节点配置成:由第一网络元件(AAnF)向应用功能(AF)提供所导出的网络侧应用特定密钥(K_{AF})以及用于在UE处认证所导出的网络侧应用特定密钥(K_{AF})的预定时间段和$Counter_{AF}$。

[0046] 在实施例中,网络侧协商密钥(K_{AKMA})是由所选择的AUSF基于第一应用身份参数(GPSI)、第二UE身份参数(SUPI)、RI、RAND和新鲜度参数($Counter_{AKMA}$)以及用于在网络侧标识UE的订户相关上下文的AKMA服务的AKMA密钥ID中的至少一者导出的。

[0047] 在实施例中,多个网络节点配置成:由AUSF从第三网络元件(UDM)获得UE的第二UE身份参数(SUPI),其中第三网络元件(UDM)提供与第一UE(SUPI)身份参数(GPSI)对应的第二UE身份参数。

[0048] 在实施例中,多个网络节点配置成:由第一网络元件(AAnF)基于由第一网络元件(AAnF)导出的K_{AF}来生成网络侧MAC-I;由第一网络元件(AAnF)向AF发送所生成的网络侧MAC-I。

[0049] 在实施例中,UE:基于第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧协商密钥(K_{AKMA});基于第一应用身份参数(GPSI)、RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧的UE标识符(密钥ID),其中UE侧的UE标识符(密钥ID)由UE在应用会话建立请求消息中向AF提供。

[0050] 在实施例中,在由AF向UE发送应用会话建立响应之后,UE:基于UE侧协商密钥(K_{AKMA})、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID RI和新鲜度参数($Counter_{AKMA}$)中的至少一者生成UE侧应用特定密钥(K_{AF})。

[0051] 在实施例中,AF向UE发送应用会话建立响应以在UE与应用功能(AF)之间建立安全接口,其中UE:在接收到来自AF的应用会话建立响应之后导出UE侧MAC-I,验证UE侧MAC-I与网络侧MAC-I匹配并且基于验证的成功结果来在UE与应用功能(AF)之间建立安全接口。

[0052] 在实施例中,多个网络节点配置成:由第一网络元件(AAnF)对所获得的第二应用身份参数(SUPI)执行UE的授权检查。

[0053] 在实施例中,多个网络节点配置成:由第一网络元件(AAnF)基于应用会话建立请求消息中所包括的RI来标识所请求的UE的第三网络元件(UDM);以及由第一网络元件(AAnF)在从第三网络元件(UDM)接收到的订阅数据响应消息中获得来自UDM的第二应用身份参数(SUPI),其中第三网络元件(UDM)向第一网络元件(AAnF)提供与第一应用身份参数

(GPSI)对应的第二应用身份参数(SUPI)。

[0054] 在实施例中,多个网络节点配置成:由第一网络元件(AAnF)向AUSF发送AKMA密钥请求,该AKMA密钥请求包括UE侧认证令牌、第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和作为AKMA密钥ID的新鲜度参数($Counter_{AKMA}$)。

[0055] 在实施例中,UE或网络侧协商密钥(K_{AKMA})的格式由128位的最低有效位(LSB)定义,UE或UE标识符(密钥ID)的格式与$Counter_{AKMA}$相同,并且UE侧认证令牌由连续64位的最高有效位(MSB)按位格式定义。

[0056] 在实施例中,应用功能(AF)与第三方实体对应,第一网络元件与AKMA锚功能(AAnF)对应。

[0057] 在实施例中,应用ID(AF ID)标识AF的哪个应用正在发出应用会话建立请求。

[0058] 在实施例中,如果KAF密钥先前在AAnF中对UE可用,那么AAnF跳过向AUSF请求密钥(KAF)。

[0059] 在实施例中,多个网络节点配置成:由第一网络元件AAnF向应用功能(内部)发送UE标识符SUPI和/或向应用功能(外部)发送GPSI,向应用功能提供UE标识符(SUPI或GPSI)以标识或认证UE。

[0060] 在实施例中,多个网络节点配置成:由应用功能使用$Counter_{KAF}$或使用Ua*协议(如果其支持)刷新所导出的K_{AF}。

[0061] 在实施例中,UDM向AAnF提供与SUPI对应的GPSI和/或订阅数据。

[0062] 本发明的模式

[0063] 为了促进对本发明的原理的理解,现在将参考图式中所说明的实施例并且将使用特定语言对其进行描述。然而,应理解,本发明的范围并不因此受到限制,所图示的系统中的这种变更和进一步修改以及如其中所说明的本发明的原理的这种进一步应用正如本发明所涉及的领域的技术人员通常会想到的一般进行了预期。

[0064] 本领域的技术人员应理解,前述一般描述和以下详细说明是对本发明的解释,而不旨在限制本发明。

[0065] 贯穿本说明书对“一个方面”、“另一方面”或类似语言的引用意指结合实施例描述的特定特征、结构或特点被包括在本发明的至少一个实施例中。因此,贯穿本说明书出现的短语“在实施例中”、“在另一实施例中”和类似语言可以但并不一定都指相同实施例。

[0066] 术语“包括(comprises/comprising)”或其任何其他变型旨在涵盖非排他性包括,使得包括步骤列表的进程或方法不仅包括那些步骤,而且还可以包括未明确列出或这种进程或方法固有的其他步骤。类似地,以“包括……”为开头的一个或多个设备或子系统或元件或结构或组件在没有更多约束的情况下不排除其他设备或其他子系统或其他元件或其他结构或其他组件或附加设备或附加子系统或附加元件或附加结构或附加组件的存在。

[0067] 除非另外定义,否则本文中所使用的所有技术和科学术语都具有与本发明所属领域的普通技术人员通常理解的含义相同的含义。本文中所提供的系统、方法和示例仅仅是说明性的并且不旨在作为限制。

[0068] 下面将参考附图详细地描述本发明的实施例。

[0069] 图1图示了AKMA的网络模型。

[0070] 3GPP目前正在研究应用认证和密钥协商(AKMA)服务,如图1中所示出,旨在针对第

三方和/或3GPP应用和服务基于5G系统中的3GPP网络接入凭证来支持认证和密钥管理的网络服务。AKMA本质上是认证和密钥协商服务,其中对应用功能/服务器的接入以及UE与应用功能(AF)之间的安全接口的建立是基于已建立的网络接入安全凭证(在初级认证期间建立的)。由AF表示的使用AKMA的应用提供商(应用功能或应用服务器)将AF用户的认证委托给HPLMN(本地公共陆地移动网络)。因此,服务提供商利用由MNO提供的安全凭证。

[0071] 如图1中所示出,AAnF(AKMA锚功能)是HPLMN中的锚功能,该锚功能生成要在UE与AF之间使用的密钥材料并且维持要用于后续引导请求的UE AKMA上下文。AAnF针对AKMA服务启用AKMA锚密钥(K_{AKMA})推导。在调用AKMA服务之前,UE应已成功注册到5G核心,这导致在成功的5G主要认证[TS 33.535v020]之后将K_{AUSF}存储在AUSF(认证服务器功能)和UE处。

[0072] 贯穿本文,术语"应用功能"或"AKMA应用功能"可互换地用于AKMA和应用密钥推导过程。术语"AF ID"指示AKMA应用功能ID,其用作标识从应用功能向5GC网络请求的单独应用的参数。术语"Kaaf"、"K_{AAF}"和"K_{AF}"可互换地用于指示从K_{AKMA}导出的应用功能密钥。

[0073] 图2图示了AKMA密钥层级结构。

[0074] 如图2中所示出的密钥层级结构包括以下密钥:K_{AUSF}、K_{AKMA}、K_{AF},K_{AUSF}由如TS 33.501中规定的AUSF生成。

[0075] AAnF的密钥:

[0076] K_{AKMA}是由ME和AUSF从K_{AUSF}导出的密钥。

[0077] AF的密钥:

[0078] K_{AF}是由ME和AAnF从K_{AKMA}导出的密钥。

[0079] AKMA密钥层级结构描述了用于在UE和AUSF处导出密钥K_{AKMA}的方法。AUSF向锚功能发送K_{AKMA}。K_{AKMA}等效于TS 33.220中的GBA的密钥Ks。AAnF和UE两者应使用K_{AKMA}来导出AKMA应用功能(AF)所需的应用特定密钥。

[0080] 基于如[TS 33.535v020]中规定的运营商策略,锚密钥K_{AKMA}应使用隐式使用寿命,并且应用密钥K_{AF}应使用显式使用生命。应为应用密钥提供最长使用寿命。当应用密钥使用寿命到期时,应重新协商。一旦从锚密钥导出应用密钥,锚功能就有必要向应用功能通知所导出的应用密钥的有效性。

[0081] 因此,当使用所导出的密钥进行网络接入认证(主要认证)时,以下是需要解决以便导出每UE和每AF唯一独立密钥的问题:

[0082] 由网络使用UE的应用身份(例如通用公共订阅标识符(GPSI)或订阅永久标识符(SUPI))标识UE的密钥K_{AKMA};

[0083] 由AKMA功能标识适当AUSF以获得密钥生成服务;

[0084] 使用由网络供应的路由标识符来标识AAnF

[0085] 生成唯一独立的K_{AKMA}和K_{AF}密钥;

[0086] 导出随机化密钥ID的机制;

[0087] 生成用于验证UE的真实性的验证令牌;以及

[0088] 所导出的AKMA和应用密钥的密钥使用寿命和撤销。

[0089] 因此,需要克服上面提及的缺陷的解决方案。

[0090] 图3A和图3B图示了根据本公开的实施例的用于在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的

应用特定密钥的流程图。

[0091] 在如图3A和图3B中所描绘的实施方式中,本主题涉及在无线通信网络中生成用于获得应用认证和密钥协商(AKMA)服务以在用户设备(UE)与应用功能(AF)之间建立安全接口的应用特定密钥的方法。方法300在网络侧执行。

[0092] 根据本公开的实施例,方法300在步骤301中,应用功能(AF)从UE接收应用会话建立请求消息,其中应用会话建立请求消息包括与KAKMA相关联的AKMA密钥ID、用作外部标识符(GPSI)的第一UE身份参数、路由标识符(RI)和新鲜度参数。作为示例,应用功能(AF)可以是第三方实体,UE的第一应用身份参数可以是GPSI,UE侧的UE标识符可以是密钥ID,以及新鲜度参数CounterAKMA。

[0093] 现在,步骤303,AF基于由网络供应的RI来标识第一网络元件AKMA锚功能(AAnF)。特定地,AF在不脱离本发明的范围的情况下标识被称为第一网络元件的AAnF。

[0094] 在另一实施方式中,第一网络元件(AAnF)发送AKMA密钥请求,该AKMA密钥请求包括UE侧认证令牌、UE侧的UE标识符、第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和新鲜度参数。

[0095] 此后,步骤305,第一网络元件(AAnF)基于RI来选择正确的对应的第二网络元件,该正确的对应的第二网络元件是所请求的UE的认证服务器功能(AUSF)。

[0096] 然后,在步骤307中,AUSF从第三网络元件获得UE的第二UE身份参数,其中第三网络元件提供与第一UE身份参数(SUPI)对应的第二UE身份参数。作为示例,在不脱离本发明的范围的情况下,第三网络元件可以是UDM,并且UE的第二UE身份参数可以是SUPI。

[0097] 此后,在步骤309中,所选择的AUSF基于第一应用身份参数、第二应用身份参数、RI、RAND和新鲜度参数中的至少一者来导出网络侧协商密钥。所选择的AUSF进一步导出用于在网络侧标识UE的订户相关上下文的AKMA服务的AKMA密钥ID。作为示例,在不脱离本发明的范围的情况下,网络侧协商密钥可以是KAKMA,UE标识符可以是在网络侧导出的密钥ID。

[0098] 此后,在步骤311中,AUSF验证网络侧的AKMA密钥ID(密钥ID)与接收到的密钥ID类似。

[0099] 此后,在步骤313中,第一网络元件(AAnF)基于网络侧协商密钥(KAKMA)、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID(RI)和新鲜度参数(CounterAKMA)中的至少一者来导出网络侧应用特定密钥。作为示例,AF ID标识AF的哪个应用正在发出应用会话建立请求。作为示例,在不脱离本发明的范围的情况下,网络侧应用特定密钥可以是KAF。

[0100] 在步骤315中,第一网络元件(AAnF)向应用功能(AF)提供所导出的网络侧应用特定密钥(KAF)以及用于在UE处认证所导出的网络侧应用特定密钥(KAF)以便在UE与应用功能(AF)之间建立安全接口的预定时间段和CounterAF。

[0101] 在另一实施方式中,在步骤315之后,第一网络元件(AAnF)基于由第一网络元件(AAnF)导出的KAF来生成网络侧MAC-I。然后,向AF发送所生产的网络侧MAC-I。此后,第一网络元件AAnF向UE发送包括新鲜度参数和网络侧MAC-I的应用会话建立响应用于进一步认证进程。特定地,AF向UE发送应用会话建立响应以在UE与应用功能(AF)之间建立安全接口。另外,预定时间段和CounterAF也包括在应用会话建立响应中。

[0102] 在又一实施方式中,在步骤315中由AF向UE发送应用会话建立响应之后,UE基于UE

侧协商密钥(KAKMA)、应用ID(AF ID)、第一应用身份参数(GPSI)、路由ID RI和新鲜度参数(CounterAKMA)中的至少一者来生成UE侧应用特定密钥(KAF)。此后,UE在接收到来自AF的应用会话建立响应之后进一步导出UE侧MAC-I。然后,UE验证UE侧MAC-I是否与被称为密钥建立过程的网络侧MAC-I匹配,此后,在验证的成功结果后,UE在UE与应用功能(AF)之间建立安全接口。

[0103] 现在,在实施步骤301之前,UE基于第一应用身份参数(GPSI)、第二应用身份参数(SUPI)、RI和新鲜度参数(CounterAKMA)中的至少一者来生成UE侧协商密钥(KAKMA)。UE进一步基于第一应用身份参数(GPSI)、RI和新鲜度参数(CounterAKMA)中的至少一者来生成UE侧认证令牌(密钥ID)。UE因此在应用会话建立请求消息中进一步向AF提供UE侧认证令牌(密钥ID)的UE标识符。

[0104] 图4图示了根据本公开的实施例的如图3A和图3B中所解释的方法300的详细实施方式。

[0105] 在实施如图2中所描述的步骤301之前的步骤1:UE 401导出密钥KAKMA,如下:

[0106] KAKMA=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0107] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户。

[0108] -UE 401和AUSF 407应将计数器CounterAKMA与密钥KAUSF相关联。对于KAKMA的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入参数,以减轻重放攻击。

[0109] 步骤2:另外,UE 401导出所导出的KAKMA(密钥ID)的身份,如下:

[0110] 密钥ID=KDF(KAUSF、RAND、GPSI、CounterAKMA、其他可能参数)。密钥ID被称为UE侧的UE标识符,这是由于其在UE端处生成。

[0111] 为了导出AKMA服务的新UE标识符以标识UE 401的订户相关上下文,而不发送比如SUCI、GUTI、SUPI的任何3GPP特定身份或由网络供应比如GUTI、恢复ID。密钥ID可以是消息认证令牌并且将由UE和AAnF使用,以标识KAKMA。

[0112] 步骤3与图3A和图3B的步骤301对应:UE 401通过向应用功能发送应用会话建立请求来发起应用会话建立。UE 401在请求消息中包括以下参数中的至少一者:AKMA密钥Id(作为Auth令牌)、GPSI、路由ID、CounterAKMA。

[0113] -UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)。

[0114] -GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0115] 步骤4:在从UE 401接收到应用会话建立请求后,AF 403解析AAnF405,要么到达具有路由ID的NEF要么AF预先配置有AAnF细节。然后,AF 403将具有从UE接收到的相关参数的请求消息中继/转发到AAnF 405。

[0116] 步骤5与图3A和图3B的步骤305对应:在从AF 403接收到请求后,AAnF 405标识拥有UE 401的KAUSF的适当AUSF 407。

[0117] 在实施例中,AAnF 405使用由UE 401提供的路由ID来标识AUSF 407。在替代实施例中,AAnF 405预先配置有要联系的AUSF细节(用于标识和路由)。

[0118] 步骤6与图3A和图3B的步骤307对应:AUSF 407要标识与UE 401对应的KAUSF,这需

要UE 401的SUPI。因此,AUSF 407向UDM 409发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0119] 步骤7:UDM 409向AUSF 407提供与GPSI对应的SUPI和/或订阅数据。

[0120] UDM向AAnF提供409与SUPI对应的GPSI和/或订阅数据。

[0121] 步骤8与图3A和图3B的步骤309、311对应:一旦使用SUPI标识了KAUSF,AUSF 407就导出密钥KAKMA和密钥ID(如步骤1和步骤2中详述的)。

[0122] AUSF 407应仅接受大于所存储的CounterAKMA值的CounterAKMA值。仅如果接收到的Auth令牌的验证成功,AUSF 407才应存储接收到的CounterAKMA。

[0123] AUSF 407验证所导出的Auth令牌是否与接收到的令牌相同。如果相同,那么AUSF继续进行。

[0124] 步骤9:AUSF 407在AKMA密钥响应消息中向AAnF 405提供所导出的密钥KAKMA。

[0125] 步骤10与图3A和图3B的步骤313对应:AAnF 407导出被称为网络侧应用特定密钥的AF特定密钥KAF,如下:

[0126] Kaaf=KDF{KAKMA、GPSI、AF ID、路由指示符、CounterAF、其他可能参数}

[0127] -AF ID的格式如下:

[0128] AF ID=AF||Ua*安全协议标识符的FQDN

[0129] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离。

[0130] -AAnF 405和UE 104应将计数器CounterAF与密钥KAF相关联。对于KAF的每次新的运算,CounterAF应由AAnF 405递增。CounterAF用作KAF推导的新鲜度输入,以减轻重放攻击。

[0131] 步骤11与图3A和图3B的步骤315对应:AAnF 405向AF 403提供所导出的密钥KAF以及显式时间和CounterAF。

[0132] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)

[0133] 锚功能有必要向应用功能通知所导出的Kaaf的有效性。可为Kaaf提供最长使用寿命。当应用密钥使用寿命到期时,应重新协商。

[0134] 步骤12与图3A和图3B的步骤315对应:在从AAnF 405接收到应用密钥响应消息后,AF 403向UE发送应用会话建立响应。响应消息包括CounterAF和在响应消息上导出的MAC-I。

[0135] 步骤13:UE 401在步骤12中由AF向UE发送应用会话建立响应之后导出如步骤10中详述的AF特定密钥KAF(步骤315)。

[0136] 步骤14:使用所导出的密钥KAF,UE 401验证接收到的MAC-I。

[0137] UE 401应仅接受大于所存储的CounterAF值的CounterAF值。仅如果接收到的MAC-I的验证成功,UE才应存储接收到的CounterAF。

[0138] MAC-I用于认证AKMA锚功能。

[0139] 如果验证成功,那么密钥建立过程成功。

[0140] 在另一实施例中,认为应用功能间接(经由NEF)到达5GC网络,即,如果运营商不允许应用功能直接接入网络,那么AF将使用NEF与5GC间接交互。当NEF处理AF请求时,应使用AF服务标识符来授权AF请求。

[0141] 在另一实施例中,认为使用路由标识符标识AAnF是由网络供应的。

[0142] AF ID用于密钥推导、密钥分离和为Kaaf提供新鲜度。

[0143] -AF ID的格式如下:

[0144] AF ID=AF||Ua*安全协议标识符的FQDN

[0145] -其中Ua*安全协议标识符指示哪种安全协议用于UE与应用功能之间的通信。根据应用要求在UE与应用功能之间可以存在多种安全协议正在运行。

[0146] 图5图示了根据本公开的实施例的在图4处实施的方法的替代实施例。将参考图3A、图3B和图4进行解释。本实施例以按位格式定义了UE或网络侧协商密钥(KAKMA)、UE标识符(密钥ID)、UE侧认证令牌的格式。其余步骤与图3A、图3B和图4中解释的相同。另外,出于简洁起见,此处未重复附图标记。在不脱离本发明的范围的情况下,在适当时可以从此处省略进一步的类似步骤。

[0147] 步骤1与如图4中所描述的步骤1对应:UE导出AKMA主密钥KAKMA-MK,如下:

[0148] KAKMA-MK=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0149] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0150] -UE和AUSF应将计数器CounterAKMA与密钥KAUSF相关联。对于KAKMA-MK的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入,以减轻重放攻击。

[0151] -根据本实施例的另一方面,AUSF导出(256位)密钥KAKMA-MK。将所导出的密钥KAKMA-MK的一部分当作KAKMA、密钥ID和Auth令牌。出于说明的目的,KAKMA用KDF的输出(KAKMA-MK)的128个最低有效位(LSB)来标识,密钥ID用KDF的输出的3个最高有效位(MSB)来标识,并且将KDF的输出的接下来的64个最高有效位(MSB)标识为认证令牌。

[0152] 在该变体中,密钥ID不是单独导出的,而是将MSB 3位视为密钥ID,并且还将接下来的64个MSB位视为Auth令牌。

[0153] 步骤2与图4的步骤3对应:UE通过向应用功能发送应用会话建立请求来发起应用会话建立。UE在请求消息中包括以下参数中的至少一者:AKMA密钥Id、Auth令牌、GPSI、路由ID、CounterAKMA。

[0154] -UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)。

[0155] GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0156] 步骤3与图4的步骤4对应:在从UE接收到应用会话建立请求后,AF解析AAnF,要么到达具有路由ID的NEF要么AF预先配置有AAnF细节。然后,AF将具有从UE接收到的相关参数的请求消息中继/转发到AAnF。

[0157] 步骤4与图4的步骤5对应:在从AF接收到请求后,AAnF标识拥有UE的KAUSF的适当AUSF。AAnF使用由UE提供的路由ID标识AUSF。

[0158] 步骤5与图4的步骤6对应:AUSF要标识与UE对应的KAUSF,需要UE的SUPI。因此,AUSF向UDM发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0159] 步骤6与图4的步骤7对应:UDM向AUSF提供与GPSI对应的SUPI和/或订阅数据。

[0160] 步骤7与图4的步骤8对应:一旦使用SUPI标识了KAUSF,AUSF就导出密钥KAKMA和密钥ID(如步骤1中详述的)。

[0161] AUSF应仅接受大于所存储的CounterAKMA值的CounterAKMA值。仅如果接收到的Auth令牌的验证成功,AUSF才应存储接收到的CounterAKMA。

[0162] AUSF验证所导出的Auth令牌是否与接收到的令牌相同。如果相同,那么AUSF继续进行。

[0163] 步骤8与图4的步骤9对应:AUSF在AKMA密钥响应消息中向AAnF提供所导出的密钥KAKMA。

[0164] 步骤9与图4的步骤10对应:AAnF导出AF特定密钥KAF,如下:

[0165] Kaaf=KDF{KAkma、GPSI、路由指示符、AF ID、CounterAF、其他可能参数}

[0166] -AF ID的格式如下:

[0167] AF ID=AF||Ua*安全协议标识符的FQDN

[0168] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离。

[0169] -AAnF和UE应将计数器CounterAF与密钥KAF相关联。对于KAF的每次新的运算,CounterAF应由AAnF递增。CounterAF用作KAF推导的新鲜度输入,以减轻重放攻击。

[0170] -在用于导出应用特定密钥的该变体中,由AF提供的AF ID也用作用于导出应用密钥的输入参数中的一者。

[0171] 步骤10与图4的步骤11对应:AAnF向AF提供所导出的密钥KAF以及显式时间和CounterAF。

[0172] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)

[0173] 步骤11与图4的步骤12对应:在从AAnF接收到应用密钥响应消息后,AF向UE发送应用会话建立响应。响应消息包括CounterAF和在响应消息上导出的MAC-I。

[0174] 步骤12与图4的步骤13对应:UE导出如步骤9中详述的AF特定密钥KAF。

[0175] 步骤13与图4的步骤14对应:使用所导出的密钥KAF,UE验证接收到的MAC-I。

[0176] UE应仅接受大于所存储的CounterAF值的CounterAF值。仅如果接收到的MAC-I的验证成功,UE才应存储接收到的CounterAF。

[0177] MAC-I用于认证AKMA锚功能。

[0178] 如果验证成功,那么密钥建立过程成功。

[0179] 图6图示了根据本公开的实施例的在图4处实施的方法的替代实施例。将参考图3A、图3B、图4和图5进行解释。本实施例以按位格式定义了UE或网络侧协商密钥(KAKMA)、UE标识符(密钥ID)、UE侧认证令牌的格式。其余步骤与图3A、图3B和图4中解释的相同。出于简洁起见,此处未重复附图标记。在不脱离本发明的范围的情况下,在适当时可以从此处省略进一步的类似步骤。

[0180] 在实施如图2中所描述的步骤301之前步骤1:UE导出AKMA主密钥KAKMA-MK,如下:

[0181] KAKMA-MK=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0182] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0183] -根据该实施例的另一方面,UE和AUSF应将计数器CounterAKMA(其也被视为AKMA密钥ID)与密钥KAUSF相关联。对于KAKMA的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入,以减轻重放攻击。此外,CounterAKMA(在等效于密钥ID时)是消息认证令牌并且将由UE和AAnF使用,以标识KAKMA。

[0184] -根据本实施例的另一方面,AUSF导出(256位)密钥KAKMA-MK。将所导出的密钥KAKMA-MK的一部分当作KAKMA和Auth令牌。出于说明的目的,KAKMA用KDF的输出(KAKMA-MK)的128个最低有效位(LSB)标识,并且将KDF的输出的64个最高有效位(MSB)标识为认证令牌。将CounterAKMA的值当作AKMA密钥ID的值。

[0185] 步骤2与图4的步骤3对应:UE通过向应用功能发送应用会话建立请求来发起应用会话建立。UE在请求消息中包括以下参数中的至少一者:Auth令牌、GPSI、路由ID、CounterAKMA。

[0186] -UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)。

[0187] GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0188] 步骤3与图4的步骤4对应:在从UE接收到应用会话建立请求后,AF解析AAnF,要么到达具有路由ID的NEF要么AF预先配置有AAnF细节。然后,AF将具有从UE接收到的相关参数的请求消息中继/转发到AAnF。

[0189] 步骤4与图4的步骤5对应:在从AF接收到请求后,AAnF标识拥有UE的KAUSF的适当AUSF。AAnF使用由UE提供的路由ID标识AUSF。

[0190] 步骤5与图4的步骤6对应:AUSF要标识与UE对应的KAUSF,需要UE的SUPI。因此,AUSF向UDM发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0191] 步骤6与图4的步骤7对应:UDM向AUSF提供与GPSI对应的SUPI和/或订阅数据。

[0192] 步骤7与图4的步骤8对应:一旦使用SUPI标识了KAUSF,AUSF就导出密钥KAKMA和密钥ID(如步骤1中详述的)。

[0193] AUSF应仅接受大于所存储的CounterAKMA值的CounterAKMA值。仅如果接收到的Auth令牌的验证成功,AUSF才应存储接收到的CounterAKMA。

[0194] AUSF验证所导出的Auth令牌是否与接收到的令牌相同。如果相同,那么AUSF继续进行。

[0195] 步骤8与图4的步骤9对应:AUSF在AKMA密钥响应消息中向AAnF提供所导出的密钥KAKMA。

[0196] 步骤9与图4的步骤10对应:AAnF导出AF特定密钥KAF,如下:

[0197] Kaaf=KDF{KAkma、GPSI、AF ID、CounterAF、其他可能参数}

[0198] -AF ID的格式如下:

[0199] AF ID=AF||Ua*安全协议标识符的FQDN

[0200] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离

[0201] -AAnF和UE应将计数器CounterAF与密钥KAF相关联。对于KAF的每次新的运算,CounterAF应由AAnF递增。CounterAF用作KAF推导的新鲜度输入,以减轻重放攻击。

[0202] -在用于导出应用特定密钥的该变体中,由AF提供的AF ID也用作用于导出应用密

钥的输入参数中的一者。

[0203] 步骤10与图4的步骤11对应:AAnF向AF提供所导出的密钥KAF以及显式时间和CounterAF。

[0204] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)。

[0205] 步骤11与图4的步骤12对应:在从AAnF接收到应用密钥响应消息后,AF向UE发送应用会话建立响应。响应消息包括CounterAF和在响应消息上导出的MAC-I。

[0206] 步骤12与图4的步骤13对应:UE导出如步骤9中详述的AF特定密钥KAF。

[0207] 步骤13与图4的步骤14对应:使用所导出的密钥KAF,UE验证接收到的MAC-I。

[0208] UE应仅接受大于所存储的CounterAF值的CounterAF值。仅如果接收到的MAC-I的验证成功,UE才应存储接收到的CounterAF。

[0209] MAC-I用于认证AKMA锚功能。

[0210] 如果验证成功,那么密钥建立过程成功。

[0211] 图7图示了根据本公开的实施例的在图4处实施的方法的替代实施例。将参考图3A、图3B、图4、图5和图6进行解释。根据本公开的实施例,AAnF在不通过AUSF进行干预的情况下与第三网络元件UDM/SMF/PCF进行通信。另外,AAnF对标识参数执行附加授权检查。其余步骤与图3A、图3B、图4、图5和图6中解释的保持相同。下面将详细解释其消息流。出于简洁起见,此处未重复附图标记。在不脱离本发明的范围的情况下,在适当时可以从此处省略进一步的类似步骤。

[0212] 步骤1与如图4中所描述的步骤1对应:UE导出AKMA主密钥KAKMA-MK,如下:

[0213] KAKMA-MK=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0214] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0215] -根据该实施例的另一方面,UE和AUSF应将计数器CounterAKMA(其也被视为AKMA密钥ID)与密钥KAUSF相关联。对于KAKMA的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入,以减轻重放攻击。此外,CounterAKMA(在等效于密钥ID时)是消息认证令牌并且将由UE和AAnF使用,以标识KAKMA

[0216] -AUSF导出(256位)密钥KAKMA-MK。将所导出的密钥KAKMA-MK的一部分当作KAKMA和Auth令牌。出于说明的目的,KAKMA用KDF的输出(KAKMA-MK)的128个最低有效位(LSB)标识,并且将KDF的输出的64个最高有效位(MSB)标识为认证令牌。将CounterAKMA的值当作AKMA密钥ID的值。

[0217] 步骤2与图4的步骤3对应:UE通过向应用功能发送应用会话建立请求来发起应用会话建立。UE在请求消息中包括以下参数中的至少一者:Auth令牌、GPSI、路由ID、CounterAKMA。

[0218] UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)。

[0219] GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0220] 步骤3与图4的步骤4对应:在从UE接收到应用会话建立请求后,AF解析AAnF,要么到达具有路由ID的NEF要么AF预先配置有AAnF细节。然后,AF将具有从UE接收到的相关参数的请求消息中继/转发到AAnF。

[0221] 步骤4:AAnF使用由UE提供的路由ID标识UDM。另外,为使AUSF标识与UE对应的KAUSF,需要UE的SUPI。因此,AAnF在不通过AUSF进行干预的情况下直接向UDM发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0222] 步骤5:UDM向AAnF提供与GPSI对应的SUPI和/或订阅数据。

[0223] UDM向AAnF提供409与SUPI对应的GPSI和/或订阅数据。

[0224] 步骤6:如果在步骤5中接收到,那么AAnF基于接收到的订阅数据来进行UE的授权检查。否则,跳过该步骤。如果授权检查由AAnF进行,那么仅如果授权检查成功,AAnF才会继续进行以下步骤,否则AAnF拒绝请求。

[0225] 步骤7与图4的步骤5对应:AAnF向UDM发送AKMA密钥请求。AAnF在请求中包括以下参数:Auth令牌、GPSI、SUPI、路由ID、CounterAKMA、其他可能参数。

[0226] 步骤8与图4的步骤8对应:AUSF导出KAKMA如下(与由UE导出的步骤1类似):

[0227] KAKMA=KDF{KAUSF、RAND、GPSI、路由指示符、SUPI、CounterAKMA、其他可能参数}

[0228] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0229] AUSF验证所导出的Auth令牌是否与接收到的令牌相同。如果相同,那么AUSF继续进行。

[0230] 步骤9与图4的步骤9对应:AUSF在AKMA密钥响应消息中向AAnF提供所导出的密钥KAKMA和密钥ID/CounterAKMA。

[0231] 步骤10与图4的步骤10对应:在从AUSF接收到AKMA密钥响应消息后,AAnF如下导出Kaaf:

[0232] Kaaf=KDF{KAKMA、GPSI、AF ID、Counteraaf}

[0233] -AF ID的格式如下:

[0234] AF ID=AF||Ua*安全协议标识符的FQDN

[0235] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离

[0236] 步骤11与图4的步骤11对应:AAnF向应用功能发送应用密钥响应。该消息中所包括的参数是:AKMA密钥ID(CounterAKMA)、Kaaf、exp时间、Counteraaf、其他可能参数。

[0237] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)

[0238] 步骤12与图4的步骤12对应:在从AAnF接收到应用密钥响应消息后,AF向UE发送应用会话建立响应。响应消息包括AKMA密钥ID、CounterAF和在响应消息上导出的MAC-I。

[0239] 步骤13与图4的步骤13对应:UE导出如步骤10中详述的AF特定密钥KAF。

[0240] 步骤14与图4的步骤14对应:使用所导出的密钥KAF,UE验证接收到的MAC-I。

[0241] UE应仅接受大于所存储的CounterAF值的CounterAF值。

[0242] 仅如果接收到的MAC-I的验证成功,UE才应存储接收到的CounterAF。

[0243] MAC-I用于认证AKMA锚功能。

[0244] 如果验证成功,那么密钥建立过程成功。

[0245] 图8图示了根据本公开的实施例的在图4处实施的方法的替代实施例。将通过参考图3A、图3B、图4、图5、图6和图7进行解释。根据本公开的实施例,KAKMA可以由AUSF导出。另外,根据本发明的实施例,AF导出MAC-I并且验证该MAC-I。其余步骤与图4和图7中解释的相

同。出于简洁起见,此处未重复附图标记。在不脱离本发明的范围的情况下,在适当时可以从此处省略进一步的类似步骤。下面将详细解释其消息流。

[0246] 步骤1与图4的步骤1对应:UE导出密钥KAKMA,如下:

[0247] KAKMA=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0248] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0249] -UE和AUSF应将计数器CounterAKMA与密钥KAUSF相关联,其中CounterAKMA被视为AKMA密钥ID。对于KAKMA的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入,以减轻重放攻击。此外,CounterAKMA(在等效于密钥ID时)是消息认证令牌并且将由UE和AAnF使用,以标识KAKMA。

[0250] 步骤2与图4的步骤2对应:另外,UE导出AKMA应用功能的密钥如下:

[0251] Kaaf=KDF(KAkma、GPSI、CounterAKMA、AF ID、CounterAF、其他可能参数)

[0252] -AF ID的格式如下:

[0253] AF ID=AF||Ua*安全协议标识符的FQDN

[0254] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离

[0255] -UE和AAnF应将计数器CounterAF与密钥KAF相关联。对于KAF的每次新的运算,CounterAF应由UE递增。CounterAF用作KAF推导的新鲜度输入,以减轻重放攻击。

[0256] 步骤3:根据实施例,UE计算或导出请求消息的MAC-I如下:

[0257] MAC-I=AES(Kaaf,<请求消息>)

[0258] 通过使用所支持的算法中的任一者来导出MAC-I。该MAC-I在该过程中用于检查AKMA锚功能的真实性。

[0259] 步骤4与图4的步骤3对应:UE通过向应用功能发送应用会话建立请求来发起应用会话建立。UE在请求消息中包括以下参数:MAC-I、GPSI、路由ID、Counteraaf、CounterAKMA。

[0260] -UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)。

[0261] -GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0262] -Counteraaf和CounterAKMA用作用于导出KAAF和KAKMA的新鲜度参数,

[0263] -在会话建立请求中添加请求UE的MAC-I并且向AF发送该MAC-I以进行进一步的验证过程。

[0264] 步骤5与图4的步骤4对应:在从UE接收到应用会话建立请求后,AF解析AAnF,要么到达具有路由ID的NEF要么AF预先配置有AAnF细节。然后,AF将具有从UE接收到的相关参数的请求消息中继/转发到AAnF。

[0265] 步骤6:AAnF使用由UE提供的路由ID标识UDM。另外,为使AUSF标识与UE对应的KAUSF,需要UE的SUPI。因此,AAnF向UDM发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0266] 步骤7:UDM向AAnF提供与GPSI对应的SUPI和/或订阅数据。

[0267] 步骤8:如果在步骤7中接收到,那么AAnF基于接收到的订阅数据来进行UE的授权检查。否则,跳过该步骤。如果授权检查由AanF执行,那么仅如果授权检查成功,AAnF才会继

续进行以下步骤,否则AAnF拒绝请求。

[0268] 步骤9与图4的步骤5对应:AAnF向AUSF发送AKMA密钥请求。AAnF在请求中包括以下参数:Auth令牌、GPSI、SUPI、路由ID、CounterAKMA、其他可能参数。

[0269] 步骤10:AUSF导出KAKMA如下:

[0270] KAKMA=KDF{KAUSF、RAND、GPSI、路由指示符、SUPI、CounterAKMA、其他可能参数}

[0271] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0272] 步骤11与图4的步骤9对应:AUSF在AKMA密钥响应消息中向AAnF提供所导出的密钥KAKMA和AKMA密钥ID/CounterAKMA。

[0273] 步骤12与图4的步骤10对应:在从AUSF接收到AKMA密钥响应消息后,AAnF导出Kaaf如下:

[0274] Kaaf=KDF{KAKMA、GPSI、AF ID、Counteraaf、其他可能参数}

[0275] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)

[0276] 步骤13与图4的步骤11对应:AAnF向应用功能发送应用密钥响应。该消息中所包括的参数是:AKMA密钥ID(CounterAKMA)、Kaaf、显式时间、Counteraaf、其他可能参数。

[0277] 步骤14:使用所导出的密钥Kaaf,AF验证从UE接收到的MAC-I。

[0278] 步骤15:在成功验证后,AF在应用会话建立响应消息上导出MAC-I。

[0279] 步骤16与图4的步骤12对应:AF向UE发送应用会话建立响应。响应消息包括AKMA密钥ID(CounterAKMA)、CounterAF、在响应消息上导出的MAC-I和其他可能参数。

[0280] 步骤17与图4的步骤14对应:使用所导出的密钥KAF,UE验证接收到的MAC-I。

[0281] UE仅接受大于所存储的CounterAF值的CounterAF值。仅如果接收到的MAC-I的验证成功,UE才存储接收到的CounterAF。

[0282] 如果验证成功,那么密钥建立过程成功。

[0283] 图9图示了根据本公开的实施例的在图4处实施的方法的替代实施例。将通过参考图3A、图3B、图4、图5、图6、图7和图8进行解释。出于简洁起见,此处未重复附图标记。在不脱离本发明的范围的情况下,在适当时可以从此处省略进一步的类似步骤。

[0284] 步骤1与图4的步骤1对应:UE导出密钥KAKMA,如下:

[0285] KAKMA-MK=KDF(KAUSF、RAND、GPSI、路由指示符(RI)、SUPI、CounterAKMA、其他可能参数)

[0286] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0287] -从所导出的256位长的KAKMA-MK中,至少128位可以被视为KAKMA,并且CounterAKMA是AKMA密钥ID。对于KAKMA的每次新的运算,CounterAKMA应由UE递增。CounterAKMA用作KAKMA推导的新鲜度输入,以减轻重放攻击。此外,CounterAKMA(在等效于密钥ID时)是消息认证令牌并且将由UE和AAnF使用,以标识KAKMA。

[0288] 步骤2:另外,UE如下导出认证令牌:

[0289] Auth令牌=KDF{KAKMA、GPSI、RI、CounterAKMA、其他可能参数}

[0290] 步骤3与图4的步骤3对应:UE通过向应用功能发送应用会话建立请求来发起应用会话建立。UE在请求消息中包括以下参数:Auth令牌、GPSI、路由ID、CounterAKMA、其他可能

参数。

[0291] -UE包括由HPLMN供应的路由ID,以标识适当AUSF(其拥有密钥KAUSF)或UDM。

[0292] -GPSI是UE的在AKMA服务中唯一地标识UE的ID。

[0293] -CounterAKMA用作用于导出CounterAKMA的新鲜度参数,

[0294] 步骤4与图4的步骤4对应:在从UE接收到应用会话建立请求后,AF将具有从UE接收到的相关参数的请求消息中继/转发到AAnF。

[0295] 步骤5:AAnF使用由UE提供的路由ID标识UDM。另外,为使AUSF标识与UE对应的KAUSF,需要UE的SUPI。因此,AAnF向UDM发起请求,以获得与GPSI对应的SUPI和/或订阅数据(其包含SUPI和GSPI的映射)。

[0296] 步骤6:UDM向AAnF提供与GPSI对应的SUPI和/或订阅数据。

[0297] 步骤7:如果在步骤6中接收到,那么AAnF基于接收到的订阅数据来执行UE的授权检查。否则,跳过该步骤。如果授权检查由AAnF进行,那么仅如果授权检查成功,AAnF才会继续进行以下步骤,否则AAnF拒绝请求。

[0298] 步骤8与图4的步骤5对应:AAnF向UDM发送AKMA密钥请求。AAnF在请求中包括以下参数:Auth令牌、GPSI、SUPI、路由ID、CounterAKMA、其他可能参数。

[0299] 步骤9:AUSF导出KAKMA(与步骤1类似)如下:

[0300] KAKMA=KDF{KAUSF、RAND、GPSI、路由指示符、SUPI、CounterAKMA、其他可能参数}

[0301] SUPI作为导出KAKMA的输入参数中的一者而被提供,其用于区分正在请求各种AKMA服务的每个订户

[0302] 步骤10:AUSF向AAnF提供所导出的密钥KAKMA和CounterAKMA。

[0303] 步骤11:AAnF验证在请求消息中接收到的Auth令牌(步骤4)。

[0304] 步骤12:在成功验证后,AAnF导出Kaaf如下:

[0305] Kaaf=KDF{KAKMA、GPSI、AF ID、Counteraaf、其他可能参数}

[0306] -AF ID的格式如下:

[0307] AF ID=AF||Ua*安全协议标识符的FQDN

[0308] AF ID用于标识AF正在发出请求的应用。以这种方式,通过添加AF ID作为KAF推导的输入参数中的一者,实现了密钥分离。

[0309] 步骤13与图4的步骤11对应:AAnF向应用功能发送应用密钥响应。该消息中所包括的参数是AKMA密钥ID(CounterAKMA)、Kaaf、显式时间、Counteraaf、其他可能参数。

[0310] 如果KAF密钥在AAnF中已经对UE可用,那么AAnF将跳过向AUSF请求密钥(KAF)

[0311] 步骤14与图4的步骤11对应:在接收到应用密钥响应后,AF向UE发起响应消息。

[0312] 步骤15与图4的步骤13对应:在接收到响应消息后,UE与步骤12类似地导出Kaaf。

[0313] 步骤16与图4的步骤14对应:使用所导出的密钥KAF,UE验证接收到的MAC-I。

[0314] UE仅接受大于所存储的CounterAF值的CounterAF值。仅如果接收到的MAC-I的验证成功,UE才存储接收到的CounterAF。

[0315] 如果验证成功,那么密钥建立过程成功。

[0316] 在实施例中,UE接入AKMA服务的授权由AAnF使用从UDM接收到的UE的订阅数据或服务简档来执行。

[0317] 在另一实施例中,UE接入AKMA服务的授权由AUSF使用从UDM接收到的UE的订阅数

据或服务简档来执行。

[0318] 在实施例中,AAnF使用由UE提供的路由ID标识AUSF。

[0319] 在实施例中,UE的GPSI或AKMA应用ID(由网络分配为对AKMA服务的订阅的一部分)或UE的应用ID或UE的公共ID到永久ID(例如SUPI)的映射通过以下操作执行:由AAnF或AUSF从UDM或5GC中的任何其他网络实体(例如AMF、SMF或PCF)获得订阅数据或服务简档。

[0320] 在实施例中,AKMA密钥ID是路由ID||CounterAKMA的串接。

[0321] 在实施例中,KAAF的密钥ID是路由ID||CounterAAF的串接。在本文中,路由ID是由本地网络运营商分配并且在USIM中供应的值,这允许与本地网络标识符一起将网络/应用信令路由到能够为订户(UE)服务的AUSF和/或UDM实例。

[0322] 图10是实施3GPP和5G技术的无线通信系统的实施方式。如图中所示出,gNode B 1001和eNode B可以彼此共存并且可以与UE 1009交互。另外,gNode B 1001和eNode B可以包括配置为与UE 1009交互的发送器/接收器1003。gNode B 1001和eNode B可以进一步包括具有一个或多个网络元件的多个网络节点。一个或多个网络元件包括与存储器耦合的一个或多个处理器1005以实施如图3A至图10中所示出的方法。因此,出于简洁起见,在本文中未对此进行公开。

[0323] 在示例中,处理器1005可以是单个处理单元或多个单元,所有这些单元都可以包括多个计算单元。处理器203可以实施为一个或多个微处理器、微型计算机、微控制器、数字信号处理器、中央处理单元、状态机、逻辑电路系统和/或基于操作指令来操纵信号的任何设备。在其他能力中,处理器1005配置为获取和执行存储在存储器中的计算机可读指令和数据。处理器可以包括一个或多个处理器。此时,一个或多个处理器可以是通用处理器,诸如中央处理单元(CPU)、应用处理器(AP)等;仅图形处理单元,诸如图形处理单元(GPU)、视觉处理单元(VPU);和/或AI专用处理器,诸如神经处理单元(NPU)。一个或多个处理器根据存储在非易失性存储器和易失性存储器中的预定义操作规则或人工智能(AI)模型来控制输入数据的处理。通过训练或学习来提供预定义操作规则或人工智能模型。

[0324] 作为示例,一个或多个网络元件可以用一个或多个处理器来实施。作为示例,各种网络元件可以包括但不限于AF、AAnF、AUSF、UDM/SMF/PCF。

[0325] 存储器可以包括本领域中已知的任何非暂时性计算机可读介质,包括例如易失性存储器,诸如静态随机存取存储器(SRAM)和动态随机存取存储器(DRAM);和/或非易失性存储器,诸如只读存储器(ROM)、可擦除可编程ROM、闪速存储器、硬盘、光盘和磁带。

[0326] 发送器/接收器1003可以是发送器和接收器单元。发送器/接收器1003可以经由诸如3G、4G、5G等无线标准中的任一者与用户和/或其他IoT设备进行通信,也可以使用诸如Wi-FI、蓝牙等其他无线技术。此外,任何流程图的动作都不需要按所示出的顺序实施;也不一定需要进行所有行为。此外,不依赖于其他行为的那些行为可以与其他行为并行进行。实施例的范围决不受这些具体示例限制。诸如结构、尺寸和材料使用的差异的许多变化(无论是否在说明书中明确给出)都是可能的。实施例的范围至少与以下权利要求所给出的范围一样广泛。

[0327] 图11图示了根据本公开的实施例的网络实体。

[0328] 参考图11,网络实体1100可以包括处理器1110、收发器1120和存储器1130。然而,所有所图示的组件都不是必需的。网络实体1100可以由比图11中所图示的组件更多或更少

的组件来实施。此外,根据另一实施例,处理器1110和收发器1120以及存储器1130可以实施为单个芯片。

[0329] 现在将详细描述前述组件。

[0330] 处理器1110可以包括控制所提出的功能、进程和/或方法的一个或多个处理器或其他处理设备。网络实体1100的操作可以由处理器1110实施。

[0331] 收发器1120可以包括用于对所发送的信号进行上变频和放大的RF发送器和用于对接收到的信号的频率进行下变频的RF接收器。然而,根据另一实施例,收发器1120可以由比组件中所图示的组件更多或更少的组件来实施。

[0332] 收发器1120可以连接到处理器1110并且发送和/或接收信号。信号可以包括控制信息和数据。此外,收发器1120可以通过无线信道接收信号并且将信号输出到处理器1110。收发器1120可以通过无线信道发送从处理器1110输出的信号。

[0333] 存储器1130可以存储由网络实体1100获得的信号中所包括的控制信息或数据。存储器1130可以连接到处理器1110并且存储用于所提出的功能、进程和/或方法的至少一个指令或协议或参数。存储器1130可以包括只读存储器(ROM)和/或随机存取存储器(RAM)和/或硬盘和/或CD-ROM和/或DVD和/或其他存储设备。

[0334] 图12图示了根据本公开的实施例的用户设备(UE)。

[0335] 参考图12,UE 1200可以包括处理器1210、收发器1220和存储器1230。然而,所有所图示的组件都不是必需的。UE 1200可以由比图12中所图示的组件更多或更少的组件来实施。此外,根据另一实施例,处理器1210和收发器1220以及存储器1230可以实施为单个芯片。

[0336] 现在将详细描述前述组件。

[0337] 处理器1210可以包括控制所提出的功能、进程和/或方法的一个或多个处理器或其他处理设备。UE 1200的操作可以由处理器1210实施。

[0338] 收发器1220可以包括用于对所发送的信号进行上变频和放大的RF发送器和用于对接收到的信号的频率进行下变频的RF接收器。然而,根据另一实施例,收发器1220可以由比组件中所图示的组件更多或更少的组件来实施。

[0339] 收发器1220可以连接到处理器1210并且发送和/或接收信号。信号可以包括控制信息和数据。此外,收发器1220可以通过无线信道接收信号并且将信号输出到处理器1210。收发器1220可以通过无线信道发送从处理器1210输出的信号。

[0340] 存储器1230可以存储由UE 1200获得的信号中所包括的控制信息或数据。存储器1230可以连接到处理器1210并且存储用于所提出的功能、进程和/或方法的至少一个指令或协议或参数。存储器1230可以包括只读存储器(ROM)和/或随机存取存储器(RAM)和/或硬盘和/或CD-ROM和/或DVD和/或其他存储设备。

[0341] 上面已经针对具体实施例描述了益处、其他优点和问题的解决方案。然而,益处、优点、问题的解决方案和可以使任何益处、优点或解决方案出现或变得更加明显的任何组件不应被解释为任何或所有权利要求的关键、所需或基本特征或组件。

[0342] 虽然已经使用特定语言来描述本主题,但不旨在对此产生任何限制。如对于本领域的技术人员显而易见,可对方法进行各种工作修改以便实施如本文中所教导的本发明构思。图式和前述描述给出了实施例的示例。本领域的技术人员应了解,所描述的元件中的一

者或多者可以良好地组合成单个功能元件。替代地,某些元件可以拆分成多个功能元件。来自一个实施例的元件可以添加到另一实施例。

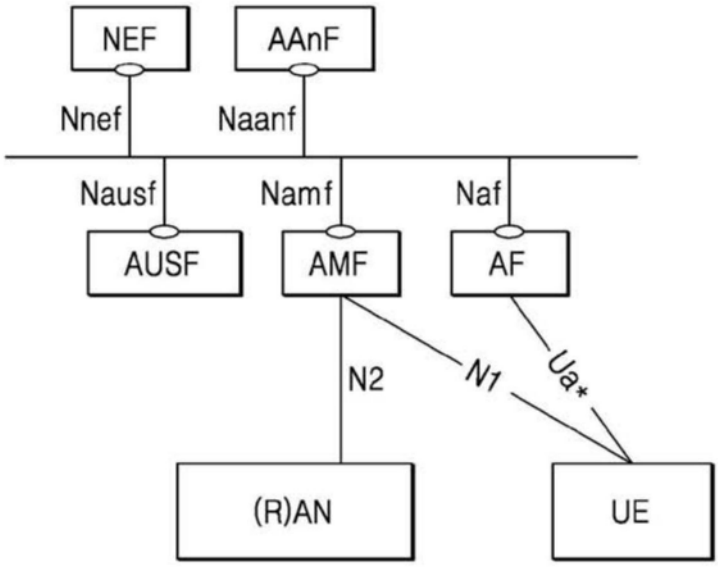

NEF
AAnF
Nnef
Naanf
Nausf
Namf
Naf
AUSF
AMF
AF
N2
N1
Ua*
(R)AN
UE

图1

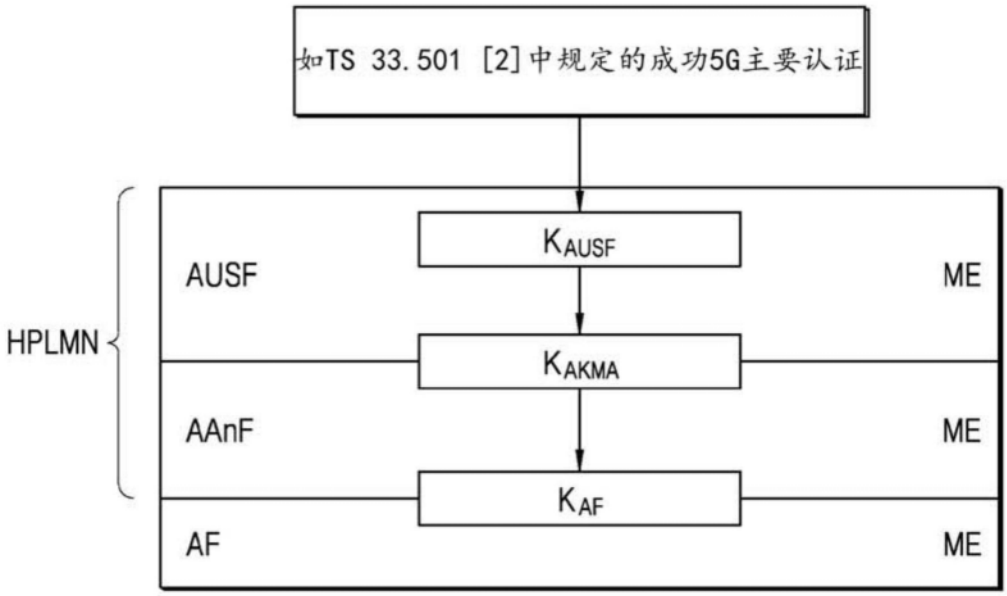

如TS 33.501 [2]中规定的成功5G主要认证
HPLMN
AUSF
ME
K_{AUSF}
K_{AKMA}
AAnF
ME
K_{AF}
AF
ME

图2

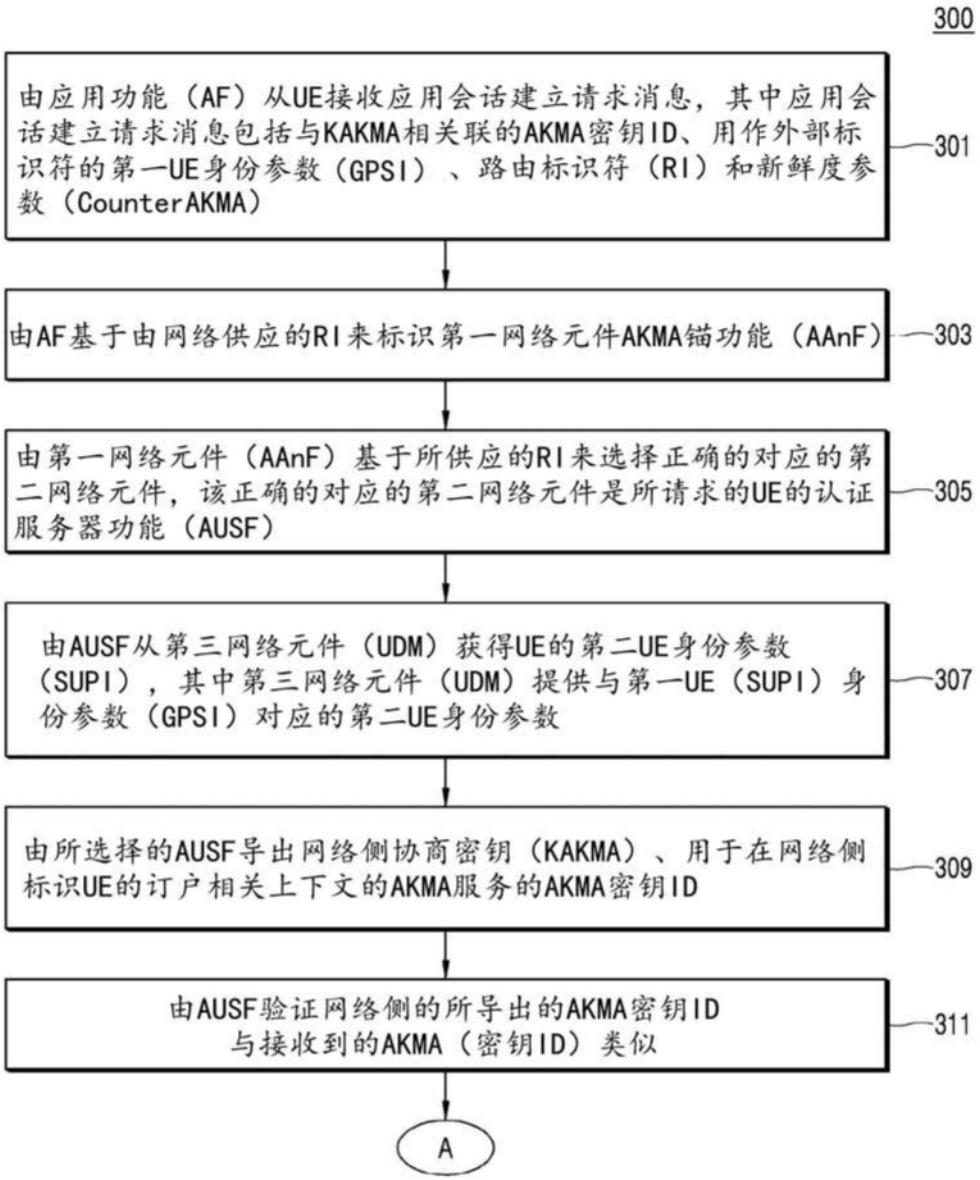

300
由应用功能（AF）从UE接收应用会话建立请求消息，其中应用会话建立请求消息包括与KAKMA相关联的AKMA密钥ID、用作外部标识符的第一UE身份参数（GPSI）、路由标识符（RI）和新鲜度参数（CounterAKMA）
301
由AF基于由网络供应的RI来标识第一网络元件AKMA锚功能（AAnF）
303
由第一网络元件（AAnF）基于所供应的RI来选择正确的对应的第二网络元件，该正确的对应的第二网络元件是所请求的UE的认证服务器功能（AUSF）
305
由AUSF从第三网络元件（UDM）获得UE的第二UE身份参数（SUPI），其中第三网络元件（UDM）提供与第一UE（SUPI）身份参数（GPSI）对应的第二UE身份参数
307
由所选择的AUSF导出网络侧协商密钥（KAKMA）、用于在网络侧标识UE的订户相关上下文的AKMA服务的AKMA密钥ID
309
由AUSF验证网络侧的所导出的AKMA密钥ID与接收到的AKMA（密钥ID）类似
311
A

图3A

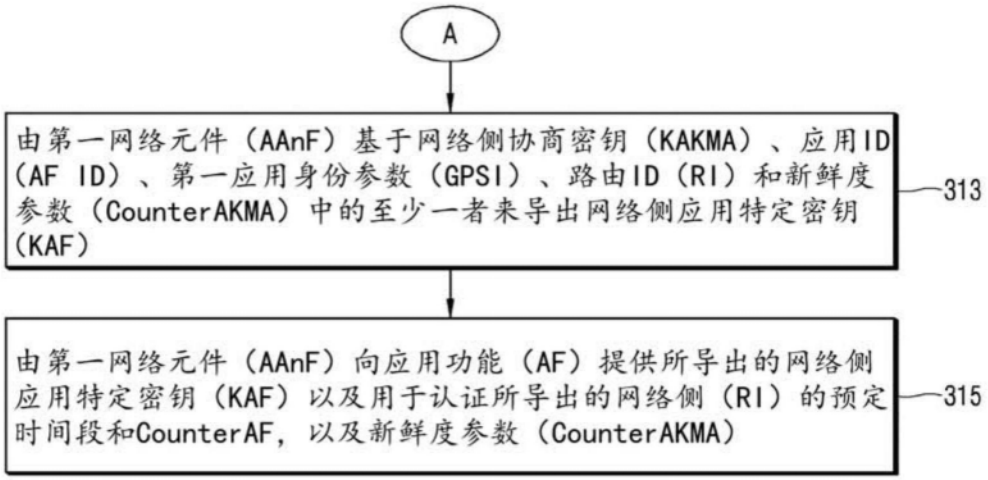

A
由第一网络元件（AAnF）基于网络侧协商密钥（KAKMA）、应用ID（AF ID）、第一应用身份参数（GPSI）、路由ID（RI）和新鲜度参数（CounterAKMA）中的至少一者来导出网络侧应用特定密钥（KAF）
313
由第一网络元件（AAnF）向应用功能（AF）提供所导出的网络侧应用特定密钥（KAF）以及用于认证所导出的网络侧（RI）的预定时间段和CounterAF，以及新鲜度参数（CounterAKMA）
315

图3B

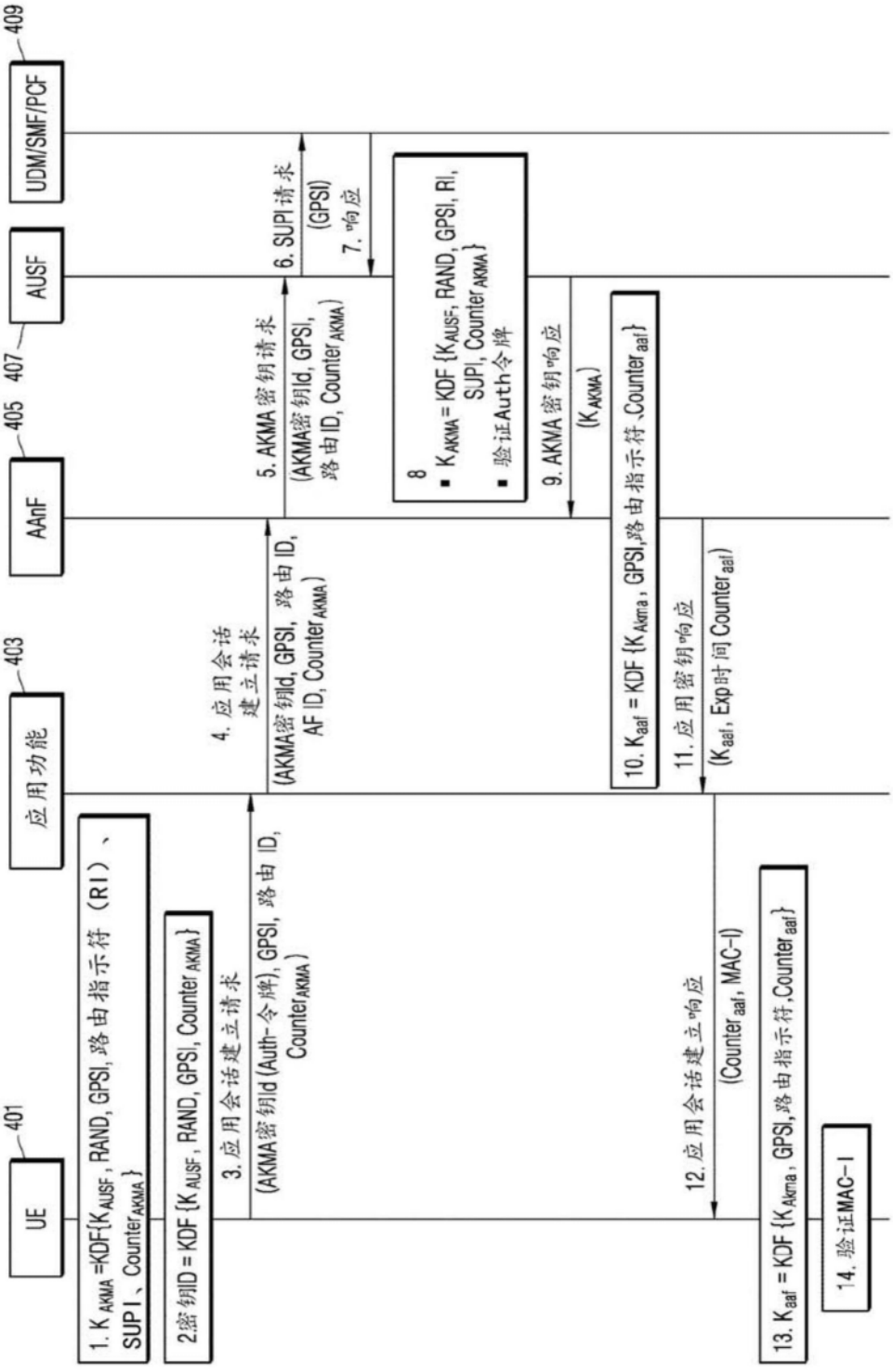

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K AKMA =KDF{K AUSF , RAND, GPSI, 路由指示符（RI）、SUPI、Counter AKMA }
2.密钥ID = KDF {K AUSF , RAND, GPSI, Counter AKMA }
3. 应用会话建立请求
(AKMA密钥Id (Auth-令牌), GPSI, 路由 ID, Counter AKMA)
4. 应用会话建立请求
(AKMA密钥Id, GPSI, 路由 ID, AF ID, Counter AKMA)
5. AKMA 密钥请求
(AKMA密钥Id, GPSI, 路由 ID, Counter AKMA)
6. SUPI 请求
(GPSI)
7. 响应
8
K AKMA = KDF {K AUSF , RAND, GPSI, RI, SUPI, Counter AKMA }
验证Auth令牌
9. AKMA 密钥响应
(K AKMA)
10. K aaf = KDF {K Akma , GPSI,路由指示符 ,Counter aaf }
11. 应用密钥响应
(K aaf , Exp时间 Counter aaf)
12. 应用会话建立响应
(Counter aaf , MAC-I)
13. K aaf = KDF {K Akma , GPSI,路由指示符 ,Counter aaf }
14. 验证MAC-I

图4

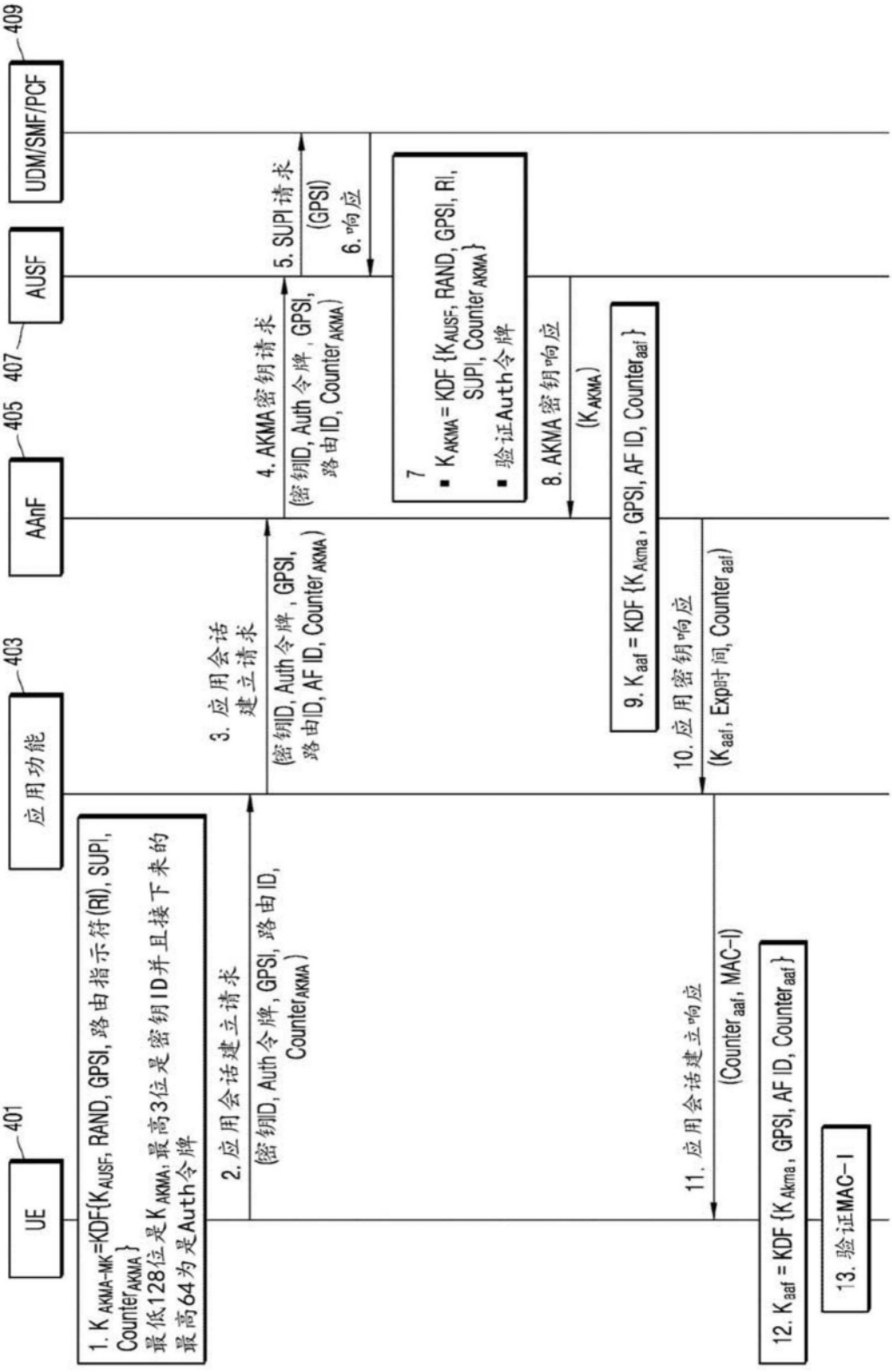

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K AKMA-MK=KDF(K AUSF, RAND, GPSI, 路由指示符(RI), SUPI, Counter AKMA }
最低128位是K AKMA; 最高3位是密钥ID并且接下来的最高64为是Auth令牌
2. 应用会话建立请求
(密钥ID, Auth令牌, GPSI, 路由ID, Counter AKMA)
3. 应用会话建立请求
(密钥ID, Auth令牌, GPSI, 路由ID, AF ID, Counter AKMA)
4. AKMA密钥请求
(密钥ID, Auth令牌, GPSI, 路由ID, Counter AKMA)
5. SUPI请求
(GPSI)
6. 响应
7
■ K AKMA = KDF {K AUSF, RAND, GPSI, RI, SUPI, Counter AKMA }
■ 验证Auth令牌
8. AKMA密钥响应
(K AKMA)
9. K aaf = KDF {K Akma, GPSI, AF ID, Counter aaf }
10. 应用密钥响应
(K aaf, Exp时间, Counter aaf)
11. 应用会话建立响应
(Counter aaf, MAC-I)
12. K aaf = KDF {K Akma, GPSI, AF ID, Counter aaf }
13. 验证MAC-I

图5

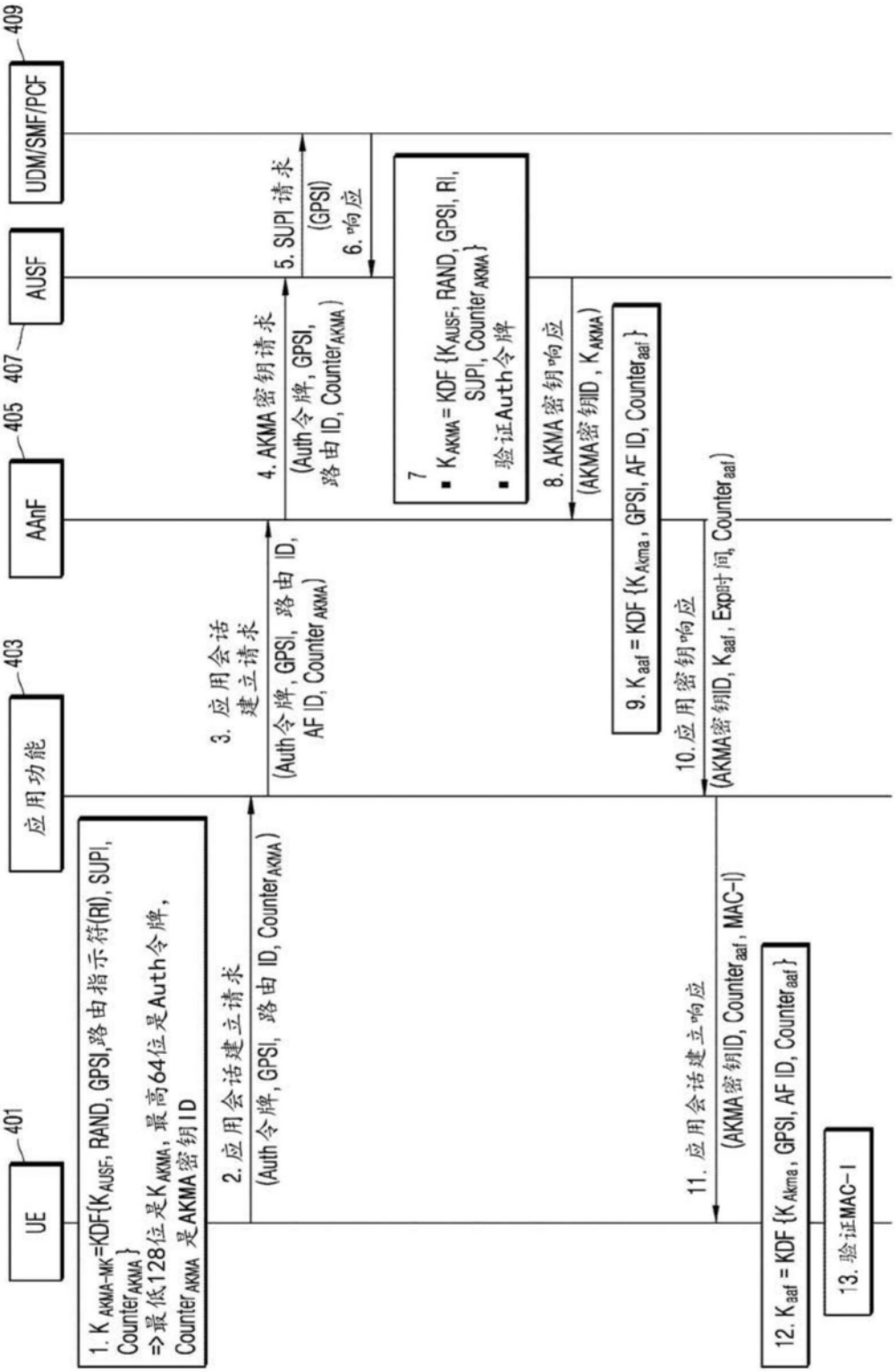

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K AKMA-MK=KDF(K AUSF, RAND, GPSI,路由指示符(RI), SUPI, Counter AKMA }
=>最低128位是K AKMA，最高64位是Auth令牌，
Counter AKMA 是AKMA密钥ID
2. 应用会话建立请求
(Auth令牌, GPSI, 路由 ID, Counter AKMA)
3. 应用会话建立请求
(Auth令牌, GPSI, 路由 ID, AF ID, Counter AKMA)
4. AKMA密钥请求
(Auth令牌, GPSI, 路由 ID, Counter AKMA)
5. SUPI 请求
(GPSI)
6. 响应
7
■ K AKMA = KDF {K AUSF, RAND, GPSI, RI, SUPI, Counter AKMA}
■ 验证Auth令牌
8. AKMA密钥响应
(AKMA密钥ID , K AKMA)
9. K aaf = KDF {K Akma , GPSI, AF ID, Counter aaf }
10. 应用密钥响应
(AKMA密钥ID, K aaf , Exp时间, Counter aaf)
11. 应用会话建立响应
(AKMA密钥ID, Counter aaf , MAC-I)
12. K aaf = KDF {K Akma , GPSI, AF ID, Counter aaf }
13. 验证MAC-I

图6

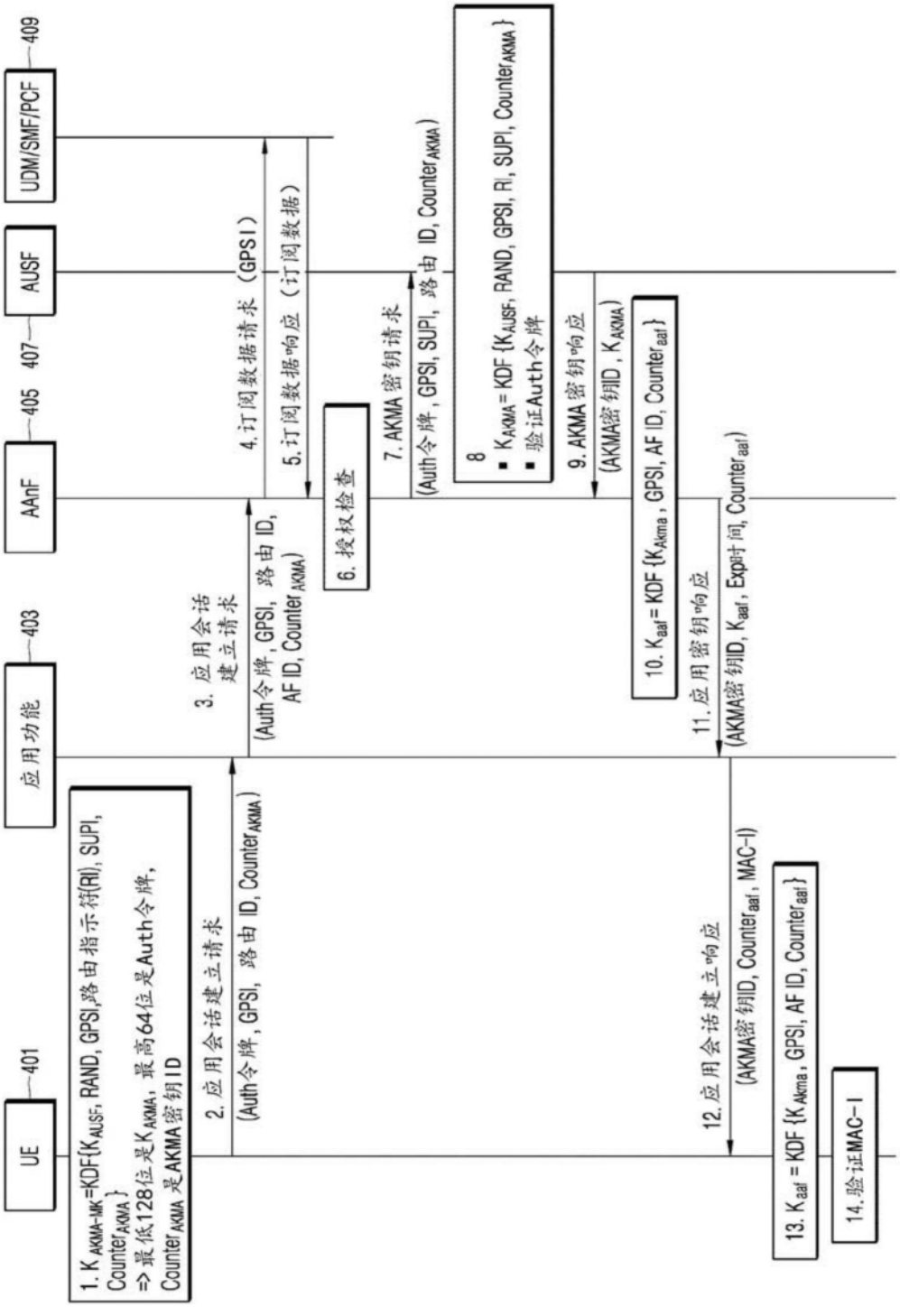

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K AKMA-MK=KDF{K AUSF, RAND, GPSI,路由指示符(RI), SUPI, Counter AKMA }
=>最低128位是K AKMA，最高64位是Auth令牌，
Counter AKMA 是AKMA密钥ID
2. 应用会话建立请求
(Auth令牌, GPSI, 路由 ID, Counter AKMA)
3. 应用会话
建立请求
(Auth令牌, GPSI, 路由 ID,
AF ID, Counter AKMA)
4. 订阅数据请求 (GPSI)
5. 订阅数据响应 (订阅数据)
6. 授权检查
7. AKMA密钥请求
(Auth令牌, GPSI, SUPI, 路由 ID, Counter AKMA)
8
■ K AKMA= KDF (K AUSF, RAND, GPSI, RI, SUPI, Counter AKMA }
■ 验证Auth令牌
9. AKMA密钥响应
(AKMA密钥ID, K AKMA)
10. K aaf= KDF (K AKma , GPSI, AF ID, Counter aaf }
11. 应用密钥响应
(AKMA密钥ID, K aaf, Exp时间, Counter aaf)
12. 应用会话建立响应
(AKMA密钥ID, Counter aaf, MAC-I)
13. K aaf = KDF (K AKma , GPSI, AF ID, Counter aaf }
14. 验证MAC-I

图7

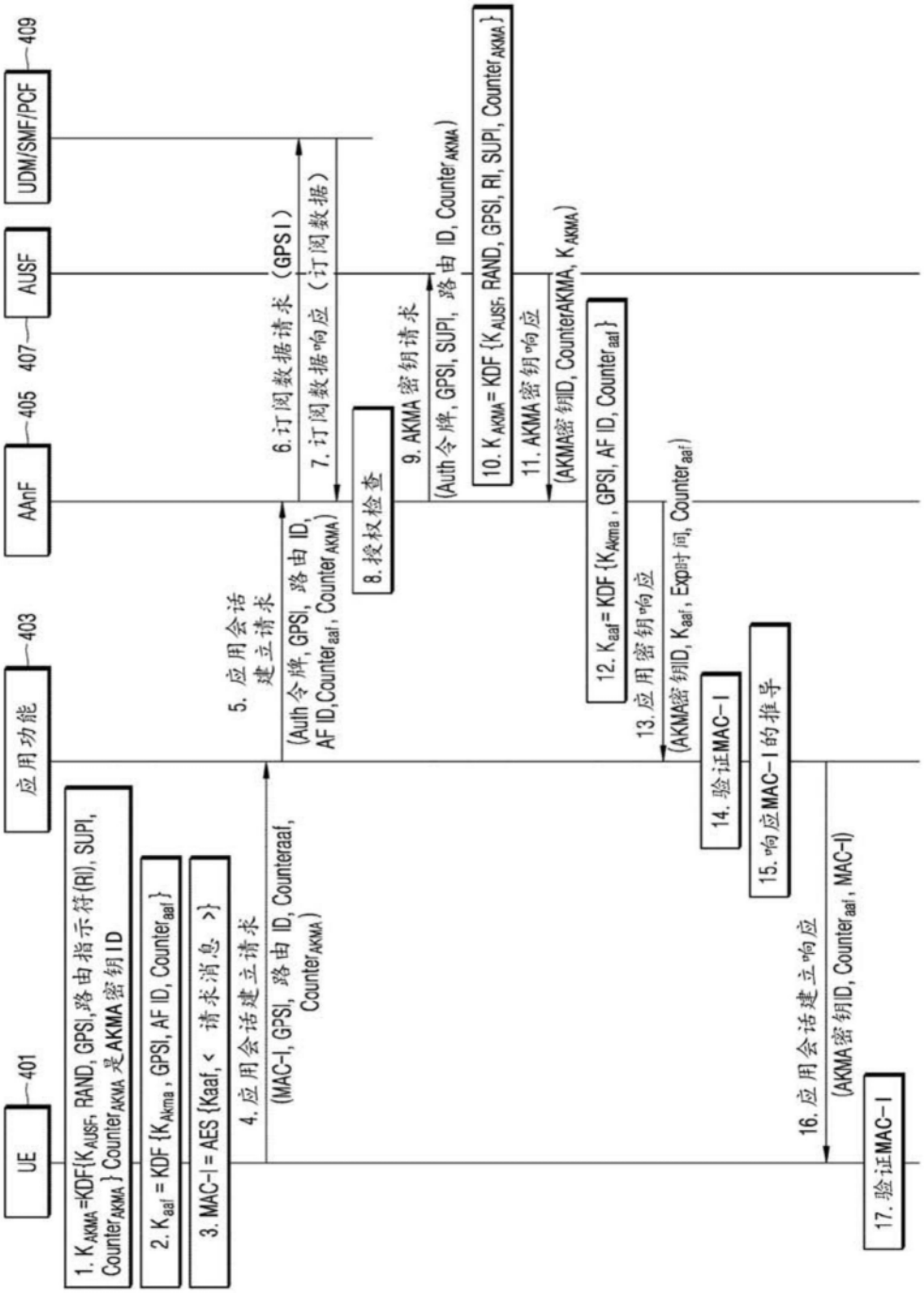

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K_AKMA=KDF{K_AUSF, RAND, GPSI,路由指示符(RI), SUPI, Counter_AKMA } Counter_AKMA 是AKMA密钥ID
2. K_aaf = KDF {K_Akma , GPSI, AF ID, Counter_aaf }
3. MAC-I = AES {Kaaf, < 请求消息 >}
4. 应用会话建立请求
(MAC-I, GPSI, 路由 ID, Counteraaf, Counter_AKMA)
5. 应用会话建立请求
(Auth令牌, GPSI, 路由 ID, AF ID,Counter_aaf , Counter_AKMA)
6. 订阅数据请求 (GPSI)
7. 订阅数据响应 (订阅数据)
8. 授权检查
9. AKMA密钥请求
(Auth令牌, GPSI, SUPI, 路由 ID, Counter'_AKMA)
10. K_AKMA = KDF {K_AUSF, RAND, GPSI, RI, SUPI, Counter_AKMA }
11. AKMA密钥响应
(AKMA密钥ID, CounterAKMA, K_AKMA)
12. K_aaf = KDF {K_Akma , GPSI, AF ID, Counter_aaf }
13. 应用密钥响应
(AKMA密钥ID, K_aaf , Exp时间, Counter_aaf)
14. 验证MAC-I
15. 响应MAC-I的推导
16. 应用会话建立响应
(AKMA密钥ID, Counter_aaf , MAC-I)
17. 验证MAC-I

图8

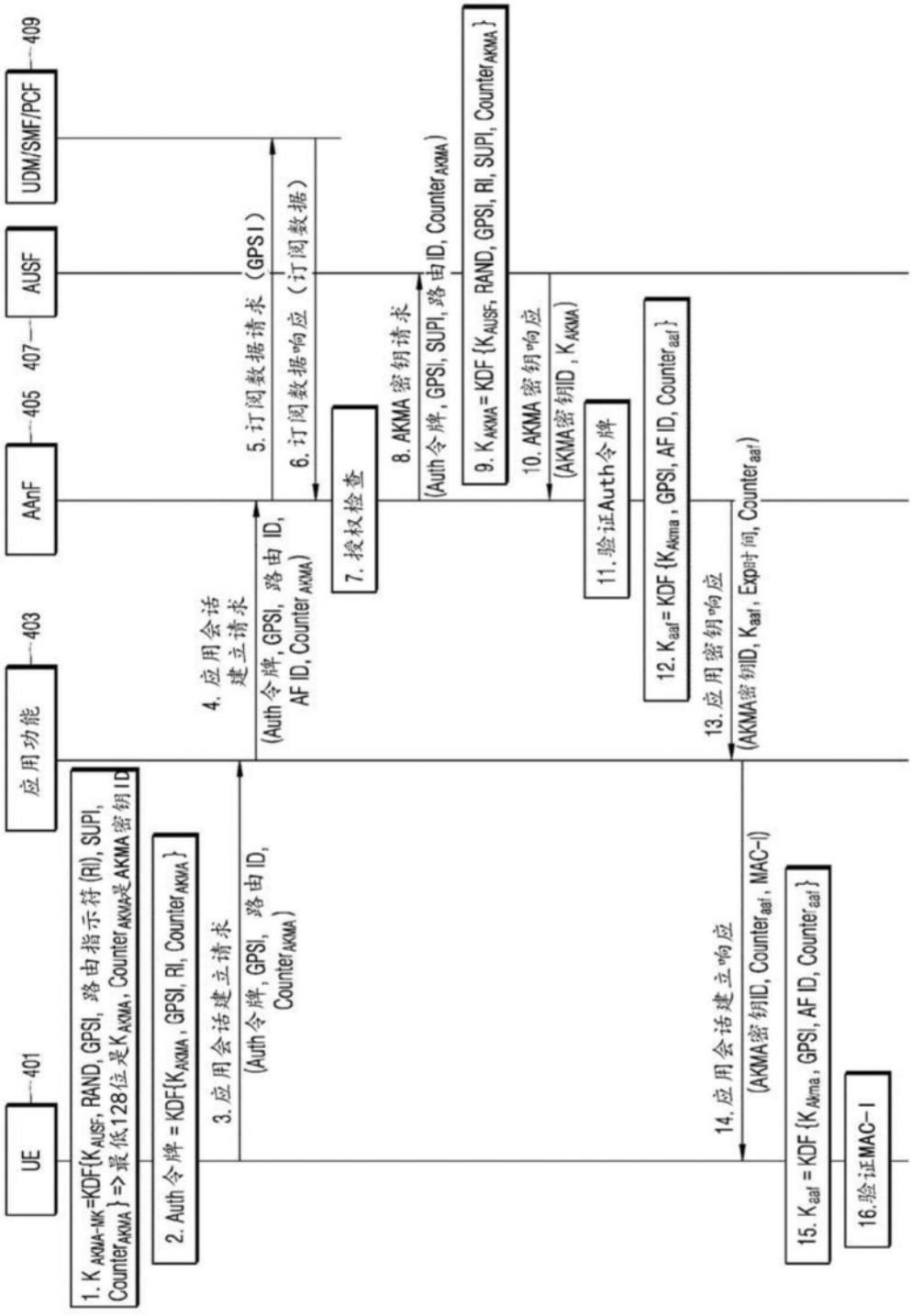

UE
401
应用功能
403
AAnF
405
AUSF
407
UDM/SMF/PCF
409
1. K AKMA-MK=KDF{K AUSF, RAND, GPSI, 路由指示符(RI), SUPI, Counter AKMA } => 最低128位是K AKMA, Counter AKMA是AKMA密钥ID
2. Auth令牌 = KDF{K AKMA, GPSI, RI, Counter AKMA }
3. 应用会话建立请求
(Auth令牌, GPSI, 路由ID, Counter AKMA)
4. 应用会话建立请求
(Auth令牌, GPSI, 路由ID, AF ID, Counter AKMA)
5. 订阅数据请求 (GPSI)
6. 订阅数据响应 (订阅数据)
7. 授权检查
8. AKMA密钥请求
(Auth令牌, GPSI, SUPI, 路由ID, Counter AKMA)
9. K AKMA = KDF {K AUSF, RAND, GPSI, RI, SUPI, Counter AKMA }
10. AKMA密钥响应
(AKMA密钥ID, K AKMA)
11. 验证Auth令牌
12. K aaf = KDF {K Akma, GPSI, AF ID, Counter aaf }
13. 应用密钥响应
(AKMA密钥ID, K aaf, Exp时间, Counter aaf)
14. 应用会话建立响应
(AKMA密钥ID, Counter aaf, MAC-I)
15. K aaf = KDF {K Akma, GPSI, AF ID, Counter aaf }
16. 验证MAC-I

图9

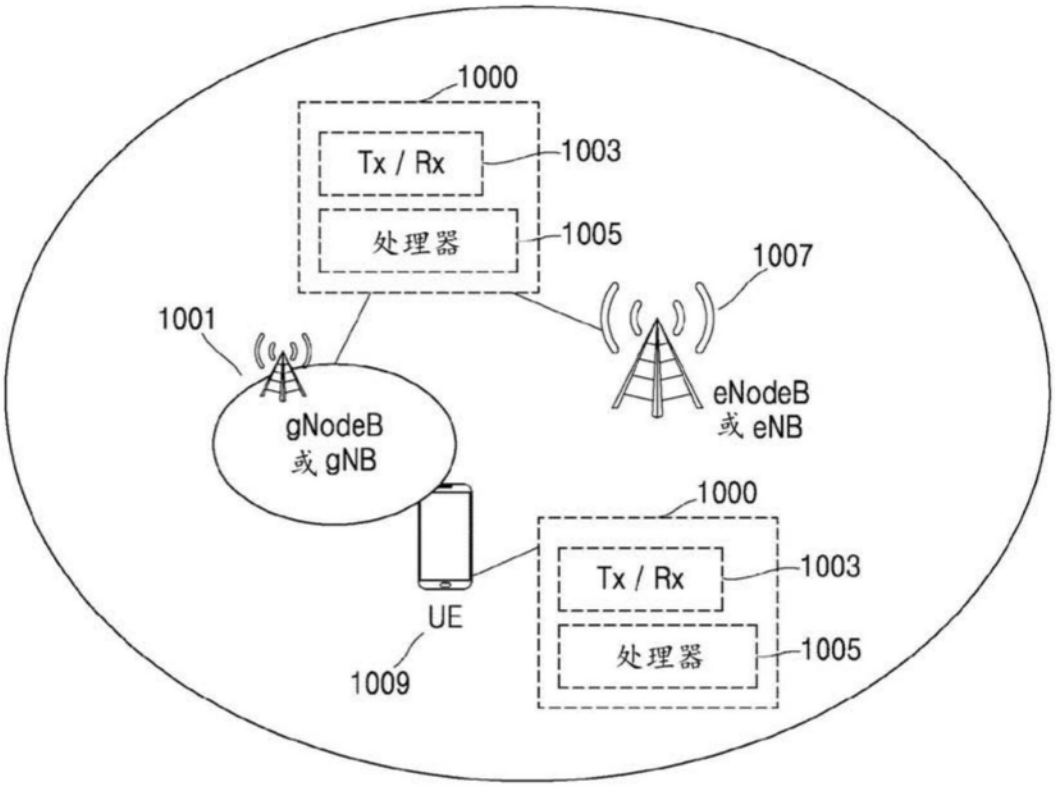

1000
Tx / Rx
1003
处理器
1005
1007
1001
gNodeB
或 gNB
eNodeB
或 eNB
1000
Tx / Rx
1003
处理器
1005
UE
1009

图10

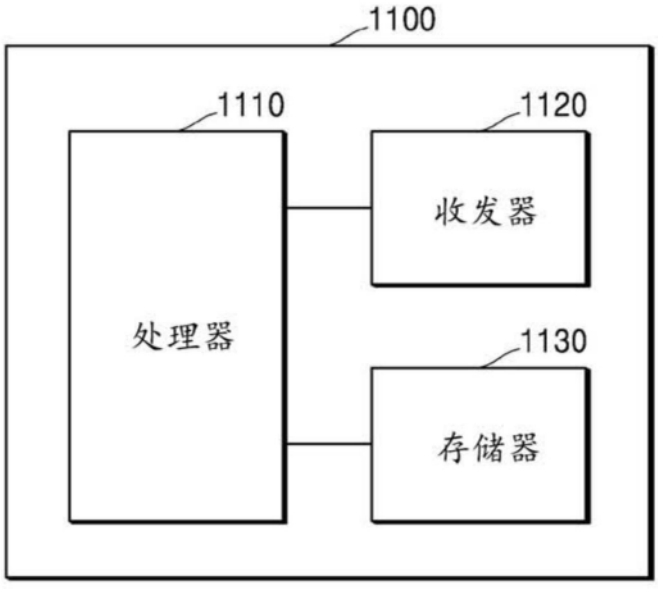

1100
1110
1120
处理器
收发器
1130
存储器

图11

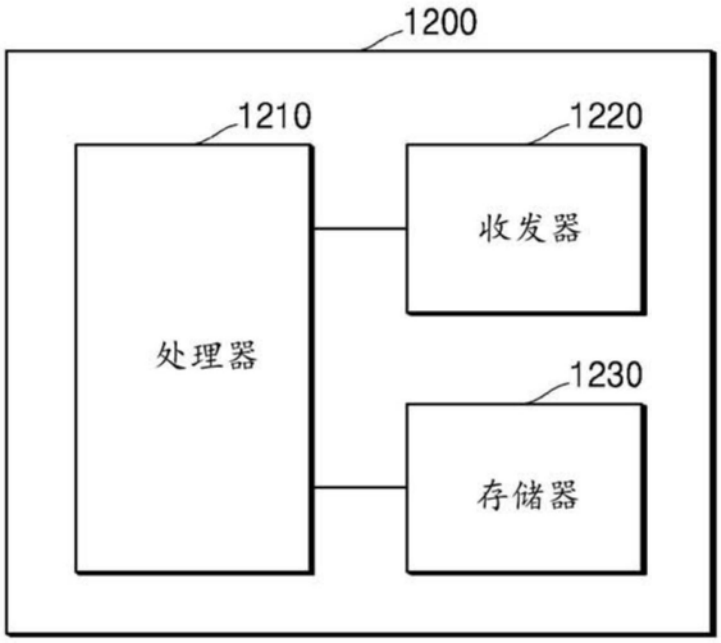


图12