(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 104067648 B
(45)授权公告日 2018.12.11

(21)申请号 201380007316.7

(22)申请日 2013.01.28

(65)同一申请的已公布的文献号
申请公布号 CN 104067648 A

(43)申请公布日 2014.09.24

(30)优先权数据
61/592126 2012.01.30 US
13/677451 2012.11.15 US

(85)PCT国际申请进入国家阶段日
2014.07.30

(86)PCT国际申请的申请数据
PCT/EP2013/051550 2013.01.28

(87)PCT国际申请的公布数据
WO2013/113647 EN 2013.08.08

(73)专利权人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩

(72)发明人 K.诺尔曼 M.维夫韦松

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 徐予红 汤春龙

(51)Int.Cl.
H04W 12/04(2006.01)
H04W 36/00(2006.01)

(56)对比文件
CN 101309500 B,2011.07.20,
WO 2011140695 A1,2011.11.17,
CN 101860862 A,2010.10.13,
3GPP.Security architecture.《3GPP TS 33.401 V10.1.1》.2011,
3GPP.3G Security Security architecture.《3GPP TS 33.102 V11.0.0》.2011,

审查员 宋雪莹

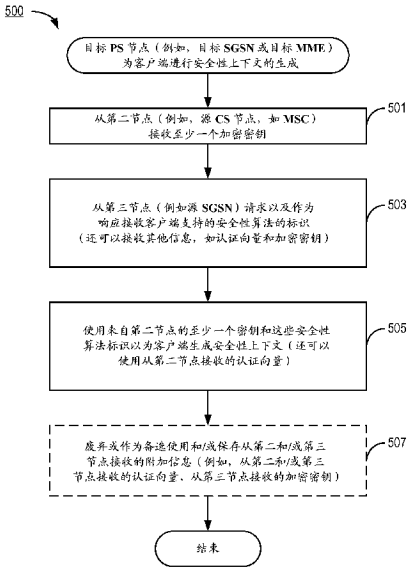
权利要求书3页 说明书10页 附图8页

(54)发明名称

在支持不同安全性上下文的蜂窝通信系统节点之间的呼叫切换

(57)摘要

在有助于蜂窝通信系统(101)中呼叫的电路交换到分组交换的切换的上下文中,第一节点(611、711、800)(例如,分组交换目标节点)为正在切换其呼叫的客户端(601、701)生成安全性上下文。这包括第一节点(611、711、800)从第二节点(607、707)(例如,支持现有连接的电路交换节点)接收(501)至少一个加密密钥以及从第三节点(609、709)(例如,支持现有连接的分组交换节点)接收(503)客户端(601、701)支持的安全性算法的标识;第一节点(611、711、800)使用(505)至少一个加密密钥和标识来为客户端(601、701)生成安全性上下文。



CN 104067648 B

1.一种在蜂窝通信系统(101)中操作第一节点(611、711、800)以便为客户端(601、701)生成安全性上下文的方法，其中所述第一节点(611、711、800)包括处理电路(801)，所述方法包括：

所述第一节点(611、711、800)执行如下操作：

从第二节点(607、707)接收(501)至少一个加密密钥；

从第三节点(609、709)接收(503)所述客户端(601、701)支持的安全性算法的标识；以及

使用(505)所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文。

2.如权利要求1所述的方法，其中所述第一和第三节点(611、711、800、609、709)是分组交换节点以及所述第二节点(607、707)是电路交换节点。

3.如权利要求2所述的方法，其中所述第一节点(611、711、800)是MME，所述第二节点(607、707)是MSC以及所述第三节点(609、709)是SGSN。

4.如权利要求2所述的方法，其中所述第一节点(611、711、800)是第一SGSN，所述第二节点(607、707)是MSC以及所述第三节点(609、709)是第二SGSN。

5. 如权利要求1所述的方法，还包括：

促使所述第一节点(611、711、800)从所述第二节点(607、707)接收(2''')一个或多个认证向量；以及

废弃(507)从所述第二节点(607、707)接收的所述认证向量。

6.如权利要求1所述的方法，其中所述第一节点(611、711、800)是SGSN，以及其中所述方法还包括：

使用(507、615)所述至少一个加密密钥的其中一个或多个来保护第四节点与所述客户端(601、701)之间的业务。

7.如权利要求1所述的方法，其中所述第一节点(611、711、800)是MME，以及其中所述方法还包括：

从所述至少一个加密密钥的其中一个或多个导出(507、715)访问安全性管理实体(K_ASME)的密钥。

8. 如权利要求1所述的方法，还包括：

从所述第三节点(609、709)接收(4”、4''')分组交换加密密钥以在分组交换连接中使用；以及

废弃(507、615、715)所述分组交换加密密钥。

9. 如权利要求1所述的方法，还包括：

从所述第三节点节点(609、709)接收(4''、4''')至少一个认证向量；以及

存储(507、615、715)所接收的至少一个认证向量。

10.如权利要求1所述的方法，还包括从所述第三节点(609、709)接收附加信息；以及

其中使用(505)所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文包括，使用(505)所述至少一个加密密钥和所述标识以及所述附加信息来为所述客户端(601、701)生成所述安全性上下文。

11.一种在蜂窝通信系统(101)中操作第一和第二节点(611、711、800、607、707)的方

法，所述方法执行操作以便作为将客户端(601、701)的支持从所述第二节点(607、707)切换到所述第一节点(611、711、800)的过程的一部分生成安全性上下文，其中所述第一和第二节点(611、711、800、607、707)各包括处理电路，所述方法包括：

所述第二节点(607、707)根据与所述客户端(601、701)关联的至少一个现有密钥和所述第二节点(607、707)生成的nonce生成(613、713)至少一个新的加密密钥；

所述第二节点(607、707)将所述至少一个新的加密密钥传送(2''、2'''、501)到所述第一节点(611、711、800)；

所述第一节点(611、711、800)从第三节点(609、709)接收(503)所述客户端(601、701)支持的安全性算法的标识；以及

所述第一节点(611、711、800)使用(505)所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文。

12.如权利要求11所述的方法，其中所述第一和第三节点(611、711、800、609、709)是分组交换节点以及所述第二节点(607、707)是电路交换节点。

13.一种在蜂窝通信系统(101)中用于操作第一节点(611、711、800)以便为客户端(601、701)生成安全性上下文的装置(500、801)，所述装置包括：

配置成从第二节点(607、707)接收至少一个加密密钥的电路(501)；

配置成从第三节点(609、709)接收所述客户端(601、701)支持的安全性算法的标识的电路(503)；以及

配置成使用所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文的电路(505)。

14.如权利要求13所述的装置，其中所述第一和第三节点(611、711、800、609、709)是分组交换节点以及所述第二节点(607、707)是电路交换节点。

15.如权利要求14所述的装置，其中所述第一节点(611、711、800)是MME，所述第二节点(607、707)是MSC以及所述第三节点(609、709)是SGSN。

16.如权利要求14所述的装置，其中所述第一节点(611、711、800)是第一SGSN，所述第二节点(607、707)是MSC以及所述第三节点(609、709)是第二SGSN。

17. 如权利要求13所述的装置，所述装置还包括：

配置成从所述第二节点(607、707)接收(2''')一个或多个认证向量的电路；以及

配置成废弃(507)从所述第二节点(607、707)接收的所述认证向量的电路。

18.如权利要求13所述的装置，其中所述第一节点(611、711、800)是SGSN，以及其中所述装置还包括：

配置成使用(507、615)所述至少一个加密密钥的其中一个或多个来保护第四节点与所述客户端(601、701)之间的业务的电路。

19.如权利要求13所述的装置，其中所述第一节点(611、711、800)是MME，以及其中所述装置还包括：

配置成从所述至少一个加密密钥的其中一个或多个导出(507、715)访问安全性管理实体(K_ASME)的密钥的电路。

20. 如权利要求13所述的装置，所述装置还包括：

配置成从所述第三节点(609、709)接收(4”、4''')分组交换加密密钥以在分组交换连

接中使用的电路;以及

配置成废弃(507、615、715)所述分组交换加密密钥的电路。

21.如权利要求13所述的装置,所述装置还包括:

配置成从所述第三节点节点(609、709)接收(4''、4''')至少一个认证向量的电路;以及

配置成存储(507、615、715)所接收的至少一个认证向量的电路。

22.如权利要求13所述的装置,所述装置还包括:配置成从所述第三节点(609、709)接收附加信息的电路;以及

其中配置成使用(505)所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文的电路包括,配置成使用(505)所述至少一个加密密钥和所述标识以及所述附加信息来为所述客户端(601、701)生成安全性上下文的电路。

23.一种在蜂窝通信系统(101)中操作第一和第二节点(611、711、800、607、707)的装置,所述装置执行操作以便作为将客户端(601、701)的支持从所述第二节点(607、707)切换到所述第一节点(611、711、800)的过程的一部分生成安全性上下文,所述装置包括:

配置成根据与所述客户端(601、701)关联的至少一个现有密钥和所述第二节点(607、707)生成的nonce生成(613、713)至少一个新的加密密钥的第二节点电路;

配置成将所述至少一个新的加密密钥传送(2''、2'''、501)到所述第一节点(611、711、800)的第二节点电路;

配置成从第三节点(609、709)接收(503)所述客户端(601、701)支持的安全性算法的标识的第一节点(611、711、800)电路;以及

配置成使用(505)所述至少一个加密密钥和所述标识来为所述客户端(601、701)生成所述安全性上下文的第一节点(611、711、800)电路。

24.如权利要求23所述的装置,其中所述第一和第三节点(611、711、800、609、709)是分组交换节点以及所述第二节点(607、707)是电路交换节点。

在支持不同安全性上下文的蜂窝通信系统节点之间的呼叫切换

技术领域

[0001] 本发明涉及蜂窝通信系统，更具体来说，涉及支持不同安全性上下文的蜂窝通信系统之间的呼叫的切换。

背景技术

[0002] 蜂窝通信系统典型地包括基于陆地的网络，该基于陆地的网络对在该网络的覆盖区内移动时能够持续接收服务的移动终端提供无线覆盖。术语“蜂窝”源于整个覆盖区域被划分成所说的“小区”，每个小区典型地由与基于陆地的网络关联的特定无线电收发器站(或等效装置)提供服务。此类收发器站往往统称为“基站”，即便是在为了非常精确地阐明其基站版本的特具特色的功能和体系结构，特定通信标准设置体应用不同的术语(例如，WCDMA中的“NodeB”和LTE中的“eNodeB”)时。当移动设备从一个小区移动到另一个小区时，网络将服务该移动设备的职责从当前服务小区切换到“新”小区。以此方式，移动设备的用户体验到服务的连续性而无需重新建立到网络的连接。切换由系统定义的小区再选择机制来控制。图1图示一个蜂窝通讯系统，其通过多个小区103，提供系统覆盖区域101。

[0003] 当新通信系统出现时，它们带来处理呼叫的新特征、功能和方式。移动通信设备(下文称为“用户设备”或“UE”)必须以兼容预期与之通信的系统的方式来工作。为了提供就使用而言的最大灵活性，UE往往设计成与多于一种系统兼容。一方面，这使得用户在将UE从一种类型的通信系统覆盖的地理区域带到不同类型的通信系统所服务的另一个区域中时一直能够使用该UE。

[0004] 具有多模式功能也是有用的，因为较新的系统往往是逐个推出的，由此即使用户待在一个运营商的系统的地理限制内，UE仍可以在有时发现自己由较旧的设备服务，以及有时由较新的设备服务。图2中图示了此情景，示出其中UE 201当前由符合较旧通信标准(例如，2G -如GERAN或3G - 如UTRAN标准之一)的设备205支持的第一小区203内提供服务的蜂窝通信系统的一部分。在本示例中，UE 201靠近符合较新的通信标准(例如，4G规范，如E-UTRAN，也称为“长期演进”或“LTE”)的设备209所支持的第二(相邻)小区207。如果用户在应该执行从较旧的设备205到较新的设备209的切换时参与呼叫，则期望能够以将该呼叫的干扰减到最小的优雅方式切换该呼叫。

[0005] 但是，因为较旧的通信系统未设计为知悉将需要什么信息来支持至较新的设备的切换，所以设计人员应对如何使此类切换最佳地方式进行的问题(即，如何向新设备提供使之处于最佳位置来获得对当前由较旧的设备服务的正在进行呼叫的支持的信息)。因此需要对此问题的解决方案，包括方法、装置和/或软件。

发明内容

[0006] 应该强调的是，术语“包括”和“包含”在本说明书中使用时被采用来指明所提出的特征、整体、步骤或组件的存在，但是这些术语的使用不排斥一个或多个其他特征、整体、步

骤、组件或它们的集合的存在或附加。

[0007] 从下文对非限制性详细披露以及所附独立权利要求和附图，将显见到本发明的其他目的、特征和优点。一般，除非本文中明确地另行定义，否则权利要求中使用的所有术语应根据其在技术领域中的通用含义来解释。除非明确另行陈述，否则对“一/一个/该[元件、设备、组件、部件、步骤等]”的引述应开放地解释为所述元件、设备、组件、部件、步骤等的至少一个实例。除非明确地陈述，否则本文披露的任何方法的步骤无需按披露的具体顺序来执行。

[0008] 根据本发明的一个方面，用在蜂窝通信系统中用于操作第一节点以为客户端生成安全性上下文的方法和装置达到前述和其他目的，其中第一节点包括处理电路。此类操作包括第一节点从第二节点接收至少一个加密密钥，以及从第三节点接收客户端支持的安全性算法的标识。使用该至少一个加密密钥和这些标识以为客户端生成安全性上下文。

[0009] 在一些实施例中，第一和第三节点是分组交换节点以及第二节点是电路交换节点。例如，第一节点可以是MME，第二节点可以是MSC以及第三节点是SGSN。在其他备选实施例中，第一节点是SGSN，第二节点是MSC以及第三节点是第二SGSN。

[0010] 在一些实施例中，操作还包括第一节点从第二节点接收一个或多个认证向量。然后废弃从第二节点接收的这些认证向量。

[0011] 在第一节点是SGSN的一些实施例中，操作包括使用至少一个加密密钥的其中一个或多个来保护第四节点与客户端之间的业务。

[0012] 在第一节点是MME的一些实施例中，操作包括从至少一个加密密钥的其中一个或多个导出访问安全性管理实体(K_ASME)的密钥。

[0013] 在一些实施例中，操作包括从第三节点接收分组交换加密密钥以在分组交换连接中使用，并且废弃分组交换加密密钥。

[0014] 在一些实施例中，操作包括从第三节点接收至少一个认证向量，并存储所接收的至少一个认证向量。

[0015] 在一些实施例中，操作包括从第三节点接收附加信息，以及在这些实施例的其中一些中，使用至少一个加密密钥和标识来为客户端生成安全性上下文包括，使用至少一个加密密钥和标识以及附加信息来为客户端生成安全性上下文。

[0016] 一些实施例同时涵盖第一和第二节点中的操作，以使第二节点根据与客户端关联的至少一个现有密钥和第二节点生成的nonce来生成至少一个新的加密密钥，并将该至少一个新加密密钥传送到第一节点。第一节点然后从第三节点接收客户端支持的安全性算法的标识，并使用至少一个加密密钥和标识来为客户端生成安全性上下文。

附图说明

[0017] 图1图示蜂窝通讯系统，其通过多个小区提供系统覆盖区域。

[0018] 图2示出蜂窝通信系统的一部分，其中UE当前由符合较旧通信标准(例如，2G或3G标准之一)的设备支持的第一小区内提供服务，并且应该切换到符合较新的通信标准的设备支持的第二小区。

[0019] 图3示出将呼叫从电路交换域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标UTRAN/GERAN支持设备所涉及的信令的多个方面。

[0020] 图4示出将呼叫从CS域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标E-UTRAN(即,4G设备)支持设备所涉及的信令的多个方面。

[0021] 图5在一个方面中是根据与本发明相符的一些但是不一定是全部的切换机制示范实施例的目标PS节点执行的步骤/过程的流程图。

[0022] 图6是与本发明相符的切换信令和步骤的一个实施例的多个方面的信令图。

[0023] 图7是与本发明相符的切换信令和步骤的备选实施例的信令图。

[0024] 图8是PS域中工作的目标节点(例如,SGSN/MME)的框图。

具体实施方式

[0025] 现在将结合附图描述本发明的多个不同特征,其中相似的部分以相同的引用字符标识。

[0026] 现在将结合多个示范实施例来更详细地描述本发明的多个方面。为了便于理解本发明,依据能够执行编程的指令的计算机系统或其他硬件的元件执行的动作序列来描述本发明的多个方面。但是,将认识到,在每个实施例中,可以由专门的电路(例如,互连以执行专门的功能的模拟和/或离散逻辑门)、由利用适合的指令集编程的一个或多个处理器或由二者的组合来执行这些不同的动作。术语"配置成执行一个或多个所述动作的电路"在本文中用于指任何此类实施例(即,一个或多个专门的电路和/或一个或多个编程的处理器)。而且,本发明附加地能够认为整体地以任何形式的计算机可读载体来实施,如使得处理器执行本文描述的技术的适合计算机指令集的固态存储器、磁盘或光盘。因此,本发明的多种方面可以采用多种不同的形式来实施,并且所有此类形式可设想在本发明的范围内。对于本发明的多种方面的每一个方面,上文描述的任何此类形式的实施例可以在本文称为"配置用于执行所述动作的逻辑"或作为备选称为执行所述动作的"逻辑"。

[0027] 在下文披露中,为方便起见且由于缩略语在本领域中广泛使用,所以使用多个缩略语。由此,下面多个缩略语及其含义是基于每个缩略语是本领域技术人员容易理解的标准术语来给出。

[0028] ·3GPP(第三代合作伙伴项目)

[0029] ·3GPP TSG SA WG3(第三代合作伙伴项目技术规范组系统体系结构工作组3)

[0030] ·AKA(认证和密钥协议)

[0031] ·AMF(认证管理域)

[0032] ·AS(接入层)

[0033] ·BSC(基站控制器)

[0034] ·BSS(基站子系统)

[0035] ·CK(加密密钥)

[0036] ·CKSN(加密密钥序列号)

[0037] ·CR(更改请求)

[0038] ·CS(电路交换)

[0039] ·eNB(eNodeB)

[0040] ·E-UTRAN(演进的通用地面无线电接入网)

[0041] ·EPS(演进的分组系统)

[0042] ·FC(功能码)

[0043] ·FFS(供将来研究)

[0044] ·GERAN(GSM/EDGE无线电接入网)

[0045] ·HLR(归属位置注册器)

[0046] ·HO(切换)

[0047] ·HSPA(高速分组接入)

[0048] ·HSS(归属订户服务器)

[0049] ·IE(信息元素)

[0050] ·IK(完整性密钥)

[0051] ·IMS(IP多媒体子系统)

[0052] ·IMSI(国际移动订户标识)

[0053] ·IRAT(无线电接入间技术)

[0054] ·ISDN(综合业务数字网络)

[0055] ·K_{ASME}(密钥访问安全性管理实体)

[0056] ·KDF(密钥导出功能)

[0057] ·KSI(密钥组标识符)

[0058] ·LA(位置区域)

[0059] ·LTE(长期演进)

[0060] ·ME(移动设备)

[0061] ·MSC(移动交换中心)

[0062] ·MSISDN(移动订户ISDN)

[0063] ·MM(移动性管理)

[0064] ·MME(移动性管理实体)

[0065] ·MS(移动台)

[0066] ·NAS(非接入层)

[0067] ·NB(节点B)

[0068] ·NONCE(“一次性使用的数字”-(伪)随机生成的位串)

[0069] ·PLMN(公共陆地移动网络)

[0070] ·PS(分组交换)

[0071] ·PRNG(伪随机数发生器)

[0072] ·RAT(无线电接入技术)

[0073] ·RNC(无线电网络控制器)

[0074] ·RRC(无线电资源控制)

[0075] ·SA(系统体系结构)

[0076] ·SGSN(服务GPRS支持节点)

[0077] ·SGW(信令网关)

[0078] ·SIM(订户标识模块)

[0079] ·SRNC(服务RNC)

[0080] ·SRVCC(单个无线电语音呼叫连接性)

[0081] ·SQN(序列号)

[0082] ·UE(用户设备)

[0083] ·USIM(通用订户标识模块)

[0084] ·UTRAN(通用地面无线电接入网)

[0085] ·UMTS(通用移动电信系统)

[0086] ·UP(用户面)

[0087] 正如本披露的背景技术部分中所提到的,不同类型的蜂窝通信设备之间的不兼容性表现为阻碍实现呼叫从一种类型的设备到另一种类型的高质量切换。例如,考虑当较新的所说“4G”设备要负责当前由较旧的“2G”或“3G”设备服务的呼叫时有关安全性上下文可能产生的问题。设计成在2G/3G设备中以及在较新的4G设备中工作的双模/多模UE将可能具有专用于4G设备的安全性功能。因此,呼叫被切换到的4G网络节点应该接收到指示该UE的4G安全性参数(例如,密钥、选定的且支持的加密算法等)是什么的信息。但是考虑再从2G/3G设备到4G设备的常规切换期间所发生的:

[0088] 至少必须将要切换到4G的任何2G/3G呼叫(能够在电路交换CS或分组交换PS模式中工作)连接到SGSN(PS设备),即便该服务正在通过与MSC(CS设备)的连接来处理。当UE连接到分组交换域中的网络时,它向SGSN提供所说的“UE网络能力”,其包括E-UTRAN中终端支持的安全性算法。3GPP TS 23.060 V10.6.0(2011-12)规范中条款6.14规定“无线电接入类标记”包含“UE网络能力”。“UE网络能力”包含该UE支持的E-UTRAN安全性算法。具体来说,3GPP TS 23.060的条款6.14.1陈述UE(由于历史原因,在规范中称为“MS”、“移动台”)将无线电接入能力发送到网络。感兴趣的读者可以参阅3GPP TS 23.060,以获取有关此方面的更多信息。

[0089] 现在来看电路交换域,UE不将“UE网络能力”提供到网络(在此情况中为MSC),而是仅提供其2G/3G(UTAN/GERAN)相关的能力。这可以从3GPP TS 24.008 V10.5.0(2011-12)的条款9.2.15中找到的位置更新请求消息定义中见到。位置更新请求消息用于执行该连接。

[0090] 从UTRAN(3G)到E-UTRAN(4G)的分组交换RAT间切换在3GPP TS 23.401 V10.6.0(2011-12)的条款5.5.2.2中进行了描述。特别注意到的是规范中如图5.5.2.2.2-1所示的步骤3(转发重定位请求)。这些安全性参数(例如,密钥、选定且支持的加密算法等)包含在MM上下文中。具体来说,MM上下文包含安全性相关的信息,例如,UE网络能力和所使用的UMTS完整性和加密算法以及密钥,正如条款5.7.2(用于MME的信息存储)中所描述的。UE网络能力包括E-UTRAN安全性能力,其包括例如UE支持的LTE加密和完整性算法的标识(这些算法标识符在LTE安全性规范TS 33.401中称为EPS加密算法和EPS完整性保护算法)。

[0091] 从GERAN到E-UTRAN的分组交换RAT间切换在3GPP TS 23.401的条款5.5.2.4中进行了描述。

[0092] 让源节点(PS域的SGSN)将UE网络能力转发到目标节点的原理与呼叫在CS域中始发时所规定的切换过程完全相同。但是,在CS域中,源节点是MSC,如上文所提到的,MSC不具有UE的E-UTRAN安全性能力。(实际上,在CS域中,无需MSC具有此类信息,因为目标节点也是MSC。)因此,常规切换不提供用于将此信息提供到目标节点(E-UTRAN中的MME)的任何机制。

[0093] 图3示出此情形,其中示出将呼叫从CS域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标UTRAN支持设备所涉及的信令的多个方面。参与此信令的图示的组件

是UE 301、源BSC/RNC 303、目标RNC 305、MSC服务器307、源SGSN/MME 309和目标SGSN 311。

[0094] 最初，UE 301启用多种源UTRAN或GERAN设备支持的CS呼叫。响应作出执行CS(UTRAN或GERAN)向PS(UTRAN)切换的决定，在步骤1中，源BSC/RNC 303向MSC服务器307发送“需要HO”消息。

[0095] MSC服务器307然后生成(步骤313)$NONCE_{MSC}$，并根据如下公式使用$NONCE_{MSC}$来生成加密密钥：

[0096] $CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC})$，

[0097] 其中符号“||”表示串联函数。

[0098] 在步骤2中，MSC服务器307将“CS至PS HO请求”传送到目标SGSN 311，并将所生成的加密密钥($CK'_{PS} \,||\, IK'_{PS}$)包含在此消息中。

[0099] 作为响应，在步骤3中，目标SGSN 311向源SGSN/MME 309发送“上下文请求”，以便实现为UE 301请求上下文信息的目的。(此处和信令的其他表示中使用的虚线表示可选步骤。)SGSN/MME 309然后向目标SGSN 311回送“上下文响应”(包含所请求的信息)(步骤4)。

[0100] 如果目标SGSN 311从针对SRVCC增强的MSC服务器307接收到GPRS Kc’和$CKSN'_{PS}$，则目标SGSN 311根据GPRS Kc’计算(步骤315)CK'_{PS}和IK'_{PS}。目标SGSN 311将CK'_{PS}和IK'_{PS}与KSI'_{PS}关联，将其设为等于从针对SRVCC增强的源MSC服务器307接收的$CKSN'_{PS}$。

[0101] 目标SGSN 311然后将CK'_{PS}、IK'_{PS}发送到目标RNC 305(步骤5)。作为响应，目标RNC 305发送分配资源响应(步骤6)。

[0102] 在步骤7中，目标SGSN 311向源MSC服务器307发送CS至PS HO响应消息。

[0103] 在步骤8中，MSC服务器307向源BSC/RNC 303发送CS至PS HO响应。此CS至PS HO响应尤其包含$NONCE_{MSC}$。

[0104] 在步骤9中，源BSC/RNC 303向UE 301发送CS至PS HO命令。此命令尤其包含$NONCE_{MSC}$。UE 301使用接收到的$NONCE_{MSC}$根据适用的标准所规定的密钥导出公式导出CK'_{PS}和IK'_{PS}(步骤317)。

[0105] 在步骤10中，UE 301向目标RNC 305返回CS至PS HO确认。CK'_{PS} AND IK'_{PS}成为UE 301中以及目标RNC 305中的活动密钥集。

[0106] 图4中示出相同类型情形的备选图示，其中示出将呼叫从CS域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标E-UTRAN(即，4G设备)支持设备所涉及的信令的多个方面。参与此信令的图示的组件是UE 401、源BSC/RNC 403、目标eNB 405、MSC服务器407、源SGSN/MME 409和目标MME 411.

[0107] 最初，UE 401启用多种源UTRAN或GERAN设备支持的CS呼叫。响应作出执行CS(UTRAN或GERAN)向PS(E-UTRAN)切换的决定，在步骤1’中，源BSC/RNC 403向MSC服务器407发送“需要HO”消息。

[0108] MSC服务器407然后生成(步骤413)$NONCE_{MSC}$，并根据如下公式使用$NONCE_{MSC}$来生成加密密钥：

[0109] $CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC})$，

[0110] 其中符号“||”表示串联函数。

[0111] 在步骤2’中，MSC服务器407将“CS至PS HO请求”传送到目标MME 411，并将所生成的加密密钥($CK'_{PS} \,||\, IK'_{PS}$)包含在此消息中。

[0112] 作为响应，在步骤3’中，目标MME 411向源SGSN/MME 409发送“上下文请求”，以便实现为UE 401请求上下文信息的目的。SGSN/MME 409然后向目标MME 411回送“上下文响应”(包含所请求的信息)(步骤4’)。

[0113] 在步骤415中，目标MME 411通过如下操作创建映射的EPS安全性上下文：将映射的EPS安全性上下文的K'_{ASME}设为等于串联CK'_{PS} || IK'_{PS}，其中CK'_{PS}和IK'_{PS}是在CS至PS切换请求中接收的(参见步骤2’)。目标MME 411还将K'_{ASME}与KSI_{SGSN}。KSI_{SGSN}的值与CS至PS切换请求中接收的KSI'_{PS}的值相同。

[0114] 再有，作为步骤415的一部分，目标MME 411通过应用适用的标准中定义的KDF，使用映射的密钥K'_{ASME}和$2^{32}-1$作为上行NAS COUNT参数的值来导出K_{eNB}。在目标MME 411中，将用于映射的EPS安全性上下文的上行和下行NAS COUNT值设为起始值(即，0)。

[0115] 目标MME 411然后将K_{eNB}和NAS参数发送到目标eNB 405(步骤5’)。作为响应，目标eNB 405发送分配资源响应(步骤6’)。

[0116] 在步骤7’中，目标MME 411向源MSC服务器407发送CS至PS HO响应消息。

[0117] 在步骤8’中，MSC服务器407向源BSC/RNC 403发送CS至PS HO响应。此CS至PS HO响应尤其包含$NONCE_{MSC}$。

[0118] 在步骤9’中，源BSC/RNC 403向UE 401发送CS至PS HO命令。此命令尤其包含$NONCE_{MSC}$。UE 401使用接收的$NONCE_{MSC}$来导出K'_{ASME}，将其与NAS安全性透明容器IE中接收的KSI_{SGSN}关联，遵循与步骤2’、3’和4’中所执行的MSC服务器407和目标MME 411相同的密钥导出来导出NAS密钥和K_{eNB}，所有这些步骤均按照适用的标准所规定的。

[0119] 在步骤10’中，UE 401向目标eNB 405返回CS至PS HO确认。按上文建立的映射的EPS安全性上下文成为AS处的当前EPS安全性上下文。

[0120] 一种新的切换机制解决常规技术的问题。图5中示出此新切换机制的多个方面，在一个方面中，图5是根据与本发明相符的一些但是不一定是全部的示范实施例的目标PS节点执行的步骤/过程的流程图。在另一方面中，可以将图5视为示出包括配置成执行所描述的功能的多种图示电路(例如，硬连线和/或适合编程的处理器)的示范部件500。

[0121] 为了易于术语理解，在此处理的上下文中，可以将目标PS节点视为蜂窝通信系统中为客户端生成安全性上下文的“第一节点”。在一个方面中，第一节点从第二节点接收至少一个加密密钥(步骤501)。第二节点可以是源CS节点，如MSC。

[0122] 第一节点从第三节点(例如，源SGSN)请求，并作为响应，接收到客户端支持的安全性算法的标识(步骤503)。在一些但不一定所有的实施例中，第一节点还可以接收其他信息，如一个或多个认证向量和/或加密密钥。

[0123] 第一节点然后使用从第二节点接收的至少一个加密密钥以及安全性算法标识来为客户端生成安全性上下文(步骤505)。在一些但不一定所有的实施例中，还可以使用从第二节点接收的认证向量。

[0124] 在此时点，第一节点已经为客户端生成安全性上下文。在一些但不一定所有的实施例中，第一节点可以执行附加功能的任何一个或组合，例如但不限于：

[0125] ·废弃从第二和/或第三节点接收的附加信息(例如，从第二和/或第三节点接收的认证向量，第三节点接收的加密密钥)

[0126] ·使用(例如，如果目标PS节点是SGSN)和/或保存(例如，如果目标PS节点是MME)从

第二和/或第三节点接受的附加信息(例如从第二和/或第三节点接收的认证向量)。例如，如果目标PS节点是MME且后来将切换到从中接收这些认证向量所在的完全相同的源SGSN(在此情况中，在后来的切换时将这些认证向量返回到SGSN)。

[0127] 可以从图6认识到与本发明相符的实施例的附加方面，图6是与本发明相符的一个实施例的信令图。具体来说，此示意图着重于支持目标PS节点能够作为将呼叫从CS域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标UTRAN支持设备的一部分为客户端创建安全性上下文的多个方面。图示的实施例的一个方面是目标PS节点从源PS节点以及也从源CS节点接收安全性相关信息，并且将所收集的信息的选定部分组合以生成一组新的安全性相关信息。下文对此作更详细的描述。

[0128] 参与此示范实施例的信令的图示的组件是UE 601(客户端)、源BSC/RNC 603、目标RNC 605、MSC服务器607、源SGSN/MME 609和目标SGSN 611。

[0129] 最初，UE 601启用多种源UTRAN或GERAN设备支持的CS呼叫。响应作出执行CS(UTRAN或GERAN)向PS(UTRAN/GERAN)切换的决定，在步骤1”中，源BSC/RNC 603向MSC服务器607发送“需要HO”消息。

[0130] MSC服务器607然后生成(步骤613)$NONCE_{MSC}$，并根据如下公式使用$NONCE_{MSC}$和与UE 601共享的现有密钥生成加密密钥：

[0131] $CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC})$，

[0132] 其中符号“||”表示串联函数。

[0133] 在步骤2”中，MSC服务器607将“CS至PS HO请求”传送到目标SGSN 611，并将所生成的加密密钥($CK'_{PS} \,||\, IK'_{PS}$)和认证向量包含在此消息中。

[0134] 作为响应，在步骤3”中，目标SGSN 611向源SGSN/MME 609发送“上下文请求”，以便实现为UE 601请求上下文信息的目的。(此处和信令的其他表示中使用的虚线表示可选步骤。)SGSN/MME 609然后向目标SGSN 611回送“上下文响应”(包含所请求的信息，该请求的信息包含PS加密密钥和如UE 601支持的安全性算法的ID的其他安全性参数)(步骤4”)。

[0135] 在步骤615中，目标SGSN 611执行：

[0136] ·将从MSC 607接收的加密密钥发送到目标RNC 605以实现保护目标SGSN 611与UE 601(即客户端)之间的业务的目的

[0137] ·废弃从源SGSN/MME 609接收的任何PS密钥

[0138] ·废弃从MSC服务器607接收的AV

[0139] ·在一些但不一定所有的实施例中，存储从源SGSN 609接收的AV

[0140] ·在一些但不一定所有的实施例中，可以使用AV中的数据来对UE 601重新认证。

[0141] ·使用从源SGSN/MME 609接收用于为客户端(即UE 601)创建新安全性上下文所需的其他信息

[0142] 遵循步骤615，信令是根据如图3中所示以及图3的支持文本中描述的步骤5、6、7、8、9和10。

[0143] 可以从图7认识到与本发明相符的实施例的其他方面，图7是与本发明相符的备选实施例的信令图。具体来说，此示意图着重于支持目标PS节点能够作为将呼叫从CS域中工作的源UTRAN或GERAN支持设备切换到PS域中工作的目标E-UTRAN(即，4G)支持设备的一部分为客户端创建安全性上下文的多个方面。参与此信令的图示的组件是UE 701(客户端)、

源BSC/RNC 703、目标eNB 705、MSC服务器707、源SGSN/MME 709和目标MME 711.

[0144] 最初，UE 701启用多种源UTRAN或GERAN设备支持的CS呼叫。响应作出执行CS(UTRAN或GERAN)向PS(E-UTRAN)切换的决定，在步骤1'''中，源BSC/RNC 703向MSC服务器707发送"需要HO"消息。

[0145] MSC服务器707然后生成(步骤713)$NONCE_{MSC}$，并使用$NONCE_{MSC}$从与UE 701共享的现有密钥生成新的加密密钥。此密钥导出根据：

[0146] $CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC})$，

[0147] 其中符号"||"表示串联函数。

[0148] 在步骤2'''中，MSC服务器707将"CS至PS HO请求"传送到目标MME 711，并将新生成的加密密钥($CK'_{PS} \,||\, IK'_{PS}$)和AV包含在此消息中。将观察到MSC服务器707不具有LTE安全性参数，所以此通信中不传送(或无法传送)任何参数。

[0149] 作为响应，在步骤3'''中，目标MME 711向源SGSN/MME 709发送"上下文请求"，以便实现为UE 701请求上下文信息的目的。SGSN/MME 709然后向目标MME 711回送"上下文响应"(包含所请求的信息)(步骤4''')。此请求的信息包含PS密钥和LTE安全性参数(即，UE 701支持的LTE安全性算法的ID)。在源SGSN 709的上下文中，如果源SGSN 709与LTE标准的发行版8或更新相符，则有此信息可用。

[0150] 在步骤715中，目标MME 711执行：

[0151] ·通过如下操作创建映射的EPS安全性上下文：将映射的EPS安全性上下文的K'_{ASME}设为等于串联$CK'_{PS} \,||\, IK'_{PS}$，其中CK'_{PS}和IK'_{PS}是在CS至PS切换请求中接收的(参见步骤2''')。目标MME 711还将K'_{ASME}与KSI_{SGSN}。KSI_{SGSN}的值与CS至PS切换请求中接收的KSI'_{PS}的值。再有，作为此步骤的一部分，目标MME 711通过应用适用的标准中定义的KDF，使用映射的密钥K'_{ASME}和$2^{32}-1$作为上行NAS COUNT参数的值来导出K_{eNB}。在目标MME 711中，将用于映射的EPS安全性上下文的上行和下行NAS COUNT值设为起始值(即，0)。

[0152] ·废弃从源SGSN/MME 709接收的PS密钥

[0153] ·废弃从MSC服务器707接收的AV

[0154] ·可选地，存储从源SGSN 709接收的AV。(将没有从源MME 709接收的任何AV。)如果将有PS IRAT HO返回到从中接收这些AV所在的非常相同的源SGSN 709(在此情况中，在后来的切换时将这些AV返回到SGSN)，则这些存储的AV能够在后来被使用。

[0155] ·使用从源SGSN/MME 709接收用于为UE 701(即，为客户端)创建LTE安全性上下文所需的其他信息。此类附加信息可以是例如，KSI或CKSN，它们各为3位长字符串。例如，MME 711可以使用KSI/CKSN来标识LTE中的安全性上下文。

[0156] 遵循步骤715，信令是根据如图4中所示以及图4的支持文本中描述的步骤5'、6'、7'、8'、9'和10'。

[0157] 图8是PS域中工作的目标节点800(例如，SGSN/MME)的框图，其中目标节点800包括控制器801，控制器801是配置成除了典型的通信系统节点功能性外，还执行上文中结合图5至图7描述的多个方面中任何一个或组合的电路。此类电路可以是例如，完全硬连线电路(例如，一个或多个ASIC)。但是，图8的示范实施例中示出的是可编程电路，其包括耦合到一个或多个存储器装置805(例如，随机存取存储器、磁盘驱动器、光盘驱动器、只读存储器等)的处理器803。存储器装置805存储程序部件807(例如，处理器指令集)，程序部件807配置成

促使处理器803控制其他节点电路/硬件组件809，以便执行上文所述功能的任何一个功能。存储器805还可以存储数据811，数据811表示执行如程序部件807指定的那些功能的功能时处理器803可能接收、生成和/或其他需要的多种常量和多种参数。

[0158] 上文描述的与本发明相符的实施例的多个不同方面针对有关呼叫在CS与PS设备之间进行切换的问题提供解决方案，这些问题包括呼叫始发于CS域时如何生成PS域中有用的安全性上下文。

[0159] 本发明是参考特定实施例来描述的。但是对于本领域人员来说，将容易地显见到，采用与上文描述的实施例的形式所不同的特定形式来实施本发明是可能的。

[0160] 例如，多个不同方面，如从源CS节点获取一些信息以及从PS节点获取其他信息以及过滤和/或处理此信息以导出目标PS节点中有用的安全性上下文，即使某些其他细节有所更改时仍是适用的。例如，能够预见多个实施例，其中代之让MSC生成传送到目标PS节点(例如，目标SGSN或MME)的NONCE，而是目标节点(目标MME)能够自行生成NONCE，然后根据此生成的NONCE导出加密密钥。

[0161] 相应地，这些描述的实施例仅是说明性的而不应以任何方式视为限制。本发明的范围由所附权利要求而非由前文描述来给出，并且应将落在权利要求的范围内的所有变化和等效物涵盖在其中。

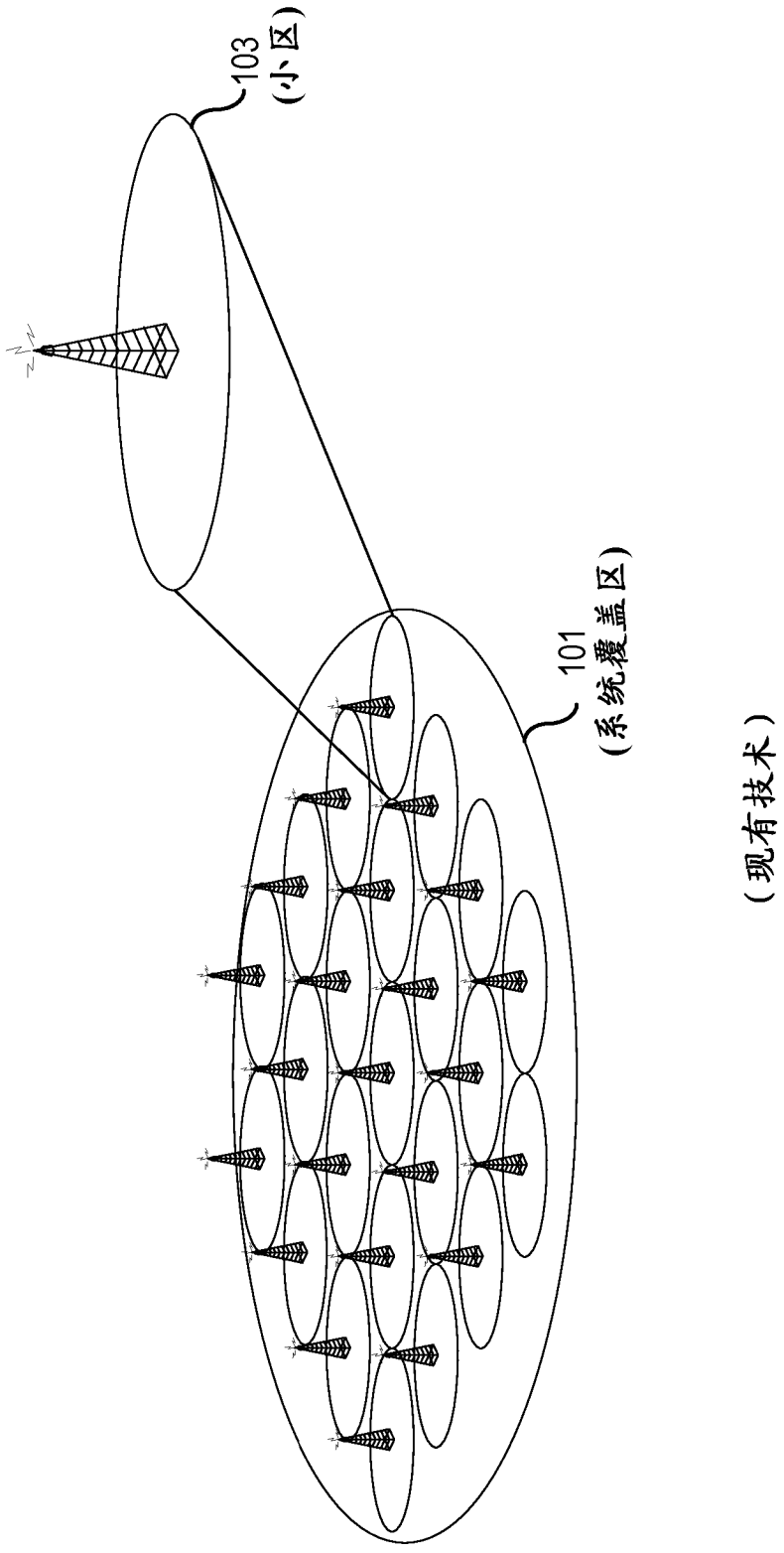


图 1

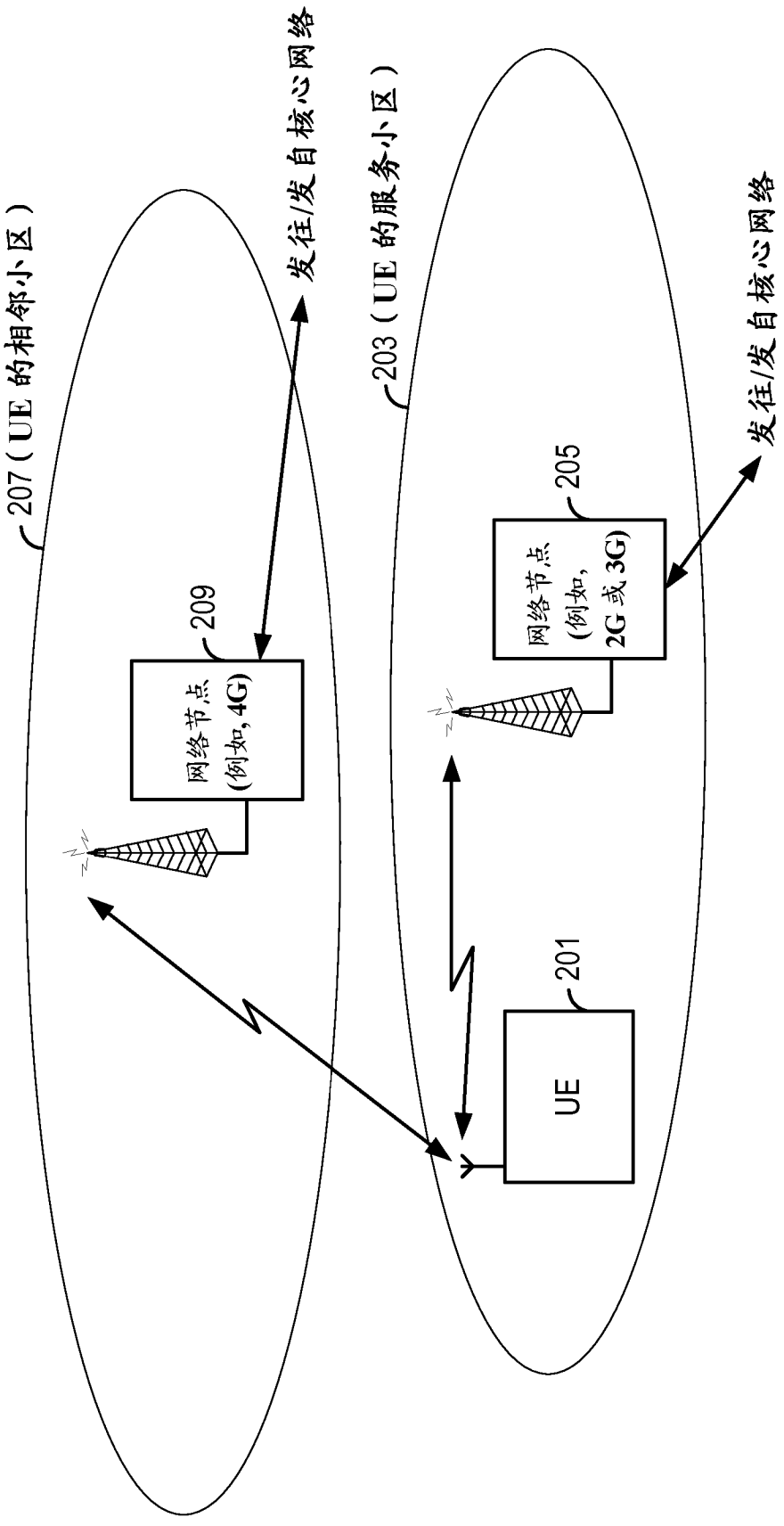

207（UE 的相邻小区）
发往/发自核心网络
209
网络节点
(例如, 4G)
203（UE 的服务小区）
205
网络节点
(例如,
2G 或 3G)
发往/发自核心网络
201
UE

图 2

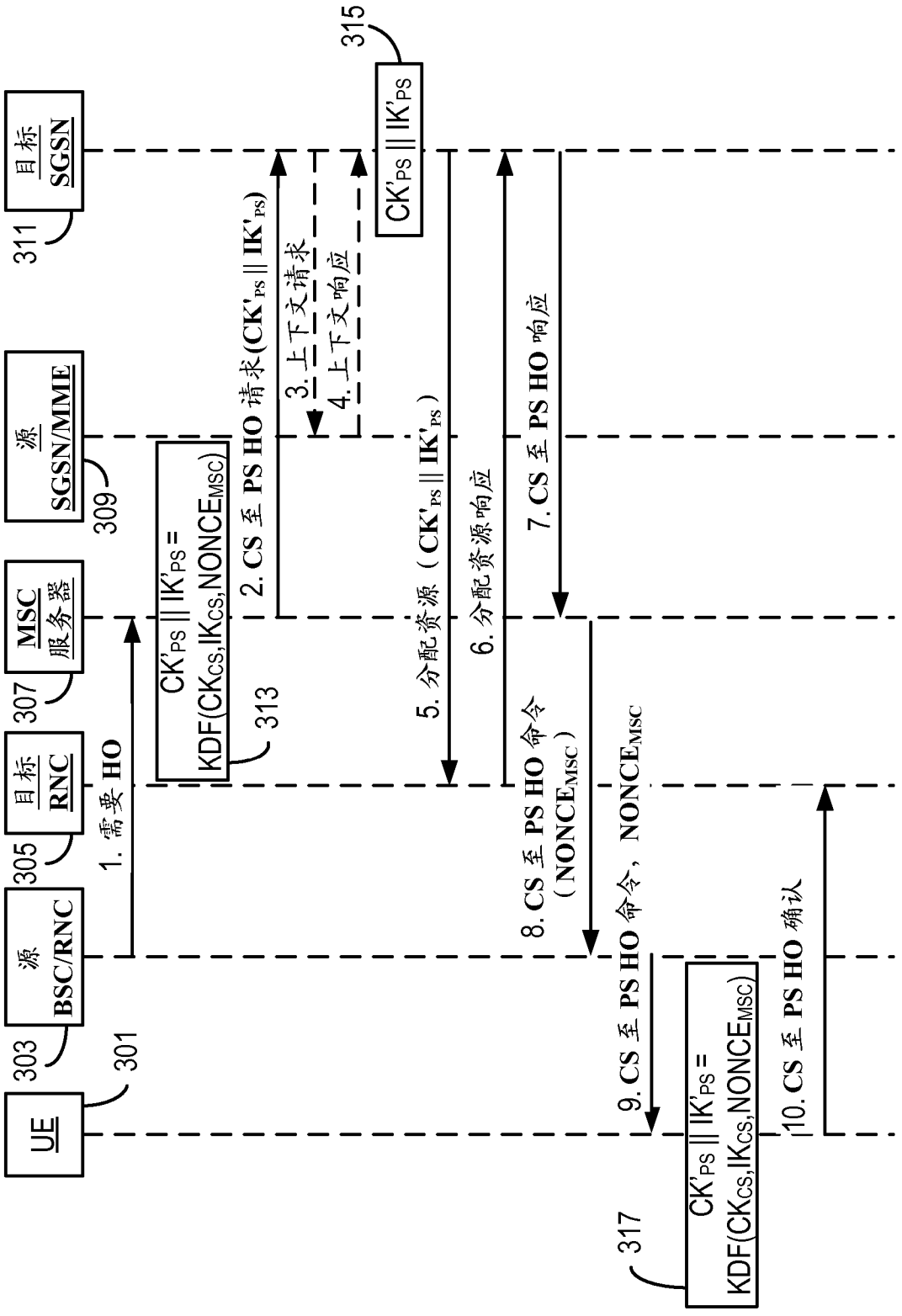

UE
301
源 BSC/RNC
303
目标 RNC
305
MSC 服务器
307
源 SGSN/MME
309
目标 SGSN
311
1. 需要 HO
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
313
2. CS 至 PS HO 请求(CK'PS || IK'PS)
3. 上下文请求
4. 上下文响应
315
CK'PS || IK'PS
5. 分配资源（CK'PS || IK'PS）
6. 分配资源响应
7. CS 至 PS HO 响应
8. CS 至 PS HO 命令（NONCEMSC）
9. CS 至 PS HO 命令，NONCEMSC
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
317
10. CS 至 PS HO 确认

图 3

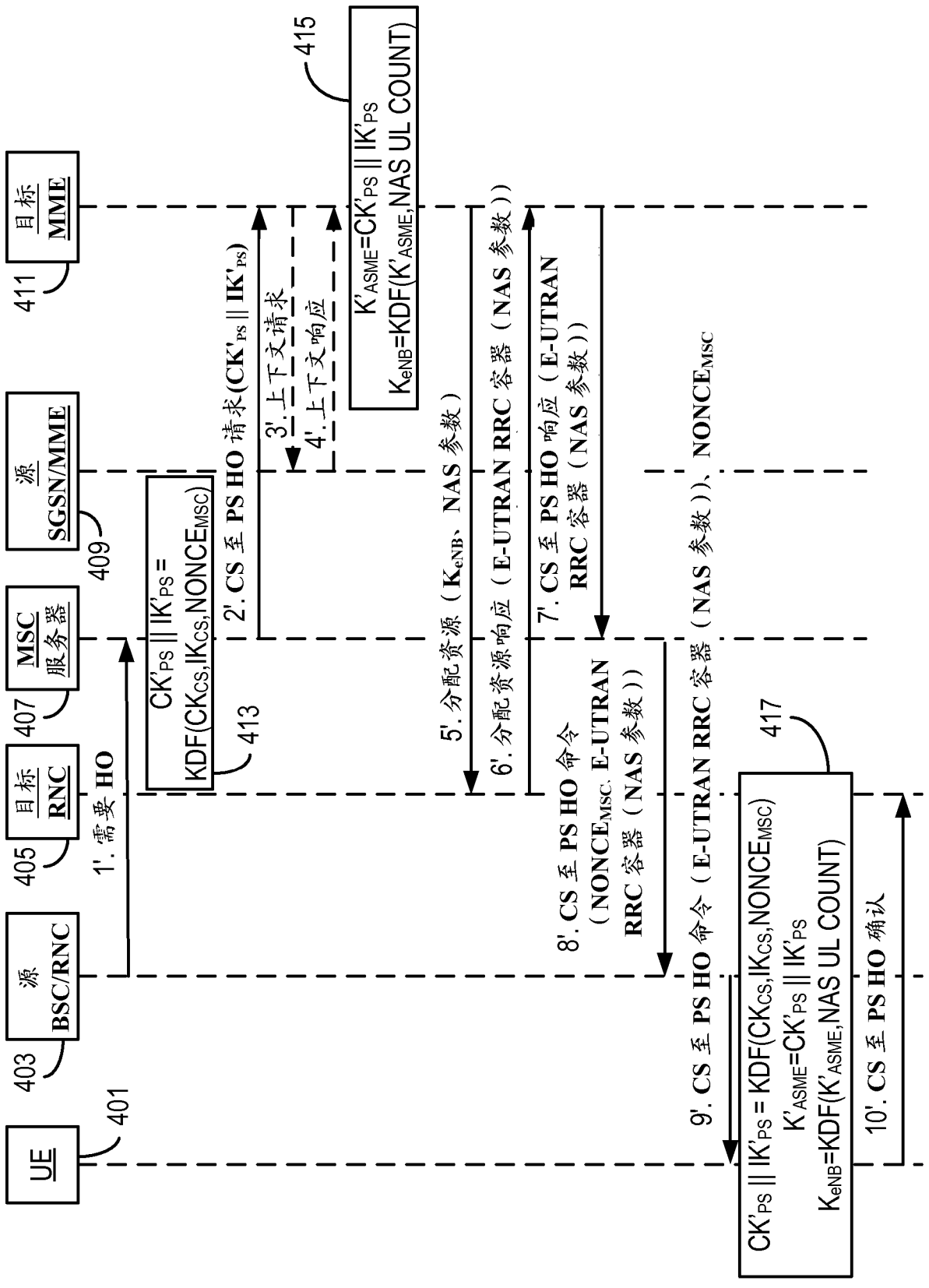

UE
401
源 BSC/RNC
403
目标 RNC
405
MSC 服务器
407
源 SGSN/MME
409
目标 MME
411
1'. 需要 HO
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
413
2'. CS 至 PS HO 请求(CK'PS || IK'PS)
3'. 上下文请求
4'. 上下文响应
K'ASME=CK'PS || IK'PS
KeNB=KDF(K'ASME,NAS UL COUNT)
415
5'. 分配资源（KeNB、NAS 参数）
6'. 分配资源响应（E-UTRAN RRC 容器（NAS 参数））
7'. CS 至 PS HO 响应（E-UTRAN RRC 容器（NAS 参数））
8'. CS 至 PS HO 命令（NONCEMSC、E-UTRAN RRC 容器（NAS 参数））
9'. CS 至 PS HO 命令（E-UTRAN RRC 容器（NAS 参数））、NONCEMSC
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
K'ASME=CK'PS || IK'PS
KeNB=KDF(K'ASME,NAS UL COUNT)
417
10'. CS 至 PS HO 确认

图 4

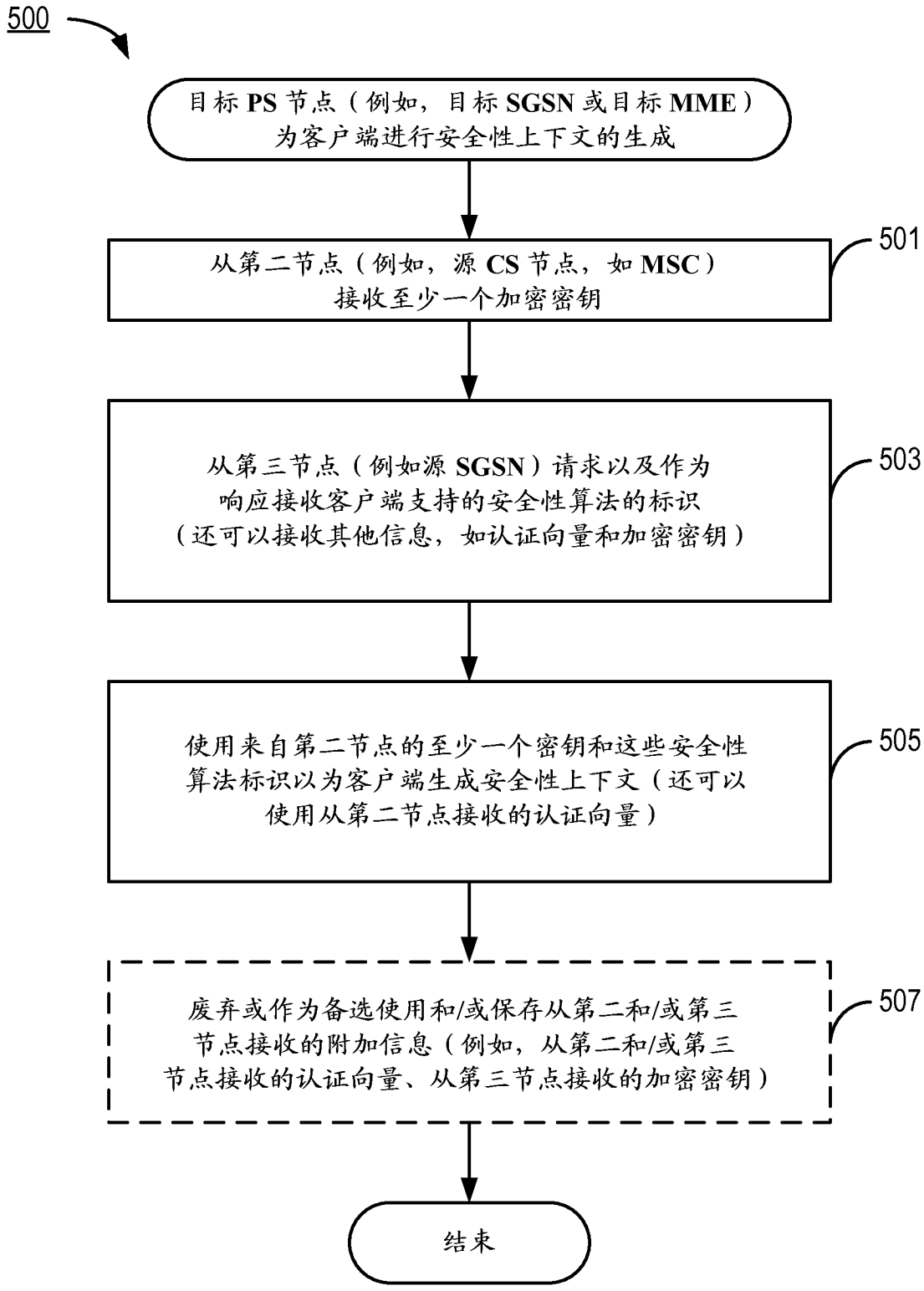

500
目标 PS 节点（例如，目标 SGSN 或目标 MME）为客户端进行安全性上下文的生成
从第二节点（例如，源 CS 节点，如 MSC）接收至少一个加密密钥
501
从第三节点（例如源 SGSN）请求以及作为响应接收客户端支持的安全性算法的标识（还可以接收其他信息，如认证向量和加密密钥）
503
使用来自第二节点的至少一个密钥和这些安全性算法标识以为客户端生成安全性上下文（还可以使用从第二节点接收的认证向量）
505
废弃或作为备选使用和/或保存从第二和/或第三节点接收的附加信息（例如，从第二和/或第三节点接收的认证向量、从第三节点接收的加密密钥）
507
结束

图 5

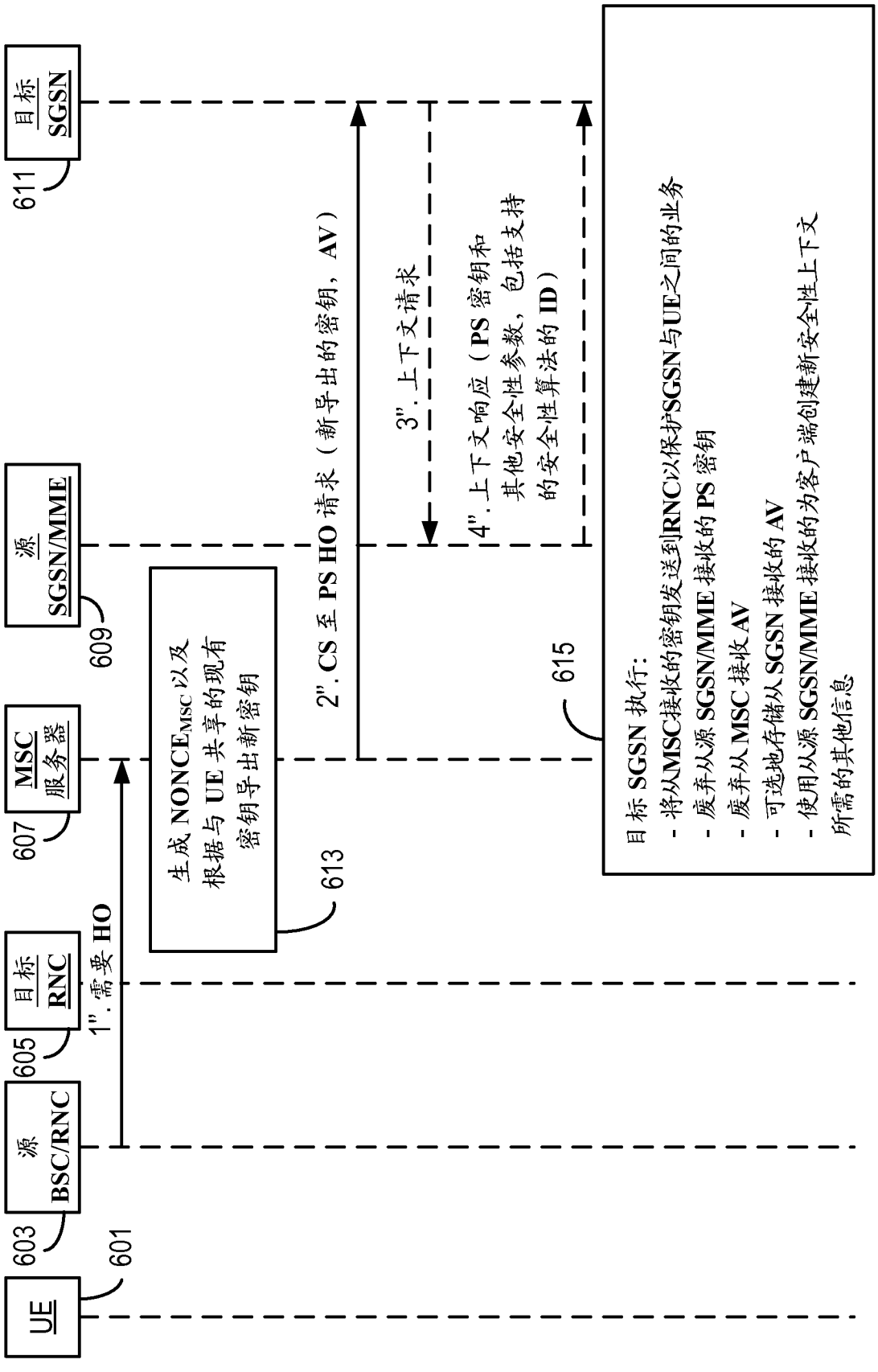

UE
601
源 BSC/RNC
603
目标 RNC
605
MSC 服务器
607
源 SGSN/MME
609
目标 SGSN
611
1". 需要 HO
生成 NONCE$_{MSC}$ 以及
根据与 UE 共享的现有
密钥导出新密钥
613
2". CS 至 PS HO 请求（新导出的密钥，AV）
3". 上下文请求
4". 上下文响应（PS 密钥和
其他安全性参数，包括支持
的安全性算法的 ID）
615
目标 SGSN 执行：
- 将从MSC接收的密钥发送到RNC以保护SGSN与UE之间的业务
- 废弃从源 SGSN/MME 接收的 PS 密钥
- 废弃从 MSC 接收 AV
- 可选地存储从 SGSN 接收的 AV
- 使用从源 SGSN/MME 接收的为客户端创建新安全性上下文
所需的其他信息
步骤 5、6、7、8、9 和 10 如图 3 所示

图 6

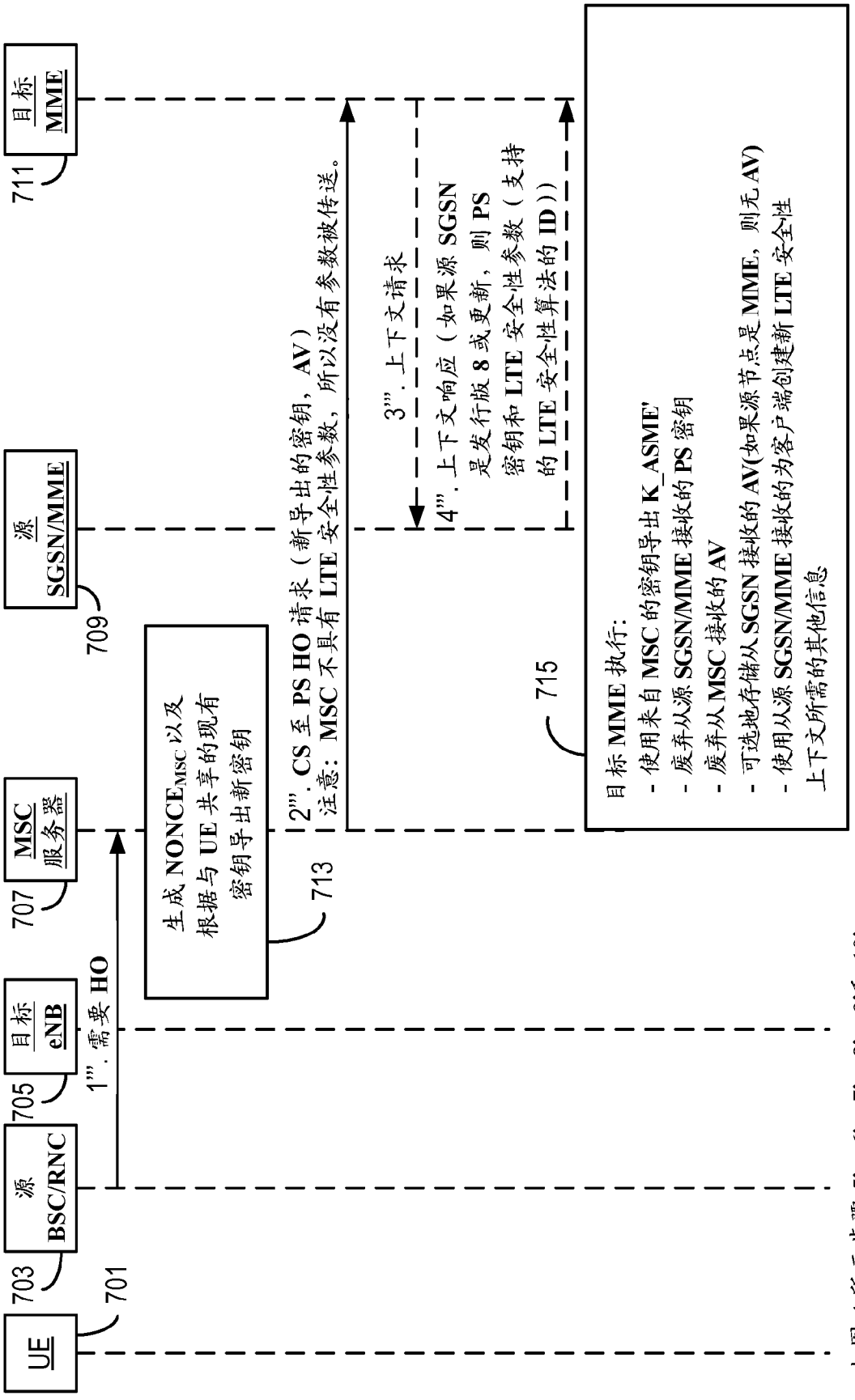

UE
701
源 BSC/RNC
703
目标 eNB
705
MSC 服务器
707
源 SGSN/MME
709
目标 MME
711
1'''. 需要 HO
生成 NONCE$_{MSC}$ 以及根据与 UE 共享的现有密钥导出新密钥
713
2'''. CS 至 PS HO 请求（新导出的密钥，AV）
注意：MSC 不具有 LTE 安全性参数，所以没有参数被传送。
3'''. 上下文请求
4'''. 上下文响应（如果源 SGSN 是发行版 8 或更新，则 PS 密钥和 LTE 安全性参数（支持的 LTE 安全性算法的 ID））
715
目标 MME 执行:
- 使用来自 MSC 的密钥导出 K_ASME'
- 废弃从源 SGSN/MME 接收的 PS 密钥
- 废弃从 MSC 接收的 AV
- 可选地存储从 SGSN 接收的 AV(如果源节点是 MME，则无 AV)
- 使用从源 SGSN/MME 接收的为客户端创建新 LTE 安全性上下文所需的其他信息
如图 4 所示步骤 5'、6'、7'、8'、9'和 10'

图 7

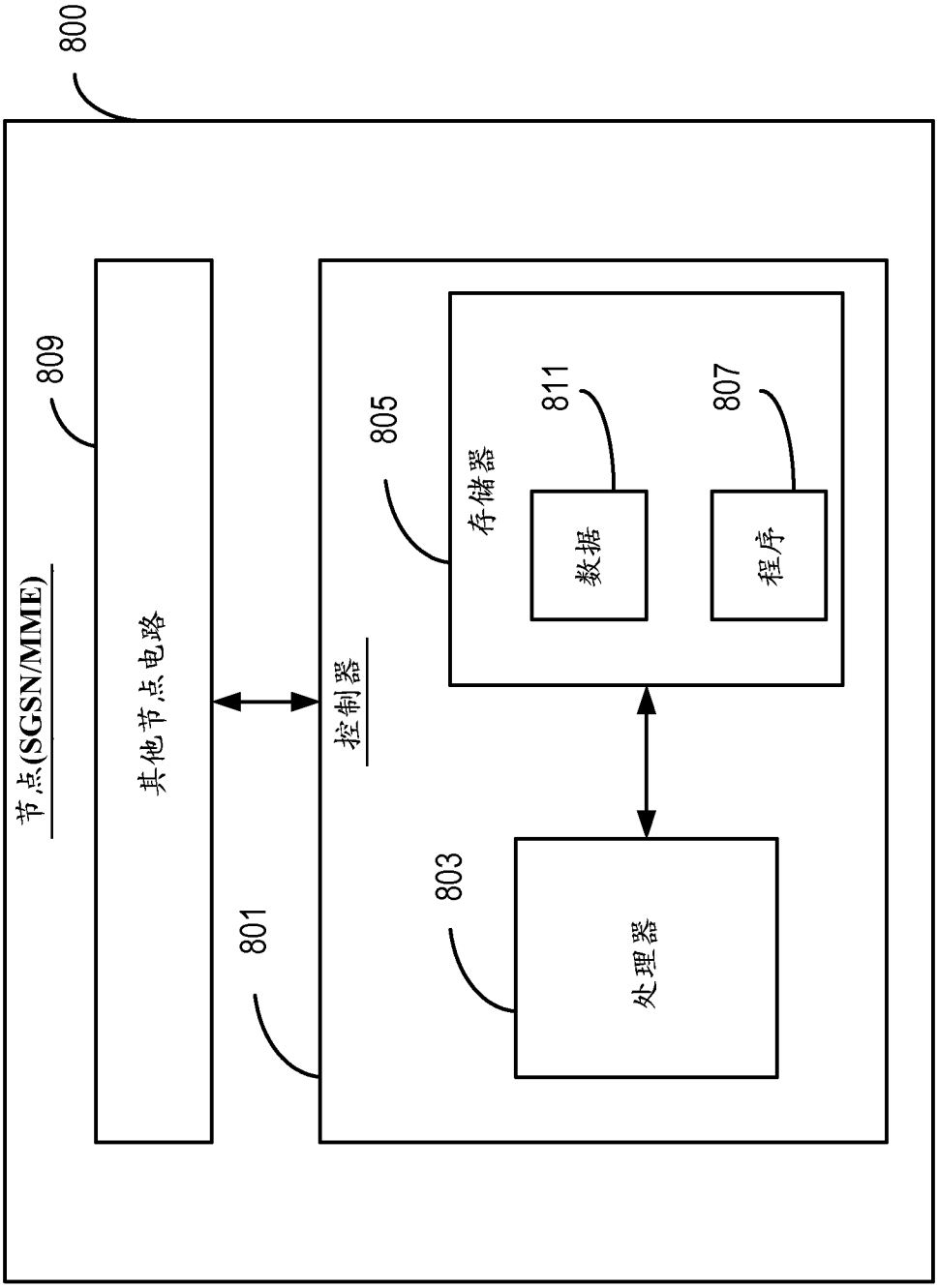


图 8