(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 102804826 B
(45)授权公告日 2016.03.02

(21)申请号 201180014253.9
(22)申请日 2011.03.16
(30)优先权数据
61/314,634 2010.03.17 US
(85)PCT国际申请进入国家阶段日
2012.09.17
(86)PCT国际申请的申请数据
PCT/EP2011/053999 2011.03.16
(87)PCT国际申请的公布数据
WO2011/113873 EN 2011.09.22
(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 卡尔·诺曼 托马斯·黑德伯格
马茨·内斯隆德
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮
(51)Int.Cl.
H04W 12/04(2006.01)
H04W 36/00(2006.01)
(56)对比文件
WO 2006/067561 A1,2006.06.29,
US 7181218 B2,2007.02.20,
CN 101257723 A,2008.09.03,
审查员 刘露玲

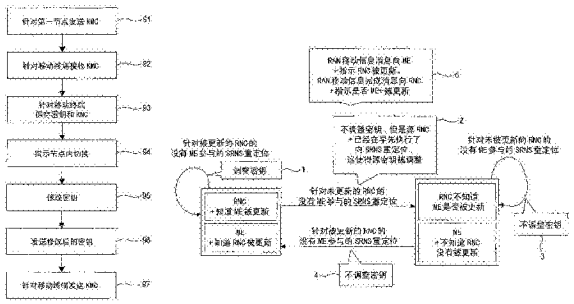
权利要求书2页 说明书18页 附图13页

(54)发明名称

用于SRNS重定位的增强密钥管理

(57)摘要

本申请公开了一种方法，该方法包括：在通过由至少一个第一密钥保护的连接服务于移动终端的第一节点中，保持所述第一密钥和与所述移动终端的密钥管理能力有关的信息。在将所述移动终端重定位到第二节点时，该方法包括：当且仅当所述密钥管理能力指示所述移动终端所支持的增强的密钥管理能力时，通过所述第一节点来修改所述第一密钥，由此创建第二密钥；将所述第二密钥从所述第一节点发送至所述第二节点；以及向所述第二节点发送与所述移动终端的密钥管理能力有关的信息。



CN 102804826 B

1. 一种用于服务无线电网络子系统 SRNS 重定位的增强密钥管理方法，包括：

在通过由至少一个第一密钥保护的连接服务于移动终端的第一无线电网络控制器中，保持所述第一密钥和与所述移动终端的密钥管理能力有关的信息；以及

在将所述移动终端重定位到第二无线电网络控制器时，

当且仅当所述密钥管理能力指示所述移动终端所支持的增强的密钥管理能力时，通过所述第一无线电网络控制器来修改所述第一密钥，由此创建第二密钥；

将所述第二密钥从所述第一无线电网络控制器发送至所述第二无线电网络控制器；以及

向所述第二无线电网络控制器发送与所述移动终端的密钥管理能力有关的所述信息。

2. 根据权利要求 1 所述的方法，还包括：

在所述第一无线电网络控制器修改所述第一密钥之前，所述第一无线电网络控制器指示所述移动终端执行到所述第一无线电网络控制器的节点内重定位。

3. 根据权利要求 1 或 2 所述的方法，其中，所述发送步骤是由所述移动终端或所述第一无线电网络控制器执行的。

4. 根据权利要求 2 所述的方法，包括：在与重定位的完成有关的一个或多个信令消息中发送所述信息。

5. 根据权利要求 1 或 2 所述的方法，包括：在重定位准备阶段，基于所述信息来确定所述移动终端是否支持所述增强的密钥管理能力。

6. 根据权利要求 1 或 2 所述的方法，其中，修改所述第一密钥包括：利用所述第一密钥和与所述第二无线电网络控制器有关的信息来修改所述第一密钥。

7. 根据权利要求 1 或 2 所述的方法，还包括：在将所述移动终端从第三无线电网络控制器重定位至所述第一无线电网络控制器时，从所述第一无线电网络控制器向所述移动终端发送与所述第一无线电网络控制器的密钥管理能力有关的信息。

8. 根据权利要求 7 所述的方法，还包括：在将所述移动终端从所述第三无线电网络控制器重定位之后，在所述第一无线电网络控制器处接收来自所述移动终端的与所述移动终端的密钥管理能力有关的信息。

9. 根据权利要求 7 所述的方法，包括：将所述信息包括在与所述移动终端从所述第三无线电网络控制器至所述第一无线电网络控制器的重定位的完成有关的一个或多个信令消息中。

10. 根据权利要求 7 所述的方法，其中，与所述第一无线电网络控制器的密钥管理能力有关的信息包括所述第一无线电网络控制器支持增强的密钥管理能力的信息。

11. 一种用于服务无线电网络子系统 SRNS 重定位的增强密钥管理方法，包括：

在第一无线电网络控制器通过由至少一个第一密钥保护的连接所服务的移动终端中，保持所述第一密钥和与所述第一无线电网络控制器的密钥管理能力有关的信息；以及

在将所述移动终端从所述第一无线电网络控制器重定位到第二无线电网络控制器时，

当且仅当所述密钥管理能力指示所述第一无线电网络控制器所支持的增强的密钥管理能力时，通过所述移动终端来修改所述第一密钥，由此创建第二密钥。

12. 根据权利要求 11 所述的方法，还包括：

在所述移动终端修改所述第一密钥之前，所述移动终端执行到所述第一无线电网络控

制器的节点内重定位。

13. 根据权利要求 11 或 12 所述的方法，还包括：从所述移动终端向所述第二无线电网络控制器发送与所述移动终端的密钥管理能力有关的信息。

14. 根据权利要求 11 或 12 所述的方法，还包括：在将所述移动终端重定位至所述第二无线电网络控制器之后，在所述移动终端处接收与所述第二无线电网络控制器的密钥管理能力有关的信息。

15. 根据权利要求 13 所述的方法，还包括：在与重定位的完成有关的一个或多个信令消息中发送所述信息。

16. 根据权利要求 11 或 12 所述的方法，其中，修改所述第一密钥包括：利用所述第一密钥和与所述第二无线电网络控制器有关的信息来修改所述第一密钥。

17. 一种用于服务移动终端的无线电网络控制器，所述无线电网络控制器包括：

模块，用于保持与由所述无线电网络控制器通过由至少一个第一密钥保护的连接所服务的移动终端的密钥管理能力有关的信息以及所述第一密钥；以及

模块，用于在将所述移动终端重定位到第二无线电网络控制器时，当且仅当所述密钥管理能力指示所述移动终端所支持的增强的密钥管理能力时，修改所述第一密钥，由此创建第二密钥；以及

模块，用于将所述第二密钥从所述无线电网络控制器发送至所述第二无线电网络控制器。

18. 根据权利要求 17 所述的无线电网络控制器，还包括：用于向所述第二无线电网络控制器发送与所述移动终端的密钥管理能力有关的信息的模块。

19. 一种移动终端，包括：

模块，用于保持与通过由至少一个第一密钥保护的连接服务所述移动终端的第一无线电网络控制器的密钥管理能力有关的信息以及所述第一密钥；以及

模块，用于在将所述移动终端从所述第一无线电网络控制器重定位到第二无线电网络控制器时，当且仅当所述密钥管理能力指示所述第一无线电网络控制器所支持的增强的密钥管理能力时，通过所述移动终端来修改所述第一密钥，由此创建第二密钥。

20. 根据权利要求 19 所述的移动终端，还包括：用于从所述移动终端向所述第二无线电网络控制器发送与所述移动终端的密钥管理能力有关的信息的模块。

用于 SRNS 重定位的增强密钥管理

技术领域

[0001] 本发明涉及一种使得节点能够保持与诸如相应节点的密钥管理能力之类的能力有关的信息（例如，服务于移动终端的节点可以保持与该移动终端的密钥管理能力有关的信息）的方法。本发明还涉及具有该能力的节点。

背景技术

[0002] 已知诸如无线电通信之类的无线通信由于其相对容易受到损害而需要通过加密进行保护（这里所使用的术语“无线”旨在包括电磁波（而不是某种有线形式）通过部分或整个通信路径承载信号的任意通信。将参照无线电通信描述本发明的示例，无线电通信使用无线电频率电磁波来承载通信，并且是无线通信的一个示例，但是本发明不局限于无线电通信）。为此，通常使用基于为无线网络或在其间发送无线通信的至少始发终端和端接终端所知（或者“共享”）的一个或多个密钥的加密方法来保护无线通信的安全。在一项已知的技术中，使用两个密钥“保密密钥”和“完整性密钥”作为信息 / 数据机密性和完整性 / 可靠性的基础。

[0003] 在许多情况下，在诸如无线电链路之类的无线链路上定义安全性。在移动终端（例如移动电话）与固定基站之间通信的情况下，这意味着移动终端和基站 BS（或“接入点”AP）是针对安全性的端接点，因此需要访问用于保护通信安全的密钥。然而，将密钥分发给多个容易访问的节点造成威胁，因为这增大了攻击者获得密钥的机会。

[0004] 这在 WCDMA（宽带码分多址接入，3G 移动电信网络中使用的一项标准）中已经不成问题，这是因为安全性在位于相对而言受到更好保护的位置处的无线电网络控制器 (RNC) 中结束。然而，在 LTE（“长期演进”）移动电信标准中，无线电链路保护的末端已经下移到更加暴露的基站（在 LTE 中称为“eNB”）。此外，新的 3G 演进 /HSPA（高速分组接入）架构使得 RNC 功能（或其部分，例如保密）移到基站（在 WCDMA 中称为“NodeB”）。这意味着必须保护基站中存储并使用的密钥。一种方式是改善密钥管理方式。

[0005] LTE 标准包括一特征 :密钥在每一个 LTE 内切换时改变。因此，如果“$K_{eNB}1$”表示用于保护图 1 中的移动终端（也称为移动设备 (ME)）1 与第一基站 2(eNB1) 之间的无线业务 4 的密钥，则在 ME 切换到新基站 3(eNB2) 之后，新基站 3 将不使用原始密钥 $K_{eNB}1$ 来与 ME1 通信。取而代之的是，在切换之后，新基站 3 将使用从原始密钥 $K_{eNB}1$ 推导的新密钥 $K_{eNB}2$，例如 $K_{eNB}2 = f(K_{eNB}1, eNB2\_ID)$，其中 eNB2_ID 是与新基站 3 相关联的标识符。在下文中，将函数 f 应用于密钥称为“调整 (tweaking)”密钥。函数 f 是密钥推导函数，通常基于适合的加密函数，例如（假定的）单向函数或伪随机函数。如果不止一个密钥需要调整，这可以通过使用一组函数 F 来实现，其中，针对 F 中的 f_i，应用 f_i 来获得第 i 个密钥。

[0006] 密钥 $K_{eNB}2$ 是第一基站 2 计算的，并从第一基站 2 经由通信信道（例如，X2 接口）发送至新基站 3，该通信信道连接这两个基站。由于 ME1 知悉函数 f，因此 ME 1 也可以通过本地执行相同的计算来推导出新密钥 $K_{eNB}2$(ME 仅仅需要 $K_{eNB}1$ 的知识和 eNB2 的标识，这二者是可得到的）。因此，在切换之后，使用新密钥 $K_{eNB}2$ 而不是使用原始密钥 $K_{eNB}1$ 来保护新基

站 3 与 ME 之间的无线通信 5。

[0007] 这意味着，即便有人能够从新基站 3 提取出新密钥 $K_{eNB}2$，在适当选择了函数 f 的情况下，在无法根据通过提取密钥 $K_{eNB}2$ 所取得的信息推导出原始密钥 $K_{eNB}1$ 的意义上，原始密钥 $K_{eNB}1$ 仍然是“安全的”。因此，入侵者无法记录第一基站 2 与移动终端 1 之间的加密业务，在 ME 已经切换到新基站 3（假设受到危害）之后无法获得密钥，并且无法使用密钥来破译至 / 自第一基站 2 的业务。

[0008] 应注意，在 LTE 中也存在用于在重定位时改变密钥（并且结合 ME 的特定状态改变）的其他机制。然而，这些机制全都需要另一个网络节点（所谓的移动管理实体 (MME)）生成新密钥，因此不对此进行进一步的讨论。

[0009] 应理解，希望在第一基站 2 计算新密钥 $K_{eNB}2$，这是因为否则的话可能至少暂时在新基站 3 中也暴露原始密钥 $K_{eNB}1$。

[0010] 当前的 WCDMA 网络除非运行认证密钥管理 (AKA) 过程，否则无法改变密钥，AKA 过程强加了信令延迟，并导致 AuC/HLR（认证中心 / 归属位置寄存器）、RNC、MSC（移动交换中心）和其他节点上的负载。

[0011] 当前在 3GPP 中有一个工作组研究 UTRAN 的密钥管理增强 (TS 33.102，3rd Generation Partnership Project ;Technical Specification Group Services and System Aspects ;3G Security ;Security architecture，http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/33102-910.zip)，即，针对基于 WCDMA 的接入网络。其目的是着眼于针对在切换时改变密钥的问题的方案。然而，到现在为止，几乎没有对解决方案进行任何讨论，并且迄今为止该研究仅仅讨论了如何在将密钥从核心网 (VLR/MSC/SGSN) 传送到 RNC 时（即，在初始附着或在路由区域更新 (RAU) 时）改变密钥。核心网 (CN) 与无线电接入网 (RAN) 之间的“垂直”密钥改变的问题比 RAN 内的“水平”密钥改变的问题简单得多，并且所具有的解决方案很大程度上独立于针对 RAN 内的“水平”密钥改变的解决方案。已经肯定在 SRNS 重定位时（即，当 ME 改变其服务 RNC 时）也应该可以改变密钥，但具体如何实现仍然是开放的（参见 S3-100319，3GPPTR 33.ukh V0.3.0(2010-02)）。

[0012] 考虑现有 3GPP 规范中定义的移动 / 切换的不同情况，对于任意完整规定的解决方案，需要考虑的三种情况的“水平”密钥推导。这些情况与导致 RNC 改变的移动性事件一致 :SRNS(Serving Radio Network Subsystem)relocation without ME involvement（参见 TS 23.060 的 6.9.2.2.1，3rd Generation Partnership Project ;Technical Specification Group Services and System Aspects ;General Packet Radio Service (GPRS) ;Service description ;Stage 2，http://www.3gpp.org/ftp/Specs/archive/23_series/23.060/23060-930.zip)，combined hard handover and SRNS relocation（参见 TS23.060 的 6.9.2.2.2) 和 combined cell/URA update and SRNS relocation（参见 6.9.2.2.3 of TS 23.060)。相比较而言，在 LTE 标准中，存在的唯一情况是与组合的硬切换和 SRNS 重定位相对应的情况。换言之，无法在 UTRAN 中以任何直接方式采用现有的 LTE 解决方案，因为它不覆盖所有情况。此外，在 LTE 中不存在与传统终端和网络设备的互操作性的问题，因为它从一开始就被设计为支持上述密钥改变机制。下面将讨论在已经部署的、但不具有这种功能的网络中引入这种密钥改变机制的问题。

[0013] 在执行没有 ME 参与的 SRNS 重定位的情况下，网络将服务 RNC 从源 RNC（“源 RNC”

是当前正在提供服务的 RNC) 改变到目标 RNC(当前正在变化的 RNC),即便 ME 保持连接到同一个基站 (NodeB)。这在图 2(a) 中示出,图 2(a) 示出了两个 RNC,连接到核心网 7 的 6a(或 RNC 1) 和 6b(或 RNC 2)。每一个基站都由一个 RNC 控制,例如如图 2(a) 所示,两个基站 8a(NodeB1) 和 8b(NodeB2) 由 RNC 1 控制,以及一个基站 8c(NodeB3) 由 RNC2 控制。在 SRNC 重定位之前,ME 1 由一个 RNC(例如,RNC1) 经由基站 (NodeB1) 服务。在 SRNS 重定位之后,如图中的虚线所示,ME 由另一个 RNC(例如,RNC2) 经由与 SRNS 重定位之前相同的基站服务。只有在没有 ME 参与的 SRNS 重定位过程结束时,目标 RNC(在本示例中,RNC2 是目标 RNC) 才向 ME 通知服务 RNC 的改变。因此,在完成之前,ME 不知道 RNC 的改变,并且这使得 ME 很难确定使用了哪些密钥来保护特定消息 (稍后更详细描述)- 针对 UTRAN 所采用的任意解决方案必须克服这个问题。

[0014] 在利用 SRNS 重定位的组合的硬切换中,源 RNC 通知 ME 它应当改变基站,以及同时通知它要由目标 RNC 服务。这在图 2(b) 中示出,图 2(b) 示出了连接到核心网的两个 RNC。在 SRNS 重定位之前,ME 1 由一个 RNC 经由基站服务,例如由 RNC1 经由基站 NodeB1 服务。在 SRNS 重定位之后,如虚线所示,ME 由另一个 RNC(例如,RNC2) 经由与 SRNS 重定位之前不同的基站 (例如,基站 NodeB3) 服务。

[0015] 在利用 SRNS 重定位更新的组合的小区 /URA 中,ME 意识到它已经移进新小区,并向源 RNC 发送更新消息。这在图 2(c) 中示出,图 2(c) 示出了连接到核心网的两个 RNC。注意,图 2(c) 与图 2(b) 相同,除了信令顺序不同。在重定位之前,ME1 由一个 RNC 经由基站服务,例如由 RNC1 经由基站 NodeB1 服务。在重定位之后,如虚线所示,ME1 由另一个基站服务,另一个基站可以是由与重定位之前的基站相同的 RNC 服务的基站 (例如 NodeB2) 或者备选地可以是由与重定位之前的基站不同的 RNC 服务的基站 (例如,由 RNC2 而不是 RCN1 服务的 NodeB3)。网络判断更新是否是可接受的,并且如果是,则将服务 RNC 改变为目标 RNC(如果需要的话),然后目标 RNC 向 ME 通知 RNC 的改变。仅在该过程结束时,再一次向 ME 通知 RNC 的改变。

[0016] 在 SRNS 重定位期间,源和目标 RNC 经由核心网彼此通信,以协调重定位。在较新版本的 UTRAN 标准中,还存在称为增强 SRNS 重定位的过程,其中 RNC 经由 Iur 接口 (如图 2(a) 至 2(c) 示意性示出的) 彼此直接通信。

[0017] ME 和网络侧独立提供密钥调整的现有方案在上面所讨论的过程中有很多问题。例如,如上面所提到的,新的 3G 演进 /HSPA 架构允许 RNC 与 NodeB 共同定位 (可能在相同的硬件机壳中)。这意味着,在网络外围 (无线电设备机壳可能位于黑客在物理上攻击以访问保密密钥的不友善环境中) 的位置中执行保密和完整性保护。这使得必须调查 HSPA 中使用的密钥的增强保护。具体地,在 SRNS 重定位时改变 RNS 的情况下改变密钥是有益的。然而,与 LTE 标准不同的是,没有将系统设计为从一开始就考虑在重定位时改变密钥的需要。如果引入了在重定位时改变密钥的特征,则需要提供 :

[0018] - 在与传统设备互相作用时的后向兼容。

[0019] - 与现有信令的后向兼容,尽可能不改变现有过程。

[0020] 应注意,WiMAX(IEEE 802.16) 和 WLAN(IEEE 802.11) 都不包括在 BS 间 /AP 间切换时改变密钥 (作为切换过程的必要部分) 的标准化的方式。相反,在这些无线电接入技术中,在切换时改变密钥的唯一可能性基于在终端 (STA) 与目标 BS/AP 之间执行完整的 (或

在 WLAN 的情况下优化的 802.11r) 认证。这在 WCDMA 中是不可接受的，因为期望零信令开销（从密钥管理的角度，当然会有移动信令发生）。

发明内容

[0021] 本发明的第一方面提供了一种方法，包括在通过由至少一个第一密钥保护的连接服务于移动终端的第一节点中，保持所述第一密钥和与所述移动终端的密钥管理能力有关的信息。在将所述移动终端重定位到第二节点时，当且仅当所述密钥管理能力指示所述移动终端所支持的增强的密钥管理能力时，所述第一节点修改所述第一密钥，由此创建第二密钥，将所述第二密钥从所述第一节点发送至所述第二节点。向所述第二节点发送与所述移动终端的密钥管理能力有关的信息。

[0022] 本发明使得节点（在这种情况下为第一节点）可以保持与相应节点（在这种情况下为移动终端）的密钥管理能力有关的信息。例如，节点可以是 RNC，例如第一节点可以是被更新的源 RNC，第二节点可以是目标 RNC（可以被更新或者可以不被更新）。在移动终端重定位到第二节点时，当且仅当与移动终端的密钥管理能力有关的信息指示移动终端支持增强的密钥管理能力时，第一节点修改第一密钥，以创建第二密钥，否则第一节点不修改第一密钥。因此，如果第一节点从保持的信息中获悉移动终端能够调整密钥，则第一节点在重定位时调整密钥是安全的，因为第二节点和移动终端将能够在重定位之后利用所调整的密钥来进行通信。本发明因此确保 (1) 第一节点和移动终端均修改第一密钥；或者 (2) 第一节点和移动终端都不修改第一密钥，以使得在重定位之后在网络侧使用的密钥与在重定位之后在移动侧使用的密钥相同。此外，将与是否更新移动终端有关的信息发送至目标 RNC，以使得目标 RNC 意识到移动终端是否被更新（假设目标 RNC 被更新；如果目标 RNC 没有被更新，那么将忽略从源 RNC 接收到的信息）。

[0023] 在连接由两个或多个密钥保护的情况下，理论上可能只改变（调整）一些密钥，从而不是所有密钥都被改变。然而，实际上，通常期望以最大的安全性来改变密钥（在支持增强的密钥管理能力的情况下）。

[0024] 此外，向第二节点发送与移动终端的密钥管理能力有关的信息意味着：在第二节点随后将移动终端交付给另一节点时，第二节点将意识到移动终端是否是能够在重定位时调整密钥的更新后的移动终端。第二节点由此知道它是否能够在更新移动终端的后续重定位时（再次假设目标 RNC（第二节点）调整密钥；如果目标 RNC 不被更新，则如先前所提及的，将忽略从源 RNC 接收的信息）。

[0025] 该方法还包括：在所述第一节点修改所述第一密钥之前，所述第一节点指示所述移动终端执行到所述第一节点的节点内重定位。

[0026] 与移动终端的密钥管理能力有关的信息可以由所述移动终端或所述第一节点发送到第二节点。

[0027] 该信息可以在与重定位的完成有关的一个或多个信令消息中发送。这使得本发明在不需要在重定位时交换任何附加消息就能实现。

[0028] 第一节点可以在重定位准备阶段，基于所述信息来确定所述移动终端是否支持所述增强的密钥管理能力。重定位通常包括两个阶段：准备阶段和执行阶段。两个阶段都包括在源 RNC 与目标 RNC 之间的特定信令。例如，重定位“准备阶段”可以如 3GPP TS 25.331

针对有UE参与的SRNS重定位情况、没有UE参与的SRNS重定位情况、以及组合的小区/URA更新和SRNS重定位情况所定义的。在本实施例中，当源RNC确定该将终端重定位到目标RNC时，源RNC开始准备阶段时，然后可以确定移动终端是否支持增强的密钥处理。此后，源RNC可以选择通过还运行执行阶段来完成重定位。

[0029] 修改所述第一密钥可以包括：利用所述第一密钥，并且可选地但优选地也利用与所述第二节点有关的信息，来修改所述第一密钥。

[0030] 该方法可以包括：在将所述移动终端从第三节点重定位至所述第一节点时，从所述第一节点向所述移动终端发送与所述第一节点的密钥管理能力有关的信息。

[0031] 该特征涉及：在移动终端的较早重定位时，即，重定位到更新的目标RNC（第一节点假设为被更新），第一节点是“目标”节点。在重定位时，向移动终端发送目标RNC（第一节点）是更新的RNC的信息，以使得移动终端意识到：在重定位之后，它正在由更新的RNC服务（假设，移动终端被更新；如果移动终端不被更新，则将忽略从目标RNC接收到的信息）。

[0032] 该方法还可以包括：在将所述移动终端从所述第三节点重定位至所述第一节点之后，在所述第一节点处接收来自所述移动终端的与所述移动终端的密钥管理能力有关的信息。例如，如果移动终端被更新，则它将向目标RNC通知。在较早重定位中的目标RNC（即，第一节点）存储它接收到的与移动终端的密钥管理能力有关的任何信息。

[0033] 可以在与所述移动终端从所述第三节点重定位至所述第一节点的完成有关的一个或多个信令消息中包括并发送所述信息，再次避免在重定位时交换任何附加消息的需要（与现有的系统/信令方案相比）。

[0034] 由第一节点发送至移动终端的与所述第一节点的密钥管理能力有关的信息可以包括所述第一节点支持增强的密钥管理能力的信息。

[0035] 本发明的第二方面提供了一种方法，该方法包括：在第一节点通过由至少一个第一密钥保护的连接所服务的移动终端中，保持所述第一密钥和与所述第一节点的密钥管理能力有关的信息。在将所述移动终端从所述第一节点重定位到第二节点时，当且仅当所述密钥管理能力指示所述第一节点所支持的增强的密钥管理能力时，所述移动终端修改所述第一密钥，由此创建第二密钥。例如，第一节点可以是RNC。移动终端（被更新的）意识到正在服务移动终端的RNC是否被更新，并因此将在重定位到目标RNC（第二节点）时调整密钥。

[0036] 该方法还可以包括：在所述移动终端修改所述第一密钥之前，所述移动终端执行到所述第一节点的节点内重定位（在接收到来自第一节点的指令时进行）。

[0037] 该方法还可以包括：当移动终端从第一节点切换到第二节点时，移动终端向第二节点发送与移动终端的密钥管理能力有关的信息。

[0038] 该信息可以包括在与重定位的完成有关的一个或多个信令消息中。

[0039] 修改所述第一密钥包括：利用所述第一密钥，并且可选地但优选地利用与所述第二节点有关的信息，修改所述第一密钥。

[0040] 本发明的第三方面提供了一种用于服务移动终端的节点，所述节点包括：用于保持与由所述节点通过由至少一个第一密钥保护的连接所服务的移动终端的密钥管理能力有关的信息以及所述第一密钥的模块。该节点还包括：用于在将所述移动终端重定位到第二节点时，当且仅当所述密钥管理能力指示所述移动终端所支持的增强的密钥管理能力

时，修改所述第一密钥，由此创建第二密钥的模块，并且还具有用于将所述第二密钥从所述第一节点发送至所述第二节点的模块。

[0041] 该节点还可以包括：用于向所述第二节点发送与所述移动终端的密钥管理能力有关的信息的模块。

[0042] 本发明的第四方面提供了一种移动终端，包括：用于保持与通过由至少一个第一密钥保护的连接服务所述移动终端的第一节点的密钥管理能力有关的信息以及所述第一密钥的模块。该移动终端还可以包括用于在将所述移动终端从所述第一节点重定位到第二节点时，当且仅当所述密钥管理能力指示所述第一节点所支持的增强的密钥管理能力时，通过所述移动终端来修改所述第一密钥，由此创建第二密钥的模块。

[0043] 该移动终端还可以具有：用于从所述移动终端向所述第二节点发送与所述移动终端的密钥管理能力有关的信息的模块。

[0044] 在第三方面的节点或第四方面的移动终端中，模块可以采用硬件实现为单独的硬件模块，或组合在一个硬件模块中，或者它们可以实现为在适当变成的处理器上操作的一个或多个软件模块，或者它们可以实现为硬件和软件模块的组合。

附图说明

[0045] 将参照附图，作为示例描述本发明的优选实施例，在附图中：

[0046] 图 1 示意了在至 / 自移动终端的通信中的“密钥调整”的原理；

[0047] 图 2(a) 示意了没有 ME 参与的 SRNS 重定位；

[0048] 图 2(b) 示意了利用 SRNS 重定位的硬切换；

[0049] 图 2(c) 示意了利用 SRNS 重定位更新的组合的小区 /URA；

[0050] 图 3 示意了根据本发明的第一实施例的方法中的消息流；

[0051] 图 4 示意了根据第一实施例的方法的主要步骤；

[0052] 图 5 示意了根据本发明的第二实施例的方法中的消息流；

[0053] 图 6 示意了根据第二实施例的方法的主要步骤；

[0054] 图 7 示意了根据本发明的第三实施例的方法中的消息流；

[0055] 图 8 示意了根据第三实施例的方法的主要步骤；

[0056] 图 9 是示出了根据本发明的实施例的方法的主要步骤的流程框图；

[0057] 图 10 是示出了根据本发明的另一实施例的方法的主要步骤的流程框图；

[0058] 图 11 是示出了根据本发明的实施例的节点的主要组件的框图；

[0059] 图 12 是示出了根据本发明的实施例的移动终端的主要组件的框图。

具体实施方式

[0060] 为了讨论的简单起见，用“RNC+”表示能够知道应当在 SRNS 重定位时改变密钥（如果可能的话）的被更新的 RNC。类似地，“ME+”表示被更新的 ME，这是也意识到可能需要在 SRNS 重定位时改变密钥的 ME。“源 RNC”或“源 RNC+”是在重定位之前（经由基站）服务 ME/ME+ 的 RNC 或 RNC+，“目标 RNC”或“目标 RNC+”是在重定位之后服务 ME/ME+ 的 RNC 或 RNC+。

[0061] 要解决的问题包括：

[0062] - 重定位之后在网络中（即，在目标 RNC(+) 中）使用的密钥始终与重定位之后在 ME(+) 中使用的密钥相同是至关重要的，因为否则的话安全性处理将失败，并且丢失到网络的连接。

[0063] - 期望在尽可能多的情况下在重定位时改变密钥，即，如果移动终端是 ME+，并且至少一个源或目标 RNC 是 RNC+，则期望改变密钥。

[0064] - 期望在源 RNC 中使用的密钥在尽可能大的程度上对于目标 RNC 保密。在实践中，这意味着应当在将密钥传送至目标 RNC（可以更新或者可以不更新）之前在源 RNC+ 中执行密钥改变（密钥调整）（可能的话）。

[0065] 作为 ME，源 RNC 和目标 RNC 均可以更新或者可以不更新，存在多种情形，例如：

[0066] 1. 如果在从 RNC+ 到 RNC+ 的 SRNS 重定位中涉及 ME+，则期望密钥在 ME+ 和源 RNC+ 二者中都发生改变（假设密钥在源 RNC+ 中改变，并且给目标 RNC+ 传送新密钥）。ME+ 和 RNC+ 如何（相互）获悉彼此的能力？如果 ME+ 和 RNC+ 均没有被适当地通知另一方的能力，则 ME+ 和 RNC+ 之一可以执行密钥修改，而另一方不执行，从而会导致密钥失配，这意味着例如加密失败并且因此将丢失到网络的连接。

[0067] 2. 如果在 RNC 与 RNC+ 的任意组合（即，RNC+ 到 RNC 或 RNC 到 RNC+）之间的 SRNS 重定位中涉及 ME+，则网络侧必然不改变密钥，这是因为密钥不能在 ME 侧改变。假设源 RNC 是 RNC+，那么它如何获悉要给目标 RNC 提供哪些密钥，即它如何获悉 ME 实际上是否是 ME+ 和 / 或目标 RNC 是否能够处理密钥调整？

[0068] 3. 如果 ME+ 执行从 RNC 到 RNC 的重定位，那么密钥必然不在 ME+ 中改变，这是因为密钥肯定不会在 RNC 侧改变（当源 RNC 和目标 RNC 均为传统 RNC 时）。由于 ME+ 不知道 RNC 是否被更新，那么 ME+ 如何获悉是否要“调整”密钥？

[0069] 4. 如果 ME+ 执行源和目标 RNC 为不同类型的情况下的重定位（即，RNC+ → RNC 或 RNC → RNC+），那么是否可以改变密钥？如果可以，则是目标 RNC 还是源 RNC 改变密钥？ ME+ 如何获悉密钥是否在网络侧被调整，即，它是否应当调整密钥？

[0070] 5. 如果 ME+ 从一个 RNC（已更新或未更新）切换到 RNC+，则目标 RNC+ 如何获悉 ME 是 ME+ ？

[0071] 如先前所说明的，这些问题不会出现在根据当前 LTE 标准操作的终端和网络中，因为移动网络和终端将始终能够在重定位时调整密钥 - 以使得网络和移动终端始终都知道另一实体能够改变密钥。此外，在 LTE 标准中，如上所述，密钥改变始终与图 2(b) 所示的硬切换相关联，并且在 LTE 中不出现图 2(a) 和 2(c) 所示的切换。然而，如果将来在 LTE 中引入增强的密钥管理能力和 / 或新的重定位机制，本发明也可以应用于其中。

[0072] 将参照图 2(a) 至 2(c) 所述的三种可能的重定位方案来描述本发明的实施例。如上所述，源和目标 RNC 可以经由核心网彼此通信，以协调重定位，或者在较新版本的 UTRAN 标准中，RNC 可以经由 Iur 接口彼此直接通信。为了简单起见，以下说明描述在 RNC 可以彼此直接通信时如何实现本发明，但是本发明可以容易地应用于 RNC 经由核心网彼此通信的情况。

[0073] 将参照通过两个或多个密钥（例如，保密密钥和完整性密钥）来保护 RNC 与 ME 之间的通信安全的实施例来描述本发明，并且因此本发明将涉及改变或“调整”密钥，但是本发明可以容易地应用于仅通过单个密钥来保护 RNC 与 ME 之间的通信安全的情况，这是因为

可以应用相同原理。类似地，在使用多个密钥的情况下，可以将“调整”应用于所有密钥，或者仅应用于选择的密钥子集，例如分组交换 (PS) 域密钥，但不应用于电路交换 (CS) 域密钥等。

[0074] 此外，下面描述的本发明将集中于决定（在 ME+ 和源 / 目标 RNC+ 中，互相地）是否修改（调整）密钥的问题。因此，假设密钥修改函数（上面指出的 f）是固定的，因此仅就应用 f 或是不应用 f 进行选择。然而，在一般情况下，也存在应用哪种函数 f 的不同选择。具体地，本发明涉及保持与对一个或多个密钥管理能力的支持（除了对给定 f 函数的支持 / 不支持以外，通常还可以包括支持哪些 f 函数（如果有的话））有关的信息。另外，可以采取类似方式处理较为普遍的安全能力。

[0075] 此外，本发明不涉及密钥修改函数的具体形式，并且可以使用任意适当的密钥修改函数。作为示例，密钥修改函数可以利用密钥，并且可选地但优选地，也利用与目标节点有关的信息，来修改密钥，例如可以根据 $K_{eNB}2 = f(K_{eNB}1, eNB2\_ID)$ 来修改密钥，但这仅仅是一个可能的示例，并且本发明不局限于此。

[0076] 在所有实施例中，密钥修改函数 f 优选地基于适当的（强）密钥函数，例如 SHA256、HMAC、AES 等等。

[0077] 在本发明的描述中，将使用以下术语：

[0078] 传统实体 不知道增强密钥处理的实体

[0079] 被更新的实体 被更新的能够处理增强密钥处理的实体

[0080] 术语“源”和“目标”通常指的是在 RNC 改变之前 / 之后 ME 连接到的实体。

[0081] 如以上所使用的，被更新的实体的名称附有 + 符号，例如被更新的 ME 写成“ME+”。如果实体是否被更新或者特定属性是否应用于被更新的实体和传统实体二者不相关，则使用符号“+”，例如使用 ME(+) 来表示被更新的 ME（即，ME+）或传统 ME 中的二者 / 任一个。

[0082] 本发明利用以下属性：被更新的节点 / 移动终端可以向信令消息添加信息单元 (IE)，并且接收到该信令消息的传统节点 / 终端将简单地忽略这些 IE。作为示例，3GPP 网络协议是按照这种方式指定的。这意味着：

[0083] - 对于被更新的节点而言，向信令消息添加新 IE 是安全的，即便它不知道信令消息被发送至的节点是否被更新。

[0084] - 如果被更新的节点检测到信令消息中存在新 IE，则它知道（或者更确切地说，它可以可靠地推断）产生信令消息的节点也是被更新的。

[0085] 本发明的原理如下。

[0086] 在被更新的 ME（即，ME+）初始附着到网络时，被更新的 ME 将通知具有增强密钥管理功能的网络（没有被更新的 ME 自然不会进行这项操作）。存在若干个服务器选项，用于在初始附着时处理 ME 的增强密钥能力。一个选项是：当附着到网路的 ME(+) 向核心网通知其能力时，这可以经由正常注册过程来实现。对于关于核心网的现有的 ME 能力信令而言，所需要的只是被修改为包括与 ME 的增强密钥能力有关的信息（新 IE），以使得核心网获悉附着的 ME 是被更新的 ME。然后，核心网向 RNC 通知 ME 的增强密钥能力。

[0087] 另一个选项是，ME 向核心网单独地通知其关于核心网和无线电接入网的增强密钥能力。RAN(RNC) 于是可能需要负责独立于核心网地向 ME 通知其能力。一备选但较不灵活的方案是需要仅允许 RNC+ 连接到被更新的 VLR/MSC/SGSN，这是因为 VLR/MSC/SGSN 接着可

以代表 RNC 向 ME 通知其能力。

[0088] 应理解，在初始附着时使用的具体过程在本发明的范围之外。将在以下假设下对本发明进行描述：已经使用某一适当的过程（可以是上述过程之一或者可以是一些其他的过程）在 RNC(+) 与 ME(+) 之间初始（以及相互）建立能力。

[0089] 一旦 ME+ 已经附着到网络，则本发明的一项重要特征是保持 ME+ 始终知道当前（服务的）RNC 是否是被更新的 RNC 以及被更新的服务 RNC 始终知道 ME 是否是被更新的 ME 的属性。

[0090] 本发明在与传统节点互相作用方面的问题在于，在 ME 从传统 RNC 进行 SRNS 重定位之后，这可能导致簿记 (book-keeping) 中的漏洞，这是因为传统 RNC 可能无法向服务 ME 的下一个 RNC 通知传统 RNC 不支持和 / 或理解的 ME 的属性。为了示意，在 RNC 重定位序列中：从 RNC+ 到 RNC，然后到新 RNC+，即便第一个 RNC+ 向 RNC 传送了 ME 能力，也无法确保该 RNC 能够将这些能力传递到序列中的最后 RNC+。这需要解决，因为否则的话，只要有单个传统 RNC 参与到 RNC 改变链中，就必须在所有未来 RNC 改变中采取传统密钥处理（即便后续的服务 RNC 和 ME 都被更新）。本发明利用 ME+ 与 RNC+ 之间的通信和 / 或 RNC 之间的通信来保持该属性 (ME+ 始终知道当前（服务的）RNC 是否是被更新的 RNC 以及服务的被更新的 RNC（即，RNC+) 始终知道 ME 是否是被更新的 ME 的属性）。通过向 ME 通知它正在移至的 RNC 是否被更新、以及通过向目标 RNC 通知 ME 是否被更新来保持该属性。

[0091] 本发明的一个部分涉及 SRNS 重定位，这发生在活动模式（例如 TS23.060 中所定义的）下（或者在 UTRAN RRC 规范 25.331 中所定义的 RRC CONNECTED 状态下）。采用与初始附着类似的方式来处理如 TS 23.060(6.9.2.1 节）所描述的 IDLE（空闲）模式 RAU（路由区域更新）过程。当 UE 在 IDLE 模式下移动并且出现在新 RNC 下时，UE 建立新的 RRC 连接，并且这里也可以使用在初始附着时所采用的相应动作。

[0092] 注意，本发明不是特地解决至 / 自其它无线电接入技术（例如，TS43.129 的 PS 切换的所有方面）的 IRAT（异系统切换）。这意味着，从根据 GERAN(GSM EDGE 无线电接入网络）或 E-UTRAN 标准操作的网络切换的 ME 将不再使用增强的密钥管理能力，即便 ME 和 RAN 二者都被更新。这是必需的，因为我们无法信任源网络能够检测到 ME 具有特定的增强 UTRAN 能力，并且因此我们无法假设 GSM/LTE 网络能够将该信息传送给 3G/UMTS 网络。从被更新的 ME（即，ME+) 的角度，这不成问题，因为被更新的 ME（即，ME+) 知道在任意 IRAT 切换之后网络应当将其（至少初始地）视为传统 ME。

[0093] 为了简单起见，说明书不就讨论 PS 还是 CS 密钥（其使用取决于所使用的服务类型）进行区分，这是因为相同的原理应用于每一种类型的密钥。此外，还应当注意控制面密钥可以不同于用户面密钥。具体地，控制面密钥始终基于最新的安全激活的域 (CS/PS)，该域可以不同于当前数据面服务在其中运行的域。在这种情况下，可以将本发明应用于两组密钥。

[0094] 将针对参照图 2(a) 到 2(c) 描述的所有三种 SRNS 重定位的情况来描述本发明如何修改密钥，以及如何在各个实体（即，ME 和 RNC) 中保持与相应实体是否被更新有关的知识：没有 ME 参与的 SRNS 重定位（图 2(a)，参见 TS 23.060 的 6.9.2.2.1）；组合的硬切换与 SRNS 重定位（图 2(b)，参见 TS 23.060 的 6.9.2.2.2）；和组合的小区 /URA 更新和 SRNS 重定位（图 2(c)，参见 TS 23.060 的 6.9.2.2.3)。由于在初始附着到系统之后，被更新的

ME(即,ME+)知道它是否连接到被更新的RNC(即,RNC+)与否(反之亦然),只需要针对每一种SRNS重定位变型考虑两种子情况:

[0095] 1. 系统在该过程开始之前的初始状态是ME+连接到RNC+。

[0096] 2. 系统在该过程开始之前的初始状态是ME+连接到RNC。

[0097] 不需要考虑ME没有被更新的情况。这是因为,本发明使得所有被更新的RNC都具有关于ME是否被更新的知识,并且只能是被更新的RNC对密钥执行任意增强的改变(或调整),本发明的方法在ME没有被更新的情况下不执行任何密钥调整。然而,在传统ME的情况下,仍然需要关于哪些实体被更新以及哪些不被更新的指示,以使得被更新的RNC确实能够知道它对应的是传统的ME。注意,只有被更新的实体传送显式信息来指示其状态。传统实体不发送与正在被更新的有关的任何信息,所以在传统实体的情况下,通过在相应节点处没有接收到信息来产生该实体没有被更新的指示。

[0098] 在下表中列出这些情况,以便查看。

[0099]

	源RNC被更新	源RNC没有被更新
没有ME参与的SRNS重定位	图3	使用传统过程,即不进行密钥调整
组合的硬切换与SRNS重定位	图5	使用传统过程,即不进行密钥调整
组合的小区/URA更新和SRNS重定位	图7	使用传统过程,即不进行密钥调整

[0100] 首先将描述本发明对于没有ME参与的SRNS重定位的应用。

[0101] 图3示出了在没有ME参与的SRNS重定位时发生的信令。图3取自TS 23.060的6.9.2.2.1条款,并示出了没有ME参与的SRNS重定位的PS版本。本发明只使用信令中的下列属性:

[0102] -存在从源RNC(+)到目标RNC(+)的信令路径(这是所谓的源RNC到目标RNC透明容器)

[0103] -存在从ME(+)所响应的目标RNC(+)发起的过程(针对PS,这是RAN移动信息消息交换)。

[0104] 针对CS情况,使用相应的特征。

[0105] 在图3所示的信令中,在1处作出关于执行SRNS重定位的决定,在2处源RNC发

信号通知当前（旧）SGSN（服务 GPRS 支持节点）需要 SRNS 重定位，并且在 3 处当前 SGSN 通知目标（新的）SGSN 需要 SRNS 重定位。

[0106] 在 4 处目标 SGSN 通知目标 RNC 需要 SRNS 重定位，并且在目标 SGSN 与目标 RNC 之间建立无线电承载。在 4’处目标 RNC 向目标 SGSN 返回肯定确认。在 5 处目标 SGSN 通知当前 SGSN 针对 SRNS 重定位的请求正在被处理。

[0107] 在 6 处当前 SGSN 向源 RNC 发送重定位命令，以向源 RNC 通知目标 RNC 的标识，并且在 7 和 8 处源 RNC 向源 RNC 发送数据和重定位提交信号。目标 RNC 通过在 9 处发送重定位检测消息来向新的 SGSN 通知该重定位。在 10 处目标 RNC 向移动站发送 RAN 移动信息，并且移动站在 10’处通过发送 RAN 移动信息确认消息来进行肯定应答。在 11 处，目标 RNC 通知目标 SGSN 重定位完成，在 12 处目标 SGSN 通知旧 SGSN 重定位完成，并在 12’处旧 SGSN 向目标 SGSN 肯定应答它已经接收到重定位完成消息。

[0108] 目标 SGSN 在 13 处向 GGSN（网关 GPRS 支持节点）发送更新 PDP 上下文请求，并且 GGSN 在 13’处发送响应。此外，旧 SGSN 在 14 处向源 RNC 发送 Iu 释放命令，并且在 Iu 释放完成时，源 RNC 在 14’处发信号通知旧 SGSN。然后在 15 处执行路由区域更新。

[0109] 如上所述，对于每一种重定位机制有两种情况要考虑：(A) 源 RNC 被更新的情况和 (B) 源 RNC 没有被更新的情况。将先描述情况 A。

[0110] 密钥调整 - 在源 RNC 被更新的情况 A 中，主要问题源于 ME+ 在接收到 RAN 移动信息 10 消息之前没有意识到 RNC 的改变。这意味着，在 ME+ 知道它应当改变其 CK 和 IK 之前，ME+ 必须接收、验证 RAN 移动信息消息 10 的完整性保护，并对消息 10 进行解密。不幸的是，当 ME+ 接收到消息 10 时，从 ME+ 的角度来看，ME+ 仅仅接收到了一个信令消息，而并不知道这是正在进行的重定位过程的一部分（因为 ME+ 尚未参与到重定位中）。因此，ME+ 无法知道它接收到的消息是否是源 RNC 发送的（并且在由旧的、未调整的 CK/IK 保护的情况下）或者它是否是目标 RNC+ 所发送的 RAN 移动信息消息（并且因此由调整后的 CK/IK 保护）。

[0111] 本发明克服这一点的一种方式是，ME+ 初始使用当前 CK/IK，然后如果利用当前 CK/IK 对接收到的消息进行的完整性保护失败，则尝试调整后的 CK/IK。然而，这不是非常正规的，也不算最优的安全设计。取而代之地，一优选实施例是，源 RNC+ 在这种情况下执行回到其自身的本地 SRNS 重定位（“RNC 内 SRNS 重定位”），然后立即进行针对目标 RNC 的真实 SRNS 重定位（回到其自身的本地 SRNS 重定位可以在上图中的步骤 8 之前执行）。当进行第二次 SRNS 重定位时，这是到目标 RNC 的重定位，源 RNC+ 向目标 RNC 提供在第一次 RNC 内 SRNS 重定位时推导出的经调整的密钥 CK/IK。这么做的结果是，在牵涉到目标 RNC 的情况下，只可能连累到在 ME+ 与源 RNC 之间在时间上在两个 SRNS 重定位之间发送的业务。此外，不需要改变现有的过程。

[0112] 保持关于哪些实体被更新的知识 - 由于源 RNC+ 被更新，因此它知道 ME+ 是否被更新，并且在这种情况下源 RNC+ 向目标 RNC+ 发送关于 ME+ 是否被更新的指示。在优选实施例中，该指示是通过源 SRNC 到目标 RNC 透明容器从源 RNC 发送到目标 RNC 的 MS 能力中的新的信息单元 (IE)，该容器包括在重定位所需消息（图 3 中的消息 2) 中，然后被转发给目标 RNC（例如，经由消息 3 和 4)。这意味着，在没有 ME 参与的 SRNS 重定位之后，目标 RNC(+) 知道 ME+ 是否被更新（如果目标 RNC 自身被更新）。

[0113] 当目标 RNC(+) 向 ME+ 发送 RAN 移动信息消息 10 时，根据本发明，当且仅当目标

RNC(+) 是被更新的 RNC 时，它在消息 10 中包括目标 RNC(+) 是被更新的 RNC 的显式信息。如果 ME+ 在消息 10 中接收到这样的显式信息，则它知道目标 RNC 被更新。如果 RAN 移动信息消息 10 中没有这种显式信息，则 ME+ 可以断定目标 RNC(+) 没有被更新。备选地，可以通过“较晚的”消息来发送目标 RNC(+) 是否被更新的信息，但是这可能导致与下面要描述的组合的小区 /URA 重定位中的序列的竞争条件。例如，如果目标 RNC（为了清楚起见，这在本示例中称为 RNC1）没有在消息 10 中向移动终端通知它是否被更新，则可能出现竞争条件，并且在 RNC1 已经通知了移动终端它是否被更新之前存在到另一个 RNC（这将称为 RNC2）的另外重定位。如果发生这种情况，则移动终端可能不知道在从 RNC1 到 RNC2 的另外重定位时是否调整密钥，这是因为移动终端不知道 RNC1 是否是被更新的 RNC。将“ME+ 能力指示”包括在小区 /URA 更新确认消息中也是有益的，这是因为移动终端可以从没有保持 ME 被更新的知识的“旧 RNC”到达具有被更新的 RNC 的小区。

[0114] 由于当前的 UTRAN 标准不能确保传统 RNC 应当转发 ME 能力信息的未知部分，所以不能假设传统 RNC 将转发关于 ME 是否被更新的信息。然而，对于这个问题的解决方案是，ME+ 可以在 RAN 移动信息确认消息（参见图 3 的消息流中的消息 11）中包括关于它被更新的指示。如果目标 RNC(+) 发现消息 11 中没有该指示，则可以断定 ME 没有被更新。

[0115] 现在将描述本发明在针对源 RNC 没有被更新的情况 B 的没有 ME 参与的 SRNS 重定位的应用。

[0116] 密钥调整 - 传统源 RNC 完全不知道增强密钥改变，并且仅仅根据其现有行为进行操作。由于 ME+ 知道它是连接到传统 RNC 或被更新的 RNC，因此在 ME+ 当前连接到传统 RNC 的情况下，ME+ 在被通知已经发生了没有 ME 参与的 SRNS 重定位时不执行任何密钥调整。

[0117] 保持被更新实体的知识 - 传统源 RNC 完全不知道增强密钥改变，并且仅仅根据现有行为进行操作。

[0118] 当目标 RNC(+) 在消息 10 向 ME+ 发送 RAN 移动信息消息时，根据本发明，当且仅当目标 RNC(+) 是被更新的 RNC 时，该消息包括它被更新的信息。这确保 ME+ 知道目标 RNC(+) 是否被更新（如果目标 RNC(+) 没有提供它被更新的信息），ME+ 将把这个当作目标 RNC(+) 是传统 RNC 的指示。在来自 ME+ 的响应消息 (RAN 移动信息完成消息 10’）中，ME+ 包括它是否被更新的指示（传统 ME 不会这么做）。这确保目标 RNC（如果它是被更新的 RNC) 知道 ME(+) 是否被更新。

[0119] 图 4 是示出了在没有 ME 参与的 SRNS 重定位时如何在 RNC(+) 和 ME+ 中保持知识的状态图。

[0120] 图 4 的左边示出了 ME+ 正在由被更新的 RNC（即，RNC+) 提供服务的状态。ME+ 知道 RNC 被更新，并且 RNC+ 知道 ME 被更新。如果对于被更新的目标 RNC 发生没有 ME 参与的 SRNS 重定位，则在 1 处由 RNC+ 和 ME+ 二者调整密钥。

[0121] 如果对于没有被更新的目标 RNC 发生没有 ME 参与的 SRNS 重定位，则在重定位时不调整密钥。然而，如上所述，源 RNC 可以执行内 SRNS 重定位，这使得在重定位到新 RNC 之前，在 2 处由源 RNC+ 和 ME+ 二者调整密钥。

[0122] 图 4 的右边示出了 ME+ 正在由没有被更新的 RNC 提供服务的状态。ME 知道源 RNC 没有被更新，但是 RNC 不知道 ME 被更新。如果发生没有 ME 参与的 SRNS 重定位，则由于源 RNC 没有被更新，如在 3 和 4 处所示的，它无法调整这些密钥，并且 ME+ 也不调整密钥（即便

ME+ 能够调整密钥）。

[0123] 如 5 处所示，关于目标 RNC 是否被更新的信息优选地包括在从目标 RNC 到 ME+ 的 RAN 移动信息消息（消息 10）中，并且关于 ME 是否被更新的信息优选地包括在到目标 RNC 的移动信息完成消息（消息 10'）中（或者包括在源 RNC 到目标 RNC 透明容器中）。

[0124] 如果在这个过程期间 SGSN 或 MSC/VLR 有改变，则在没有 ME 参与的 SRNS 重定位之后的路由 / 位置区域更新过程中处理关于 ME(+) 和 / 或 SGSN/MSC/VLR 是否被更新的信息。在核心网侧，备选方案是：在传送 MS 能力时，源 SGSN/MSC/VLR 向目标 SGSN/MSC/VLR 通知 ME(+) 的增强的密钥处理能力。如果 SGSN/MSC/VLR 将它不理解的 MS 能力中的新信息单元丢弃，则该备选方案无法运作。

[0125] 接下来，将描述本发明在组合的硬切换和 SRNS 重定位中的应用。

[0126] 图 5 示出了在组合的硬切换和 SRNS 重定位时发生的信令。图 5 来自 TS 23.060 的 6.9.2.2.2 条款，并且示出了组合的硬切换和 SRNS 重定位的 PS 版本。本发明只使用信令中的下列属性：

[0127] - 存在从源 RNC(+) 到目标 RNC(+) 的信令路径（这是源 RNC 到目标 RNC 透明容器）

[0128] - 存在从目标 RNC(+) 到源 RNC(+) 的信令路径（这是目标 RNC 到源 RNC 透明容器）

[0129] - 目标 RNC 到源 RNC 透明容器包含在容器中接收到时要由目标 RNC(+) 传递给 ME(+) 的消息（这是容器中包含的 RRC 消息）。

[0130] 针对 CS 情况，使用相应的特征。

[0131] 在图 5 所示的信令中，消息 1 至 7 对应于图 3 中的消息 1 至 7，不再进行描述。

[0132] 在 8 处源 RNC 向移动终端发送 RRC（无线电资源控制）消息。在 9 处，源 RNC 将 SRNS 上下文转发给旧 SGSN，并在 9a 处，旧 SGSN 将 SRNS 上下文转发给新 SGSN。然后，新 SGSN 在 9b 处向旧 SGSN 发送肯定应答，并在 9c 处将 SRNS 上下文转发给目标 RNC。在目标 RNC 已经检测到移动终端之后，目标 RNC 通过在 10 处发送重定位检测消息来向新 SGSN 通知该重定位，并且移动终端在 8' 处向目标 RNC 发送 RRC 消息。

[0133] 图 5 中的消息 11 至 15 对应于图 3 中的消息 11 至 15，不再进行描述。

[0134] 如上所述，对于每一种重定位机制有两种情况要考虑：(A) 源 RNC 被更新的情况和 (B) 源 RNC 没有被更新的情况。将先描述情况 A。

[0135] 情况 A（源 RNC 被更新）- 密钥调整 - 在这种情况下，密钥调整可以与实际的重定位信令结合，并且在重定位之前，源 RNC(+) 不需要执行单独的内 SRNS 重定位以调整 CK/IK（如针对没有 ME 参与的 SRNS 重定位的情况一样）。由于这里所描述的重定位比没有 ME 参与的 SRNS 重定位更为时间关键，因此该组合提供了更大的益处。

[0136] 由于源 RNC+ 知道 ME+ 被更新，因此它将在源 RNC 到目标 RNC 的透明容器中将 CK/IK 发送至目标 RNC(+) 之前调整 CK/IK。该容器包括在重定位所需消息（上述流程图中的消息 2）中。目标 RNC(+) 按照与传统系统相同的方式来使用密钥，并且因此不知道（并且不需要知道）它们是否已经被调整。

[0137] 如果 ME 被更新，则它知道正在向其提供服务的源 RNC(+) 是否被更新，并且根据本发明，当（并且仅当）源 RNC(+) 是被更新的 RNC 时，ME 调整 CK/IK。ME+ 和目标 RNC+ 开始使用来自 ME+ 的经调整的密钥，并且包括从 ME+ 到目标 RNC+ 的 RRC 消息（图 5 中的上行链路消息 8）。

[0138] 保持被更新实体的知识 - 根据本发明，源 RNC+ 通过源 RNC 到目标 RNC 透明容器向目标 RNC(+) 发送关于 ME 是否被更新的指示（备选地，该指示可以包括在 MS 能力 IE 中）。按照这种方式，目标 RNC+ 将知道 ME(+) 是否被更新。

[0139] 根据本发明，目标 RNC+ 将它被更新的信息包括在目标 RNC 到源 RNC 透明容器所包括的 RRC 消息的新 IE 中。然后，由源 RNC(+) 在图 5 的下行链路消息 8 中将该 RRC 消息转发至 ME。目标 RNC 可能不包括它是否是传统 RNC 的这种信息。这样，根据是否接收到该信息，通知 ME(+) 目标 RNC(+) 是否被更新。

[0140] 情况 B（源 RNC 没有被更新）- 调整密钥 - 由于源 RNC 没有被更新，因此 ME+ 或是源 RNC 都不执行密钥调整。

[0141] 情况 B（源 RNC 没有被更新）- 保持被更新实体的知识 -ME(+) 按照与源 RNC(+) 被更新的情况完全相同的方式获悉目标 RNC(+) 是否被更新。

[0142] 在源 RNC 是传统 RNC 的情况下，它将不向目标 RNC(+) 提供关于 ME(+) 是否被更新的任何信息。这意味着，目标 RNC(+) 将不知道 ME+ 是否被更新。然而，根据本发明，被更新的 ME+ 可以将它被更新的信息包括在上述流程图中的上行链路 RRC 消息编号 8’ 中。这意味着被更新的 RNC+ 在未来的 SRNS 重定位中仍然能够使用密钥调整。

[0143] 图 6 是示出了在组合的硬切换和 SRNS 重定位时如何在 RNC(+) 和 ME+ 中保持知识的状态图。

[0144] 图 6 的左边示出了 ME+ 正在由被更新的 RNC（即，RNC+）提供服务的状态。ME+ 知道 RNC 被更新，并且 RNC 知道 ME 被更新。如果对于被更新的目标 RNC 发生组合的硬切换和 SRNS 重定位，则密钥在 1 处由源 RNC+ 和 ME+ 二者调整。

[0145] 如果对于没有被更新的目标 RNC 发生组合的硬切换和 SRNS 重定位，则密钥在 2 处还由源 RNC+ 和 ME+ 二者调整。

[0146] 图 6 的右边示出了 ME+ 正在由没有被更新的 RNC 提供服务的状态。ME+ 知道 RNC 没有被更新，但是 RNC 不知道 ME 被更新。如果发生组合的硬切换和 SRNS 重定位，则如 3 和 4 处所示，源 RNC 由于其没有被更新而无法调整密钥，并且因此 ME+ 也不调整密钥（即便 ME+ 能够调整密钥）。

[0147] 如 5 处所示，关于目标 RNC 是否被更新的信息优选地包括在到 ME+ 的 RRC 消息中（图 5 中的消息 8），并且关于 ME 是否被更新的信息优选地包括在到目标 RNC 的 RRC 消息（消息 8’）中（原则上，它也可以包括在源 RNC 到目标 RNC 透明容器中）。

[0148] 接下来，将描述本发明对于组合的小区 /URA 更新和 SRNS 重定位的应用。

[0149] 图 7 示出了在组合的小区 /URA 更新和 SRNS 重定位时发生的信令。图 7 来自 TS 23.060 的 6.9.2.2.3 条款，并且示出了组合的小区 /URA 更新和 SRNS 重定位的 PS 版本。本发明只使用信令中的下列属性：

[0150] - 存在从源 RNC(+) 到目标 RNC(+) 的信令路径（这是源 RNC 到目标 RNC 的透明容器）

[0151] - 存在从目标 RNC(+) 到源 RNC(+) 的信令路径（这是目标 RNC 到源 RNC 的透明容器）

[0152] - 目标 RNC 到源 RNC 的透明容器包含在容器中接收到时要由目标 RNC(+) 传递给 ME(+) 的消息（这是容器中包含的 RRC 消息）。

[0153] 针对 CS 情况，使用相应的特征。

[0154] 在图 7 所示的信令中，移动终端初始在 1 处向源 RNC 发送小区更新 /URA 更新消息或小区更新 /GRA 更新消息。

[0155] 在图 7 所示的信令中，消息 2 至 9 对应于图 3 中的消息 2 至 9，不再进行描述。

[0156] 在 10 处目标 RNC 向移动终端发送小区更新确认 /URA 更新确认消息或小区更新确认 /GRA 更新确认消息。在 10’处移动终端向目标 RNC 发送 UTRAN 移动信息消息。

[0157] 在图 7 所示的信令中，消息 11 至 15 对应于图 3 中的消息 11 至 15，不再进行描述。

[0158] 如上所述，对于每一种重定位机制有两种情况要考虑 :(A) 源 RNC 被更新的情况和 (B) 源 RNC 没有被更新的情况。将先描述情况 A，然后描述情况 B。

[0159] 情况 A(源 RNC 被更新)- 密钥调整 - 这种情况与参照图 3 所描述的没有 ME 参与的 SRNS 重定位的情况非常相似，直到重定位检测消息 (消息 9)(除了在不存在没有 ME 参与的 SRNS 重定位的情况下优选地在消息 8 之前执行的 RNC 内 SRNS 重定位以外)。然而，图 7 的消息 10 与图 3 相比有显著不同 :使用经调整的密钥的第一消息源自网络侧 (如果遵循相同的策略)。此时，ME(+) 必须仍然准备接受来自源 RNC(+) 的信令，例如作为其他同时运行过程的一部分。

[0160] 该过程中的第一消息 (小区更新 /URA 更新消息 (消息 1)) 不加密，因为它通过公共控制信道 (CCCH) 发送。ME(+) 将该消息发送至目标 RNC(+)，目标 RNC(+) 在上行链路信令传送指示消息 (图 7 中未示出) 中将其路由至源 RNC(+)。

[0161] 根据本发明，源 RNC(+) 知道 ME(+) 是否被更新，并且当前仅当 ME(+) 被更新时，它在通过源 RNC 到目标 RNC 透明容器将 CK/IK 发送至目标 RNC(+) 之前调整 CK/IK。该容器包括在重定位所需消息 (图 7 中的消息 2) 中。目标 RNC(+) 按照与传统系统相同的方式使用密钥，并且因此不知道 (并且不需要知道) 它们是否已经被调整过。

[0162] ME+ 知道它所连接到的源 RNC(+) 是否是被更新的 RNC，并且根据本发明，当 (且仅当) 源 RNC(+) 被更新时，调整 CK/IK，并且该调整在发送小区更新 /URA 更新消息 (消息 1) 之后进行。由于小区更新 /URA 更新消息没有被加密，并且被更新的源 RNC(+) 知道被更新的 ME+ 在发送小区更新 /URA 更新消息之后始终会调整密钥，所以源 RNC(+) 也在验证了消息的完整性之后调整密钥。从此时起，ME+ 开始接受具有经调整的密钥的下行链路业务。ME(+) 期望接收的来自网络的下一个下行链路消息是来自目标 RNC(+) 的小区更新确认 /URA 更新确认消息 (图 7 中的消息 10)。

[0163] 情况 A(源 RNC 被更新)- 保持被更新实体的知识 - 根据本发明，源 RNC+ 在源 RNC 到目标 RNC 透明容器 (备选地，可以包括在 MS 能力 IE 中) 中向目标 RNC(+) 发送关于 ME 是否被更新的指示。按照这种方式，如果它是更新的 RNC，则目标 RNC(+) 知道 ME(+) 是否被更新。

[0164] 如果目标 RNC(+) 没有在 SIB(系统信息块) 中广播其增强的密钥处理能力，则它能够在小区更新确认 /URA 更新确认消息中包括针对 ME(+) 的指示。传统的目标 RNC 不包括这种指示。按照这种方式，如果 ME(+) 是 ME+，则它能够知道目标 RNC(+) 是否被更新。

[0165] 情况 B(源 RNC 没有被更新)- 调整密钥 - 由于源 RNC 没有被更新，因此在这种情况下 ME(+) 和源 RNC 均不执行密钥调整。

[0166] 情况 B(源 RNC 没有被更新)- 保持被更新实体的知识 -ME(+) 按照与源 RNC(+) 被

更新的情况完全相同的方式获悉目标 RNC(+) 被更新。

[0167] 在源 RNC 是传统 RNC 的情况下，它将不向目标 RNC(+) 提供关于 ME(+) 是否被更新的任何信息。这意味着，目标 RNC(+) 将不知道 ME+ 是否被更新。然而，被更新的 ME+ 可以将它被更新的指示包括在上行链路消息 (UTRAN 移动信息确认 - 图 7 中的消息 10') 中。这意味着，如果目标 RNC 是 RNC+，则目标 RNC+ 能够使用密钥调整来进行下一个 SRNS 重定位，这是因为它意识到 ME 是被更新的 ME 并且也能够调整密钥。

[0168] 图 8 是示出了在组合的小区 /URA 更新和 SRNS 重定位时如何在 RNC(+) 和 ME+ 中保持知识的状态图。

[0169] 图 8 的左边示出了 ME+ 正在由被更新的 RNC 提供服务的状态。ME+ 知道 RNC 被更新，并且 RNC 知道 ME 被更新。如果针对被更新的目标 RNC 发生组合的小区 /URA 更新和 SRNS 重定位，则在 1 处由源 RNC+ 和 ME+ 二者调整密钥。

[0170] 如果针对没有被更新的 RNC 发生组合的小区 /URA 更新和 SRNS 重定位，则密钥也由源 RNC+ 和 ME+ 二者在 2 处调整。

[0171] 图 8 的右边示出了 ME+ 正在由没有被更新的 RNC 提供服务的状态。ME 知道源 RNC 没有被更新，但是 RNC 不知道 ME 被更新。如果组合的小区 /URA 更新和 SRNS 重定位发生，则由于源 RNC 没有被更新，如在 3 和 4 处所示的，它无法调整密钥，并且 ME+ 也不调整密钥 (即便 ME+ 能够调整密钥)。

[0172] 如 5 处所示，关于目标 RNC 是否被更新的信息优选地包括在从目标 RNC 到 ME+ 小区更新确认 /URA 更新确认 (或小区更新确认 /URA 确认) 消息 (图 7 中的消息 10) 中或者包括在 SIB 消息中，并且关于 ME 是否被更新的信息优选地包括在 UTRAN 移动信息确认消息中，并且在该消息中从源 RNC 发送至目标 RNC(+)(图 7 中的消息 10') 或者包括在源 RNC 到目标 RNC 透明容器中。

[0173] 图 9 是示出了本发明的方法的主要步骤的流程框图。

[0174] 如步骤 93 所示，节点 (例如，通过由至少一个第一密钥保护的连接服务于移动终端的源 RNC) 保持所述第一密钥和与该移动终端的密钥管理能力 (KMC) 有关的信息。如果移动终端经历到新 RNC 的 SRNC 重定位，则在步骤 95，当且仅当所存储的密钥管理能力指示该移动终端支持增强的密钥管理能力时，该节点修改第一密钥，以创建第二密钥。然后，节点在步骤 96 将第二密钥发送至新 RNC(即，目标 RNC)。(如果所存储的密钥管理能力指示移动终端不支持增强的密钥管理能力，即，移动终端是传统移动终端，则节点将不执行步骤 95，并且节点将在步骤 96 发送未修改的第一密钥)。

[0175] 在步骤 97，将与移动终端的密钥管理能力有关的信息发送至目标 RNC。该信息可以由节点 (即，由源 RNC) 或者由移动终端发送。

[0176] 如上所述，如果 SRNS 重定位是没有 ME 参与的 SRNS 重定位，则源 RNC 可以指示移动终端在修改第一密钥之前执行节点内重定位，这在图 9 的步骤 94 示出。

[0177] 图 9 的步骤 91 和 92 示意了在节点通过来自第三节点 (充当重定位的源节点) 的 SRNS 重定位而变成服务于移动终端的 RNC 时可能发生的步骤。在步骤 91 处，节点可以向移动终端发送与节点的密钥管理能力有关的信息 - 以使得移动终端能够意识到它正在被重定位至被更新的 RNC(因为传统 RNC 不发送该信息)。在步骤 92，节点可以接收与移动终端的密钥管理能力有关的信息 - 该信息可以由移动终端或由第三节点发送。

[0178] 如先前所说明的，如果执行步骤 91 和 92，则步骤 96 和 97 可以利用与 SRNS 重定位有关的信令消息，以避免对于附加消息的需要。

[0179] 图 10 是示意了在移动终端处执行的本发明的方法的主要步骤的流程框图。

[0180] 由源 RNC 通过由至少一个第一密钥保护的连接所服务的移动终端保持第一密钥。在步骤 101，移动终端保持第一密钥和与源 RNC 的密钥管理能力有关的信息。如果移动终端经历到新 RNC 的 SRNS 重定位，在步骤 103，当且仅当所存储的密钥管理能力指示源 RNC 支持增强的密钥管理能力时，移动终端修改第一密钥，以创建第二密钥。（如果所存储的密钥管理能力指示移动终端不支持增强的密钥管理能力，即，移动终端是传统移动终端，则移动终端将不执行步骤 103）。

[0181] 如上所述，如果 SRNS 重定位是没有 ME 参与的 SRNS 重定位，则源 RNC 可以指示移动终端在修改第一密钥之前执行节点内重定位。节点内重定位的执行在图 10 的步骤 103 示出。

[0182] 在步骤 104，移动终端可以向作为 SRNS 重定位中的目标 RNC 的 RNC 发送与移动终端的密钥管理能力有关的信息。在重定位之后，移动终端在步骤 105 接收与作为 SRNS 重定位中的目标 RNC 的 RNC 的密钥管理能力有关的信息（假设，目标 RNC 是被更新的 RNC- 如果目标 RNC 是传统 RNC，则移动终端将不会接收到与 RNC 的密钥管理能力有关的信息，并且将根据没有接收到该信息而获悉它正在由传统 RNC 服务）。

[0183] 图 11 是示出了根据本发明实施例的节点 1101 的主要组件的框图。该节点具有输入节点 1105 和输出接口 1103、处理器 1104 和存储器 1102。这些组件是或者可以是传统组件，并且将不再进一步描述。

[0184] 节点 1101 具有用于保持与由所述节点通过由至少一个第一密钥保护的连接所服务的移动终端的密钥管理能力有关的信息以及第一密钥的模块 1102a。模块 1102a 可以是图 11 所述的节点中的存储器 1102 的一部分，或者模块 1102a 可以独立于节点的存储器 1102。

[0185] 节点 1101 还具有用于在将所述移动终端重定位到第二节点时，当且仅当存储在模块 1102a 中的移动终端的密钥管理能力指示移动终端所支持增强的密钥管理能力时，修改第一密钥以创建第二密钥的模块 1104a。模块 1104a 可以是在图 11 所示的处理器 1104 上运行的软件模块，或者备选地模块 1104a 可以是独立于处理器 1104 的硬件模块（包括软件）。

[0186] 节点 1101 还具有用于将第二密钥发送至第二节点的模块 1103a。模块 1103a 可以是如图 11 所述的节点中的输出接口 1103 的一部分，或者模块 1103a 可以独立于节点中的输出接口 1103。

[0187] 节点可选地还包括用于将移动终端的密钥管理能力发送至第二节点的模块。

[0188] 图 12 是示出了根据本发明实施例的移动终端 1201 的主要组件的框图。该移动终端具有无线接口 1204、处理器 1024 和存储器 1202。为了清楚起见，省略诸如显示器和数据输入设备（例如键盘）之类的其他组件（或者既充当显示器又充当数据输入设备的触摸屏之类的组件）。

[0189] 移动终端 1201 还具有用于保持与通过由至少一个第一密钥保护的连接服务移动终端的第一节点的密钥管理能力有关的信息以及第一密钥的模块 1202a。模块 1202a 可

以是图 12 所述的移动终端中的存储器 1202 的一部分，或者模块 1202a 可以独立于存储器 1202。

[0190] 移动终端 1201 还具有模块 1204a，用于在将移动终端从第一节点重定位到第二节点时，当且仅当存储在模块 1202a 中的密钥管理能力指示第一节点支持增强的密钥管理能力时，修改第一密钥以创建第二密钥。模块 1204a 可以是在图 12 所示的处理器 1204 上运行的软件模块，或者备选地模块 1204a 可以是独立于处理器 1204 的硬件模块（包括软件）。

[0191] 移动终端 1201 可选地还具有模块 1203a，用于将其密钥管理能力发送至第二节点。模块 1203a 可以是如图 12 所述的节点中的无线接口 1203 的一部分，或者模块 1203a 可以独立于移动终端 1201 中的无线接口 1203。

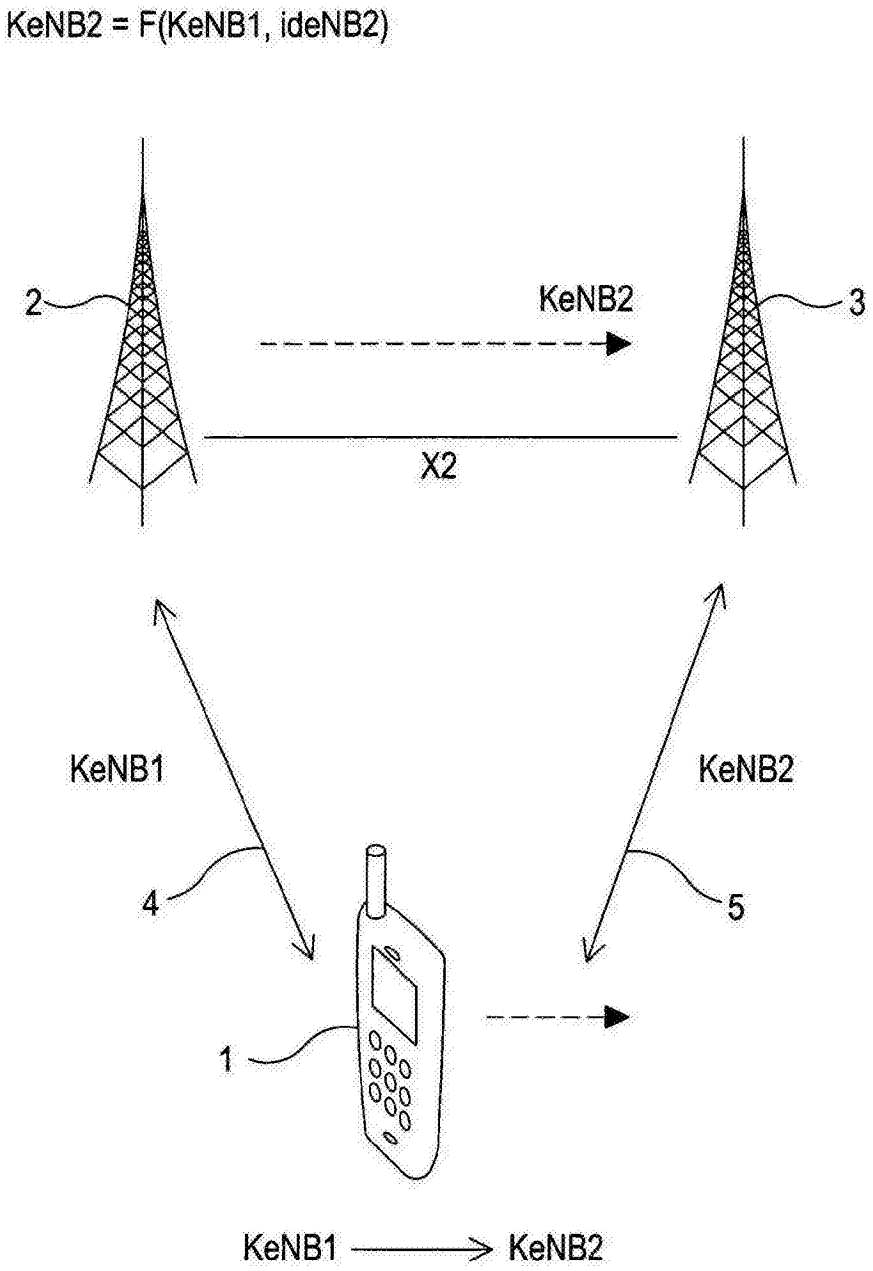


图 1

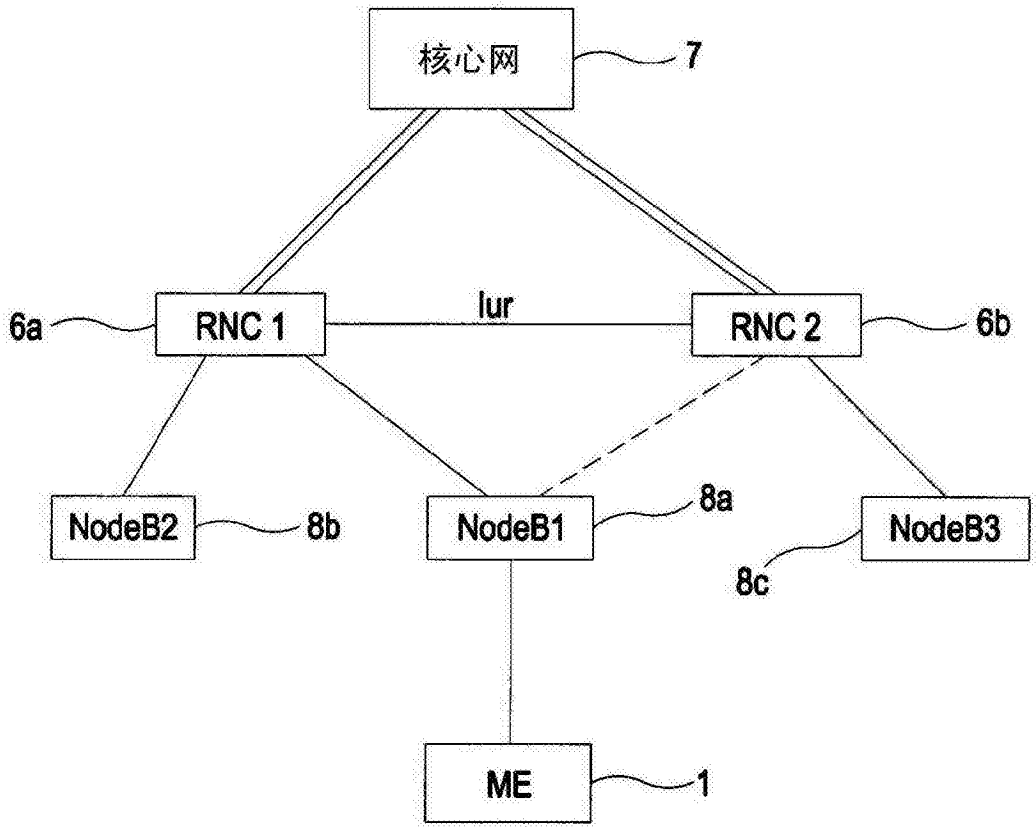


图 2(a)

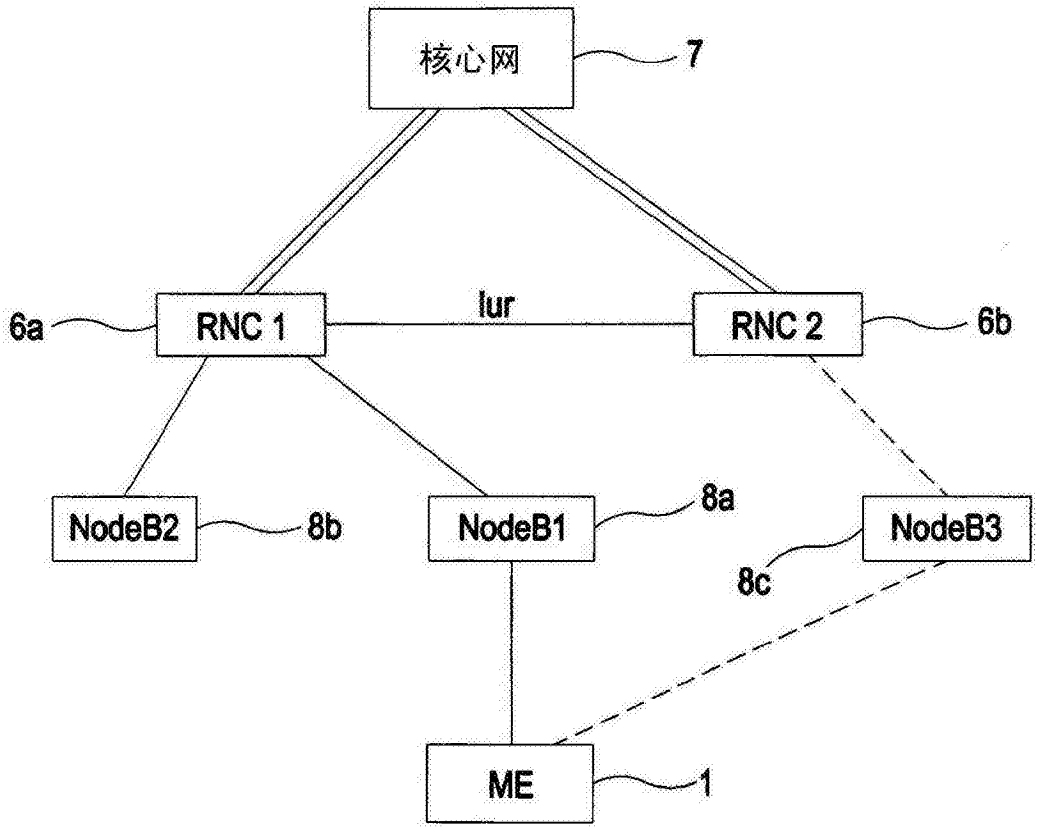


图 2(b)

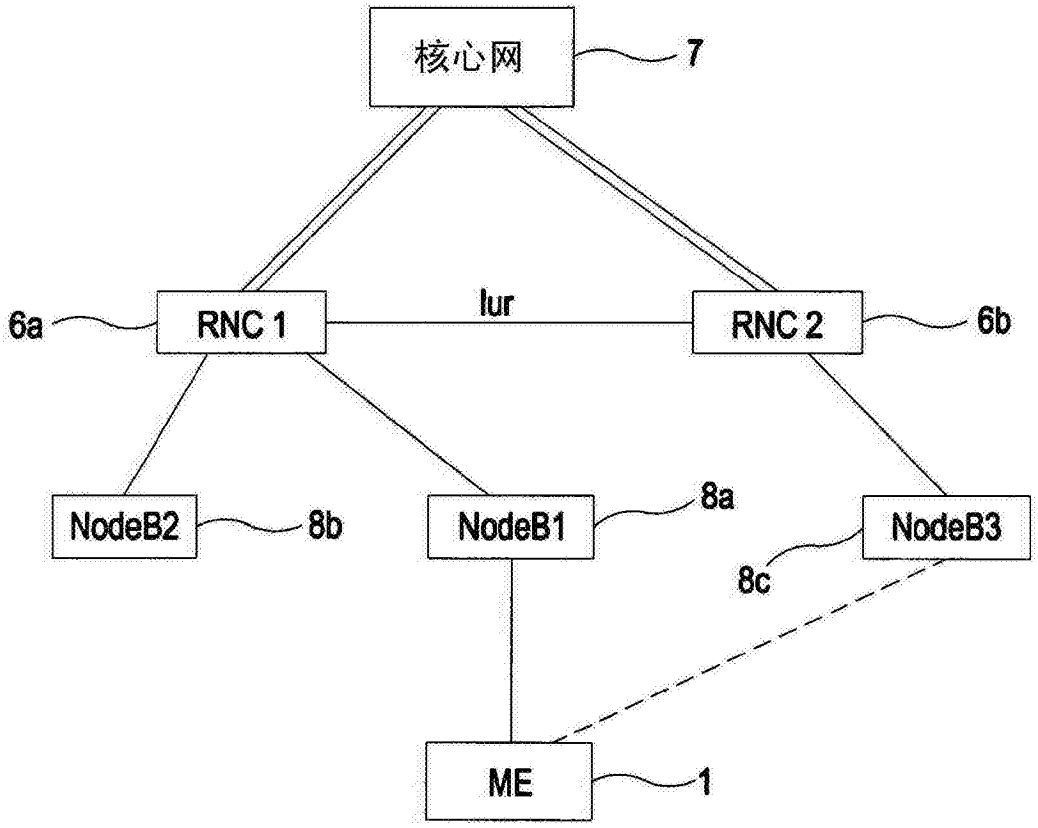
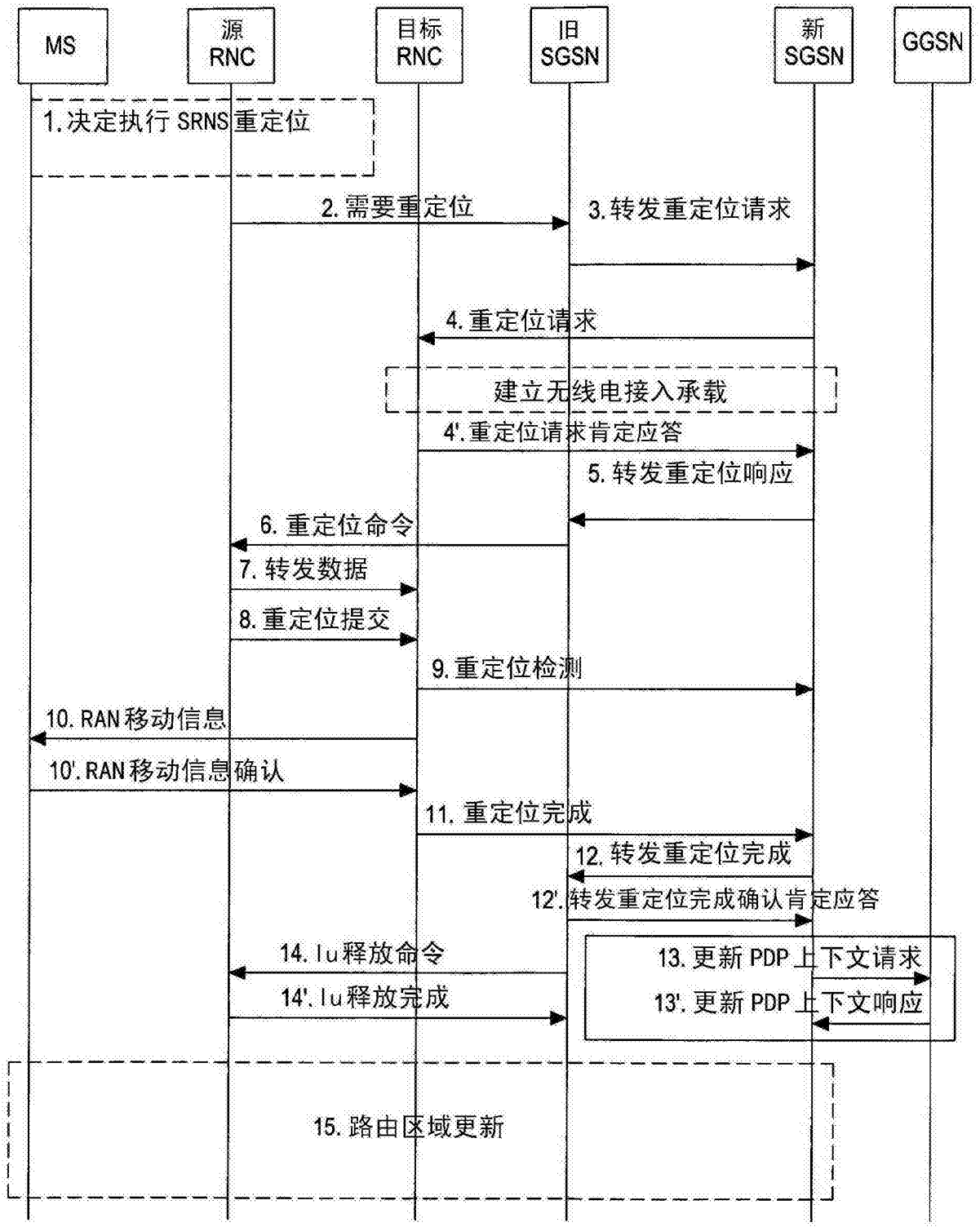


图 2(c)



情况 A（源 RNC 没有被更新）

图 3

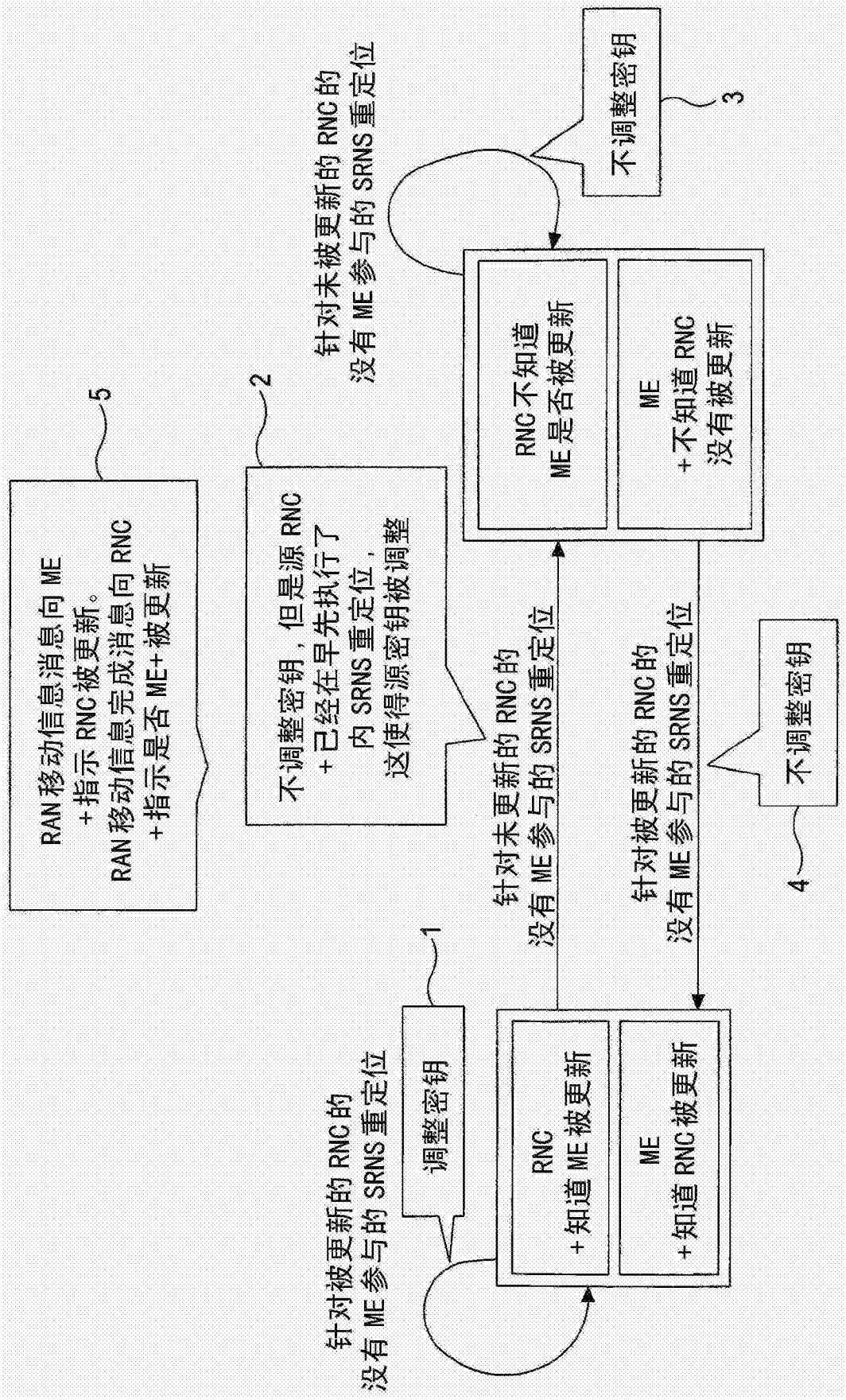

RAN 移动信息消息向 ME
+指示 RNC 被更新。
RAN 移动信息完成消息向 RNC
+指示是否 ME+被更新
5
不调整密钥，但是源 RNC
+已经在早先执行了
内 SRNS 重定位，
这使得源密钥被调整
2
针对未被更新的 RNC 的
没有 ME 参与的 SRNS 重定位
不调整密钥
3
RNC不知道
ME 是否被更新
ME
+不知道 RNC
没有被更新
针对未更新的 RNC 的
没有 ME 参与的 SRNS 重定位
针对被更新的 RNC 的
没有 ME 参与的 SRNS 重定位
不调整密钥
4
针对被更新的 RNC 的
没有 ME 参与的 SRNS 重定位
1
调整密钥
RNC
+知道 ME 被更新
ME
+知道 RNC 被更新

图 4

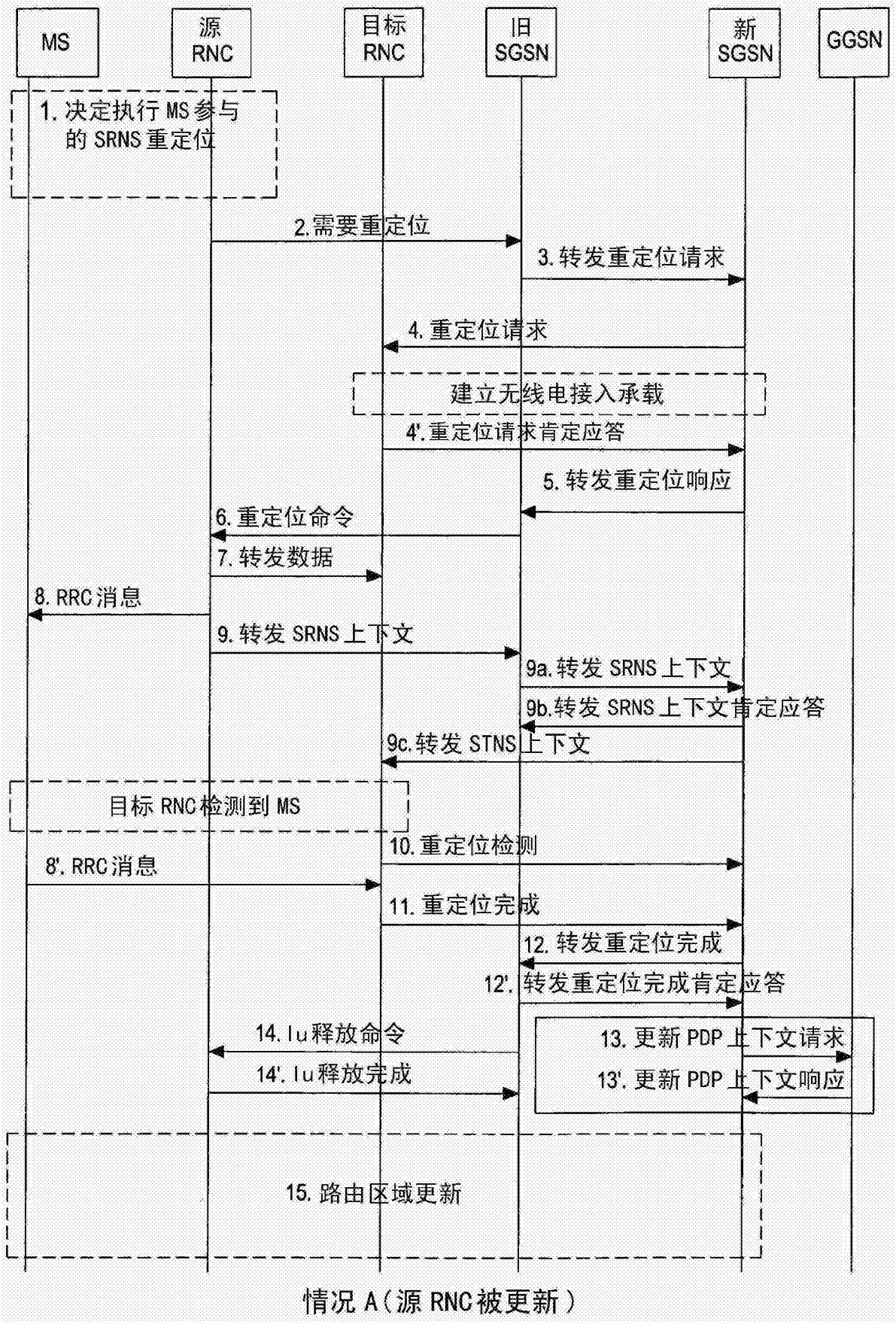

MS
源 RNC
目标 RNC
旧 SGSN
新 SGSN
GGSN
1. 决定执行 MS 参与的 SRNS 重定位
2. 需要重定位
3. 转发重定位请求
4. 重定位请求
建立无线电接入承载
4'. 重定位请求肯定应答
5. 转发重定位响应
6. 重定位命令
7. 转发数据
8. RRC 消息
9. 转发 SRNS 上下文
9a. 转发 SRNS 上下文
9b. 转发 SRNS 上下文肯定应答
9c. 转发 STNS 上下文
目标 RNC 检测到 MS
10. 重定位检测
8'. RRC 消息
11. 重定位完成
12. 转发重定位完成
12'. 转发重定位完成肯定应答
14. Iu 释放命令
13. 更新 PDP 上下文请求
14'. Iu 释放完成
13'. 更新 PDP 上下文响应
15. 路由区域更新
情况 A（源 RNC 被更新）

图 5

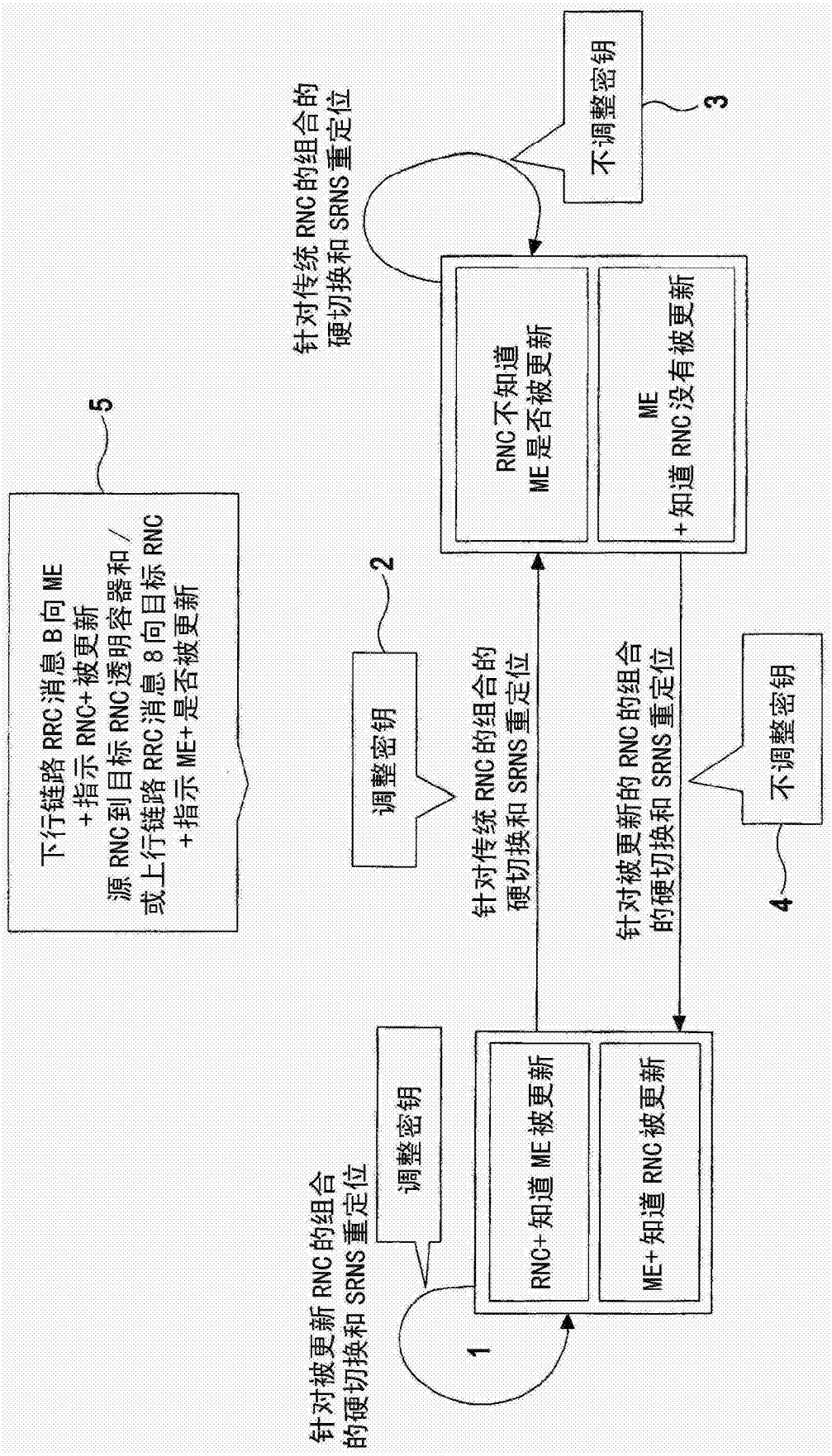
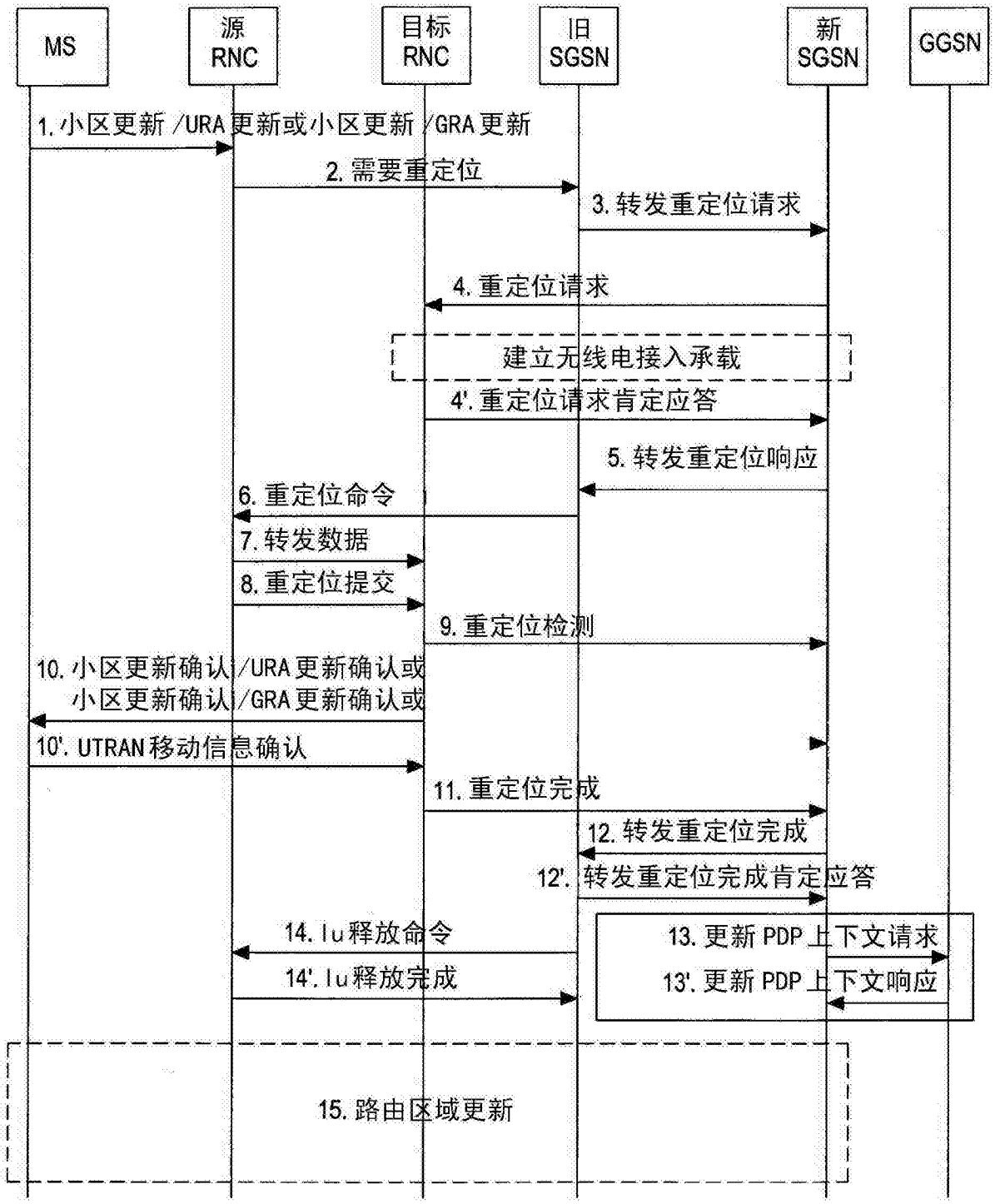

针对被更新 RNC 的组合
的硬切换和 SRNS 重定位
调整密钥
RNC+ 知道 ME 被更新
ME+ 知道 RNC 被更新
1
针对传统 RNC 的组合的
硬切换和 SRNS 重定位
调整密钥
2
针对被更新的 RNC 的组合
的硬切换和 SRNS 重定位
不调整密钥
4
针对传统 RNC 的组合的
硬切换和 SRNS 重定位
RNC 不知道
ME 是否被更新
ME
+ 知道 RNC 没有被更新
不调整密钥
3
下行链路 RRC 消息 B 向 ME
+ 指示 RNC+ 被更新
源 RNC 到目标 RNC 透明容器和 /
或上行链路 RRC 消息 8 向目标 RNC
+ 指示 ME+ 是否被更新
5

图 6



情况 A（源 RNC 被更新）

图 7

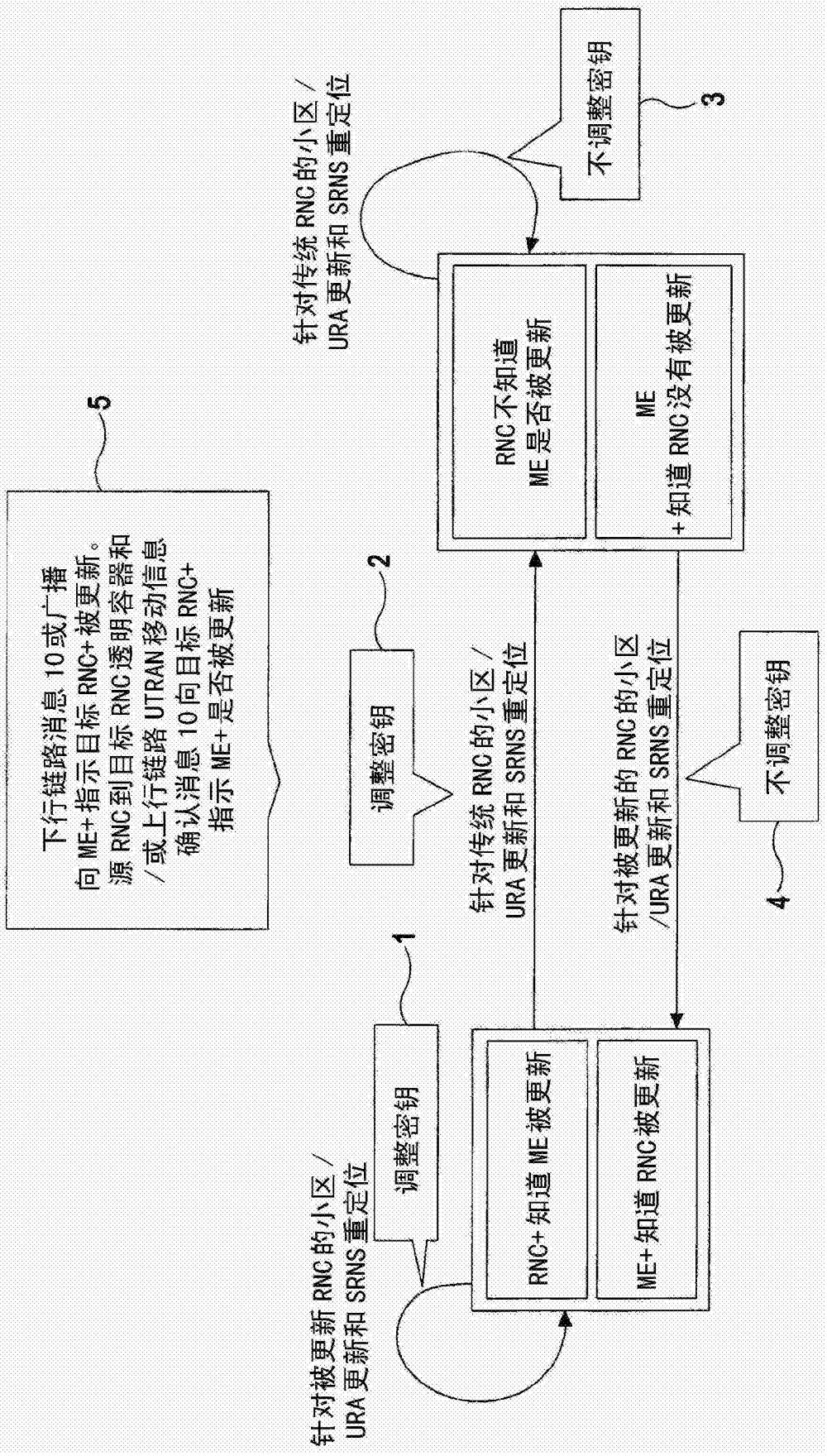

下行链路消息 10 或广播
向 ME+ 指示目标 RNC+ 被更新。
源 RNC 到目标 RNC 透明容器和
/ 或上行链路 UTRAN 移动信息
确认消息 10 向目标 RNC+
指示 ME+ 是否被更新
5
针对传统 RNC 的小区 /
URA 更新和 SRNS 重定位
不调整密钥
3
RNC 不知道
ME 是否被更新
ME
+ 知道 RNC 没有被更新
2
调整密钥
针对传统 RNC 的小区 /
URA 更新和 SRNS 重定位
针对被更新的 RNC 的小区
/URA 更新和 SRNS 重定位
不调整密钥
4
1
调整密钥
针对被更新 RNC 的小区 /
URA 更新和 SRNS 重定位
RNC+ 知道 ME 被更新
ME+ 知道 RNC 被更新

图 8

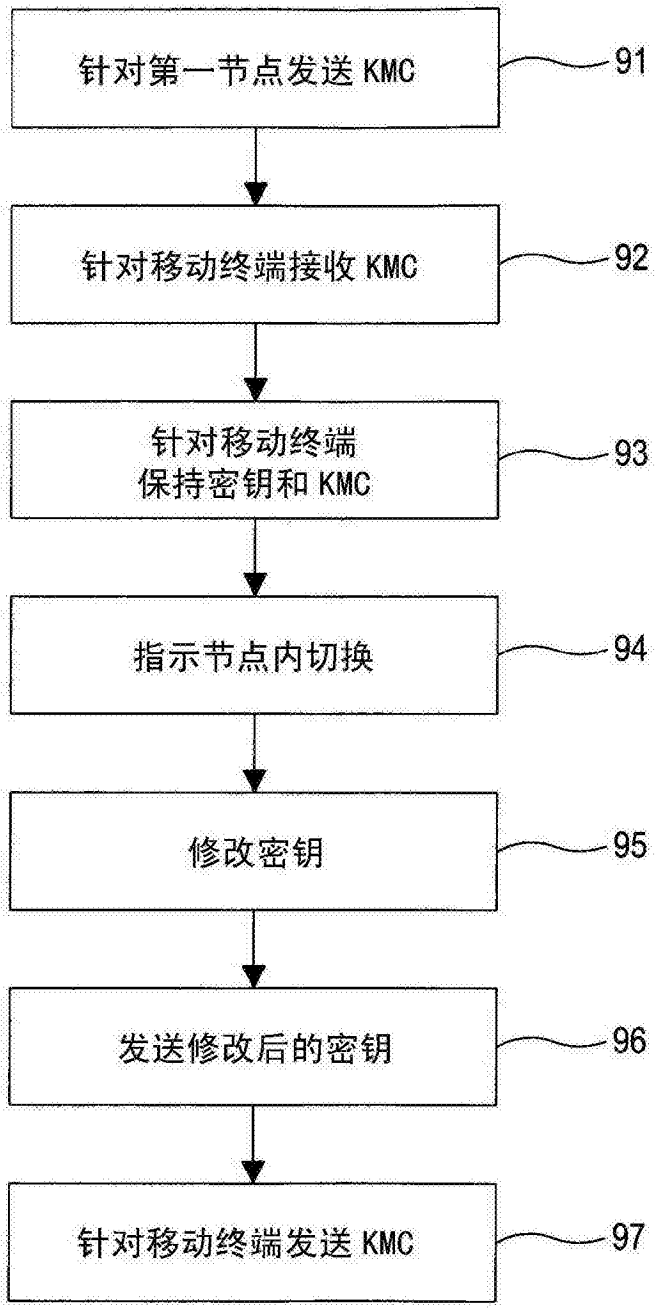

针对第一节点发送 KMC
91
针对移动终端接收 KMC
92
针对移动终端
保持密钥和 KMC
93
指示节点内切换
94
修改密钥
95
发送修改后的密钥
96
针对移动终端发送 KMC
97

图 9

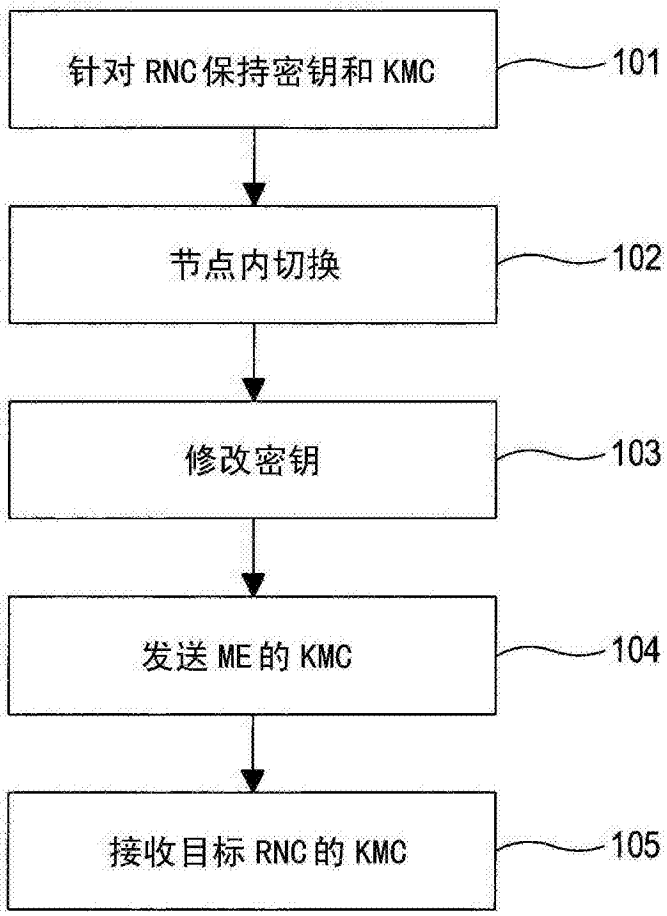

针对 RNC 保持密钥和 KMC
101
节点内切换
102
修改密钥
103
发送 ME 的 KMC
104
接收目标 RNC 的 KMC
105

图 10

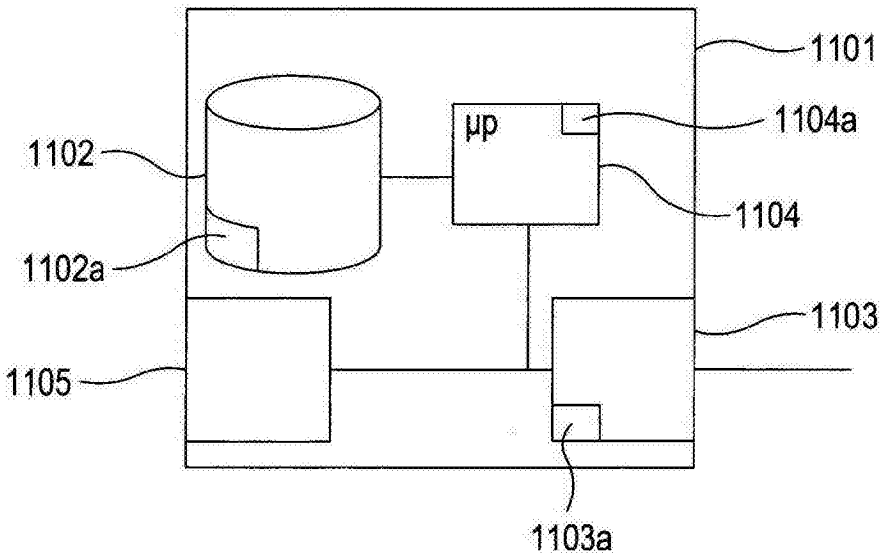

1101
μp
1104a
1102
1104
1102a
1103
1105
1103a

图 11

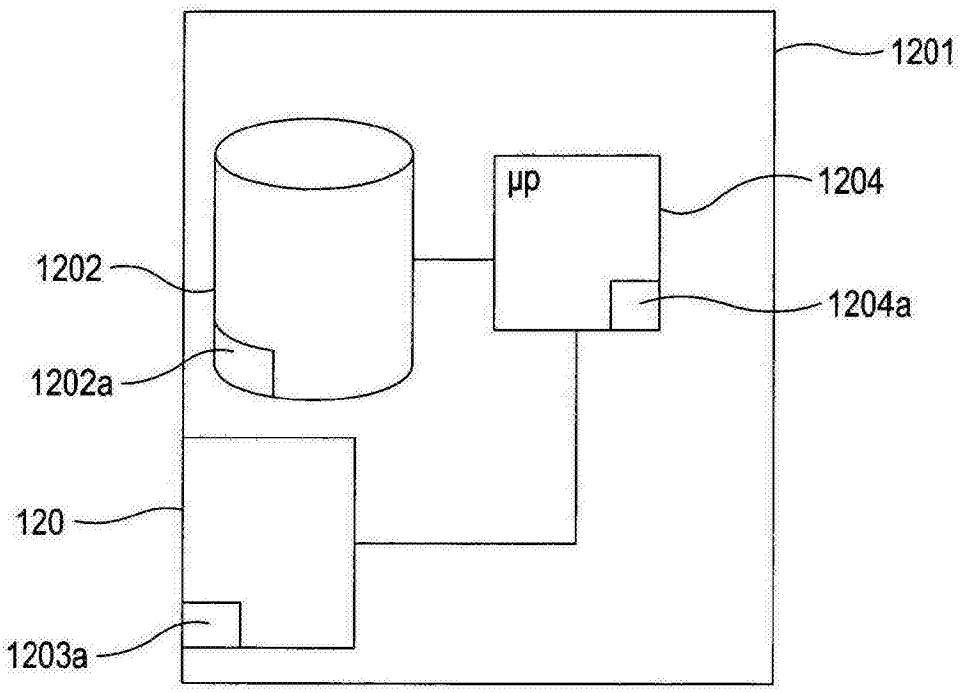


图 12