[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38

[12] 发明专利说明书

[21] ZL 专利号 00813435.9

[45] 授权公告日 2004 年 7 月 14 日

[11] 授权公告号 CN 1157982C

[22] 申请日 2000.9.26 [21] 申请号 00813435.9
[30] 优先权
[32] 1999. 9.28 [33] US [31] 09/406,377
[86] 国际申请 PCT/IB2000/001359 2000.9.26
[87] 国际公布 WO2001/024562 英 2001.4.5
[85] 进入国家阶段日期 2002.3.27
[71] 专利权人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 塞尔吉·豪蒙特
审查员 陈 军

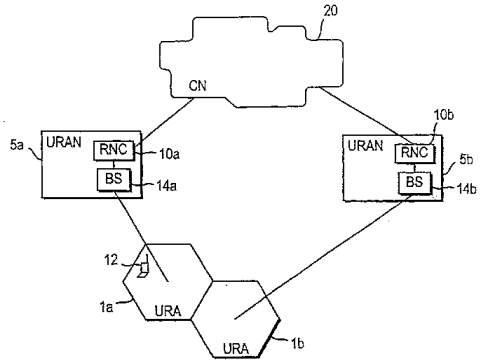
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李德山

权利要求书 10 页 说明书 12 页 附图 5 页

[54] 发明名称 通用移动电话业务的安全进程

[57] 摘要

本发明公开了一种用于移动通信系统中的通信业务的安全进程，该移动通信系统具有一个核心网，连接到分别在无线接入网区域上提供无线电覆盖的多个无线接入网，每个无线接入网具有一个无线网络控制器和一个基站，其特征在于，所述进程包括下述步骤，由无线网络控制器检测由于安全操作故障导致的该无线网络控制器和移动台之间的通信故障，其中所述安全操作故障阻止了该移动台和该移动通信系统的通信业务之间的通信，该无线网络控制器控制该移动台所处无线接入网络区域的无线电覆盖；从该无线网络控制器发送一个请求到该核心网，指示所检测到的通信故障；以及响应来自无线网络控制器的请求，在该核心网和移动台之间执行移动台鉴权进程。



ISSN1008-4274

知识产权出版社出版

1. 一种用于移动通信系统中执行通信业务的安全进程的方法，该移动通信系统具有一个核心网（20），连接到分别在无线接入网区域（1a，1b）上提供无线电覆盖的多个无线接入网（5a，5b），每个无线接入网具有一个无线网络控制器(10a,10b)和一个基站(14a,14b)，其特征在于，所述进程包括下述步骤，

（a）由无线网络控制器（10a，10b）检测由于安全操作故障导致的该无线网络控制器（10a，10b）和移动台（12）之间的通信故障，其中所述安全操作故障阻止了该移动台和该移动通信系统的通信业务之间的通信，该无线网络控制器（10a，10b）控制该移动台（12）所处无线接入网络区域（1a，1b）的无线电覆盖；

（b）从该无线网络控制器（10a，10b）发送一个请求到该核心网（20），指示在步骤（a）检测到的通信故障；以及

（c）响应来自无线网络控制器（10a，10b）的请求，在该核心网（20）和移动台（12）之间执行移动台鉴权进程。

2. 根据权利要求1的方法，其中所述步骤（b）还包括由核心网（20）确定在步骤(a)检测到的通信故障是否需要移动台鉴权的步骤，而且只有在步骤（b）中确定需要鉴权时，在执行所述步骤（c）。

3. 根据权利要求1的方法，其中所述步骤（b）还包括发送在所述步骤（a）检测到的通信故障的原因指示。

4. 根据权利要求1的方法，其中所述步骤（c）还包括步骤:

（i）在核心网（20）接收到来自无线网络控制器（10a，10b）的请求后，由该核心网（20）和移动台（12）执行鉴权;

（ii）确定在步骤（i）后移动台（12）是否被核心网（20）鉴权;以及

（iii）如果在步骤（ii）确定该鉴权成功，则从该核心网（20）发送一个确认到无线网络控制器（10a，10b）。

5. 根据权利要求 4 的方法，其中所述步骤（iii）包括发送一个包含新安全参数的确认到该无线网络控制器（10a，10b）。

6. 根据权利要求 2 的方法，其中所述步骤（c）还包括步骤:

（i）在核心网（20）接收到来自无线网络控制器（10a，10b）的请求后，由核心网（20）和移动台（12）执行鉴权;

（ii）确定在步骤（i）后移动台（12）是否被核心网（20）鉴权;以及

（iii）如果在步骤（ii）确定该鉴权成功，则从该核心网（20）发送一个确认到无线网络控制器（10a，10b）。

7. 根据权利要求 6 的方法，其中所述步骤（iii）包括发送一个包含新安全参数的确认到该无线网络控制器（10a，10b）。

8. 根据权利要求 1 的方法，其中所述步骤（c）还包括步骤:

（i）在核心网接收到来自无线网络控制器（10a，10b）的请求后，由核心网（20）和移动台（12）执行鉴权;

（ii）确定在步骤（i）后移动台（12）是否被核心网（20）鉴权;以及

（iii）如果在步骤（ii）确定该鉴权不成功，则从该核心网（20）发送一个确认到无线网络控制器（10a，10b）。

9. 根据权利要求 4 的方法，其中步骤（i）包括在鉴权中心和移动台（12）独立运行一个鉴权算法并为它们各自生成一个输出，而且所述步骤（ii）包括在核心网比较这两个输出。

10. 根据权利要求 1 的方法，还包括步骤:

（i）联系移动台（12）的鉴权中心，并在所述步骤（b）和（c）之间生成新的安全参数；以及

（ii）在所述步骤（c）后利用该新安全参数更新无线网络控制器（10a，10b）。

11. 根据权利要求 4 的方法，其中所述步骤（iii）包括发送一个包含新完整性算法的确认到该无线网络控制器（10a，10b）。

12. 根据权利要求 4 的方法，其中所述步骤（iii）包括发送一个包含新密码本的确认到该无线网络控制器（10a，10b）。

13. 根据权利要求 4 的方法，其中所述步骤（iii）包括发送一个包含新完整性密钥的确认到该无线网络控制器（10a，10b）。

14. 根据权利要求 1 的方法，其中所述检测步骤包括，确定在步骤（a）检测到的通信故障是否在移动台（12）从一个无线接入网区域（1a，1b）移动到另一区域期间，由一个失败的完整性校验导致。

15. 根据权利要求 1 的方法，在所述步骤（c）之前，还包括确定当存储于移动台（12）的完整性密钥或密码本与存储于无线网络控制器（10a，10b）中的完整性密钥或密码本不匹配时，是否需要一个新完整性密钥或新密码本的步骤。

16. 根据权利要求 1 的方法，其中所述步骤（a）包括：由所述无线网络控制器（10a，10b）通过检测一个反复的完整性校验故障来检测该通信故障。

17. 根据权利要求 1 的方法，其中该移动通信业务包括通用移动

电话业务。

18. 一种用于移动通信系统中执行通信业务的方法，该移动通信系统有一个核心网（20），连接到分别在无线接入网区域（1a，1b）上提供无线电覆盖的多个无线接入网（5a，5b），每个无线接入网具有一个无线网络控制器（10a，10b）和一个基站（14a，14b），其特征在于，所述进程还包括步骤:

（a）由无线网络控制器（10a，10b）检测由于安全操作故障导致的该无线网络控制器（10a，10b）和移动台（12）之间的通信故障，这个安全操作故障阻止了该移动台和该移动通信系统的通信业务之间的通信，该无线网络控制器（10a，10b）控制该移动台（12）所处的无线接入网络区域（1a，1b）；

（b）从该无线网络控制器（10a，10b）发送一个请求到该核心网，指示在步骤（a）检测到的通信故障;

（c）联系移动台（12）的数据库，并同时利用步骤（b）由所述核心网（20）生成一个加密密钥;

（d）在核心网接收到来自无线网络控制器（10a，10b）的请求后由核心网（20）执行鉴权;

（e）确定在步骤（c）之后移动台（12）是否被核心网（20）鉴权；以及

（f）如果在步骤（e）确定该移动台（12）被鉴权，则利用在所述步骤（c）生成的加密密钥替换无线网络控制器（10a，10b）和移动台（12）中的原加密密钥。

19. 根据权利要求18的方法，其中所述步骤（d）还包括步骤:

（i）从核心网（20）发送一个查询到移动台（12）；

（ii）利用鉴权中心和移动台（12）中的鉴权算法执行查询，并为它们各自生成一个输出;

（iii）通过比较鉴权中心和移动台（12）生成的输出，确定步骤

（ii）的鉴权是否成功；以及

（iv）如果在步骤（iii）确定该鉴权成功，则从核心网（20）发送一个确认到该无线网络控制器（10a，10b）。

20. 根据权利要求 18 的方法，其中步骤（f）还包括利用在所述步骤（c）生成的加密密钥替换数据库中存储的原加密密钥。

21. 根据权利要求 18 的方法，其中在所述步骤（c）生成的所述加密密钥包括一个密码本。

22. 根据权利要求 19 的方法，其中在所述步骤（c）生成的所述加密密钥包括一个完整性密钥。

23. 根据权利要求 18 的方法，其中所述步骤（a）包括：由所述无线网络控制器（10a，10b）通过检测一个反复的完整性校验故障来检测该通信故障。

24. 根据权利要求 18 的方法，其中该移动通信业务包括通用移动电话业务。

25. 根据权利要求 18 的方法，其中步骤（c）的数据库是与所述移动台相关的归属位置寄存器的一部分，而且所述步骤（c）包括联系移动台（12）的归属位置寄存器。

26. 一种移动通信系统，包括：一个核心网（20）；分别在无线接入网区域（1a，1b）上提供无线电覆盖的多个无线接入网（5a，5b），每个所述无线接入网（5a，5b）连接到所述核心网（20），而且每个接入网有一个无线网络控制器（10a，10b）和一个基站（14a，14b），其特征在于，该移动通信系统还包括：

用于由其中一个所述网络控制器（10a，10b）来检测在其中一个所述无线网络控制器（10a，10b）和由所述无线网络控制器（10a，10b）所控制的通用无线接入网络区域（1a，1b）内的移动台（12）之间的通信故障的装置，其中该通信故障阻止了该移动台和该移动通信系统中的通信业务之间的通信，而且是由一个安全操作故障导致的；

用于从其中一个所述无线网络控制器（10a，10b）发送一个请求到所述核心网（20），响应所述检测以便执行该移动台（12）的鉴权和改变安全参数的装置；

用于响应从其中一个所述无线网络控制器（10a，10b）接收的鉴权移动台（12）的请求，而由核心网（20）鉴权该移动台（12）的装置；

用于响应从其中一个所述无线网络控制器（10a，10b）接收的改变安全参数的请求，而由该核心网（20）设置一个新安全参数的装置；

用于利用该新安全参数替换在其中一个所述无线网络控制器（10a，10b）和移动台（12）中存储的现有安全参数的装置；以及

如果该移动台（12）没有被所述鉴权装置成功鉴权，则通过该核心网（20）从所述其中一个所述无线网络控制器（10a，10b）分离该移动台（12）的装置。

27. 根据权利要求26的系统，其中所述移动台包括一个移动电话，而且所述检测通信故障的装置包括用于检测其中一个所述无线网络控制器和移动电话之间的通信故障的装置。

28. 根据权利要求26的系统，其中所述安全参数包括一个密码本。

29. 根据权利要求26的系统，其中所述安全参数包括一个完整性密钥。

30. 根据权利要求26的系统，其中所述安全参数包括一个完整性

算法或一个加密算法。

31. 根据权利要求26的系统，还包括一个鉴权中心，其中所述鉴权装置还包括用于独立执行鉴权算法并在所述鉴权中心和所述移动台生成一个输出，以及比较所述移动台和所述鉴权中心的输出的装置。

32. 根据权利要求26的系统，其中所述通信系统用于通用移动电话业务。

33. 一种通信系统的核心网（20），所述通信系统还包括连接到该核心网（20）的多个无线接入网（5a，5b）以及一个移动台（12），每个所述无线接入网（5a，5b）在无线接入网区域（1a，1b）上提供无线电覆盖，而且具有一个无线网络控制器（10a，10b）和一个基站（14a，14b），该无线网络控制器（10a，10b）存储在该无线网络控制器（10a，10b）和移动台（12）通信期间使用的安全参数，

其特征在于，所述核心网（20）包括:

用于检测其中一个所述无线网络控制器和由位于所述无线网络控制其所控制的通用无线接入网区域中的移动台之间的通信故障的装置;

响应于接收到的来自其中一个无线网络控制器（10a，10b）的鉴权移动台的请求，通过发送一个鉴权查询到移动台（12），从该移动台（12）接收鉴权查询的结果，并比较该结果与鉴权移动台（12）所需结果而鉴权该移动台的装置，该鉴权请求由该无线网络控制器启动，以响应阻止移动台（12）和核心网（20）之间通信的安全操作故障;

用于响应接收到改变安全参数的请求而设置新安全参数的装置;

如果该移动台被成功鉴权，则利用新安全参数替换在无线网络控制器（10a，10b）和移动台（12）中存储的现有安全参数的装置；以及

如果该移动台（12）没有被所述鉴权装置成功鉴权，则从所述无

线网络控制器（10a，10b）分离该移动台（12）的装置。

34. 根据权利要求33的核心网，其中所述安全参数包括一个密码本。

35. 根据权利要求33的核心网，其中所述安全参数包括一个完整性密钥。

36. 根据权利要求33的核心网，其中所述安全参数包括一个完整性算法或一个加密算法。

37. 根据权利要求33的核心网，还包括一个鉴权中心，其中所述鉴权装置还包括用于在所述鉴权中心独立执行鉴权算法并生成所需结果的装置，以及用于比较该移动台（12）生成的结果与所述鉴权中心生成的所需结果的装置。

38. 根据权利要求33的核心网，其中所述核心网（20）包括用于通用移动电话业务的通用核心网。

39. 一种移动通信系统的无线接入网，所述移动通信系统包括一个移动台（12）、一个连接到所述无线接入网（5a，5b）的核心网（20）的多个无线接入网，每个无线接入网（5a，5b）分别在无线接入网络区域（1a，1b）上提供无线电覆盖；

所述移动通信系统还包括：

一个无线网络控制器（10a，10b），其存储有一个安全参数，用于在所述每个无线接入网（5a，5b）与该移动台（12）通信期间使用；

以及一个基站（14a，14b），

其特征在于，每个无线接入网（5a，5b）还包括：

在无线网络控制器（10a，10b）中，用于检测在该无线网络控制

器（10a，10b）和位于所述无线网络控制器（10a，10b）控制的通用无线接入网络区域的移动台（12）之间的通信故障的装置，该通信故障由阻止该移动台和所述核心网（20）之间通信的安全操作故障导致；

用于从所述无线网络控制器（10a，10b）发送一个请求到该核心网（20），以鉴权该移动台（12）和改变一个安全参数，以便响应于所述检测装置检测到通信故障的装置；

用于从该核心网（20）传递一个鉴权查询指令到该移动台（12）的装置；

用于从该移动台（12）传递鉴权查询的结果到核心网（20）的装置；以及

在该核心网执行鉴权后，用于从该核心网（20）接收一个新安全参数的装置。

40. 根据权利要求 39 的无线接入网，其中所述安全参数包括一个密码本。

41. 根据权利要求 39 的无线接入网，其中所述安全参数包括一个完整性密钥。

42. 根据权利要求 39 的无线接入网，其中所述安全参数包括一个完整性算法或一个加密算法。

43. 根据权利要求 39 的无线接入网，其中所述无线接入网包括一个用于通用移动电话业务的通用核心网。

44. 一种移动通信系统的移动台，所述移动通信系统包括一个核心网（20）以及分别在无线接入网络区域（1a，1b）上提供无线电覆盖的多个无线接入网络（5a，5b），每个所述无线接入网（5a，5b）连接到核心网（20），并且

所述移动通信系统还包括一个无线网络控制器（10a，10b）和基站（14a，14b），

所述移动台（12）包括:

存储了该移动台（12）的唯一标识符和鉴权算法的数据库;

用于在无线网络控制器（10a，10b）检测到所述移动台和无线接入网（5a，5b）之间由于一个安全操作故障导致的通信故障后，从所述核心网（20）借助一个无线接入网（5a，5b）接收一个鉴权查询指令的装置，所述鉴权查询包含一个利用该移动台（12）数据库中的唯一标识符，执行鉴权算法以生成一个结果的指令;

用于利用该鉴权算法和唯一标识符执行鉴权查询，以响应接收到该鉴权查询和生成鉴权查询结果的装置；以及

借助无线接入网发送该鉴权查询的结果到该核心网，以由该核心网鉴权该移动台的装置。

45. 根据权利要求 44 的移动台，其中所述移动台（12）包括用于通用移动电话业务的通用移动台。

通用移动电话业务的安全进程

技术领域

本发明涉及一种用于通用移动电话业务（UMTS）的安全进程，执行该安全进程是响应在一个移动台（MS）和一个与安全相关的无线网络控制器（RNC）之间检测到的通信故障，如完整性校验故障或加密故障。

背景技术

通用移动电话业务（UMTS）为用于第三代移动通信系统的网络平台，旨在为用户提供无缝服务，而且能跨越许多网络使用。一般来说，UMTS 系统包括一个连接到多个通用无线接入网（URAN）的核心网（CN）。CN 包括两部分：适用于电路交换业务的第一部分（例如，移动交换中心（MSC）和来访位置寄存器（VLR））以及适用于分组交换业务的第二部分（例如服务 GPRS 支持节点（SGSN））。每个 URAN 提供越过一个称为 URAN 区域（URA）的指定地理区域的无线电覆盖。为提供这种覆盖，每个 URAN 包括一个无线网络控制器（RNC），其控制至少一个基站（BS）。该 RNC 与其它 RNC 互连以执行交换操作和移动性管理。CN 可连接到所有其它类型的网络以提供用户无缝服务。

MS 从一个 URA（称为原 URA）到一个新 URA 的移动启动了由新 URA 的 RNC 执行的 URA 更新，以便能在需要时到达 MS。为了网络运营商的利益应确保启动 URA 更新的 MS 为有效用户。该确认涉及 RNC 执行完整性校验，这是 RNC 和 MS 之间的分组传输的鉴权。

每个 MS（也称为 UMTS 设备（UE））包括一个用户识别模块（SIM）卡，卡内包含数据库和可执行文件。SIM 卡在其数据库包含一个国际移动用户身份（IMSI），关于 MS 当前位置的位置信息，完整性密钥

IK，以及其它安全和管理信息。当手持电话被正确去活而且当 MS 从一个 URA 移动到另一个 URA 时，每个呼叫结束后在 SIM 卡刷新位置信息。位置信息包括每个 URA 内使用的一个临时匿名识别，它可称为临时移动用户身份（TMSI），分组 TMSI（PTMSI），或无线网络临时识别（RNTI）。TMSI 或其它临时识别用作提供匿名识别而不是利用 IMSI 识别该特定 MS 的安全措施。作为另一个安全措施，MS 和 URAN 之间的通信利用一个加密密钥加密。该加密密钥通常为一个密码本 CK，其存储于鉴权中心（AuC）或归属位置寄存器（HLR）。

现在参考图 5 描述在 UMTS 系统中的现有技术完整性校验。当 MS 通过发送一个 COUNT 参数到 RNC 启动一个无线电资源连接（RRC）的建立时，启动该完整性校验（步骤 1）。COUNT 为一个随时间变化的值，其在无线电链路的两侧每隔 10ms 增大。用户存储最近使用过的 COUNT 参数并将其加 1 以确保对相同完整性密钥 IK（网络）不再用 COUNT 值。

RNC 存储接收到的 COUNT 参数（步骤 2）。MS 接着发送一个初始 L3 消息，如位置更新请求、通信管理（CM）业务请求或路由区更新请求到相关 CN（步骤 3）。初始 L3 消息将包含相关的移动性管理（MM）信息；使用例如上述的临时识别的 MS 识别；MS 级别 IE，其包括有关该 MS 支持的 UMTS 完整性算法（UIA）和 UMTS 加密算法（UEA）等信息；以及电键标识符（KSI），其为在对这个 CN 域作最后鉴权时由 CN 分配的号码。

MS 发送完毕所有这些信息后，可执行分组鉴权以及生成新安全密钥，如完整性密钥 IK 和密码本 CK（步骤 4）。接着也将分配一个新 KSI。因此，该鉴权进程除了用于鉴权用户发送的信息分组还用于改变 IK 和 CK。

为执行分组鉴权，CN 选择允许使用的 UIA 和 UEA。CN 通过发送一个 RANAP 消息“安全模式指令”到 RNC 启动完整性校验（步骤 6）。这个消息包括允许的 UIA 和要使用的 IK。如果要求加密更新，该消息还可包含允许的 UEA 和要使用 IK。这个消息还包括通过 RNC

透明发送到 MS 的 UE 级别 IE。

RNC 确定将使用那些允许的 UIA 和 UEA，生成一个随机值 FRESH 并启动下行链路完整性保护（步骤 7）。RNC 接着生成 RRC 消息“安全控制指令”，其包括一个随机查询 RAND 和一个表示网络鉴权 AUTN 的鉴权。这个消息还包括 UE 级别 IE、UIA 以及随机值 FRESH。如果正执行加密更新，则也可包含要使用的 UEA 以及与开始加密相关的附加信息。在这一点上有两个 CN，每个 CN 有其自己的 IK。因此，网络必须表明使用哪一个 IK。这是通过在“安全控制指令”消息中包含一个 CN 型指示器信息实现的。在发送“保密控制指令”消息到 MS 之前，RNC 生成一个 MAC-I（用于完整性的消息鉴权码）并将这个信息附在该消息中。

一接收到包含具有 MAC-I 的 RAND AUTN 的“安全控制指令”消息，MS 验证从 RNC 接收的 UE 级别 IE 是否等于在初始 L3 消息中发送的 UE 级别 IE，接着基于通过利用指示的 UIA、存储的 COUNT 以及接收的 FRESH 参数接收到的消息计算 XMAC-I。UE 接着通过比较接收的 MAC-I 与生成的 XMAC-I 验证该消息的数据完整性（步骤 9）。

如果步骤 9 成功，MS 计算一个 RRC 消息的安全控制响应（RES），并为这个消息生成第二 MAC-I。MS 接着发送具有第二 MAC-I 的“安全控制响应”到 RNC（步骤 10）。

一接收到 RES 消息，RNC 基于作为 UIA 的输入的 RES 计算第二 XMAC-I。RNC 接着通过比较接收的第二 MAC-I 与生成的第二 XMAC-I 验证该消息的数据完整性（步骤 11）。当在步骤 11 验证数据完整性时，RNC 发送一个 RANAP“安全模式完成”消息到 CN 以结束该完整性进程（步骤 12）。

“安全模式指令”在步骤 6 对 MS 启动下行链路完整性保护，即发送到该 MS 的所有后面消息被完整性保护。MS 发送的“安全控制响应”启动上行链路完整性保护，即从 MS 发送的所有后面消息被完整性保护。

如果由于上述的完整性校验失败或由于解密失败而出现通信故

障，RNC 不知道该如何操作（因为它无法执行 MS 的鉴权进程）而且 MS 将断开连接。出现这种情况的一种可能原因是一个有效 MS 的密码本 CK 或完整性密钥 IK 与 RNC 中存储的密码本或完整性密钥 IK 不匹配。这种情形本身也表示如果一个无线电链路被破坏而且重新启动，在此情况下，RNC 或 MS 由于安全原因被禁止与原密码本 CK 或完整性密钥 IK 通信。由于在此情况下 MS 不自动更新，这就存在失配。值得注意，如果 RNC 在完整性校验（反复）失败的情况下只释放该连接，那么恶意用户能通过发送一个错误分组导致有效用户连接中断。因此，需要一种安全进程用于 UMTS 以便有效 MS 可在上述情况下接入该系统。

全球移动通信系统（GSM）技术规范定义了一种标记为算法 A3 的鉴权进程，这种算法在 ETSI TS 100 929 GSM 03.20 版本 6.1.0（1997-07），数字蜂窝通信系统（阶段 2+）；有关安全的网络功能，EN 300 940 GSM 04.08 版本 6.3.1（1999-08），数字蜂窝通信系统（阶段 2+）；移动无线电接口层 3 规范，和 Mouly et al，GSM 移动通信系统（第 7 章，432-498 页）中有描述。A3 算法在 GSM 使用完整性密钥 K_i，完整性密钥对每个移动台是唯一的。然而，在 UMTS，MS 的完整性密钥 IK 和密码本 CK 均可改变。

发明内容

本发明的一个目的是为通用移动电话业务（UMTS）的使用提供一个安全进程，以触发移动台（MS）的鉴权和/或通过核心网（CN）生成一个新完整性密钥（IK）和/或一个新密码本（CK），以便响应通用无线接入网（URAN）的无线网络控制器（RNC）检测到通信故障。

这个目的是通过用于 UMTS 通信系统的安全进程实现的，该 UMTS 通信系统有一个核心网（CN），连接到分别在 URAN 区域（URA）的无线电覆盖上提供多个 URAN。每个 URAN 有一个 RNC 和一个基站（BS）。当 RNC 检测到 MS 和其之间的一个通信故障时启动该安

全进程。RNC 接着确定该检测到的通信故障是否要求 MS 鉴权。如果要求鉴权，CN 在其和 MS 之间执行一个鉴权进程以鉴权 MS，并选择性地改变完整性密钥 IK 和密钥 CK。

该目的也可通过用于 UMTS 通信系统的安全进程实现，该 UMTS 通信系统有一个 CN 连接到分别在 URA 的无线电覆盖上提供多个 URAN。每个 URAN 有一个 RNC 和一个 BS。该安全进程包括由 RNC 检测 MS 和其之间的通信故障的步骤。RNC 接着发送一个请求到 CN 以执行 MS 的鉴权。该请求最好包含一个描述该故障（即，“完整性校验故障”）的原因参数。CN 在其接收到来自 RNC 的请求后执行 MS 的鉴权。

如果 MS 的鉴权失败，CN 向 RNC 指示该情况。如果鉴权成功，CN 例如利用“安全模式指令”消息指示 RNC 该新安全参数。另外，CN 可利用该鉴权进程修正其它安全参数。例如，为响应“完整性校验失败”，CN 可修正 UMTS 完整性算法（UIA）。

根据本发明的一个方面，提供了一种用于移动通信系统中的通信业务的安全进程，该移动通信系统具有一个核心网 20，连接到分别在无线接入网区域 1a，1b 上提供无线电覆盖的多个无线接入网 5a，5b，每个无线接入网具有一个无线网络控制器 10a，10b 和一个基站 14a，14b，其特征在于，所述进程包括下述步骤，

（a）由无线网络控制器 10a，10b 检测由于安全操作故障导致的该无线网络控制器 10a，10b 和移动台 12 之间的通信故障，其中所述安全操作故障阻止了该移动台和该移动通信系统的通信业务之间的通信，该无线网络控制器 10a，10b 控制该移动台 12 所处无线接入网络区域 1a，1b 的无线电覆盖；

（b）从该无线网络控制器 10a，10b 发送一个请求到该核心网 20，指示在步骤（a）检测到的通信故障；以及

（c）响应来自无线网络控制器 10a，10b 的请求，在该核心网 20 和移动台 12 之间执行移动台鉴权进程。

根据本发明的一个方面，提供了一种用于移动通信系统中的通信

业务的安全进程，该移动通信系统有一个核心网 20，连接到分别在无线接入网区域 1a，1b 上提供无线电覆盖的多个无线接入网 5a，5b，每个无线接入网具有一个无线网络控制器 10a，10b 和一个基站 14a，14b，其特征在于，所述进程还包括步骤:

（a）由无线网络控制器 10a，10b 检测由于安全操作故障导致的该无线网络控制器 10a，10b 和移动台 12 之间的通信故障，这个安全操作故障阻止了该移动台和该移动通信系统的通信业务之间的通信，该无线网络控制器 10a，10b 控制该移动台 12 所处的无线接入网络区域 1a，1b;

（b）从该无线网络控制器 10a，10b 发送一个请求到该核心网，指示在步骤（a）检测到的通信故障;

（c）联系移动台 12 的数据库，并同时利用步骤（b）由所述核心网 20 生成一个加密密钥;

（d）在核心网接收到来自无线网络控制器 10a，10b 的请求后由核心网 20 执行鉴权;

（e）确定在步骤（c）之后移动台 12 是否被核心网 20 鉴权；以及

（f）如果在步骤（e）确定该移动台 12 被鉴权，则利用在所述步骤（c）生成的加密密钥替换无线网络控制器 10a，10b 和移动台 12 中的原加密密钥。

根据本发明的一个方面，提供了一种移动通信系统，包括：一个核心网 20；分别在无线接入网区域 1a，1b 上提供无线电覆盖的多个无线接入网 5a，5b，每个所述无线接入网 5a，5b 连接到所述核心网 20，而且每个接入网有一个无线网络控制器 10a，10b 和一个基站 14a，14b，其特征在于，该移动通信系统还包括:

用于由其中一个所述网络控制器 10a，10b 来检测在其中一个所述无线网络控制器 10a，10b 和由所述无线网络控制器 10a，10b 所控制的通用无线接入网络区域 1a，1b 内的移动台 12 之间的通信故障的装置，其中该通信故障阻止了该移动台和该移动通信系统中的通信业务

之间的通信，而且是由一个安全操作故障导致的；

用于从其中一个所述无线网络控制器 10a，10b 发送一个请求到所述核心网 20，响应所述检测以便执行该移动台 12 的鉴权和改变安全参数的装置；

用于响应从其中一个所述无线网络控制器 10a，10b 接收的鉴权移动台 12 的请求，而由核心网 20 鉴权该移动台 12 的装置；

用于响应从其中一个所述无线网络控制器 10a，10b 接收的改变安全参数的请求，而由该核心网 20 设置一个新安全参数的装置；

用于利用该新安全参数替换在其中一个所述无线网络控制器 10a，10b 和移动台 12 中存储的现有安全参数的装置；以及

如果该移动台 12 没有被所述鉴权装置成功鉴权，则通过该核心网 20 从所述其中一个所述无线网络控制器 10a，10b 分离该移动台 12 的装置。

根据本发明的一个方面，提供了一种通信系统的核心网 20，所述通信系统还包括连接到该核心网 20 的多个无线接入网 5a，5b 以及一个移动台 12，每个所述无线接入网 5a，5b 在无线接入网区域 1a，1b 上提供无线电覆盖，而且具有一个无线网络控制器 10a，10b 和一个基站 14a，14b，该无线网络控制器 10a，10b 存储在该无线网络控制器 10a，10b 和移动台 12 通信期间使用的安全参数，

其特征在于，所述核心网 20 包括：

用于检测其中一个所述无线网络控制器和由位于所述无线网络控制其所控制的通用无线接入网区域中的移动台之间的通信故障的装置；

响应于接收到的来自其中一个无线网络控制器 10a，10b 的鉴权移动台的请求，通过发送一个鉴权查询到移动台 12，从该移动台 12 接收鉴权查询的结果，并比较该结果与鉴权移动台 12 所需结果而鉴权该移动台的装置，该鉴权请求由该无线网络控制器启动，以响应阻止移动台 12 和核心网 20 之间通信的安全操作故障；

用于响应接收到改变安全参数的请求而设置新安全参数的装置；

如果该移动台被成功鉴权，则利用新安全参数替换在无线网络控制器 10a，10b 和移动台 12 中存储的现有安全参数的装置；以及

如果该移动台 12 没有被所述鉴权装置成功鉴权，则从所述无线网络控制器 10a，10b 分离该移动台 12 的装置。

根据本发明的另一个方面，提供了一种移动通信系统的无线接入网，所述移动通信系统包括一个移动台 12、一个连接到所述无线接入网 5a，5b 的核心网 20 的多个无线接入网，每个无线接入网 5a，5b 分别在无线接入网络区域 1a，1b 上提供无线电覆盖；

所述移动通信系统还包括：

一个无线网络控制器 10a，10b，其存储有一个安全参数，用于在所述每个无线接入网 5a，5b 与该移动台 12 通信期间使用；

以及一个基站 14a，14b，

其特征在于，每个无线接入网 5a，5b 还包括：

在无线网络控制器 10a，10b 中，用于检测在该无线网络控制器 10a，10b 和位于所述无线网络控制器 10a，10b 控制的通用无线接入网络区域的移动台 12 之间的通信故障的装置，该通信故障由阻止该移动台和所述核心网 20 之间通信的安全操作故障导致；

用于从所述无线网络控制器 10a，10b 发送一个请求到该核心网 20，以鉴权该移动台 12 和改变一个安全参数，以便响应于所述检测装置检测到通信故障的装置；

用于从该核心网 20 传递一个鉴权查询指令到该移动台 12 的装置；

用于从该移动台 12 传递鉴权查询的结果到核心网 20 的装置；以及

在该核心网执行鉴权后，用于从该核心网 20 接收一个新安全参数的装置。

根据本发明的再一个方面，提供了一种移动通信系统的移动台，所述移动通信系统包括一个核心网 20 以及分别在无线接入网络区域（1a，1b）上提供无线电覆盖的多个无线接入网络 5a，5b，每个所述无线接入网 5a，5b 连接到核心网 20，并且

所述移动通信系统还包括一个无线网络控制器 10a，10b 和基站 14a，14b，

所述移动台 12 包括:

存储了该移动台 12 的唯一标识符和鉴权算法的数据库;

用于在无线网络控制器 10a，10b 检测到所述移动台和无线接入网 5a，5b 之间由于一个安全操作故障导致的通信故障后，从所述核心网 20 借助一个无线接入网 5a，5b 接收一个鉴权查询指令的装置，所述鉴权查询包含一个利用该移动台 12 数据库中的唯一标识符，执行鉴权算法以生成一个结果的指令;

用于利用该鉴权算法和唯一标识符执行鉴权查询，以响应接收到该鉴权查询和生成鉴权查询结果的装置；以及

借助无线接入网发送该鉴权查询的结果到该核心网，以由该核心网鉴权该移动台的装置。

附图说明

为更好地理解本发明、其操作优点以及通过其使用获得的特定目标，应参考示意和描述本发明优选实施例的附图和描述性文字。

附图中类似的附图标记表示所有这些附图中的类似元件:

图 1 示出了 UMTS 基本部分的原理图;

图 2 为根据本发明一个实施例的安全进程的信号流程图;

图 3 为根据本发明一个实施例的安全进程的流程图;

图 4 为图 2 的安全进程的鉴权部分的流程图；以及

图 5 为 UMTS 完整性校验的信号流程图。

具体实现方式

通用移动电话业务（UMTS）是一种用于第三代移动系统的网络平台，旨在为用户提供到各种业务的无缝连接，而且能跨越多个网络使用。这些网络可例如包括移动电话业务，诸如用于寻呼机和移动电话的短文本消息业务，通用分组无线电业务（GPRS），以及诸如因特

网接入用户、email 业务、传真发送和远程计算机接入业务等其它数据业务。

图 1 示出了核心网 20，其连接到第一通用无线接入网（URAN）5a 和第二 URAN 5b。第一和第二 URAN 5a、5b 分别提供 URAN 区域（URA）1a、1b 与核心网 20 之间的无线电相关接入。第一 URAN 5a 包括第一无线网络控制器（RNC）10a 以及第一基站（BS）14a，第一基站监视移动台（MS）12 在相关 URA 1a 内的移动。MS 可例如包括移动电话、寻呼机、计算机或其它能从 URAN 接收信号的类似设备。第二 URAN 包括第二 RNC 10b 和第二 BS 14b 以监视第二 URA 1b。RNC 10a、10b 分别连接用于控制 BS 14a、14b。一般来说，一个 RNC 可连接到一个以上 BS，而每个 URAN 可有一个以上 RNC。URAN 5a、5b 监视 MS 12 的移动性，并管理在任何一个 URA 1a、1b 发送一个呼入或消息到 MS 12 或连接 MS 12 到一个预期业务或网络所必需的资源。

当 MS 从一个 URA 移动到另一个 URA，例如从第一（原）URA 1a 移动到第二（新）URA 1b 时，必须由新 URAN 5b 中的 RNC 10b 执行 URA 更新，以便新 URAN 5b 和核心网 20 具有支持 MS 12 所需的上述功能所要求的正确信息。为确保 MS 12 启动 URA 更新是有效的，新 URAN 5b 的 RNC 10b 执行完整性校验。

根据本发明的安全进程响应一个通信故障，例如如果这个完整性校验失败而执行。该通信故障可以是 MS 提供的保密签名与该 RNC 从原 RNC 接收的签名之间的失配造成的，或如果该 RNC 不了解该 MS——即，如果在加密密钥（密钥和/或完整性密钥）之间有差异可能导致通信故障。完整性校验可能反复失败，从而导致反复通信故障，如果新 RNC 不支持前一 RNC 使用的 UMTS 完整性算法（UIA）和/或 UMTS 加密算法（UEA），由此使得新 RNC 无法与 MS 通信。此外，该安全进程也可独立于 MS 从一个 URA 到另一 URA 的移动而执行。例如，该通信故障可包括 RNC 和 MS 之间的无线电链路被破坏。如果RNC和MS之间的无线电链路被破坏并重新启动，出于安全考虑，

可禁止 RNC 使用原加密密钥。此外，长数据发送期间（如，不检查用户数据的安全性的呼叫），在 RNC 和 MS 之间执行的周期性鉴权期间也可发生通信故障，在此 RNC 发送一个只包含一个完整性校验字段的鉴权请求作为轻（light）安全进程。

参考图 2 和图 3，当新 URAN 的 RNC 检测到通信故障时本发明的进程在步骤 100 启动。该通信故障（即，完整性校验故障）可首先发生在 RNC 或 MS。如果该通信故障出现在 MS，MS 通知 RNC 且 RNC 检测该故障。然而，RNC 可使用一种诸如“MS 故障”的特定进程向 CN 报告这个故障。检测到这个通信故障后，RNC 确定通信故障类型并发送一个通信故障消息到 CN，该消息包含该进程的指示连同一个根据本发明要求 CN 执行安全检查的请求（步骤 110）。CN 接着确定是否需要鉴权 MS（步骤 120）。如果该故障为持续故障则不需要鉴权。例如，如果最近成功执行了 MS 的鉴权，如在一个预定时帧内，而且该故障持续，那么该解决方案将断开 MS 的连接（步骤 210）。在一个可选实施例中，该进程可跳过步骤 120 并且每当在步骤 110 请求安全检查时自动执行该鉴权。

CN 根据通信故障的原因确定是否需要一个新的安全参数，如一个新的鉴权向量密钥（步骤 130）。如果在步骤 130 确定需要一个新安全参数，CN 将在步骤 130 期间从未使用过的鉴权向量密钥存储库中提供该鉴权向量密钥（即，完整性密钥 IK 和/或密钥 CK）。如果 CN 不再有未使用过的鉴权向量密钥，CN 接着可从鉴权中心（AUC）或 HLR 请求新的鉴权向量密钥。此外，CN 可从通信故障的原因确定 RNC 无法支持 MS 使用的 UIA 或 UEA。如果正是这样，CN 可能选择一个新的允许 UIA 和/或 UEA 并在安全模式指令中发送它到 RNC。

现在参考图 4，CN 执行鉴权进程 140 如下：这个鉴权步骤可包括从 AUC 接收一个查询和结果（步骤 142）。查询消息可包括在步骤 130 生成的安全参数，如果生成了新的安全参数的话。CN 发送该查询到 MS（步骤 150）。为响应该查询，MS 必须使用一个其所知晓的唯一标识符并将该标识符应用到一个算法以产生一个结果（步骤 160）。

MS 生成的查询结果从 MS 发送到 CN（步骤 170），CN 比较来自 MS 的结果与来自 AUC 的结果（步骤 180）。如果这些结果匹配，CN 借助“安全模式指令”消息发送一个确认到 RNC（步骤 190）。该“安全模式指令”消息包括在鉴权期间生成用于更新 RNC 的任何新安全参数以及可能一个新的 UIA 和/或 UEA。如果 MS 不被鉴权，即结果不匹配，CN 发送一个“鉴权拒绝”到 MS（步骤 200）。该鉴权故障借助对请求安全检查的响应指示给 RNC（步骤 190）。然而，由于 MS 不是有效的 MS，与有效用户相关的参数在 RNC 中不会被抹去。

执行完上述进程后，该系统可能尝试发生通信故障的进程。

本发明并不受仅提供作为例子的上述实施例的限制，而是可在所附权利要求书定义的保护范围内对本发明进行各种改进。

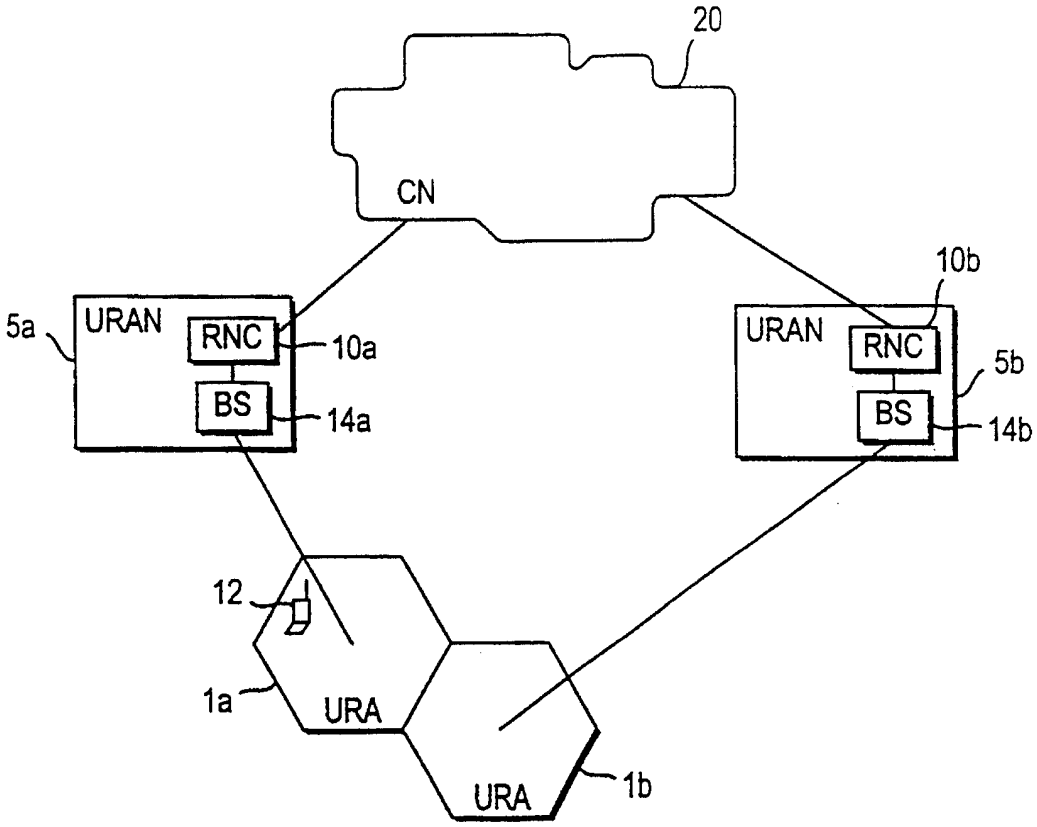

20
CN
10b
5a
URAN
RNC
10a
BS
14a
URAN
RNC
5b
BS
14b
12
1a
URA
URA
1b

图 1

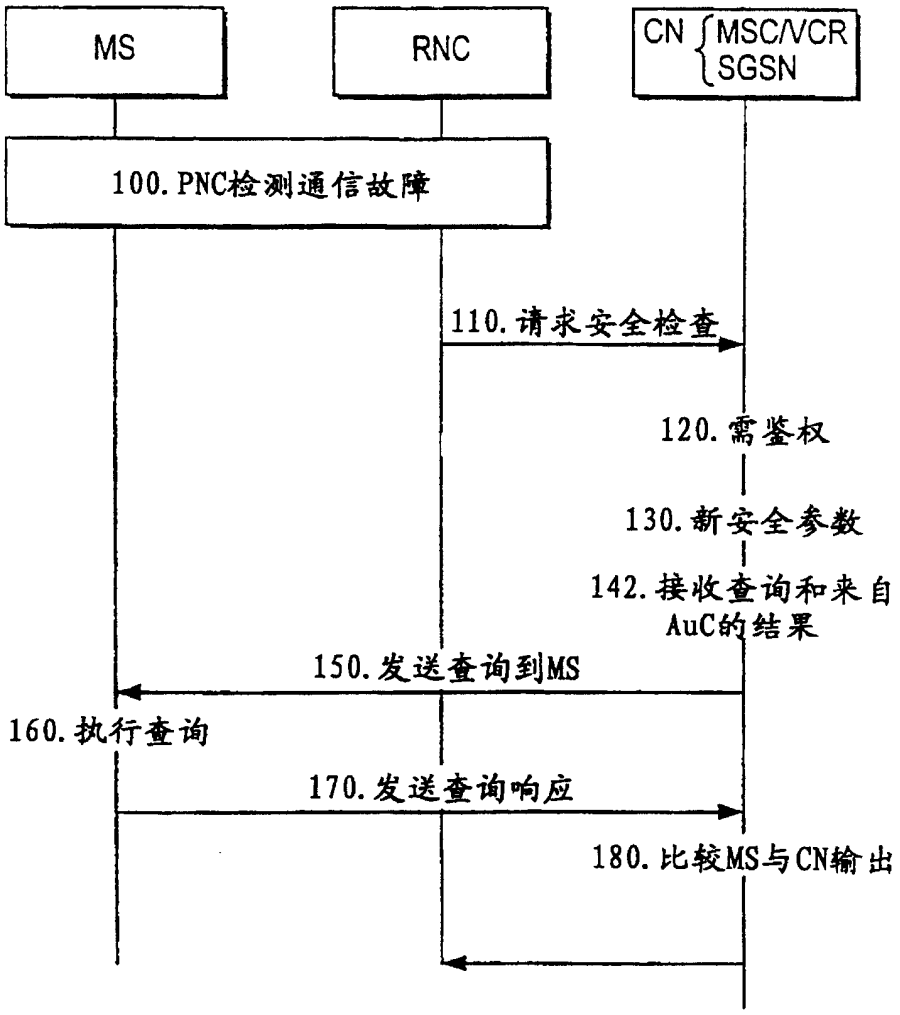

MS
RNC
CN
MSC/VCR
SGSN
100. PNC检测通信故障
110. 请求安全检查
120. 需鉴权
130. 新安全参数
142. 接收查询和来自AuC的结果
150. 发送查询到MS
160. 执行查询
170. 发送查询响应
180. 比较MS与CN输出

图 2

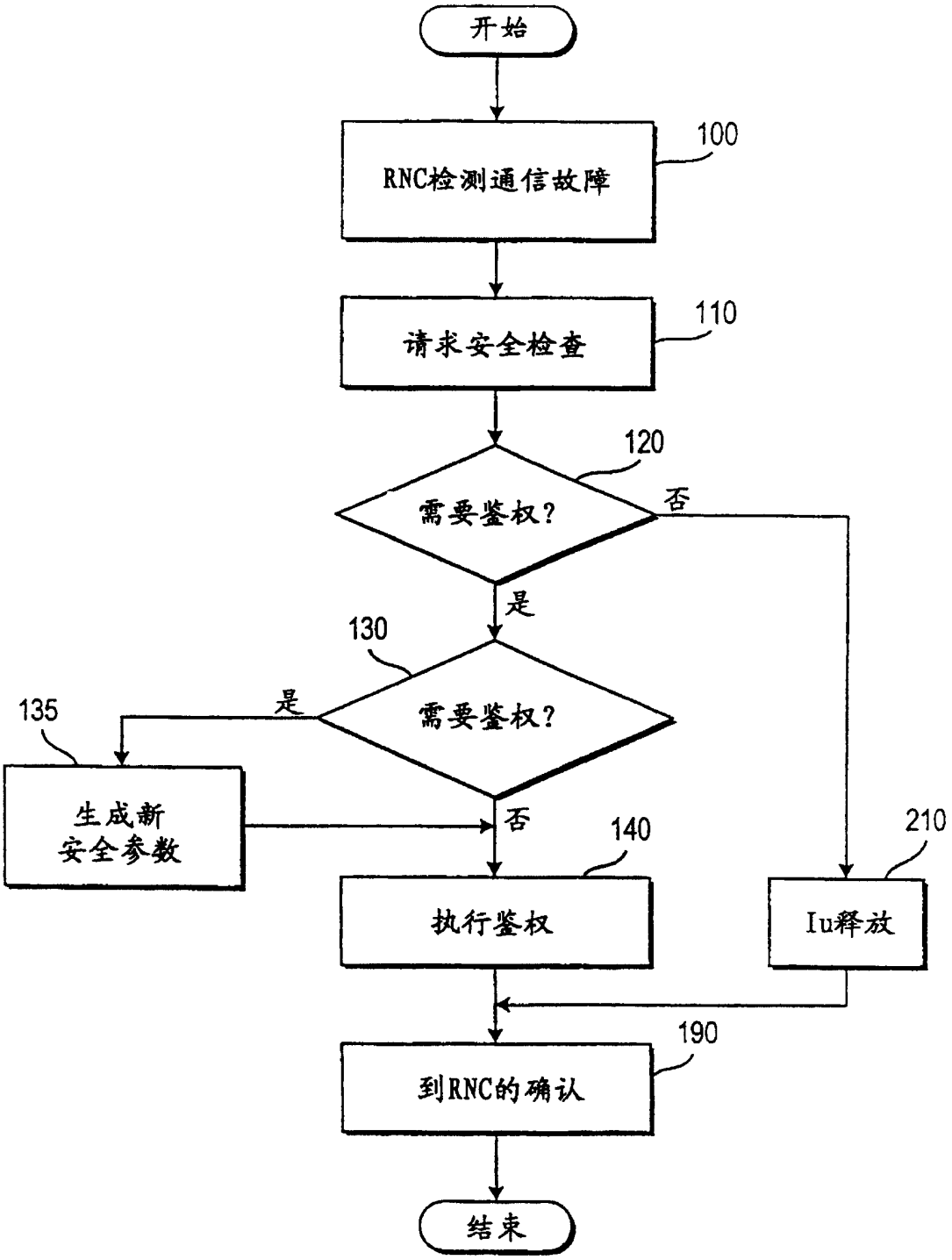

开始
RNC检测通信故障
100
请求安全检查
110
120
需要鉴权?
否
是
130
需要鉴权?
是
135
生成新
安全参数
否
140
执行鉴权
210
Iu释放
190
到RNC的确认
结束

图 3

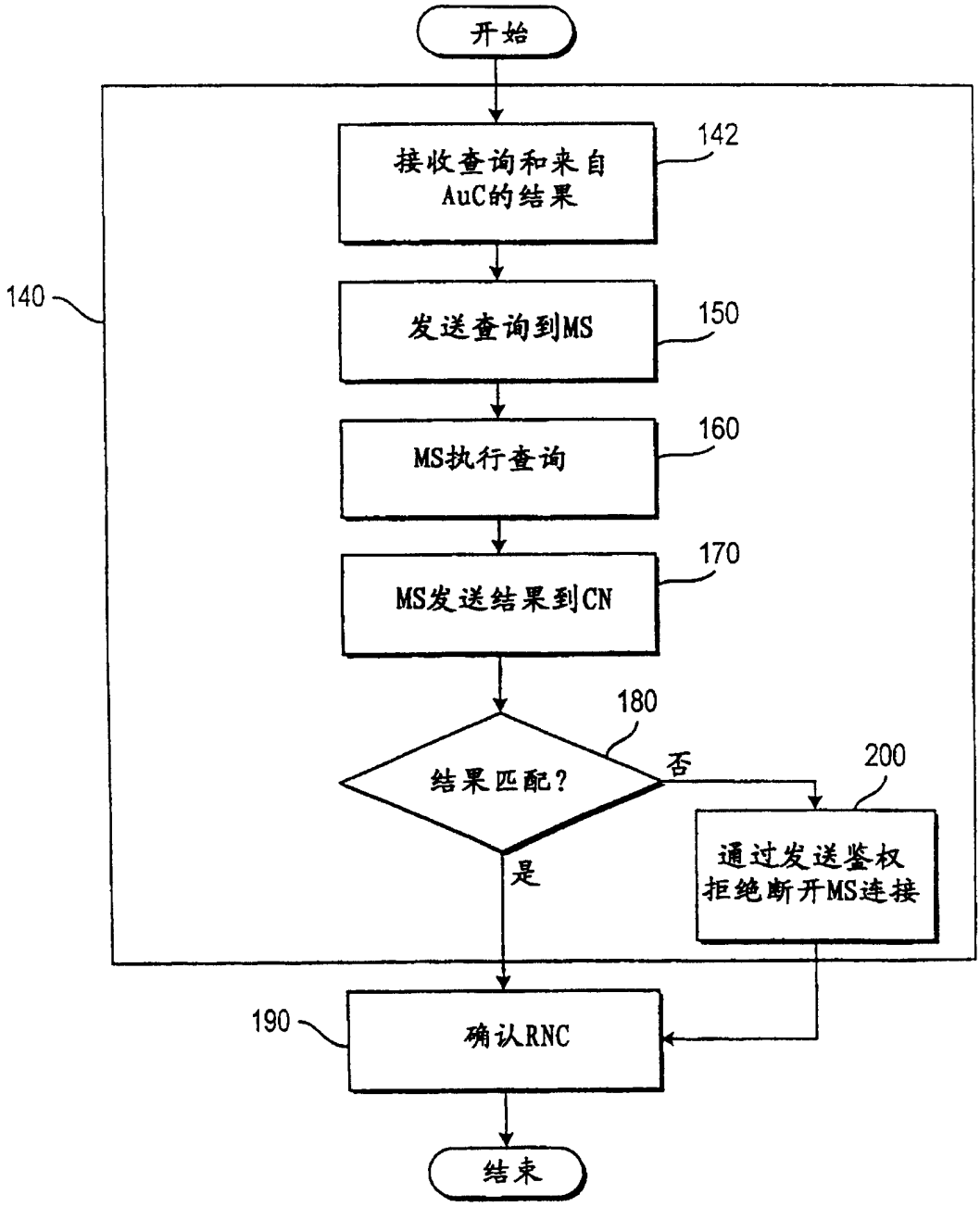

开始
接收查询和来自AuC的结果
142
140
发送查询到MS
150
MS执行查询
160
MS发送结果到CN
170
结果匹配?
180
否
200
通过发送鉴权拒绝断开MS连接
是
确认RNC
190
结束

图 4

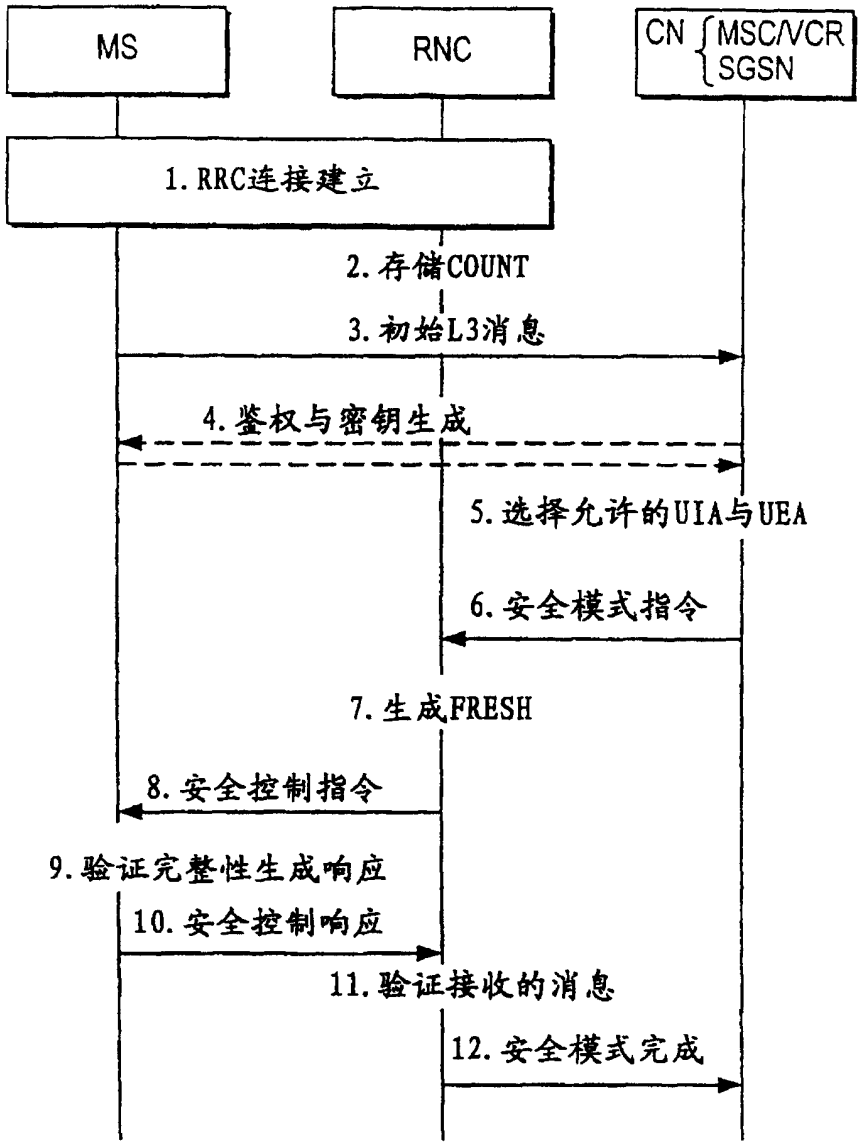

MS
RNC
CN
MSC/VCR
SGSN
1. RRC连接建立
2. 存储COUNT
3. 初始L3消息
4. 鉴权与密钥生成
5. 选择允许的UIA与UEA
6. 安全模式指令
7. 生成FRESH
8. 安全控制指令
9. 验证完整性生成响应
10. 安全控制响应
11. 验证接收的消息
12. 安全模式完成

图 5