(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 1973564 B
(45)授权公告日 2010.12.08

(21)申请号 200580019819.1
(22)申请日 2005.04.08
(30)优先权数据
04/04043 2004.04.16 FR
(85)PCT申请进入国家阶段日
2006.12.15
(86)PCT申请的申请数据
PCT/EP2005/051570 2005.04.08
(87)PCT申请的公布数据
WO2005/112497 FR 2005.11.24
(73)专利权人 塔莱斯公司
地址 法国耐伊市(赛纳河上)
(72)发明人 弗朗索瓦·德拉沃
多米尼克·厄尔吉耶
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 韩宏
(51)Int.Cl.
H04W 24/06(2009.01)

(56)对比文件
WO 99/12228 A2,1999.03.11, 全文.
EP 1051053 A2,2000.11.08, 全文.
CN 1359215 A,2002.07.17, 全文.

审查员 冯美玉

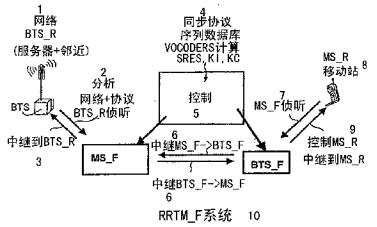
权利要求书 2 页 说明书 9 页 附图 1 页

(54)发明名称

用于控制和分析电话网络中的通信的方法

(57)摘要

本发明涉及一种控制和分析在移动终端和基站BTS间交换的蜂窝无线通信的方法和系统。本发明的特征在于,包括虚拟基站BTS_F和虚拟移动终端MS_F的虚拟移动电话网络RRTM_F被插入到真实网络RRTM_R中,所述虚拟网络负责在真实网络和真实移动电话间交换的消息的解码和透明且同步的中继,以及来自真实网络或者从虚拟网络的真实移动电话访问控制。



CN 1973564 B

1. 一种控制和分析真实移动终端和真实基站 BTS 间交换的蜂窝无线电通信的方法，其特征在于，包括虚拟基站 BTS_F 和虚拟移动终端 MS_F 的虚拟移动电话网络 RRTM_F 被插入到真实网络 RRTM_R 中，该虚拟移动电话网络保证该真实网络和真实移动终端间交换的消息的解码和透明且同步的中继，并且保证对来自该真实网络或者来自该虚拟移动电话网络的该真实移动终端的访问的控制。

2. 根据权利要求 1 所述的方法，其特征在于，所述交换的消息为网络访问阶段中的广播消息和专用信令消息，或者用于通信已建立时的业务。

3. 根据权利要求 1 所述的方法，其特征在于，其包括至少以下步骤：

o 所述虚拟移动终端进行所述真实网络的计划记录，并且确定每个小区的特性，

o 所述虚拟移动终端结合虚拟信标信号对频率和时间参数的选择进行优化，

o 所述虚拟基站在该选择的频率上以所选择的时间参数传输所述虚拟信标信号，所述虚拟信标信号临时和通常由所述真实网络发射的信号叠加，并且由所述真实基站的所述真实移动终端作为真实传输解释。

4. 根据权利要求 3 所述的方法，其特征在于，在所述真实网络的所述计划记录之后，所述虚拟移动终端 MS_F 发射选择性的干扰信号，其适用于阻止存在的真实移动终端使用某些频率、某些时间间隔或者某些时隙，并且用于保持这些真实移动终端同所述虚拟基站的连接。

5. 根据权利要求 4 所述的方法，其特征在于，在所述真实移动终端 MS_R 连接到所述虚拟基站 BTS_F 后，所述虚拟基站至少执行以下步骤：

o 以透明且同步的方式解码、解释并中继在所述真实基站和所述真实移动终端之间传输的消息，并且：

o 鉴权所述真实移动终端，

o 通过使用通话信道和专用信道，执行合适的程序，

o 引导所述真实移动终端根据合适的模式和重复率提供其参数：IMSI，IMEI，TMSI，SRES，

o 随后引导所述虚拟移动电话网络通过本发明特定的处理获得所述真实移动终端 MS_R 的密钥 Ki，

o 引导所述虚拟移动电话网络在上述处理之后获得用于以后的会话的所述真实移动终端 MS_R 的密钥 Kc，

o 引导所述真实移动终端在其存储器或者其 SIM 卡的存储器内登记由所述虚拟移动电话网络指示的参数和应用程序，

o 引导所述真实移动终端在由所述虚拟移动电话网络所指示的频率上发射信令、访问和业务信号。

6. 根据权利要求 5 所述的方法，其特征在于，所述虚拟移动电话网络拒绝所述真实移动终端 MS_R，其是这样实现的：通过强制执行小区转换或者切换或者重新分配到除 BTS_R 之外的所述真实网络的真实小区上的过程，或者通过故意劣化该通信以使其中断，或者通过强制截取协议。

7. 根据权利要求 1 至 6 所述的方法，其特征在于使用移动电话蜂窝数字公共网。

8. 一种用于控制和分析在真实移动终端和真实基站 BTS 之间交换的蜂窝无线电通信

的系统，其包括虚拟移动电话网络 RRTM_F，该虚拟移动电话网络 RRTM_F 包括虚拟基站 BTS_F 和虚拟移动终端 MS_F，该虚拟移动电话网络被插入到真实网络 RRTM_R 中，其特征在于，该虚拟移动电话网络适用于保证该真实网络和真实移动终端间交换的消息的解码和透明且同步的中继，并且保证对来自该真实网络或者来自该虚拟移动电话网络的真实移动终端的访问的控制。

用于控制和分析电话网络中的通信的方法

[0001] 本发明具体涉及，例如，蜂窝数字公共网中用于恢复并解释通信框架内在一个或多个移动电话 (MS) 和基站 (BTS) 之间交换的信息的方法和装置。

[0002] 例如，其位于，在基站 (BTS) 和移动终端 (MS) 间通信中所交换的信令消息和业务消息内容的协议记录、控制和产生的框架中。

[0003] 本发明还涉及本领域的技术人员所熟悉的分析设备中的测量和分析方法这一领域。这些分析设备是，例如，用于移动终端的协议测试器 (TPTM) 和用于基站的协议测试器 (TPBS) 中的测试移动电话 (MT)。

[0004] 当前，用于分析第二代蜂窝无线电网络中的移动终端所进行的通信以及产生消息内容的方案是基于虚拟基站和测试移动电话间的关联的，虚拟基站和测试移动电话同时作为用于真实网络的计划记录的测量系统，和虚拟基站和真实网络间的中继。专利 EP1 051 053B1 描述了这种方法的例子。

[0005] 这种系统的限制主要为以下几点：

[0006] - 就测量能力而言，测试移动电话 MT 在得到操作整个系统所必需的网络总体情况方面经常存在实际困难，因此，其被迫处于通信待机模式。这样，系统的范围及其整体可靠性大大降低。

[0007] - 就测试移动电话 MT 的能力而言，在真实网络和基站 BTS_F 间的中继系统中，不能精确控制由测试移动电话发送和接收的消息间的同步，也不能精确控制 BTS_F 发送时刻间的同步。

[0008] - 测试移动电话通常需要使用 SMI 卡（用户标识模块）来在网络中进行注册，以对网络进行测量，并且以随后和真实网络谈判用于建立会话密钥的协议步骤，以保证由 BTS_F 解码的消息中继到真实网络，然后网络就看不到真实移动电话 MS_R 了。

[0009] - 寻求绕过使用 SIM 卡的现存系统及其变型必须保证真实移动终端的特定数据，以在网络注册方法中用自身替代所述终端。

[0010] 图 1 简要示出在传统系统中所实现的步骤。测试移动电话使用其 SIM 卡与网络建立通信。

[0011] 这三个主要弱点引起许多不足之处，如：

[0012] - 当真实移动电话的 SIM 卡的特定数据未知时，真实移动电话 MS_R 和真实网络 BTS_R 的计费会出现异常（经中继的呼出通信被归属于和测试移动电话相关的 SIM 卡的用户），

[0013] - 从网络联系真实移动终端 MS_R 实际上不可能（呼入通话不能完成，因为测试移动电话 MT 不能合适地保证中继），

[0014] - 各种操作异常，如真实移动电话 MS_R 查询其消息时，查寻特定电话号码时，等等，

[0015] - 范围和可靠性的限制等。

[0016] 本发明的要旨具体在于，以同时和同步的方式，利用已经用于骨干发射机或者蜂窝无线终端的测量或者质量控制应用的高性能设备，该设备配备有发射系统、接收系统并

且实现本发明的特定过程。

[0017] 本发明涉及移动终端和基站 BTS 间交换的蜂窝无线通信的控制和分析方法，其特征在于，包括虚拟基站 BTS_F 和虚拟移动终端 MS_F 的虚拟移动电话网络 RRTM_F 被插入到真实移动电话网络 RRTM_R 中，虚拟网络保证真实网络和真实移动电话间交换的消息的解码和透明且同步的中继，并且控制从真实网络或者从虚拟网络对真实移动电话的访问。

[0018] 所交换的消息为，例如，网络访问阶段中的广播消息和专用信令，或者通信已建立时的业务（电话、数据、短消息、DTMF）。

[0019] 该方法可以包括至少以下步骤：

[0020] ○虚拟移动电话进行网络计划记录，并且确定网络的每个小区的特性，

[0021] ○虚拟移动电话结合虚拟信标信号对频率和时间参数的选择进行优化，

[0022] ○虚拟基站在该选择的频率上以所选择的时间参数发射虚拟信标信号，该虚拟信标信号临时和通常由网络发射的信号叠加，并且由真实基站的移动电话作为真实发射解释。

[0023] 在网络的计划记录之后，虚拟移动电话 MS_F 进行发射，例如发射选择性的干扰信号，用于阻止存在的移动终端使用某些频率、某些时间间隔或者某些时隙，并且用于保持它们同虚拟基站的连接 (goingon-hook to)。

[0024] 在移动电话 MS_R 连接到虚拟基站 BTS_F 后，虚拟基站至少执行以下步骤：

[0025] ○以透明且同步的方式解码、解释并中继在真实基站和真实移动电话之间传输的消息，而不考虑呼入和呼出通话的来源，

[0026] ○鉴权移动终端，

[0027] ○通过使用通话信道和专用信道，执行合适的过程，

[0028] ○引导移动电话根据合适的模式和重复率提供其参数：IMSI，IMEI，TMSI，SRES，

[0029] ○随后引导虚拟网络通过本发明特定的处理获得移动电话 MS_R 的密钥 Ki，

[0030] ○引导虚拟网络在处理之后获得用于以后的会话的移动电话 MS_R 的密钥 Kc，

[0031] ○引导移动电话在其存储器或者其 SIM 卡的存储器内注册由移动网络指示的参数和应用程序，

[0032] ○引导移动电话在由虚拟网络所指示的频率上发射信令、访问和业务信号。

[0033] 该方法用于，例如，移动电话蜂窝数字公共网中。

[0034] 本发明还涉及用于控制和分析在移动终端和基站 BTS 间交换的蜂窝无线电通信的系统，其包括虚拟移动电话网络 RRTM_F，该虚拟移动电话网络 RRTM_F 包括虚拟基站 BTS_F 和虚拟移动终端 MS_F，该虚拟网络被插入到真实移动电话网络 RRTM_R 中，其特征在于，虚拟网络用于保证真实网络和真实移动电话间交换的消息的解码和透明且同步的中继，并且控制从真实网络或者从虚拟网络对真实移动电话的访问。

[0035] 本发明具体具有以下有益方面：

[0036] ○其实现虚拟移动构成部分 MS_F 和虚拟基站 BTS_F 在将消息从真实网络向真实移动电话进行透明中继的阶段的交互和同步的精确控制，并且实现对虚拟网络 RRTM_F 在真实网络 RRTM_R 上的同步的精确控制。

[0037] ○其使发射信号 BCCH_F 和由真实基站 BTS_R 发射的信号之间的精确同步成为可能，因此限制了真实网络中的缺点的影响。

[0038] ○其使避免虚拟网络的组成部分在真实网络中的注册成为可能，即，避免使用 SIM 卡或者关于真实移动终端的特定数据的信息。

[0039] ○使用这样的方法同时增加了对环境中的真实移动终端 MS_R 的动作的范围、可靠性和完整性。

[0040] ○范围和灵敏度是最优的。其使用，例如，基于标准的推荐的处理来接收（进行均衡解调，即已知的“数据辅助”训练序列、解码等）。因此，硬件配置和处理是最优的，而传统系统的硬件配置和处理通常非常差，尤其是解调 / 均衡部分。

[0041] ○其可以和天线处理、适应性滤波、信号的接收处理、均衡，或者和干扰技术结合，如在专利申请 FR2 766 320 和 FR2 829241 中所描述的。

[0042] 本发明的其他特点和有益方面将通过以下说明而更为显而易见，以下说明完全为非限定性的，并且带有附图，其中

[0043] 图 1 是传统的通信系统；

[0044] 图 2 是根据本发明的系统的示例性架构。

[0045] 为了更好地阐述本发明的原理，下面的例子完全为非限定性的，其说明在移动电话蜂窝数字公共网中，用于一个或多个移动电话 (MS) 和基站 BTS 间的通信系统。

[0046] 图 2 示出的示例性架构包括真实网络 BTS_R、移动电话 MS_R、包括如虚拟基站 BTS_F 和虚拟移动电话 MS_F 的虚拟移动电话网络 RRTM_F。该虚拟电话网络具有实现根据本发明的方法的特定硬件和过程。其为本网络所包括的真实网络 RRTM_R 和移动终端 MS_R 所覆盖。该虚拟电话网络还包括控制设备，其功能在下文中详细阐述。

[0047] 虚拟移动电话 MS_F 的具体功能包括

[0048] ●扫描频率，

[0049] ●对网络的不同小区的信令进行解码和解释，

[0050] ●记录小区的计划，

[0051] 其具体确定周围的每个小区的一个或多个小区特性，例如：

[0052] ●接收的电平和 C/(I+N) 比，

[0053] ●小区的 BSIC 色彩码（基站的标识码或者基站标识码），LAC 码（局域码）、和 MCC/MNC 码（移动国家码和移动网络），

[0054] ●分配给小区的频率计划或者小区的 CA 列表（小区分配列表），

[0055] ●邻近小区的频率列表，由“BA 列表”表示，

[0056] ●小区重新选择标准（表示为 C1、C2 等）。

[0057] 对于周围的真实小区，而且作为所记录的和各个周围小区相关的特性，虚拟移动电话 MS_F 优化相关的时间参数，例如：

[0058] ●属于所选基站 BTS_R 的 BA 列表的频率 Fsel 的选择，

[0059] ●虚拟信标信号 BCCH_F 的时间特性和同步特性以及发射时间的选择，

[0060] ●为了优化链路规划而对其进行干扰的频率的选择。

[0061] 虚拟基站

[0062] 虚拟基站 BTS_F 在选择的频率 Fsel 以所选择和控制的时间特性发射虚拟信标信号 BCCH_F，该虚拟信标信号 BCCH_F：

[0063] ●在频率和时间上都和通常由网络发射的信号叠加，

[0064] ●由真实小区 BTS_R 的真实移动电话 MS_R 解释为网络的真实发射。

[0065] 该虚拟信标信号包括根据所需的用于以下内容的动作的各种信令数据：

[0066] ●强制实现重新分配到虚拟基站 BTS_F 的过程，因此真实电话 MS_R 在与其进行通话时被引导发送其参数（TMSI：临时移动电话用户标识，IMSI：国际移动电话用户标识，IMEI：国际移动设备标识），

[0067] ●禁止访问网络，

[0068] ●禁止真实小区 BTS_R 的终端对虚拟小区 BTS_F 的作用，

[0069] ●拒绝最初禁止连接到真实网络的移动终端。

[0070] 控制设备（包括空中接口的层 1、2、3）具体适于：

[0071] -用于精确分析真实网络环境 RRTM_R，以检测该环境中出现的小区及其邻近小区，以记录重新选择各个小区的标准，这些以完全被动的模式进行，

[0072] -用于解码和解释来自真实网络 RRTM_R 的信令和业务消息，

[0073] -用于以同步方式将这些消息中继到移动终端，这些消息经过修改或者未经修改，

[0074] -主动地或者根据由真实网络发起的过程，或者在虚拟网络的强制过程中，对来自移动电话 MS_R 的信令消息和业务消息进行解码和解释，

[0075] -用于以同步方式将这些消息中继到真实网络 RRTM_R，这些消息经过修改或者未经修改，

[0076] -对于真实网络 RRTM_R 的所选小区 BTS_R，发射特性（频率、发射开始时刻、同步、信令消息的内容、电平等）已确定的信标信号 BCCH_F，使得所选小区 BTS_R 的移动终端 MS_R 被引导同该信标 BCCH_F 连接，因此其由虚拟网络 RRTM_F 的基站 BTS_F 控制，

[0077] -一旦信标信号 BCCH_F 已发射后，或者在发射该信号之前，或者在发射该信号的同时，用于管理选择性的干扰信号，使禁止所选小区 BTS_R 的真实移动电话 MS_F 同它可访问的真实网络的其他小区建立任何连接，因此更有利于将 MS_R 继续连接到虚拟网络的 BTS_F，

[0078] -一旦移动电话 MS_F 连接到 BTS_F，用于管理由标准提供的网络过程的全部状态，而且其中真实移动电话 MS_R 和真实基站 BTS_R 易于被找到，

[0079] -用于强制实现由标准提供的任何过程，以管理移动电话的移动性或者通话，如呼叫、重新分配、小区转移或者切换、鉴权、识别、特殊会话的建立，应答呼入或者呼出通话等，

[0080] -用于通过由标准授权的过程来将数据或者应用程序下载到真实移动电话 MS_R，例如，下载 RAM“远程小程序管理”或者 RFM“远程文件管理”功能，其分别允许将“SIM 应用程序工具包”和多媒体数据下载到 SIM 卡或者终端上，

[0081] -用于根据前一阶段解码的数据产生具体信息；

[0082] -用于根据前一阶段解码的数据产生真实移动电话 MS_R 的特定信息。

[0083] 该方法实现，例如下面描述的步骤和阶段。

[0084] 前期阶段

[0085] 虚拟移动电话 MS_F 执行网络的计划记录。

[0086] 一个或多个移动电话连接的阶段

[0087] 然后，移动电话可以发射选择性的干扰信号，以便：

[0088] -禁止真实网络 RRTM_R 中的移动终端使用某些频率 F_{nonaut} 或者某些时隙；

[0089] - 更有利于移动终端连接到虚拟基站 BTS_F。

[0090] 这具体使得通过谨慎地选择信号 BCCH_F 和选择性的干扰信号的频率、发射时刻和时间特性以及同步特性，来处理若干个邻近小区 (BTS_R1、BTS_R2、…、BTS_RN) 成为可能。

[0091] 移动电话连接后的阶段

[0092] 真实移动电话 MS_R 连接到虚拟基站 BTS_F 后，该虚拟基站 BTS_F：

[0093] - 对由真实基站 BTS_R 发射向真实移动电话 MS_R 的消息进行解码、解释和透明且同步；

[0094] - 对由真实移动电话 MS_R 发射向真实基站 BTS_R 的消息进行解码、解释和透明且同步；

[0095] - 然后，虚拟基站进行各种来自虚拟网络 RRTM_F 的本发明实现的特定过程和处理操作，部分或全部过程是网络的正常操作，如：

[0096] ○终端的鉴权、标识和 / 或注册；

[0097] ○将功能或者参数下载到终端；

[0098] ○终端的通话等。

[0099] 使用通话信道 (PCH) 和专用信道 (DCCH)，虚拟基站进行各种本领域的技术人员熟知的各种过程：

[0100] ○引导真实移动电话将其参数 IMSI、IMEI、TMSI、SRES 以适当的模式和重复率发送给虚拟基站；

[0101] ○随后引导虚拟网络利用本发明的特定处理获得移动电话 MS_R 的鉴权密钥 Ki；

[0102] ○在合适的处理后，引导虚拟网络获得由真实移动电话 MS_R 的系统为随后的会话所创建的密钥 Kc；

[0103] ○引导真实移动电话在其存储器内或 SIM 卡内注册由虚拟网络指示的参数和应用程序等。

[0104] 通过将消息从移动电话中继到网络，并且从网络中继到移动电话，虚拟网络对其内容进行解码。

[0105] 该方法随后可以包括以下步骤：

[0106] 在连接并且执行前述步骤后，虚拟网络 BTS_F 拒绝真实移动电话 MS_R，例如，

[0107] - 通过强制执行小区转换或者切换或者重新分配到非 BTS_R 的网络的真实小区上的过程；

[0108] - 或者通过故意降低该通信以使其中断；

[0109] - 或者通过强制截取协议。

[0110] 真实移动电话 MS_R 的专用信令消息以及呼出和呼入业务消息的解码和解释

[0111] 要解码和解释真实移动电话 MS_R 的专用信令消息以及呼出和呼入业务消息，虚拟移动电话 MS_F 和虚拟小区 BTS_F 被设计成同步方式，这样真实移动电话 MS_R 在虚拟小区 BTS_F 进行注册，并且：

[0112] ○当接收 A5/0 事务的网络中的移动电话 MS_R 进行呼出通话时，通话到达虚拟基站 BTS_F，协议消息被 BTS_F 解码并解释，而且发送到虚拟移动电话 MS_F，虚拟移动电话 MS_F 对协议消息稍加修改并将其中继到真实网络，进而解码和解释真实网络的响应，将其中继

到虚拟小区 BTS_F，虚拟小区 BTS_F 将其中继到真实移动电话；为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0113] ○当接收 A5/0 事务的网络中的移动电话 MS_R 进行呼入通话时，通话到达虚拟移动电话 MS_F，通话消息被 MS_F 解码并解释，而且发送到虚拟 BTS BTS_F，虚拟 BTS BTS_F 对通话消息稍加修改并将其中继到真实移动电话 MS_R，进而解码和解释真实移动电话的响应，将其中继到虚拟移动电话 MS_F，虚拟移动电话 MS_F 对其稍加修改并将其中继到真实网络；为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0114] ○在不接收 A5/0 事务的网络中的移动电话 MS_R 以密钥 Ki 进行呼出通话时，密钥 Ki 已知或者之前通过实现本发明获得，通话到达虚拟基站 BTS_F，协议消息被 BTS_F 解码并解释，而且发送到虚拟移动电话 MS_F，虚拟移动电话 MS_F 将协议消息中继到真实网络 BTS_R，同时为此目的计算会话密钥 Kc，进而解码和解释真实网络的响应，将其中继到虚拟小区 BTS_F，虚拟小区 BTS_F 使用所计算的会话密钥将其中继到真实网络，；为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0115] ○在不接收 A5/0 事务的网络中的移动电话 MS_R 以密钥 Ki 进行呼入通话时，密钥 Ki 已知或者之前通过实现本发明获得，通话到达虚拟移动电话 MS_F，通话消息被 MS_F 解码并解释，而且发送到虚拟基站 BTS_F，虚拟基站 BTS_F 将协议消息中继到真实移动电话 MS_R，同时为此目的计算会话密钥 Kc，进而解码和解释 MS_R 的响应，将其中继到虚拟移动电话 MS_F，虚拟移动电话 MS_F 使用所计算的会话密钥将其中继到真实网络；为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0116] ○在不接收 A5/0 事务的网络中的移动电话 MS_R 以未知的密钥 Ki 进行呼出通话时，通话到达虚拟基站 BTS_F，

[0117] ●在建立会话密钥之前，协议消息被 BTS_F 解码并解释，而且发送到虚拟移动电话 MS_F，虚拟移动电话 MS_F 将协议消息中继到真实网络 BTS_R，进而解码和解释真实网络的响应，将其中继到虚拟小区 BTS_F，虚拟小区 BTS_F 将其中继到真实移动电话 MS_R；

[0118] 为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0119] ●为了建立虚拟网络和真实移动电话 MS_R 之间的会话密钥，虚拟 BTS BTS_F 向移动电话指示 A5/0 通话模式，

[0120] ●为了继续虚拟网络和真实网络 BTS_R 之间的中继，虚拟移动电话 MS_F 与真实网络建立普通的通信，并且以同步方式在 BTS_F 和 MS_R 之间建立链路，并且使用 SIM 卡实现这些；

[0121] ○在不接收 A5/0 事务的网络中的移动电话 MS_R 以未知的密钥 Ki 进行呼入通话时，通话到达虚拟基站 MS_F，

[0122] ●在建立会话密钥之前，协议消息被 MS_F 解码并解释，而且发送到虚拟 BTS BTS_F，虚拟 BTS BTS_F 将协议消息中继到真实移动电话 MS_R，进而解码和解释真实移动电话 MS_R 的响应，将其中继到虚拟移动电话 MS_F，虚拟移动电话 MS_F 将其中继到真实网络 BTS_R，；为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡；

[0123] ●为了建立虚拟网络和真实移动电话MS_R之间的会话密钥，虚拟BTS BTS_F向移动电话指示A5/0通话模式，

[0124] ●为了继续虚拟网络和真实网络BTS_R之间的中继，虚拟移动电话MS_F与真实网络建立普通的通信，并且以同步方式在BTS_F和MS_R之间建立链路，并且使用SIM卡实现这些；

[0125] ○在接收A5/2事务的网络中的移动电话MS_R以未知的密钥Ki进行呼出通话时，通话到达虚拟基站BTS_F，在网络访问协议中由MS_R发送的第一消息被BTS_F解码并解释，而且发送到虚拟移动电话MS_F，虚拟移动电话MS_F对其稍加修改并将其中继到BTS_R，在网络访问协议中由BTS_R发送的第一消息被MS_F解码并解释，而且发送到BTS_F，BTS_F对其稍加修改并将其中继到MS_R。BTS_F与MS_R建立A5/2会话，并且MS_F与BTS_R建立A5/2会话，然后虚拟网络的控制设备实现任何现有的方法，以使在足够短的时间内获得会话密钥Kc成为可能。BTS_F解码并解释MS_R的消息，将其中继到MS_F，MS_F再将其中继到BTS_R。MS_F解码并解释BTS_R的消息，将其中继到BTS_F，BTS_F再将其中继到MS_R。为了实现这个，虚拟移动电话MS_F不需建立任何其自身与真实网络的连接，也不需要SIM卡；

[0126] ○在接收A5/2事务的网络中的移动电话MS_R以未知的密钥Ki进行呼入通话时，通话到达虚拟移动电话MS_F，在网络访问协议中由BTS_R发送的第一消息被MS_F解码并解释，而且发送到BTS_F，BTS_F对其稍加修改并将其中继到MS_R，在网络访问协议中由MS_R发送的第一消息被BTS_F解码并解释，而且发送到MS_F，MS_F对其稍加修改并将其中继到BTS_R。MS_F与BTS_R建立A5/2会话，并且BTS_F与MS_R建立A5/2会话，然后虚拟网络的控制设备实现任何现有的方法，以使在足够短的时间内获得会话密钥Kc成为可能。MS_F解码并解释BTS_R的消息，将其中继到BTS_F，BTS_F再将其中继到MS_R；BTS_F解码并解释MS_R的消息，将其中继到MS_F，MS_F再将其中继到BTS_R。为了实现这个，虚拟移动电话MS_F不需建立任何其自身与真实网络的连接，也不需要SIM卡；

[0127] ○在只接收A5/1事务的网络中的移动电话MS_R以未知的密钥Ki进行呼出通话时，通话到达虚拟基站BTS_F，在网络访问协议中由MS_R发射的第一消息被BTS_F解码并解释，而且发送到虚拟移动电话MS_F，虚拟移动电话MS_F对其稍加修改并将其中继到BTS_R，在网络访问协议中由BTS_R发送的第一消息被MS_F解码并解释，而且发送到BTS_F，BTS_F对其稍加修改并将其中继到MS_R。BTS_F与MS_R建立第一A5/2会话，然后虚拟网络的控制设备实现任何现有的方法，以使在足够短的时间内获得会话密钥Kc成为可能。一旦获得密钥Kc，BTS_F建立新的A5/1会话，同时MS_F与BTS_R建立A5/1会话。MS_F解码并解释BTS_R的消息，将其中继到BTS_F，BTS_F再将其中继到MS_R；BTS_F解码并解释MS_R的消息，将其中继到MS_F，MS_F再将其中继到BTS_R。为了实现这个，虚拟移动电话MS_F不需建立任何其自身与真实网络的连接，也不需要SIM卡；

[0128] ○在只接收A5/1事务的网络中的移动电话MS_R以未知的密钥Ki进行呼入通话时，通话到达虚拟移动电话MS_F，在网络访问协议中由BTS_R发送的第一消息被MS_F解码并解释，而且发送到BTS_F，BTS_F对其稍加修改并将其中继到MS_R，在网络访问协议中由MS_R发射的第一消息被BTS_F解码并解释，而且发送到MS_F，MS_F对其稍加修改并将其中继到BTS_R。BTS_F与MS_R建立第一A5/2会话，然后虚拟网络的控制设备实现任何现有的

方法，以使在足够短的时间内获得会话密钥 Kc 成为可能。一旦获得密钥 Kc，BTS_F 建立新的 A5/1 会话，同时 MS_F 与 BTS_R 建立 A5/1 会话。BTS_F 解码并解释 MS_R 的消息，将其中继到 MS_F，MS_F 再将其中继到 BTS_R；MS_F 解码并解释 BTS_R 的消息，将其中继到 BTS_F，BTS_F 再将其中继到 MS_R。为了实现这个，虚拟移动电话 MS_F 不需建立任何其自身与真实网络的连接，也不需要 SIM 卡。

[0129] 使用特定的处理和天线来进行上述动作，具体地：

[0130] ●接收、解调和解码信号，

[0131] ●记录消息的内容，

[0132] ●确定到达的方向和 BTS_R 以及 MS_R 的距离，进而确定它们的位置。

[0133] 虚拟网络 RRTM_F 的虚拟移动电话 MS_F 和虚拟基站 BTS_F 使用，例如，特定的天线和适应性天线处理，来发射和接收并且解调。

[0134] 处理为，例如：

[0135] ○特别进行性能改进，

[0136] ○形成通过引用专利 FR 2 766 320、FR 99 16775、FR 2 829 241、FR 01/12976 而提交的方法的主题，

[0137] ○引导虚拟网络对远离其被分配的小区进行操作，

[0138] ○允许虚拟网络确定到达方向并定位 BTS_F 和 MS_R。

[0139] 通过非限定性的例子，本发明使在移动终端 MS_R 上进行过程及产生下述信息成为可能（下面的列举是非限定性的）：

[0140] -拒绝访问网络的移动电话 MS_R，

[0141] -禁止移动电话对小区、网络等的访问，

[0142] -移动终端 MS_R 的标识参数 (IMSI、IMEI、当前 TMSI)，

[0143] -移动终端 MS_R 的鉴权参数 (SRES)，

[0144] -和移动终端 MS_R 的密钥 Ki 相关的信息，及和随后的会话的密钥 Kc 相关的信息，

[0145] -在协议的每个阶段的可能中断时，重新分配移动终端 MS_R，

[0146] -在协议的每个阶段的可能中断时，呼叫移动终端 MS_R，

[0147] -向移动终端 MS_R 分配在 SIM 卡的存储器中注册的参数，

[0148] -将应用程序下载到移动终端 MS_R，

[0149] -下载在移动终端 MS_R 的 SIM 卡的存储器中或者移动终端 MS_R 的存储器中注册的参数，-

[0150] -中继 MS_R 发起的向 BTS_R 的通话尝试（呼出通话），直到建立通信，强制向用户指示忙碌通话的具体过程（消息或者网络不可用等），

[0151] -中继 BTS_R 发起的向 MS_R 的通话尝试（呼入通话），直到建立通信，

[0152] -移动终端 MS_R 的呼入和呼出通信的内容（语音、数据、SMS、DTMF 等），等。

[0153] 根据本发明的方法具体产生以下改进，所给出的例子近作为解释而非限定，例如：

[0154] ●避免虚拟网络的组成部分在真实网络中的实际注册，也就是说，避免使用 SIM 卡（用户标识模块）或者关于真实移动终端的特定数据的信息，

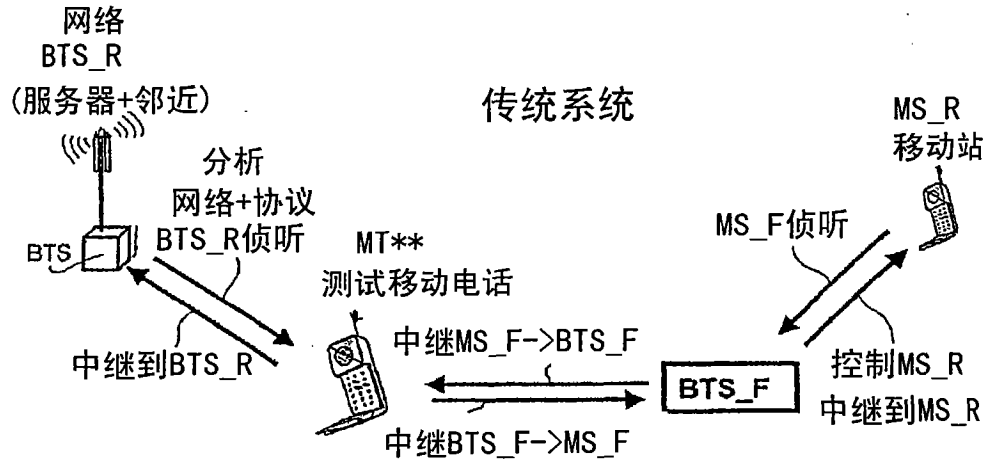
[0155] ●在远程小区对终端的控制以及控制每个终端，

[0156] ●对从网络到终端的通话的检测和解释，

[0157] ●呼入通信的中继，

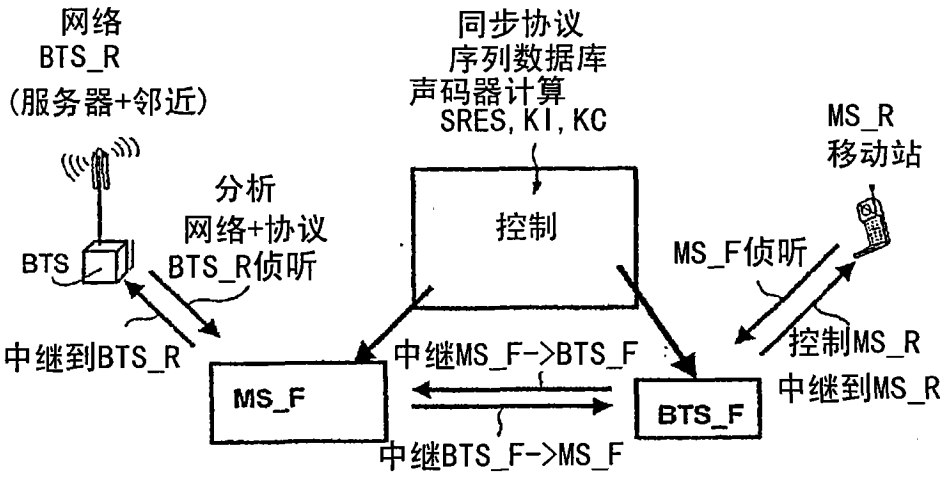
[0158] ●和呼入通信相关的各种信令和业务消息的解码和解释，

[0159] ●将数据或者应用程序下载到终端上。



**测试移动电话使用其SIM卡建立和网络的通信
=>通信非直接中继
=>MS_R自网络不可见

图1



RRTM_F系统

图2