[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04L 29/06

[12] 发明专利说明书

专利号 ZL 01813647.8

[45] 授权公告日 2005 年 8 月 10 日

[11] 授权公告号 CN 1214561C

[22] 申请日 2001.7.31 [21] 申请号 01813647.8
[30] 优先权
[32] 2000. 8. 1 [33] FI [31] 20001734
[86] 国际申请 PCT/FI2001/000689 2001.7.31
[87] 国际公布 WO2002/011362 英 2002.2.7
[85] 进入国家阶段日期 2003.1.30
[71] 专利权人 诺基亚有限公司
地址 芬兰埃斯波
[72] 发明人 V·尼米 K·尼梅莱 S·哈米蒂 G·塞比尔
审查员 李 明

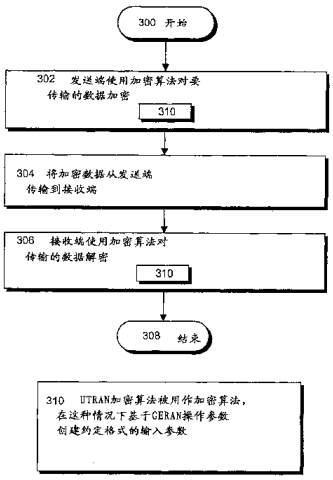
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 罗 朋

权利要求书 6 页 说明书 15 页 附图 7 页

[54] 发明名称 数据传输方法、用户设备和 GPRS/EDGE 无线接入网

[57] 摘要

本发明涉及用于在移动系统的 GPRS/EDGE 无线接入网与用户设备之间传输数据的一种方法，并涉及使用该方法的用户设备，以及涉及 GERAN。在该方法中，(302)发送端用加密算法对要传输的数据加密，(304)加密数据从发送端传输到接收端，以及(306)接收端用加密算法对该传输的数据解密。使用的加密算法是采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法，在这种情况下基于 GPRS/EDGE 无线接入网 GERAN 的操作参数创建加密算法所要求的约定格式的输入参数。



ISSN1008-4274

知识产权出版社出版

1. 一种用于在移动系统的 GPRS/EDGE 无线接入网 GERAN 与用户设备之间传输数据的方法，包含以下步骤：

（302）发送端用加密算法对要传输的数据加密，

（304）加密数据从发送端传输到接收端，

（306）接收端用加密算法对该传输的数据解密，

其特征在于（310）将采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法用作该加密算法，在这种情况下，基于 GPRS/EDGE 无线接入网 GERAN 的操作参数且通过取决于当前所使用的协议而至少修改该操作参数的一个计数器参数来创建该加密算法所要求的约定格式的输入参数。

2. 如权利要求 1 中要求的方法，其中加密算法的输入参数的约定格式定义输入参数的数目和每个参数的长度。

3. 如前面权利要求的任何一条中要求的方法，其中加密算法是一个黑盒，并且其实现在 GPRS/EDGE 无线接入网 GERAN 和采用宽带码分多址接入方法的无线接入网 UTRAN 中都完全相同。

4. 如权利要求 1 中要求的方法，其中输入参数包含计数器参数。

5. 如权利要求 4 中要求的方法，其中计数器参数包含定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号。

6. 如权利要求 1 中要求的方法，其中输入参数包含载体参数，并且其中一个载体参数值保留给要加密的信令平面数据。

7. 如权利要求 4 中要求的方法，其中当在协议栈的 MAC 层中执行加密算法时，计数器参数包含扩展的 TDMA 帧号。

8. 如权利要求 7 中要求的方法，其中扩展 TDMA 帧号是基于对 GSM 的 T1 计数器部分进行扩展。

9. 如权利要求 7 中要求的方法，其中有关最后使用的扩展 TDMA 帧号的信息存储在用户设备中用于下次连接。

10. 如权利要求 9 中要求的方法，其中要存储的有关最后使用的扩展 TDMA 帧号的信息包含扩展 TDMA 帧号的特定数目的最高有效比特，并且在新的无线连接中使用该信息以构成扩展 TDMA 帧号前，使该最高有效比特构成的数的值增加一。

11. 如权利要求 4 中要求的方法，其中当在协议栈的 MAC 层中执行

加密算法时，计数器参数包含时隙号。

12. 如权利要求 4 中要求的方法，其中当在协议栈的 RLC 层中执行加密算法时，计数器参数包含超帧号。

13. 如权利要求 12 中要求的方法，其中有关最后使用的超帧号的信息存储在用户设备中用于下次连接，并且在新的无线连接中使用该信息以构成超帧号前，使该最高有效比特构成的数的值增加一。

14. 如权利要求 13 中要求的方法，其中要存储的有关最后使用的超帧号的信息包含超帧号的特定数目的最高有效比特。

15. 如权利要求 1 中要求的方法，其中当用户设备的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，将有关最后使用的扩展 TDMA 帧号或超帧号的信息提供给新的无线接入网，并且将与旧的无线接入网中相同的加密密钥输入参数用作新的无线接入网中加密算法的加密密钥输入参数。

16. 如权利要求 15 中要求的方法，其中要提供的信息包含特定数目的最高有效比特，并且在新的无线接入网中使用该信息前，使该最高有效比特构成的数的值增加一。

17. 移动系统的用户设备（UE），包含:

使用加密算法（400）对要发送到 GPRS/EDGE 无线接入网 GERAN 的数据进行加密的装置（416），

使用加密算法（400）对从 GPRS/EDGE 无线接入网 GERAN 接收到的数据进行解密的装置（416），

其特征在于，加密算法（400）是采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法，并且用户设备包含装置（402、404、406、408、410）用于基于 GPRS/EDGE 无线接入网 GERAN 的操作参数且通过取决于当前所使用的协议而至少修改该操作参数的一个计数器参数来创建该加密算法（400）所要求的约定格式的输入参数。

18. 如权利要求 17 中要求的用户设备，其中加密算法（400）的输入参数的约定格式定义了输入参数的数目和每个参数的长度。

19. 如权利要求 17 到 18 中要求的用户设备，其中加密算法（400）是一个黑盒，并且其实现在 GPRS/EDGE 无线接入网 GERAN 和采用宽带码分多址接入方法的无线接入网 UTRAN 中都完全相同。

20. 如权利要求 17 中要求的用户设备，其中输入参数包含计数器参数（402）。

21. 如权利要求 20 中要求的用户设备，其中计数器参数包含定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号。

22. 如权利要求 17 中要求的用户设备，其中输入参数包含载体参数（406），并且其中一个载体参数（406）值保留给要加密的信令平面数据。

23. 如权利要求 20 中要求的用户设备，其中当在协议栈的 MAC 层中执行加密算法（400）时，计数器参数（402）包含扩展的 TDMA 帧号。

24. 如权利要求 23 中要求的用户设备，其中扩展 TDMA 帧号是基于对 GSM 的 T1 计数器部分进行扩展。

25. 如权利要求 23 中要求的用户设备，其中用户设备（UE）包含装置用来存储有关最后使用的扩展 TDMA 帧号的信息用于下次连接。

26. 如权利要求 25 中要求的用户设备，其中要存储的有关最后使用的扩展 TDMA 帧号的信息包含扩展 TDMA 帧号的特定数目的最高有效比特，并且用户设备（UE）包含装置，用于在新的无线连接中使用该信息以构成扩展 TDMA 帧号前，使该最高有效比特构成的数的值增加一。

27. 如权利要求 20 中要求的用户设备，其中当在协议栈的 MAC 层中执行加密算法（400）时，计数器参数（402）包含时隙号。

28. 如权利要求 20 中要求的用户设备，其中当在协议栈的 RLC 层中执行加密算法（400）时，计数器参数（402）包含超帧号。

29. 如权利要求 28 中要求的用户设备，其中用户设备（UE）包含装置用来存储有关最后使用的超帧号的信息用于下次连接。

30. 如权利要求 29 中要求的用户设备，其中要存储的有关最后使用的超帧号的信息包含超帧号的特定数目的最高有效比特，并且用户设备（UE）包含装置（402），用于在新的无线连接中使用该信息以构成超帧号前，使该最高有效比特构成的数的值增加一。

31. 如权利要求 17 中要求的用户设备，其中用户设备包含装置（190、192、194），用于当用户设备（UE）的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，将有关最后使用的扩展 TDMA 帧号或超帧号的信息提供给新的无线接入网，并且用于将与旧的无线接入网中相同的加密密钥参数（408）

用作新的无线接入网中加密算法（400）的加密密钥参数（408）。

32. 如权利要求 31 中要求的用户设备，其中要提供的信息包含特定数目的最高有效比特，并且用户设备（UE）包含装置（402），用于在新的无线接入网中使用该信息前，使该最高有效比特构成的数的值增加一。

33. 一种移动系统的 GPRS/EDGE 无线接入网 GERAN，包含：

使用加密算法（400）对要发送到用户设备（UE）的数据进行加密的装置（416），

使用加密算法（400）对从用户设备（UE）接收到的数据进行解密的装置（416），

其特征在于，加密算法（400）是采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法，并且 GPRS/EDGE 无线接入网 GERAN 包含装置（402、404、406、408、410）用来基于 GPRS/EDGE 无线接入网 GERAN 的操作参数且通过取决于当前所使用的协议而至少修改该操作参数的一个计数器参数来创建该加密算法（400）所要求的约定格式的输入参数。

34. 如权利要求 33 中要求的 GPRS/EDGE 无线接入网，其中加密算法（400）的输入参数的约定格式定义了输入参数的数目和每个参数的长度。

35. 如权利要求 33 到 34 中要求的 GPRS/EDGE 无线接入网，其中加密算法（400）是一个黑盒，并且其实现在 GPRS/EDGE 无线接入网 GERAN 和采用宽带码分多址接入方法的无线接入网 UTRAN 中都完全相同。

36. 如权利要求 33 中要求的 GPRS/EDGE 无线接入网，其中输入参数包含计数器参数（402）。

37. 如权利要求 36 中要求的 GPRS/EDGE 无线接入网，其中计数器参数包含定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号。

38. 如权利要求 37 中要求的 GPRS/EDGE 无线接入网，其中输入参数包含载体参数（406），并且其中一个载体参数（406）值保留给要加密的信令平面数据。

39. 如权利要求 36 中要求的 GPRS/EDGE 无线接入网，其中当在协议栈的 MAC 层中执行加密算法（400）时，计数器参数（402）包含扩展

TDMA 帧号。

40. 如权利要求 39 中要求的 GPRS/EDGE 无线接入网，其中扩展 TDMA 帧号是基于对 GSM 的 T1 计数器部分进行扩展。

41. 如权利要求 39 中要求的 GPRS/EDGE 无线接入网，其中 GPRS/EDGE 无线接入网 GERAN 包含装置用来存储有关最后使用的扩展 TDMA 帧号的信息用于下次连接。

42. 如权利要求 41 中要求的 GPRS/EDGE 无线接入网，其中要存储的有关最后使用的扩展 TDMA 帧号的信息包含扩展 TDMA 帧号的特定数目的最高有效比特，并且 GPRS/EDGE 无线接入网 GERAN 包含装置（402），用于在使用该信息以构成扩展 TDMA 帧号前，使该最高有效比特构成的数的值增加一。

43. 如权利要求 36 中要求的 GPRS/EDGE 无线接入网，其中当在协议栈的 MAC 层中执行加密算法（400）时，计数器参数（402）包含时隙号。

44. 如权利要求 36 中要求的 GPRS/EDGE 无线接入网，其中当在协议栈的 RLC 层中执行加密算法（400）时，计数器参数（402）包含超帧号。

45. 如权利要求 44 中要求的 GPRS/EDGE 无线接入网，其中 GPRS/EDGE 无线接入网 GERAN 包含装置用来存储有关最后使用的超帧号的信息用于下次连接。

46. 如权利要求 45 中要求的 GPRS/EDGE 无线接入网，其中要存储的有关最后使用的超帧号的信息包含超帧号的特定数目的最高有效比特，并且 GPRS/EDGE 无线接入网 GERAN 包含装置（402），用于在使用该信息以构成超帧号之前，使该最高有效比特构成的数的值增加一。

47. 如权利要求 33 中要求的 GPRS/EDGE 无线接入网，其中 GPRS/EDGE 无线接入网 GERAN 包含装置（180），用于当用户设备（UE）的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，接收去往用户设备（UE）的有关最后使用的扩展 TDMA 帧号或超帧号的信息，并且用于将按照接收信息的加密密钥参数（408）用作加密算法（400）的加密密钥参数（408）。

48. 如权利要求 47 中要求的 GPRS/EDGE 无线接入网，其中要提供的信息包含特定数目的最高有效比特，并且 GPRS/EDGE 无线接入网

GERAN 包含装置（402），用于在使用该信息前，使该最高有效比特构成的数的值增加一。

数据传输方法、用户设备和 GPRS/EDGE 无线接入网

领域

本发明涉及用于在移动系统的 GPRS/EDGE（通用分组无线业务/GSM 演进的增强数据速率）无线接入网 GERAN 与用户设备之间传输数据的一种方法，涉及用户设备和涉及 GPRS/EDGE 无线接入网 GERAN。

背景

当从 GERAN 传输数据到用户设备和反向传输时，出于安全原因，要传输的数据必须在发送前进行加密（译成密码）。加密可使对信令和用户数据的窃听更困难。发送端用加密算法对要传输的数据加密并且加密数据从发送端传输到接收端，在接收端用加密算法对传输的数据解密。两端使用相同的加密算法。

通过使用 XOR 操作（逻辑异或操作）将加密算法创建的加密掩码附着于要加密的数据上，因此加密本身并未增加要传输的比特数目。这可用下式来表示

$$C=M\oplus P \qquad (1)$$

其中 C 是加密数据，M 是加密掩码，P 是未加密的数据而⊕是 XOR 操作。

加密算法需要输入参数以使由该算法创建的加密掩码对于每个用户和每个使用时刻都不同。最重要的参数是加密密钥，其长度为比如 128 比特。每个用户使用不同的加密密钥，因而也使用不同的加密掩码。然而，对于不同内容的数据不能使用相同的加密掩码两次的事实引发了一个问题。这一禁止情况可用下式描述

$$\begin{array}{r} P_1 \oplus M = C_1 \\ \oplus \quad P_2 \oplus M = C_2 \\ \hline P_1 \oplus P_2 = C_1 \oplus C_2 \end{array} \qquad (2)$$

其中 P1 和 P2 是有不同内容的未加密数据而 C1 和 C2 是有不同内容的加密数据。可见，一个可能的窃听者可通过在具有不同内容和使用相同掩码加密的数据之间执行 XOR 操作而去除该掩码，因而破坏了该加密。

因此，其他参数也可用于加密算法中，比如采用通用移动电信系统

（UMTS）的宽带码分多址接入方法的无线接入网（UTRAN）的加密算法将随时间而变化的计数器参数、方向性参数（上行链路/下行链路）和载体参数用作输入参数。

GERAN 中要使用的加密算法的结构还未确定。然而它应该至少满足下列要求：

- 隐式加密同步，尤其是与切换相连时，
- 对实时和非实时业务类似的方式，
- 增加的冗余，
- 几个不同用户复用到同一时隙，
- 几个不同的无线载体复用到同一用户设备，
- 使能多时隙操作。

发明简述

本发明的一个目的是提供用于在移动系统的GPRS/EDGE无线接入网GERAN与用户设备之间传输数据的一种改进方法、一种改进的用户设备和一种改进的 GPRS/EDGE 无线接入网 GERAN。作为本发明的一个方面，提出了按照权利要求 1 的方法，用于在移动系统的 GPRS/EDGE 无线接入网 GERAN 与用户设备之间传输数据。作为本发明的第二方面，提出了按照权利要求 17 的用户设备。作为本发明的第三方面，提出了按照权利要求 33 的 GPRS/EDGE 无线接入网 GERAN。本发明的优选实施方案公布于从属的权利要求中。

本发明基于在 GERAN 中同样地重用 UTRAN 的加密算法。通过将加密算法的内部操作定义为一个黑盒并且通过按照GERAN设置的要求来修改加密算法所要求的输入参数，使之成为可能。

本发明的方法和设备提供了几个改进之处。设计新的加密算法是非常费力的操作。当使用本发明时，无需对于 GERAN 设计新的加密算法，而相反可使用已设计的 UTRAN 加密算法。这节省了可观的工作量以及由此引起的产品开发成本。本发明还易于设计能与 UTRAN 和 GERAN 接触的用户设备。

附图简述

下面，将通过优选实施方案并参考附图更详细地描述本发明，其中

图 1A 示意了蜂窝网的结构实例，

图 1B 是更详细地示意蜂窝网的框图，

图 1C 示意了电路交换的连接，

图 1D 示意了分组交换的连接，

图 2 示意了蜂窝网特定部分的协议栈实例，

图 3 是示意用于数据传输的一种方法的流程图，

图 4 示意了发送端的加密和接收端的解密。

实施方案描述

主页为http://www.3gpp.org的 3GPP（第三代伙伴计划）正在发展的第三代移动系统如 UMTS 的规范包含涉及系统的一般结构和加密的规范，该规范提供了使本领域内的技术人员能使用本发明的很好描述。特别涉及加密的规范在这里引入作为参考：

- 3G TS 33.102 V3.2.0: Security Architecture（安全性体系结构）

- 3G TS 25.301 V3.4.0: Radio Interface Protocol Architecture（无线接口协议体系结构）

- 3G TS 33.105 V3.3.0: Cryptographic Algorithm Architecture（加密算法体系结构）

参考图 1A 和图 1B 描述了一个典型的无线系统结构及其与公共交换电话网和分组传输网的连接。图 1B 只包含对于描述实施方案很关键的块，但是本领域内的技术人员很清楚：传统的蜂窝网也包含这里无需更详细描述的其他功能和结构。本发明的无线系统使用 GPRS/EDGE 无线接入网 GERAN。术语 GERAN 指的是 GSM(全球移动通信系统)系统、TDMA/136（时分多址接入）系统和 EDGE 系统的演进，它力图提供完全的第三代（UMTS/WCDMA/cdma2000）移动业务。

因而在一定意义上，GERAN 是基于 GSM 的 GPRS 或 EGPRS（增强型通用分组无线业务）与采用宽带码分多址接入的通用移动电信系统 UMTS 的一种中间形式，其中无线接入网的结构概括为 UMTS 类型而无线接入网称为比如 GERAN，并且其中无线接口却是通常的基于 GSM 的无线接口或者采用 EDGE 调制的无线接口。EGPRS 是使用分组交换传输的基于 GSM 的系统。EGPRS 使用 EDGE 技术来增加数据传输容量。除了 GSM 中通常使

用的 GMSK（高斯最小频移键控）调制外，还可能对分组数据信道使用 8-PSK（8 相移键控）调制。其目的主要是不仅实现非实时数据传输业务，如文件复制和使用因特网浏览器，还实现比如语音和视频图像传输中的实时分组交换业务。

图 1A 和 1B 的描述主要基于 UMTS。一个移动系统的主要部分是核心网 CN、UMTS 陆地无线接入网 UTRAN 和用户设备 UE。CN 与 UTRAN 之间的接口称为 Iu，而 UTRAN 与 UE 之间的无线接口称为 Uu。

UTRAN 由无线网络子系统 RNS 构成。RNS 间的接口称为 Iur。RNS 由无线网络控制器 RNC 和一个或多个节点 B 构成。RNC 与 B 之间的接口称为 Iub。图 1B 中节点 B 的覆盖区域即小区被标注为 C。RNS 也可用其更传统的名称即基站系统（BSS）来称谓。因而无线系统的网络部分包含无线接入网 UTRAN 和核心网 CN。

图 1A 中的描述很抽象，所以图 1B 中通过大致指示 GSM 系统的哪一部分对应于 UMTS 中的哪一部分来阐明。应该注意，提供的描述绝不是约束性的而只出于示意的目的，因为 UMTS 的不同部分的职责和功能仍在设计中。

用户设备 150 比如可以固定安装于交通工具中，或者是便携式的。用户设备 150 也称为移动台 MS。无线接入网 UTRAN 的基础设施由无线网络子系统 RNS 即基站系统构成。无线网络子系统 RNS 由无线网络控制器 RNC 102 即基站控制器和它控制的至少一个节点 B 100 即基站构成。

基站 B 具有复用器 116、收发信机 114 以及控制该收发信机 114 和复用器 116 的操作的控制单元 118。收发信机 114 使用的业务和控制信道通过复用器 116 放置于传输链路 160 上。

基站 B 的收发信机 114 连接到天线单元 112，该天线单元实现到用户设备 150 的双向无线链路 Uu。双向无线链路 Uu 中传输的帧结构已有详细的定义。

无线网络控制器 RNC 包含群交换域 120 和控制单元 124。群交换域 120 用于语音和数据连接和用于连接信令电路。由基站 B 和无线网络控制器 RNC 形成的基站系统还包含代码转换器 122。无线网络控制器 RNC 与基站 B 之间的工作分配以及它们的物理结构取决于实现而变化。如上所述，基站 B 通常负责无线通路的实现。无线网络控制器 RNC 通常负责下列方面：无线资源管理、小区间的切换控制、功率调整、定时和同步、

寻呼用户设备。

代码转换器 122 的位置通常要尽可能地接近移动交换中心 132，因为这样就可在代码转换器 122 与无线网络控制器 RNC 之间以移动电话系统格式传输语音，从而节约了传输容量。代码转换器 122 将公共交换电话网与移动网之间使用的不同数字编码格式的语音转换为相互兼容的，比如从公共网的 64kbit/s 格式转换为蜂窝网的另一（如 13kbit/s）格式，反之亦然。这里没有详细描述所需硬件，但可注意到除语音外的其他数据并未在代码转换器 122 中转换。控制单元 124 负责呼叫控制、移动性管理、统计收集和信令。

核心网 CN 包含属于移动电话系统并在 UTRAN 之外的基础设施。在属于核心网 CN 的电路交换传输的设备中，图 1B 示意了移动交换中心 132。

如图 1B 所示，通过交换域 120 可经由移动交换中心 132 连接（黑点所示）到公共交换电话网 134 并且也可连接到分组交换网 142。公共交换电话网 134 中的典型终端 136 是传统的电话或者 ISDN（综合业务数字网）电话。从经由因特网 146 连接到移动系统的计算机 148 传输分组到连接到用户设备 150 的便携式计算机 152。不采用用户设备 150 和便携式计算机 152 的组合，而使用 WAP（无线应用协议）电话。

建立分组传输网 142 与交换域 120 之间的连接是通过服务 GPRS 支持节点（SGSN）140 进行的。服务支持节点 140 的任务是在基站系统与网关 GPRS 支持节点（GGSN）144 之间传输分组，并记录其区域内的用户设备 150 的位置。

网关支持节点 144 连接公共分组传输网 146 和分组传输网 142。接口中可使用互联网协议或者 X.25 协议。网关支持节点 144 通过封装来对公共分组传输网 146 隐藏分组传输网 142 的内部结构，这样对于公共分组传输网 146 来说，分组传输网 142 像是一个子网，而公共分组传输网 146 可定址分组到其中的用户设备 150 和从其接收分组。

分组传输网 142 通常是使用互联网协议并传送信令和用户数据的私有网。网络 142 的结构在其互联网协议层下的体系结构和协议都有变化，这取决于运营商。

公共分组传输网 146 可以是因特网，比如通过它，与之相连的终端 148 如服务器可传输分组到用户设备 150。

图 1C 示意了用户设备 150 与公共交换电话网终端 136 之间如何建立电路交换传输链路。在图中，粗线示意了数据是如何经过该系统在无线接口 170 上从天线 112 发送到收发信机 114 并在复用器 116 的复用之后从那里经过传输链路 160 到交换域 120，交换域与代码转换器 122 的输出有连接，并从那里开始，通过移动交换中心 132 中完成的连接而到达与公共交换电话网 134 相连的终端 136。在基站 100 中，进行传输时控制单元 118 控制复用器 116，而在基站控制器 102 中，控制单元 124 控制交换域 120 来实现正确连接。

图 1D 示意了分组交换传输链路。现在便携式计算机 152 与用户设备 150 相连。粗线示意了传输的数据是如何从服务器 148 送到便携式计算机 152 的。数据自然也可以以相反传输方向传输，即从便携式计算机 152 到服务器 148。数据经过系统在无线接口之上即 Um 接口 170 从天线 112 传递到收发信机 114，并从那里出发，在经过复用器 116 中的复用之后，经传输链路 160 和 Abis 接口到交换域 120，在 Gb 接口上、已建立从那里到支持节点 140 的输出的一个连接，从支持节点 140 出发，数据在分组传输网 142 中传输，经过网关节点 144 到达与公共分组传输网 146 相连的服务器 148。

为了清楚起见，图 1C 和 1D 并未示意电路交换和分组交换数据同时传输的情况。然而，这完全是可能而普遍的，因为可灵活地使用从电路交换数据传输到分组交换传输的自由的容量。也可建立一个网络，其中只传输分组数据。在这种情况下，网络的结构可简化。

让我们再次观察图 1D。UMTS 系统的不同实体-CN、UTRAN/GERAN、RNS/BSS、RNC/BSC、B/BTS-在图中都用虚线框来概括。在分组交换环境下，核心网 CN 包含支持节点 140、分组传输网 142 和网关节点 144。

除了所述之外，GPRS 还有两个特定元素：信道编译码器单元 CCU 和分组控制单元 PCU。CCU 的任务包括含 FEC（前向差错编码）和交织的信道编码、无线信道测量功能如接收信号的质量级别、接收信号的接收功率和涉及定时提前测量的信息。PCU 的任务包括分段和重组 LLC（逻辑链路控制）段、ARQ（自动重复请求）功能、PDCH（分组数据信道）调度、信道接入控制和无线信道管理功能。CCU 182 位于基站 100，并且它可视为时隙特定的或者收发信机特定的单元，这取决于其实现。PCU 180 经 Abis 接口与 CCU 182 相连。PCU 可位于基站 100 中或者位于基站

控制器 102 中。图 1C 示意了基站控制器 102 中的 PCU 180，但为了清楚起见，未示意它在基站 100 中的位置。

图 1D 也示意了用户设备 UE 的结构中本申请所关心的相关部分。用户设备 UE 包含天线 190，经由它收发信机 192 可从无线通路 170 接收信号。用户设备 UE 的操作由控制单元 194 控制，它通常是具有必需软件的微处理器。该软件也执行后边描述的协议处理。除了描述的部分外，用户设备 UE 也包含用户接口，它通常包含扬声器、麦克风、显示器和键盘，以及电池。然而，这里并没有更详细地描述这些，因为本发明对此不感兴趣。

这里并未更加详细地描述基站 B 中的收发信机的结构或者用户设备 UE 中的收发信机的结构，因为本领域内的技术人员很清楚该设备是如何实现的。比如，可能使用按照 EGPRS 的通常的无线网收发信机和用户设备收发信机。对于本申请，唯一重要的是可实现无线链路 170，因为应用所需的操作然后是在较高的 OSI（开放系统互连）模型层中进行的，尤其是在第三层中进行。

图 2 示意了 EGPRS 控制平面的分组协议堆栈。然而，应当注意，该实施方案并不局限于 EGPRS。协议栈是按照 ISO（国际标准化组织）的 OSI（开放系统互连）模型构成的。在 OSI 模型中，协议栈分为层。原理上有七层。图 2 对于每个网络元素，示意了所讨论的网络元素中处理的分组协议部分。网络元素是移动台 MS、基站系统 BSS 和支持节点 SGSN。基站和基站控制器没有分开示意，因为它们之间的接口还未定义。因而基站系统 BSS 的协议处理集合原理上可在基站 100 与基站控制器 102 之间自由分布，然而不在代码转换器 122 上，即便代码转换器 122 确实属于基站系统 BSS。网络元素 MS、BSS 和 SGSN 由它们之间的接口 Um 和 Gb 分隔。

每个设备 MS、BSS 和 SGSN 中的一层与另一设备中的一层进行逻辑通信。只有最低的物理层可相互直接通信。其他层总是使用下一层提供的服务。因而消息可在层间垂直地在物理上前进，而只有在最底层消息才能在层间水平地前进。

实际的比特级数据传输首先使用最低第一层 L1 即物理层 RF 来进行。物理层定义物理传输路径相联系的机械、电子和功能特性。下一层，第二层即数据链路层，使用物理层的服务以实现可靠的数据传输并负责

比如传输纠错。在无线接口 170 上，数据链路层分为 RLC/MAC（无线链路控制/媒体接入控制）子层和 LLC（逻辑链路控制）子层即逻辑链路控制协议。第三层即网络层使上层与负责设备间连接的数据传输和交换技术无关。网络层负责比如连接的建立、维护和释放。在 GSM 中，网络层也称为信令层。它有两个主要任务：为消息选路，并使得能够在两个实体间同时的几个独立的连接。

网络层包含会话管理子层 SM 和 GPRS 移动性管理子层 GMM。

GPRS 移动性管理子层 GMM 负责移动台用户移动的结果，这并不直接涉及无线资源管理。在公共交换电话网一边，此子层可负责证实用户并使得该用户与网络相连。在蜂窝网中，该子层支持用户移动性、注册和移动性产生的数据的管理。另外，该子层检查移动台的标识和允许的业务的标识。该子层的消息传输发生在移动台 MS 与支持节点 SGSN 之间。

会话管理子层 SM 管理涉及分组交换呼叫管理的所有功能，但并不检测用户的移动。会话管理子层 SM 建立、维护和释放连接。对于移动台 150 发起或者终止于移动台 150 的呼叫，它有自己的规程。该子层的消息传输也发生在移动台 MS 与支持节点 SGSN 之间。

在基站系统 BSS 中，会话管理子层 SM 和 GPRS 移动性管理子层 GMM 的消息都透明地处理，即它们只向前或者向后传送。

按照现有技术，逻辑链路控制协议 LLC 在 SGSN 与 MS 之间建立可靠的加密的逻辑链路。LLC 独立于下层以便无线接口的改变能尽可能少的影响移动网的网络部分。逻辑链路控制协议的业务包括：对等实体之间的非常可靠的逻辑链路、支持可变长度的信息帧、支持确认和未确认的数据传输，每帧包含发送或接收移动台的明确的识别符，支持不同的服务准则，如数据传输的不同特性、传输数据和用户标识的加密。在 Um 与 Gb 接口之间通过逻辑链路控制协议中继 LLC RELAY 传输 LLC 数据。按照此应用中描述的解决方案，加密不在 LLC 子层中进行，而在 MAC 或 RLC 子层中进行。也可把 LLC 子层的其他任务给予其他层，这样 LLC 子层就可完全省去。

MAC 层负责下列任务：在上行链路（移动台到网络部分）和下行链路（网络部分到移动台）连接上复用数据和信令、上行传输路径资源请求的管理和下行传输路径业务资源的分配和定时。业务优先级管理也属于此层。RLC 层负责传输 LLC 层数据即 LLC 帧到 MAC 层；RLC 将 LLC 帧

分为 RLC 数据块并将其传输到 MAC 层。在上行链路方向，RLC 构建 RLC 数据块的 LLC 帧并将其传输到 LLC 层。物理层通过无线链路在 Um 接口实现，比如 GSM 定义的无线接口。比如，要传输的数据的载波调制、交织和纠错、同步和发送机功率控制都在物理层进行。

BSSGP（基站子系统 GPRS 协议）层在 BSS 与 SGSN 之间传输高层的数据和涉及选路和服务质量的信息。FR（帧中继）层执行此信息的物理传输。NS（网络服务）传输按照 BSSGP 协议的消息。

现在已经给出了移动系统的结构和其中使用的协议栈的例子，就可能查看使用 GERAN 的移动系统中加密的实现。图 4 示意了数据流是如何从发送端到达接收端的。发送端在图的左边而右边的接收端通过垂直的虚线与之相隔。在 GERAN 中，加密在上述的分组控制单元 180 中和在用户设备的控制单元 194 中进行。加密的进行要使用位于所述的协议栈中的功能。必需的功能可实现为比如运行于通用处理器中的软件，在这种情况下所需的功能作为软件组件执行。硬件实现也是可能的，比如 ASIC（专用集成电路）或者由单独的组件构成的控制逻辑。

加密算法 400 也是采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法，也称为 f8。加密算法是一个黑盒，并且其实现在 GPRS/EDGE 无线接入网 GERAN 和采用宽带码分多址接入方法的无线接入网 UTRAN 中都完全相同。实际中这意味着相同的加密算法实现，无论是 ASIC 或是软件，都可用于 GERAN 和 UTRAN 中。

UTRAN 对于加密算法的输入参数具有约定格式。该约定格式定义输入参数的数目和每个参数的长度。UTRAN 输入参数在上述 3GPP 规范中有定义。它们是：加密密钥、随时间而变的计数器参数、方向性参数（上行链路/下行链路）和载体参数。另外，需要表示加密掩码 412 的长度的参数，它本身并不影响加密算法 400 的内部操作，但只表示可从密钥流中拿出多少个创建的符号给加密掩码 412。

通过 XOR 操作 416 将未加密数据 414 与加密掩码 416 相组合以获得加密数据 418。

在接收端，使用如发送端那样的类似操作去除该加密，即通过 XOR 操作 416 将加密掩码 412 与接收到的加密数据 418 相组合以获得该原始的未加密数据 414。

发送端和接收端必须相互同步，意义是用来对特定数据 414 加密的

加密算法 400 的参数 402、404、406、408、410 必须也用来对对应于该未加密数据 414 的加密数据 418 解密。实现此可能需要在发送端与接收端之间的信令。这个问题或者数据调制和信道编码都没在这里更详细地描述，因为它们对于本发明来说并不关键，并且对于本领域内的技术人员来说都是熟知的动作。发送端包含装置 400、416 使用加密算法 400 对要传输到接收端的数据进行加密，而接收端相应包含装置 400、416 使用加密算法 400 对从发送端接收到的数据进行解密，注意到这一点就足够了。因为 GERAN 与用户设备之间的连接是双向的，所以两者都可充当发送端和接收端。因而，GERAN 与用户设备都包含加密装置和解密装置。

GPRS/EDGE 无线接入网 GERAN 包含装置 402、404、406、408、410 用来基于 GPRS/EDGE 无线接入网 GERAN 的操作参数而创建加密算法 400 所需的约定格式的输入参数。用户设备 UE 包含相同的装置 402、404、406、408、410。为清楚起见，图 4 使用了相同的参考编号 402、404、406、408、410 以描述加密算法 400 的参数和处理它们的装置。实际当中，该装置优选地通过用户设备 UE 的控制单元 194 中或者 GPRS/EDGE 无线接入网 GERAN 的分组控制单元 180 中的软件来实现：

	RLC 协议	MAC 协议
计数器参数 402： 长度 32 比特	- RLC 序列号：长度 7 或者 11 比特，取值范围 0－127 或者 0－2047 - 定义要加密的数据是第二层信令平面的数据还是其他数据的符号：长度 1 比特，取值 1。 - 超帧号：长度 24 或 20 比特	- 扩展的 TDMA 帧号：长度 28 比特，取值范围 0－（2^{28}－1） - 时隙号：长度 3 比特，取值 0－7。 - 定义要加密的数据是第二层信令平面的数据还是其他数据的符号：长度 1 比特，取值 1。
方向性参数 404： 长度 1 比特，取值		

0/1		
载体参数 406: 长度 5 比特		
长度参数 410: 长度 16 比特	取值: 有效负荷的长度，或者没有无线载体识别符和RLC序列号的全部块的长度	取值: 全部块的长度
加密密钥参数 408: 长度 128 比特		

表 1

表 1 示意了发送用户平面数据时所需格式的输入参数是如何从 GERAN 操作参数而得的。该表最左边一列示意了 UTRAN 所需的参数。中间列示意了一种替代，其中加密在 RLC 协议层中进行，而最右边一列示意了一种替代，其中加密在 MAC 协议层中进行。

UTRAN 方向性参数 404 定义了要加密的数据要传送的传输方向。值 0 为上行链路，而值 1 为下行链路。方向性参数 404 也同样地可在 GERAN 中使用。

UTRAN 中，载体参数 406 定义了使用的无线载体的识别符。这样在用户同时使用已复用到相同的物理层帧的几个不同无线载体时就可能使用相同的加密密钥 408。载体参数 406 同样地可在 GERAN 中使用。

UTRAN 中，长度参数 410 定义了所需的密钥流长度，即加密掩码 412 的长度。长度参数 410 同样地可在 GERAN 中使用。当使用 RLC 协议时，其取值为有效负荷的长度或者没有无线载体识别符和 RCL 序列号的全部块的长度。当使用 MAC 协议时，其取值为全部块的长度，在这种情况下，无线载体识别符并未包括在信息流中，而在开始传输前就是被约定的。

在 UTRAN 中，加密密钥参数 408 定义了加密密钥。加密密钥参数 408 同样地可在 GERAN 中使用。

UTRAN 计数器参数 410 是随时间而变的 32 比特计数器，并由比如超帧号和 RLC 序列号构成。在原来的 GSM 系统中，22 比特的 TDMA 帧号用作计数器参数。这意味着计数器参数在大约 3.5 小时的加密后就已经到达其最大值。当计算器参数重新开始时，掩码开始再次获得相同值，而如果不使用新的加密密钥的话就会破坏加密。

计数器参数 410 不能同样地在 GERAN 中使用，而是在长度保持在 32 比特时其内容必须改变。当使用 RLC 协议时，计数器参数 410 由 RLC 序列号、定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号，以及超帧号构成。超帧号的长度可以是 24 比特，这种情况下 RLC 序列号的长度是 7 比特，或者超帧号可以是 20 比特长，这种情况下 RLC 序列号是 11 比特长。当要加密的数据是其他数据而非第二层信令平面的数据时，定义该要加密的数据是第二层信令平面数据还是其他数据的 1 比特符号在这种情况下取值为 1。实际当中，当使用 RLC 协议时，计数器参数的有效长度变为 31 比特，而 1 比特符号是不变的。

当使用 MAC 协议时，计数器参数 410 由扩展的 TDMA 帧号、时隙号和定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号构成。TDMA 帧号的长度因而扩展到 28 比特。当要加密的数据是其他数据而非第二层信令平面的数据时，定义要加密的数据是第二层信令平面的数据还是其他数据的 1 比特符号在这种情况下取值为 1。如果只使用一个时隙，则时隙号可不变。实际当中，当使用 MAC 协议时，计数器参数的有效长度变为 28 比特，而 1 比特符号和时隙号都不变。这是目前 GSM 计算器参数的循环的 64 倍，因而实践中足够了。

与超帧号的相同思路也用于扩展的 TDMA 帧号。在目前的 GSM 系统中，TDMA 帧号的 11 位最高有效比特被用来计算复帧。这 11 比特构成 T1 计数器部分，当扩展到 16 比特时它能提供扩展的 TDMA 帧号。5 比特的 T2 计数器部分和 6 比特的 T3 计数器部分也可放在扩展的 TDMA 帧号中。

当使用 RLC 协议时，对用户的有效负荷而非无线载体识别符或者 RLC 块头标进行加密以保证 RLC 序列号的接收。另一种替代是对用户的有效负荷和块的头标进行加密，而非 RLC 序列号或者无线载体识别符。当使用 MAC 协议时，对整个 MAC 块加密。

表 2 示意了当发送第二层信令平面数据时所需格式的输入参数是如何从 GERAN 操作参数得到的。然后加密必须在 MAC 协议层中进行。

当发送第二层信令平面数据时，方向性参数 404、长度参数 410 和加密密钥参数 408 可以以与发送其他数据时相同的方式使用。

第二层信令平面数据没有无线载体识别符，所以给予载体参数 406 一个常数值，如“00000”。如后所述，也可对此常数值定义特定意义。

	MAC 协议
计数器参数 402: 长度 32 比特	扩展的 TDMA 帧号：长度 28 比特，取值范围 0－（2^{28}-1） －时隙号：长度 3 比特，取值 0－7。 － 定义要加密的数据是第二层信令平面的数据还是其他数据的符号：长度 1 比特，取值 0。
方向性参数 404: 长度 1 比特，取值 0/1	
载体参数 406: 长度 5 比特	取值“00000”
长度参数 410: 长度 16 比特	取值：全部块的长度
加密密钥参数 408: 长度 128 比特	

表 2

当使用 MAC 协议时对于第二层信令平面数据可以以与对于其他数据相同的方式构成计数器参数 410，即计数器参数 410 由扩展的 TDMA 帧号、时隙号和定义要加密的数据是第二层信令平面的数据还是其他数据的一个符号构成。当要加密的数据是第二层信令平面的数据时，定义要加密的数据是第二层信令平面的数据还是其他数据的 1 比特符号在这种情况下取值为 0。对整个 MAC 块都进行加密。

很自然，1 比特符号可能的取值也可以按其他方式定义，即值 1 意味着要加密的数据是第二层信令平面的数据，而值 0 意味着要加密的数据是其他数据。

下面描述本发明的替代优选实施方案。

在优选实施方案中，其中一个载体参数值保留给要加密的信令平面数据。这就是上述的常数值，如表 2 所说的“00000”。这样，就可能替换该定义要加密的数据是第二层信令平面的数据还是其他数据的符号。值“00000”定义了要加密的数据是第二层信令平面的数据，而任

何其他数值定义所使用的无线载体识别符。如上所述，对于第二层信令平面数据没有使用无线载体识别符。该方法提供了计数器参数的有效长度增加一比特的优点，和对于一个无线载体识别符必须定义特定意义的缺点。

在优选实施方案中，当使用 MAC 协议时，要存储的有关最后使用的扩展 TDMA 帧号的信息被存储在用户设备 UE 中用于下次连接，实际中它一般存于用户设备 UE 的 SIM（用户标识模块）卡上。UTRAN 已知的超帧号管理应用于此。如果几个无线载体用在相同的连接上，则存储该扩展的 TDMA 帧号，它已取得最大值。当建立新连接时，则只需要传送一个值，而这个值用来开始新连接的加密。在 UTRAN 中，该值被称为 START。有关最后使用的扩展 TDMA 帧号的信息优选地包含扩展 TDMA 帧号中特定数目的最高有效比特。相应地，当使用 RLC 协议时，有关最后使用的超帧号的信息存储在用户设备 UE 中用于下次连接。要存储的有关最后使用的超帧号的信息优选地包含超帧号的特定数目的最高有效比特。所说的用于下次连接的扩展 TDMA 帧号和/或超帧号的存储也可在 GPRS/EDGE 无线接入网 GERAN 中进行，最优选是在分组控制单元 180 中进行。当建立新连接时，该所存数值的信令传输怎样才能在用户设备与 GPRS/EDGE 无线接入网 GERAN 之间最容易而又最有效地进行，会影响存储位置的选择。一个存储的 START 数值用 RLC 协议和 MAC 协议处理与相同用户的连接，即存储所使用数值的最大者。

在优选实施方案中，当用户设备 UE 的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，将有关最后使用的扩展 TDMA 帧号或者超帧号的信息提供给新的无线接入网，并且将与旧的无线接入网中相同的加密密钥输入参数 408 用作新的无线接入网中加密算法 400 的加密密钥输入参数 408。这样，就可能避免对于有不同内容的未加密数据 414 使用相同掩码 412。没有这个规程，就必须总执行所需的信令传输，这是通过当比如因为切换而连接改变时，启动用户设备 UE 与 GPRS/EDGE 无线接入网 GERAN 之间的新加密密钥进行的。原理上，这一规程可以两种方式实现，或者是使得用户设备包含装置 190、192、194，用于当用户设备 UE 的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，将有关最后使用的扩展 TDMA 帧号或超帧号的信息提供给新

的无线接入网，或者是使得 GPRS/EDGE 无线接入网 GERAN 包含装置 180，用于当用户设备 UE 的连接在 GPRS/EDGE 无线接入网 GERAN 与采用宽带码分多址接入方法的无线接入网 UTRAN 之间改变时，用于接收去往用户设备 UE 的、有关最后使用的扩展 TDMA 帧号或超帧号的信息。

所述的规程优选地以这样一种方式实现，以致于要存储或提供的信息包含特定数目的最高有效比特，并且在新的无线连接或者无线接入网中使用该信息前，使该最高有效比特构成的数的值增加一。这样，就可能避免对于不同内容的未加密数据 414 两次使用相同的加密掩码 412。这可实现为，使得用户设备 UE 或者 GPRS/EDGE 无线接入网 GERAN 包含装置 402，用于在新的连接或者新的无线接入网中使用该信息前，使该最高有效比特构成的数的值增加一。比如，当从 GERAN 移动到 UTRAN 时，可存储 20 位最高有效比特，而当从 UTRAN 移动到 GERAN 时，可存储 17 位最高有效比特。这样，较低有效部分之间的差异保持了不重要性，而这就可能保证相同的加密掩码 412 不被使用两次。

参考图 3 中的流程图，下面给出了用于在移动系统的 GPRS/EDGE 无线接入网 GERAN 与用户设备 UE 之间传输数据的方法中采取的步骤。该方法从块 300 开始。

在块 302 中，发送端用加密算法 400 对要传输的数据加密。

在块 304 中，加密数据从发送端传输到接收端。

在块 306 中，在接收端处用加密算法 400 对传输的数据解密。

在发送端和接收端都放有块 310 描述了一个事实，即将采用通用移动电信系统的宽带码分多址接入方法的无线接入网 UTRAN 的加密算法 400 用作加密算法 400，在这种情况下，基于 GPRS/EDGE 无线接入网 GERAN 的操作参数，来创建加密算法 400 所需的约定格式的输入参数 402、404、406、408、410。

正如附带的权利要求所显示的那样，该方法可用用户设备 UE 和 GPRS/EDGE 无线接入网 GERAN 的上述优选实施方案进行修改。

虽然上面参考实例按照附图已对本发明进行了解释，但很显然，本发明并不局限于此，而是可以以附带的权利要求中公布的创造性思想的范围之内的很多方式进行修改。

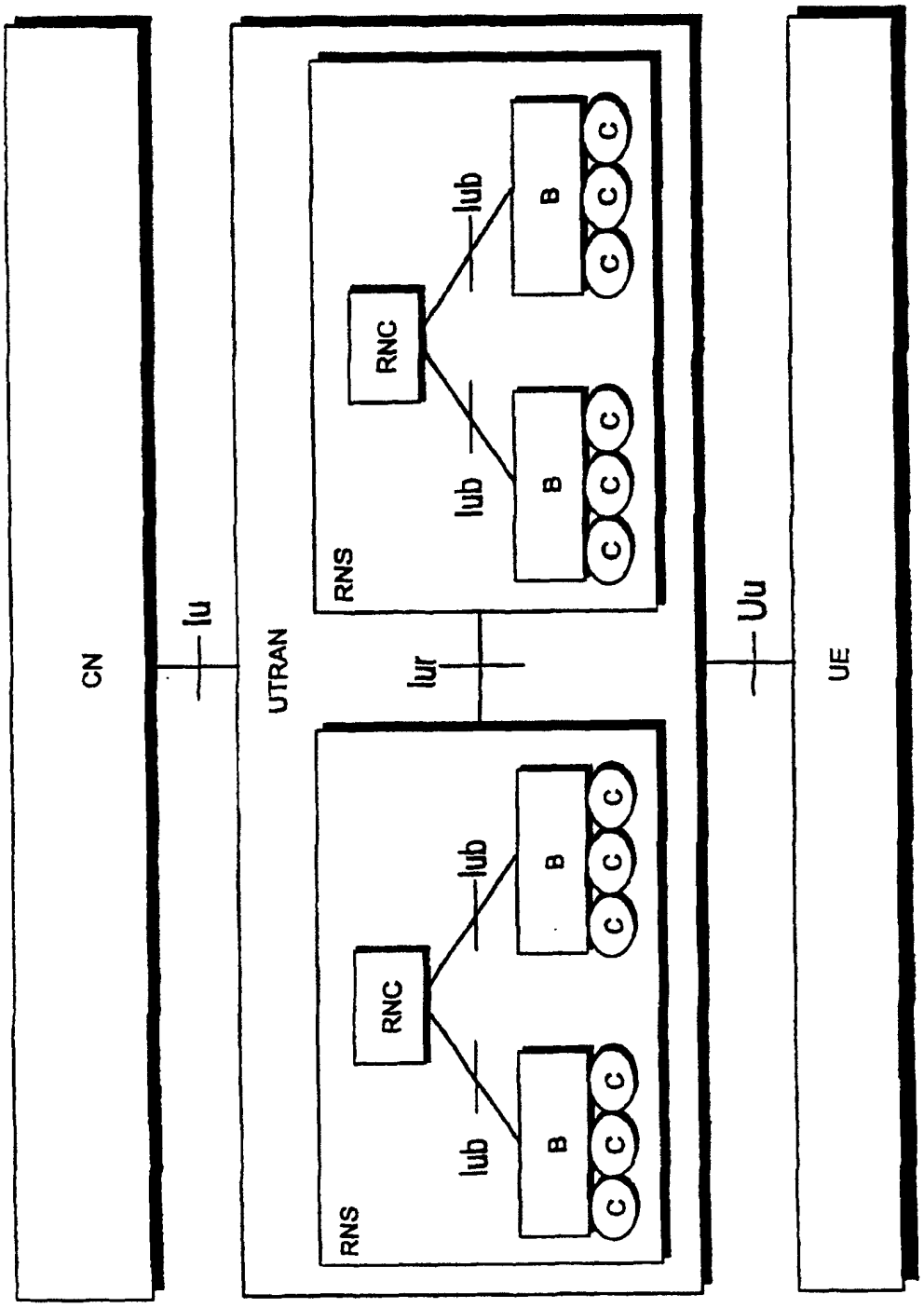


图 1A

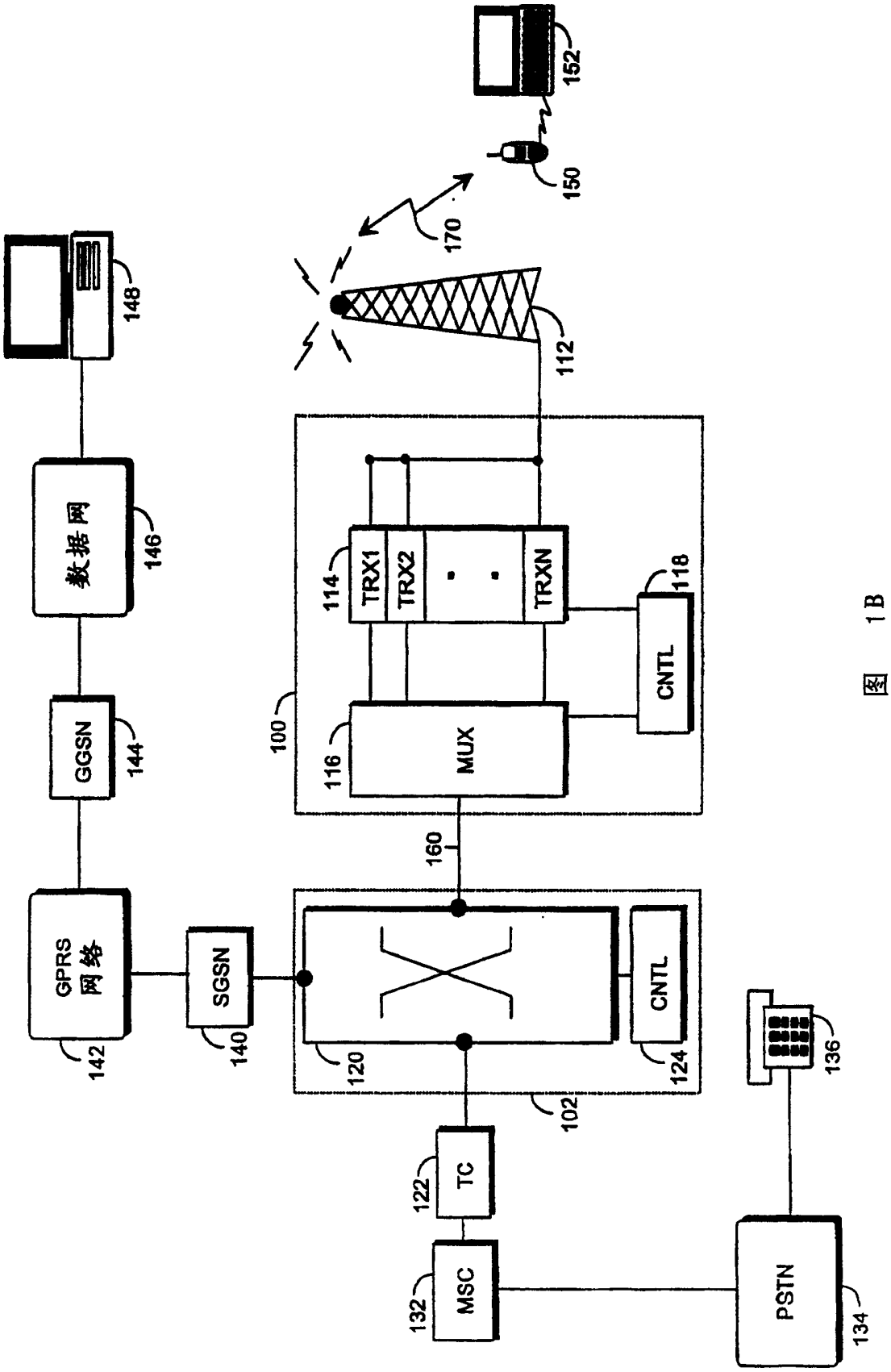

152
150
170
112
148
数据网
146
GGSN
144
GPRS
网络
142
SGSN
140
100
114
TRX1
TRX2
TRXN
118
CNTL
116
MUX
160
120
CNTL
124
102
136
122
TC
132
MSC
PSTN
134

图 1B

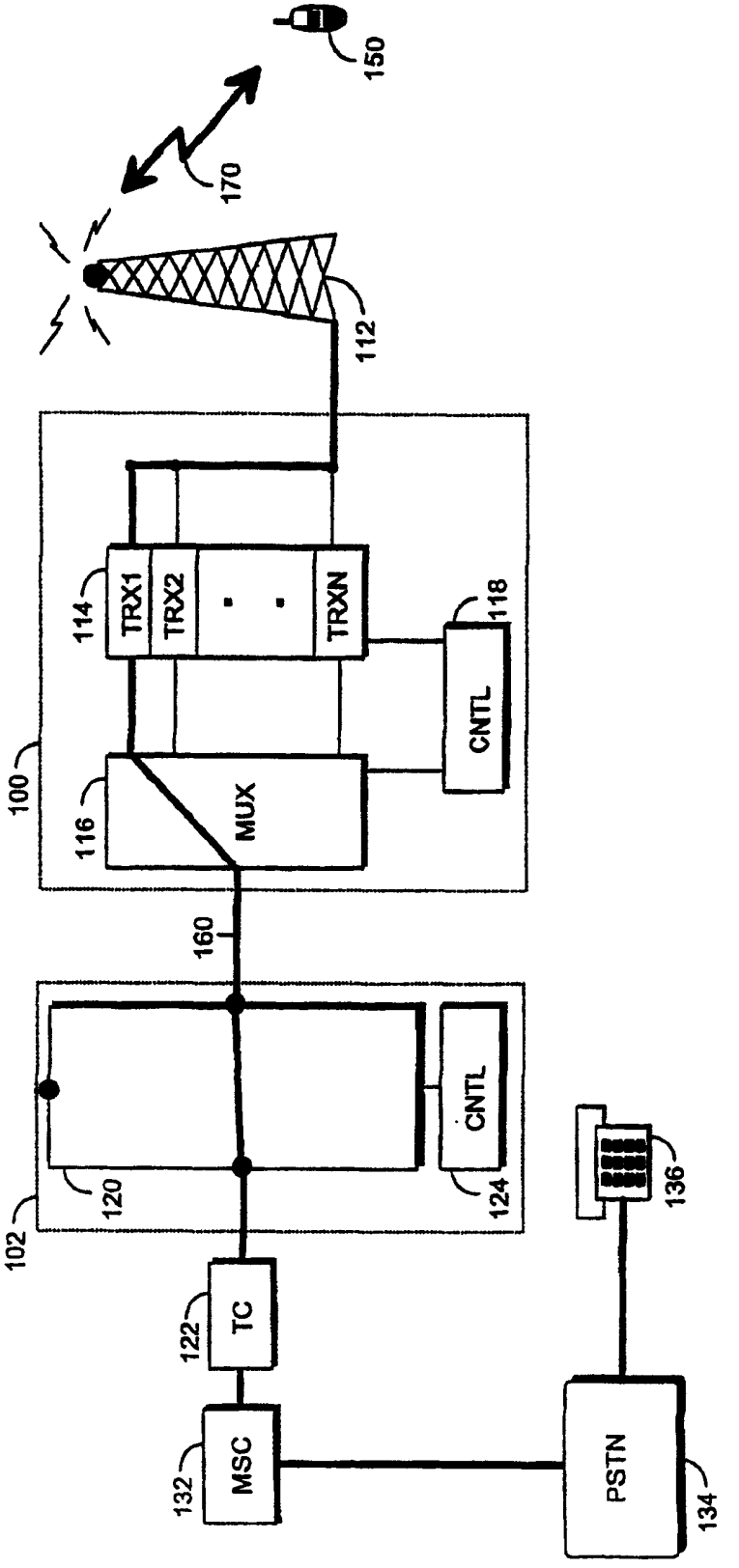

150
170
112
TRX1
TRX2
TRXN
114
118
CNTL
100
116
MUX
160
CNTL
120
124
102
136
122
TC
132
MSC
PSTN
134

图 1C

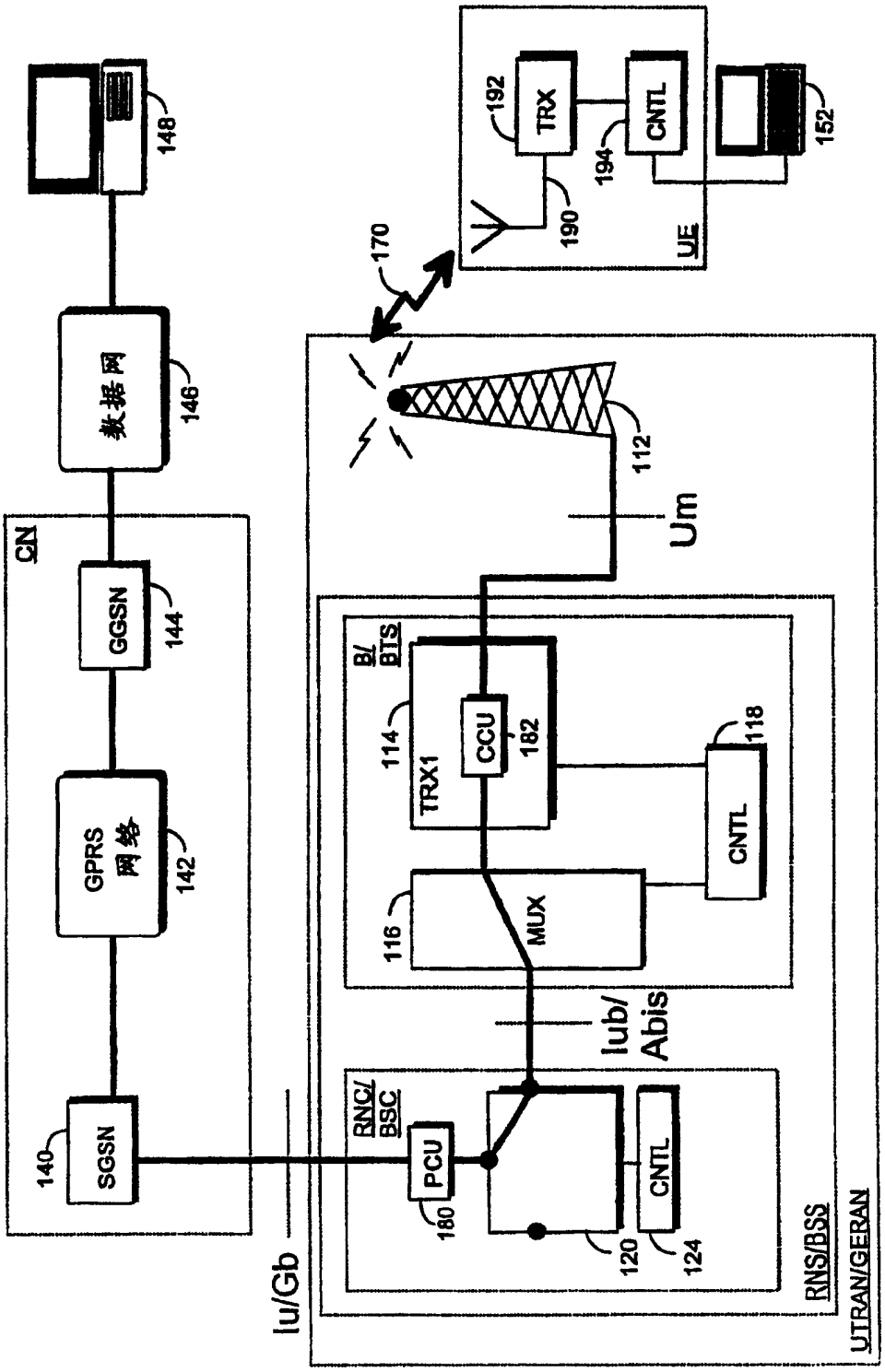

148
数据网
146
GGSN
144
GPRS 网络
142
SGSN
140
CN
Iu/Gb
192
TRX
194
CNTL
190
UE
152
170
112
Um
B/ BTS
114
TRX1
CCU
182
118
CNTL
116
MUX
Iub/ Abis
RNC/ BSC
PCU
180
120
CNTL
124
RNS/BSS
UTRAN/GERAN

图 1D

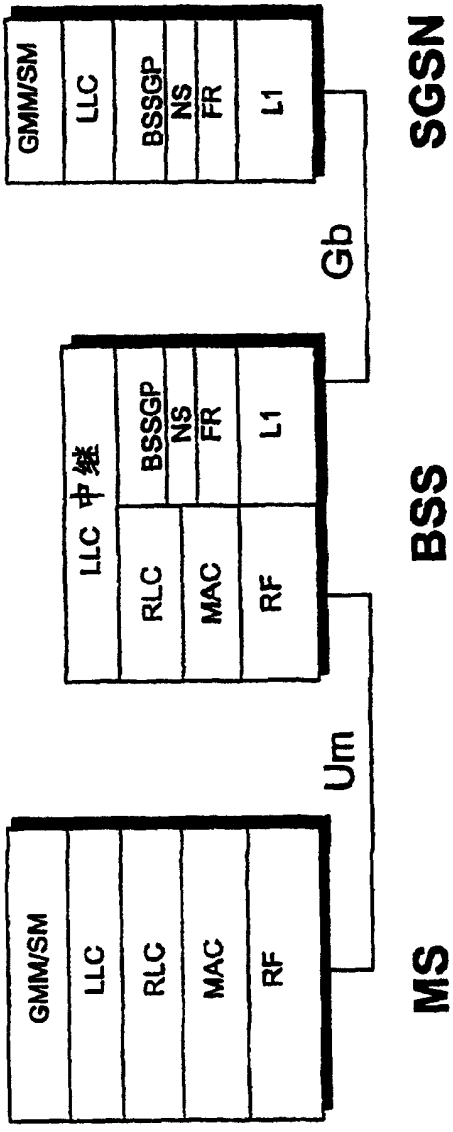

GMM/SM
LLC
RLC
MAC
RF
MS
Um
LLC 中继
BSSGP
NS
FR
L1
RLC
MAC
RF
BSS
Gb
GMM/SM
LLC
BSSGP
NS
FR
L1
SGSN

图 2

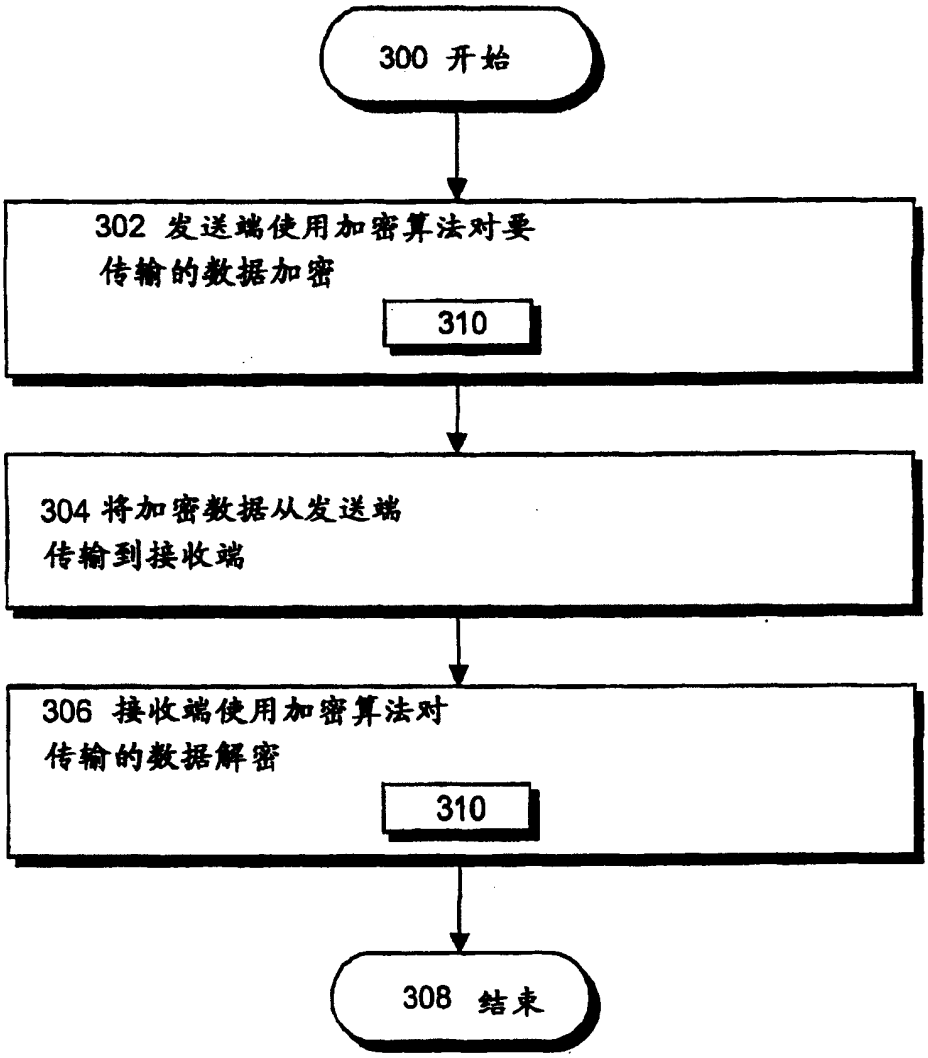

300 开始
302 发送端使用加密算法对要传输的数据加密
310
304 将加密数据从发送端传输到接收端
306 接收端使用加密算法对传输的数据解密
310
308 结束
310 UTRAN加密算法被用作加密算法，在这种情况下基于GERAN操作参数创建约定格式的输入参数

图 3

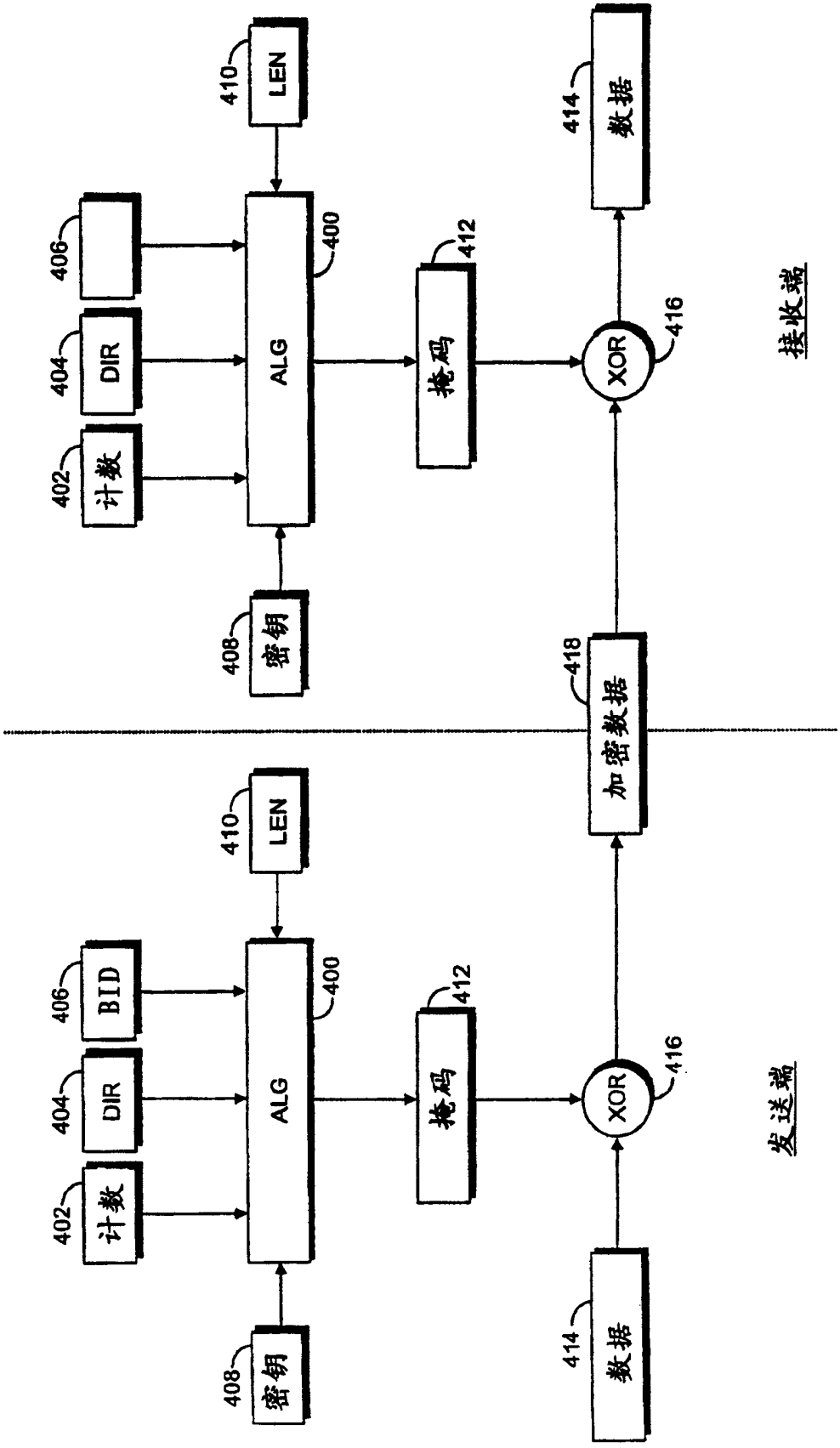

接收端
发送端
402 计数
404 DIR
406
410 LEN
400 ALG
408 密钥
412 掩码
414 数据
416 XOR
418 加密数据
BID

图 4